Freistaat
SACHSEN

Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten

Berichtszeitraum: 1. Januar 2019 bis 31. Dezember 2019

Tätigkeitsbericht
des
Sächsischen Datenschutzbeauftragten
2019

Berichtszeitraum: 1. Januar 2019 bis 31. Dezember 2019

Vorbemerkung zum Sprachgebrauch in diesem Bericht:

Logisch ist zu unterscheiden zwischen biologischem und grammatischem Geschlecht (sexus und genus). Es wäre ein Verlust, diese Unterscheidung aufzugeben; sie erleichtert das Verständnis von Texten und hilft, sich auf das Wesentliche zu konzentrieren. Frauen bitte ich, sich auch von scheinbar männlichen, in Wahrheit nur generellen Bezeichnungen gemeint zu wissen: Bauherr, Lehrer, Beamter, Betroffener etc. (Übrigens gibt es auch den umgekehrten Fall: Der [männliche] Entbindungspfleger ist eine Hebamme i. S. v. § 53 Absatz 1 Nummer 3 StPO.)

Herausgeber: Sächsischer Datenschutzbeauftragter
Andreas Schurig
Devrientstraße 5 Postfach 11 01 32
01067 Dresden 01330 Dresden
Telefon: 0351/85471-100
Fax : 0351/85471-109

Besucheranschrift: Devrientstraße 5
01067 Dresden

Herstellung: Staatsbetrieb Sächsische Informatik Dienste

Bildnachweis
(Motiv auf Umschlagseite): © sdecoret - stock.adobe.com

Vervielfältigung erwünscht.

Inhaltsverzeichnis

1	**Datenschutz im Freistaat Sachsen**	**21**
2	**Grundsätze der Datenverarbeitung**	**24**
2.1	Datenverarbeitungsgrundsätze, Begriffsbestimmungen	24
2.1.1	Abgrenzung der Anwendungsbereiche von DSGVO und Richtlinie (EU) 2016/680	24
2.1.2	Verantwortliche im Bereich der Kultusverwaltung	27
2.1.3	Reichweite des Prinzips der Datenminimierung - Zulässigkeit der Verarbeitung von Daten nicht-anonymisierter Gutachten	28
2.1.4	„iFRAME“-Problematik und die Frage der datenschutzrechtlichen Verantwortlichkeit	29
2.1.5	Nicht rechtsfähiger Verein als Verantwortlicher	30
2.2	Rechtsmäßigkeitsvoraussetzungen der Datenverarbeitung	31
2.2.1	Anforderungen an Webseiten öffentlicher Stellen	31
2.2.2	Die Befugnis zur personenbezogenen Datenverarbeitung bei Ordnungswidrigkeitenanzeigen durch Private	34
2.2.3	Zulässigkeit der Datenverarbeitung mittels elektronischer Wasserzähler	37
2.2.4	Zulässiger Inhalt einer Eingliederungsvereinbarung nach SGB II	37
2.2.5	In Rede stehende unbefugte Übermittlung von Mieterdaten	38
2.2.6	Anforderungen an die Nutzung des Geburtenregisters zu Forschungszwecken und gesetzlich vorgesehene Mitteilung an den Datenschutzbeauftragten	39
2.2.7	Einsichtnahme in Patientenakten zu Forschungszwecken	40

2.2.8 Tonbandaufzeichnungen zur Protokollierung von Stadtrats- und Ausschusssitzungen 42

2.2.9 Übersendung von Versammlungsanzeigen durch Versammlungsbehörden an das Landesamt für Verfassungsschutz 44

2.2.10 Asylbewerberbescheid im Internet 45

2.2.11 Zulässigkeit der Verarbeitung personenbezogener Daten durch Auskunfteien; prinzipiell weitgehend unveränderte Rechtslage, zumeist Artikel 6 I Buchstabe f) DSGVO 46

2.2.12 Personenbezogenen Datenverarbeitung durch Parkraumservice-Gesellschaften 47

2.2.13 Veröffentlichung von Freistellungsbescheinigungen nach § 48b EStG 48

2.2.14 Novellierung des Steuerberatergesetzes – Steuerberater als Verantwortliche 48

2.2.15 Videoüberwachung in Fahrstühlen 49

2.2.16 Der Einbruch im Grünen Gewölbe und durchgeführte Videoüberwachung 50

2.2.17 Offenbarung einer Bewerbung gegenüber dem bisherigen Arbeitgeber 53

2.2.18 Datenweitergabe an Inkassounternehmen 54

2.2.19 Fotografieren von Parkverstößen 56

2.3 Einwilligungsfragen 57

2.3.1 Zweckbestimmung der Datenverarbeitung – Keine Datenverarbeitung ohne konkreten Verarbeitungszweck bei Einwilligungen 57

2.3.2 Fotos beim Neujahrsempfang 58

2.3.3 Datenverarbeitung bei Adoptionsverfahren 60

2.3.4 Verarbeitung sensibler Daten durch einen Lohnsteuerhilfeverein 62

2.3.5 Internet-Gratisangebote mit Werbebezugsklausel - „Service gegen Daten“ 62

2.3.6 Erforderlichkeit der Einholung einer Einwilligung zur Offenlegung von Vergleichsmieten 65

2.4 Sensible Daten, besondere Kategorien personenbezogener Daten 66

2.4.1 Datenzugriff durch Medizinstudenten, Famulanten und Schülern bei Tätigkeit in Arztpraxen 66

2.4.2 Arztpraxisübernahme, An wen darf ein Arzt, der eine Praxis übernommen hat, die Originalunterlagen der Patienten seines Vorgängers herausgeben? 67

2.4.3 Fehlversand einer Arztrechnung - Zustellung einer fremden Rechnung unter kuriosen Umständen 69

3 Betroffenenrechte 71

3.1 Spezifische Pflichten des Verantwortlichen (inklusive Informationspflichten) 71

3.1.1 Informationspflicht bei Videoüberwachung 71

3.2 Auskunftsrecht 75

3.2.1 Auskunft über Melderegisterauskünfte 75

3.2.2 Erst zu beschaffende Informationen sind nicht Gegenstand des Auskunftsanspruchs 75

3.2.3 Zurückbehaltungsrecht und öffentlich-rechtliche Pflichten des Verantwortlichen 76

4 Pflichten Verantwortlicher und Auftragsverarbeiter 78

4.1 Verantwortung für die Verarbeitung, Technikgestaltung 78

4.1.1 Einsatz des Standard-Datenschutzmodells 78

4.1.2 Einsatz von Messengern durch Verantwortliche im dienstlichen und schulischen Umfeld 79

4.1.3 E-Mails mit offenem Verteiler 82

4.1.4 Pflegeheime - Freier Zugang zu Postfächern der Bewohner in Foyer 84

4.1.5 Gewahrsamsaufgabe bei Personalunterlagen 84

4.1.6 Umgang mit personalisierten E-Mail-Adressen bei Ausscheiden von Beschäftigten 85

4.1.7 E-Mail-Nutzung durch Steuerberater 86

4.2 Gemeinsam Verantwortliche 87

4.3 Auftragsverarbeitung 87

4.3.1 Auftragsverarbeitung bei Dentallaboren 87

4.3.2 Verwahrung von Patientenakten durch den Praxisnachfolger - Auftragsverarbeitung oder Verarbeitung durch gemeinsam Verantwortliche 89

4.4 Verzeichnis von Verarbeitungstätigkeiten, Kooperationspflicht mit der Aufsichtsbehörde 90

4.5 Sicherheit der Verarbeitung 90

4.5.1 Handlungspflichten im Hinblick auf den Verlust von Daten und Datenträgern 90

4.6 Meldung von Datenschutzverletzungen 92

4.6.1 Meldung von Datenschutzverletzungen 92

4.6.2 Risikobewertung bei Datenschutzverletzungen 95

4.7 Betroffenenbenachrichtigung 97

4.8 Datenschutz-Folgenabschätzung 97

4.8.1 Datenschutz-Folgenabschätzung mit SDM 97

4.8.2 Projektierung eines einheitlichen Bewerbermanagementverfahrens im Bereich der Staatsverwaltung 99

4.9 Datenschutzbeauftragte 105

4.9.1 Sprachliche Befähigung des Datenschutzbeauftragten 105

4.9.2 Benennung eines Dachverbandes als Datenschutzbeauftragter 105

4.10 Verhaltensregeln und Zertifizierung 106

4.10.1 ISO/IEC 27701 – eine Norm für Datenschutzmanagement 106

4.10.2 Akkreditierungen gemäß Artikel 42, 43 DSGVO 108

5 Internationaler Datenverkehr 109

5.1 Zeichnungserfordernis bei Standardvertragsklauseln 109

5.2 Durchsetzung der DSGVO wegen des räumlichen Anwendungsbereichs gegenüber Verantwortlichen in Drittländern 109

6 Sächsischer Datenschutzbeauftragter - Tätigkeit, Aufgaben, Befugnisse 110

6.1 Zuständigkeit 110

6.1.1 Zuständigkeit des Sächsischen Datenschutzbeauftragten bei Medienunternehmen 110

6.1.2 Zuständigkeit für Konzernniederlassungen 111

6.1.3 Kurioses – Kurz und knapp 112

6.2 Aufgabenbearbeitung im Berichtszeitraum und Statistik 112

6.2.1 Überblick und Arbeitsschwerpunkte 112

6.2.2 Petitionen, Beschwerden, Hinweise 113

6.2.2.1 Videoüberwachung von Nachbargrundstücken und öffentlichen Verkehrsflächen – Was die Aufsichtsbehörde von Beschwerdeführern erwartet 115

6.2.2.2 Darf die Aufsichtsbehörde Petenten über Kamerabetreiber informieren? 117

6.2.2.3 § 29 Absatz 3 Bundesdatenschutzgesetz – Mitwirkung betroffener Personen 119

6.2.3 Beratung 120

6.2.3.1 Jedwede Rechtsberatung für Verantwortliche? 120

6.2.4 Prüfungen - Rechtsetzung, Verwaltungsvorschriften (§ 20 SächsDSDG) 121

6.2.5 Register der benannten Datenschutzbeauftragten 121

6.2.6 Meldungen gemäß Artikel 33 DSGVO, Konsultationen – Artikel 36 DSGVO 122

6.3 Datenschutzaufsichtliche Befugnisse, verwaltungsrechtliche Entscheidungen 123

6.3.1 Überblick zum Berichtszeitraum 123

6.3.2 Akteneinsicht im Aufsichtsverfahren 123

6.4 Geldbußen und Sanktionen, Strafanträge 126

6.4.1 Ordnungswidrigkeitenverfahren im nicht-öffentlichen Bereich 126

6.4.2 Ordnungswidrigkeitenverfahren im öffentlichen Bereich 128

6.5 Öffentlichkeitsarbeit, Internetauftritt und Presse 132

6.6 Vortrags- und Schulungstätigkeit 134

7 Zusammenarbeit der Datenschutzaufsichtsbehörden, Datenschutzkonferenz 135

7.1 Materialien der Datenschutzkonferenz – Entschließungen 135

7.2 Materialien der Datenschutzkonferenz – Beschlüsse 136

7.3 Materialien der Datenschutzkonferenz – Orientierungshilfen 137

7.4 Dokumente des Europäischen Datenschutzausschusses: Leitlinien, Empfehlungen, bewährte Verfahren 138

8 Richtlinienbereich - Richtlinie (EU) 2016/680 und sonstige Bereiche 140

8.1 Unklare Bitte der Polizei an Hotels um Mithilfe 140

8.2 Gesichtserkennung nach neuem Polizeirecht 142

8.3 Datenerhebung einer Justizvollzugsanstalt bei Beantragung von Langzeitbesuch 145

8.4 Videoüberwachung von Hafträumen im sächsischen Justizvollzug 148

8.5 Erhebung von Verkehrsdaten des Anschlusses eines Rechtsanwalts 150

8.6 Abschalten der Videoüberwachung der Chemnitzer Innenstadt bei Versammlungen 154

8.7 Umgang des Landesamtes für Verfassungsschutz mit von Versammlungsbehörden übersandten Versammlungsanzeigen 159

9 Rechtsprechung zum Datenschutz 161

9.1 Das Ende des Videoüberwachungsverbesserungsgesetzes im nicht-öffentlichen Bereich – BVerwG, Urteil vom 27. März 2019, 6 C 2/18 161

9.2 Verwaltungsgerichtliche Entscheidungen in Verfahren unter Beteiligung des Sächsischen Datenschutzbeauftragten 163

9.3 Zur Frage, ob Betriebsräte eigene Verantwortliche gemäß Artikel 4 Nummer 7 DSGVO sind 165

9.4 Verwaltungsaktqualität datenschutzaufsichtlicher Verwarnungen, Artikel 58 Absatz 2 Buchstabe b) DSGVO - Verwarnung als feststellender Verwaltungsakt 167

9.5 Verhältnis der DSGVO zum Kunsturheberrechtsgesetz 167

9.6 Der Umfang des Auskunftsanspruchs gemäß Artikel 15 DSGVO, Landgericht Köln 168

9.7 Datenschutzrechtliche Zulässigkeit eines Ortungssystems im Beschäftigungsverhältnis, VG Lüneburg, Teilurteil vom 19. März 2019, 4 A 12/19 169

9.8 Verdeckte Videoaufnahmen zur Aufdeckung von Missständen in Pflegeheimen 170

9.9 Ansprüche betroffener Personen gegenüber der Aufsichtsbehörde auf konkrete Maßnahmen 170

9.10 Cookies zu Werbezwecken nur mit aktiver Einwilligung – Europäischer Gerichtshof 172

Abkürzungsverzeichnis 13

Sachgebietsregister 17

Abkürzungsverzeichnis

Vorschriften

Nachstehend werden Gesetze und andere Vorschriften nach der alphabetischen Reihenfolge der *amtlichen, in Ausnahmefällen auch nichtamtlichen Abkürzung, ersatzweise der amtlichen Kurzbezeichnung* aufgeführt.

BDSG	in Teil 1 des Tätigkeitsberichts: Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I Satz 66), zuletzt geändert durch Artikel 10 Absatz 2 des Gesetzes vom 31. Oktober 2017 (BGBl. I Satz 3618)
	in Teil 2 des Tätigkeitsberichts: Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 7 des Gesetzes vom 30. Juni 2017 (BGBl. I S. 2097)
BGB	Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Artikel 1 des Gesetzes vom 20. Juli 2017 (BGBl. I S. 2787)
BMG	Bundesmeldegesetz vom 3. Mai 2013 (BGBl. I S. 1084), geändert durch Artikel 11 Absatz 4 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745)
GG	Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 1 des Gesetzes vom 13. Juli 2017 (BGBl. I S. 2347)
OWiG	Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602), zuletzt geändert durch Artikel 5 des Gesetzes vom 27. August 2017 (BGBl. I S. 3297)
SächsDSDG	Sächsisches Datenschutzdurchführungsgesetz vom 26. April 2018 (SächsGVBl. S. 198, 199)
SächsDSG	Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz) vom 25. August 2003

	(SächsGVBl. S. 330), zuletzt geändert durch Artikel 17 des Gesetzes vom 29. April 2015 (SächsGVBl. S. 349)
SächsGemO	Sächsische Gemeindeordnung in der Fassung der Bekanntmachung vom 3. März 2014 (SächsGVBl. S. 146), zuletzt geändert durch Artikel 2 des Gesetzes vom 13. Dezember 2016 (SächsGVBl. S. 652)
SächsPolG	Polizeigesetz des Freistaates Sachsen in der Fassung der Bekanntmachung vom 13. August 1999 (SächsGVBl. S. 466), zuletzt geändert durch Artikel 1 des Gesetzes vom 17. Dezember 2013 (SächsGVBl. S. 890)
SächsPresseG	Sächsisches Gesetz über die Presse vom 3. April 1992 (SächsGVBl. S. 125), zuletzt geändert durch Artikel 2 des Gesetzes vom 17. Dezember 2013 (SächsGVBl. S. 896)
SächsPVDG	Gesetz über die Aufgaben, Befugnisse, Datenverarbeitung und Organisation des Polizeivollzugsdienstes im Freistaat Sachsen vom 11. Mai 2019 (SächsGVBl. 2019 Nummer 9 S. 358)
SächsStVollzG	Sächsisches Strafvollzugsgesetz vom 16. Mai 2013 (SächsGVBl. S. 250)
SächsVerf	Verfassung des Freistaates Sachsen vom 27. Mai 1992 (SächsGVBl. S. 243), zuletzt geändert durch Gesetz vom 11. Juli 2013 (SächsGVBl. S. 502)
SächsVSG	Gesetz über den Verfassungsschutz im Freistaat Sachsen (Sächsisches Verfassungsschutzgesetz) vom 16. Oktober 1992 (SächsGVBl. S. 459), zuletzt geändert durch Artikel 3 des Gesetzes vom 17. Dezember 2013 (SächsGVBl. S. 890)
SGB I	Erstes Buch Sozialgesetzbuch – Allgemeiner Teil – (Artikel I des Gesetzes vom 11. Dezember 1975, BGBl. I S. 3015), zuletzt geändert durch Artikel 5 des Gesetzes vom 14. August 2017 (BGBl. I S. 3214)
SGB X	Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I S. 130), zuletzt geändert durch Artikel 2 Absatz 6 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2739)

StGB	Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Artikel 1 des Gesetzes vom 17. August 2017 (BGBl. I S. 3202)
StPO	Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Artikel 1 des Gesetzes vom 27. August 2017 (BGBl. I S. 3295)
Verordnung (EU) 2016/679 auch: DSGVO	Datenschutz-Grundverordnung – Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG
VwVfG	Verwaltungsverfahrensgesetz in der Fassung der Bekanntmachung vom 23. Januar 2003 (BGBl. I S. 102), zuletzt geändert durch Artikel 11 Absatz 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2752)
ZPO	Zivilprozessordnung in der Fassung der Bekanntmachung vom 5. Dezember 2005 (BGBl. I S. 3202; 2006 I S. 431; 2007 I S. 1781), zuletzt geändert durch Artikel 2 des Gesetzes vom 12. Juli 2018 (BGBl. I S. 1151)

Sonstiges

a. F.	alte Fassung
AG	Arbeitsgruppe
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BSG	Bundessozialgericht
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
BVerwGE	Bundesverwaltungsgerichtsentscheidung

Dakks	Deutsche Akkreditierungsstelle
d. h.	das heißt
etc.	et cetera
EU	Europäische Union
ggf.	gegebenenfalls
i. V. m.	in Verbindung mit
JVA	Justizvollzugsanstalt
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
Rdnr.	Randnummer
SächsABl.	Sächsisches Amtsblatt
SächsGVBl.	Sächsisches Gesetz- und Verordnungsblatt
SVN	Sächsisches Verwaltungsnetz
u. a.	unter anderem
z. B.	zum Beispiel

Verweise im Text auf Ausführungen in früheren Tätigkeitsberichten des Sächsischen Datenschutzbeauftragten sind durch Angabe der Nummer des jeweiligen Tätigkeitsberichtes sowie der jeweiligen Abschnitt-Nummer – getrennt durch einen Schrägstrich – gekennzeichnet (z. B. 4/5.1.2.6).

Sachgebietsregister

** | ausschließlich öffentlicher Bereich – öB*

nicht markiert | nicht-öffentlicher Bereich – nöB bzw. ggfs. auch öffentlicher Bereich - öB/nöB

Verordnung (EU) 2016/697 (DSGVO)	**Fundstelle** *(Ziffern der Gliederung)*
Archivwesen*	
Auftragsverarbeitung	4.3
Beliehene*	
Beschäftigtendatenschutz (inklusive Personalvertretungen*, Betriebsräte, sonstige Vertretungen und Beauftragte)	2.1.2, 2.2.4, 4.1.6, 4.9.1, 7.1 (Nummer 9), 9.3
Betrieblicher Datenschutzbeauftragter, siehe *Datenschutzbeauftragter*	4.9
Betroffenenrechte (Information, Auskunft, Löschung etc.)	3
Bildung und Wissenschaft	
• Hochschulen, Forschungseinrichtungen	2.2.6, 2.2.7, 4.6.2
• Schulen, Schulbehörden*, Bildungseinrichtungen	4.1.2, 4.6.2
• Sonstiges, Allgemeines	2.1.2
Datenschutzbeauftragter	4.9
Datenschutz-Folgenabschätzung	4.8
Dashcam, siehe Videografie	
E-Government*	
Einwilligung	2.2, 2.3, 9.10
Freie Berufe, siehe ggfs. auch Gesundheitswesen	
• Rechtsanwälte	
• Notare	
• Steuerberater, Wirtschaftsprüfer	2.2.14, 2.3.4, 3.2.3, 4.1.7
• Architekten, Ingenieure	
• Sonstiges, Allgemeines	
Gemeinsam Verantwortliche	4.2
Gesundheitswesen	
• Behördliche Aufsicht und Überwachung*	
• Krankenhäuser	2.2.7, 7.3 (Nummer 1)
• Pflegedienste	

Verordnung (EU) 2016/697 (DSGVO)	**Fundstelle** *(Ziffern der Gliederung)*
• Apotheker	
• Ärzte	2.4.1, 4.3.2
• Heilberufe	
• Sonstiges, Allgemeines	
Fachverwaltung (z. B. Bauverwaltung, Ausländerbehörden), siehe ggfs. *Registerbehörden*	
Finanz-, Steuer- und Fördermittelverwaltung (inklusive kommunale Stellen)*	2.2.13, 2.3.4
Gerichtsvollzieher*	
Handel, Dienstleistungen, Gewerbe, Industrie	
• Auskunfteien und Detekteien	2.2.11
• Banken, Finanzwirtschaft	
• Handel, siehe auch *Internet/E-Commerce*	4.5.1
• Handwerk, Industrie	2.1.3
• Hotel und Gastronomie, Freizeit, Tourismus, Sport	8.1, 9.2, 9.1
• Versicherungen	
• Werbung, Markt- und Meinungsforschung	2.2.1, 2.3.5, 7.2 (Nummern 2 und 4)
• Sonstiges, Allgemeines	2.2.12
Infrastruktureller Sektor	
• Energie- und Versorgungswirtschaft	2.2.3
• Verkehrs- und Beförderungswesen	3.1.1, 8.5, 9.1
• Wohnungswirtschaft, Immobilienverwaltung	2.2.5, 2.2.15, 2.3.6, 4.9.2
• Sonstiges, Allgemeines	
Internet	
• Allgemeines	
• E-Commerce	
• Social Media, Telemedien	2.2.1, 7.3 (Nummer 3)
• Sonstiges, Allgemeines	
Kammern, berufsständische Körperschaften des öffentlichen Rechts*	2.1.3, 4.3.1
Kommunale Selbstverwaltung*, siehe ggfs. *Fachverwaltung*, siehe ggfs. *Registerbehörden,* siehe ggfs. *Finanzverwaltung*	2.1.1, 2.2.5, 2.2.8, 2.2.9, 2.3.2, 3.2.1, 8.6

Verordnung (EU) 2016/697 (DSGVO)	**Fundstelle** *(Ziffern der Gliederung)*
Ordnungswidrigkeiten – Sächsischer Datenschutzbeauftragter	6.4
Sächsischer Landtag als Verwaltung*	
Rechnungshof*	
Registerbehörden (u. a. Melderecht, Personenstandswesen)*	3.2.1
Religionsgemeinschaften	
Sächsischer Datenschutzbeauftragter	6
Schule, siehe *Bildung und Wissenschaft*	
Sensible Daten, Artikel 9 DSGVO	2.4, 8.6
Sicherheit der Verarbeitung	4.5
Sozialwesen	
• Soziale Leistungserbringer	
• Kindertagesstätten	
• Sonstiges, Allgemeines	2.3.3
Statistikwesen*	
Technische und organisatorische Maßnahmen	4
Telekommunikation	
Vereine (auch Parteien), Verbände, Stiftungen	2.1.4, 2.1.5, 2.3.4, 4.5.1, 4.9.2, 9.4, 9.10
Verkehrswesen	
Verzeichnis von Verarbeitungstätigkeiten	
Videografie, Video- und Bildüberwachung	
• Behördliche Überwachung*	2.2.16, 8.2, 8.4, 8.6
• Beschäftigte, vgl. ansonsten *Beschäftigtendatenverarbeitung*	9.8
• Dashcam	
• Handel, Gewerbe	
• Sonstiges, Allgemeines	2.2.2, 2.2.15, 3.1.1, 6.4.1, 6.2.2.2, 7.3 (Nummer 7 und 9), 9.1
Wahlrecht*	
Zertifizierung	4.10

Richtlinie (EU) 2016/680 (Strafverfolgung, Polizei, Justiz)	
Polizei*	8.1, 8.2, 8.6
Ordnungswidrigkeitenbehörden*	2.1.1
Strafverfolgung*	8.5
Strafvollzug*	8.3, 8.3, 8.4
Sonstige Bereiche außerhalb Verordnung 2016/697 und Richtlinie EU 2016/680	
Sächsischer Landtag als Parlament	
Verfassungsschutz	8.7
Weitere datenverarbeitende Stellen	

1 Datenschutz im Freistaat Sachsen

„Nous sommes dans un siècle où l'obscurité protège mieux que la loi,
et rassure plus que l'innocence."

„Wir leben in einem Jahrhundert, in dem die Anonymität besser als das Gesetz schützt
und stärker als die Unschuld beruhigt."

(Antoine de Rivarol (1753-1801) im endenden 18. Jahrhundert in den Zeiten der französischen Revolution)

Der vorstehende Satz des französischen Schriftstellers de Rivarol war unter dem Eindruck politischer Umwälzungen und der Verfolgung politischer Andersdenkender entstanden. Wir leben in einer anderen Zeit, einer Zeit, in der die Informationsgesellschaft vielfache Bequemlichkeit und praktische Vorzüge bietet, und in der ein Rechtsrahmen existiert, der die Würde des Menschen und seine Grundrechte garantiert. Doch angesichts von persönlichkeitsrechtlichen Gefährdungen und Fehlentwicklungen, in der Menschen sich weltweit vernetzen und private Lebensinhalte über soziale Netzwerke publizieren, nicht selten an den Pranger gestellt oder medial stigmatisiert werden, umgeben von einem Umfeld, das nichts vergisst, wirkt derselbe Satz wie eine Mahnung, die durchaus auch heute noch Bedeutung hat. Hinzu kommt die ohnehin immer lückenlosere Datenverarbeitung des Staates und des nicht-öffentlichen Sektors, denen der Bürger nicht-willentlich ausgesetzt ist. Kann der Einzelne in der heutigen Gesellschaft noch seine Anonymität und Freiheit bewahren? Bleibt er als Individuum Herr seiner Daten?

Wer sich mit dem digitalen Fortschritt befasst und Informationsverarbeitung bejaht, beschäftigt sich auch mit deren Grenzen. Und die Befürworter einer weitgehenden personenbezogenen Datenverarbeitung durch Staat und Wirtschaft haben sich auch ethischer und ordnungspolitischer Kritik zu stellen. Das Bundesverfassungsgericht hat den Begriff der „Selbstbestimmung" bei seiner wegweisenden Entscheidung zur Volkszählung im Jahre 1983 bei der Benennung des „informationellen Selbstbestimmungsrechts" verwendet. Die Wortbedeutung erfasst den Sinngehalt des Datenschutzes in präziser Weise,

wenn man die gegenteilige Bedeutung betrachtet, die „Fremdbestimmung“. Und nur so erschließt sich in der Vorstellung auch der menschenrechtliche Gedanke, der dem Grundrecht innewohnt. Für die freiheitliche Gesellschaft ist die Frage insoweit auch immer eine Schicksalsfrage.

Richtet man den Blick auf die Diskussionen um zukünftige Technologien, wiederholt sich der Widerstreit bei fortschrittlichen Interessen seitens des Staates und der Wirtschaft mit dem grundgesetzlichen Bedürfnis auf Selbstbestimmung des Einzelnen immer wieder. Er ist (natürlich) auch ein essentieller Aspekt um Vorstellungen zur künstlichen Intelligenz, als Teilgebiet der Informatik. Die Automatisierung intelligenten Verhaltens und maschinellen Lernens, insbesondere der Einsatz von relationalen Datenbanken, die den Einzelnen in seinen Lebensverhältnissen und in vielfältigen Bezügen abzubilden in der Lage sind, schafft Transparenz für die Datenverarbeiter, den Staat, Auskunfteien und werbende Unternehmen. Gleichsam gegenläufig stehen dem Einzelnen nicht selten Großorganisationen gegenüber und die tatsächlichen Verarbeitungsprozesse entziehen sich den betroffenen Personen immer mehr einem tieferen Verständnis. Wir befinden uns insoweit auch in einer Phase der digitalen Entfremdung. Seit der Anwendbarkeit der DSGVO habe ich in meiner Aufsichtstätigkeit die Erfahrung gemacht, dass auch die Gruppe der informatikaffinen und datenschutzwilligen Menschen nicht mehr zu überblicken vermag, welche Verarbeitungsprozesse und Datenflüsse mittels der von ihnen genutzten und eingesetzten Produkte und Dienste tatsächlich erfolgen und ausgelöst werden. Bei digitalen Diensten und Produkten gibt es zudem ein immer größeres Machtgefälle zwischen Anbietern und Nutzern. Der Anwender ist abhängig und muss akzeptieren, was ihm Dienstleister und Unternehmen anbieten und abverlangen. Wie kann bei dieser Entwicklung digitale Souveränität tatsächlich gesichert werden? Was kann und muss der Staat als Regulierer leisten? Welche Kriterien müssen Anbieter erfüllen? Wie kann man Anwender unterstützen? Wie können die Datenschutzaufsichtsbehörden auf die Verantwortlichen einwirken, dass diese den Nutzern durch Transparenz, Maßnahmen der und die Prinzipien „privacy by default“ und privacy by design“ Einsicht in die Prozesse und Entscheidungsfindung erleichtern?

Selbstbestimmung in seiner reinen Form ist in einer komplexen Gesellschaft unmöglich. Menschen sind als soziale Wesen immer zugleich auch fremdbestimmt, nicht nur in Bezug auf den Staat und dessen Gesetze, sondern auch in ihren gesellschaftlichen Zusammenhängen. Wo verlaufen die informationellen Grenzen für den Staat und die datenver-

arbeitende Wirtschaft, um in der globalen Konkurrenz und Moderne noch zu funktionieren, dem Einzelnen aber nicht zu viel abzuverlangen? Welche Datenverarbeitungsmaßnahmen zur Effektivierung im Gesundheitswesen sind noch verträglich? Die Fragen führen zu der immer wieder gleichen Frage der Selbstbestimmung zurück: Wann und inwieweit ist die Würde des Menschen durch die Eingriffe berührt?

Diese Kernfrage ist Maßstab des Handelns meiner Behörde.

2 Grundsätze der Datenverarbeitung

2.1 Datenverarbeitungsgrundsätze, Begriffsbestimmungen

2.1.1 Abgrenzung der Anwendungsbereiche von DSGVO und Richtlinie (EU) 2016/680

Mit der unmittelbaren Anwendbarkeit der DSGVO am 25. Mai 2018 und der Ausnahme ihrer Anwendung auf die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit (Artikel 2 Absatz 2 Buchstabe d) DSGVO) - die EU-rechtliche Regelung zur Verarbeitung personenbezogener Daten in diesem Bereich findet sich in der Richtlinie (EU) 2016/680 - stellte sich die Frage der Abgrenzung der Anwendungsbereiche von DSGVO und Richtlinie.

Nachdem sich die Auffassung durchgesetzt hatte, dass auch Ordnungswidrigkeiten nach deutschem Recht unter den europarechtlichen, in DSGVO und Richtlinie verwandten Begriff der "Straftaten" zu subsumieren sind und somit in den Anwendungsbereich der Richtlinie fallen, wurde klar, dass nicht nur Strafverfolgungsbehörden und der Polizeivollzugsdienst, sondern auch kommunale und sonstige Behörden, die Ordnungswidrigkeiten verfolgen, insoweit mangels Anwendbarkeit nicht die Vorschriften der DSGVO, sondern diejenigen nationalen und landesrechtlichen Vorschriften zu beachten haben, mit denen die Richtlinie umgesetzt wurde.

Insbesondere kommunale Ordnungswidrigkeitenbehörden sahen sich mit einem Abgrenzungsproblem konfrontiert, das nicht selten als ebenso so künstlich wie sachfremd empfunden wurde, was vor allem daraus resultierte, dass Kommunen als "Bündelungsbehörden" verschiedenste Zuständigkeiten haben und unterschiedlichste gesetzliche Aufgaben erfüllen - nicht selten in engen organisatorischen und personellen Zusammenhängen und Überschneidungen. Es konnte insofern zunächst durchaus als besondere zusätzliche Belastung gesehen werden, sich neben all den Veränderungen, die die DSGVO mit sich brachte, nun auch damit arrangieren zu müssen, dass ein (kleiner) Bereich der vielfältigen Verwaltungstätigkeit gerade nicht in deren Anwendungsbereich fallen sollte.

Das Bundesministeriums des Innern, für Bau und Heimat (BMI) erstellte am 4. Januar 2019 ein Papier zur Abgrenzung der Anwendungsbereiche von DSGVO und Richtlinie, das dessen in Übereinstimmung mit der Auffassung des Bundesministeriums der Justiz

und für Verbraucherschutz befindliche Position in dieser Frage wiedergibt (im Folgenden: BMI-Papier) und mittlerweile bundesweit, d.h. auch bei Kommunen und Landkreisen, bekannt sein dürfte.

Nach dem BMI-Papier umfasst der Anwendungsbereich der Richtlinie nur die straftatenbezogene Gefahrenabwehr durch die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten zuständigen Behörden. Die Verarbeitung personenbezogener Daten durch die Polizei oder die Ordnungsbehörden im Rahmen der nicht straftatenbezogenen Gefahrenabwehr unterlägen hingegen dem Anwendungsbereich der DSGVO. Datenverarbeitungen zum Zwecke der Gefahrenabwehr, die dem Datenschutzregime der DSGVO unterliegen, fielen (erst) dann in den Anwendungsbereich der Richtlinie, wenn das von den zuständigen Behörden (Polizei- oder Ordnungsbehörden) geführte Verfahren in ein konkretes Ordnungswidrigkeitenverfahren übergehe. Für den Übergang vom Verwaltungsverfahren in das Ordnungswidrigkeitenverfahren sei darauf abzustellen, ob die jeweilige Behörde ihre Maßnahmen auf das Verwaltungsverfahrensgesetz oder das Gesetz über Ordnungswidrigkeiten (OWiG) stütze. Datenschutzrechtlich finde mit dem Übergang in das Ordnungswidrigkeitenverfahren die Richtlinie und damit auch Teil 3 des Bundesdatenschutzgesetzes (BDSG 2018) bzw. das OWiG Anwendung.

Die im BMI-Papier vorgenommene Abgrenzung führt zu einem relativ einfachen, übersichtlichen und vor allem praktikablen Prüfschema für gefahrenabwehrend tätige Polizei- und Ordnungsbehörden:

- straftatenverhütende Gefahrenabwehr durch den Polizeivollzugsdienst (PVD) erfolgt im Anwendungsbereich der Richtlinie (und damit des SächsDSUG);

- sonstige gefahrenabwehrende Tätigkeit des PVD sowie die gefahrenabwehrende Tätigkeit der allgemeinen Polizei- und Ordnungsbehörden fallen in den Anwendungsbereich der DSGVO;

- nicht straftatenverhütende Gefahrenabwehr des PVD sowie der allgemeinen Polizei- und Ordnungsbehörden „wechselt" vom Anwendungsbereich der DSGVO in den der Richtlinie (d.h. in den 3. Teil des BDSG bzw. in den des SächsDSUG), sobald ein konkretes Ordnungswidrigkeitenverfahren eröffnet wird.

Trotz einiger dogmatischer Unklarheiten wird damit ein rechtlich gut vertretbarer und vor allem praktikabler Weg zur Abgrenzung zwischen DSGVO und Richtlinie gewiesen, der auch im Freistaat Sachsen beschritten werden kann.

§ 45 BDSG, der den Anwendungsbereich von Teil 3 des BDSG bestimmt und auf dessen Wortlaut und Begründung sich die im BMI-Papier vorgenommene Abgrenzung ganz wesentlich stützt, ist in seinen ersten drei Sätzen mit § 1 Absatz 1 des Sächsischen Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 (Sächsisches Datenschutz-Umsetzungsgesetz – SächsDSUG) identisch. § 45 Satz 3 BDSG nimmt in der Argumentation im BMI-Papier eine zentrale Rolle ein, er findet sich wortgleich in § 1 Absatz 1 Satz 3 SächsDSUG: „Die Verhütung von Straftaten im Sinne des Satzes 1 umfasst den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit."

Insoweit gilt die Feststellung der Begrenzung des in den Anwendungsbereich der Richtlinie fallenden Teils der Gefahrenabwehr auf die straftatenverhütende Abwehr von Gefahren für die öffentliche Sicherheit gleichermaßen für den Freistaat und die hiesigen gesetzlichen Umsetzungsregelungen in § 1 Absatz 1 Sätze 1 und 3 SächsDSUG.

Der ganz überwiegende Teil gefahrenabwehrender Tätigkeiten – hierin liegt ein Schwerpunkt der Aufgaben der Kommunen als allgemeine Polizeibehörden (sei es im Waffenrecht, Baurecht, Versammlungsrecht und sonst überall dort, wo Genehmigungsverfahren, Auflagen, Anordnungen der Abwehr von Gefahren dienen) – ist nicht "straftatenbezogen", er dient nicht der Verhütung von Straftaten. Kommunen (Ortspolizeibehörden) wehren allgemeine und konkrete Gefahren ab; die Abwehr von Gefahren für die öffentliche Sicherheit durch die Verhütung von Straftaten ist Aufgabe des Polizeivollzugsdienstes (§ 2 Absatz 1 Satz 3 SächsPVDG).

Für Gemeinden, Landkreise und Kreisfreie Städte gestaltet sich die Abgrenzung der Anwendungsbereiche von DSGVO und Richtlinie damit relativ klar: gefahrenabwehrende Tätigkeiten ihrer Ämter und Behörden, ganz gleich, ob „Fachbehörden", „Polizeibehörden" oder sonstige „allgemeine" Ämter/Behörden, fällt in den Anwendungsbereich der DSGVO, die Verarbeitung personenbezogener Daten zur Verfolgung und Ahndung von Ordnungswidrigkeiten folgt – soweit das OWiG und die Strafprozessordnung keine vorrangigen speziellen Rechtsvorschriften enthalten – den datenschutzrechtlichen Regelungen im 3. Teils des BDSG bzw. im SächsDSUG.

Neben der Einfachheit der Abgrenzung resultiert daraus, dass allein die Organisationseinheit, die Bußgeldverfahren durchführt, ihre Datenverarbeitung an den Vorgaben des 3. Teils des BDSG bzw. des SächsDSUG auszurichten hat.

Wesentliche Änderungen der Verwaltungspraxis dürften damit nicht verbunden sein. Auch bisher wurden Maßnahmen zur Gefahrenabwehr (Genehmigungen, Anordnungen,

Untersagungen) auf Fachgesetze des besonderen Verwaltungsrechts oder Normen des Verwaltungsverfahrensgesetzes gestützt; mit der Einleitung von Bußgeldverfahren kamen OWiG und in entsprechender Anwendung die Strafprozessordnung zur Anwendung. Neu ist allerdings, dass nicht mehr das SächsDSG als ein allgemeines Datenschutzgesetz für alle öffentlichen sächsischen Stellen unabhängig von ihrer Tätigkeit einschlägig ist, sondern für den Anwendungsbereich der DSGVO die DSGVO selbst und ergänzend das SächsDSDG und für den Anwendungsbereich der Richtlinie der 3. Teil des BDSG (festgelegt durch § 500 StPO) und subsidiär das SächsDSUG Anwendung finden. Inhaltlich wiederum ist der ganz überwiegende Teil der jeweiligen Vorschriften nahezu identisch.

2.1.2 Verantwortliche im Bereich der Kultusverwaltung

In meinem letzten Tätigkeitsbericht hatte ich mich unter 2.1.1 wegen mehrfacher Nachfragen dahingehend festgelegt, dass Betriebsräte und Personalvertretungen keine eigenen Verantwortlichen sind, sondern dem jeweiligen Unternehmen bzw. der öffentlichen Stelle zuzuordnen sind. Dies bedeutet zum einen, dass diese keinen eigenen Datenschutzbeauftragten benennen müssen, zum anderen aber durch denjenigen des Verantwortlichen kontrolliert werden können.

Zahlreiche Anfragen erreichten mich auch zur Verantwortlichkeit und damit zur Pflicht zur Bestellung eines Datenschutzbeauftragten im Bereich der Kultusverwaltung. Hier gilt Entsprechendes.

Bei den Eltern- und Schülerräten an Schulen sind letztere die Verantwortlichen. Es müssen daher auch durch die Eltern- und Schülervertretungen keine Datenschutzbeauftragten benannt werden. Gleiches gilt für die regionalen Vertretungen, namentlich den Kreiselternrat, den Landeselternrat, den Kreisschülerrat sowie den Landesschülerrat. Nach der Auffassung des Sächsischen Staatsministeriums für Kultus, die ich für vertretbar und sachgerecht halte, ist auf Kreis- und auf Landesebene das Landesamt für Schule und Bildung Verantwortlicher. Hierfür sprechen die sowohl in der Schülermitwirkungsverordnung als auch in der Elternmitwirkungsverordnung geregelten Vorlage-, Genehmigungs- und Unterstützungspflichten.

2.1.3 Reichweite des Prinzips der Datenminimierung - Zulässigkeit der Verarbeitung von Daten nicht-anonymisierter Gutachten

Ein öffentlich bestellter und vereidigter Sachverständiger für das Sachgebiet Bewertung von bebauten und unbebauten Grundstücken beschwerte sich darüber, dass er von einer sächsischen IHK aufgefordert wurde, den Mitgliedern des Sachverständigenausschusses der IHK zwei Wertgutachten vorzulegen. Der Aufforderung kam der Petent dadurch nach, dass er dem Ausschuss anonymisierte Gutachten übersandte. Wegen der Anonymisierung wurden diese Gutachten, so die Aussage des Petenten, von der IHK als schwer verständlich, nicht nachvollziehbar und nicht verwertbar abgelehnt, verbunden mit der Forderung, nach 30 Jahren Tätigkeit als Sachverständiger die öffentlichen Bestellung zurückzugeben.

Ich habe mich zu der datenschutzrechtlichen Frage betreffend das Abfordern ungeschwärzter Unterlagen wie folgt geäußert:

Die Sachverständigenordnung der betreffenden Industrie- und Handelskammer (kurz: Ordnung) regelt die Voraussetzungen für die öffentliche Bestellung und stellt insoweit eine Rechtsgrundlage für die Rechtmäßigkeit der Verarbeitung nach Artikel 6 DSGVO dar.

Die Sachverständigenordnung regelt nach § 20 dieser Ordnung Auskunftspflichten sowie die Pflicht zur Überlassung von Unterlagen. Der Sachverständige hat danach auf Verlangen der Industrie und Handelskammer die zur Überwachung seiner Tätigkeit und der Einhaltung seiner Pflichten sowie zur Prüfung seiner Eignung erforderlichen mündlichen oder schriftlichen Auskünfte innerhalb der gesetzten Frist und unentgeltlich zu erteilen und angeforderte Unterlagen vorzulegen. Er kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen seiner Angehörigen (§ 52 Strafprozessordnung) der Gefahr strafrechtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde.

Der Sachverständige hat auf Verlangen der Industrie und Handelskammer die aufbewahrungspflichtigen Unterlagen (siehe hierzu § 14 der Ordnung) in deren Räumen vorzulegen und angemessene Zeit zu überlassen.

Die Schweigepflicht des Sachverständigen erstreckt sich ausdrücklich gemäß § 16 der Ordnung nicht auf die Anzeige- und Auskunftspflichten nach §§ 19 und 20 der Ordnung. Die Ordnung sieht keine Anonymisierung der einzureichenden Unterlagen vor.

2.1.4 „iFRAME“-Problematik und die Frage der datenschutzrechtlichen Verantwortlichkeit

Im letzten Berichtszeitraum wandten sich an Privatpersonen und eine Gewerkschaft an meine Behörde und beschwerten sich über eine Internetpräsenz mit Sitz in Sachsen. Auf deren Webseite seien, so der Hinweis, personenbezogene Informationen, einer sehr großen Anzahl von Unterstützern gegen eine politische Partei mit deren Vor- und Zunamen, Gemeindeangaben und ihren beruflichen Funktionen publiziert worden. Die Beschwerdeführer waren, da es sich um einen journalistischen Auftritt handelte, auf meine beschränkte sachliche Zuständigkeit gemäß § 11 a Satz 4 Sächsisches Gesetz über die Presse hinzuweisen, vergleiche zur eingeschränkten sachlichen Zuständigkeit meiner Behörde auch den Beitrag unter 4.1.1.

Allerdings stellte sich aufgrund meiner vorsorglich durchgeführten Nachfrage bei dem Verantwortlichen allerdings auch heraus, dass die journalistische Seite auf eine Seite eines aktionistischen Vereins mit Sitz in Berlin verlinkt hatte. Auf dessen Seite wiederum waren auch zum Zeitpunkt meiner Befassung ein Erhebungsformular, bei dem Vorname, Nachname, Postleitzahl, Ort obligatorisch und die Angabe einer zugehörigen Organisation und Funktion freiwillig eingetragen und per Webformular abgesandt werden konnte, abrufbar gewesen. Die Verantwortlichen der sächsischen Interpräsenz gaben wiederum an, dass die Daten und Listen lediglich mittels "IFRAME" dargestellt worden seien, diese mithin auf dem Server der benannten Vereinigung zum Abrufen verblieben waren, ohne dass sich die personenbezogenen Daten auf einem Server oder einem Datenträger der journalistischen Vereinigung gefunden hätten. Der Verantwortliche versicherte zudem, dass von der öffentlichen Datenbank zu keinem Zeitpunkt eine lokale Kopie erstellt und auf den eigenen Rechnern gespeichert worden sei. Soweit diese Angaben so zugetroffen haben, wäre nach meiner Einschätzung nicht die journalistische Vereinigung primär als Verantwortlicher anzusehen gewesen, sondern der von dieser benannte Verein.

Die journalistische Vereinigung berichtete weiter, dass nachdem andere Medien auf die Veröffentlichung auf der Internetpräsenz aufmerksam gemacht hätten, auch die Daten verarbeitende Stelle, der Verein mit Sitz in Berlin darauf aufmerksam gemacht worden

sei, dass eine öffentlich zugängliche Datenbank in dem Pressebeitrag verlinkt worden sei. Betroffene Personen, die die journalistischen Vereinigung kontaktiert hätten oder sich an diverse Zeitungen gewandt hätten, hätten demnach nicht gewusst, dass sie mit der Eingabe ihrer Daten auf der Webseite des Betreibers des Vereins einer Veröffentlichung unwissentlich zugestimmt hätten. Betroffenen Personen hatte die journalistische Vereinigung gegenüber erklärt, dass man zu keinem Zeitpunkt eine Liste erstellt habe und an den Betreiber der Vereinsplattform verwiesen. Daraufhin seien die Liste „offline" genommen worden. Gleichzeitig sei damit auch die Liste über die eigene Webseite nicht mehr per Anfrage erreichbar gewesen. Die journalistische Vereinigung reklamiert für sich, dass sie letztendlich durch ihre Veröffentlichung auf das Datenleck aufmerksam gemacht und dazu beigetragen habe, dass die Veröffentlichung im Internet eingestellt worden sei. Nach Erkenntnis der journalistischen Vereinigung standen die personenbezogenen Daten dabei wohl bereits mehrere Jahre im Internet öffentlich abrufbar bereit.

Nach dieser Darstellung, die mir schlüssig erschien, verwies ich die Beschwerdeführer an den von der journalistischen Vereinigung benannten eingetragenen Verein sowie an die Berliner Beauftragte für Datenschutz und Informationsfreiheit. Mit der Frage, ob der Betreiber einer Website, der in diese Internetpräsenz ein Plugin einbindet, ebenso als für die Verarbeitung Verantwortlicher im Sinne der DSGVO angesehen werden konnte, hatte ich mich aufgrund der sachlichen Unzuständigkeit gemäß § 11 a Satz 4 Sächsisches Gesetz über die Presse nicht weiter zu auseinanderzusetzen gehabt, vergleiche Urteil des Europäischen Gerichtshofs in der Rechtssache in der Rechtssache C 40/17, Randnummern 64 ff.

2.1.5 Nicht rechtsfähiger Verein als Verantwortlicher

In einer meinerseits zu erarbeiten Beschwerde gegen eine Wählervereinigung, die nicht als eingetragener Verein organisiert war, wandte sich eine betroffene Person gegen eine erfolgte Verarbeitung im Wege einer E-Mail-Kommunikation. Zwischenzeitlich war die Wählervereinigung umorganisiert worden. Insoweit ergab sich die Schwierigkeit, den Verantwortlichen anzusprechen.

Grundsätzlich lässt sich folgendes feststellen: Auch nicht rechtsfähige Vereine sind Träger von Rechten und Pflichten. Und auch sie stellen ein eigenes Rechtssubjekt dar, auch wenn sie nicht ausdrücklich als Rechtsinstitut im Bürgerlichen Gesetzbuch aufgeführt sind. Die Rechtsverhältnisse, die für die Gesellschaft bürgerlichen Rechts als Trägerin

von Rechten und Pflichten gelten, gelten auch für den nichtrechtsfähigen Verein. Nach der jüngeren Rechtsprechung ist der nichtrechtsfähige Verein auch aktiv und passiv parteifähig, was Berücksichtigung in der Zivilprozessordnung gefunden hat, § 50 Absatz 2 Zivilprozessordnung. Allerdings gelten die Haftungsbedingungen der Gesellschaft bürgerlichen Rechts nicht für den nichtrechtsfähigen Verein. Deliktisch wird § 31 Bürgerliches Gesetzbuch entsprechend angewandt, wodurch eine Haftung des Vereins und nicht seiner Mitglieder begründet wird, §§ 823 ff. bzw. 831 Bürgerliches Gesetzbuch.

In Würdigung der Rechtslage wendet sich meine Behörde datenschutzaufsichtlichen Angelegenheiten wie bei der Inanspruchnahme von Störern an die in Erscheinung getretene bzw. handelnde (Daten verarbeitende) Person des Vereins, des Verantwortlichen, als Adressaten. Sollen aus dessen Sicht wiederum andere Personen des Vereins datenschutzaufsichtlich adressiert werden, ist meine Behörde auf entsprechende Mitwirkung bzw. Hinweise angewiesen.

2.2 Rechtsmäßigkeitsvoraussetzungen der Datenverarbeitung

2.2.1 Anforderungen an Webseiten öffentlicher Stellen

Regelmäßig erreichen mich Beschwerden von Bürgern, die sich die Webauftritte ihrer Gemeinde oder anderer öffentlicher Stellen einmal näher angeschaut haben. Und oft sind die Beschwerden berechtigt und die Stellen müssen ihre Webauftritte an die datenschutzrechtlichen Vorschriften anpassen. Doch was ist erlaubt und was ist verboten, welche Maßstäbe gelten und wie kann eine öffentliche Stelle einen modernen Webauftritt ohne Verstöße gegen den Datenschutz realisieren?

Die Datenschutzkonferenz hat im März 2019 die Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien (OH Telemedien) verabschiedet, welche die Rechtsgrundlagen für private Datenverbeiter bei der Gestaltung von Webseiten enthält. Im Wesentlichen geht es um die Grenze der Rechtsgrundlage des Artikel 6 Absatz 1 Buchstabe f) DSGVO, das berechtigte Interesse des Datenverarbeiters. Im Internet wird von vielen Webseitenbetreibern oft pauschal auf ein solches berechtigtes Interesse verwiesen und damit jegliche Werbung, Tracking und Einbindung von Drittanbietern legitimiert. Dass diese dritten Parteien die aufgrund der Einbindung gewonnenen Daten für eigene, in aller Regel kommerzielle Zwecke verwenden, wird dabei geflissentlich ignoriert. Als prominentes Beispiel sei an die Einbindung von Facebook in Form des Teilen- oder Gefälltmir-Buttons auf Webseiten erinnert. Facebook erhält so Zugriff auf sämtliche Daten der

Webseitenbesucher, die auch der Betreiber der Webseite erhält, kann also sehr genau nachvollziehen, was ein Besucher auf der jeweiligen Seite tut. Zusätzlich werden die IP-Adresse und weitere spezifische Daten des Endgeräts des Nutzers (Browserdaten mit Rückschlüssen auf das verwendete Gerät) übertragen. Facebook kann diese Daten mit Hilfe von Zusatzinformationen (ist der Nutzer zum Zeitpunkt der Übertragung Mitglied bei Facebook oder nicht?) zu Profilen verarbeiten, die umso aussagekräftiger werden, je öfter der Mechanismus auf verschiedenen Webseiten greift. Dieses seitenübergreifende Tracking, also die Nachverfolgung und das zielgerichtete Sammeln von Informationen über das Verhalten von Einzelnen, stellen ein hohes Risiko für Rechte und Freiheiten natürlicher Personen dar, zumal diese Mechanismen sich alle Mühe geben möglichst unbemerkt Daten zu sammeln. Auch der Webseitenbetreiber, der Dienste von Dritten einbindet, steht daher in der Mitverantwortung.

Ein geltend gemachtes berechtigtes Interesse ist daher immer einer Interessenabwägung mit den Risiken für Rechte und Freiheiten natürlicher Personen zu unterziehen. Sobald ein Dritter Daten für eigene Zwecke nutzt, entstehen dadurch Risiken, welche durch die Rechtsgrundlage des berechtigten Interesses in aller Regel nicht gedeckt sind. Für solche Fälle muss ein privater Webseitenbetreiber eine Einwilligung einholen, welche den Vorgaben der DSGVO (freiwillig und vollständig informiert) entspricht. Zur Klarstellung: Das Datenschutzrecht verhindert nicht, dass Webseitenbetreiber Messungen zur Nutzung ihres Angebots durchführen, noch soll damit Werbung als Finanzierungsinstrument eines kostenlosen Angebots verhindert werden. Aber das Datenschutzrecht schützt Besucher vor einer unkontrollierten Weitergabe ihrer Daten an Dritte, welche damit kommerzielle Interessen verfolgen.

Wie können öffentliche Stellen, die in der OH Telemedien nicht genannt werden, nun ihre Webseiten gestalten? Hier ist zunächst zu unterscheiden, in welcher Rechtsform die öffentliche Stelle tätig wird. Im Bereich der Pflichtaufgaben kommt als Rechtsgrundlage nur Artikel 6 Absatz 1 Buchstabe e) DSGVO in Betracht. Die Webseite einer öffentlichen Stelle ist ein Informationsangebot im öffentlichen Interesse, damit einher geht auch eine Datenverarbeitung in engen Grenzen um das Angebot zu optimieren. Die Grenze des Zulässigen bildet auch hier das resultierende Risiko für Rechte und Freiheiten natürlicher Personen. Zulässig ist eine Nutzungsstatistik, welche Rückschlüsse über die Nutzung des eigenen Webangebots zulässt. Dies kann im Eigenbetrieb mit selbst betriebener Software erfolgen oder als Auftragsverarbeitung durch einen Dienstleister. Folgende Vorgaben sind dabei zu beachten:

Eine Verarbeitung der IP-Adresse ist nur gekürzt erlaubt. Wenn also zu Zwecken der Geoanalyse (Aus welcher Region greifen Nutzer auf das Angebot zu?) IP-Adressen verarbeitet werden, müssen diese vor der Verarbeitung gekürzt werden.

Cookies und andere Techniken, welche eine Wiedererkennung des Nutzers erlauben, müssen in der Datenschutzerklärung klar benannt werden und sollten eine Wiedererkennung wiederholter Besuche nur innerhalb eines kurzen Zeitraums (7 Tage) ermöglichen.

Besuchern ist innerhalb der Datenschutzerklärung eine Widerspruchsmöglichkeit gegen die Aufnahme in die Statistik angeboten worden.

Wird ein Auftragsverarbeiter gebunden, ist sicherzustellen, dass dieser die erhobenen Daten ausschließlich für Zwecke der Bereitstellung von Statistiken für den Auftraggeber nutzt und nicht für eigene Zwecke weiterverarbeitet. Dazu gehört auch, dass der Auftragsverarbeiter die erhaltenen Daten der öffentlichen Stelle nicht mit den Daten anderer Kunden zusammenführt.

Eine Einwilligung in eine Verarbeitung ist für den Bereich der Wahrnehmung einer Aufgabe im öffentlichen Interesse in der DSGVO nicht vorgesehen. Dienstleister und Dienste, welche für private Anbieter nur im Rahmen der Einwilligung möglich sind, scheiden daher für öffentliche Stellen aus, weil keine Rechtsgrundlage vorhanden ist. Ein Dienst wie Google Analytics, als meistgenutztes Analysetool für Webseiten, ist aus diesen Gründen für öffentliche Stellen nicht einsetzbar.

Aus meiner Kontroll- und Beratungstätigkeit haben sich über die Frage der Messung des Nutzungsverhaltens hinaus noch weitere Fragen ergeben, deren mögliche Lösungen in der Praxis ich nachfolgend kurz skizziere:

Einbindung von Videos, Karten oder „sozialen“ Medien:

Die immer noch anzutreffende Einbindung von Google Maps zur Anzeige des Standorts der Behörde ist nicht zulässig, da dies mit einer Datenübertragung von Nutzungsdaten an Google verbunden ist. Aufgrund des Geschäftsmodells von Google ist davon auszugehen, dass sämtliche Daten auf Google-Servern zu kommerziellen Zwecken verwendet werden. Als Alternative können Kartendaten auch unter Beachtung des Urheberrechts als Bild auf

dem eigenen Webserver hinterlegt werden oder die Kartendienste des Staatsbetriebs Geobasisinformationen und Vermessung Sachsen (https://geoportal.sachsen.de/cps/karten-dienste.html) genutzt werden.

Werbung und Messung des Erfolgs:

Über eine öffentliche Stelle, die auch auf dem freien Markt als Anbieter von Weiterbildung tätig ist, lag mir eine Beschwerde wegen des Einbindens von Google-Code auf dessen Webseite vor. Grund war auf Nachfrage, dass der Anbieter Werbung für eigene Angebote bei Google geschaltet hatte und mit der Verknüpfung die Wirksamkeit der Werbung und damit den Erfolg messen wollte. Damit verbunden war allerdings, dass Google die Nutzung der gesamten Webseite nachvollziehen konnte. Dafür war keine Rechtsgrundlage ersichtlich. Im Ergebnis wurde mit dem Dienstleister, welcher die Webseite technisch betreut, folgende Lösung gefunden: Die bei Google beworbenen Angebote bekommen eine eigene Einstiegsseite, wenn diese aus der Google-Suchmaschine als Werbeanzeige aufgerufen werden. Die Zählung der Aufrufe wiederum erfolgt intern mit Mitteln des Webservers. Der Google-Code, der sämtliche Besucherdaten an Google weitergeleitet hat, konnte damit entfernt werden.

Werbung auf der eigenen Seite:

Wenn öffentliche Stellen zur Querfinanzierung des Webauftritts Werbung auf der eigenen Seite platzieren wollen, ist das grundsätzlich statthaft. Nicht erlaubt ist die Verwendung eines Dienstleisters, welcher mittels der Werbung Profile der Nutzer erstellt und diese womöglich seitenübergreifend nachverfolgen kann. Da mir zum gegenwärtigen Zeitpunkt kein datenschutzfreundlicher Anbieter bekannt ist, bleibt als Möglichkeit Werbung rechtskonform einzubinden nur ein Hosting auf der eigenen Seite und das Zählen der Seitenaufrufe zu Abrechnungszwecken.

2.2.2 Die Befugnis zur personenbezogenen Datenverarbeitung bei Ordnungswidrigkeitenanzeigen durch Private

Vereinzelt bin ich mit der Frage konfrontiert worden, ob Privatpersonen berechtigt sind, zu Zwecken einer Anzeige und zum Nachweis festgestellter Ordnungswidrigkeiten, Abbildungen und Videoaufnahmen anzufertigen.

Die Verarbeitung personenbezogener Daten zum Zweck einer Anzeige und des Nachweises einer wahrgenommenen Ordnungswidrigkeit – unter anderem durch Beweisfotos oder Videoaufnahmen – gegenüber der jeweiligen zuständigen Behörde stellt regelmäßig keine ausschließlich persönliche oder familiäre Tätigkeit im Sinne von Artikel 2 Absatz 2 Buchstabe c) DSGVO dar und bedarf daher einer Rechtsgrundlage gemäß Artikel 6 Absatz 1 DSGVO. Der Anzeigeerstatter ist insoweit, zum Beispiel bei der Erstellung einer Abbildung mit Personen oder personenbeziehbaren Informationen zum Beweis einer Verfehlung, Verantwortlicher im Sinne von Artikel 4 Nummer 7 DSGVO.

Die einschlägige Rechtsprechung in dieser Frage differenziert dabei im Wesentlichen nach dem Interesse, das die anzeigende Privatperson verfolgt. In der Regel werden Anzeigen von Gesetzesverstößen (inkl. Beweisfotos) als gerechtfertigt angesehen, auch wenn durch sie zugleich in subjektive Rechte des Angezeigten eingegriffen bzw. dessen persönliche Belange beeinträchtigt werden. In diesen Fällen wird die in der Anzeigeerstattung liegende Verarbeitung der Daten des Dritten als zur Wahrung der berechtigten Interessen des Verantwortlichen (Anzeigeerstatter) erforderlich angesehen, weil dieser mit der Anzeige das legitime Ziel verfolgt, die Beeinträchtigung seiner Rechte zu beenden und den Verursacher von künftigen Rechtsbeeinträchtigungen abzuhalten. Die nach Artikel 5 und 6 DSGVO notwendige Rechtsgrundlage für die Erhebung und Übermittlung personenbezogener Daten an die Behörde bietet in diesen Fällen Artikel 6 Absatz 1 Satz 1 Buchstabe f) DSGVO.

Nicht ausreichend als Rechtfertigung ist beispielsweise das Fertigen von Fotografien einer mutmaßlichen Ordnungswidrigkeit und deren Übersendung an die Verfolgungsbehörde zum Zweck des beabsichtigten Schutzes der öffentlichen Ordnung ohne Beeinträchtigung eigener Interessen. Zu betonen ist, dass der Einzelne eben nicht Sachwalter öffentlicher Interessen ist. So erkannte das Amtsgericht Bonn die Erstellung und Übersendung von Bildaufnahmen an die zuständige Behörde, die eine Privatperson von Spaziergängern mit in einem Naturschutzgebiet unangeleinten Hunden fertigte, auch wenn die Handlung eine Ordnungswidrigkeit darstellte, als rechtswidrig. Das Landgericht Bonn bestätigte die Entscheidung; zu beachten ist hier allerdings, dass es sich um Aufnahmen einer Person und nicht nur eines Kraftfahrzeugs inkl. Kfz-Kennzeichen handelte, AG Bonn - Urteil vom 28.01.2014, Az. 109 C 228/13. In Niedersachsen erkannte das Amtsgericht Hannover Aufnahmen, die eine Privatperson mittels Dashcam erhoben und mit denen sie über Jahre hinweg (vermeintliche) Verkehrsordnungswidrigkeiten Dritter dokumentiert und zur Anzeige gebracht hatte, als rechtswidrig, weil die Person damit aus

Sicht des Gerichts keine schützenswerten eigenen Interessen verfolgte; das OLG Celle bestätigte die Entscheidung, OLG Celle - Beschluss vom 04.10.2017, Az. 3 Ss (OWi) 163/17.

Vereinzelt wird hingegen seitens öffentlicher Stellen, zum Teil ohne Differenzierung, immer noch davon ausgegangen, dass jedermann gegenüber Polizeibehörden bzw. dem Ordnungsamt Rechtsverstöße melden und dabei auch Fotografien von Handlungen, etwa von unzulässig abgestellten Kraftfahrzeugen anfertigen und der Behörde übermitteln könne. Entscheidend ist nach Einschätzung meiner Dienststelle aber, ob Anzeige und „Beweisfotos“ des privaten Anzeigeerstatters zur Wahrung dessen eigener berechtigten Interessen oder derjenigen eines Dritten erforderlich sind und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen, vergleiche den Wortlaut des Artikel 6 Absatz 1 Satz 1 Buchstabe f) DSGVO.

Die Verwertbarkeit datenschutzrechtlich zweifelhafter bzw. unzulässig gefertigter Aufnahmen eines Anzeigeerstatters im Ordnungswidrigkeitenverfahren bleibt trotz dieser Überlegungen und Feststellungen in der Praxis zumeist ohne Auswirkung. Nach deutschem Recht zieht die Rechtswidrigkeit einer Datenerhebung nicht die Unverwertbarkeit unrechtmäßig erhobener Daten nach sich, sondern es ist im Einzelfall die Beweisverwertbarkeit zu prüfen. Der Bundesgerichtshof hatte am 15. Mai 2018 - kurz vor Inkrafttreten der DSGVO - zum Beispiel entschieden, dass die permanente und anlasslose Aufzeichnung des Verkehrsgeschehens mit den datenschutzrechtlichen Regelungen des Bundesdatenschutzgesetzes zwar nicht vereinbar, die Verwertung von sogenannten Dashcam-Aufzeichnungen, die ein Unfallbeteiligter vom Unfallgeschehen gefertigt hat, als Beweismittel im Unfallhaftpflichtprozess aber dennoch zulässig sei, BGH, Urteil vom 15.05.2018, Az. VI ZR 233/17.

Auch im Bußgeld- und Strafverfahren führt die datenschutzwidrige Fertigung von Bildaufnahmen Privater nicht zu deren Unverwertbarkeit bei der Verfolgung und Ahndung von Ordnungswidrigkeiten und Straftaten; Ausnahmen sind allerdings geboten, wenn die Aufnahmen den Kernbereich privater Lebensgestaltung berühren oder gar im Auftrag der Verfolgungsbehörde gefertigt wurden.

2.2.3 Zulässigkeit der Datenverarbeitung mittels elektronischer Wasserzähler

Bereits in meinem letzten Tätigkeitsbericht hatte ich unter 2.2.6 über die datenschutzrechtlichen Anforderungen für die Nutzung elektronischer Wasserzähler berichtet. Ich konnte mittlerweile das Sächsische Staatsministerium des Innern davon überzeugen, dass diese bereits bei vielen sächsischen Wasserversorgern zum Einsatz kommen und daher Handlungsbedarf besteht. Es hat daraufhin „Hinweise zum datenschutzrechtlichen Rahmen, insbesondere bei kommunaler Wasserversorgungssatzung“ entworfen, die ich ausdrücklich begrüße – auch wenn vom Entwurf einer Mustersatzung abgesehen wurde. Ich gehe davon aus, dass diese nach dem Ende des Berichtszeitraums an die Aufgabenträger der öffentlichen Trinkwasserversorgung versandt werden.

2.2.4 Zulässiger Inhalt einer Eingliederungsvereinbarung nach SGB II

Die Frage nach dem datenschutzrechtlich zulässigen Inhalt einer Eingliederungsvereinbarung nach dem SGB II war Gegenstand einer Anfrage.

In der Eingliederungsvereinbarung nach § 15 Absatz 2 SGB II soll unter anderem bestimmt werden, welche Bemühungen erwerbsfähige Leistungsberechtigte in welcher Häufigkeit zur Eingliederung in Arbeit mindestens unternehmen sollen und in welcher Form diese Bemühungen nachzuweisen sind. Soweit eine Vereinbarung nach Absatz 2 nicht zustande kommt, sollen die Regelungen gemäß § 15 Absatz 3 SGB II durch Verwaltungsakt getroffen werden.

Insoweit fanden sich in dem vom Jobcenter gegenüber dem Petenten erlassenen Verwaltungsakt entsprechende Aufforderungen zum Nachweis seiner Bewerbungsbemühungen.

Inwieweit der Verwaltungsakt hier formell und materiell rechtmäßig erlassen wurde, insbesondere die dort dem Petenten aufgegebenen Anforderungen hinsichtlich ihres Umfangs verhältnismäßig sind, sowie ob verfassungsrechtliche Bedenken hinsichtlich der möglichen Sanktionsverhängung gegen den vorübergehenden vollständigen Wegfall des Leistungsanspruchs nach dem SGB II bestehen (siehe das beim Bundesverfassungsgericht hierzu anhängige Verfahren mit Aktenzeichen: 1 BvL 7/16), sind in der Sache keine datenschutzrechtliche Fragen, so dass sich dies meiner datenschutzrechtlichen Prüfung entzieht und auf dem Rechtsweg zu klären wäre.

Die Verpflichtung zur Vorlage nicht nur der Liste der Eigenbemühungen, sondern unter anderem auch des Schriftverkehrs mit den Arbeitgebern wird seitens der Rechtsprechung als zulässiger Inhalt eines Eingliederungsverwaltungsakts angesehen (siehe Sozialgericht München, Beschluss v. 31.05.2017 – S 40 AS 1142/17 ER).

Der Petent hatte insbesondere Bedenken, zum Nachweis von Bewerbungsbemühungen hierzu den E-Mail-Verkehr mit potentiellen Arbeitgebern gegenüber dem Jobcenter offenzulegen. Aus meiner Sicht steht es dem Bezieher von SGB II-Leistungen dabei frei, diesen Nachweis auch in anderer Form gegenüber der SGB-II-Stelle nachzuweisen. Soweit der Petent dabei den Einwand erhob, die Vorlage von E-Mails sei deshalb nicht möglich, da diese nicht an Dritte weitergegeben werden dürften, bezieht sich dieser in den Mails aufgenommene Hinweis nach meiner Kenntnis darauf, dass bei Versand eines Schreibens auf diesem Kommunikationsweg sicherzustellen ist, dass die E-Mail nur dem berechtigten Empfänger zugestellt wird. Dies war aber bei dem Petenten ja eingehalten, da dieser ordnungsgemäßer Empfänger der von potentiellen Arbeitgebern an ihn versandten Mails ist.

Sein diesbezüglicher Einwand steht daher einer Weitergabe von ihm ordnungsgemäß zugegangenen Mails an die SGB II -Stelle nicht entgegen.

2.2.5 In Rede stehende unbefugte Übermittlung von Mieterdaten

Eine Petentin informierte mich darüber, dass sie einen Mietvertrag mit einer sächsischen Kommune kündigte – und darauf von ihrer Freundin angesprochen wurde. Nachdem die Petentin bislang niemanden über diese Kündigung informierte, war sie über den Informationsstand ihrer Freundin sehr verwundert. Sie vermutete eine unzulässige Datenübermittlung durch die Kommune.

Nachdem ich diese um Stellungnahme gebeten hatte, teilte diese mir mit, dass sie keine derartigen Informationen übermittelt habe. Sie habe jedoch den Lebenspartner der Freundin der Petentin als Tischler damit beauftragt, ein Aufmaß der gekündigten Wohnung zu erstellen. Dieser war somit über die Kündigung informiert.

Einen Datenschutzverstoß der Kommune konnte ich demnach nicht feststellen. Ich habe die Petentin über den vermutlichen Informationsfluss in Kenntnis gesetzt.

2.2.6 Anforderungen an die Nutzung des Geburtenregisters zu Forschungszwecken und gesetzlich vorgesehene Mitteilung an den Datenschutzbeauftragten

Die Mitarbeiterin einer Universität in Mecklenburg-Vorpommern bat mich im Rahmen des Forschungsvorhabens „Todesfälle bei Fluchtversuchen über die Ostsee“ um Mithilfe. Sie suchte nach Hintergrundinformationen zu den Biographien der Personen, die im Zuge ihres Fluchtvorhabens tödlich verunglückt waren.

Eine dieser Personen war ein Mann, der im März 1937 in einer sächsischen Stadt geboren worden war. Seine Geburtsurkunde lag der Universitätsmitarbeiterin bereits vor und sie erhoffte sich aus dem Auszug aus dem Geburtenregister zu ihm weitere Erkenntnisse. Das hierfür zuständige sächsische Standesamt wies zurecht für die Benutzung der Personenstandsregister auf die Vorschriften des Personenstandsgesetzes (PStG) hin, insbesondere auf § 66 PStG:

Die Nutzung der Personenstandsregister für wissenschaftliche Zwecke ist nur unter bestimmten Voraussetzungen möglich. Insbesondere ist dabei die Zustimmungserklärung der für den Fachbereich des Forschungsvorhabens zuständigen obersten Bundes- oder Landesbehörde oder einer von dieser bestimmten Stelle erforderlich, § 66 Absatz 2 Satz 2 PStG. Die Zustimmung muss den Empfänger, die Art der Nutzung der Personenstandseinträge, den Kreis der Betroffenen und das Forschungsvorhaben bezeichnen, sie ist dem zuständigen Datenschutzbeauftragten mitzuteilen, § 66 Absatz 2 Satz 3 PStG.

Das Standesamt bat daher um Nachreichung der entsprechenden Zustimmungserklärung. Die Universitätsmitarbeiterin war nun ein wenig ratlos, an welche Behörde und an welchen Datenschutzbeauftragten sie sich konkret wenden musste, um diese erwünschte Zustimmung zu erhalten.

Nach Rücksprache mit dem Sächsischen Staatsministerium des Innern kam ich zu folgendem Ergebnis:

§ 66 Absatz 2 Satz 2 PStG schreibt eine Zustimmung der für den Fachbereich des Forschungsvorhabens zuständigen obersten Bundes- oder Landesbehörde vor. Die örtliche Zuständigkeit richtet sich dabei nach dem Sitz der Forschungseinrichtung und nicht nach dem Standesamt, bei dem eine Benutzung beantragt wird § 66 Absatz 2 Satz 2, 2.HS PStG. Damit wird gleichzeitig sichergestellt, dass die Zustimmung nur einer obersten

Landesbehörde erforderlich ist und bei Benutzung mehrere Standesämter verschiedener Bundesländer, nicht sämtliche obersten Landesbehörden die Zustimmung erteilen müssen. Die obersten Landesbehörden vertrauen damit der Prüfung der Erforderlichkeit und Zulässigkeit durch die jeweils zuständige oberste Landesbehörde, in der die wissenschaftliche Einrichtung ihren Sitz hat. Dies dient sowohl der Verfahrensvereinfachung als auch der Verfahrensbeschleunigung, denn anderenfalls müsste die Antragstellerin an allen Bundesländern, in denen sie Standesämter benutzen will, die Zustimmung beantragen.

Nichts anderes konnte nach Meinung des Sächsischen Staatsministeriums des Innern für die Mitteilung an den Datenschutzbeauftragten gem. § 66 Absatz 2 Satz 3 PStG gelten:

Die Hürden für die Benutzung der Personenstandsregister und deren weitere Verwendung für wissenschaftliche Zwecke sind vom Gesetzgeber (zu Recht) hoch angesetzt. Hinzu kommt, dass die Zustimmungserklärung der obersten Landesbehörde den Standesbeamten nicht von einer Interessenabwägung und Entscheidung über die Registerbenutzung entbindet, § 2 Absatz 2 PStG, § 55 Absatz 2 PStV, Nummer 66.1 S.5 PStG-VwV, so dass hier noch eine weitere Prüfung stattfindet und der Standesbeamte die Amtshandlung im Zweifel ablehnen und dem Amtsgericht zur Entscheidung vorlegen kann. § 66 Absatz 2 PStG wird daher so verstanden, dass jeweils nur eine oberste Behörde und ein Datenschutzbeauftragter an dem Genehmigungsverfahren zu beteiligen sind, die örtliche Zuständigkeit ergibt sich aus dem Sitz der Forschungseinrichtung, hier also der Datenschutzbeauftragte in Mecklenburg-Vorpommern.

Im Ergebnis folgte daraus:

Die Universitätsmitarbeiterin musste sich zwecks Zustimmungserteilung an ihre Aufsichtsbehörde, das Ministerium für Bildung, Wissenschaft und Kultur in Mecklenburg-Vorpommern wenden und die Zustimmung meinem Kollegen in Schwerin mitteilen.

2.2.7 Einsichtnahme in Patientenakten zu Forschungszwecken

Mich erreichte eine Anfrage zu einem Forschungsvorhaben betreffend die Forensischen Kliniken des Freistaates Sachsen.

Die dabei geplante Einsichtnahme in die Patientenakten stellt in datenschutzrechtlicher Hinsicht eine Übermittlung personenbezogener Daten seitens der betreffenden Krankenhäuser dar.

Die mir hierfür als Erlaubnisnorm genannte Vorschrift des § 34 SächsKHG findet hier keine Anwendung. Denn das Gesetz gilt nach § 2 SächsKHG für Krankenhäuser im Sinne von § 2 Nummer 1 KHG, die auf Grund des Krankenhausfinanzierungsgesetzes (KHG) gefördert werden. Nach diesem Gesetz gemäß § 5 KHG werden indes Einrichtungen in Krankenhäusern für Personen, die im Maßregelvollzug auf Grund strafrechtlicher Bestimmungen untergebracht sind, nicht gefördert.

Maßgeblich ist vielmehr das neu gefasste SächsPsychKG vom 22.8.2019, konkret § 38c Absatz 1 SächsPsychKG, der u.a. § 23 des Sächsischen Justizvollzugsdatenschutzgesetzes vom 22. August 2019 für entsprechend anwendbar erklärt.

§ 23 SächsJVollzDSG regelt die Auskunft und Akteneinsicht für wissenschaftliche Zwecke. Nach Absatz 1 der Vorschrift gilt für die Übermittlung personenbezogener Daten in Akten an Hochschulen, andere Einrichtungen, die wissenschaftliche Forschung betreiben, und öffentliche Stellen für wissenschaftliche Zwecke § 476 der Strafprozessordnung entsprechend mit der Maßgabe, dass auch elektronisch gespeicherte personenbezogene Daten übermittelt werden können. Die Übermittlung kann auch auf elektronischem Wege erfolgen.

Diese Vorschrift stellt ganz konkrete Anforderungen an die Verfahrensweise bei Auskünften und Akteneinsicht zu Forschungszwecken, die also hier zu beachten waren und für das hier zu beurteilende Vorhaben wie folgt umzusetzen waren:

Eine Einsichtnahme in die Patientenakte gemäß § 476 Absatz 2 StPO erfolgt in der jeweiligen Klinik vor Ort und ausschließlich durch die die Forschung betreibende Person zu dem konkret benannten Forschungsvorhaben. Die Daten werden dort unmittelbar bei der Erhebung pseudonymisiert. Sofort nach Beendigung der Datenerfassung in der jeweiligen Klinik wird die Liste von Pseudonymen vernichtet – ebenfalls von der Forschungsperson selbst - so dass eine Zuordnung von Daten zu einer Person physikalisch nicht mehr möglich ist (frühestmögliche Anonymisierung gemäß der Vorgabe nach § 476 Absatz 6 StPO).

Bei dieser Verfahrensweise werden auch die Anforderungen des § 476 Absatz 5 StPO eingehalten.

Hinsichtlich der nach § 476 Absatz 2 StPO vorzunehmenden Abwägung habe ich gegen die Durchführung des Vorhabens ebenfalls keine Bedenken vorgebracht.

Nach § 476 Absatz 3 StPO werden personenbezogene Daten nur an solche Personen übermittelt, die Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind oder die zur Geheimhaltung verpflichtet worden sind. § 1 Absatz 2, 3 und 4 Nummer 2 des Verpflichtungsgesetzes findet auf die Verpflichtung zur Geheimhaltung entsprechende Anwendung.

Ob dies hier zutraf bat ich den Forscher, dies eigenständig mit seiner Klinik abzuklären, so dass im Zweifelsfall noch eine entsprechende Verpflichtung zu seiner Person vorgenommen werden konnte.

Aufgrund des Bestehens einer gesetzlichen Übermittlungsbefugnis bedarf es keiner (zusätzlichen) Einholung einer Einwilligung der Probanden.

Abschließend musste ich erneut wie bei vielen an mich herangetragenen Forschungsvorhaben mitteilen, dass ich keine ausdrückliche Genehmigung oder Zustimmung bezüglich eines Forschungsvorhabens aussprechen kann, die datenschutzrechtlichen Bestimmungen sehen eine solche nicht vor und machen eine solche insbesondere auch nicht zur Voraussetzung für die Durchführung des Forschungsvorhabens. Ich kann daher lediglich eine Stellungnahme bzw. Einschätzung abgeben, ob ich das betreffende Forschungsvorhaben datenschutzrechtlich für bedenklich oder unbedenklich halte. Insoweit steht es allerdings der Forschung betreibenden Stelle stets frei gegenüber Dritten, hier waren es die betreffenden Kliniken, auf mein Schreiben zu verweisen.

2.2.8 Tonbandaufzeichnungen zur Protokollierung von Stadtrats- und Ausschusssitzungen

Ich wurde anlässlich der Neufassung der Geschäftsordnung des Stadtrates einer sächsischen Kommune um Beratung hinsichtlich der Zulässigkeit von Tonbandaufzeichnungen zur Protokollierung von Stadtrats- und Ausschusssitzungen ohne Einwilligung vor dem Hintergrund der DSGVO gebeten.

Bei der Tonbandaufnahme handelt es sich nicht um eine Niederschrift im Sinne von § 40 Absatz 2 SächsGemO. Ein Tonband stellt bereits keine Niederschrift im Wortsinne dar, da es sich nicht um eine schriftliche Aufzeichnung, sondern um eine Tonaufzeichnung handelt. Das Tonband erfüllt auch nicht den Zweck einer Niederschrift. Die Tonaufnahme stellt vielmehr nur ein Hilfsmittel dar, das der Erstellung der Niederschrift vorausgeht.

Ich rege in diesem Zusammenhang an, in der Geschäftsordnung zu regeln, dass als Hilfsmittel für das Anfertigen der Niederschrift Tonbandaufnahmen gefertigt werden können.

Ich habe mitgeteilt, dass bei entsprechender Regelung in der Geschäftsordnung zweckgebundene Tonbandaufzeichnungen für die Erstellung der Niederschrift von Gemeinderatssitzungen mit dem Schutz auf informationelle Selbstbestimmung der Gemeinderäte vereinbar sind. Dies gilt entsprechend auch, wenn in der Gemeinderatssitzung Einwohner bei Fragestunden oder Anhörungen zu Wort kommen (§ 44 Absatz 3, 4 SächsGemO). Es ist jedoch gemäß Artikel 13 DSGVO entsprechend zu informieren (beispielsweise über entsprechende Aufstelltafeln am Eingang).

Auf jeden Fall besteht gemäß Artikel 7 DSGVO die Verpflichtung zur unverzüglichen Löschung der Tonbänder nach der Erfüllung von deren Zweckbestimmung, d.h. nach Fertigung und Genehmigung der Niederschrift (so bereits zu alten Rechtslage VG Bayreuth, Urteil vom 26. April 2013 – B 5 K 11.594).

Die Frage einer anderen sächsischen Kommune betraf das Recht von Stadträten, die gemachten Aufnahmen nachträglich anzuhören.

Von dem Recht gemäß § 40 Absatz 2 SächsGemO, Einsicht in die Niederschrift zu nehmen und gegebenenfalls Einwendungen dagegen zu erheben, ist auch das Recht umfasst, die Tonträgeraufzeichnungen abzuhören, aufgrund derer die Niederschrift gefertigt wurde. Gerade in Fällen, in denen die Zweifel der Antragsteller an der Richtigkeit der Niederschrift durch die Tonträgeraufzeichnungen erhärtet oder zerstreut werden können, müssen die Mitglieder der Gemeindevertretung die Möglichkeit haben, sich vor der Beschlussfassung über ihre Einwendungen Klarheit darüber zu verschaffen, ob sie ihre Einwendungen aufrechterhalten wollen oder nicht (HessVGH, Beschluss vom 6.4.1987 – 2 TG 912/87).

Schließlich besteht daneben ein Anspruch aus Artikel 15 Absatz 3 DSGVO auf Kopie, der wohl auch als geringeres Mittel ein Abhören umfasst. Dieser wird aber nur die eigenen Beiträge umfassen. Gemäß Artikel 15 Absatz 4 DSGVO dürfen dadurch aber die Rechte und Freiheiten anderer Personen nicht beeinträchtigt werden. Nachdem die möglicherweise mit aufgezeichneten Zwischenrufe etc. aber auch während des Beitrags gehört werden konnten, wird davon im Regelfall nicht auszugehen sein.

2.2.9 Übersendung von Versammlungsanzeigen durch Versammlungsbehörden an das Landesamt für Verfassungsschutz

Im Rahmen der datenschutzrechtlichen Prüfung einer Beschwerde bin ich darauf aufmerksam geworden, dass mindestens eine sächsische Versammlungsbehörde in der Vergangenheit Versammlungsanzeigen mit darin enthaltenen personenbezogenen Daten des oder der Anmelder ohne konkreten Anlass an das Landesamt für Verfassungsschutz übermittelt hat. Das Landesamt für Verfassungsschutz wurde also generell über angemeldete Versammlungen informiert, Versammlungsanzeigen wurden gewissermaßen „automatisch durchgereicht“. Zudem erfolgt die entsprechende Information in vielen Versammlungsbehörden mit einer E-Mail, die auch die zuständige Polizeidirektion als Empfänger hatte.

Die regionale Presse griff das Thema auf; es war zudem Thema einer Kleinen Anfrage im Sächsischen Landtag (LT-Drs. 6/18584)

Versammlungsbehörden sind gemäß § 15 SächsVG zuständig für die Erstellung von Versammlungsbescheiden mit gegebenenfalls beschränkenden Verfügungen, die auf der Grundlage von Gefahrenprognosen ergehen. Nur wenn dabei eine sich konkret abzeichnende Versammlungslage als potentiell konfliktträchtig eingeschätzt wird und sich im gesetzlich bestimmten Beobachtungsfeld des Landesamt für Verfassungsschutz bewegt (insbesondere bei vermuteter extremistischer Beteiligung), ist eine Übermittlung an das Landesamt für Verfassungsschutz zulässig, um von diesem eine Lageeinschätzung zu erhalten. Es kann dabei auch ausreichend sein, zunächst anonymisierte Daten zu übermitteln und die personenbezogenen Daten auf Anforderung an das Landesamt für Verfassungsschutz nachzutragen.

Eine automatisierte Übermittlung genügt diesen Anforderungen eben so wenig, wie die durch andere Versammlungsbehörden vorgenommene Übermittlung personenbezogene Daten an das Landesamt für Verfassungsschutz „zur Information“ ohne eine derartige Prüfung.

Es ist auch nicht ersichtlich, dass die Polizeidirektionen über diese Übermittlungen an das Landesamt für Verfassungsschutz durch eine gemeinsame E-Mail zu informieren sind. Es sind vielmehr jeweils einzelne E-Mails zu verschicken.

Das von mir um Stellungnahme gebetene Sächsische Staatsministerium des Innern teilt meine Rechtsauffassung und hat die Versammlungsbehörden entsprechend informiert. Ich gehe davon aus, dass diese künftig eine sorgfältige Prüfung vor einer Übermittlung an das Landesamt für Verfassungsschutz vornehmen werden.

Eine datenschutzrechtliche Bewertung der Verarbeitung der derart übermittelten Daten durch das Landesamt für Verfassungsschutz finden Sie im Beitrag 8.7.

2.2.10 Asylbewerberbescheid im Internet

Im Oktober 2019 wandte sich ein Hinweisgeber mit einer Datenschutzbeschwerde an mich. Er teilte mit, dass am selbigen Tage um 07:48 Uhr auf den Web-Seiten von Twitter, Facebook und ähnlichen sozialen Medien personenbezogene Daten eines sächsischen Ausländeramtes zum Thema Asylbewerberleistungen, möglicherweise ohne Zustimmung der Betroffenen, veröffentlicht wurden. In dem Internetbeitrag war die Kopie eines Bescheides über die Gewährung von Leistungen nach § 2 Asylbewerberleistungsgesetz über eine ganze Familie veröffentlicht. In den verschiedenen Foren wurde über den Inhalt der Bescheide, ob diese Schriftstücke echt wären und über die Höhe der Leistungen, spekuliert. Mit welchem Ziel wurden diese sensiblen persönlichen Daten einfach so veröffentlicht?

Ich bat das zuständige Amt um Überprüfung des Sachverhaltes und Stellungnahme, ob dieser Bescheid durch die Behörde ausgestellt wurde und möglicherweise eine Offenbarung der Bescheiddaten seitens Beschäftigter des Amtes erfolgte und ob noch weitere personenbezogene Daten aus diesem Zuständigkeitsbereich im Internet veröffentlicht wurden.

Die Behörde teilte mit, dass der Sachverhalt der verantwortlichen Stelle bereits bekannt war. Das Schriftstück wurde nicht durch Mitarbeiter der Behörde in die Öffentlichkeit gegeben. Ein Datenschutzverstoß durch die verantwortliche Behörde lag nicht vor.

Bereits im Vorfeld hat das Amt mittels Pressemeldung auf seiner Homepage über den Fall sowie auch über das Zustandekommen der Leistungshöhe umfangreich informiert. Weitere Informationen, z. B. ob die in den sozialen Medien veröffentlichten Fotos der abgebildeten Schriftstücke der Behörde zuzuordnen sind, dürfen durch das zuständige Amt gegenüber Dritten nicht offenbart werden. Auch diese Informationen fallen unter den Sozialdatenschutz.

Ob das Schriftstück durch die Betroffene selbst oder durch Dritte im Internet veröffentlicht worden ist, konnte nicht ermittelt werden. Das Abfotografieren und zur Verfügung stellen im Internet ohne Kenntnis und Einwilligung der Betroffenen ist unzulässig. Aus datenschutzrechtlichen Gründen stellt die Veröffentlichung personenbezogener Daten ohne die Einwilligung der Betroffenen einen Verstoß gegen die DSGVO dar und kann mit Bußgeld geahndet werden. Jeder Ersteller und Verteiler derartiger Beiträge mit personenbezogenen Daten ist als Schuldiger auszumachen. Gegen diese rechtswidrige Veröffentlichung der Dokumente in den sozialen Medien im Internet wird anwaltlich vorgegangen.

2.2.11 Zulässigkeit der Verarbeitung personenbezogener Daten durch Auskunfteien; prinzipiell weitgehend unveränderte Rechtslage, zumeist Artikel 6 Absatz 1 Buchstabe f) DSGVO

Immer wieder erreichen mich Nachfragen zur Zulässigkeit der Datenverarbeitung von Auskunfteien, die seitens betroffener Personen grundsätzlich in Frage gestellt werden. Häufig wird auch seitens der betroffenen Person darauf verwiesen, dass keine Einwilligung zur Speicherung der personenbezogenen Daten erfolgt sei.

Ich verweise in Bezug auf die rechtlichen Rahmenbedingungen auch in diesem Kontext auf §§ 30, 31 Bundesdatenschutzgesetz. Natürlich, eine personenbezogene Datenverarbeitung ist nur insoweit zulässig, als dass eine gesetzliche Erlaubnis hierfür besteht. Bei Auskunfteien kommen die Tatbestände der Einwilligung des Betroffenen – Artikel 6 Absatz 1 Buchstabe a) DSGVO –, die Verarbeitung zur Erfüllung eines Vertrags oder zur Durchführung einer vorvertraglichen Maßnahmen – Artikel 6 Absatz 1 Buchstabe b) DSGVO – sowie die Verarbeitung zur Wahrung berechtigter Interessen seitens des Verantwortlichen gemäß Artikel 6 Absatz 1 Buchstabe f) DSGVO in Betracht. In einer Vielzahl der Vorgänge wird die personenbezogene Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen stattfinden. Es hat zwar eine Interessenabwägung zu erfolgen, doch wäre der Verantwortliche dabei im Einzelfall regelmäßig auf die Geltendmachung von Angaben seitens der betroffenen Person angewiesen, die deren Interessen oder Grundrechte, die den Schutz personenbezogener Daten erfordern, überwiegen. Auch nach der alten Rechtslage, den Vorschriften des Bundesdatenschutzgesetzes, war die Verarbeitung personenbezogener Daten durch Auskunfteien mit einer Interessenabwägung verbunden gewesen. So kann allgemein und bedingt auf die bisherige datenschutzrecht-

liche Beurteilung zurückgegriffen werden. Nach der bisherigen Spruchpraxis meiner Behörde und der Rechtsprechung wird ein einfaches (potentielles) und generelles Interesse der Betroffenen am Schutz von Bank- und Finanzierungsinformationen und der finanziellen Situation allgemein nicht als ausreichend angesehen, da auch das bei einer Teilnahme am Wirtschaftsleben immerwährende präsente Interesse der Verantwortlichen, Investitions- und kreditorische Risiken zu erfassen, in der Abwägung nicht geringer einzuschätzen sein wird, da dieses Interesse der Erhaltung eines relativ gesicherten Rechts-und Wirtschaftsverkehrs dient. Kommen also keine weiteren Gesichtspunkte zu Gunsten der betroffenen Personen hinzu, die eine Abwägung des Verantwortlichen so verändern, dass der Datenkranz der Wirtschaftsauskunftei eingeschränkt oder eine Speicherung ganz gehindert wird, wird man die herkömmliche Verarbeitung der personenbezogenen Wirtschaftsdaten auf der Grundlage der Bestimmungen des Artikel 6 DSGVO zu gestatten haben.

2.2.12 Personenbezogenen Datenverarbeitung durch Parkraumservice-Gesellschaften

Häufig erhalte ich Beschwerden zur Datenverarbeitung durch so genannte „Parkraumbewirtschaftungsgesellschaften“ oder „Parkraumservice-Gesellschaften“. In diesen Fällen wenden sich zumeist die betroffenen Personen und Kunden, insbesondere im Einzelhandel, aufgrund von Zahlungsaufforderungen der Parkraumgesellschaften wegen Vertragsstrafen aufgrund einer Überschreitung der Höchstparkdauer auf den Parkstellplätzen von Supermärkten, Discountern und anderen Einzelhandelsgeschäften an meine Behörde. Es handelt sich nicht um „Strafzettel“, also um ordnungsbehördliches Tätigwerden, sondern um privatrechtliches Handeln. Regelmäßig haben die Eigentümer, die Einzelhändler, die Parkraumbewirtschaftung ausgelagert und um eine Fehlbelegung ihrer Parkplätze zu unterbinden, die Parkraumgesellschaften beauftragt.

Im Regelfall werden die Parkraumbewirtschaftungsunternehmen bei einer Überschreitung der vorgegebenen Parkdauer oder bei Nichtauslage einer Parkuhr tätig, indem sie den Fahrzeughalter mit einer Anfrage bei der Registerbehörde ermitteln und diesen anschreiben und als mutmaßlichen Fahrzeugführer zur Zahlung auffordern. Mit der Nutzung der Stellflächen gehen die Fahrzeugführer einen Vertrag mit der Parkraumgesellschaft ein, worauf auch regelmäßig mit gut sichtbaren Hinweistafeln hingewiesen wird. Die Erhebung und Verarbeitung personenbezogener Daten der Fahrzeugkennzeichen, Abstellzeiten, Bildaufnahmen, Fahrzeughalter und weitere mögliche personenbezogenen

Daten sind nach meiner Überzeugung zu vertraglichen Zwecken bzw. aus berechtigtem Interesse heraus gemäß Artikel 6 Absatz 1 Buchstaben b), f) DSGVO bei ordnungsgemäßer Vorgangsbearbeitung durch diese Unternehmen nicht zu beanstanden. Zivilrechtliche Störungen ist meine Behörde hingegen nicht zu lösen in der Lage.

2.2.13 Veröffentlichung von Freistellungsbescheinigungen nach § 48b EStG

Bauleistende Unternehmen veröffentlichen zum Teil Freistellungsbescheinigungen nach § 48b EStG (Steuerabzug bei Bauleistungen) zum Nachweis ihrer Rechtskonformität auf ihrer Internetpräsenz. Der Leistungsempfänger einer Bauleistung wird so von der Pflicht zum Abzug der Bauabzugssteuer befreit.

Mir gegenüber wurde die Frage gestellt, ob die Veröffentlichung zulässig sei, da auf der Bescheinigung Namens- und Kontaktdaten von bearbeitenden Bediensteten erkennbar seien. Die Praxis erkenne ich aus dem legitimen Interesse an einer reibungslosen (Online-)Verfügbarkeit entsprechender Bescheinigungen dennoch als zulässig an, auch soweit bearbeitende Bedienstete des ausstellenden Finanzamts auf den Dokumenten erkennbar sind. Diese Informationen sind zwar personenbezogen, die Bediensteten aber lediglich als Amtswalter betroffen sind. Gleichwohl wären Schwärzungen für den Verantwortlichen durchführbar, sind doch auch Informationen für interessierte Auftraggeber telefonisch über das Finanzamt oder über die Internetseite des Bundesamtes für Finanzen abrufbar. Den Finanzbehörden wiederum obliegt es, ggfs. einer veränderten Kommunikationskultur Rechnung zu tragen und Dokumente ohne Hinweise auf einzelne Bearbeiter abzusetzen.

2.2.14 Novellierung des Steuerberatergesetzes – Steuerberater als Verantwortliche

In meinem letzten Tätigkeitsbericht hatte ich bereits zu der Frage der Lohn und Gehaltsabrechnung durch Steuerberater und ob diese Tätigkeit einer Auftragsverarbeitung darstellt, berichtet, 4.3.3 Tätigkeitsbericht 2017/2018 (Teil 2). Zwischenzeitlich hatte der Bundesgesetzgeber das Steuerberatungsgesetz novelliert. § 11 Absatz 1 Steuerberatergesetz erlaubt nunmehr die Verarbeitung auch besonderer Kategorien personenbezogener Daten gemäß Artikel 9 Absatz 1 DSGVO. Darüber hinaus soll diese Verarbeitung durch Steuerberater unter Beachtung deren Berufspflichten weisungsfrei erfolgen, § 11 Absatz

2 Steuerberatergesetz. Der Gesetzgeber stellt in Absatz 2 zudem klar, dass die Personengesellschaften, die Steuerberater nach § 3 sind, sämtliche personenbezogene Daten ihrer Mandantin als Verantwortliche gemäß Artikel 4 Nummer 7 DSGVO verarbeiten.

Durch die Initiative des Bundesgesetzgebers wurden damit nach dem Wirksamwerden der DSGVO entstandene juristische Schwierigkeiten ausgeräumt.

Letztendlich wurde meine im letzten Tätigkeitsbericht geäußerte Rechtssicht zu den Berufspflichten und zur Weisungsfreiheit der Steuerberater bestätigt.

2.2.15 Videoüberwachung in Fahrstühlen

In großen mit Fahrstühlen ausgestatteten Mietshäusern stellt sich oftmals die Frage, ob zur Vandalismusprävention und Erhöhung des subjektiven Sicherheitsgefühls der Mieter einerseits sowie zur Beweissicherung und Sachverhaltsaufklärung andererseits auch die Fahrstühle videoüberwacht werden dürfen.

Einschlägig für die Beurteilung der Zulässigkeit von Videoüberwachungstechnik in Fahrstühlen ist Artikel 6 Absatz 1 Satz 1 Buchstabe f) DSGVO. Im Rahmen der danach vorzunehmenden Interessenabwägung ist zunächst eine konkrete Gefährdungslage für die Einzelmaßnahme darzulegen. Das Verfolgen lediglich allgemeiner präventiver Zwecke und die Erhöhung des Sicherheitsgefühls der Bewohner, ohne dass es in der Vergangenheit bereits relevante Vorfälle gegeben hat oder die begründete Annahme besteht, dass damit zukünftig zu rechnen ist, mag zwar noch ein berechtigtes Interesse darstellen; jedoch fehlt es in diesem Fall schon an der Verhältnismäßigkeit, insbesondere der Erforderlichkeit. Ist die Erforderlichkeit im Einzelfall nachgewiesen, ist noch die Hürde der schutzwürdigen Interessen der betroffenen Personen zu überwinden. Zu meiner Überzeugung wird daran dann aber regelmäßig die Zulässigkeit einer solchen Überwachungsmaßnahme scheitern. Die Überwachung eines Fahrstuhls stellt aufgrund der geringen Raumgröße und der Tatsache, dass man dieser Überwachung nur bedingt ausweichen kann, eine besonders eingriffsintensive Maßnahme dar. Dabei ist zu bedenken, dass die regelmäßig zur Verfügung stehenden Treppenhäuser oftmals keine Alternative darstellen. Gründe dafür könnten viele angeführt werden. So spielen beispielsweise der Gesundheitszustand bzw. die körperliche Verfassung eine Rolle, mitzuführendes Gepäck bzw. Lasten oder die Begleitpersonen, wie zum Beispiel Kleinkinder. In diesen Fällen erfassen Videokameras praktisch anlasslos auch den insoweit einzigen Zugang zur eigenen Wohnung. Betroffene Bewohner können sich einer solchen Videoüberwachung daher nicht mehr

entziehen. Bereits die Möglichkeit, dass ein Dritter jederzeit kontrollieren kann, welcher Bewohner wann, welchen Besuch empfängt, kommt oder geht, setzt die Bewohner einem erheblichen Überwachungs- und Anpassungsdruck aus.

Etwas anderes kann beispielsweise unter der wohl nur seltenen Voraussetzung, dass mehrere alternativ zu nutzende Fahrstühle zur Verfügung stehen und zumindest ein Fahrstuhl nicht überwacht wird, gelten. Eine weitere Ausnahme könnte ich mir dahingehend vorstellen, dass die Aktivierung der Kamera an die Betätigung des in Fahrstühlen regelmäßig zu findenden Notfallknopfs gebunden ist und das Videosignal dann zugleich bei der zuständigen Notfallzentrale aufläuft. In diesem Fall fände keine Dauerüberwachung statt; diese würde stattdessen nur anlassbedingt ausgelöst.

Es versteht sich von selbst, dass im Fall einer zulässigen Überwachung deutlich auf diese hinzuweisen ist, dabei ist den Informationspflichten nach Artikel 13 DSGVO vollumfänglich zu entsprechen. Insoweit wird auf die Muster zur Kennzeichnung von Videoanlagen verwiesen, [Verweis auf Ordnungsnummer] Anlagen 1 und 2.

2.2.16 Der Einbruch im Grünen Gewölbe und durchgeführte Videoüberwachung

Am 25. November 2019 erfolgte ein spektakulärer Einbruch in das Historische Grüne Gewölbe in Dresden, der weltweit Beachtung fand. Binnen weniger Minuten entwendeten unbekannte Täter Juwelenschmuck in Millionenwerten. „Unglaublich und ungelöst“ titelte noch im März 2020 die Sächsische Zeitung. Daran konnte auch Videoüberwachungstechnik etwas ändern. Doch der Reihe nach:

Seit dem Einbruch am Montagmorgen im November 2019 fahndete die Polizei unter Hochdruck nach den Tätern. Noch am gleichen Abend veröffentlichte sie Tataufnahmen der örtlichen Überwachungskameras, auf denen zwei Einbrecher eher weniger gut, d. h. praktisch kaum zu sehen waren. Die Kameras waren und sind in den Museumsräumen installiert, datenschutzrechtlich unbedenklich. Tatsächlich waren sie jedoch völlig veraltet und konnten daher – auch wegen der äußeren Bedingungen (Dunkelheit) – offensichtlich keinen wesentlichen Beitrag zur Aufklärung des Einbruchs leisten. Dies verdeutlicht, dass Videoüberwachungskameras oft nicht halten, was sie versprechen und nur eine Scheinsicherheit vortäuschen. Während sich potentielle Straftäter darauf einstellen und ihre Aktionen entsprechend planen, d. h. sich vermummen und natürlich im Schutz der Dunkelheit agieren und daher oftmals unerkannt bleiben, geraten die Aufnahmen zu re-

gelmäßig unbescholtenen rechtstreuen Personen, die sich unverdeckt und in den Erfassungsbereichen bewegen, deutlich besser. Datenschutzrechtlich ist abzuwägen zwischen der Vielzahl der Personen, die, ohne sich etwas zuschulden kommen zu lassen haben, von der Videoüberwachung betroffen sind und deren personenbezogene Daten mit allen damit verbundenen Risiken anlasslos mitverarbeitet werden und denjenigen, denen die Videoüberwachung eigentlich gilt, die der Überwachung aufgrund Sonderwissens und mit bewussten Ausweichhandlungen unter Umständen aber gerade entgehen. In diesem Zusammenhang anzuwendende Kriterien der „Geeignetheit", „Erforderlichkeit" und „Verhältnismäßigkeit", sind jeder Abwägung vor Einrichtung einer entsprechenden optisch-elektronischen Überwachung zugrunde zu legen, was dann eben auch bei entsprechenden tatsächlichen Bedingungen und Verhalten oft zu einer Unzulässigkeit einer Maßnahme führen kann.

Zurück zum Einbruch im Grünen Gewölbe: Tagsüber – bei helllichten Museumsräumen – war die Videoüberwachungstechnik zwar auch nicht leistungsfähiger, aber die besseren Umgebungsbedingungen sollten zumindest zu einer besseren Aufnahmequalität gereichen und niemand wird bestreiten können, dass die Ausstellungsstücke auch während der Öffnungszeiten gewöhnlich einem erheblichen Diebstahlrisiko unterliegen, so dass an der Zulässigkeit der Videoüberwachung, also wie bereits erwähnt, kein Zweifel bestanden hatte.

Wenige Tage nach dem Einbruchereignis kam dann aber eine weitere Videoaufnahme ins Spiel. Nachdem ein Zusammenhang mit einem Tiefgaragenbrand in Dresden-Pieschen hergestellt werden konnte, hatte die Polizei die potentiellen Anfahrts- und Fluchtwege nach möglicherweise weiteren Hinweisen, insbesondere auch in den öffentlichen Bereich hinein filmende Überwachungskameras, abgesucht und konnte an einem Geschäftshaus Videotechnik ausmachen. An einem Fenster im zweiten Obergeschoss war eine Kamera montiert, die jedenfalls so ausgerichtet war, dass sie auch den öffentlichen Straßenraum eines Abschnitts auf der Neustädter Seite hätte erfassen können. Die von der Polizei vorgenommene Auswertung der Videoaufnahmen bestätigte die Vermutung: Die betreffende Kamera erfasste die vor dem Geschäftsgrundstück befindliche Straße in voller Breite einschließlich der Gehwege sowie der Gebäudefront auf der gegenüberliegenden Straßenseite bis in Höhe der Oberkante des Erdgeschosses. Nachdem die Polizei dann auch tatsächlich noch das vermutliche Fluchtfahrzeug auf den Videoaufnahmen ermittelt und eine Aufnahme im Rahmen der Fahndung veröffentlich hatte, dauerte es nicht lange, bis mich erste Nachfragen und Beschwerden erreichten.

Bei meiner datenschutzaufsichtlichen Prüfung ging es nicht um die Veröffentlichung des Fahndungsfotos, sondern allein um die Problematik der permanenten Überwachung des öffentlichen Verkehrsraums durch eine nicht-öffentliche Stelle sowie um die durchgängige Überwachung eines auf der gegenüberliegenden Straßenseite befindlichen Hauseingangs und Gebäudeteils.

Allgemein rechtlich bekannt sein sollte, dass es Privaten grundsätzlich nicht erlaubt ist, öffentliche Verkehrsbereiche oder Nachbargrundstücke bzw. -gebäude mit Videotechnik zu überwachen. Regelmäßig als Zweck einer Videoüberwachung vertreten werden kann der Schutz des eigenen Grundstücks bzw. der darauf befindlichen Gebäude, Fahrzeuge und des sonstigen dort befindlichen Eigentums. Artikel 6 Absatz 1 Buchstabe f) DSGVO besagt, dass eine Verarbeitung personenbezogener Daten, hier: eine Videoüberwachung, nur 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. Für die Gewährleistung des Eigentumsschutzes am eigenen Grundstück fehlt es hingegen regelmäßig schon an der Geeignetheit und Erforderlichkeit einer Videoüberwachung angrenzender öffentlicher Verkehrsbereiche; eine Berufung auf eigene berechtigte Interessen ist nicht möglich bzw. schutzwürdige Interessen aller sich dort bewegenden Verkehrsteilnehmer stehen dem entgegen. Von notwehrähnlichen Situationen abgesehen verfügen nicht-öffentliche Verantwortliche nicht über die Befugnis, per Videografie personenbezogen den öffentlichen Verkehrsraum zu erfassen. Das verfassungsmäßige 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 daraus ergebenden schutzwürdigen Interessen betroffener Personen überwiegen das Interesse an einer präventiven Überwachung des Eigentums einerseits sowie der Beweissicherung im Fall von Sachbeschädigungen und Diebstählen andererseits.

Erst recht und ausnahmslos gilt dies für Nachbargebäude und die schutzwürdigen Belange der betroffenen Personen überwiegen das Interesse der Betreiber von Videoüberwachungsanlagen zudem immer dann, wenn die Kameras auch den regulären Zugang zu den Wohnungen erfassen. Die Bewohner können sich einer solchen Videoüberwachung in der Regel nicht entziehen, weil der Hauseingang im Normalfall der einzige reguläre

Zugang zu ihrer Wohnung und zu den Briefkästen ist. Bereits die Möglichkeit, dass ein Dritter jederzeit kontrollieren kann, welcher Bewohner wann welchen Besuch empfängt, kommt oder geht, setzt die Mieter einem erheblichen Überwachungs- und Anpassungsdruck aus.

Dem Verantwortlichen war dem Vernehmen nach bis zum Zeitpunkt der Veröffentlichung weder bekannt noch bewusst, dass die betreffende Kamera auch den Straßenbereich erfasste. Tatsächlich sollte sie nur der Überwachung des zwischen Geschäftshaus und Grundstücksgrenze (Gehweg) befindlichen Hofbereiches dienen. Seiner Auffassung nach musste die Kamera im Zuge von Fensterarbeiten versehentlich verstellt worden sein. Da er kein Monitoring der durch ihn betriebenen Videokameras durchgeführt habe und Auswertungen der Aufzeichnungen nur anlassbedingt durch einen Dienstleister vorgenommen würden, sei die Veränderung des Erfassungsbereiches von ihm selbst bis dahin unbemerkt geblieben, anschließend aber sofort korrigiert worden. Jedenfalls von letzterem konnte ich mich überzeugen. Bei einem unangekündigten Kontrollbesuch konnte ich feststellen, dass die öffentlichen Verkehrsbereiche nunmehr komplett ausgeblendet, d. h. geschwärzt worden waren. Wenige Tage danach ist – dies hatte mir der Verantwortliche bereits bei meinem Kontrollbesuch angekündigt – die Kamera zudem umgesetzt worden und befindet sich nunmehr in Erdgeschosshöhe im Hofbereich. Damit können auch nicht mehr Bereiche außerhalb des eigenen Hofes überwacht werden.

2.2.17 Offenbarung einer Bewerbung gegenüber dem bisherigen Arbeitgeber

Im letzten Berichtszeitraum wandte sich eine betroffene Person an meine Dienststelle und stellte dar, dass sie sich bei einem Arbeitgeber beworben und dabei um Erstattung der Fahrkosten gebeten habe, woraufhin dieser das dem aktuellen Arbeitgeber der betroffenen Person mitgeteilt habe. Der Beschwerdeführer erklärte, dass er daraufhin von seinem bisherigen Arbeitgeber zu einer Erklärung aufgefordert worden sei.

Die Einholung von Informationen durch potentielle Arbeitgeber bei dem gegenwärtigen oder früheren Arbeitgeber eines Bewerbers ist eine in der Praxis häufig auftretende Rechtsfrage. Nach alter Rechtslage war die Erhebung von Informationen gemäß § 4 Absatz 2 Bundesdatenschutzgesetz a.F. ohne Mitwirkung des Betroffenen nur zulässig, wenn die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordert hätte und keine schutzwürdigen Interessen des Betroffenen beeinträchtigt worden wären. Grundsätzlich waren Informationen zum Bewerber mit dessen Kenntnis und allenfalls

noch mit Einwilligung bei Dritten, insbesondere beim Noch-Arbeitgeber, einzuholen gewesen. Die Rechtslage hat sich nicht im Wesentlichen verändert. Auch nach neuer Rechtslage sind die Interessen des Bewerbers gemäß Artikel 6 Absatz 1 Buchstabe f) DSGVO zu berücksichtigen. Bei einer Einwilligung zur Befragung des bisherigen Arbeitgebers ist allerdings zu beachten, dass eine Freiwilligkeit des Bewerbers aufgrund der Möglichkeit, dass eine Verweigerung zu Nachteile im Bewerbungsverfahren führt, eingeschränkt sein wird. Ohnehin wird auch der bisherige oder ehemalige Arbeitgeber nicht ohne weitere Auskünfte zu erteilen befugt sein, Artikel 6 Absatz 1 DSGVO. Eine Einwilligung wird lediglich in Ausnahmefällen, etwa der Beiziehung von Unterlagen, über die der bisherige Arbeitgeber verfügt, als zulässig zu betrachten sein. Umfang, Tiefe und Ausmaß der Verarbeitung der Bewerberdaten hat sich an der Erforderlichkeit auszurichten, unter anderem Artikel 6 Absatz 1 Buchstaben b) und f) DSGVO. Darüber hinausgehende Datenverarbeitung ist unzulässig.

Im vorliegenden Fall war nach dem Vortrag der betroffenen Person noch nicht mal die Einholung weiterer Informationen über den Bewerber beabsichtigt und eine Erforderlichkeit zur Erreichung eines rechtlich anerkannten Zwecks nicht erkennbar.

2.2.18 Datenweitergabe an Inkassounternehmen

Die Weitergabe personenbezogener Daten an Inkassounternehmen war auch im Jahr 2019 erneut Gegenstand von aufsichtsrechtlichen Verfahren. Kern von entsprechenden Beschwerden ist vielfach, dass die Betroffenen schon das Bestehen der zugrundeliegenden Forderung bestreiten.

Soweit Betrugsvorwürfe im Raum stehen, kann ich die betroffenen Personen im Regelfall nur auf den Verbraucherschutz, die Staatsanwaltschaft und die Zivilgerichte verweisen. Bei typischen Konstellationen mit zweifelhafter Forderungsbegründung steht meine Behörde im Austausch mit der Verbraucherzentrale Sachsen. Eine Verweisung an die zuständige Inkassoaufsicht wegen Verstößen gegen den Rechtsrahmen für Inkassodienstleistungen hatte sich bei einzelnen Vorgängen bislang allerdings noch nicht aufgedrängt.

Datenschutzrechtlich ist folgendes zu beachten: Grundsätzlich ist der behauptete Forderungsinhaber auch bei bestrittenen Forderungen berechtigt, die personenbezogenen Daten des mutmaßlichen Schuldners an ein Inkassounternehmen weiterzuleiten. Dies gilt jedoch nur für diejenigen Daten, die zur Identifizierung von Gläubiger und Forderung nach § 11a Rechtsdienstleistungsgesetz absolut notwendig sind. Rechtsgrundlage hierfür ist nach

meiner Auffassung die Interessenabwägung nach Artikel 6 Absatz 1 Buchstabe f) DSGVO.

In Literatur und Instanzrechtsprechung wird zum Teil vertreten, derartige Datenweitergaben seien bei einem Zahlungsverzug zur Erfüllung eines (mutmaßlich) zugrundeliegenden Vertrags schon nach Artikel 6 Absatz 1 Buchstabe b) DSGVO zulässig. Hiergegen kann der Wortlaut der Vorschrift, die ausdrücklich voraussetzt, dass die Datenverarbeitung „für die Erfüllung eines Vertrags […] erforderlich" sein muss, ins Feld geführt werden. Die Beauftragung eines Inkassounternehmens kann zweckmäßig und unterstützend für die Durchsetzung der Erfüllung einer Forderung wirken, wird aber regelmäßig nicht erforderlich sein. Der Einzelfall ist zu betrachten. Eine Datenweitergabe ist nach meiner Einschätzung jedenfalls immer dann als unzulässig zu betrachten, wenn der behauptete Schuldner nicht zuvor (erfolglos) gemahnt, und die Beauftragung eines Inkassounternehmens angedroht worden ist. Dies folgt aus der Voraussetzung der Erforderlichkeit – unabhängig von der genauen Rechtsgrundlage – und aus dem Gebot der Datenminimierung aus Artikel 5 Absatz 1 Buchstabe c) DSGVO. Gleiches gilt, wenn der Schuldner eindeutig kundgetan hat, dass er die Forderung bestreitet, und sich in einem möglichen Rechtsstreit verteidigen will. Denn ohne Mahnung und Androhung erscheint eine Datenweitergabe nicht erforderlich, bei manifester Verteidigungsabsicht schon nicht geeignet. Ansonsten kann, in den Fällen, in denen Forderungen nicht beglichen bzw. nicht vollständig beglichen wurden, grundsätzlich davon ausgegangen werden, dass Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen, vgl. den Wortlaut von Artikel 6 Absatz 1 Buchstabe f) DSGVO.

Das tatsächliche Bestehen der geltend gemachten Forderung kann hingegen in die datenschutzrechtliche Bewertung nur in Extremfällen einfließen. Ein solcher Extremfall wäre etwa anzunehmen, wenn der behauptete Gläubiger weiß, oder davon ausgehen muss, dass die behauptete Forderung vor Gerichten keinen Bestand haben würde. Die entsprechende Bösgläubigkeit ist Ziel gerichtlicher (Muster-)Verfahren seitens einzelner Petenten oder des Verbraucherschutzes. Bei evidentem Missbrauchsverdacht, auffälligen und gehäuft in Beschwerden auftretenden Gläubiger-/Inkassokonstellationen regt meine Behörde entsprechende Klärungen an.

Die Weitergabe von besonders sensiblen Daten nach Artikel 9 Absatz 1 DSGVO an Inkassounternehmen kann zwar nach Artikel 9 Absatz 2 Buchstabe f) DSGVO zur Geltendmachung oder Ausübung von Rechtsansprüchen zulässig sein. Das oben zur Erforderlichkeit und Eignung Ausgeführte gilt hier allerdings in besonderem Maße.

2.2.19 Fotografieren von Parkverstößen

Der Datenschutzbeauftragte eines sächsischen Landratsamts informierte mich über folgenden Sachverhalt: Eine Privatperson fotografiert ein unrechtmäßiges geparktes Fahrzeug und übermittelt dieses Foto an das Landratsamt. Dieses leitet daraufhin ein Bußgeldverfahren ein. Die Fahrzeughalterin war der Auffassung, dass der Fotograf eine Datenschutzverletzung begangen hat und erstattete nun ihrerseits eine entsprechende Anzeige. Der Datenschutzbeauftragte bat mich dazu um Mitteilung, ob ein derartiges Foto im Rahmen von Ordnungswidrigkeiten weiter verarbeitet werden darf, also als Bestandteil der Akte zum Verfahren gespeichert werden darf.

Zunächst stellt das Fotografieren eine Verarbeitung personenbezogener Daten dar. Zwar ist nach Artikel 2 Absatz 2 Buchstabe c) DSGVO das Datenschutzrecht dann nicht anwendbar, wenn die Datenverarbeitung durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten erfolgt. Dies ist hier jedoch nicht der Fall, da sie im vorliegenden Fall zum Zweck der Weiterleitung an eine Behörde erfolgte.

Ich gehe jedoch davon aus, dass hier in Bezug auf den Fotografen ein berechtigtes Interesse gemäß Artikel 6 Absatz 1 Buchstabe f) DSGVO vorlag. Dieses umfasst neben wirtschaftlichen auch ideelle Interessen, vorliegend das Interesse an einer wirksamen Verfolgung von den Anzeigenden selbst behindernden Parkverstößen.

Es bestehen daher keine datenschutzrechtlichen Bedenken gegen die Verarbeitung derartiger Fotos in Ordnungswidrigkeitenverfahren. Vielmehr ist zu prüfen, ob genügend Anhaltspunkte aufgezeigt werden, die auf das tatsächliche Begehen einer Ordnungswidrigkeit hindeuten (§ 152 Absatz 2 StPO i.V. mit § 46 Absatz 1 OWiG).

So ist die für die Verfolgung von Ordnungswidrigkeiten zuständige Behörde auf eine entsprechende Anzeige hin berechtigt, den Sachverhalt weiter aufzuklären. Dies beinhaltet auch das Recht, die der zuständigen Behörde geschilderte Situation - hier in Form einer Bilddokumentation - in dem erforderlichen Umfang in einer geeigneten Art und Weise so zu dokumentieren, so dass die gewonnenen Erkenntnisse im Verwaltungsverfahren bzw.

in einem gegebenenfalls nachfolgenden gerichtlichen Verfahren belegbar bzw. nachprüfbar sind. Anhaltspunkte dafür, dass die Anfertigung des betreffenden Lichtbildes und dessen Speicherung in der Verwaltungsakte im vorliegenden Fall ausnahmsweise unverhältnismäßig sein könnte, sind nicht ersichtlich.

2.3 Einwilligungsfragen

2.3.1 Zweckbestimmung der Datenverarbeitung – Keine Datenverarbeitung ohne konkreten Verarbeitungszweck bei Einwilligungen

Die Verarbeitung personenbezogener Daten ist außerhalb ausschließlich persönlicher und privater Verhältnisse nur auf Rechtsgrundlage des Artikels 6 Absatz 1 zulässig. Der in der Praxis jedoch sehr häufige Rechtsgrund für eine Datenverarbeitung ist die Einwilligung der betroffenen Person, Artikel 6 Absatz 1 Buchstabe a) DSGVO.

Neben der Freiwilligkeit, der Wirksamkeit und dem Widerruf von Einwilligungen sind in meiner Beratungs- und Aufsichtspraxis insbesondere die Reichweite einer Einwilligung und deren Bindung an einen konkreten Zweck von Relevanz.

Die Vorschriften der Artikel 6 Absatz 1 Buchstabe a) und Artikel 9 Absatz 2 Buchstabe a) DSGVO legen fest, dass eine Einwilligung immer nur auf einen oder mehrere konkret bestimmte Verarbeitungszwecke bezogen ist. Nach Artikel 5 Absatz 1 Buchstabe b) DSGVO ist die Zweckgebundenheit jeder Verarbeitung personenbezogener Daten ein entscheidender Grundsatz jeder Verarbeitung personenbezogener Daten. Demzufolge sind Blankett- oder vorsorgliche Einwilligungen oder solche mit unklaren Zweckbestimmungen unwirksam.

Soweit eine freiwillige, in informierter Weise und unmissverständlich für den konkreten Fall erteilte Einwilligung vorliegt, sind auf deren Grundlage wiederum nur solche Verarbeitungen zulässig, die „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt“ sind, Artikel 5 Absatz 1 Buchstabe c) DSGVO. Das Gebot der Datenminimierung untersagt also die Verarbeitung personenbezogener Daten, wenn der von der Einwilligung umfasste Zweck auch mit vermindertem oder aufgehobenem Personenbezug etwa mittels Pseudonymisierung, aggregierter oder anonymisierter Daten, erreicht werden kann. In diesem Sinne ist die Verarbeitung personenbezogener Daten auf Einwilligungsgrundlage auch an der Erforderlichkeit zu messen.

Verschiedentlich ist demgegenüber ein Fehlverständnis der datenschutzrechtlich Verantwortlichen zu beobachten, dass diese eine Einwilligung als Möglichkeit für einen „Freibrief“ für beliebige Datenverarbeitung ansehen, indem entweder ein konkreter Zweck fehlt oder indem Informationen verarbeitet werden sollen, die nur bedingt dem der Einwilligung zu Grunde liegenden Zweck zu dienen geeignet sind.

Die vorgenannte Voraussetzung der Erforderlichkeit der konkreten Datenverarbeitung für den verfolgten Zweck ist auch auf der Ebene der Wirksamkeit der Einwilligung von Bedeutung. Nach Artikel 4 Nummer 11 DSGVO gilt als wirksame Einwilligung nur die freiwillig abgegebene Willensbekundung. Für die Beurteilung der Freiwilligkeit ist nach Artikel 7 Absatz 4 DSGVO wiederum essentiell, ob die betreffende Verarbeitung personenbezogener Daten für die Erfüllung des Vertrags erforderlich ist. Entsprechend liegt im Regelfall keine wirksame Einwilligung vor, wenn die von der abverlangten Einwilligungserklärung umfasste Datenverarbeitung für den Vertragsgegenstand nicht erforderlich ist, vergleiche Artikel 7 Absatz 4 DSGVO. Die Grenzen des Koppelungsverbots – des Abverlangens einer Einwilligung, ohne dass diese für das der Datenverarbeitung zu Grunde liegende Rechtsverhältnis erforderlich wäre – sind in der Rechtsprechung und aufsichtsrechtlichen Spruchpraxis noch nicht abschließend geklärt worden. Auch ist die Grundfrage, wieweit bereits die Finanzierung der Vertragsleistung einen ausreichenden Zusammenhang mit der Vertragserfüllung im Sinne einer Vereinbarung von „Geld gegen Daten“ darstellen kann, noch Gegenstand von Gesetzgebungsverfahren. Dennoch ist jedenfalls eine Datenverarbeitung, deren Zweck in keinem direkten Bezug zum Vertragszweck steht, im Regelfall nicht wirksam durch eine Einwilligung zu rechtfertigen.

Es gilt: Keine Datenverarbeitung ohne konkreten Zweck bei Einwilligungen.

Zweckänderungen sind schließlich nur unter den engen Voraussetzungen des Artikel 6 Absatz 4 DSGVO als Folge einer vorzunehmenden weitreichenden Abwägung, die das Verhältnis zum Ursprungszweck, die Interessen der betroffenen Personen, die Art der personenbezogenen Daten, und informationssicherheitstechnische und datenschutzorganisatorische Vorkehrungen einzubeziehen hat, zulässig.

2.3.2 Fotos beim Neujahrsempfang

Ich wurde darauf hingewiesen, dass eine Anmeldung zum Neujahrsempfang des Oberbürgermeisters einer sächsischen Kommune nur mit einer Einwilligung in die Erstellung

und Veröffentlichung von Fotos möglich war. Nach einem unverzüglich erfolgten Widerruf der Einwilligung sei mitgeteilt worden, dass eine Teilnahme an der Veranstaltung nunmehr nicht mehr möglich sei.

Ich habe die betroffene Kommune dazu auf Folgendes hingewiesen:

Fraglich ist zunächst, ob diese Verknüpfung einen Verstoß gegen das Kopplungsverbot des Artikel 7 Absatz 4 DSGVO darstellt. Dies könnte der Fall sein, wenn die Teilnahme am Neujahrsempfang einen Vertrag darstellt und die Einwilligung für die Teilnahme am bzw. die Durchführung des Neujahrsempfangs nicht erforderlich ist. Ein Vertrag wird bei einer derartigen Einladung mangels Gegenleistung jedoch regelmäßig nicht vorliegen.

Jedenfalls muss diese Einwilligung aber gemäß Artikel 7 Absatz 3 DSGVO frei widerruflich sein. Es muss den Teilnehmern daher möglich sein, diese jederzeit, also beispielsweise auch nach der Teilnahme am Neujahrsempfang zu widerrufen. Die Kommune müsste dann bereits gemachte Veröffentlichungen sowohl in analoger als auch in digitaler Form nachträglich entsprechend bearbeiten.

Vorzugswürdig ist daher, Fotos des Neujahrsempfangs als solchen zu veröffentlichen und nicht einzelne Individuen abzubilden. Dies ist gemäß § 23 Absatz 1 Nummer 3 KUG grundsätzlich ohne Einwilligung zulässig. Zu berücksichtigen sind dabei jedoch die berechtigten Interessen der Abgebildeten gemäß § 23 Absatz 2 KUG.

Bei einzelnen Individuen können die Voraussetzungen des § 23 Absatz 1 Nummer 1 KUG (Personen der Zeitgeschichte) vorliegen. Darüber hinaus kann im Einzelfall eine Veröffentlichung aber auch wegen eines berechtigten Interesses der Landeshauptstadt Dresden gemäß Artikel 6 Absatz 1 Buchstabe f) DSGVO ohne Einwilligung zulässig sein. Dem steht auch nicht Artikel 6 Absatz 1 Satz 2 DSGVO entgegen (wonach sich Behörden bei der Erfüllung ihrer Aufgaben nicht auf ein berechtigtes Interesse berufen können), da eine entsprechende Öffentlichkeitsarbeit nicht zu den gesetzlich zugewiesenen Aufgaben einer Behörde zählt. In diesem Fall wäre nur ein Widerspruch der Abgebildeten unter den Voraussetzungen des Artikels 21 DSGVO möglich.

In jedem Fall sind die Teilnehmer bei der Anmeldung jedoch gemäß Artikel 13 DSGVO beispielsweise über den Zweck der Erhebung oder die Aufbewahrungsdauer zu informieren.

2.3.3 Datenverarbeitung bei Adoptionsverfahren

Fragen zur Datenerhebung und Datenverarbeitung im Rahmen von Adoptionsverfahren waren Gegenstand einer Anfrage, konkret ob diese auf eine gesetzliche Grundlage oder Einwilligung gestützt werden können.

Das Adoptionsvermittlungsgesetz ist im Katalog des § 68 SGB I aufgenommen, dort unter Nummer 12. Es finden somit die Regelungen des SGB Anwendung. Auf die Geltung der § 67 ff SGB X – mit der Maßgabe einer engen Zweckbindung - verweist ausdrücklich auch § 9d AdVermiG.

Insoweit differenziert das SGB X (auch weiterhin) danach, ob es sich um eine Datenerhebung – in diesem Fall gilt § 67a SGB X - oder um eine sonstige Datenverarbeitung nach § 67b SGB X handelt.

Im Gegensatz zu § 67b Absatz 2 SGB X, der folgenden Wortlaut hat:

2) Zum Nachweis im Sinne des Artikels 7 Absatz 1 der Verordnung (EU) 2016/679, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat, soll die Einwilligung schriftlich oder elektronisch erfolgen. Wird die Einwilligung der betroffenen Person eingeholt, ist diese auf den Zweck der vorgesehenen Verarbeitung, auf die Folgen der Verweigerung der Einwilligung sowie auf die jederzeitige Widerrufsmöglichkeit gemäß Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 hinzuweisen

findet sich eine entsprechende Regelung gerade nicht in der Datenerhebungsvorschrift des § 67a SGB X. Dies entspricht auch der bisherigen Rechtslage, vgl. bereits meine Ausführungen im 11. Tätigkeitsbericht meiner Behörde unter Verweis auf die Rechtsprechung des BSG.

Die Erhebung personenbezogener Daten ist schon deswegen nicht aufgrund bloßer Einwilligung zulässig, weil § 67a Absatz 1 Satz 1 SGB X dies für die Datenerhebung im Unterschied zur (weiteren) Verarbeitung von Sozialdaten und deren Nutzung gemäß § 67b Absatz 1 Satz 1 SGB X gar nicht als Erlaubnistatbestand vorsieht, wie auch das Bundessozialgericht in seiner Entscheidung vom 28. November 2002, B7/1 A 2/00 R, hervorgehoben hat (im Einzelnen siehe 11. Tätigkeitsbericht unter 10.2.2, S. 113, drittletzter Absatz).

Etwas Anderes galt indes auch bereits früher für die sonstige Datenverarbeitung. So hat das Bundessozialgericht in seinem Urteil vom 25. Januar 2012 (Az.: B 14 AS 65/11 R, gefunden in: juris) dort eine Gleichrangigkeit von gesetzlicher Ermächtigungsgrundlage und Einwilligung des Betroffenen ausgesprochen, indem es pauschal erklärt:

…„ Denn die Verarbeitung (Anm.: Die Verarbeitung umfasst auch die Übermittlung von Sozialdaten, § 67 Absatz 6 Satz 1 SGB X) von Sozialdaten ist nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat (§ 67b Absatz 1 Satz 1 SGB X).“

Aufgrund der weiterhin geltenden Gesetzessystematik hinsichtlich der Trennung zwischen Datenerhebung und sonstiger Datenverarbeitung gehe ich nicht davon aus, dass nunmehr § 67b Absatz 2 SGB X auch im Rahmen des § 67a SGB X Anwendung finden soll.

Insoweit ist - auch weiterhin und unter Geltung der DSGVO - zu prüfen, welche personenbezogenen Daten die zuständige Adoptionsvermittlungsstelle zur Aufgabenerfüllung benötigt, die dann auf Grundlage des § 67a SGB erhoben werden dürfen, ohne dass es hierzu einer Einwilligung des Betroffenen bedarf. Insoweit ist dann auch keine Einwilligung einzuholen, damit würde man dem Betroffenen ein Entscheidungsrecht über das Abfassen seiner personenbezogenen Daten suggerieren, die er aber nach geltender Rechtslage gar nicht hat. Insoweit wird vertreten, dass das Einholen einer Einwilligung - wenn denn eine gesetzliche Grundlage besteht - rechtswidrig ist; zumindest geht diese ins Leere.

Der Weg über die Verarbeitung personenbezogener Daten auf Einwilligungsbasis findet daher nur bei den in § 67b SGB X normierten Verarbeitungsschritten statt.

Ergänzend verweise ich gerade in dem wie hier sensiblen Bereich der Adoptionsvermittlung noch auf Erwägungsgrund 43 Satz 1 zu Artikel 7 DSGVO (Bedingungen für die Einwilligung):

„Um sicherzustellen, dass die Einwilligung freiwillig erfolgt ist, sollte diese in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall

unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern."

2.3.4 Verarbeitung sensibler Daten durch einen Lohnsteuerhilfeverein

Im letzten Berichtszeitraum wendeten sich Beschwerdeführer wegen der personenbezogenen Datenverarbeitung eines Lohnsteuerhilfevereins an meine Behörde. Die Petenten trugen vor, dass ihnen zur Erledigung ihrer Steuererklärung von dem Verein wegen der sensiblen Daten per Einwilligung abverlangt werde, dass auch besonders schützenswerte Daten im Sinne von Artikel 9 DSGVO verarbeitet werden. Moniert wurde unter anderem, dass damit auch Informationen zu politischen Meinungen, sexuellen Neigungen und Gesundheitsdaten verarbeitet werden könnten. Die Beschwerdeführer führten an, dass diese Informationen für die Erledigung der Steuererklärung nicht erforderlich seien. Dementsprechend habe man sich mit der Datenverarbeitung nicht einverstanden erklärt. Der Lohnsteuerhilfeverein wiederum aber aufgrund der Verweigerung keine Steuererklärung an das Finanzamt weitergeleitet.

In meiner Antwort an die Petenten teilte ich diesen mit, dass aufgrund der Tätigkeit eines Lohnsteuerhilfevereins auch damit zu rechnen sei, dass Informationen zu politischen Meinungen, sexuellen Neigungen bzw. Gesundheitsdaten verarbeitet werden könnten. Namentlich kämen Beitragsbestätigungen politischer Parteien oder andere nicht von dem Verein voraussehbare Unterlagen, aus denen sich gesundheitliche Informationen ergeben, wie zum Beispiel körperliche Einschränkungen in Betracht, die mithilfe bestimmter Belege steuerlich geltend gemacht werden könnten.

Es versteht sich, dass Informationen dieser Art nicht in jedem Streitfall verarbeitet werden müssen. Die entsprechende Information und Einwilligungsanforderung des Vereins hielt ich dennoch für zutreffend und erforderlich. Seitens des Vereins als Verantwortlichem kann wiederum im Vorhinein nicht erkannt werden, welche (sensiblen) Unterlagen konkret eingereicht werden müssen.

2.3.5 Internet-Gratisangebote mit Werbebezugsklausel - „Service gegen Daten"

Internetnutzern ist es geläufig: Wo immer etwas umsonst zu sein scheint, lauert irgendwo ein Hintertürchen, das dem Anbieter dann irgendwie Geldquellen und monetäre Einnahmen verschaffen soll, nicht zuletzt auch mittels Werbung. Zum Teil wird juristisch hergeleitet, dass solche Modelle unter dem Regime der DSGVO generell unzulässig seien,

so z. B. Taeger in Taeger/Gabel, DSGVO, BDSG, Ktr. 2019, zu Artikel 7 DSGVO Rdn. 91.

Eine rechtsstaatliche ordnungsgemäße Aufsichtspraxis kann Grundfreiheiten einzelner Unternehmen und Vertragsparteien nicht ausblenden, während es zudem trotz der Befugnisse der Aufsichtsbehörden nach der EU-Verordnung - für die Öffentlichkeit wahrnehmbar - zunehmend schwerer wird, marktbeherrschende Internetkonzerne und deren datenverarbeitungsintensive Geschäftsmodelle zu regulieren.

Eine zu der vorbeschriebenen Problematik passende Beschwerde betraf denn auch ein kleines in Sachsen ansässiges Webportal, das den „kostenlosen“ Download einer Art Checkliste ermöglicht, wofür im Gegenzug die Zusendung eines Werbe-Newsletters hingenommen werden sollte. Das Dokument wollte der Beschwerdeführer beziehen, nicht jedoch den Newsletter empfangen.

Im Ergebnis der rechtlichen Prüfung des Vorgangs hatte meine Behörde dem Petenten mitzuteilen, dass sein in Ansatz gebrachtes Argument, infolge Nichtigkeit einer aus Sicht des Betroffenen nicht freiwilligen Einwilligung zum Newsletter stünde ihm der Download quasi bedingungslos zu, aus datenschutzaufsichtlicher Sicht nicht durchgreifen könne.

Eine verfassungskonforme Anwendung der DSGVO bietet keine rechtsstaatlich konforme Handhabe, die in letzter Konsequenz eine Untersagung des beschriebenen Geschäftsmodells zulassen würde. Regulierende Eingriffsbefugnisse auf Grundlage des europäischen Rechts aufgrund besonderer Marktmacht eines Marktteilnehmers waren im zu prüfenden Einzelfall nicht entscheidend. Auch waren dafür weder Anhaltspunkte vorgetragen noch auf andere Weise ersichtlich geworden.

Auf folgende grundsätzliche Erwägungen hat meine Dienststelle ihre Auffassung gestützt: Rechtsgut des Erlaubnistatbestandsmerkmals „Vertrags” des Artikel 6 Absatz 1 Buchstabe b) DSGVO ist eben dieses aus der Vertragsfreiheit stammende schuldrechtliche Institut, das Eingriffe in die informationelle Selbstbestimmung nach der Verordnung zu begründen können soll. Dass, wer einen Vertrag schließt, nicht mehr gänzlich frei darin ist, damit einhergehende erforderliche Datenverarbeitung jederzeit beenden zu können, leuchtet dabei bereits nach allgemeinem Rechtsgefühl ein. Bei dem Erlaubnistatbestand des Artikel 6 Absatz 1 Buchstabe b) wird das informationelle Selbstbestimmungsrecht

den vertraglichen Umständen und der Vertragsfreiheit angepasst. Ein der Datenverarbeitung entgegenstehender Wille des Betroffenen wird von der Rechtsordnung als rechtlich irrelevant angesehen, worin man auch eine Ausprägung von venire contra factum proprium sehen kann: wer einen bestimmten Vertrag will, kann sich rechtlich der Datenverarbeitung nicht entziehen, die für diesen Vertrag erforderlich ist.[1]

Möglicherweise in entsprechender Anwendung zur gefestigten Rechtsprechung für das Bezahl-Segment hatte der Portalbetreiber die Verbindlichkeit der Bestellung mit einem betitelten Button „Ja ich möchte in den Newsletter aufgenommen werden“ hergestellt, der nach meiner Überzeugung nutzerseitig als eindeutig und unmissverständlich zu erkennen war. Die Annahme eines Werbe-Newsletters ließ sich daher nicht anders als eine mit dem Vertragsschluss geschuldete Gegenleistung verstehen. Für diese Fälle gilt nach Rechtsmeinung meiner Dienststelle folgendes: Wird die Datenverarbeitung zum Zwecke der Werbung zum integralen Bestandteil des Vertrages gemacht, wird das Kopplungsverbot nicht berührt. Bei einer solchen Lösung muss jedoch klar und verständlich zum Ausdruck gebracht werden, dass die Gegenleistung des Nutzers in dem Bereitstellen seiner Daten zum Zwecke der Werbung besteht.[2] Die Klarheit und Eindeutigkeit der vertraglichen Bedingungen war in dem mir zur Prüfung vorgelegenen Fall den Umständen nach nicht fraglich. Inwieweit die Verarbeitung der personenbezogenen Datenverarbeitung bzw. der weitere Versand des Newsletters nach einem Widerspruch einer betroffenen Person einzustellen gewesen wäre, war nicht zu betrachten. Artikel 21 Absatz 2, Absatz 3 DSGVO regelt den Widerspruch (scheinbar) unmittelbar nur für die Fälle, in denen eine Verarbeitung auf Grundlage einer Interessenabwägung in Wahrnehmung berechtigter Interessen erfolgt ist, Artikel 6 Absatz 1 Buchstabe f) DSGVO.

Als Praxishinweis bleibt den Anbietern unentgeltlicher und mit Werbung refinanzierter Vertriebsmodelle im Internet noch anzuraten, die sinngemäße, aber sodann möglichst akkurate Übernahme der im Bezahl-Segment geltenden und etablierten Anforderungen an Transparenz und benutzerfreundliche Technikanwendung zu empfehlen; insbesondere gilt dies für den Einbau eines hinreichend wahrnehmbaren und leicht verständlichen

[1] Veil (2019), https://www.cr-online.de/blog/2019/03/18/die-schutzgutmisere-des-datenschutzrechts-teil-ii/

[2] Biesterfeld-Kuhn (2018), https://www.lhr-law.de/magazin/datenschutzrecht/kopplungsverbot-datenschutz-grundverordnung-dsgvo

Schalters auf der grafischen Benutzeroberfläche („Button“), mit dessen Betätigen ein Angebot vom Nutzer verbindlich angenommen werden kann.

2.3.6 Erforderlichkeit der Einholung einer Einwilligung zur Offenlegung von Vergleichsmieten

Verantwortliche berufen sich bisweilen auf Datenschutz, zu schützende Persönlichkeitsrechte Dritter und die Erforderlichkeit einer Einwilligung zur Abwehr der Einsichtnahme oder Offenlegung ihrer Unterlagen gegenüber Personen, mit denen sie in Rechtsbeziehung stehen, obwohl entsprechendes bei genauer Betrachtung eben gerade nicht verlangt ist. Derartige Konstellationen werden mir zuweilen auch aus dem Bereich der Wohnungswirtschaft zugetragen. In einem Fall behauptete der Vermieter, der eine Mieterhöhung durchzusetzen bestrebt war, Datenschutzgründe, um betroffenen Mietern die Einsichtnahme in seine den Mieterhöhungsanspruch belegenden Unterlagen zu verwehren.

Hierzu vertrete ich nachstehende Auffassung: Vermieter können sich nicht auf das Datenschutzrecht berufen, um sich ihrer (datenschutzkonform erfüllbaren) Pflichten und Obliegenheiten zu entledigen. So obliegt einem Vermieter, der eine Mieterhöhung auf Basis von Vergleichsmieten begehrt, drei vergleichbare Wohnungen und deren Miete zu benennen, § 558a Absatz 2 Nummer 4 BGB. Die Notwendigkeit der überprüfbaren Vergleichbarkeit macht regelmäßig die genaue Identifizierung der betreffenden Wohnungen erforderlich, was wiederum typischerweise den Mieter identifizierbar macht. Die konkrete Vergleichsmiete kann also – abhängig von der genauen Situation – ein personenbezogenes Datum darstellen, das datenschutzrechtlich geschützt ist. Vermieter können daher regelmäßig Vergleichsmieten nicht aus ihrem eigenen Vermietungsbestand belegen, ohne eine Einwilligung der betroffenen Mieter einzuholen. Fehlende Einwilligungen befreien jedoch Vermieter nicht von seiner Obliegenheit zum Beleg der konkreten Vergleichsmiete. Dies ergibt sich zum einen aus der Parallelität von Miet- und Datenschutzrecht, zum anderen aus den vielfältigen anderen Möglichkeiten für Vermieter, entsprechende Vergleichsmieten zu belegen.

2.4 Sensible Daten, besondere Kategorien personenbezogener Daten

2.4.1 Datenzugriff durch Medizinstudenten, Famulanten und Schülern bei Tätigkeit in Arztpraxen

Ein betrieblicher Datenschutzbeauftragter wandte sich im Berichtszeitraum mit einer Anfrage an die Aufsichtsbehörden des Bundes und der Länder. Die Anfrage bezog sich auf den Umgang in einer Arztpraxis mit Studenten, Ärzten im Praktikum und Schülern o. a., die dort tätig werden, aber in keinem Anstellungsverhältnis zur Arztpraxis stehen. Konkret ging es um die Frage der Einsichtnahme in Patientenakten und um die Verarbeitung von Patientendaten.

Die Aufsichtsbehörden sind übereingekommen, dass bei länderübergreifenden Anfragen nur eine abgestimmte Antwort erfolgt, die von der Aufsichtsbehörde koordiniert und erstellt wird, in deren Zuständigkeitsbereich die anfragende Stelle oder der Verantwortliche ihren Sitz haben.

Die Verarbeitung von Gesundheitsdaten als besondere Kategorie personenbezogener Daten ist nach Artikel 9 Absatz 1 DSGVO grundsätzlich nicht statthaft, es sei denn gesetzliche Ausnahmen greifen. In Artikel 9 Absatz 2 DSGVO sind wiederum Ausnahmen vom grundsätzlichen Verbot der Verarbeitung abschließend geregelt. Es war insoweit zu überlegen, ob bei den o. g. mitwirkenden Auszubildenden einer der in Artikel 9 Absatz 2 DSGVO aufgeführten Ausnahmetatbestände vorliegt.

Nach Auffassung meiner Behörde unterfallen Medizinstudenten, die in einer Praxis z. B. als Famulanten tätig werden, der ärztlichen Schweigepflicht nach § 203 Absatz 3 Satz 2 StGB. Danach stehen den in Absatz 1 und Satz 1 Genannten ihre berufsmäßigen Gehilfen und die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind. In der einschlägigen Kommentarliteratur zum Strafgesetzbuch und zur Vorschrift des § 203 Absatz 3 wird als Beispiel für Personen, die zur Vorbereitung auf den Beruf tätig sind, der „famulierende Medizinstudent“ genannt, vgl. z. B. Eisele in Schönke/Schröder, Kommentar zum StGB, 30. Auflage 2019, Randnummer 27 zu § 203 StGB.

Danach unterliegt ein Medizinstudent, selbst wenn er ohne Vertrag ein Praktikum in der Arztpraxis ableistet, der Geheimhaltungspflicht nach § 203 Absatz 3 Satz 2 StGB. Dann fällt er auch unter die Ausnahme des Artikel 9 Absatz 3 i. V. m. Artikel 9 Absatz 2 Buchstabe h) DSGVO, wenn er während des Praktikums Einsicht in Patientendaten nimmt und

diese verarbeitet. Einer gesonderten Einwilligung für Einsichtnahme und Verarbeitung der Daten bedarf es dann nicht. Der in der Anfrage auch angesprochene „Arzt im Praktikum“ wurde vor längerem abgeschafft.

Zum Teil wird aber auch die Meinung vertreten, dass die Tätigkeit der Auszubildenden unter keinen der Ausnahmetatbestände des Artikels 9 Absatz 2 Buchstabe b) bis j) DSGVO fällt. Würde man dem folgen, hätte die Kenntnisnahme der Gesundheitsdaten durch mitwirkende Auszubildende dann ausschließlich aufgrund einer Einwilligungserklärung des Patienten zu erfolgen; erst dann wäre die Verarbeitung nach Artikel 9 Absatz 2 Buchstabe a) DSGVO zulässig.

Sofern jedenfalls die Verarbeitung auf eine Einwilligung gestützt wird, hat der Verantwortliche nach Artikel 7 DSGVO nachweisen, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. Die Einwilligung ist auch nur dann wirksam, wenn sie ausdrücklich und durch eine eindeutige bestätigende Handlung erfolgt, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Ohne Einwilligung des Patienten darf der Arzt z. B. dem oben benannten Personenkreis weder Einsicht in die Patientenakte noch eine Teilnahme an Patientengesprächen gewähren. Zur Erfüllung des Ziels der jeweiligen Ausbildungsmaßnahme besteht jedoch grundsätzlich die Möglichkeit, diesem Personenkreis anonymisierte Patientenakten zur Bearbeitung oder als Anschauungsmaterial zur Verfügung zu stellen. Darüber hinaus steht es dem Patienten frei, die Einwilligung jederzeit ohne Angabe von Gründen für die Zukunft zu widerrufen.

Übereinstimmend vertreten jedenfalls sämtliche Aufsichtsbehörden die Auffassung, dass bei Schülern keiner der Ausnahmetatbestände des Artikels 9 Absatz 2 Buchstabe b) bis j) DSGVO vorliegt. Diese dürfen insoweit nur bei Vorliegen einer Einwilligung nach Artikel 9 Absatz 2 Buchstabe a) DSGVO in Patientendaten Einsicht nehmen und diese verarbeiten.

2.4.2 Arztpraxisübernahme, An wen darf ein Arzt, der eine Praxis übernommen hat, die Originalunterlagen der Patienten seines Vorgängers herausgeben?

Ein Arzt, der eine Praxis übernommen hat (Praxisnachfolger), stellte mir mehrere Fragen in Bezug auf den Umgang mit Patientenakten, die er von seinem Vorgänger übernommen

hat. Er bat um Stellungnahme, ob er Originalunterlagen von Patienten herausgeben dürfe, die er selbst nie behandelt bzw. gesehen hat.

Der Behandelnde hat nach § 630f Absatz 3 BGB die Patientenakte für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach anderen Vorschriften andere Aufbewahrungsfristen bestehen.

Die berufsrechtliche Dokumentationspflicht bzw. Aufbewahrungsfrist für ärztliche Aufzeichnungen beträgt nach § 10 Absatz 3 Berufsordnung der Sächsischen Landesärztekammer 10 Jahre, soweit nicht nach gesetzlichen Vorschriften eine längere Aufzeichnungspflicht besteht.

Von der Aufbewahrungspflicht zu unterscheiden ist die Frage des Zugriffs, d. h. die Verfügungsbefugnis über die Patientenakten des übergebenden Arztes (Vorgänger des Praxisnachfolgers). Bei der Praxisübergabe an einen Praxisnachfolger wurde aus Praktikabilitätsgründen bei manuell geführten Patientenakten und -daten das sog. „Zwei-Schrank-Modell“ entwickelt. Der Praxisnachfolger verpflichtet sich durch den Übernahmevertrag die Patientenakten seines Vorgängers zu verwahren und nur auf die einzelne Patientenakte Zugriff zu nehmen, wenn der jeweilige Patient den Praxisnachfolger aufsucht und von diesem behandelt wird.

Bei diesem Modell wird zwischen der Übertragung des generellen Gewahrsams an dem Gesamtaktenbestand und der daten- und patientenschutzrechtlich sensiblen konkreten Einsichtnahme unterschieden.

§ 10 Absatz 4 Satz 2 der Berufsordnung der Sächsischen Landesärztekammer legt fest, dass der Arzt, dem bei einer Praxisaufgabe oder Praxisübergabe ärztliche Aufzeichnungen über Patienten in Obhut gegeben werden, diese Unterlagen unter Verschluss zu halten hat und sie nur mit Einwilligung des Patienten einsehen oder weitergeben darf.

Bei elektronisch geführten Patientendaten sind der alte Bestand zu sperren und der Zugriff hierauf z. B. mittels Passwort zu sichern. Für einen erstmaligen Zugriff auf einen Patientendatensatz durch den Praxisnachfolger ist die Zustimmung des Patienten erforderlich. Liegt diese vor, so darf insoweit der Datensatz vom Praxisnachfolger freigeschaltet und weitergenutzt werden.

Wechselt ein Patient des übergebenden Arztes zu einem anderen Arzt, ohne dass der Praxisnachfolger den Patient behandelt hat, so ist aus datenschutzrechtlicher Sicht die Weitergabe des Originals der Patientenakte an den anderen Arzt mit dem Einverständnis des Patienten zulässig.

Des Weiteren bat mich der Praxisnachfolger um Stellungnahme, ob er die Originalunterlagen eines Patienten, der den Arzt wechselt, herausgeben darf, den er schon behandelt bzw. gesehen hat.

Behandelt der Praxisnachfolger einen Patienten seines Vorgängers, so klärt er üblicherweise zu Beginn der Behandlung, ob dieser einverstanden ist, dass der Praxisnachfolger die Patientenakte seines Vorgängers übernimmt. Erteilt der Patient dazu sein Einverständnis, so kann der Praxisnachfolger Zugriff auf dessen bisherige Patientenakte nehmen.

Wechselt dieser Patient anschließend zu einem anderen Arzt, so kann der Patient nicht fordern, dass der Praxisnachfolger dem anderen Arzt die Originalakte zu überlassen hat, falls er zu Beginn der Behandlung damit einverstanden war, dass der Praxisnachfolger die Patientenakte seines Vorgängers übernimmt. Ebenso verhält es sich in Bezug auf die (fortgeführte) Originalakte, zu der Behandlung, die durch den Praxisnachfolger selbst vorgenommen wurde. Der Patient hat jedoch die Möglichkeit, bei einem Arztwechsel über den Arzt oder selbst, einem dritten und neu behandelnden Arzt eine Kopie der Akte weiterzugeben.

2.4.3 Fehlversand einer Arztrechnung - Zustellung einer fremden Rechnung unter kuriosen Umständen

Mich erreichte die Rüge einer Beschwerdeführerin, die bei einer Bank in einem anderen Bundesland arbeitet. Diese monierte, dass sie über die Leipziger Filiale ihrer Bank einen an sie adressierten Umschlag einer Leipziger Ärztin, die ihr nicht bekannt sei, erhalten habe. Der Umschlag habe eine Rechnung für eine Patientin enthalten, die sie ebenso nicht kenne. Der Briefumschlag sei an eine nachnamensgleiche Person in Leipzig, unter dem Straßennamen der Bankfiliale der Bank in Leipzig, bei der sie beschäftigt sei, adressiert gewesen. Leipzig sei jedoch nicht ihr Dienstsitz. Die innenliegende Rechnung führe Name und Adresse einer Patientin mit einem anderen Nachnamen sowie eine Kostenposition für eine Behandlung samt einem Geldbetrag auf.

Die Beschwerdeführerin führte aus, dass bei einem Anruf in der Arztpraxis, um aufzuklären, wie es dazu kommen konnte, dass ein an sie adressierter Brief samt Rechnung an ihre Leipziger Firmenadresse versandt worden sei, habe sie keine zufriedenstellende Antwort erhalten. Ihre schriftliche Aufforderung an die Arztpraxis auf Auskunft über die Herkunft ihrer personenbezogenen Daten nach Artikel 15 DSGVO sei zudem unbeantwortet geblieben.

Mit ihrer Beschwerde bat sie um Aufklärung, woher die Arztpraxis ihren Namen und ihren Arbeitgeber kenne und wieso diese ihr eine Rechnung einer ihr nicht bekannten Person sende. Des Weiteren rügte sie die nicht erteilte Auskunft.

Die Ärztin, teilte in ihrer Stellungnahme zu dem Vorfall mit, dass ihre Praxismitarbeiterin das Schreiben an eine kommunale Behörde habe senden wollte. Diese verfügt in Leipzig, im gleichen Bürogebäude wie die Filiale der Bank, bei der die Beschwerdeführerin arbeitet, über einen Geschäftssitz. Versehentlich habe die Praxismitarbeiterin die Behörde nicht auf dem Briefumschlag eingetragen, sondern lediglich einen Nachnamen, nämlich den der Behördenbediensteten und die Straßenanschrift. Der in der handschriftlichen – schwer lesbaren bzw. unleserlichen - Schreibweise auf dem Umschlag der der Beschwerdeführerin ähnelnde Nachname sei tatsächlich der der zuständigen Bearbeiterin der Behörde, der die Rechnung für die Behandlung der Patientin zugestellt werden sollte. Nicht erklärbar sei, so die Arztpraxis, angesichts der ungenauen Adressatenangaben gewesen, wieso der Brief von dem Postdienstleister an die Filiale der Bank, die sich im gleichen Gebäude befindet, zugestellt wurde. Eine Rücksendung seitens der Post mit dem Vermerk „Nicht zustellbar/Anschrift nicht korrekt“ sei nicht erfolgt.

Wie es letztendlich zur Zustellung an die Bank kam, ließ sich nicht mehr vollständig aufklären. Auch bei der Adressierung des fraglichen Briefumschlags hatten nach meiner Überzeugung keine personenbezogenen Daten der Beschwerdeführerin Verwendung gefunden, da die Angabe nicht auf den Namen der Petentin, sondern auf den der Bearbeiterin der Behörde lauten sollte. Der Arztpraxis wurde gleichwohl aufgegeben, die geforderte (Negativ-)Auskunft nach Artikel 15 DSGVO nachträglich zu erteilen und darzutun, wie es zu der gekommen war. Des Weiteren wurde der Ärztin aufgegeben, die betroffene Patientin von der Fehlzustellung der sie betreffenden Rechnung zu informieren sowie datenschutzorganisatorische Maßnahmen zur künftigen Fehlervermeidung zu ergreifen.

3 Betroffenenrechte

3.1 Spezifische Pflichten des Verantwortlichen (inklusive Informationspflichten)

3.1.1 Informationspflicht bei Videoüberwachung

Die Anforderungen an eine transparente und umfassende Information der betroffenen Person ergeben sich bei einer Videoüberwachung auch aus Kapitel III der DSGVO, insbesondere den Artikeln 12 und 13 DSGVO. Nach deren Vorgaben ist auf die Video-überwachung transparent und fair und damit adressatengerecht hinzuweisen. Diese Hinweise haben regelmäßig frühzeitig zu erfolgen, so dass betroffene Personen noch die Möglichkeit bleibt, der Videoüberwachung auszuweichen bzw. ihr Verhalten darauf entsprechend auszurichten.

Um den sich aus dem Umfang der nach Artikel 13 DSGVO bereitzustellenden Informationen praxisgerecht entsprechen zu können, hatten sich die deutschen Aufsichtsbehörden auf die Empfehlung verständigt, dass betroffene Personen in zwei Schritten informiert werden können. Inzwischen besteht darüber auch auf europäischer Ebene Konsens, vgl. dazu Punkt 7 der Leitlinien des Europäischen Datenschutzausschusses zur Videoüberwachung (Guidelines 3/2019 on processing of personal data through video devices, Version 2.0, adopted on 29 January 2020).

Ein optisch präsentes und geistig erfassbares Hinweisschild (Bild 1) soll zunächst sicherstellen, dass die betroffenen Personen über den Umstand der Videoüberwachung informiert und ihnen die wichtigsten Informationen dazu bereitgestellt werden. Die vollständigen Informationen können dann – innerhalb des überwachten Bereichs – an geeigneter, gut zugänglicher Stelle ausgelegt, ausgehängt oder auch im Internet vorgehalten werden (Bild 2). Wesentlich ist dabei, dass das einfache Hinweisschild einen klaren Hinweis darauf enthalten muss, wo die vollständigen Informationen eingesehen werden können.

In speziellen Fällen ist selbst das vorgelagerte Hinweisschild wenig praktikabel, weil infolge der jeweiligen spezifischen Anwendungsbereiche mitunter eine Wahrnehmung der darauf enthaltenen Informationen durch die betroffenen Personen praktisch nicht möglich ist, etwa weil sie diesen Bereich einfach zu schnell passieren oder unter Umständen eine Beeinträchtigung des Verkehrsflusses im Raum steht. Beispiele sind etwa Tankstellen,

bei denen diese Schilder bereits an der Einfahrt angebracht werden müssten, oder auch öffentliche Verkehrsmittel, bei denen diese Schilder außen am Verkehrsmittel an-zubringen wären. In solchen Fällen wird als Erstinformation auch ein Hinweisschild mit dem bloßen Piktogramm Videoüberwachung (standardisierte Bildsymbol nach DIN 33450) zu akzeptieren sein. Das vorgelagerte Hinweisschild müsste dann an der Tank-säule bzw. im Fahrgastraum angebracht; die vollständigen Informationen könnten im Tankstellenshop bzw. auf der Website der Verkehrsbetriebe bereitgestellt werden. Es bleibt den Verantwortlichen selbstredend unbenommen, die umfassende Information auch bereits an den Tanksäulen bzw. im Verkehrsmittel anzubringen.

Nach wie vor gilt: Allein das Aufstellen einer geeigneten Beschilderung führt nicht zur Zulässigkeit einer ansonsten rechtswidrigen Videoüberwachung, insbesondere führt dies auch weder dazu, dass die Videoüberwachung von den betroffenen Personen als angemessen hingenommen werden muss, noch dass diese Kenntnis in eine Akzeptanz der Videoüberwachung umgedeutet werden kann.

Bild 1

Beispiel für ein vorgelagertes Hinweisschild nach Art. 13 der Datenschutz-Grundverordnung bei Videoüberwachung[1]

Weitere Informationen erhalten Sie:
- per Aushang (wo genau?)
- an unserer Kundeninformation / Rezeption / Kasse im Erdgeschoss
- (ggf.) zusätzlich im Internet unter ...

Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters:

Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden):

Zwecke und Rechtsgrundlage der Datenverarbeitung:

berechtigte Interessen, die verfolgt werden:

Speicherdauer oder Kriterien für die Festlegung der Dauer:

[1] *Hinweis: Die Informationen sind unentgeltlich in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitzustellen. Sie können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden (vgl. Art. 12 DSGVO). Um Lesbarkeit zu erreichen, sollte der Ausdruck mindestens in DIN A4 erfolgen.*

Bild 2

Beispiel für ein vollständiges Informationsblatt (Aushang) nach Art. 13 der Datenschutz-Grundverordnung bei Videoüberwachung[1]

Sie finden diese Informationen zusätzlich im Internet unter ...

Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters:

Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden):

Zwecke und Rechtsgrundlage der Datenverarbeitung:

berechtigte Interessen, die verfolgt werden:

Speicherdauer oder Kriterien für die Festlegung der Dauer:

Empfänger oder Kategorien von Empfänger der Daten (sofern Datenübermittlung stattfindet):

bei Absicht des Verantwortlichen, die personenbezogenen Daten **an ein Drittland oder eine internationale Organisation zu übermitteln**: Informationen über Angemessenheitsbeschluss der Kommission bzw. geeignete oder angemessene Garantien:

Hinweise auf die Rechte der Betroffenen

Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein **Recht auf Auskunft** über diese personenbezogenen Daten und auf die in Art. 15 DSGVO im einzelnen aufgeführten Informationen.

Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die **Berichtigung** sie betreffender unrichtiger personenbezogener Daten und ggf. die **Vervollständigung** unvollständiger personenbezogener Daten zu verlangen (Art. 16 DSGVO).

Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, sofern einer der in Art. 17 DSGVO im einzelnen aufgeführten Gründe zutrifft, z. B. wenn die Daten für die verfolgten Zwecke nicht mehr benötigt werden (**Recht auf Löschung**).

Die betroffene Person hat das Recht, von dem Verantwortlichen die **Einschränkung der Verarbeitung** zu verlangen, wenn eine der in Art. 18 DSGVO aufgeführten Voraussetzungen gegeben ist, z. B. wenn die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat, für die Dauer der Prüfung durch den Verantwortlichen.

Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten **Widerspruch** einzulegen. Der Verantwortliche verarbeitet die personenbezogenen Daten dann nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 21 DSGVO).

Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das **Recht auf Beschwerde bei einer Aufsichtsbehörde**, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt (Art. 77 DSGVO). Die betroffene Person kann dieses Recht bei einer Aufsichtsbehörde in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes geltend machen. In (Bundesland) ist die zuständige Aufsichtsbehörde: ...

[1] *Hinweis: Die Informationen sind unentgeltlich in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitzustellen. Sie können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden (vgl. Art. 12 DSGVO). Um Lesbarkeit zu erreichen, sollte der Ausdruck mindestens in DIN A3 erfolgen.*

3.2 Auskunftsrecht

3.2.1 Auskunft über Melderegisterauskünfte

Ein Petent setzte mich darüber in Kenntnis, dass er derzeit Opfer von Stalking sei. Dieses würde seine Privatadresse betreffen, obwohl diese nirgends veröffentlicht sei. Er vermutete in diesem Zusammenhang, dass seine Privatadresse aus dem Melderegister in Erfahrung gebracht wurde.

Er wandte sich daraufhin an das zuständige Meldeamt einer sächsischen Kommune, um in Erfahrung zu bringen, ob und gegebenenfalls an wen seine Meldedaten im Rahmen einer einfachen Melderegisterauskunft nach § 44 BMG übermittelt wurden. Zu seinem Erstaunen wurde ihm diese Auskunft verweigert. Zur Begründung wurde darauf verwiesen, dass das § 10 BMG eine solche Auskunft nicht umfasse; § 11 Absatz 1 Nummer a) BMG schließe sie vielmehr ausdrücklich aus.

Die Rechtsauffassung der Kommune ist unzutreffend. Auch wenn die Wiedergabe der Normen des BMG zutreffend ist, ergibt sich wegen des Anwendungsvorrangs des Europarechts ein Auskunftsanspruch direkt aus Artikel 15 Absatz 1 Nummer c) DSGVO. Die Voraussetzungen für eine mögliche Ausnahme nach Artikel 23 DSGVO liegen nicht vor. Das Sächsische Staatsministerium des Innern hat auf meine Anregung hin die sächsischen Kommunen entsprechend informiert.

Mittlerweile ist der Bundesgesetzgeber tätig geworden und hat die einfache Melderegisterauskunft nach § 44 BMG aus § 11 Absatz 1 Nummer a) BMG entfernt. Ein Auskunftsanspruch ergibt sich daher jetzt (auch) aus § 10 BMG.

3.2.2 Erst zu beschaffende Informationen sind nicht Gegenstand des Auskunftsanspruchs

In einer Beschwerde gegen einen Reiseveranstalter begehrte der Beschwerdeführer Auskunft gemäß Artikel 15 DSGVO. Die Auskunft bezog sich auch auf die Vertretungsverhältnisse bzw. die Firma, die mit der Durchführung des Fluges einer Reise beauftragt worden waren, um gegen dieses Unternehmen zivilrechtlich vorgehen zu können. Übrige Auskünfte wurden im Nachgang erteilt. Der Reiseveranstalter konnte aber der Auskunft begehrenden betroffenen Person – dem Reisekunden – keine ladungsfähige Anschrift des

beauftragten Unternehmens und dessen Vertreter mitteilen. Der Rechtsbeistand der betroffenen Person erkannte hierin ein Verstoß gegen Artikel 15 DSGVO.

Ich teilte dem Beschwerdeführer mit, dass eine Beauskunftung grundsätzlich zu erfolgen hat. Soweit wegen der lückenhaften Verwaltung der Rechtsgeschäfte kein Unternehmen benannt werden konnte, könnte man hierin allerdings einen Vertragsverstoß oder einen Verstoß gegen die Nebenpflichten des Reisevertrags erkennen und geltend machen. Derartige Bezüge sind aber nicht Gegenstand meiner Datenschutzaufsicht. Auskünfte gemäß Artikel 15 DSGVO können letztendlich nur in Bezug auf tatsächlich gespeicherte Informationen erteilt werden. Gegenstand der datenschutzrechtlichen Auskunftspflicht sind hingegen nicht etwa zusätzliche Informationen, die (noch) nicht vorhanden sind, zu beschaffen. Im Hinblick auf die streitigen Informationen zu der Fluggesellschaft wären gegebenenfalls auch die für dieses Unternehmen zuständigen im Ausland ansässigen Behörden zu kontaktieren gewesen.

3.2.3 Zurückbehaltungsrecht und öffentlich-rechtliche Pflichten des Verantwortlichen

Eine Anfrage einer Steuerberatung hatte zum Inhalt, ob eine Verpflichtung zur Herausgabe bzw. eine Zustimmung zum elektronischen Datenübertragen auf einen anderen Steuerberater bei Wechsel des Steuerberaters seitens des Mandanten bestehe, soweit dieser noch offene Steuerberaterforderungen zu begleichen habe und inwieweit sich der Mandant auf Artikel 15 und Artikel 20 DSGVO berufen könne.

Dem Unternehmen teilte ich mit, dass der Verantwortliche aufgrund öffentlichen Rechts gemäß DSGVO pflichtig sei. Nicht entscheidend sei, ob der Schuldner seinen vertraglichen Pflichten erfüllt habe oder nicht, sondern lediglich, dass die Datenverarbeitung auf eine Einwilligung bzw. auf einem vertraglichen Verhältnis beruhe. Insoweit könne die betroffene Person den Anspruch ohne Rücksicht auf inhaltliche Fragen des Schuldverhältnisses geltend machen und durchsetzen. Ein Zurückbehaltungsrecht gemäß § 273 Absatz 1 BGB bzw. § 66 Absatz 2 Steuerberatungsgesetz erkannte ich bei datenschutzrechtlicher Geltendmachung der Betroffenenrechte nicht.

Artikel 15 Absatz 1 DSGVO benennt enumerativ die Informationen, die zu beauskunften sind. Dieser Anspruch ist seitens der betroffenen Person zunächst gegenüber dem Verantwortlichen geltend zu machen. Artikel 15 Absatz 3 DSGVO gewährt der betroffenen

Person den Anspruch, eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen. Auch die Anfertigung einer Kopie ist seitens der betroffenen Person geltend zu machen.

Ein Anspruch auf Datenportabilität gemäß Artikel 20 DSGVO wiederum, so teilte ich es dem Steuerberater mit, erstrecke sich lediglich auf die von der betroffenen Person selbst bereitgestellten personenbezogenen Daten, zudem nicht auf jedwede Informationen, sondern nur speziell auf Informationen mit Personenbezug. Der Anspruch wäre seitens der betroffenen Person auch zunächst geltend zu machen.

Die Betroffenenrechte der Artikel 15 und Artikel 20 DSGVO stehen in keinem Verhältnis der Spezialität zueinander. Es handelt sich um zwei unterschiedliche Ansprüche.

4 Pflichten Verantwortlicher und Auftragsverarbeiter

4.1 Verantwortung für die Verarbeitung, Technikgestaltung

4.1.1 Einsatz des Standard-Datenschutzmodells

Das Standard-Datenschutzmodell wurde vor 5 Jahren von einer gemeinsamen Arbeitsgruppe verschiedener Datenschutzaufsichtsbehörden entwickelt und befindet sich seit dem in einem konstanten Prozess der Erprobung und Weiterentwicklung. Die aktuelle Version bildet die Anforderungen der DSGVO vollständig ab und überträgt diese für eine vereinfachte Modellierung von Schutzmaßnahmen in die bekannten Gewährleistungsziele aus denen wiederum entsprechende Maßnahmen abgeleitet werden. Neu ist die Beschreibung eines beispielhaften Datenschutzmanagements auf Grundlage des SDM und kontinuierlicher Verbesserungsprozesse (Plan, Do, Change, Act) sowie Ausführungen zum Verhältnis zwischen SDM und der Grundschutzmethodik des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Ich habe seit Beginn der Entwicklung am Modell mitgewirkt und innerhalb meines Zuständigkeitsbereiches auf zahlreichen Vorträgen, Workshops und Beratungen eine Erprobung des SDM gefördert. Diese Bemühungen haben dazu geführt, dass zahlreiche öffentliche Stellen, aber auch private Datenverarbeiter, Erfahrungen mit dem SDM gesammelt haben und dies inzwischen routiniert einsetzen.

- Das Sächsische Verwaltungsnetz (SVN) wird vom Staatsbetrieb Sächsische Informatik Dienste im Auftrag des Freistaates Sachsen betrieben. Vertragspartner für die Bereitstellung und den Betrieb der technischen Infrastruktur ist T-Systems. Bis vor der Einführung des SVN 2.0 im Jahr 2016 waren sämtliche Verfahren in einer Datenschutz-Matrix erfasst und beschrieben, wie die Anforderungen des damals geltenden Sächsischen Datenschutzgesetzes (SächsDSG) erfüllt werden. Im Rahmen der Migrationsplanung auf das SVN 2.0 wurde diese Matrix an den Anforderungen des SDM und den Gewährleistungszielen neu strukturiert. Im Ergebnis waren die erforderlichen Anpassungen, welche durch die DSGVO (DSGVO) erforderlich wurden, minimal, da das SDM bereits in der Version 1.1 die Anforderungen der DSGVO abgebildet hat.

- Ein IT-Dienstleister, welcher eine Vielzahl sächsischer Kommunen zu seinem Kundenstamm zählt, hat mit In-Kraft-Treten der DSGVO ein Beratungsangebot gestartet, welches auf Grundlage des SDM ein Komplettpaket zum Datenschutzmanagement enthält und damit auch Anwendern, welche bislang wenig Berührungspunkte mit der Methode hatten, einen einfachen Einstieg erlaubt. Einzelne Module des Pakets wurden durch meine Behörde geprüft und gemeinsam verbessert.

- Eine sächsische Krankenkasse hat die von ihr verantworteten Verfahren anhand der im SDM dargestellten Anforderungen der DSGVO strukturiert und die getroffenen technisch-organisatorischen Maßnahmen mit dem generischen Maßnahmenkatalog des SDM modelliert. Der Aufwand bei der Einführung neuer Verfahren und Aktualisierungen bestehender Verfahren bei Änderungen hat sich damit deutlich vereinfacht und ermöglicht eine strukturierte Einbeziehung von Beteiligten, ohne dass diese fundierte Kenntnisse des Datenschutzrechts haben müssen.

Ich ermutige jeden Verantwortlichen, sich das SDM näher anzuschauen und für eigene Anwendungen zu erproben. Die Datenschutzaufsichtsbehörden sind auf diese Erfahrungen angewiesen und berücksichtigen Rückmeldungen auch in der stetigen Weiterentwicklung des Modells.

Vergleiche auch den Beitrag unter 5.8.1.

4.1.2 Einsatz von Messengern durch Verantwortliche im dienstlichen und schulischen Umfeld

Gelegentlich wenden sich öffentliche Stellen an mich, die ihren Bediensteten einen "Messenger als modernes Arbeitsmittel" zur Verfügung stellen wollen. Frage ich dann nach, in welchem Zusammenhang, zu welchen Zwecken und auf welchen Geräten ein solcher Dienst zur Verfügung gestellt werden soll, sind die Vorstelllungen oft noch nicht allzu weit fortgeschritten. Meist steht lediglich ein konkretes Produkt im Vordergrund und der Datenschutzbeauftragte der öffentlichen Stelle wird gefragt, ob dies eingesetzt werden darf oder auch lediglich informiert, dass es eingesetzt werden wird. Mitunter wendet sich der Datenschutzbeauftragte dann an mich. Eine erste Prüfung des jeweils benannten Produktes führt dann meist zu zweierlei Erkenntnis: a) Das Produkt ist eine Cloud-Lösung mit klarer Zielgruppe Privatanwender und b) die Datenschutzerklärung ist

schwammig formuliert, zahlreiche Verantwortliche in Drittländern sind benannt, die alle Zugriff auf personenbezogene Daten erhalten sollen. Normalerweise ein klarer Fall, Prüfung beendet, ein rechtskonformer Einsatz ist nicht möglich. Ist ein Einsatz von Messengern im öffentlichen Bereich damit unmöglich? Nein, folgende Dinge müssen aber bei der Planung und der Umsetzung beachtet werden:

1. Ein Messenger sollte als normales Arbeitsmittel betrachtet werden. Oft hilft es, die Analogie zum Telefon oder zur E-Mail als etablierte Arbeitsmittel herzustellen und zu überlegen, welche Kommunikationsszenarien mit einer neuen Lösung abgedeckt werden sollen und inwieweit ein Messenger dafür geeignet und erforderlich ist.

2. Welche Zielgruppen sollen kommunizieren und miteinander Kontakt aufnehmen können? Müssen einzelne Nutzergruppen untereinander isoliert werden, braucht es einen Verzeichnisdienst und ist eine Kommunikation mit externen Kommunikationspartnern erlaubt oder gewollt? Welche Rollen müssen besetzt werden, gibt es Bedarf für Eingriffe in die Kommunikation (z. B. Moderation)? Diese Fragen sind im Vorfeld zu klären, am Einfachsten werden die Fragen am Beispiel einer Schule deutlich, hier gibt es als potenzielle Kommunikationspartner Lehrer, Eltern und Schüler (Klassen).

3. Auf welche Rechtsgrundlage kann ein solcher Dienst gestützt werden und welche Auswirkungen hat dies? Wird ein Messenger als Arbeitsmittel innerhalb der dienstlichen Infrastruktur (wie z. B, die dienstliche E-Mail) für interne Beschäftigte bereitgestellt, ist in der Regel keine Einwilligung (mögliches Problem: siehe 4) erforderlich. Bei der Einbindung externer Kommunikationsteilnehmer (Schüler, Eltern, Externe) ist dagegen eine Einwilligung erforderlich, abhängig vom Alter der Kommunikationsteilnehmer auch ggf. die der Erziehungsberechtigten.

4. Wie wird die Lösung betrieben? Prinzipiell besteht die Möglichkeit, eine solche Lösung im Eigenbetrieb als administrierte Nutzergruppe zu pflegen. Gängige Möglichkeiten für einen solchen Eigenbetrieb sind, oft als freie Software, vorhanden, setzen aber Aufwand, Wissen und die Ressourcen dauerhafter Pflege voraus. Eine andere Möglichkeit ist die Nutzung eines Dienstes als Auftragsverarbeitung. Vo-

raussetzung dafür ist, dass eine solche Möglichkeit seitens eines Anbieters rechtskonform bereitgestellt wird. Wichtig ist es, in einer Vorprüfung auf folgende Dinge zu achten:

- Erfüllt eine Auftragsverarbeitung der Voraussetzungen der DSGVO, insbesondere von Artikel 28?

- Wo befinden sich die Server des Auftragsverarbeiters?

- Werden Nutzungsdaten ausschließlich zur Bereitstellung des Dienstes und nicht für eigene Zwecke des Auftragsverarbeiters genutzt oder ohne Rechtsgrundlage an Dritte weitergegeben?

- Sind die bereitgestellten Informationen ausreichend und besteht eine hinreichende Kontrolle seitens des Auftraggebers?

Die marktgängigen Dienstleiter für den privaten Nutzer und damit auch die bekannten Platzhirsche werden in aller Regel einer solchen Prüfung nicht standhalten und kommen daher als Auftragsverarbeiter nicht in Betracht.

5. Welche Dienste werden von übergeordneten Stellen oder Verbänden bereitgestellt oder empfohlen? Hier lohnt sich eine Recherche, ob für die jeweilige Branche (ggf. hilft auch der Blick in andere Bundesländer) eine etablierte Lösung existiert, die mit geringerem Aufwand eingesetzt werden kann. An dieser Stelle möchte ich das Landesamt für Schule und Bildung lobend erwähnen, welches mit Lernsax einen sicheren und stetiger Weiterentwicklung unterzogenen Werkzeugkasten bereitstellt, welcher auch eine Messenger-Lösung für Schulen beinhaltet.

6. Welche Endgeräte sollen verwendet werden? Hier ergeben sich weitere Fragen, welche im Vorfeld beachtet werden müssen und die Komplexität eines datenschutzkonformen und rechtssicheren Betriebs erhöhen können. Wenn ein solcher Dienst ausschließlich auf dienstlicher Infrastruktur (PCs, Smartphones) bereitgestellt wird, ist eine Nutzung in aller Regel durch bestehende Festlegungen ausreichend rechtlich abgesichert. Deutlich komplizierter wird die Rechtslage bei Nutzung auf privaten Geräten. Ich empfehle eine solche Nutzung nach wie vor ausdrücklich nicht.

7. Sind alle Beteiligten informiert und sind Interessenvertreter ausreichend beteiligt? Ein Verantwortlicher muss auch beim Einsatz eines Messengers für Transparenz hinsichtlich der Nutzung und der verarbeiteten Daten sorgen. Sind Speicherfristen definiert, wer hat Zugriff auf Daten, ggf. auf Nutzungsdaten, welche Daten werden wie verschlüsselt, ist die Nutzung freiwillig oder wird der Dienst verpflichtend bereitgestellt, welche Inhalte dürfen kommuniziert werden und welche nicht. Diese und weitere Fragen müssen transparent kommuniziert werden und eventuelle Beteiligungsrechte des Betriebs- oder Personalrats eingehalten werden.

Je nach Einsatzszenario ergeben sich weitere Fragen, z. B. bei der Verarbeitung von besonders geschützten Daten, für Hinweise dazu empfehle ich die Lektüre der Orientierungshilfe der Datenschutzkonferenz:

Whitepaper zu technischen Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich (https://www.datenschutzkonferenz-online.de/media/oh/20191106_whitepaper_messenger_krankenhaus_dsk.pdf).

4.1.3 E-Mails mit offenem Verteiler

Wiederholt haben mich Bürger darauf hingewiesen, dass öffentliche Verwaltungen E-Mails über offene Verteiler versenden. Hierdurch werden die E-Mail-Adressen der Betroffenen allen anderen im Verteiler genannten Personen bekannt gegeben. Oftmals sind es Einladungen zu Informationsveranstaltungen oder anderweitige Informationen an Interessentengruppen, welche über offene Verteiler versendet werden. Datenschutzrechtlich war jeweils nicht ersichtlich, dass dies erforderlich war. Ein E-Mail-Versand mit Verwendung der BCC-Funktion wäre vielmehr möglich gewesen.

Beispielsweise wurden E-Mails mit offenen Verteilern an mehr als 200 Empfänger gesendet, an Vertreter aus Wirtschaft und Gesellschaft sowie Politik. Die Empfänger hatten teilweise personalisierte dienstliche Adressen, Funktionsadressen, welche frei zugänglich über Webseiten abrufbar waren und private E-Mail Adressen.

Von einem Versehen ging ein Petent bei seiner Stadtverwaltung dabei nicht aus. Er teilte mit, dass es im Übrigen auch in der Vergangenheit üblich gewesen sei, E-Mails an offene Verteiler zu senden. Die E-Mailadressen waren jeweils für alle Empfänger einsehbar. Der Beschwerdeführer wendete sich umgehend an die entsprechende Stadtverwaltung, um auf

den Datenschutzverstoß hinzuweisen. Aber auch nach Ablauf von vierzehn Tagen nach dem Vorfall erfolgte leider keine Reaktion durch die verantwortliche Stelle.

Diese Übermittlung der E-Mailadressen an Dritte, auch im Hinblick auf die erhebliche Anzahl der E-Mail-Adressen, ist nicht erforderlich und entspricht nicht den aktuellen Datenschutzanforderungen nach DSGVO. Durch diese Art der Versendung werden die E-Mail-Adressdaten in Verbindung mit weiteren personenbeziehbaren Daten (z.B. Name in Verbindung mit Daten zum Unternehmen oder Beschäftigungsverhältnis) an zahlreiche Dritte übermittelt, ohne dass dazu eine Erforderlichkeit besteht. Personenbezogene Daten dürfen an Dritte nur dann übermittelt werden, sofern eine Einwilligung vorliegt oder eine gesetzliche Grundlage gegeben ist. Die Verwendung eines offenen E-Mail-Verteilers ist datenschutzrechtlich unzulässig, wenn die Inhaber der E-Mail-Adressen dazu nicht ihre Einwilligung erteilt haben. Vor der Versendung von E-Mails ist jeweils zu überprüfen, ob beide Voraussetzungen vorliegen. Bereits in meinem 18. Tätigkeitsbericht habe ich unter 1.6 ausführliche Hinweise zur Einwilligung gemäß DSGVO dargelegt.

Für die Versendung von Einladungen zu Veranstaltungen per E-Mail empfehle ich, auf andere datenschutzgerechte Verteilertechniken, wie beispielsweise die BCC-Funktion abzustellen. Bei Eintragung der E-Mail-Adressen in das normale „AN-Feld“ oder das „CC-Feld“ sehen alle Empfänger dieser E-Mail, an welche Adressaten die E-Mail versendet wurde. Nur bei Verwendung des „BCC-Feld“ (Blind Carbon Copy) wird die Übertragung der E-Mail-Adressen an die Empfänger unterdrückt, sodass die E-Mail-Adressen der Empfänger nicht eingesehen werden können. Ferner ist aus datenschutzrechtlicher Sicht vorab zu überprüfen und festzulegen, wie und zu welchem Zweck die E-Mail-Adressen erhoben und gespeichert werden sollen und wann diese wieder gelöscht werden müssen.

Ich empfehle die Mitarbeiter in den Verwaltungen regelmäßig über die aktuell erforderlichen technischen und organisatorischen Datenschutzmaßnahmen bei der Datenübertragung per E-Mail oder Internet zu unterrichten.

Schon in früheren Tätigkeitsberichten (16. TB unter 5.1.4, 17. TB unter 13.2 sowie 7. TB nöB unter 8.2.4) habe ich dargelegt, warum der Versand einer E-Mail mit offenem Verteiler datenschutzrechtlich grundsätzlich unzulässig ist. Das Thema ist fortwährend auch nach DSGVO noch aktuell, obgleich ich regelmäßig Hingewiesen habe. Zukünftig werde

ich mir nun endgültig und ohne weiteres Zögern vorbehalten, Bußgelder zu verhängen. Andere Aufsichtsbehörden haben derartige Verstöße bereits mit einem Bußgeld geahndet.

4.1.4 Pflegeheime - Freier Zugang zu Postfächern der Bewohner in Foyer

Gegen Ende des letzten Berichtszeitraums erhielt ich eine Beschwerde über eine stationäre Pflegeeinrichtung, bei der im Foyerbereich Postfächer der Bewohner des Heims eingerichtet waren. Dabei waren die Postfächer als Ablagen organisiert, nicht verschließbar, ungesichert und für jedermann zugänglich. Der Zugang war dem offenen Raum zugewandt und daher waren die Postfächer für eintretende Personen als solche sichtbar und leicht erkennbar.

Ich habe dem Verantwortlichen gegenüber diesen Zustand moniert und auf Abhilfe gedrungen. Verwiesen habe ich hierbei auch auf Artikel 5 Absatz 1 Buchstabe f) DSGVO. Danach sind personenbezogene Daten in einer Weise zu verarbeiten, dass eine angemessene Sicherheit der Daten, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung. Dem genügen offene Postfächer nicht. Die Pflegeheimbewohner haben als betroffene Personen einen Anspruch darauf, dass ihre Briefpost und persönlichen Nachrichten in einer gesicherten Umgebung verwahrt und gelagert werden. Entsprechendes sollte eigentlich eine Selbstverständlichkeit sein.

4.1.5 Gewahrsamsaufgabe bei Personalunterlagen

Im letzten Berichtszeitraum erhielt ich eine Mitteilung der Abfallbehörde einer sächsischen Großstadt zu einem verwahrlosten Grundstück. Die Behörde informierte darüber, dass sie festgestellt habe, dass auf dem Grundstück in einem Gebäude eine größere Menge an Personaldokumenten aufgefunden wurde. Es handelte sich um eine verwahrloste Gewerbeeinheit, einen ehemaligen Beherbergungsbetrieb, der nach Einschätzung des Amtes unzureichend gesichert und an mehreren Stellen frei betreten werden konnte. Auf dem Grundstück und in dem Gebäude hielten sich nach den Angaben der Behörde wiederholt unbefugt Personen auf, mehrfach sei es auch zu Brandstiftungen gekommen. Eine große Menge von Personalakten, die sich in einem zerlesenen und durchwühlten Zustand befunden hätten, sei im Bereich des Empfangstresens, festzustellen gewesen. Ferner teilte das Amt mit, dass es sich überwiegend um Dokumente von Auszubildenden und Lehrgangsteilnehmern der ehemals auf dem Grundstück ansässigen Betriebe sowie Gästebücher der Hotelgäste handeln würde. Die Abfallbehörde übersandte mir als Anlagen anschauliche Bildaufnahmen des Zustands der Räumlichkeiten und Papierdokumente.

In der Folge nahm meine Behörde Kontakt zu der anzeigenden Behörde auf, die Sicherungsmaßnahmen, auch im Hinblick auf die Unterlagen zu verfügen beabsichtigte. Ich bin dankbar über derartige Hinweise anderer öffentlicher Stellen. Nach ersten Erkenntnissen gab es zu den aufgefundenen Unterlagen auch zunächst keinen Verantwortlichen, der in Bezug auf die Sicherung der Dokumente datenschutzrechtlich hätte herangezogen werden können. Meine Dienststelle verfügt noch über keine eigenen Kapazitäten, um derartige Unterlagen aufzubewahren und zu sichern. Insoweit bin ich auf die Amtshilfe und Zusammenarbeit mit kommunalen und staatlichen Behörden angewiesen.

Über den Fortgang des Verfahrens werde ich weiter berichten.

4.1.6 Umgang mit personalisierten E-Mail-Adressen bei Ausscheiden von Beschäftigten

Unternehmen und Institutionen richten vielfach ihren Mitarbeitern personalisierte E-Mail-Adressen ein. Nach dem Ausscheiden von Mitarbeitern stellt sich die Frage, wie die Organisation mit den entsprechenden elektronischen Postfächern umgehen soll. Hier stehen ggfs. die Interessen des Unternehmens im Spannungsverhältnis mit denen des früheren Mitarbeiters und ggf. dessen Kommunikationspartnern. Die Organisation hat ein Interesse, die Außenwirkung, die der Mitarbeiter in seiner Arbeitszeit für diese entwickelt hat, auch weiter zu nutzen, und die entsprechenden Kommunikationskanäle ggfs. geordnet überzuleiten. Der frühere Mitarbeiter und seine Kommunikationspartner hingegen wollen vor der befugten oder unbefugten Kenntnisnahme möglicherweise persönlicher Kommunikation durch Dritte geschützt werden. Zwar wäre ein automatischer Hinweis zu einem aktuellen Ansprechpartner für den Absender von E-Mails an die nachgenutzte personalisierte E-Mail-Adresse, verbunden mit einer Löschung solcher E-Mails, die datensparsamste Variante. Dennoch kann bei entsprechender Ausgestaltung auch ein zeitlich begrenztes Offenhalten des durch derartige E-Mail-Adressen eröffneten Kommunikationskanals zulässig sein. Dabei muss der Zugang dritter Mitarbeiter der Organisation engen Grenzen unterliegen. Ein Vier-Augen-Prinzip und die genaue Dokumentation des Zugangs und dessen Anlass sind ebenso erforderlich wie eine Information der ausscheidenden Mitarbeiter, um eventuelle persönliche Kommunikationspartner auf die Veränderung hinzuweisen.

4.1.7 E-Mail-Nutzung durch Steuerberater

Von einem Steuerbüro wurde ich auf die Problematik der E-Mail-Nutzung angesprochen. Dazu wurde ausgeführt, dass dort die Anhänge der an Mandanten versandten E-Mails schon seit vielen Jahren verschlüsselt würden. Daneben gäbe es aber auch noch „normale“ E-Mails; dies seien zum Beispiel Nachrichten, in denen die Mandanten an fällige Zahlungen (an Krankenkassen oder das Finanzamt) erinnert würden. Die Frage war nun, ob auch diese E-Mails verschlüsselt werden müssen. Nach Auffassung des Steuerbüros waren das keine personenbezogene Daten, sondern lediglich Informationen.

Auf diese Anfrage bezogen ist zunächst klarzustellen, dass jegliche Kommunikation mit Mandanten über deren steuerrechtliche Angelegenheiten eine Verarbeitung personenbezogener Daten (des Mandanten) darstellt. Nach Artikel 4 Nummer 1 DSGVO sind alle Informationen – und dazu gehören auch Zahlungsfälligkeiten –, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, personenbezogene Daten. Bei einer E-Mail-Kommunikation wird sich der Personenbezug dabei – wenn er nicht schon aus dem Nachrichtenbetreff oder dem sonstigen Nachrichteninhalt zu erkennen ist – spätestens aus der E-Mail-Adresse ergeben.

In Bezug auf das Verschlüsselungserfordernis gilt Folgendes:

§ 203 StGB schützt die Individualinteressen betroffener Personen in besonderer Weise dadurch, dass er Berufsgeheimnisträgern wie Steuerberatern (vgl. § 203 Absatz 1 Nummer 3 StGB) einschließlich ihrer berufsmäßig tätigen Gehilfen (vgl. § 203 Absatz 3 StGB), denen die betroffenen Personen im Rahmen der Mandatserteilung regelmäßig Geheimnisse anvertrauen, für den Fall der Verletzung ihrer Geheimhaltungs- und Verschwiegenheitspflichten entsprechende Strafen androht.

Unter besonderer Berücksichtigung dieser Tatsache (vgl. zur Thematik auch Punkt 8.13.1 meines 8. Tätigkeitsberichts zum Datenschutz im nicht-öffentlichen Bereich) einerseits wie auch der Vorgaben zum Schutz personenbezogener Daten gemäß Artikel 25 und des Artikel 32 Absatz 1 Buchstabe a) DSGVO, wonach die dort ausdrücklich genannte Verschlüsselung eine adäquate Maßnahme zur Gewährleistung der Sicherheit der Verarbeitung darstellt, andererseits, kommt damit für Steuerberater grundsätzlich nur eine verschlüsselte E-Mail-Kommunikation in Betracht. Etwas anderes gilt nur dann, wenn das Steuerbüro seine Mandanten auf die besondere Schutzbedürftigkeit der per E-Mail zu

versendenden Daten sowie die speziellen Risiken eines unverschlüsselten E-Mail-Versands hingewiesen hat, diesbezüglich sichere Kommunikationswege (z. B. Verschlüsselung, Postversand) grundsätzlich alternativ anbietet, und sich der Mandant vor diesem Hintergrund bewusst für einen unverschlüsselten E-Mail-Versand entscheidet, d. h. hierfür seine Einwilligung (Artikel 7 DSGVO) erteilt, wobei die diesbezügliche Beweislast beim Steuerberater als dem Versender liegt. Darüber hinaus dürfen solche unverschlüsselt versandten E-Mails keine personenbezogenen Daten Dritter enthalten. Zumindest dies dürfte bei Steuerberatern wegen des häufig fehlenden Drittbezugs eher gewährleistet sein als etwa bei Rechtsanwälten.

4.2 Gemeinsam Verantwortliche

Nicht belegt.

4.3 Auftragsverarbeitung

4.3.1 Auftragsverarbeitung bei Dentallaboren

Die Zahntechnikerinnung Dresden-Leipzig hatte sich nach dem Inkrafttreten der DSGVO an mich gewandt und um Stellungnahme gebeten, ob Labortätigkeiten im Zusammenhang mit der Durchführung medizinischer Behandlungen als Auftragsverarbeitung im Sinne von Artikel 4 Nummer 8 DSGVO, Artikel 28 DSGVO zu qualifizieren seien. Ich hatte ihr daraufhin mitgeteilt, dass dies nicht der Fall sei.

Im Berichtszeitraum fragte die Innung erneut an und informierte mich darüber, dass die Landeszahnärztekammer Sachsen die Sicht meiner Behörde in Zweifel ziehe, da es sich beim Verhältnis zwischen Zahnarzt und zahntechnischem Labor um einen Werkvertrag bzw. Werklieferungsvertrag und nicht um eine medizinische Leistung handele, zu deren Erfüllung der Zahnarzt dem Zahntechniker personenbezogene Daten bzw. Gesundheitsdaten übermittle und bat meine Dienststelle um Konkretisierung meiner zurückliegenden Stellungnahme.

Eine Auftragsverarbeitung im datenschutzrechtlichen Sinne liegt nur vor, wenn der Schwerpunkt der beauftragten Tätigkeit in der Verarbeitung personenbezogener Daten liegt, vgl. den Wortlaut der Vorschrift des Artikel 28 Absatz 3 DSGVO. Die Beauftragung mit fachlichen Dienstleistungen anderer Art, d. h. mit Dienstleistungen, bei denen nicht

die Datenverarbeitung Gegenstand der Hauptleistungspflicht ist bzw. bei denen die Datenverarbeitung nicht zumindest einen wichtigen (Kern-)Bestandteil ausmacht, stellt insoweit keine Auftragsverarbeitung im datenschutzrechtlichen Sinn dar.

Ein Zahnarzt nimmt die Fachleistung des zahntechnischen Labors in Anspruch, mit dem er einen Werkvertrag bzw. Werklieferungsvertrag abschließt. Er macht dem Dentallabor zwar gewisse Vorgaben. Die zu erbringende Leistung wird jedoch eigenständig vom Dentallabor ohne Weisungen und Vorgaben zur damit einhergehenden Verarbeitung personenbezogener Daten erbracht.

Ich teilte der Zahntechnikerinnung Dresden-Leipzig mit, dass meine Behörde weiterhin vertrete, dass zwischen einem Zahnarzt und einem zahntechnischen Labor keine Auftragsverarbeitung im Sinne des Artikels 4 Nummer 8, Artikel 28 DSGVO vorliege. Die Rechtsmeinung meiner Dienststelle entspricht den weiteren Datenschutzaufsichtsbehörden, die die Frage zu entscheiden hatten. Gegenteilige Spruchpraxis von Datenschutzaufsichtsbehörden ist mir nicht bekannt geworden.

Datenschutzorganisatorisch hat der Zahnarzt die Gelegenheit und Pflicht Patienten zu informieren, dass ein Dentallabor eingeschaltet und personenbezogene Daten an dieses weitergegeben werden, Artikel 13 Absatz 1 Buchstabe e) DSGVO. Ein entsprechender Vermerk in der Patientenakte dient der weitergehenden Dokumentation eines datenschutzkonformen Handelns. Ferner sind prozessuale Verfahren, in denen die an das Labor übermittelten Daten pseudonymisiert und für den empfangenden Verantwortlichen nicht zu einer Einzelperson zuordenbar sind, anzuraten. Im Übrigen sind die Vorschriften der Artikel 9 Absatz 2 Buchstaben a) und h) sowie Absatz 3 DSGVO einschlägig.

Danach meinen Überlegungen nicht von einer Auftragsverarbeitung auszugehen ist, ist das seitens des Arztes gewählte Dentallabor Verantwortlicher im Sinne von Artikel 4 Nummer 7 DSGVO in Bezug auf übergebene personenbezogene Daten bzw. Gesundheitsdaten und hat deren datenschutzgerechte Verarbeitung im Sinne der Artikel 5 DSGVO und Artikel 25 DSGVO zu gewährleisten.

Der Landeszahnärztekammer, die sich noch nachträglich direkt an mich gewandt hatte, teilte ich meine Rechtsauffassung ebenfalls mit.

4.3.2 Verwahrung von Patientenakten durch den Praxisnachfolger - Auftragsverarbeitung oder Verarbeitung durch gemeinsam Verantwortliche

Eine Rechtsanwaltskanzlei wandte sich mit einer Anfrage an alle Datenschutzaufsichtsbehörden in Deutschland. Sie bat um die Stellungnahme meiner Behörde, ob es sich bei der Übernahme der Patientenkartei durch einen Arzt und Praxisnachfolger wegen einer Praxisaufgabe oder -übernahme um einen Fall der Auftragsverarbeitung im Sinne von Artikel 28 DSGVO handele und folglich neben den Vereinbarungen eines Praxisübergabevertrags und zur Verwahrung von Akten der Abschluss eines Vertrags über die Auftragsverarbeitung erforderlich sei.

§ 10 Absatz 4 Satz 2 der Berufsordnung der Sächsischen Landesärztekammer legt fest, dass der Arzt, dem bei einer Praxisaufgabe oder Praxisübergabe ärztliche Aufzeichnungen über Patienten in Obhut gegeben werden, diese unter Verschluss zu halten hat und sie nur mit Einwilligung des Patienten einsehen oder weitergeben darf. Diese Regelung entspricht inhaltlich auch § 10 Absatz 4 Satz 2 Muster-Berufsordnung der Ärzte (MBO-Ärzte).Krankenhaus

Nach meiner Überzeugung handelt es sich bei der Verwahrung der Patientenakten durch den Praxisnachfolger unter Berücksichtigung der berufsrechtlichen Regelung des § 10 Absatz 4 Satz 2 *Berufsordnung der Sächsischen Landesärztekammer* regelmäßig weder um eine Auftragsverarbeitung noch um einen Fall der gemeinsamen Verantwortlichkeit.

Datenschutzrechtlich kann eine Verwahrung regelmäßig nicht als Auftragsverarbeitung im Sinne von Artikel 4 Nummer 8, Artikel 28 DSGVO qualifiziert werden. Denn anders als bei der Auftragsverarbeitung, bliebe bei der berufsrechtlich zugelassenen Verwahrung von Behandlungsdokumentationen durch den Erwerber der Veräußerer nicht weiter für die Rechtmäßigkeit der weiteren Aufbewahrung der Patientenunterlagen verantwortlich. Vielmehr führte der Abschluss eines Verwahrungsvertrags gerade dazu, dass der Veräußerer von seiner bislang noch ihn treffenden berufsrechtlichen Dokumentationspflicht befreit wird.

Die Übernahmen können im Übrigen auf vielfältige Weise rechtlich und praktisch ausgestaltet sein. So kann beispielsweise im Rahmen eines Auftragsverarbeitungsvertrages vorgesehen sein, Papierakten nachträglich zu digitalisieren. In derartigen Einzelfällen kann es wiederum nicht ausgeschlossen sein, dass ein Auftragsverarbeitungsvertrag Bestandteil des Rechtsverhältnisses zwischen altem und neuem Praxisinhaber ist. Darüber hinaus

könnte es im Bereich der Übernahme von Patientenakten, die in einem elektronischen Format geführt werden sollen, eine Vielzahl an Konstellationen geben, bei denen ggf. ebenso eine Auftragsverarbeitung denkbar ist, insbesondere dann, wenn der Erwerber Überwachungs- und Löschungsprozesse des Altpatientenbestands durchführen soll.

Ärzten bzw. deren beratenden Rechtsanwälten ist im Einzelfall auch die Rücksprache mit der zuständigen Landesärztekammer anzuraten.

4.4 Verzeichnis von Verarbeitungstätigkeiten, Kooperationspflicht mit der Aufsichtsbehörde

Nicht belegt.

4.5 Sicherheit der Verarbeitung

4.5.1 Handlungspflichten im Hinblick auf den Verlust von Daten und Datenträgern

Datenverlust bei Verantwortlichen, Behörden und Unternehmen ist in Anbetracht informationssicherheitstechnischer Probleme und vielfältiger Bedrohungen bis hin zum Datendiebstahl oder dem Abhandenkommen von Datenträgern eine nicht zu unterschätzende Thematik. Insbesondere für Unternehmen kann Datenverlust existenzbedrohend sein. Daher sind Datensicherungsroutinen auch kleinen Unternehmen anzuraten. Daneben können so auch erforderliche personenbezogene Daten für den Verantwortlichen und auch im Interesse der betroffenen Personen, was deren Betroffenenrechte angeht, erhalten bleiben. Zu empfehlen ist gegebenenfalls ein Datensicherungskonzept, das Teil eines Informationssicherheitskonzepts sein kann. Entsprechende geeignete Maßnahmen können als Umsetzung von Artikel 25, 32 DSGVO betrachtet werden.

Wichtige von den Verantwortlichen verarbeitete Daten sind datensicher aufzubewahren. Die Datensicherung kann man als Teil der Datensicherheit, dem Schutz vor Verlust, unberechtigter Veränderung oder unbefugter Kenntnisnahme durch Dritte, betrachten. Datensicherung ist durch das Kopieren von Daten oder vollständigen Systemabbildungen auf einem zusätzlichen Datenspeicher erreichbar. Mit gesicherten Daten, auf die in einer geschützten Umgebung zurückgegriffen werden kann, kann damit Fehlfunktionen oder ungewollten Veränderungen bis hin zum Verlust entgegengewirkt werden. Die Wiederherstellung von Datengruppen und Systemen bleibt auf diese Weise durchführbar.

Datensicherungen sind in einer geschützten Umgebung und möglichst auch örtlich entfernt von den übrigen IT-Systemen vorzuhalten. Es empfiehlt sich gegebenenfalls bei komplexen Systemabbildungen oder hohem Datendurchfluss regelmäßige „Generationen-Backups" durchzuführen, so dass gegebenenfalls auch auf den Status mehrerer zeitlich zurückliegender Datenbestände zurückgegriffen werden kann.

In der Umsetzung kann bei einfachen Datenprozessen auch eine einfach durchzuführende Volldatensicherung, bei der zum Beispiel die komplette Festplatte auf ein Sicherungsmedium gespiegelt wird, schon ausreichend sein. Mit einer Datensicherung, die auf der Volldatensicherung aufbaut und hieran anschließt und mit der lediglich Veränderungen seit dem letzten Backup gesichert werden, kann programmtechnisch eine Speicherkapazitäten schonende Dokumentation der Datenstände generiert werden. Verantwortlichen ist zu raten, entsprechende Datenschutz- und IT-Berater zu konsultieren.

Was die zu sichernden Datenbestände anbelangt, ist ohnehin zu empfehlen, dass zum Schutz der Daten im Falle eines Diebstahls oder Abhandenkommens geeignete Maßnahmen ergriffen werden, wozu personell-organisatorische Anweisungen zum datenschutzgerechten Umgang mit Daten und Datenträgern, deren Transport und informationssicherheitstechnische Lösungen in Bezug auf die Verschlüsselung der Datenbestände auf den Speichermedien gehören. Ein besonderes Augenmerk sollte dabei insbesondere auch auf den Schutz von sensiblen Daten im Sinne von Artikel 9 Absatz 1 DSGVO gelegt werden.

Das Handelsgesetzbuch, dass eine ordnungsgemäße und revisionssichere Buchführung verlangt – § 238 Handelsgesetzbuch – sieht zudem Aufbewahrungszeiträume für Buchführungsunterlagen vor, § 257 Handelsgesetzbuch, § 146 Abgabenordnung. Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff, eine Verwaltungsanweisung des Bundesministeriums der Finanzen, unterstützen in der Praxis eine vorschriftengerechte Aufbewahrung von Unterlagen.

Soweit Datenträger bzw. Daten abhandenkommen sollten, ist „unverzüglich und möglichst binnen 72 Stunden“ die zuständige Datenschutzaufsichtsbehörde zu informieren, es sei denn, dass sich voraussichtlich kein Risiko für die Rechte und Freiheiten natürlicher Personen eingestellt hat, Artikel 33 Absatz 1 DSGVO.

Handelt es sich um rein zu privaten bzw. familiären Zwecken gespeicherten Daten, ist die DSGVO allerdings nicht anwendbar, und es bestehen keine gesetzlichen Meldepflichten

oder ähnliches. Sobald dieser enge Ausnahmebereich überschritten ist, etwa bei gewerblichen oder vereinsbezogenen Daten mit Personenbezug, ergeben sich Pflichten bei Datenverlust aus Artikel 33, 34 DSGVO. Diese staffeln sich nach dem konkreten Risiko für die Betroffenen (von Bedeutung sind hier insbesondere die Art und Natur der verlorenen Daten und etwaige Sicherungen wie Verschlüsselung oder Pseudonymisierung). Danach hat der Verantwortliche unverzüglich und möglichst binnen 72 Stunden nach seiner Kenntniserlangung die Datenschutz-Aufsichtsbehörde über die Verletzung des Schutzes personenbezogener Daten zu informieren, es sei denn, diese Verletzung führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen. Für die Meldung derartiger Datenverluste befindet sich auf der Internetpräsenz des Sächsischen Datenschutzbeauftragten ein entsprechendes Meldeformular. Im Weiteren zu Meldungen von Datenpannen, vgl. 4.6.1, 6.2.6 des Tätigkeitsberichts 2017/2018 – Teil 2.

4.6 Meldung von Datenschutzverletzungen

4.6.1 Meldung von Datenschutzverletzungen

Nach Artikel 33 DSGVO sind Verantwortliche verpflichtet, im Falle der Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden der Verletzung diese der Aufsichtsbehörde zu melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Im Berichtszeitraum (01.01. bis 31.12.2019) sind bei mir knapp 450 solcher Meldungen eingegangen. Im (relativen) Vergleich zum vorjährigen Berichtszeitraum seit Geltung der DSGVO (25.05. bis 31.12.2018 – 227 Meldungen) entspricht dies einer Steigerung um ca. 30 Prozent. Damit ist erneut eine erhebliche Zunahme der Meldungen von Datenschutzverletzungen zu verzeichnen.

Die folgenden Fallgruppen sind im Berichtszeitraum besonders häufig gemeldet worden:

<u>Fehlversand</u>

Nach wie vor ist der Fehlversand die häufigste Fallgruppe der Meldungen von Datenschutzverletzungen. Dies umfasst den klassischen Versand per Post, die Übermittlung per Fax oder auch per E-Mail. Eine häufige Ursache für den Fehlversand ist die schlichte

Verwechslung der Empfängerperson aufgrund (Nach-) Namensgleichheit bzw. -ähnlichkeit. Als weitere Ursachen, die dazu führen, dass unberechtigte Dritte Kenntnis über fremde personenbezogene Daten erhalten, ist zum einen die fehlerhafte händische Zuordnung von Unterlagen sowie zum anderen die automatisierte Kuvertierung von Serienbriefen zu nennen. Betroffene Kategorien von personenbezogenen Daten sind Adressdaten, Daten im Zusammenhang von Vertragsbeziehungen, aber auch sensible Daten im Gesundheit-, Versicherungs- und Bankbereich, die grundsätzlich besonderer Vertraulichkeit unterliegen und folglich auch mit besonderer Sorgfalt zu verarbeiten sind.

Einbruch und Diebstahl

Eine weitere häufige Fallgruppe der Meldungen von Datenschutzverletzungen steht im Zusammenhang mit Einbrüchen und Diebstählen. Diese kriminellen Handlungen richten sich auf die entsprechenden Datenträger wie z.B. Computer, Festplatten, anderweitige Speichermedien, Fotoapparate, Handys und Unterlagen und werden zusammen mit bzw. aus Taschen, Autos, Büroräumen, Briefkästen sowie verschlossenen Aktenschränken und Tresoren entwendet. Auch wenn diese Handlungen häufig der Beschaffungskriminalität und folglich der schnellen finanziellen Verwertung der entwendeten Gegenstände zuzuordnen sind, kann eine damit verbundene Datenschutzverletzung nie ausgeschlossen werden. Eine datenschutzrelevante Nebenfolge bei Einbruchsdiebstählen kann stets die Verletzung der Vertraulichkeit bei frei zugänglichen Unterlagen/Akten sowie ungesicherten Speichermedien sein, da auch insoweit eine Kenntnisnahme in der Regel nicht ausgeschlossen werden kann. 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 der Wiederherstellung zu gewährleisten. Darüber hinaus sind personenbezogene Daten auf digitalen Datenträgern durch geeignete Verschlüsselung zu schützen. Die Funktionalität der vollständigen Festplattenverschlüsselung ist heute bereits in viele Betriebssysteme integriert, so dass in vielen Fällen gar keine zusätzliche Spezialsoftware erforderlich wäre. Eine Vielzahl nachfolgender Probleme ließe sich vermeiden, wenn sich die Nutzung dieser Möglichkeit von der Ausnahme zum Standard in der Praxis bei mobilen Endgeräten wie Laptops, Tablet-Computern oder Telefonen entwickeln würde.

Allgemein der Verlust von Unterlagen und Datenträgern sowie speziell der Verlust auf dem Postweg

Des Weiteren stellt neben dem Verlust durch Diebstahl auch der Verlust durch anderweitige Umstände, wie z.B. das Verlieren eines Handys sowie das versehentliche Liegenlassen von Unterlagen oder eines Laptops, eine Fallgruppe der Meldungen von Datenschutzverletzungen dar. Speziell auch der Verlust von Postsendungen ist an dieser Stelle zu erwähnen, da der Verbleib der Postsendungen mit den darin enthaltenen personenbezogenen Daten ebenso in der Regel nicht aufgeklärt und somit eine mögliche Verletzung der Vertraulichkeit nicht ausgeschlossen werden kann.

Offene E-Mail-Verteiler

Nach wie vor ein Klassiker bei den Meldungen von Datenschutzverletzungen ist die Verwendung eines offenen E-Mail-Verteilers. Mindestens dann, wenn sich die E-Mail-Adressen vor der Domainangabe aus Vornamen und Nachnamen zusammensetzen, handelt es sich um personenbezogene Daten, für deren Übermittlung regelmäßig gerade keine Rechtsgrundlage gegeben ist. In Abhängigkeit des Adressatenkreises ist hierin dann ein Risiko für die Rechte und Freiheiten natürlicher Personen zu sehen.

Cyberkriminalität

Eine weitere Fallgruppe der Meldungen von Datenschutzverletzungen kann allgemein unter dem Begriff der Cyberkriminalität zusammengefasst werden. Unter diesen sehr unspezifischen Begriff fallen generell sämtliche Handlungen/Straftaten, die durch die Nutzung von Kommunikations- und Informationstechniken begangen werden. Für den Berichtszeitraum sind beispielsweise Handlungen Dritter, die auf die Verschlüsselung sowie das Abgreifen von personenbezogenen Daten aus E-Mail-Postfächer, von Servern oder separaten Datenträgern gerichtet sind, zu nennen. Des Weiteren wurden Angriffe auf Online-Accounts gemeldet, um einen unberechtigten Zugriff hierauf und speziell auf die gespeicherten personenbezogenen Daten zu ermöglichen. Im Rahmen dieser Fallgruppe ist hinsichtlich der erforderlichen technisch-organisatorischen Maßnahmen besonderer Wert auf die Informations-/Datensicherheit zu legen.

Fehlerhafte interne Speicherung/Zugriffsberechtigung

Abschließend sei noch eine Fallgruppe erwähnt, die sich in diesem Berichtszeitraum sehr gehäuft ergeben hat. Dies ist die fehlerhafte Verwendung interner digitaler Systeme beim Verantwortlichen selbst, wodurch Mitarbeitern unberechtigt, die Möglichkeit des Zugriffs auf sensible personenbezogene Daten eingeräumt wurde, sei es durch Speicherung in unzulässigen Bereichen oder durch Einräumung unzulässiger Zugriffsberechtigungen.

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 bzgl. 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 Artikel 5 Absatz 2 DSGVO im Besonderen für die Meldefälle bestehende Dokumentationspflicht gemäß Artikel 33 Absatz 5 DSGVO sowie auf die mögliche Pflicht der Benachrichtigung der betroffenen Person nach Artikel 34 DSGVO hin.

4.6.2 Risikobewertung bei Datenschutzverletzungen

Eine sächsische Hochschule hat sich mit folgendem Problem an mich gewandt. Im Rahmen von routinemäßigen Wartungsarbeiten hat das Rechenzentrum der Hochschule festgestellt, dass auf einem aus dem Internet erreichbarer Server eine Anmeldung ohne Passwort möglich war. Das Setzen des Passworts wurde durch eine fehlerhafte Bedienung eines der Administratoren versehentlich nicht gesetzt. Der Server war ohne Kenntnis der Adresse nicht ohne weiteres erreichbar, allerdings sind für solche Lücken auch spezialisierte Suchmaschinen verfügbar, welche gezielt Angriffspunkte sichtbar machen können. Das Brisante war zudem die Funktion des Servers. Dort wurden Anmeldedaten für die Zugänge zu persönlich genutzten Dateiablagen für Studenten und Personal der Hochschule verwaltet. Das Rechenzentrum und die Hochschule haben zügig reagiert, das Passwort wurde umgehend gesetzt, alle Nutzer wurden aufgefordert ihre Passwörter zu ändern und Informationssicherheitsbeauftragter und Datenschutzbeauftragter wurden informiert. Zusätzlich wurde eine externe Firma beauftragt, den Server forensisch auf Unregelmä-

ßigkeiten und Hinweise auf nicht-autorisierte Zugriffe zu untersuchen. Der Datenschutzbeauftragte musste nun die Frage bewerten, ob ein Fall von Artikel 33 DSGVO vorliegt. Jede Schutzverletzung erfordert eine Meldung, bei hohem Risiko müssen die Betroffenen informiert werden. Soweit die gesetzliche Vorgabe, aber wie ist in Fällen mit unklarer Lage zu verfahren. Im konkreten Fall hat die Auswertung des Forensikers keine Hinweise auf einen Einbruch oder einen Missbrauch von Daten ergeben, allerdings gab es ein Delta, da die noch vorhandenen Logdaten nicht den kompletten Zeitraum umfassten, in dem der Server ohne Passwortschutz erreichbar war. Eine Verletzung kann also nicht ausgeschlossen werden. In diesen Fällen muss das Risiko geprüft werden, welches sich aus einer möglichen Verletzung ergeben kann. Im Fall der Hochschule war dieses Risiko beträchtlich. Welche Daten auf den persönlichen Ablagen durch einen eventuellen Angreifer eingesehen werden konnten, ist nicht bekannt, da die persönliche Natur der Ablagen keine administrative Einsichtnahme erlaubt. Dennoch muss davon ausgegangen werden, dass auch besonders schutzwürdige Daten, eben persönliche Daten, davon betroffen waren. Im Ergebnis muss demnach, auch unter Berücksichtigung der die hohe Anzahl der Betroffenen berücksichtigt, das Risiko für Rechte und Freiheiten natürlicher Personen als hoch eingeschätzt werden. Damit ist auch ohne Nachweis eines Schadens eine Benachrichtigung an Betroffene gemäß Artikel 34 DSGVO erforderlich. Dies umfasst eine vollständige Darstellung von Art und Umständen des Vorfalls nebst Empfehlungen zum Umgang. Die Information geht damit über die initial erfolgte Maßnahme, der Aufforderung zum Ändern der Passworte, deutlich hinaus und hatte im konkreten Fall eine zweimalige Information der Hochschule an alle Studenten und Beschäftigte zur Folge. Zu dieser Auffassung kam auch der Datenschutzbeauftragte der Hochschule, er fragte bei mir nach, weil die Leitung aufgrund der zweiten Information nachfragte, ob dies denn zwingend erforderlich sei und ob nicht aufgrund der negativen Außenwirkung darauf verzichtet werden könne. Ich habe den Datenschutzbeauftragten in seiner Ansicht gestärkt.

Die Artikel 33 und 34 DSGVO sollten ausdrücklich nicht als Pranger verstanden werden. Vielmehr geht es darum, einen aufrichtigen und für die Betroffenen hilfreichen Umgang mit Datenpannen zu fördern. Fehler können passieren, wichtig sind jedoch der transparente Umgang damit und die nachfolgende Ergreifung der geeigneten technischen und organisatorischen Maßnahmen, damit diese Datenpannen in der Zukunft nach Möglichkeit ausgeschlossen werden können. Dazu zählen auch die Abwägungsentscheidungen beim Umgang mit potenziellen Fällen von Artikel 33 und DSDVO. Auch wenn sich ein Verantwortlicher nach Abwägung entscheidet, dass kein Fall einer Verletzung vorliegt,

sollte alle maßgeblichen Entscheidungsgründe gut dokumentiert werden, um eine spätere Nachvollziehbarkeit zu ermöglichen.

4.7 Betroffenenbenachrichtigung

Nicht belegt.

4.8 Datenschutz-Folgenabschätzung

4.8.1 Datenschutz-Folgenabschätzung mit SDM

Mit der DSGVO wurde ein neues Instrument zur Bewertung von Risiken für die betroffenen Personen einer Datenverarbeitung eingeführt, die Datenschutz-Folgenabschätzung. Damit sollen vor allem hochriskante Verarbeitungen, welche auf neuen Technologien beruhen oder Verarbeitungen mit großem Umfang, im Vorfeld untersucht werden und mögliche Risiken begrenzt werden. Das Verfahren ist zweistufig angelegt, zum einen ist eine Schwellwertanalyse erforderlich, um bei unklaren Auswirkungen einer Verarbeitung die Erforderlichkeit einer Datenschutz-Folgenabschätzung abschätzen zu können und im zweiten Schritt die Datenschutz-Folgenabschätzung selbst.

Verantwortliche haben in der Praxis oft Probleme eine Schwellwertanalyse oder eine Datenschutz-Folgenabschätzung zu erstellen. Die mir im Rahmen der Aufsichtstätigkeit vorgelegten Dokumente waren diesbezüglich teilweise mangelhaft. Ein grundlegendes Problem war oft, dass Maßstäbe der Informationssicherheit für die Datenschutz-Folgenabschätzung verwendet wurden und die Risikobetrachtung aus Sicht des Verarbeiters und nicht der betroffenen Personen durchgeführt wurden. Zwar können Risiken der Informationssicherheit auch Auswirkungen auf Rechte und Risiken natürlicher Personen haben, das Schutzgut und damit der Betrachtungswinkel sind aber unterschiedlich. Ein einfaches Beispiel: Beim Einsatz von Videoüberwachung wird oftmals das Thema Verfügbarkeit und die Risiken eines Ausfalls der Überwachungsanlage ausführlich beschrieben. Und zwar aus Sicht der Organisation, welche die Anlage betreibt. Bei Eingriffen in Grundrechte sind die Verfügbarkeitsrisiken aus Sicht des Betroffenen aber wesentlich anders zu bewerten.

Welche Möglichkeiten haben Verantwortliche eine formell korrekte und somit auch dem Erfüllen der datenschutzrechtlichen Vorgaben zuträgliche Analyse der Risiken für betroffene Personen zu erstellen? Hinweise zum Vorgehen bietet das bereits seit In-Kraft-

Treten der DSGVO existierende Kurzpapier der Datenschutzkonferenz zur "Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO". Praktisch durchgeführt werden können sowohl die Schwellwertanalyse als auch die Datenschutz-Folgenabschätzung mit Hilfe des Standard-Datenschutzmodells.

Die Entscheidung, welche Relevanzschwelle für eine solche Untersuchung gilt, lässt sich mit Hilfe des Kapitels D3 des SDM klären. Dort sind die relevanten Betrachtungen zur Bestimmung möglicher Risiken aufgezeigt, welche für den konkreten Anwendungsfall näher zu spezifizieren sind. Damit kann klar festgelegt werden, ob eine Datenschutz-Folgenabschätzung erforderlich ist oder lediglich eine Schwellwertanalyse vorzunehmen ist. Es empfiehlt sich dennoch für beide Analysen die gleiche Vorgehensweise anzuwenden, da auch für Verarbeitungen ohne die Erforderlichkeit einer Datenschutz-Folgenabschätzung die Festlegung von Maßnahmen zur Minderung der Risiken für Rechte und Freiheiten natürlicher Personen zwingend ist.

Im Vorfeld der Analyse ist es erforderlich, die geplante Verarbeitung, die verfolgten Zwecke und die beteiligten Akteure sowie die Datenarten und -flüsse zu beschreiben und die Rechtsgrundlage(n) zu benennen auf welche die Verarbeitung gestützt werden soll.

Die Bestimmung der Risiken kann anhand von Teil B des SDM erfolgen, welcher die relevanten Anforderungen der DSGVO beschreibt und mit den Gewährleistungszielen des SDM in Beziehung setzt. Anhand dieser Anforderungen muss der Verantwortliche mögliche Risiken und Missbrauchsszenarien identifizieren und hinsichtlich Eintrittswahrscheinlichkeit und Schwere bewerten. Dabei müssen sowohl die Risiken, die auch bei einer rechtmäßigen Verarbeitung auftreten können (z. B. unbefugte Kenntnisnahme durch Berechtigte), als auch solche durch externe Faktoren (z. B. Angriff auf IT-Systeme) berücksichtigt werden.

Anhand der ermittelten Risiken müssen im Anschluss Maßnahmen festgelegt werden, welche diese Risiken effektiv mindern. Anhand der Gewährleistungsziele des SDM lässt sich dies effektiv durch die Anwendung der generischen Maßnahmen (Kapitel D1 des SDM) auf die konkrete Verarbeitung erreichen. Zusätzlich können die Bausteine des SDM-Maßnahmenkatalogs (https://www.datenschutz-mv.de/datenschutz/datenschutz-modell/) hinzugezogen werden. Die Bausteine wurden, auch unter Mitwirkung meiner Behörde, als Erprobungsfassung veröffentlicht. Künftig sollen diese und weitere Bau-

steine von der Datenschutzkonferenz verabschiedet und veröffentlicht werden. Zur Anwendung der Bausteine und der Verbindlichkeit der Anwendung einzelner Maßnahmen führt Kapitel E6 des SDM näher aus.

Für eine Datenschutz-Folgenabschätzung müssen im Anschluss noch Restrisiken bewertet und die Implementierung der Schutzmaßnahmen einer Bewertung, je nach Umfang der Verarbeitung und Bewertung der Restrisiken ggf. durch einen externen Dritten (z. B. in Form eines Penetrationstests oder einer Sicherheitsanalyse), unterzogen werden.

Neben dem SDM selbst sind folgende Dokumente hilfreich:

- White Paper „Datenschutz-Folgenabschätzung – Ein Werkzeug für besseren Datenschutz“ des Forschungsverbundes „Forum Privatheit“ (https://www.dsfa.eu/index.php/tag/white-paper/)

- Planspiel Datenschutz-Folgenabschätzung (DSFA) (https://www.datenschutz-mv.de/datenschutz/DSGVO/Hilfsmittel-zur-Umsetzung/)

Eine Datenschutz-Folgenabschätzung stellt also keine unüberwindbare Hürde für die Einführung eines Verfahrens dar. Vielmehr können Verantwortliche dadurch Klarheit erlangen, an welchen Stellen der Verarbeitung Risiken entstehen und wie diese minimiert werden können. Wichtig ist eine klare Ausrichtung auf die Sicht des Betroffenen und damit eine andere Sichtweise als viele Verantwortliche sie aus der Informationssicherheit kennen. Unstrittig dienen viele Maßnahmen der Informationssicherheit auch der Risikominimierung für Rechte und Freiheiten der Betroffenen. Bei der Beschreibung der Maßnahmen ist jedoch darauf zu achten, wer Adressat der getroffenen Maßnahme ist.

Vergleiche auch den Beitrag unter 4.1.1.

4.8.2 Projektierung eines einheitlichen Bewerbermanagementverfahrens im Bereich der Staatsverwaltung

Im letzten Berichtszeitraum wurde meine Dienststelle seitens der Staatskanzlei wegen der Einführung eines Bewerbermanagementverfahrens für die Ressorts des Freistaates um Beratung gebeten; dies um eine datenschutzkonforme Gestaltung der Software sicherzustellen. Unter Leitung der Staatskanzlei war eine entsprechende Projektgruppe gegründet und die Verfahrensanforderungen waren aus den jeweiligen Ressorts zusammengetragen

worden. Die einzelnen datenverarbeitenden Stellen der jeweiligen Ressorts sollten getrennt und an ihrer Zuständigkeit und Erforderlichkeit orientiert mit separaten Zugriffen auf den Datenbestand des Verfahrens bzw. Bereich zuzugreifen und Daten zu verarbeiten befugt sein. Neben weiteren herkömmlichen datenschutzrechtlichen Anforderungen, was automatisierte Verfahren betrifft, ergaben sich bei der Betrachtung des konkreten Vorhabens einige neuartige nach der DSGVO zu beurteilende Fragen.

Unter anderem war seitens der Projektierung festgelegt worden, dass die Software die Möglichkeit bieten müsse, dass Bewerbungsunterlagen automatisiert nach vorgegebenen Kriterien abgeglichen und differenziert bewertet werden sowie eine Reihenfolge der Bewerbungen bzw. Kandidaten anhand deren Geeignetheit erstellt werden können solle, ein sogenanntes „Ranking“. Das Verfahren sollte auch die Möglichkeit bieten, nach einer vordefinierten Bewertungsskala die Bewerbungen zu bewerten und entsprechend festgelegter Bewertungskriterien und -aspekte zu gewichten. Auf diese Weise sollte ein automatisierter Abgleich des Anforderungsprofils und der Bewerber erfolgen sowie anschließend eine automatisierte Bewertung stattfinden können.

Nach Artikel 35 Absatz 1 DSGVO ist eine Datenschutz-Folgenabschätzung vom Verantwortlichen vorzunehmen, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Eine Datenschutz-Folgenabschätzung ist nach Artikel 35 Absatz 3 Buchstabe a) DSGVO zudem immer dann durchzuführen, wenn eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen erfolgt, die sich auf automatisierte Verarbeitung einschließlich „Profiling“ gründet, welche als Grundlage für Entscheidungen dient, die Rechtswirkungen gegenüber Einzelnen entfaltet oder diese in ähnlich erheblicher Weise beeinträchtigt.

Nach den Projektanforderungen sollten die Daten der Bewerber automatisiert verarbeitet werden. Dabei handelte es sich um personenbezogene Daten wie zum Beispiel Name, Adress- und Kontaktdaten, Geschlecht, Schwerbehinderung, Zeugnisse sowie dienstliche Beurteilungen. Aus dieser automatisierten Verarbeitung ergäben sich Bewerberprofile, die mit den von der ausschreibenden Stelle vorgegebenen Kriterien und Gewichtungen abgeglichen werden sollten, um dann automatisiert eine Reihenfolge der Bewerber zu erstellen. Auf diese Weise würde durch das Bewerbermanagement-System eine systematische und umfassende Bewertung von persönlichen Daten des Bewerbers erfolgen. Die

durch das System erstellte Reihenfolge sollte wiederum Grundlage für die später zu treffende Entscheidung sein, welcher Kandidat zum Vorstellungsgespräch eingeladen wird. Diese - durch automatisierte Prozesse - entstehende Reihenfolge der Bewerber wäre geeignet, betroffene Personen in ähnlich erheblicher Weise zu beeinträchtigen, wie Entscheidungen mit Rechtscharakter, da mittels dieser automatisierten Entscheidung über den Zugang zu Auswahlverfahren und Stellen entschieden würde; vgl. WP 251 rev.01, Seite 24 der Artikel-29-Gruppe.

Selbst wenn durch das IT-gestützte Bewerbermanagement-System keine Bewertung (Profiling) hätte vorgenommen werden sollen, wäre dennoch eine Datenschutz-Folgenabschätzung vorzunehmen gewesen, soweit eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten im Sinne von Artikel 9 Absatz 1 DSGVO gemäß Artikel 35 Absatz 3 Buchstabe b) DSGVO erfolgt, da nach der Konzeption des Bewerbermanagements-Systems auch das Merkmal der Schwerbehinderung und damit ein personenbezogenes Datum gemäß Artikel 9 Absatz 1 DSGVO verarbeitet werden sollte und eine nach Artikel 35 Absatz 3 Buchstabe b) DSGVO erforderliche „umfangreiche Verarbeitung“ wegen des ressortübergreifenden und in der gesamten Staatsverwaltung vorgesehenen Einsatzes und der damit erwartbaren Verarbeitung von großen Mengen sensibler Daten vorauszusetzen war, vgl. Erwägungsgrund (91) der DSGVO und WP 248 Rev. 1, Seite 11 der Artikel-29-Gruppe.

Somit war bei bestehender Planung zwingend eine Datenschutz-Folgenabschätzung nach Artikel 35 Absatz 3 Buchstabe a) DSGVO für das Verfahren vorzunehmen gewesen, was ich der Staatskanzlei mitteilte. Im laufenden Berichtszeitraum konnte diese Anforderung seitens der Verantwortlichen nicht mehr umgesetzt und meinerseits inhaltlich geprüft werden.

Programmtechnisch unterstützte Verfahrensschritte in der vorgesehenen Umsetzung sind zudem grundsätzlich geeignet, als sogenanntes „Profiling“ und gleichzeitig als „automatisierte Entscheidungen“ im Sinne von Artikel 4 Absatz 4, Artikel 22 DSGVO qualifiziert zu werden. Da durch automatisierte Entscheidungen ungerechtfertigte Eingriffe in die Rechte betroffener Personen erfolgen können, unter anderem durch ungerechtfertigte Diskriminierung, stellt die DSGVO gesteigerte Anforderungen an den Einsatz von Verfahren, die automatisierte Entscheidungen generieren. Allerdings unterlag das Verfahren nach meiner Überzeugung nicht den strengen Anforderungen des Artikels 22 DSGVO,

da die Einstellungsentscheidung selbst nicht ausschließlich auf einer automatisierten Entscheidung beruhen sollte. Vielmehr sollte die automatisierte Bewertung und Erstellung der Reihenfolge der Bewerbungen die Entscheidungsgrundlage sein, mit welchen ausgewählten Bewerbern Vorstellungsgespräche stattfinden sollten. Die Einstellungsentscheidung selbst wäre hingegen nicht automatisiert worden.

Trotz des ressortübergreifenden Einsatzes des Bewerbermanagement-Systems blieb damit im Ergebnis nur eine Datenschutz-Folgenabschätzung, die allerdings sämtliche Spezifika der jeweiligen Ressorts abzubilden hatte, zu erstellen.

Im Rahmen der Projektierung war auch die Vorstellung der Staatsregierung, zum Zweck der Gewinnung von Mitarbeitern, „Active Sourcing“ zu betreiben und die Frage deren Zulässigkeit, Gegenstand meiner datenschutzrechtlichen Einschätzung gewesen. Unter „Active Sourcing“ ist die proaktive Ansprache von besonders qualifiziertem Personal zu verstehen. Dies wurde seitens der Projektverantwortlichen als erforderlich deklariert und sollte bei der Bewerbermanagement-Software über ein IT-gestütztes *Tool* unterstützt werden, welches Bewerber- bzw. Profildaten aus sozialen und berufsorientierten Internetplattformen bzw. Netzwerken auslesen und automatisch in die Bewerbermanagement-Software transferieren sollte.

Auch der Transfer und die weitere Speicherung und Verwendung von Namens-, Kontaktangaben und Lebenslaufinhalten aus Internetpräsenzen und über das Internet zugänglichen Netzwerken stellt eine personenbezogene Datenverarbeitung im Sinne des Artikel 4 Nummer 2 DSGVO dar. Deren Rechtmäßigkeit wäre wegen der nicht bestehenden Rechtsbeziehungen bzw. mangels bereichsspezifischer Vorschriften zwischen Verantwortlichen und betroffenen Personen eigentlich nach Buchstabe f) der zentralen Vorschrift des Artikel 6 Absatz 1 der DSGVO zu beurteilen gewesen.

Voranzustellen ist, dass betroffene Personen, auch nicht in beruflich-orientierten Netzwerken, gemeinhin damit zu rechnen haben, dass die öffentliche Verwaltung ohne ihre Kenntnis personenbezogene Sammlungen zu ihnen zu Stellenbesetzungszwecken anlegen könnte und das, ohne dass sie selbst Interesse an einem Wechsel in die öffentliche Verwaltung bekundet haben. Insbesondere Nutzer beruflicher Netzwerke veröffentlichen zwar ihr Profil, dies bedeutet jedoch nicht, dass diese überhaupt auf Stellensuche sind. So käme eine ungefragte Erhebung letztendlich einer Vorratsdatenspeicherung gleich, womit

sich unvermeidlich die grundsätzlich bestehende Frage der Erforderlichkeit und Verhältnismäßigkeit einer solchen weitgehenden Erhebung und Verarbeitung von potentiell für Stellenbesetzungsverfahren in Betracht kommenden Personen aufdrängt.

Auch wenn zum Zeitpunkt meiner Beteiligung das Verfahren des „Active Sourcing“ seitens der Staatskanzlei noch nicht weitergehend und präzisiert dargestellt werden konnte, teilte ich in einer ersten Einschätzung der Projektleitung vorgreifend mit, dass nach meiner Überzeugung, auch die Auffangvorschrift des Artikel 6 Absatz 1 Buchstabe f) DSGVO als Rechtsgrundlage für die Datenverarbeitung nicht in Betracht kommen kann. Die Vorschrift ist ein Ausnahmetatbestand für all jene Fälle, in denen eine Verarbeitung nicht nach den Alternativen der Buchstaben a) bis e) des Artikel 6 Absatz 1 der Verordnung möglich ist. Artikel 6 Absatz 1 letzter Satz lautet dann allerdings: „Unterabsatz 1 Buchstabe f) gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung." Absatz 1 Buchstabe f) kann demnach nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Datenverarbeitung in Anspruch genommen werden. Vielmehr obliegt es nach Vorstellung des Verordnungsgebers grundsätzlich dem Gesetzgeber per Rechtsvorschrift die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch Behörden zu schaffen, vergleiche dazu Erwägungsgrund 47 Satz 5. Insoweit ist der Anwendungsbereich des Artikel 6 Absatz 1 Buchstabe f) DSGVO als Erlaubnistatbestand für die öffentliche Verwaltung nicht eröffnet und kann nicht, wenn kein sonstiger Erlaubnistatbestand zur Datenverarbeitung vorliegt, im Rahmen einer Interessenabwägung herangezogen werden, um eine gewünschte Datenverarbeitung doch noch zu ermöglichen. Auch die Überlegung, dass die Verwaltung fiskalisch handeln könnte und daher in Analogie zu nicht-öffentlichen Stellen Artikel 6 Absatz 1 Buchstabe f) DSGVO doch Anwendung finden könnte, greift nach meiner Überzeugung nicht. Die Besetzung der Dienstposten, die zumeist auch haushaltsrechtlich Beamtenstellen sind, die öffentlichrechtlich vergeben werden, ist als Maßnahme zur Erhaltung der „Betriebsfähigkeit“ der Verwaltung, nicht wegzudenken und als Teil, jedenfalls aber als Annex der öffentlichen Aufgabenwahrnehmung einzustufen.

Zu berücksichtigen ist im Kontext zusätzlich, dass der Zugang zu öffentlichen Ämtern dem Maßstab des Artikels 33 Absatz 2 Grundgesetz unterliegt, was ungleichmäßige Aktivität seitens der öffentlichen Hand gegenüber Bewerbern nicht vorsieht bzw. ausschließt. Danach besteht nach Eignung und fachlicher Leistung gleicher Zugang zu jedem öffentlichen Amt. Dem ist bereits durch das Procedere, wie jedem potentiellen Bewerber Gelegenheit gegeben wird, auf Stellenausschreibungen der öffentlichen Verwaltung zu

reagieren, Rechnung zu tragen. Eine individuelle und ungeregelte Ansprache einzelner Personen aus sozialen Netzwerken durch die Verwaltung selbst würde hingegen die Neutralität und Chancengerechtigkeit gegenüber Personen, die diese Netzwerke nicht nutzen, in Frage stellen. Bei Bewerbungsverfahren handelt die öffentliche Verwaltung als ausschreibende Stelle, bei der potentielle Bewerber gleichmäßig und geordnet angesprochen werden sollen.

Auch praktische Schwierigkeiten könnten sich bei „Active Sourcing“ einstellen. Soweit nicht automatisiert über ein spezielles Tool der IT-gestützten Bewerbermanagementsoftware agiert, sondern die Ansprache über die Mitarbeiter der personalverwaltenden Stelle durchgeführt werden soll, ergibt sich die Problematik, dass durch die Nutzer nicht selten überschießende Informationen in den sozialen Netzwerken bereitgehalten werden, die die öffentliche Verwaltung zur Kenntnis nehmen könnte, aber im geregelten Bewerbungsverfahren überhaupt nicht erheben würde und dürfte. Beschränkende Verhaltensanweisungen, in welchen und wie sich dienstliche Rechercheure in sozialen Netzwerken zu verhalten haben, existieren seitens sächsischer Behörden zudem nicht. Eine dienstlicherseits verdeckte Sichtung der Bewerberlage ist ebenso nicht vorgesehen und auch nach meiner Überzeugung nicht vertretbar.

Als Ergebnis blieb festzuhalten, dass eine Rechtsgrundlage für die vorgesehene personenbezogene Datenverarbeitung der Bewerberdatenbank bejaht werden konnte. Der Staatskanzlei teilte ich aber auch meine Bedenken in den zuvor dargestellten Einzelfragen mit.

Als allgemeiner Hinweis für Verantwortliche bleibt zu betonen, dass aufgrund der Vielschichtigkeit der datenschutzrechtlichen Fragestellungen jedem Verantwortlichen – nicht-öffentlichen wie öffentlichen Stellen – nachhaltig anzuraten ist, bei der Einführung komplexer Verfahren zur Verarbeitung von Bewerber- und Beschäftigtendaten frühzeitig den betrieblichen bzw. behördlichen Datenschutzbeauftragen zu beteiligen.

Meine Berichterstattung über das Projekt der Staatsregierung werde ich fortführen.

4.9 Datenschutzbeauftragte

4.9.1 Sprachliche Befähigung des Datenschutzbeauftragten

In einer Anfrage eines Betriebsrats teilte mir dieser mit, dass der benannte Datenschutzbeauftragte des Unternehmens nicht auf Deutsch mit dem Betriebsrat kommuniziere, der sich mit datenschutzrechtlichen Fragen an den Datenschutzbeauftragten gewandt hatte. Der Betriebsrat bat um Rat, ob dies rechtskonform sei.

Hierzu vertrete ich folgende Auffassung: Artikel 39 Absatz 1 Buchstaben a) und b) DSGVO setzen voraus, dass eine beratende und unterrichtende Tätigkeit durch den benannten Datenschutzbeauftragten auch tatsächlich erfolgt. Der Betriebsrat ist eine funktionale Stelle, die seitens des Verantwortlichen bzw. für den Verantwortlichen selbstständig Aufgaben wahrnimmt und ist daher auch im Sinne von Artikel 39 Absatz 1 Buchstabe a) DSGVO seitens des benannten Datenschutzbeauftragten zu unterstützen. Grundsätzlich hat dies in für den Adressaten beim Verantwortlichen verständlicher Sprach- und Schriftsprache bzw. Landessprache zu erfolgen.

Denkbar ist aber auch, dass in einem Unternehmen betriebsintern eine andere Landessprache zur Kommunikation festgelegt worden ist. Dies wäre dann in einer Einzelfallbetrachtung zu prüfen gewesen, war aber im konkreten Fall nicht relevant.

4.9.2 Benennung eines Dachverbandes als Datenschutzbeauftragter

Wie bereits im Tätigkeitsbericht 2018 unter Punkt 4.8.2 dargestellt, bewerte ich die Benennung einer juristischen Person als betrieblichen Datenschutzbeauftragten als grundsätzlich zulässig. Nachdem sich nun im Berichtszeitraum ein Verband der Wohnungswirtschaft mit der speziellen Frage, ob auch er für seine Mitgliedsunternehmen als Datenschutzbeauftragter fungieren könne, an mich gewandt hatte, habe ich auch das bejaht. Das heißt, ein Verband kann durchaus die Funktion des Datenschutzbeauftragten für seine Mitgliedsunternehmen übernehmen. Notwendige Voraussetzungen hierfür sind, dass bei der Benennung des Verbandes die dort in dem zuständigen „Datenschutzbeauftragtenteam“ tätigen Mitarbeiter namentlich bezeichnet sind und die Mitgliedsunternehmen bei diesbezüglichen Änderungen unverzüglich informiert werden. Bereits im Tätigkeitsbericht 2018 (Punkt 4.8.2) hatte ich darauf hingewiesen, dass die für die juristische Person, hier den Verband, handelnden und die Aufgaben des Datenschutzbeauftragten ausführenden Personen sämtliche Voraussetzungen des Kapitels IV, Abschnitt 4, der DSGVO zu

erfüllen geeignet sein müssen. Im konkreten Fall waren die diesbezüglichen Voraussetzungen gegeben: Dem „Datenschutzbeauftragtenteam“ gehörten zwei durch den TÜV als Datenschutzbeauftragte zertifizierte Rechtsanwälte an.

Mit einer vergleichbaren Konstellation hatte ich mich auch schon im Tätigkeitsbericht 2018 unter Punkt 4.8.5 befasst. Dort ging es um Beliehene, die sich über Berufsverbände oder berufsständige Körperschaften zusammengeschlossen hatten, um der Pflicht zur Benennung eines Datenschutzbeauftragten nachzukommen.

4.10 Verhaltensregeln und Zertifizierung

4.10.1 ISO/IEC 27701 – eine Norm für Datenschutzmanagement

Alternativ zum Standard Datenschutzmodell (SDM) entwickelt die Internationale Organisation für Normung (ISO) mit der ISO/IEC 27701 eine Norm zum Nachweis der Einhaltung datenschutzrechtlicher Vorschriften. Mit Einführung dieser Norm wird das Ziel verfolgt, auch eine Möglichkeit für die Zertifizierung des Datenschutzmanagements nach Artikel 42 DSGVO zu schaffen.

Veröffentlicht wurde ISO/IEC 27701 im August 2019 unter dem Titel Datenschutzmanagement als Ergänzung des Informationssicherheits-Managementsystem (ISMS) nach ISO/IEC 27001 und 27002. Ursprünglich wurde das Datenschutzmanagement unter der Nummer ISO/IEC 27552 entwickelt.

Bei den Ergänzungen handelt es sich vordergründig um terminologische Adaptionen. Der Fokus liegt nicht mehr auf *Informationssicherheit,* sondern auf *Informationssicherheit und Datenschutz*. Inhaltlich spezifiziert ISO/IEC 27701 Anforderungen und bietet eine Anleitung für die Einrichtung, Implementierung, Aufrechterhaltung und kontinuierliche Verbesserung eines Datenschutz-Informationsmanagementsystems

Neben dem unmittelbaren Bezug auf ISO/IEC 27001 verweist der neue Standard auf Grundsätze des Datenschutzes, die in ISO/IEC 29100 definiert sind. Eingebunden werden zudem ISO/IEC 27018, ISO/IEC 29151 sowie ein expliziter Verweis auf die DSGVO.

Die Einbeziehung der DSGVO und diesbezüglicher gerichtlicher Entscheidungen sind aus Sicht des Datenschutzes durchaus zweckmäßige Erweiterungen. Im Rahmen der Ri-

sikobeurteilung verlangt ISO/IEC 27701 die Aspekte der Verarbeitung personenbezogener Daten zu berücksichtigen. Aus Perspektive der Normierung eines Managementsystems sind Insbesondere folgende Neuerungen festzustellen:

- Erweiterung der IS-Leitlinie um Datenschutz
- Festlegung eines Verantwortlichen für das Datenschutzmanagement
- Datenschutz-Schulung der Mitarbeiter
- Protokollierung von Zugriffen und Veränderungen
- Verschlüsselung besonderer Kategorien personenbezogener Daten
- Berücksichtigung des „Privacy by Design“ Grundsatzes
- Überprüfung von Sicherheitsvorfällen auf Datenschutzverletzungen

Aus konzeptioneller Perspektive ist es derzeit nicht möglich, eine DSGVO konforme Zertifizierung auf Basis der ISO/IEC 27701 zu etablieren. Die Anforderungen an eine diesbezügliche Zertifizierungsstelle sind in Artikel 43 DSGVO definiert. Als Erweiterung der ISO/IEC 27001 fokussiert ISO/IEC 27701 Managementsysteme, deren Zertifizierung sich nach ISO/IEC 17021 richten. Artikel 43 DSGVO fordert hingegen die Akkreditierung von Zertifizierungsstellen auf Basis ISO/IEC 17065, die auf eine Zertifizierung von Produkten und Prozessen ausgerichtet ist.

Dennoch bietet der neue Standard ISO/IEC 27701 Chancen um einen DSGVO-konformen Umgang mit personenbezogenen Daten zu begründen. Öffentliche und nichtöffentliche Organisationen haben die Chance ihr bestehendes ISMS durch Implementierung der ISO/IEC 27701 mit relativ geringem Aufwand um Anforderungen des Datenschutzes zu erweitern. Es ist bspw. denkbar, dass bei der Umsetzung auf Richtlinien, Prozesse und Dokumentationen zurückgegriffen werden kann, die in der Organisation bereits vorhanden sind.

4.10.2 Akkreditierungen gemäß Artikel 42, 43 DSGVO

Hinsichtlich der Thematik der Zertifikate, Datenschutzsiegel und -prüfzeichen sowie dem zugrunde liegenden Prozess der Akkreditierung und Zertifizierung verweise ich auf meinen Beitrag im letzten Tätigkeitsbericht (1. April 2017 bis 31.12.2018), Teil 2, Ziffer 4.9.1, Seite 226.

Seit dem 01.01.2019 ist die Antragsphase zur Programmprüfung bei der Deutschen Akkreditierungsstelle (DAkkS) eröffnet.

Einen Überblick mit weitergehenden Hinweisen findet man auf der Internetseite der DAkkS unter der Überschrift „Projekt Datenschutz“ unter folgendem Link: https://www.dakks.de/content/projekt-datenschutz

Darüber hinaus findet man dort eine umfassende Darstellung des gesamten Akkreditierungsprozesses gemäß Artikel 42, 43 DSGVO als schematisches Schaubild mit nachfolgender detaillierter Beschreibung, welche zusammen mit den deutschen Datenschutzaufsichtsbehörden erarbeitet wurde, unter folgendem Link: https://www.datenschutzkonferenz-online.de/media/oh/20190315_oh_akk_c.pdf

5 Internationaler Datenverkehr

5.1 Zeichnungserfordernis bei Standardvertragsklauseln

Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder setzen sich im letzten Berichtszeitraum auch mit der Frage auseinander, ob für seitens von Verantwortlichen verwendeten Standardvertragsklauseln ein Zeichnungserfordernis besteht.

Dazu vertrete ich nachstehende Auffassung: Es obliegt den die Klauseln verwendenden Unternehmen sicherzustellen, dass die Einbeziehung der Klauseln in den dem Rechtsverhältnis zu Grunde liegenden Vertrag wirksam ist. Anzuraten ist inhaltlich, dass im Hauptvertrag zu Gunsten der Standardvertragsklauseln eine Vorrangbestimmung eingebaut wird.

Rein rechtlich gesehen sieht die DSGVO für Standardvertragsklauseln kein Schriftformerfordernis vor. Auch ist eine elektronische Signatur nicht erforderlich, vergleiche Artikel 28 Absatz 9 DSGVO. Insoweit könnten Standardvertragsklauseln auch ohne Unterschrift wirksam vereinbart sein. Unabhängig davon wäre den beteiligten Vertragspartnern – mindestens auch zu Nachweiszwecken – zu raten, auch die Standardvertragsklauseln zu unterzeichnen. Dem verwendenden Unternehmen obliegt es jedenfalls, zu belegen, dass die Klauseln bzw. Anlagen Bestandteil des Vertrags geworden sind.

5.2 Durchsetzung der DSGVO wegen des räumlichen Anwendungsbereichs gegenüber Verantwortlichen in Drittländern

Gemäß Artikel 3 Absatz 2 DSGVO unterliegen auch Verantwortliche in Drittländern dem Anwendungsbereich der Verordnung. Bei meiner Dienststelle gehen zahlreiche Beschwerden gegen Unternehmen mit Sitz außerhalb der Europäischen Union ein. Soweit die Verantwortlichen kein Vertreter nach Artikel 27 DSGVO benannt haben, stellt sich die Einwirkung auf den Verantwortlichen in seiner Umsetzung als praktisch schwierig dar. Soweit Maßnahmen gegenüber diesen Verantwortlichen ergriffen werden sollen, wäre zudem ein Amtshilfeverfahren und ein Procedere auf dem diplomatischen Weg über die Außenvertretungen der Bundesrepublik Deutschland einzuleiten. Aktuell teile ich den Beschwerdeführern mit, dass ich – in Ermangelung zwischenstaatlicher Vereinbarungen – keine Möglichkeiten sehe, meine Rechtspositionen bzw. Anordnungen durchzusetzen.

6 Sächsischer Datenschutzbeauftragter - Tätigkeit, Aufgaben, Befugnisse

6.1 Zuständigkeit

6.1.1 Zuständigkeit des Sächsischen Datenschutzbeauftragten bei Medienunternehmen

Im vergangenen Berichtszeitraum erhielt ich Beschwerden von betroffenen Personen, die sich gegen Veröffentlichungen von Medienunternehmen wandten.

Bei Handlungen, die die Verarbeitung personenbezogener Daten zu journalistischen Zwecken zum Gegenstand haben, ist meine Behörde allerdings nur eingeschränkt oder sachlich gar nicht zuständig.

Zum Rechtsstand im Berichtszeitraum:

Gemäß § 11a Satz 4 Sächsisches Gesetz über die Presse ist meine Behörde nicht zuständig. Danach gilt im Freistaat Sachsen bei der Datenverarbeitung für journalistische Zwecke die DSGVO nach Maßgabe des Artikels 85 nur sehr eingeschränkt. Die entsprechende Einstufung von in der Praxis mir gegenüber benannten Internetpräsenzen hat dabei unabhängig von journalistischer Qualität zu erfolgen. Darüber hinaus findet nur Artikel 5 Absatz 1 Buchstabe f) DSGVO Anwendung, vergleiche denselben Gesetzeswortlaut. In häufig aufgezeigten datenschutz-und persönlichkeitsrechtlichen Streitfragen geht es nicht um die Sicherheit der personenbezogenen Daten und deren Gewährleistung einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (Integrität und Vertraulichkeit).

Soweit sich ein Unternehmen der Selbstregulierung durch den Pressekodex und der Beschwerdeordnung des Deutschen Presserats unterworfen hat, wäre für betroffene Personen ggfs. auch Beschwerde bei dieser Stelle vorstellbar.

Für den öffentlich-rechtlichen Rundfunk, den Mitteldeutschen Rundfunk, ist meine Dienststelle datenschutzaufsichtlich ebenso nicht berufen, sondern der MDR-Datenschutzbeauftragte als zuständige sektorale Aufsichtsbehörde, §§ 42, 42a, 42b des Staatsvertrags über den Mitteldeutschen Rundfunk.

Gemäß § 44 Absatz 1, 2 Sächsisches Privatrundfunkgesetz ist die Sächsische Landesanstalt für privaten Rundfunk und neue Medien Aufsichtsbehörde bei der Verarbeitung personenbezogener Daten zu journalistischen Zwecken. Allerdings ist sie nur insoweit Aufsichtsbehörde, als dass es sich um zugelassene Veranstalter und ihre Hilfsunternehmen in ihrem Zuständigkeitsbereich, also in Sachsen, handelt. Bei „Veranstaltern" sind im engeren Sinne Rundfunkangebote, d.h. Live-Angebote anbietende Unternehmen und Plattformen gemeint. Oft sind in dieser Gemengelage auch Aufsichtsbehörden aus anderen Bundesländern zuständig.

Bei entsprechenden Eingaben nehme ich den Vorgang regelmäßig ohne weitere Bearbeitung zu den Akten und weise die Beschwerdeführer auf meine Unzuständigkeit hin. Abgaben des Vorgangs sind wegen der nur eingeschränkten Anwendbarkeit der DSGVO zumeist nicht zweckmäßig, ggfs. wird noch auf den MDR-Datenschutzbeauftragten als spezifische Aufsichtsbehörde verwiesen.

6.1.2 Zuständigkeit für Konzernniederlassungen

Der Sächsische Datenschutzbeauftragte ist zuständig für die Durchsetzung der DSGVO im Freistaat Sachsen. Soweit Verarbeitungen personenbezogener Daten durch Verantwortliche durchgeführt werden, die in einem anderen Mitgliedstaat bzw. Bundesland ihre Haupt- oder einzige Niederlassung haben, ist die dortige Datenschutzaufsichtsbehörde im aufsichtsrechtlichen Verfahren federführend, Artikel 55 Absatz 1 DSGVO, § 19 Absatz 1 Bundesdatenschutzgesetz. Der Sächsische Datenschutzbeauftragte hat jedoch grundsätzlich eine eigene Kompetenzoption für bei ihm eingereichte Beschwerden und etwaige Datenschutzverstöße, wenn deren Gegenstand nur mit einer Niederlassung in Sachsen zusammenhängt oder betroffene Personen nur in Sachsen erheblich beeinträchtigt, Artikel 56 Absatz 2 DSGVO, § 19 Absatz 2 Bundesdatenschutzgesetz, § 14 Absatz 2 Sächsisches Datenschutzdurchführungsgesetz. Dies gilt jedoch nur insoweit, als die für die Hauptniederlassung zuständige Aufsichtsbehörde ihr Selbsteintrittsrecht nach Artikel 56 Absatz 2 DSGVO nicht ausübt.

Vergleiche im Übrigen auch 5.1.1, Tätigkeitsbericht 2017/2018 (Teil 2)

6.1.3 Kurioses – Kurz und knapp

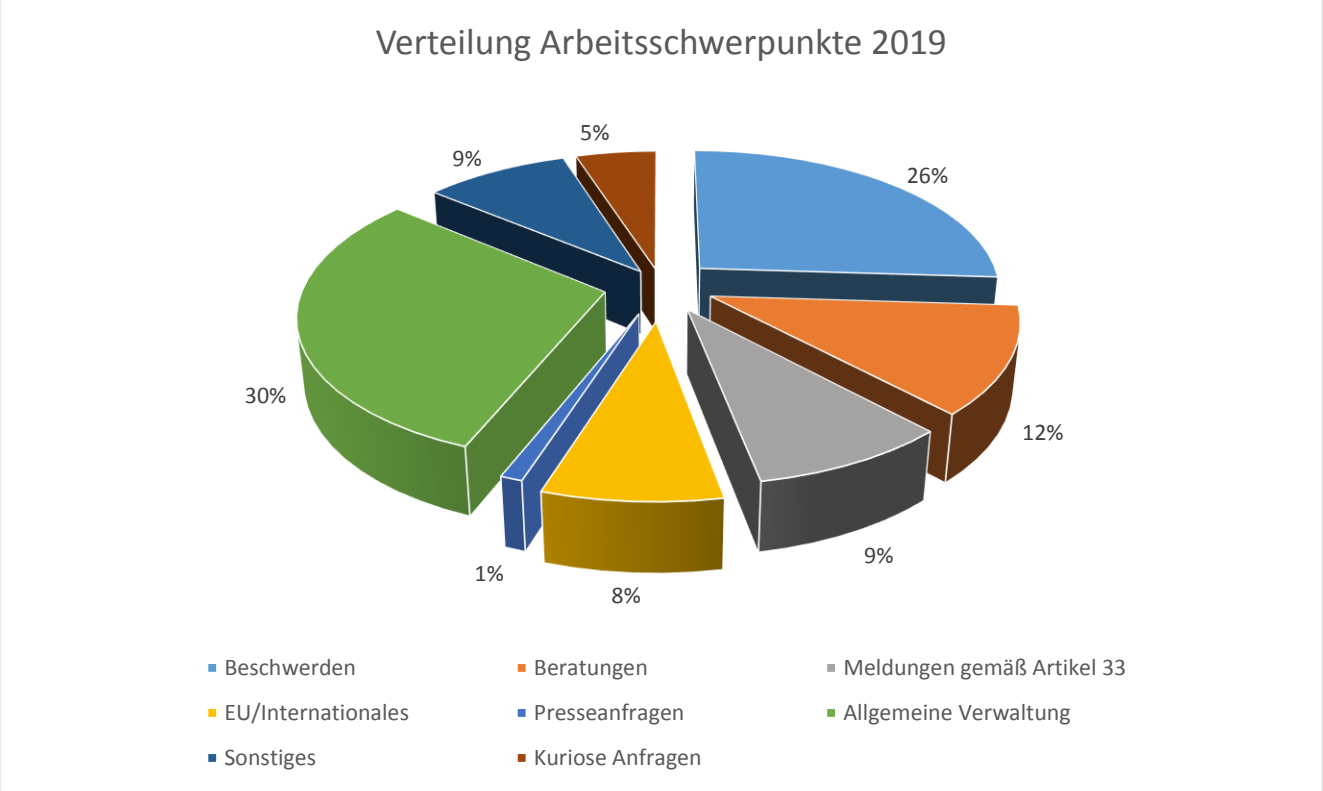
In meinem letzten Tätigkeitsbericht hatte ich bereits über kuriose Eingänge berichtet, 6.1.3 Tätigkeitsbericht 2017/2018 (Teil 2). Im neuen Berichtszeitraum erhielt ich wiederum zahlreiche Zuschriften, die ähnlich zu betrachten waren.

Im Sommer erreichte mich unter anderem eine E-Mail mit dem schlichten Wortlaut „Ich möchte kündigen“. Die E-Mail enthielt keine Zusätze, keine Anrede, keine Grußformel, keinen Namen, keine Interpunktion.

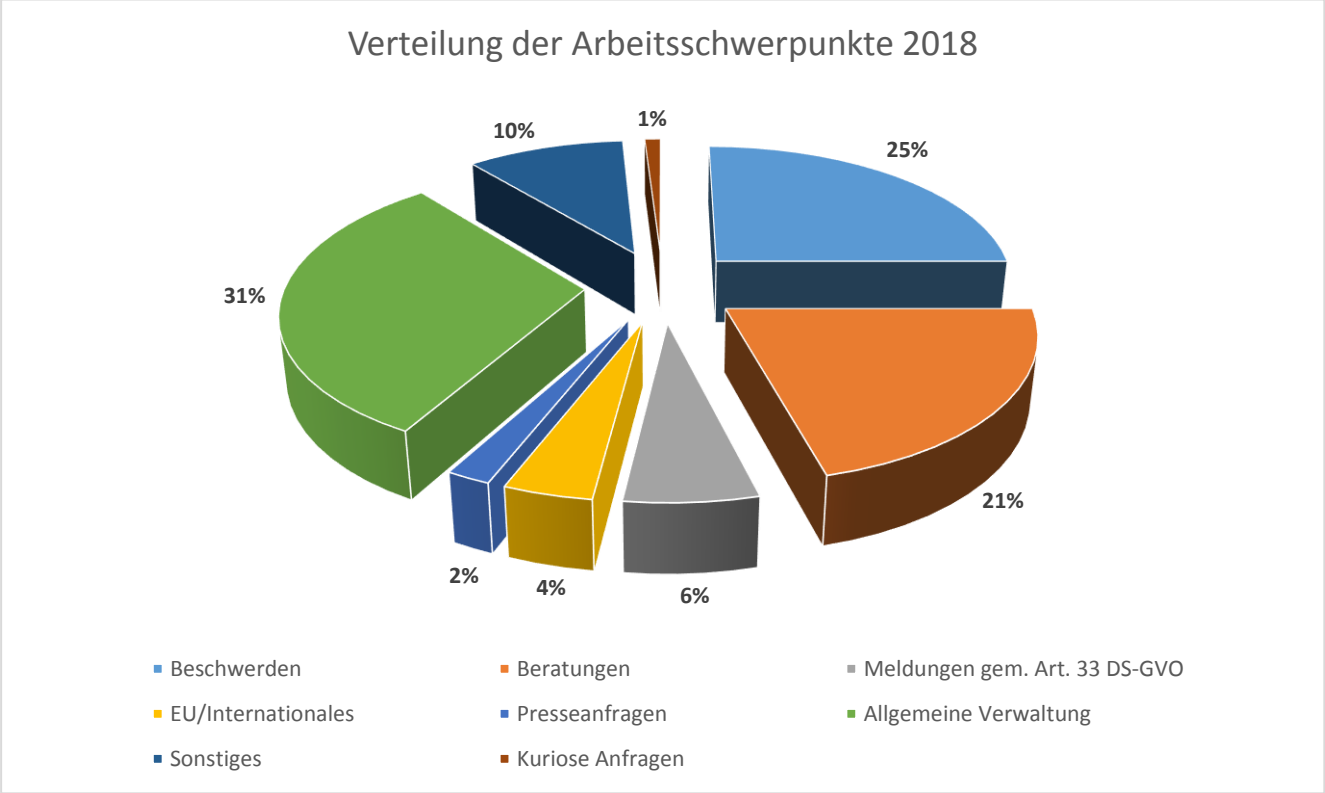
6.2 Aufgabenbearbeitung im Berichtszeitraum und Statistik

6.2.1 Überblick und Arbeitsschwerpunkte

Die Arbeitsschwerpunkte liegen auch in diesem Berichtszeitraum in der Bearbeitung der Beschwerden und Anfragen sowie die eigene Verwaltung.



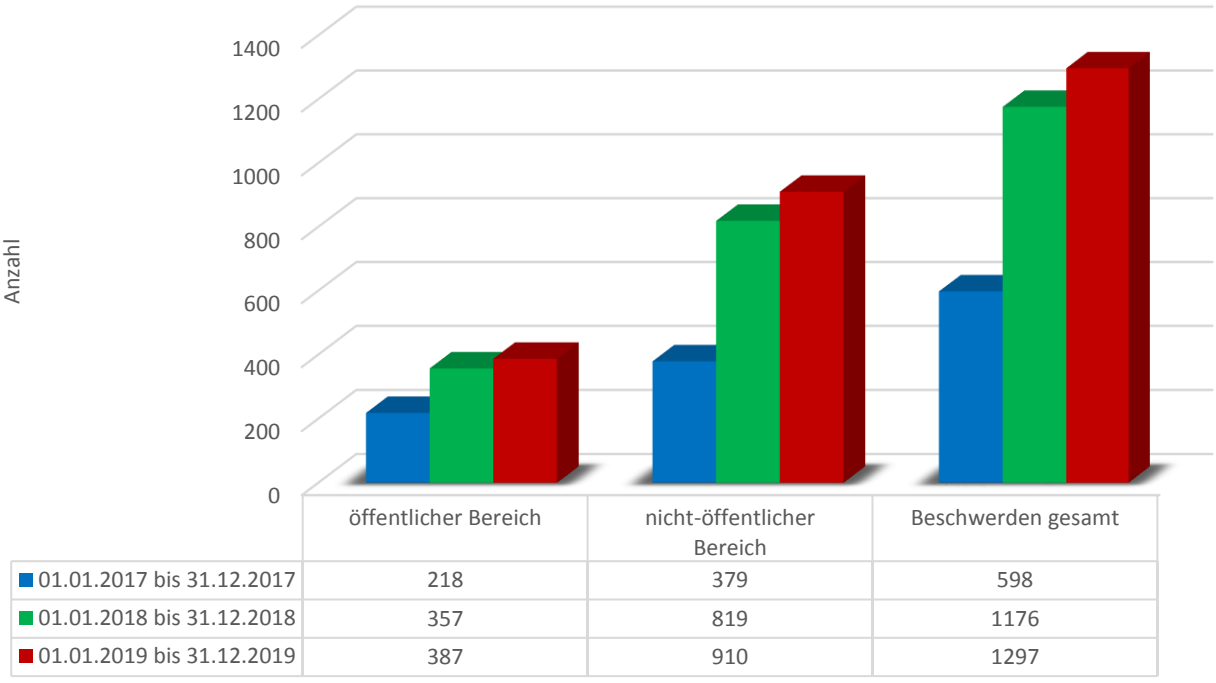
Im Vergleich zum vorherigem Berichtszeitraum ist jedoch festzustellen, dass zwar der Anteil der allgemeinen Beratungsanfragen zurückgegangen ist, jedoch der Anteil der Bearbeitungsvorgänge im Bereich EU/Internationales sich verdoppelt hat sowie der Anteil der Bearbeitungsvorgänge zu den Meldungen gemäß Artikel 33 um 67% angestiegen ist.



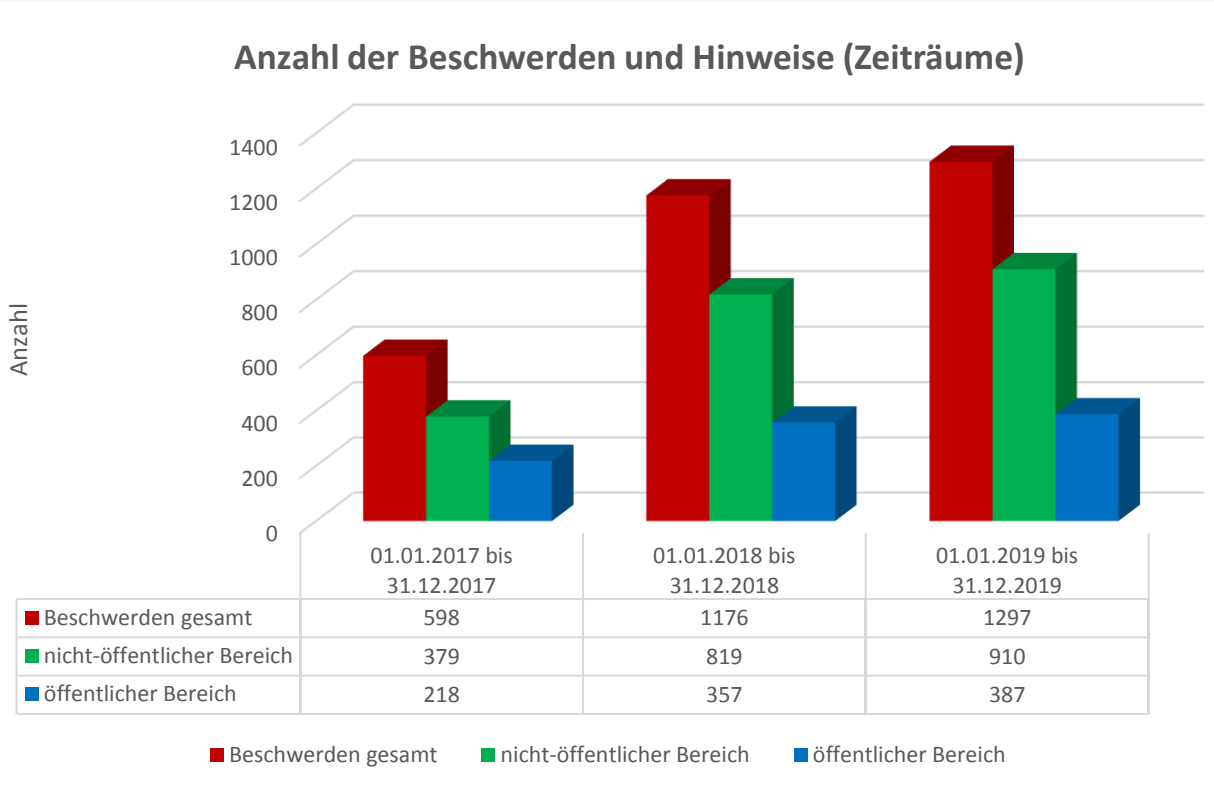
Der Anteil der kuriosen Anfragen stieg sogar um das Fünffache des vorherigen Berichtszeitraumes.

6.2.2 Petitionen, Beschwerden, Hinweise

Das Beschwerdeaufkommen stieg auch in diesem Berichtszeitraum weiter an. Die nachstehenden Diagramme stellen die Zunahme des Beschwerdeaufkommens im Berichtszeitraum im Vergleich zu den Vorjahren 2017 und 2018 dar. Es ist festzustellen, dass die Anzahl der eingegangenen Beschwerden im nicht-öffentlichen sowie im öffentlichen Teil angestiegen sind.

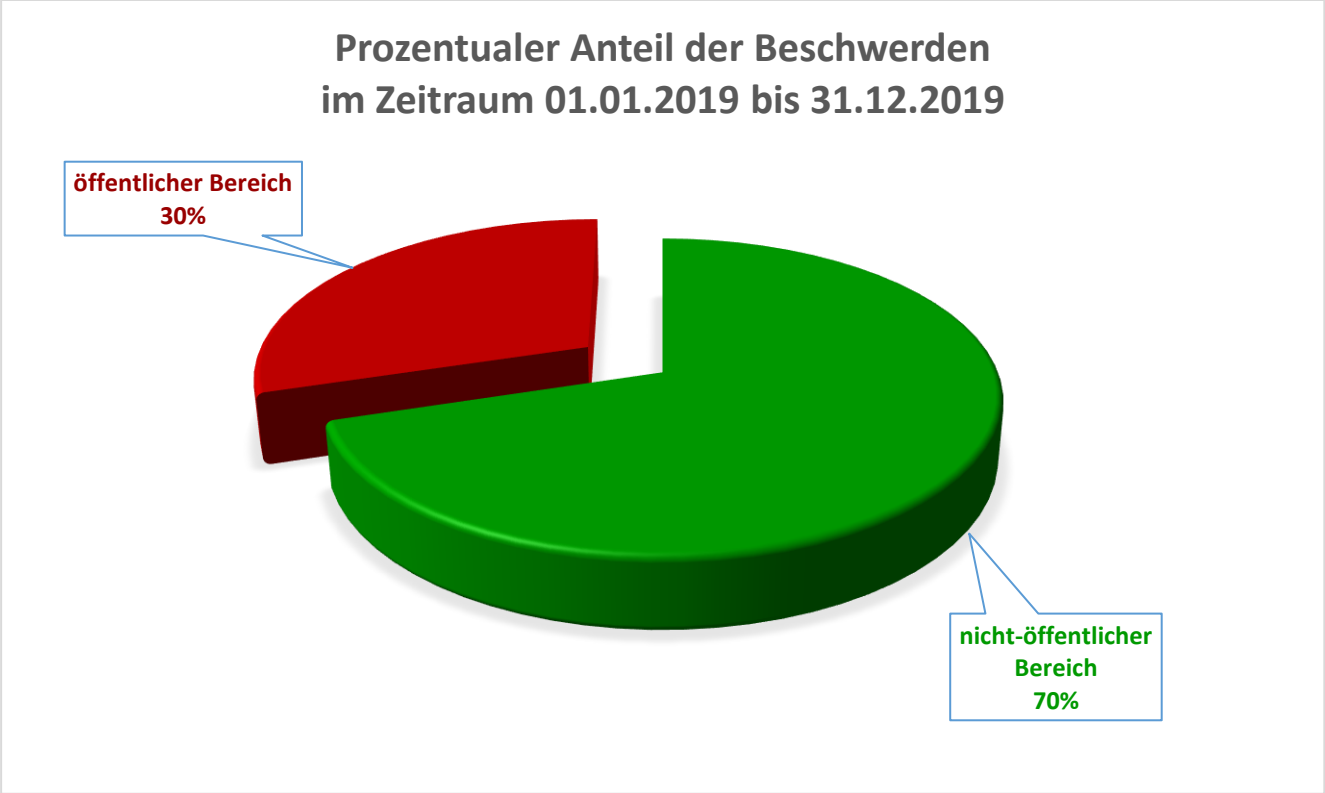


	öffentlicher Bereich	nicht-öffentlicher Bereich	Beschwerden gesamt
01.01.2017 bis 31.12.2017	218	379	598
01.01.2018 bis 31.12.2018	357	819	1176
01.01.2019 bis 31.12.2019	387	910	1297



	01.01.2017 bis 31.12.2017	01.01.2018 bis 31.12.2018	01.01.2019 bis 31.12.2019
Beschwerden gesamt	598	1176	1297
nicht-öffentlicher Bereich	379	819	910
öffentlicher Bereich	218	357	387

Es ist festzustellen, dass die Anzahl der eingegangenen Beschwerden im nicht-öffentlichen sowie im öffentlichen Teil angestiegen sind. Hierbei liegt jedoch der Schwerpunkt mit 70% der eingegangen Beschwerden im nicht-öffentlichen Bereich.



6.2.2.1 Videoüberwachung von Nachbargrundstücken und öffentlichen Verkehrsflächen – Was die Aufsichtsbehörde von Beschwerdeführern erwartet

Fast schon täglich erreichen mich Eingaben und Hinweise zu vermeintlich unzulässigen Videokameras. Schwerpunkt sind dabei überwiegend Streitigkeiten unter Nachbarn und Kameras, die (auch) in den öffentlichen Raum hinein filmen. Dazu kommen zahlreiche Hinweise – auch von Ordnungsbehörden – über Kameras an unmittelbar an den öffentlichen Verkehrsraum grenzenden Gebäuden. Oftmals ist lediglich die Anschrift des betreffenden Gebäudes benannt, verbunden mit der Aufforderung, hier schnellstmöglich Abhilfe zu schaffen. Es gibt auch Petenten, die offensichtlich gezielt durch die Straßen eines Ortes streifen, um anschließend jedwede potentiell auch in den öffentlichen Raum filmende Kamera bei meiner Behörde anzuzeigen (vgl. dazu auch Teil 2 meines Tätigkeitsberichts 2018, 6.2.1.2).

Die mir zur Verfügung stehenden personellen Ressourcen erlauben es allerdings nicht, jedem Hinweis oder jeder Beschwerde adäquat und zeitnah nachzugehen, ohne dass die

jeweiligen Hinweisgeber oder Beschwerdeführer eine gewisse Mitwirkung zeigen. Aufgrund der bloßen Mitteilung, dass an einem konkret benannten Ort eine Kamera hängt, die – am besten sofort - überprüft werden müsste, kann und werde ich nicht tätig werden. Mindestens auf Nachfrage erwarte ich weitere, den Sachverhalt präzisierende Angaben, so zum Beispiel den Namen des (wahrscheinlichen) Verantwortlichen und auch Fotos, aus denen die Installationsorte sowie die möglichen Erfassungsbereiche der monierten Kameras hervorgehen.

Darüber hinaus ist – jedenfalls von Beschwerdeführern – darzulegen, weshalb sie selbst von dieser Videoüberwachung betroffen sind. Kommen sie einer diesbezüglichen Aufforderung nicht nach oder wollen sie mich ohnehin tatsächlich lediglich informieren, kann ich sie nur als Hinweisgeber betrachten und lasse dann die geschilderten Sachverhalte in meine Aufsichtstätigkeit einfließen und entscheide nach pflichtgemäßem Ermessen über die Durchführung geeigneter Aufsichtsmaßnahmen; einen Anspruch auf weitergehende Informationen haben diese Personen dabei allerdings nicht, vgl. auch 6.2.1.1 des Tätigkeitsberichts 2017/2018 Teil 2.

Zur Darlegung der eigenen Betroffenheit gehört zum einen, dass plausibel gemacht wird, dass man sich in dem angenommenen Erfassungsbereich auch selbst bewegt hat bzw. dort regelmäßig bewegen muss, und zum anderen benötigt es gewisse Anhaltspunkte, dass mit den angezeigten Videokameras auch tatsächlich öffentlich zugängliche Bereiche überwacht werden.

Artikel 77 Absatz 1 DSGVO regelt, dass jede betroffene Person das Recht auf Beschwerde bei einer Aufsichtsbehörde hat, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt.

Voraussetzung ist also des Weiteren, dass überhaupt eine Verarbeitung der Daten des Beschwerdeführers stattfindet. Dies bedeutet, dass über die bloße Existenz einer Kamera hinausgehende Anhaltspunkte für eine Überwachung bestehen müssen; die bloße Annahme oder Vermutung einer Überwachung betrachte ich als nicht ausreichend.

Denn: Allein aus der Existenz und Ausrichtung einer Kamera kann nicht notwendigerweise darauf geschlossen werden, dass überhaupt eine Überwachung stattfindet, es sich also etwa nicht nur um Attrappen handelt, bzw. falls dies der Fall ist, welche Bereiche tatsächlich überwacht werden. Es gibt heute vielfältige technische Möglichkeiten, den Erfassungsbereich einer Kamera beispielsweise durch Ausblendungen entsprechend zu

beschränken und damit Persönlichkeitsrechtsverletzungen zu vermeiden. Zur Verifizierung der eigenen datenschutzrechtlichen Betroffenheit und damit zugleich zur Feststellung, ob es sich um aktiv betriebene, auch öffentlich zugängliche Bereiche oder Nachbargrundstücke erfassende Videokameras handelt, hat der Gesetzgeber zunächst das Instrument eines Auskunftsverlangens des Betroffenen direkt gegenüber dem Verantwortlichen vorgesehen. Ich erwarte daher von Beschwerdeführern auch, dass sie sich als Erstes schriftlich an den jeweiligen Betreiber wenden und diesen unter Fristsetzung zur Erteilung einer Auskunft nach Artikel 15 DSGVO auffordern. Auf diese Weise sind sie imstande, selbständig in Erfahrung zu bringen, ob tatsächlich und gegebenenfalls welche personenbezogenen Videoaufnahmen von ihnen zu welchem Zweck wie lange gespeichert werden. Soweit der Verantwortliche einem solchen konkreten Auskunftsverlangen entgegen seiner bestehenden Pflicht nicht entspricht oder sich dabei herausstellt, dass er (wahrscheinlich) entgegen Artikel 6 DSGVO unberechtigterweise öffentlich zugängliche Bereiche oder Nachbargrundstücke videoüberwacht, sehe ich mich gehalten, entsprechend tätig zu werden.

Vergleiche im Übrigen auch Teil 2 meines Tätigkeitsberichts 2018, 6.2.2.2.

6.2.2.2 Darf die Aufsichtsbehörde Petenten über Kamerabetreiber informieren?

Die Artikel 12 bis 15 DSGVO regeln die Anforderungen an eine transparente und umfassende Information der betroffenen Person. Diese Anforderungen sind auch bei Videoüberwachungen angemessen und adressatengerecht umzusetzen.

Soweit so gut. Hält sich ein Verantwortlicher an diese Vorgaben, werden betroffene Personen beim Betreten videoüberwachter Bereiche entsprechend informiert und können ihre Rechte gegenüber dem Verantwortlichen geltend machen bzw. sich auch mit den notwendigen Angaben zum Verantwortlichen - vergleiche Beitrag 6.2.2.1 - an die Aufsichtsbehörde wenden.

Problematisch wird es allerdings dann, wenn die Ausrichtung einer Kamera lediglich vermuten lässt, dass ein konkreter Bereich videoüberwacht wird, dies aber tatsächlich nicht der Fall ist, etwa weil es sich um eine Kameraattrappe handelt oder weil Teilbereiche des Erfassungsbereiches ausgeblendet sind. Dann findet tatsächlich überhaupt keine oder eben nur keine Überwachung des vermuteten Bereiches statt. Analog zu beurteilen ist der Fall, wenn es sich um Webcam handelt, die so eingerichtet ist, dass deren Aufnahmen

keine Identifizierbarkeit von Personen ermöglichen. Die Informationspflichten des Artikel 13 DSGVO greifen dann entweder gar nicht, weil die DSGVO insgesamt nicht anwendbar ist, oder aber sie entfalten für den Bereich mit der nur vermuteten Überwachung keine Wirkung.

Ein Datenschutzverstoß ist dem Verantwortlichen dann nicht vorzuwerfen. Dies ist dann regelmäßig auch das Ergebnis meiner Überprüfung und wird dem Petenten auch so mitgeteilt. Artikel 77 Absatz 2 DSGVO spricht nur vom Ergebnis der Beschwerdebearbeitung und fordert keine tiefergehende Begründung. § 40 Absatz 3 Satz 3 BDSG sieht eine (weitergehende) Unterrichtung der betroffenen Personen nur für den Fall vor, dass tatsächlich ein Datenschutzverstoß festgestellt worden ist. Im Fall einer zulässigen Webcam ist eine kurze Begründung sicherlich unschädlich; im Fall von Attrappen ist eine diesbezügliche Information der betroffenen Personen vom Verantwortlichen aber regelmäßig nicht gewollt; im Fall einer Videoüberwachung unmittelbar an oder geringfügig über die Grundstücksgrenze hinaus zumindest fraglich.

Genau dies wirft dann aber beim Beschwerdeführer die Frage nach dem „Warum“ auf. Für ihn sind die jeweiligen Beschränkungen der Videoüberwachung weder erkenn- noch verifizierbar, zudem muss er – zugegebenermaßen – davon ausgehen, dass der Verantwortliche jederzeit auch für ihn nicht erkennbare Veränderungen am Kamerasystem vornehmen kann. Die bloße – tatsächlich momentbezogene – Feststellung der Aufsichtsbehörde, dass kein Datenschutzverstoß vorliegt, mag daher für den Beschwerdeführer unbefriedigend sein, gleichwohl sehe ich mich nicht befugt, ihm weitergehende Informationen zukommen zu lassen, da ich bei der Ausübung meiner Kontrolltätigkeit amtlichen Verschwiegenheitspflichten unterliege und im Rahmen der Beantwortung von Eingaben Geschäftsgeheimnisse der verantwortlichen Stelle nicht unbefugt offenbaren darf.

Soweit ein Beschwerdeführer also trotz der Feststellung der Aufsichtsbehörde allein aus der weiteren Existenz und Blickrichtung einer Kamera inklusive der jederzeitigen Möglichkeit einer Veränderung der Erfassungsbereiche gleichwohl einen Überwachungsdruck für sich und seine Angehörigen ableitet, bleibt ihm immer noch der Zivilrechtsweg; alternativ kann er gegen Verantwortlichen auch (regelmäßig und vorsorglich) sein Recht auf Auskunft (Artikel 15 DSGVO) geltend machen.

Nach meinen Erfahrungen werden Kameraattrappen bzw. nicht in Betrieb befindliche oder in ihrem Erfassungsbereich beschränkte Kameras durch die Zivilgerichte kaum anders

bewertet als funktionstüchtige, tatsächlich aufzeichnende Kameras. Den Betroffenen sind insoweit nach den §§ 823, 1004 BGB je nach konkreter Sachlage Entschädigungs-, Beseitigungs- oder Unterlassungsansprüche zuerkannt worden.

Voraussetzung dafür ist natürlich, dass der Beschwerdeführer auch weiß, wer der Verantwortliche ist. In den Fällen, in denen dies für betroffene Personen infolge (zulässigerweise) fehlender Informationen nach Artikel 13 DSGVO nicht ersichtlich und auch nicht ermittelbar ist, sehe ich mich gehalten, dem Beschwerdeführer jedenfalls die Kontaktdaten der für die jeweilige Kamerainstallation verantwortlichen Person mitzuteilen. Andernfalls hätte er keine Möglichkeit selbst gegen diese Personen vorzugehen. Dabei ist auch zu berücksichtigen, dass der Beschwerdeführer gem. Artikel 78 Absatz 2 DSGVO gerichtlich gegen meine Entscheidung vorgehen kann und jedenfalls auch dann Kenntnis von der verantwortlichen Person erlangen würde.

Als Beispielfälle aus meiner Aufsichtspraxis, in denen ich Beschwerdeführer über ihnen bis dahin nicht bekannte verantwortliche Personen unterrichtet habe, kann ich etwa Eigentümer von mit Außenkameras ausgerüsteten Mehrfamilienhäusern oder auch die auf dem Dach eines Mehrfamilienhauses durch einen Mieter betriebene Webcam nennen.

6.2.2.3 § 29 Absatz 3 Bundesdatenschutzgesetz – Mitwirkung betroffener Personen

Die Untersuchungsbefugnisse meiner Behörde bestehen gemäß Artikel 58 Absatz 1 Buchstaben e) und f) DSGVO gegenüber Trägern von Berufsgeheimnissen durch die Vorschrift des § 29 Absatz 3 Bundesdatenschutzgesetz nur eingeschränkt. So ist der Zugang zu allen personenbezogenen Daten und Informationen und den Geschäftsräumen einschließlich der Datenverarbeitungsanlagen und -geräte zunächst nicht möglich. Allerdings kann eine betroffene Person, die sich als Beschwerdeführer an meine Dienststelle wendet, den Berufsgeheimnisträger von seiner Geheimhaltung gegenüber meiner Behörde entbinden und so eine Aufklärung durch meine Dienststelle möglich machen.

In einem Beschwerdevorgang wandte sich der Mandant einer Anwaltskanzlei an mich und verlangte, dass meine Dienststelle gegenüber dem Anwalt tätig wird. Meine Behörde verfährt nach dem Amtsermittlungsgrundsatz, ist sachlich neutral und unparteiisch. Soweit, ein derartiger Vorgang verfolgt werden soll, bin ich daher gehalten, den Verantwortlichen, in dem Beispielsfall die namentlich zu benennende Rechtsanwaltskanzlei zunächst zu einer Stellungnahme aufzufordern. Den Beschwerdeführer hatte ich auf meine

beschränkten Befugnisse gemäß § 29 Absatz 3 Bundesdatenschutzgesetz hingewiesen und ihn aufgefordert, ausdrücklich zu erklären, dass mir Zugang zu den personenbezogenen Daten und Informationen, die den betreffenden Vorgang berühren, gewährt werden soll, was dann auch so geschah. Unabhängig davon sollten Beschwerdeführer bereits alle ihnen zugänglichen belegenden Dokumente zum Vorgang unaufgefordert einreichen.

6.2.3 Beratung

Die Anzahl der allgemeinen Beratungsanfragen war im Berichtszeitraum mit insgesamt 608 Anfragen im Vergleich zum Vorjahr rückläufig. Dies ist u. a. darauf zurückzuführen, dass seit Inkrafttreten der DSGVO eine Vielzahl von Hinweisen, Orientierungshilfen, Handlungsleitfäden, Checklisten und weiteres Informationsmaterial für Verantwortliche, Auftragsverarbeiter und für betroffene Personen in verschiedener Form und Aufbereitung zur Verfügung stehen.

6.2.3.1 Jedwede Rechtsberatung für Verantwortliche?

Zahlreiche Anfragen erreichten mich seitens Verantwortlicher – datenverarbeitender Stellen – zu Datenschutzkonzepten, dem Inhalt von vorgesehenen Formularen mit datenschutzrechtlichen Bezug, zu Vertragstexten, zu der Zulässigkeit des Einsatzes bestimmter automatisierter Verfahren bzw. Programme oder zu deren Zertifizierung.

Regelmäßig handelte es sich dabei um Anfragen zu Angelegenheiten, die nicht genehmigungsbedürftig sind. Verantwortliche haben in eigener Zuständigkeit datenschutzrelevante Rechtstexte und den Einsatz von Softwareprodukten zu prüfen bzw. den selbst benannten Datenschutzbeauftragten zu konsultieren. Eine individuelle Rechts- und informationstechnische Beratung, insbesondere großer Vereinigungen und Unternehmen kann aufgrund des immensen Geschäftsanfalls in meiner Dienststelle nicht durchgängig erfolgen. Zudem sind derartige Beratungsleistungen meiner Behörde für Verantwortliche als gesetzliche Aufgaben gemäß Artikel 57 Absatz 1 DSGVO eigentlich nicht vorgesehen. Anderes gilt für nach der DSGVO geregelte Verfahren, wie bei der Datenschutz-Folgenabschätzung, Artikel 35, 36 DSGVO. Dennoch: Bei Fragen grundsätzlicher Bedeutung versuchen die Bediensteten meiner Behörde gleichwohl ein Lösungskonzept zu entwerfen. Auch werden kleine und ohne *Know-how* ausgestattete Verantwortliche seitens meiner Dienststelle nach Möglichkeit mit Hinweisen und Hilfestellungen betreut.

6.2.4 Prüfungen - Rechtsetzung, Verwaltungsvorschriften (§ 20 SächsDSDG)

Im Berichtszeitraum sind nach Wirksamwerden der DSGVO keine aus Datenschutzsicht Berichtens werten Normsetzungsvorhaben zu verzeichnen gewesen (für den Geltungsbereich der Richtlinie (EU) 2016/680 s. u. 8.2 und 8.4).

6.2.5 Register der benannten Datenschutzbeauftragten

Im Berichtszeitraum 2019 gingen 1.116 Meldungen zu benannten Datenschutzbeauftragten beim Sächsischen Datenschutzbeauftragten ein. Diese Meldungen umfassten Mitteilungen zur Benennung von behördlichen und betrieblichen Datenschutzbeauftragten, zu Änderungen oder zur Beendigung dieser Funktion.

Die DSGVO sieht gemäß Artikel 37 Absatz 1 DSGVO für den Verantwortlichen (öffentliche Stellen generell; nicht öffentliche Stellen unter bestimmten Bedingungen) die Pflicht vor, einen Datenschutzbeauftragten zu benennen. Nach Artikel 37 Absatz 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.

Zur Erfüllung der Meldepflicht stellt der Sächsische Datenschutzbeauftragte einen Online-Formular-Service bereit. Mittels dieses Dienstes ist es dem Verantwortlichen möglich, die Meldung einfach und bequem direkt online durchzuführen. Die meldepflichtige Stelle erhält bei der Nutzung des Online-Formular-Service eine Kopie der Meldung als PDF-Dokument per Email an die angegebene Email-Adresse. Von dem angebotenen Online-Dienst wurde im Berichtszeitraum 660-mal Gebrauch gemacht.

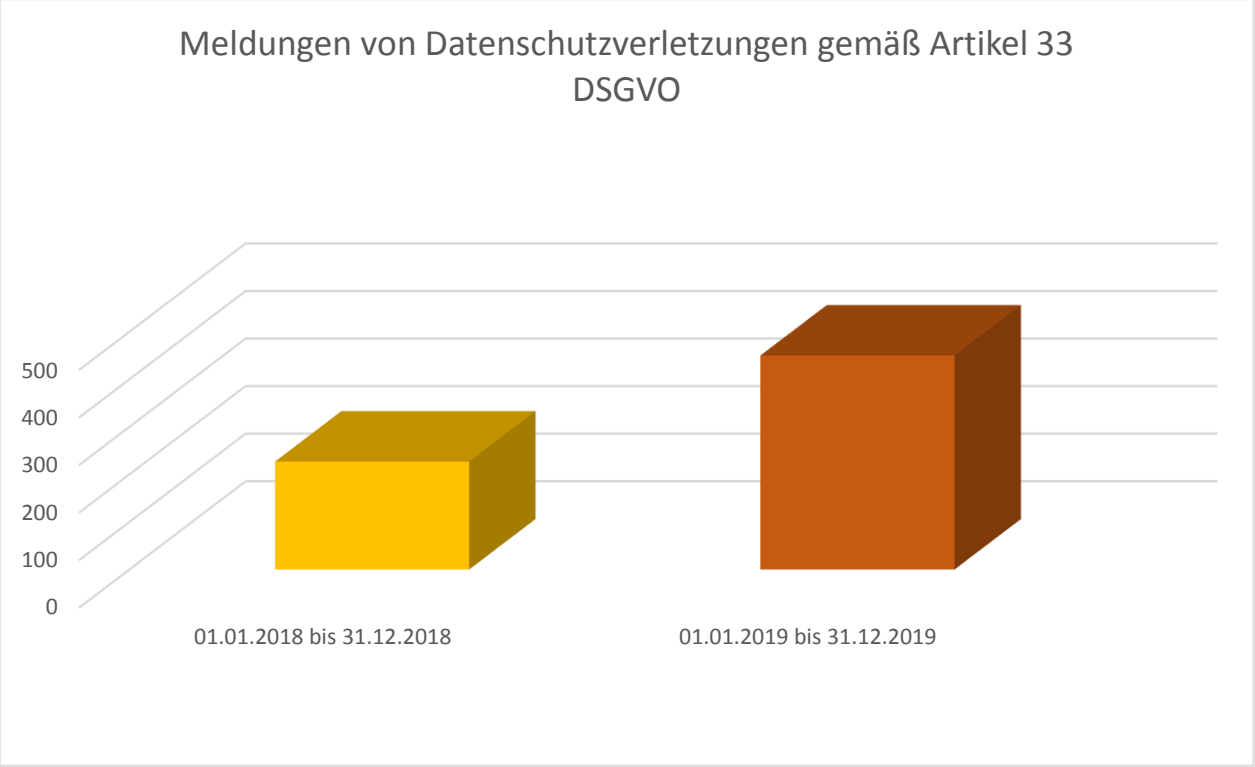
Bei postalischen Meldungen und Meldungen per E-Mail oder Fax gemäß Artikel 37 Absatz 7 DSGVO erhält die meldepflichtige Stelle wegen des hohen Verwaltungsaufwandes keine Eingangsbestätigung. In dieser Form sind 456 Meldungen nach Artikel 37 Absatz 7 DSGVO eingegangen. Viele meldepflichtige Stellen übersandten unvollständig ausgefüllte oder nicht lesbare Mitteilungen. Die Aufarbeitung dieser Unterlagen ist zeitaufwändig und ressourcenintensiv.

Die übersandten Mitteilungen werden von den Fachreferaten meiner Behörde u. a. genutzt, um die Erfüllung der Meldepflicht gem. Artikel 37 Absatz 7 DSGVO oder ein

mögliches Vorliegen von Interessenskonflikten gem. Artikel 38 Absatz 6 DSGVO zu prüfen.

6.2.6 Meldungen gemäß Artikel 33 DSGVO, Konsultationen – Artikel 36 DSGVO

Im Berichtszeitraum gingen 450 Meldungen zu Verletzungen des Schutzes personenbezogener Daten gemäß Artikel 33 DSGVO ein. Dies waren 223 mehr Meldungen als im Jahr 2018.



Folgende Fallgruppen sind im Berichtszeitraum besonders häufig gemeldet worden:

- Fehlversand
- Einbruch und Diebstahl
- Allgemein der Verlust von Unterlagen und Datenträgern sowie speziell der Verlust auf dem Postweg
- Offene E-Mailverteiler
- Cyberkriminalität
- Fehlerhafte interne Speicherung und Zugriffsberechtigung

(siehe auch Abschnitt 4.6.1).

6.3 Datenschutzaufsichtliche Befugnisse, verwaltungsrechtliche Entscheidungen

6.3.1 Überblick zum Berichtszeitraum

Auch im letzten Berichtszeitraum blieben die verwaltungsrechtlichen Entscheidungen, was die Fallmengen anbelangt, noch relativ gering, vergleiche auch den Tätigkeitsbericht 2017/2017 Teil 2, 6.3.1. Meine Behörde erreicht eine gewünschte Handlung bei den Verantwortlichen bereits mit formlosen Aufforderungen etwa zur Auskunft zur durchgeführten Datenverarbeitung oder zur Beendigung bzw. Einstellung von Datenverarbeitungsprozessen. Durchgeführte Anordnungen betreffen auch Fälle unzulässiger Videografie. Zu Rechtsfragen im Zusammenhang mit Anordnungen vergleiche auch die Darstellung der Rechtsprechung unter 9.4 und 9.9.

6.3.2 Akteneinsicht im Aufsichtsverfahren

Wenn ich mich im Rahmen der Anlassaufsicht an Verantwortliche wende und diese sich daraufhin eines Rechtsbeistandes bedienen, erreichen mich oft statt der geforderten Stellungnahmen zunächst Akteneinsichtsgesuche.

Der dahinter stehende Zweck liegt auf der Hand: Der Verantwortliche möchte zunächst Klarheit darüber gewinnen, wer ihn bei der Datenschutzaufsichtsbehörde angezeigt hat und welche Vorwürfe im Konkreten erhoben worden sind. Insbesondere bei Eingaben im Bereich des Arbeitnehmerdatenschutzes ist dies natürlich äußerst kritisch zu sehen. Grundsätzlich zu unterscheiden sind zunächst Eingaben zu individuellen einzelfallbezogenen Sachverhalten und Eingaben zu Sachverhalten mit mehreren betroffenen Personen. Im erstgenannten Fall ist der Sachverhalt regelmäßig nur unter Offenlegung der Identität des Petenten zu klären, so dass insoweit eine Akteneinsicht zunächst unkritisch ist. Zumeist hat sich der Petent in solchen Fällen ohnehin bereits (erfolglos) an den Verantwortlichen gewandt. Werden in einer Eingabe jedoch für eine Mehrzahl betroffener Personen relevante Sachverhalte thematisiert, ist es weder erforderlich noch angezeigt, den jeweiligen Petenten konkret zu benennen. Ich sichere den Petenten daher bei der Behandlung ihrer Eingabe in diesen Fällen immer auch die vertrauliche Behandlung ihrer Identität zu, denn für die Sachverhaltsaufklärung und die rechtliche Bewertung ist es eben nicht relevant, wer sich damit an die Datenschutzaufsichtsbehörde gewandt hat, sondern es geht ausschließlich um den objektiven Sachverhalt. Lediglich dann, wenn im Verlauf des Auf-

sichtsverfahrens offenkundig wird, dass sich ein Petent wider besseren Wissens nur deshalb (mit unzutreffenden Behauptungen) an mich gewandt hat, um den Verantwortlichen zu schaden, kommt im Ausnahmefall auch eine Offenlegung seiner Identität gegenüber dem Verantwortlichen in Betracht.

Unter welchen Voraussetzungen überhaupt ein Anspruch auf Akteneinsicht besteht, ist derzeit noch nicht vollumfänglich geklärt. Dabei wird insbesondere die Anwendbarkeit des Verwaltungsverfahrensrechts noch sehr unterschiedlich beurteilt:

Nach § 9 VwVfG ist ein Verwaltungsverfahren die nach außen wirkende Tätigkeit der Behörden, die auf die Prüfung der Voraussetzungen, die Vorbereitung und den Erlass u. a. eines Verwaltungsaktes gerichtet ist. Dies schließt den Erlass des Verwaltungsaktes ein.

Unstreitig dürfte also dann ein Verwaltungsverfahren vorliegen, wenn die Aufsichtsbehörde den Erlass eines Verwaltungsaktes bereits vorbereitet oder dies zumindest beabsichtigt. Dies ist jedenfalls immer dann der Fall, wenn die Aufsichtsbehörde förmlich von den ihren nach Artikel 58 DSGVO zustehenden Befugnissen Gebrauch macht, also beispielsweise Heranziehungsbescheide zur Auskunftserteilung oder Anordnungen erlässt oder vorbereitet. Bereits gerichtlich festgestellt worden ist (Verwaltungsgericht Dresden, Urteil vom 17.10.2018, 6 K 381/16, vgl. dazu auch TB 2018, Punkt 9.7 Fall c), dass bloße formlose Schreiben der Aufsichtsbehörde zur Auskunftserteilung mangels einer Bezeichnung als Bescheid sowie fehlender Rechtsbehelfsbelehrung, Anhörung und Zwangsgeldandrohung jedenfalls kein Verwaltungsakt sind. Andererseits ist inzwischen aber auch klar, dass Verwarnungen nach Artikel 58 Absatz 2 Buchstabe b) DSGVO einen (feststellenden) Verwaltungsakt darstellen (Verwaltungsgericht Hannover, Urteil vom 27.11.2019, 10 A 820/19, Randziffer 19, in: juris).

Zu Beginn eines auf einer Eingabe beruhenden Aufsichtsverfahrens ist aber regelmäßig noch nicht absehbar, ob es zu solchen förmlichen Maßnahmen der Aufsichtsbehörde überhaupt kommt und damit auch § 29 VwVfG (Akteneinsicht durch Beteiligte) anwendbar ist. Zunächst gehe ich regelmäßig davon aus, dass es sich zum einen um einen datenschutzaufsichtlichen, zum anderen aber auch um einen petitionsrechtlichen Vorgang handelt, in dem es formal keinen Anspruch auf eine Akteneinsicht gibt. Gleichwohl bin ich mir natürlich bewusst, dass die Übergänge fließend sind und auch Verantwortliche einen Anspruch auf ein transparentes Verfahren haben. Ich entscheide daher in solchen Fällen

einzelfallbezogen, ob und welche Teile der Eingabe oder des Hinweises – nur darauf kommt es den Verantwortlichen regelmäßig an – ich den Verantwortlichen in welcher Weise – in der Regel als Kopie oder Ausdruck aus meinem Vorgangsverwaltungssystem – zugänglich mache. Den schutzwürdigen Interessen der (redlichen) Petenten und Hinweisgeber trage ich dabei dadurch Rechnung, dass ich

- alle Angaben, die deren Identifizierung ermöglichen könnten, entsprechend schwärze und

- falls erforderlich, auch Abschriften anfertige.

Letzteres ist insbesondere dann relevant, wenn es sich um handschriftliche Eingaben handelt und die Gefahr besteht, dass der Verantwortliche den Petenten an der Handschrift erkennen könnte. Beispielsweise bei Eingaben von Arbeitnehmern dürfte ein solches Risiko nicht als fernliegend zu betrachten sein.

Die geschilderte Verfahrensweise (Schwärzungen) ist selbst dann noch praktikabel und gerechtfertigt, wenn der Aufsichtsvorgang schon als Verwaltungsverfahren zu qualifizieren ist. § 29 Absatz 1 VwVfG regelt, dass die Behörde den Beteiligten Einsicht in die das Verfahren betreffenden Akten (nur) zu gestatten hat, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Weiter heißt es in § 29 Absatz 2 VwVfG, dass die Behörde zur Gestattung der Akteneinsicht nicht verpflichtet ist, soweit die Vorgänge nach einem Gesetz oder ihrem Wesen nach, namentlich wegen der berechtigten Interessen der Beteiligten oder dritter Personen, geheim gehalten werden müssen. Einer vollständigen Akteneinsicht (ohne Schwärzungen) steht also sowohl entgegen, dass es für die Verteidigung der rechtlichen Interessen des Verantwortlichen allein auf die Kenntnis des objektiven Sachverhalts ankommt, es also ohne Belang ist, wer sich damit an die Aufsichtsbehörde gewandt hat, als auch, dass dies ein Erfordernis der Wahrung der schutzwürdigen Interessen des Petenten oder Hinweisgebers ist, denn es steht durchaus zu befürchten, dass dieser wegen der Eingabe persönliche Nachteile erleidet, wenn sein Arbeitgeber oder auch ein anderer Verantwortlicher davon Kenntnis erlangt.

Dies habe ich im Übrigen auch schon bei der Vorlage von Akten an das Verwaltungsgericht so praktiziert, indem ich in den vorgelegten Originalakten im Hinblick auf die zu erwartenden Akteneinsichtsanträge der Prozessgegner einzelne Blätter aus Gründen des

Informantenschutzes durch teilgeschwärzte Kopien ersetzt hatte. Die Schwärzungen betrafen ausschließlich Angaben zur Identität des Petenten, mithin also personenbezogene Daten, die ihrem Wesen nach geheim gehalten werden müssen (§ 99 Absatz 1 Satz 2 VwGO), vgl. dazu auch den Beschluss des Bundesverwaltungsgerichts vom 3. August 2011, 20 F 23/10 (in: juris).

Bestehen Verantwortliche bzw. ihre Rechtsbeistände darauf, unbeschadet meiner vorstehenden Ausführungen die gesamte Aufsichtsakte (also nicht nur die Eingabe als solche) einzusehen, müssen sie meine Dienststelle aufsuchen. § 29 Absatz 3 VwVfG regelt, dass die Akteneinsicht bei der Behörde erfolgt, die die Akten führt. Eine Übersendung der Originalakte ist meinerseits nicht vorgesehen. Für eine Kopie der Originalakte, bei der auf den Petenten bzw. Hinweisgeber hinweisende Angaben wie beschrieben geschwärzt würden, werden Verwaltungskosten erhoben.

6.4 Geldbußen und Sanktionen, Strafanträge

6.4.1 Ordnungswidrigkeitenverfahren im nicht-öffentlichen Bereich

Im Berichtszeitraum habe ich 82 Ordnungswidrigkeitenanzeigen Dritter sowie 3 Anzeigen aus dem Aufsichtsbereich meiner Behörde erhalten. Von den 82 Anzeigen Dritter haben sich allein 38 auf den Einsatz von Dashcams, weitere 13 auf sonstige Videoüberwachungsfälle bezogen. Der Schwerpunkt (60 %) bei den Ordnungswidrigkeitenanzeigen lag also ganz klar bei der Videoüberwachung.

Insgesamt waren damit 133 Ordnungswidrigkeitenverfahren bei mir anhängig. Davon konnte ich 33 Fälle im Berichtszeitraum abschließen. Dabei habe ich 12 Bußgelder festgesetzt:

- ein Bußgeld in Höhe von 500 € wegen Verstoßes gegen die Auskunftspflicht gegenüber einer betroffenen Person (Artikel 15 DSGVO)

- 11 Bußgelder zwischen 50 und 800 € wegen unrechtmäßigen Betriebs einer Dashcam (Artikel 6 DSGVO [8 Bußgelder] bzw. § 43 BDSG [Altfälle – 3 Bußgelder])

In meinem 8. Tätigkeitsbericht zum nicht-öffentlichen Bereich hatte ich mich in Punkt 13.2 bereits ausführlich zur Wahrnehmung besonderer Ermittlungsbefugnisse geäußert.

Dort habe ich klargestellt, dass dabei auch Durchsuchungen als mögliche Ermittlungsmaßnahmen in Betracht kommen, ich davon aber – gerade bei Privatpersonen – nur sehr zurückhaltend Gebrauch mache.

Im Jahr 2019 habe ich in einem Fall beim Amtsgericht einen Durchsuchungsbeschluss beantragt und auch erhalten. Zu dem Betroffenen waren bei mir über einen längeren Zeitraum immer wieder amtliche Anzeigen von Polizeidienststellen eingegangen, die mit der Bearbeitung von durch den Betroffenen erstatteten Anzeigen wegen vermeintlicher Verkehrsordnungswidrigkeiten befasst waren. Der Betroffene hatte seinen Anzeigen regelmäßig Fotos oder Videosequenzen einer durch ihn in einem dienstlich genutzten Fahrzeug betriebenen Dashcam beigefügt. Die Polizeibeamten wiederum hatten die Akten nach Bearbeitung des Verkehrsordnungswidrigkeitenvorwurfs an mich mit einer Anzeige wegen Datenschutzverstoßes weitergereicht.

Gegenüber der Polizei hatte der Betroffene angegeben, dass er jedenfalls die seinen Anzeigen beigefügten Videodateien auf dem heimischen Rechner nachbearbeitet, d. h. auch dort gespeichert haben muss. Zudem hatte er den Polizeibeamten auch diesbezügliche Videosequenzen auf seinem Mobiltelefon gezeigt. Der offensichtliche Zweck des Dashcambetriebs, Verkehrsverstöße Dritter zu dokumentieren und zur Anzeige zu bringen, legte den Verdacht nahe, dass der Betroffene mindestens eine Kamera permanent im Einsatz hat und damit – anlassfrei – jedwede Verkehrs- bzw. Personenbewegungen im unmittelbaren Umfeld seiner Fahrwege erfasst, daraus potentielle Verkehrsverstöße ermittelt, die Aufzeichnungen gezielt auf seinem PC nachbearbeitet, auch auf seinem Mobiltelefon vorhält und anschließend für seine Anzeigen verwendet. Dies stellt einen erheblichen Verstoß gegen Artikel 6 Absatz 1 Buchstabe f) DSGVO dar. Erschwerend kam hinzu, dass der Betroffene sich, nachdem seine Dashcam im Rahmen einer polizeilichen Kontrolle für eine datenschutzrechtliche Ordnungswidrigkeitenanzeige sichergestellt worden war, umgehend eine neue Dashcam besorgt und diese danach wieder in seinem Fahrzeug betrieben hatte.

Um den tatsächlichen Umfang der Verarbeitung personenbezogener Daten zu beurteilen und zu bewerten, insbesondere auch im Hinblick auf Datenumfang, Aufzeichnungsinhalte, eventuelle Tonaufnahmen sowie Speicherdauer, und diesbezügliche Beweismittel sicherstellen, war die Beantragung eines Durchsuchungs- und Beschlagnahmebeschlusses beim zuständigen Ermittlungsrichter notwendig.

Die eigentliche, sich auf die Wohnung und das vom Betroffenen (dienstlich) genutzte Fahrzeug erstreckende Durchsuchung habe ich mit Unterstützung der örtlichen Polizei durchgeführt. Die Auswertung der beschlagnahmten IT-Technik (Laptop, Mobiltelefon, Dashcam, Speichermedien) war zum Ende des Berichtszeitraums noch nicht abgeschlossen.

6.4.2 Ordnungswidrigkeitenverfahren im öffentlichen Bereich

Der Sächsische Datenschutzbeauftragte war im Berichtszeitraum im öffentlichen Bereich zuständig für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach

- § 38 Sächsisches Datenschutzgesetz (§ 38 Absatz 3 Satz 1 SächsDSG),

- Artikel 83 DSGVO (Artikel 58 Absatz 2 Buchstabe i) DSGVO, § 14 Absatz 1 SächsDSDG),

- § 22 Absatz 1 Sächsisches Datenschutzdurchführungsgesetz (§ 22 Absatz 3 SächsDSDG) und

- § 85a des Zehnten Buches Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – i. V. m. § 41 Bundesdatenschutzgesetz, Artikel 83 Absatz 5 DSGVO (Artikel 58 Absatz 2 Buchstabe i) DSGVO, § 14 Absatz 1 SächsDSDG).

Im Berichtszeitraum waren im öffentlichen Bereich insgesamt 75 Bußgeldverfahren anhängig. Davon wurden 7 mit einem Bußgeld abgeschlossen, welche allesamt Rechtskraft erlangten. Weitere 15 Bußgeldverfahren wurden eingestellt bzw. ist von der Verfolgung abgesehen worden. 53 Verfahren befanden sich zum Ende des Berichtszeitraumes noch in Bearbeitung.

Berichtszeitraum		**01.01. – 31.12.2019**
anhängig gesamt		**75**
davon	Verfahren aus vorherigem Berichtszeitraum	38
	neu eingegangene Verfahren	37
abgeschlossen		
davon	mit Bußgeld	7
	mit Verwarnungsgeld	0
	eingestellt/von Verfolgung abgesehen	15
noch in Bearbeitung		53
Summe rechtskräftige Bußgelder/Verwarnungsgelder in €		**5.950**

Gegenüber dem vergangenen Berichtszeitraum ist die Anzahl der eingegangenen und zu bearbeitenden Ordnungswidrigkeitenverfahren angestiegen. Bei einer Hochrechnung auf den bisher üblichen Zweijahreszeitraum ergibt sich jedoch im Vergleich mit den vergangenen Berichtszeiträumen ein gleichbleibendes (hohes) Aufkommen von Ordnungswidrigkeitenverfahren im öffentlichen Bereich. Die Summe der rechtskräftigen Buß- und Verwarngelder belief sich auf 5.950 Euro.

Sowohl der personelle Engpass als auch der stetig steigende Bearbeitungsaufwand im Bereich der Ordnungswidrigkeiten wirken sich auch weiterhin negativ auf die Dauer der Verfahren aus. Es konnten im Vergleich zu vergangenen Berichtszeiträumen weniger Verfahren abgeschlossen werden, was wiederum zu einer niedrigeren Summe der festgesetzten Geldbußen führte.

Bei den im Berichtszeitraum mit einem Bußgeld abgeschlossenen Verfahren handelt es sich ausschließlich um Verstöße von Polizeivollzugsbediensteten, für welche weiterhin das Sächsische Datenschutzgesetz anzuwenden war. Bußgelder nach DSGVO sind im Berichtszeitraum im öffentlichen Bereich nicht erlassen worden.

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

- Vorgänge, die in den Anwendungsbereich der DSGVO fallen – Verstöße nach Artikel 83 Absatz 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 Absatz 4 bis 6 DSGVO:

Besondere Schwierigkeiten bestanden 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.

Für Verstöße nach Artikel 83 Absatz 4 bis 6 DSGVO und das Verfahren wegen solcher gilt, auch im öffentlichen Bereich, nach § 41 BDSG das Ordnungswidrigkeitengesetz (OWiG). Bei der Bearbeitung von Ordnungswidrigkeitenverfahren, bei denen der *Tatzeitpunkt vor dem 25.05.2018* liegt, ist demnach § 4 Absatz 3 OWiG zu beachten (bei noch nicht beendeten Dauerverstößen § 4 Absatz 2 OWiG). § 4 Absatz 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 die bisher geltenden nationalen Ordnungswidrigkeiten-Normen oder die DSGVO anzuwenden war.

Für diese Fälle stellten die bisher geltenden nationalen Ordnungswidrigkeiten-Normen regelmäßig das jeweils mildere Gesetz dar. Dafür sprach insbesondere der geringere Bußgeldrahmen (§ 38 Absatz 2 SächsDSG mit bis zu 25.000 EUR, § 85 Absatz 3 SGB X a. F. 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

Im Berichtszeitraum galt gemäß § 2 Absatz 1 SächsDSG a. F. das Sächsische Datenschutzgesetz weiterhin für die Verarbeitung personenbezogener Daten durch Behörden

und sonstige öffentliche Stellen des Freistaates Sachsen, Gemeinden und Landkreise sowie sonstige der Aufsicht des Freistaates Sachsen unterstehenden juristischen Personen des öffentlichen Rechts, soweit diese innerhalb des Anwendungsbereichs nach Artikel 2 Absatz 1 und 2 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016,S. 89) tätig werden, (öffentliche Stellen).

Für die am häufigsten im öffentlichen Bereich vorkommende Ordnungswidrigkeit – unbefugte Verarbeitung von personenbezogenen Daten bzw. unbefugter Abruf personenbezogener Daten aus den polizeilichen Auskunfts- bzw. Informationssystemen durch Polizeivollzugsbedienstete – galt demnach im Berichtszeitraum das Sächsische Datenschutzgesetz weiter.

In ca. 77 % der Ordnungswidrigkeitenverfahren standen/stehen Bedienstete der sächsischen Polizei in Verdacht, unbefugt personenbezogenen Daten verarbeitet und/oder aus den polizeilichen Auskunfts- bzw. Informationssystemen abgerufen zu haben. Regelmäßig handelt es sich dabei 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 insbesondere aus dem überdurchschnittlichen Anzeigeverhalten der Polizeidienststellen, welche ein datenschutzrechtliches Fehlverhalten ihrer Bediensteten konsequent verfolgen.

Des Weiteren bestand/besteht ebenfalls gegen Bedienstete unterschiedlichster sächsischer Behörden der Verdacht, nicht offenkundige personenbezogene Daten unbefugt verarbeitet zu haben.

Die anhaltend große Anzahl an Ordnungswidrigkeitenverfahren gegen sächsische Polizeibedienstete zeigt, dass trotz einer intensiven Belehrung der Polizeidienststellen über den Datenschutz weiterhin Unklarheiten im Zusammenhang mit der Nutzung polizeilicher Datenbanken bestehen.

Insbesondere hinsichtlich Recherchen, die Polizeibedienstete in polizeilichen Dateien ohne dienstlichen Anlass zur eigenen Person (bzw. zu gegen sie gerichteten Verfahren) durchführen, bestehen nach wie vor erhebliche Unsicherheiten. Auch solche „Eigenrecherchen“ stellen regelmäßig eine Ordnungswidrigkeit dar. Hintergrund ist der Umstand, dass der Bedienstete auch in dieser Konstellation unbefugt nicht offenkundige Daten abruft (auf das Eigeninteresse oder eine Art „naturgemäße“ Einwilligung kommt es nicht an, vgl. OLG Bamberg, Beschluss vom 27.04.2010, Aktenzeichen 2 Ss 531/10) und sich in den zum Vorgang gespeicherten Unterlagen in aller Regel Daten zu Dritten finden (Anzeigeerstatter, Verdächtige, Geschädigte, Zeugen etc.). Diese Gedanken lagen auch der Entscheidung des AG Borna zugrunde, das bei einer Eigenrecherche den Tatbestand einer datenschutzrechtlichen Ordnungswidrigkeit nach § 38 Absatz 1 Nummer 1 Buchstabe c) SächsDSG als erfüllt ansah und einen Polizeibeamten 2017 entsprechend verurteilt hat (vgl. 19. Tätigkeitsbericht, 1.5).

Der einzig gesetzkonforme Weg für den Beschuldigten, über ein laufendes Verfahren Auskunft bzw. Einsicht in die Unterlagen zu erhalten, ist und bleibt im Ermittlungsverfahren derjenige über § 147 StPO. Die Staatsanwaltschaft ist dabei die für die Entscheidung über den Umfang der Auskunft entscheidende Stelle. Der (beschuldigte) Polizeibedienstete ist insoweit ein ganz „normaler“ Verfahrensbeteiligter. Über die zu seiner Person gespeicherten Daten – unabhängig von eventuell laufenden Verfahren – erhält er nach § 92 Sächsisches Polizeivollzugsdienstgesetz (SächsPVDG) und § 57 BDSG Auskunft.

Auch nach Inkrafttreten des Sächsischen Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 (Sächsisches Datenschutz-Umsetzungsgesetz – SächsDSUG) zum 01.01.2020 bleiben unbefugte Abrufe nicht offenkundiger Daten (zur eigenen Person oder zu Dritten) durch Polizeibedienstete nach § 48 Absatz 1 Nummer 1 SächsDSUG bußgeldbewehrt.

Die Bediensteten der Behörden und öffentlichen Stellen in Sachsen sind auch zukünftig zu ihrer besonderen Pflichtenwahrung und Vorbildwirkung zu ermahnen. Die Ahndung von Ordnungswidrigkeiten im öffentlichen Bereich ist daher nach wie vor unabdingbar.

6.5 Öffentlichkeitsarbeit, Internetauftritt und Presse

Es ist vorgesehen den Internetauftritt meiner Behörde neu zu konzeptionieren und zu gestalten. Aufgrund der nach dem Berichtszeitraum im Kalenderjahr 2020 erfolgten pandemiebedingten Einschränkungen konnte das Vorhaben noch nicht abgeschlossen werden.

Im Berichtszeitraum erreichten mich auch wieder vielfältige Presseanfragen. Hierbei war festzustellen, dass die Fachpresse durchaus gehäuft an meine Dienststelle herangetreten ist. Nicht nur deshalb waren die Presseauskunftsanfragen fachlich spezifischer und zum Teil aufwendiger zu bearbeiten. Zu beobachten war auch, dass Pressevertreter an sämtliche Datenschutzaufsichtsbehörden, den Bundesbeauftragten für Datenschutz und Informationsfreiheit und die Landesdatenschutzbeauftragten der anderen Bundesländer herantraten. Ich bitte Pressevertreter auch kenntlich zu machen, dass sämtliche Aufsichtsbehörden angefragt worden sind. Die Beantwortung entsprechender Anfragen wird üblicherweise von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder bzw. den zuständigen Arbeitskreisen der Datenschutzkonferenz koordiniert. Nicht selten wird auch seitens der Presse die örtliche Zuständigkeit meiner Behörde falsch eingeschätzt. Meine Dienststelle ist im Wesentlichen allein zuständig für sächsische öffentliche Stellen und die nicht-öffentlichen Stellen, die auch ihre Hauptniederlassung in Sachsen haben. Dies betrifft auch Filialunternehmen. Nicht so sehr entscheidend ist auch, ob betroffene Personen oder Beschwerdeführer ihren Wohnsitz in Sachsen haben.

Beispielhaft führe ich zur Veranschaulichung thematisch nachstehende Anfragen zu Presseauskünften auf, die zu verzeichnen gewesen sind:

Den Bereich der Innenverwaltung betreffend erfolgten Nachfragen zu Bodycams bei der Polizei, Öffentlichkeitsfahndungen, DNA-Ermittlungen, die Weitergabe von Meldedaten und von versammlungsbehördlichen Informationen an das Landesamt für Verfassungsschutz.

Weitere Presseanfragen gab es zu WhatsApp an Schulen, dem Einsatz von Dash-Cams und deren Verwertbarkeit bei Verkehrsunfällen, Fragen der Videoüberwachung (allgemein, deren Zulässigkeit in Hauseingängen, auf Parkplätzen), zu Fragen der Gesichtserkennung durch optisch-elektronische Einrichtungen, informationssicherheitstechnischen Lösungen bei Elektro-Automobilen, zu Belegungslisten und deren Verarbeitung in Asylbewerber- und Aufnahmeeinrichtungen, mutmaßlichen Datenschutzverstößen in Gemeindeverwaltungen, zu datenschutzgerechten Cloud-Lösungen im Schulbereich, zum Umgang mit Patientendaten und zu Problembereichen mit beschäftigtendatenschutzrechtlichen Bezügen.

Was eine gehäufte Anfrage in Bezug auf ein Meldeportal einer Fraktion des sächsischen Landtags zur Informationseinholung in schulischen Angelegenheiten betrifft, hatte ich auf meine Unzuständigkeit als Datenschutzaufsichtsbehörde zu verweisen. Meine Behörde kontrolliert gemäß § 14 Absatz 1 in Verbindung mit § 2 Absatz 1 Satz 3 Sächsisches Datenschutzdurchführungsgesetz nicht den sächsischen Landtag und seine Organe.

Allgemeinere Nachfragen gab es zu Datenpannen und Meldungen gemäß Artikel 33 DSGVO, Cybersicherheit, zu Fragen der ordnungsgemäßen Umsetzung der DSGVO durch mittelständische Unternehmen und zu Datenschutzverstößen und Bußgeldverfahren allgemein und im speziellen gegen Polizisten.

6.6 Vortrags- und Schulungstätigkeit

Bedienstete des Sächsischen Datenschutzbeauftragten sind beim Fortbildungszentrum des Freistaates Sachsen in Meißen bzw. an der Sächsischen Verwaltungs- und Wirtschaft-Akademie als Referenten. Vorträge und Schulungen konnten auch im Berichtszeitraum noch nicht in der vorgesehenen Breitenwirkung durchgeführt werden. Hierfür bitte ich um Verständnis. Weiterhin sind die personellen und sachlichen Ressourcen meiner Behörde begrenzt und noch nicht ausreichend, vergleiche auch 6.6 des Tätigkeitsberichts 2017/2018 Teil 2.

7 Zusammenarbeit der Datenschutzaufsichtsbehörden, Datenschutzkonferenz

7.1 Materialien der Datenschutzkonferenz – Entschließungen

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden verabschiedete die nachstehend aufgeführten Entschließungen, die in der digitalen Ausgabe des Tätigkeitsberichts verlinkt worden sind.

1. Keine massenhafte automatisierte Aufzeichnung von Kfz-Kennzeichen für Strafverfolgungszwecke (06.11.2019)

2. Gesundheitswebseiten und Gesundheits-Apps: Keine Weitergabe sensibler Daten an unbefugte Dritte! (06.11.2019)

3. Gesundheitseinrichtungen müssen unabhängig von ihrer Größe den Schutz von Patientendaten gewährleisten (06.11.2019)

4. Empfehlungen für eine datenschutzkonforme Gestaltung von Künstliche Intelligenz-Systemen (06.11.2019)

5. Positionspapier der Datenschutzkonferenz zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von Künstliche Intelligenz-Systemen (06.11.2019)

6. Digitalisierung der Verwaltung datenschutzkonform und bürgerfreundlich gestalten! (12.09.2019)

7. Keine Abschaffung der Datenschutzbeauftragten (23.04.2019)

8. Hambacher Erklärung zur künstlichen Intelligenz - Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3. April 2019

9. Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten! - Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3. April 2019

7.2 Materialien der Datenschutzkonferenz – Beschlüsse

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden verabschiedete die nachstehend aufgeführten Beschlüsse, die in der digitalen Ausgabe meines Tätigkeitsberichts verlinkt sind.

1. Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DSGVO (13.12.2019) – (englische Version: Report on Experience Gained in the Implementation of the GDPR)

2. Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu verhaltensbasierter Werbung (07.11.2019)

3. Concept of the independent data protection authorities of the Federation and the Länder for the admeasurement of fines in proceedings against undertakings (14.10.2019)

4. Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu verhaltensbasierter Werbung (25.09.2019)

5. Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder - Sachliche Zuständigkeit für E-Mail und andere Over-the-top (OTT)-Dienste (12.09.2019)

6. Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur datenschutzrechtlichen Verantwortlichkeit innerhalb der Telematik-Infrastruktur (12.09.2019)

7. Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu spezifischen Aufsichtsbehörden (12.08.2019)

8. Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder - Asset Deal – Katalog von Fallgruppen (24.05.2019)

9. Beschluss zur Beteiligung der spezifischen Aufsichtsbehörden gem. § 18 Absatz 1 Satz 4 BDSG an der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der Europäischen Union (13.05.2019)

10. Beschluss: Geplante Einführung eines regelmäßigen vollständigen Meldedatenabgleichs zum Zweck des Einzugs des Rundfunkbeitrags stoppen (26.04.2019)

11. Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung“ im Erwägungsgrund 33 der DSGVO (03.04.2019)

12. Positionierung der Datenschutzkonferenz zum datenschutzkonformen Einsatz von Windows 10 (03.04.2019)

13. Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit (01.04.2019)

14. Informationen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden zu Datenübermittlungen aus Deutschland in das Vereinigte Königreich Großbritannien und Nordirland nach deren Austritt aus der Europäischen Union (08.03.2019)

7.3 Materialien der Datenschutzkonferenz – Orientierungshilfen

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden verabschiedete die nachstehend aufgeführten Orientierungshilfen, die in der digitalen Ausgabe meines Tätigkeitsberichts verlinkt sind.

1. Whitepaper zu technischen Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich (07.11.2019)

2. Positionspapier zur biometrischen Analyse (03.04.2019)

3. Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien (29.03.2019)

4. Orientierungshilfe: Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung (29.03.2019)

5. Akkreditierungsprozess für den Bereich „Datenschutz“ gemäß Artikel 42, 43 DSGVO – Version in Graustufen sowie Version in Farbe (15.03.2019)

6. Orientierungshilfe der Datenschutzaufsichtsbehörden zu dem Einsatz von Bodycams durch private Sicherheitsunternehmen (22.02.2019)

7. Positionspapier zur Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams) (28.01.2019)

8. Positionspapier zur Nutzung von Kameradrohnen durch nicht-öffentliche Stellen (16.01.2019)

9. Zusatz zur Orientierungshilfe "Videoüberwachung durch nicht-öffentliche Stellen" des Düsseldorfer Kreises vom 19.02.2014 (08.01.2019)

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

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

1. Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679

2. Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) - Annex 1

   (deutsche Version: Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen gemäß Artikel 43 der DSGVO (2016/679))

3. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation

4. Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679

5. EDPB Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679

6. Bestätigte Leitlinien der Artikel-29-Gruppe

a. WP 259 rev.01 - Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679

b. WP 260 rev.01 - Leitlinien für Transparenz gemäß der Verordnung 2016/679

c. WP 251rev.01 - Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679

d. WP 250rev.01 - Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679

e. WP 263 rev.01 - Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR

f. WP 264 - Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data

g. WP 265 - Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data

h. WP 256 rev.01 - Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules

i. WP 257 rev.01 - Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules

j. WP 254 rev.01 - Adequacy Referential

7. EDPB statement on ePrivacy

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

Zur Abgrenzung des Richtlinienbereichs gegenüber der DSGVO vergleiche den Beitrag 2.1.

8.1 Unklare Bitte der Polizei an Hotels um Mithilfe

Im Sommer vergangenen Jahres wurde ich auf eine Pressemeldung aufmerksam gemacht, nach der eine sächsische Polizeidirektion im Vorfeld eines großen Musikfestivals ein Schreiben an Hotelbetreiber versandt hatte, mit dem auf vermehrte Taschendiebstähle auf diesem Musikfestival hingewiesen wurde. Die vorangegangenen Ermittlungen zeigten, so heißt es im Schreiben der Polizeidirektion, dass diese in der Regel auf rumänische Banden zurückzuführen seien. Die angeschriebenen Herbergsbetriebe wurden unter der Überschrift „Übermittlung von Personendaten“ gebeten, „die Ermittlungen zu unterstützen“, indem sie telefonisch mitteilen, „ob im genannten Zeitraum rumänische Staatsbürger ein Zimmer beziehen“.

Da ich keine Rechtsgrundlage für eine solche polizeiliche Bitte (oder auch Aufforderung) an Beherbergungsbetriebe, personenbezogene Daten über deren Vertragspartner (Gäste) zu übermitteln, erkennen konnte und mir nicht klar war, ob dem Anliegen der Polizei eine konkrete polizeiliche Gefahr zugrunde lag, bat ich die Polizeidirektion um Aufklärung.

Die Polizei teilte mit, dass das Schreiben bei zehn Beherbergungsstätten abgegeben und erläutert worden sei. Es sei allein eine Mitteilung des „Ob“ erbeten worden; eine Einsichtnahme in Meldescheine sei nicht verlangt worden. Die Maßnahme habe der vorbeugenden Bekämpfung bandenmäßig organisierter Diebstahlskriminalität gedient. Das Schreiben habe eine sog. Minusmaßnahme (geringere Eingriffsintensität) zu den Befugnissen nach §§ 30 Absatz 4 und 34 Absatz 4 BMG dargestellt.

Ich habe dieses Vorgehen gegenüber der Polizeidirektion kritisiert.

Zwar ist es zutreffend, dass die Polizei sich zur Erfüllung ihrer Aufgaben in Beherbergungsstätten die dort bereitzuhaltenden besonderen Meldescheine vorlegen lassen kann (§ 30 Absatz 4 BMG).

§ 30 Absatz 4 BMG setzt voraus, dass die verlangte Vorlage von Meldescheinen der Aufgabenerfüllung der Behörde dient. Aufgabe der Polizei ist die Abwehr von Gefahren, wobei polizeiliche Maßnahmen, die mit Grundrechtseingriffen verbunden sind, stets der Abwehr einer konkreten Gefahr dienen müssen. Gefahrerforschungsmaßnahmen finden im Vorfeld konkreter Gefahren statt. Wenn aber noch gar nicht klar ist, ob überhaupt eine konkrete Gefahrenlage gegeben ist, sind Grundrechtseingriffe in aller Regel unzulässig. Unzulässig wäre insoweit auch eine Erhebung und Speicherung personenbezogener Daten „auf Vorrat“ nur für den möglichen künftigen Bedarfsfall.

Weil damit eine wesentliche Voraussetzung von § 30 Absatz 4 BMG nicht vorlag, konnte das Anschreiben auch nicht als entsprechende „Minusmaßnahme“ zu dieser Befugnis deklariert werden.

Soweit die Polizeidirektion darauf hinwies, dass Auskünfte nur über das „Ob“ von angemeldeten Übernachtungen und die Übermittlung genauer Personendaten gerade nicht erbeten worden seien, habe ich die auf die offenkundige Mehrdeutigkeit des Schreibens hingewiesen. Es ist alles andere als klar, dass keine personenbezogenen Daten erbeten werden, wenn die Überschrift des Anschreibens „Übermittlung von Personendaten“ lautet.

Behörden der Eingriffsverwaltung und insbesondere der Polizeivollzugsdienst sollten nach außen stets klar und unmissverständlich auftreten und ihr Handeln auf eine sichere Rechtsgrundlage stützen können. Die Rechtsordnung hält diverse gesetzliche Befugnisse bereit, mit denen Auskünfte zur Abwehr von Gefahren oder zu Zwecken der Strafverfolgung verlangt werden können, wenn die gesetzlich bestimmten Voraussetzungen vorliegen. Mit „Bitten“ um Auskünfte und freiwilligen Angaben, insbesondere über Dritte, sind in aller Regel begründete Zweifel an der Rechtmäßigkeit des Vorgehens verbunden. Überdies birgt solch unklares Handeln Risiken für die angefragten nicht-öffentlichen Stellen – hier also die angeschriebenen Hotels – , die selbst als Verantwortliche im Sinne der DSGVO nur unter gesetzlich bestimmten Voraussetzungen Daten über ihre Vertragspartner zu vertragsfremden Zwecken an Dritte herausgeben dürfen (vgl. § 24 Absatz 1 BDSG).

8.2 Gesichtserkennung nach neuem Polizeirecht

Im Jahr 2019 fand ein Gesetzgebungsvorhaben seinen Abschluss, mit dem meine Dienststelle schon weitaus früher beschäftigt war. Nach dem Grundsatzurteil des Bundesverfassungsgerichts zu Normen des Bundeskriminalamtsgesetzes vom 20. April 2016 (Az. 1 BvR 966/09), das auch für polizeirechtliche Vorschriften der Länder Folgen hatte, und dem Inkrafttreten der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates war eine grundlegende Novellierung des sächsischen Polizeirechts notwendig geworden.

In erfreulicherweise fast schon traditioneller Weise wurde ich sehr frühzeitig in die Überlegungen zum Gesetzentwurf einbezogen; in einem konstruktiven Austausch konnte ich Bedenken, Anregungen und Vorschläge vortragen. Über meine Tätigkeit im Gesetzgebungsverfahren und meine Anmerkungen zu den Entwürfen hatte ich bereits in meinem Tätigkeitsbericht 2018 unter Punkt 6.2.4.1 berichtet.

Aus dem weit über 20 Artikel umfassenden Gesetz zur Neustrukturierung des Polizeirechtes des Freistaates Sachsen ragen in ihrer Bedeutung und ihrer Regelungstiefe das Sächsische Polizeivollzugsdienstgesetz (SächsPVDG), das Sächsische Polizeibehördengesetz (SächsPBG) und das Sächsische Datenschutzumsetzungsgesetz (SächsDSUG) heraus. Während letzteres die allgemeinen Datenschutzregelungen der Richtlinie (EU) 2016/680 in Landesrecht überführt bzw. umsetzt, bilden SächsPVDG und SächsPBG die Nachfolge des bisher geltenden Sächsischen Polizeigesetz, nunmehr als getrennte Regelungswerke für den Polizeivollzugsdienst („uniformierte Polizei“) und die allgemeinen Polizeibehörden (z.B. Kommunen als allgemeine Polizeibehörden).

Auch wenn einige neue Eingriffsbefugnisse für den Polizeivollzugsdienst insbesondere zur Abwehr erheblicher Gefahren und zur Verhütung schwerer/terroristischer Straftaten geschaffen wurden – etwa Maßnahmen zur Telekommunikationsüberwachung und zur elektronischen Aufenthaltsüberwachung („elektronische Fußfessel“) –, deren Anwendungsvoraussetzungen aus meiner Sicht sich sehr genau an den Vorgaben des Bundesverfassungsgerichts orientieren, möchte ich hier – im Anschluss an meine Ausführungen

im Tätigkeitsbericht 2018 (s.o.) – nochmals auf eine neue Maßnahme eingehen, der meines Erachtens eine ganz besondere datenschutzrechtliche Bedeutung zukommt.

Nach § 59 SächsPVDG kann die Polizei zur Verhütung grenzüberschreitender Kriminalität durch die Begehung bestimmter schwerer Straftaten personenbezogene Daten durch den offenen Einsatz technischer Mittel zur Anfertigung von Bildaufzeichnungen des Verkehrs auf öffentlichen Straßen erheben sowie Informationen über Ort, Zeit und Verkehrsrichtung der Nutzung erfassen, um diese automatisiert mit anderen personenbezogenen Daten abzugleichen. Ein solcher automatisierter Abgleich darf nur mit personenbezogenen Daten konkret bestimmter Personen erfolgen, die zur Verhütung der oben erwähnten bestimmten schweren Straftaten zur polizeilichen Beobachtung ausgeschrieben sind. Die erhobenen Daten sind spätestens nach 96 Stunden automatisiert zu löschen, soweit sich nicht bei dem automatisierten Abgleich eine Übereinstimmung ergab und die Daten zur Verhütung oder Verfolgung der bestimmten schweren Straftaten im Sinne der Anwendungsvoraussetzung erforderlich sind.

Eine zentrale Rolle bei der Anwendung der Norm spielt Gesichtserkennungssoftware.

Der Einsatz automatisierter Gesichtserkennung in der staatlichen Eingriffsverwaltung ist nach wie vor umstritten. Die bislang in Versuchen gesammelten Erfahrungen zeigen, dass mit hohen Fehlerquoten zu rechnen ist. Es ist nicht schwer, sich vorzustellen, welche gravierenden Folgen ein „falscher Treffer“ für die betroffene Person haben kann; sei es durch eine auf den Treffer folgende präventive polizeiliche Maßnahme oder – aufgrund der vermeintlichen Beweiskraft der Erfassung möglicherwiese noch schwerer wiegend – im Rahmen strafprozessualer Ermittlungsmaßnahmen.

Bereits in der Anwendung der automatisierten Kennzeichenüberwachung nach § 19a SächsPolG a.F., nunmehr § 58 SächsPVDG, zeigt sich, dass nur ein Bruchteil der technisch erfassten Treffer – also einer vom Gerät erkannten Übereinstimmung eines erfassten Kennzeichens mit dem aus einer polizeilichen Datei zur Fahndung/Suche hinterlegten Kennzeichen – als „Echttreffer“ bestätigt werden konnte. Im Bericht über die Datenerhebung mit besonderen Mitteln sowie mit technischen Mitteln zur mobilen automatisierten Kennzeichenerfassung durch die sächsische Polizei im Jahr 2018 (Landtagsdrucksache 7/759) heißt es dazu: „Im Rahmen des Einsatzes von AKES wurden bei insgesamt 10.775 (Vorjahr: 16.336) systemseits gemeldeten Fahrzeugen 302 Echttreffer verifiziert.“

Die Diskussion um die Norm des § 59 SächsPVDG erhielt noch im Gesetzgebungsverfahren neue Impulse, nachdem das Bundesverfassungsgericht in Verfassungsbeschwerden über landesrechtliche Bestimmungen zur automatisierten Kennzeichenerfassung in Abkehr von seiner bisherigen Rechtsprechung mit Beschlüssen vom 18. Dezember 2018 (1 BvR 142/15 und 1 BvR 2795/09, 1 BVR 3187/10) festgestellt hatte, dass auch im Fall von „Nichttreffern“ in der kurzen, rein technischen Erfassung des Kfz-Kennzeichens ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen vorliegt.

Damit konnte nunmehr kein Zweifel mehr daran bestehen, dass es sich bei der Erfassung von Kfz-Kennzeichen und Lichtbildern von Fahrzeuginsassen nach § 59 Absatz 1 SächsPVDG und deren 96 Stunden währende Speicherung um einen klaren und – im Vergleich zur bloß Sekundenbruchteile andauernden Erfassung eines Kennzeichens — erheblich vertieften Grundrechtseingriff handelt.

Der sächsische Gesetzgeber hat innerhalb der Vorschrift Verfahrensregelungen geschaffen, die die Auswirkungen der Maßnahme auf den Großteil der erfassten Personen – Menschen, die keinerlei polizeirelevantes Verhalten an den Tag legen – eindämmen. Das ist zu begrüßen. Bildmaterial, zu dem keine Treffer gemeldet werden, darf für keine anderen Zwecke verwendet werden und wird automatisiert gelöscht. Allein erfasste Daten, zu denen Treffermeldungen vorliegen, dürfen weiter verwendet werden, freilich auch nur in dem engen Rahmen, der durch die Anwendungsvoraussetzungen der Maßnahme definiert ist sowie entsprechende Strafverfolgungsmaßnahmen umfasst. Die Maßnahme erfolgt offen, die Polizei hat strenge Dokumentationspflichten zu erfüllen. Zudem hat der Gesetzgeber eine Evaluierung der Norm nach drei Jahren vorgeschrieben.

Das Sächsische Staatsministerium des Innern hat mir bestätigt, dass in der Praxis nur automatisierte Abgleiche der erhobenen Daten mit zuvor festgelegten Referenzdaten erfolgen sollen. Damit soll von vornherein vermieden werden, mit einer „rückwirkenden Anwendung“ einer präventiv-polizeilichen Maßnahme in den Bereich der reinen Strafverfolgung zu gelangen.

Die praktische Anwendung der Befugnis werde ich aufmerksam beobachten. § 59 SächsPVDG ist übrigens eine der Normen des Sächsischen Polizeivollzugsdienstgesetzes, deren Vereinbarkeit mit der Sächsischen Verfassung derzeit durch den Sächsischen

Verfassungsgerichtshof in Leipzig geprüft wird. Der Entscheidung des Gerichts sehe ich mit großem Interesse entgegen.

8.3 Datenerhebung einer Justizvollzugsanstalt bei Beantragung von Langzeitbesuch

Ein in einer sächsischen Justizvollzugsanstalt (JVA) Inhaftierter übersandte mir in der JVA verwendete Vordrucke, die von Gefangenen und potentiellen Besuchern auszufüllen waren, die sich im Rahmen sog. Langzeitbesuche treffen wollten, und bat um eine datenschutzrechtliche Bewertung. In den Vordrucken wurden diese Besuche, die in der Regel in besonderen, dafür vorgesehenen Räumen der JVA und unbeaufsichtigt stattfinden, als ehe- und familienfreundliche Besuche (EFB) bezeichnet.

Die Vordrucke bezogen sich zum einen auf den inhaftierten Antragsteller selbst, zum anderen sollten Angaben über die besuchende Person erhoben werden.

So sollte der Gefangene erklären, dass er über seine Pflicht belehrt worden sei, den ihn besuchenden Personenkreis über Infektionskrankheiten aufzuklären. Daneben sollte er sich mit dem Antrag auf Zulassung zum EFB damit einverstanden erklären, dass der ihn besuchende Personenkreis „in der Regel“ über seine Straftat/Straftaten (Strafgefangene) bzw. über die ihm vorgeworfene Straftat/Straftaten (Untersuchungsgefangene) unterrichtet werde.

In dem den Besucher betreffenden Vordruck soll dieser Angaben zu seiner Person machen (einschließlich der „persönlichen und beruflichen Entwicklung“ für den Fall einer eigenen Haftentlassung innerhalb der letzten fünf Jahre) und der Verarbeitung seiner Daten zustimmen oder widersprechen. Außerdem erklärt er sein Einverständnis mit der Einholung von Auskünften über ihn bei Polizeibehörden und Staatsanwaltschaften oder er erteilt es ausdrücklich nicht.

Missverständlich waren die Hinweise in den Vordrucken zu einer einem möglichen Widerspruch des potentiellen Besuchers gegen die Verarbeitung seiner Daten durch die JVA formuliert: An einer Stelle erfolgte der recht apodiktische Hinweis, dass, sofern keine Auskünfte erteilt würden bzw. dem Einholen der Auskünfte widersprochen werde, die Geeignetheit für diese Besuchsart nicht abschließend geprüft werden und somit die Zu-

lassung als Besucher nicht erfolgen könne. Andernorts findet sich im Vordruck der Hinweis, dass der Widerspruch und die Verweigerung des Einverständnisses zur Ablehnung der Zulassung zum Besuch führen könnten.

Nicht unerheblich für die Bewertung der Vordrucke war der Umstand, dass die JVA für die Zulassung derartiger Langzeitbesuche voraussetzte, der Antragsteller (Gefangener) sich mindestens seit einem Jahr in der JVA befinden musste und die zur Zulassung beantragten Besucher „mindestens acht beanstandungsfreie Besuchstermine wahrgenommen" hatten – sowohl Gefangener als auch potentieller Besucher konnten aufgrund dieser Erfahrungen durch die JVA also durchaus eingeschätzt werden.

Eine Nachfrage beim Sächsischen Staatsministerium der Justiz ergab, dass Anträge/Formulare für Langzeitbesuche in den sächsischen Justizvollzugsanstalten nicht einer einheitlich gestalteten Vorlage entsprachen, sondern durch die Anstalten individuell erstellt und verwendet wurden.

Meine datenschutzrechtliche Kritik an dem oben beschriebenen Vordruck äußerte ich gegenüber der JVA und dem Staatsministerium:

Eine Rechtspflicht des Gefangenen, den ihn besuchenden Personenkreis über Infektionskrankheiten aufzuklären, besteht nicht. Es spricht andererseits natürlich nichts gegen eine dringende Bitte an den Gefangenen, seinen Besuch über eventuelle aktuelle Infektionskrankheiten aufzuklären und während des Besuchs entsprechende Schutzmaßnahmen zu beachten. Gleiches gilt umgekehrt auch für die Besuchsperson selbst.

Ich konnte auch keine Rechtsgrundlage dafür erkennen, dass die JVA Besucher des Gefangenen „in der Regel" über dessen (vorgeworfenen) Straftaten unterrichtet; völlig unklar war auch, wann ein solcher Regelfall vorliegen sollte und wann nicht. Eine gesetzliche Voraussetzung der Zulassung eines Langzeitbesuchs ist die Geeignetheit des Gefangenen. Ich gehe davon aus, dass Gefangene, bei denen Anhaltspunkte für gewalttätiges Verhalten gegenüber Besuchern vorliegen, für Langzeitbesuche nicht geeignet sind und entsprechende Anträge abschlägig beschieden werden.

Liegen der JVA solche Anhaltspunkte aber nicht vor, darf bzw. muss also die JVA von der Geeignetheit des Gefangenen ausgehen - für eine darüber hinausgehende Aufklärung des Besuchers über die Person des Gefangenen durch die JVA ist mangels gesetzlicher Befugnis kein Raum.

Hinsichtlich der Erhebung von Daten über den potentiellen Besucher wies ich darauf hin, dass dessen Zustimmung zur Erhebung ihn betreffender Daten bei Dritten die JVA nicht von der Pflicht zur Beschränkung der den Besucher betreffenden Datenverarbeitung auf das erforderliche Maß entbindet. Damit wäre vor der Einholung von Auskünften über einen potentiellen Besucher stets zu prüfen, ob eine Einholung von Auskünften (oder Negativmeldungen) bei Behörden wirklich erforderlich ist. Für eine pauschale Überprüfung anstaltsbekannter Besucher (s.o.), insb. Familienangehöriger, fehlte eine Rechtsgrundlage, die auch nicht durch die Zustimmung der Betroffenen ersetzt werden dürfte. Sollten allerdings besondere Umstände im Einzelfall darauf hinweisen, dass ein Besuch missbraucht werden und Vollzug oder Sicherheit der Anstalt gefährdet sein könnte, wäre eine Überprüfung mittels Einholung von behördlichen Auskünften auch meiner Meinung nach sicher „erforderlich“.

Für den Fall, dass die Besuchsperson selbst innerhalb der letzten fünf Jahre aus der Haft entlassen wurde, erschien mir die sehr unbestimmte Aufforderung, Angaben zur „persönlichen und beruflichen Entwicklung“ zu machen, neben der evtl. Einholung polizeilicher oder staatsanwaltschaftlicher Auskünfte überflüssig und damit nicht erforderlich. Insbesondere bei Familienangehörigen hat sich das Interesse der JVA an der Person des Besuchers ausschließlich auf die Gewährleistung der Sicherheit und Ordnung in der Anstalt zu beschränken, dafür ist kein möglichst komplettes und über strafrechtliche Erkenntnisse hinausgehendes Bild des angehörigen Besuchers erforderlich.

Ich wies auch darauf hin, dass die dargestellten Datenverarbeitungen in vielen Fällen des Langzeitbesuchs im Licht des grundgesetzlich verankerten Schutzes von Ehe und Familie (Artikel 6 des Grundgesetzes) zu betrachten sein werden, weshalb insbesondere eine (Teil-)Verweigerung der Zustimmung zur Datenverarbeitung durch familienangehörige Besucher nicht generell zur Nichtzulassung des Besuchs führen dürfe.

Meine Auffassung deckte sich weitgehend mit der Position des Staatsministeriums der Justiz, das die Einholung von Auskünften zu Besuchern bei Behörden lediglich in Ausnahmefällen für erforderlich hält, etwa bei tatsächlichen Anhaltpunkten im Einzelfall für die Gefährdung der Sicherheit und Ordnung der Anstalt (§ 27 Nummer 1 SächsStVollzG) oder bei der Befürchtung, dass Personen, die keine Familienangehörigen des Gefangenen sind, einen schädlichen Einfluss auf die Gefangenen haben oder die Erreichung des Vollzugsziels behindern (§ 27 Nummer 2 SächsStVollzG).

Das Staatsministerium nahm den Vorgang zum Anlass, die Verfahren zur Zulassung von Langzeitbesuchen in den sächsischen Justizvollzugsanstalten zu bewerten und eine Vereinheitlichung des Vorgehens zu prüfen.

Mit der betreffenden JVA trat ich in einen konstruktiven Dialog zu einer vorläufigen Anpassung der verwendeten Vordrucke ein, in dessen Ergebnis das Kriterium der Erforderlichkeit der Datenverarbeitung im Einzelfall mehr Gewicht erhielt und die Hinweise in den Vordrucken für Gefangene und potentielle Besucher entsprechend umformuliert wurden.

Mit Inkrafttreten der Sächsischen Justizvollzugsdatenschutzgesetzes im September 2019 ist nun auch gesetzlich geregelt, dass Justizvollzugsbehörden (nur) bei tatsächlichen Anhaltspunkten einer drohenden Gefahr für die Sicherheit in der Anstalt bei Personen, die die Zulassung zum Besuch von Gefangenen oder zum Besuch der Anstalt begehren, eine Zuverlässigkeitsüberprüfung vornehmen dürfen (§ 16 Absatz 3 Satz 1 SächsJVollzDSG).

8.4 Videoüberwachung von Hafträumen im sächsischen Justizvollzug

Seit 2019 existieren für den sächsischen Justizvollzug Rechtsgrundlagen für die Videoüberwachung von Hafträumen. Das im Freistaat seit den 1990er Jahren geltende Prinzip, dass Hafträume als (einziger) Rückzugsort von Gefangenen ausnahmslos frei von Videoüberwachung bleiben sollen, wurde damit aufgegeben.

Die entsprechenden, 2019 in die Vollzugsgesetze aufgenommenen Regelungen sehen „die Beobachtung der Gefangenen, auch mit optisch-technischen Hilfsmitteln in dafür vorgesehenen Hafträumen“ (z.B. in § 83 Absatz 2 Nummer 2 SächsStVollzG) als eine unter mehreren besonderen Sicherungsmaßnahmen vor. Gegen Gefangene können besondere Sicherungsmaßnahmen angeordnet werden, wenn nach ihrem Verhalten oder aufgrund ihres seelischen Zustandes in erhöhtem Maße die Gefahr der Entweichung, von Gewalttätigkeiten gegen Personen oder Sachen, der Selbsttötung oder der Selbstverletzung besteht (§ 83 Absatz 1 SächsStVollzG).

Im Gesetzgebungsverfahren habe ich Bedenken gegen die Einführung der Videoüberwachung von Hafträumen vorgetragen. Der Gefangene verfügt grundsätzlich nicht über ei-

nen Rückzugsort ins Private, der den Schutz und die Intimität einer eigenen, grundgesetzlich von Artikel 13 des Grundgesetzes streng geschützten Wohnung bietet und in dem er sich staatlicher Beobachtung entziehen kann. Umso wichtiger ist die Gewissheit, dass er zumindest in „seinem“ Haftraum frei von Überwachung agieren kann und einen Rückzugsraum findet. Eine Videoüberwachung von Hafträumen berührt insofern nicht nur das Grundrecht des Gefangenen auf informationelle Selbstbestimmung; betroffen ist auch die Würde des inhaftierten Menschen (Artikel 1 Absatz 1 des Grundgesetzes).

Gleichwohl konnte ich mich Argumenten für eine Videoüberwachung in besonderen Ausnahmesituationen nicht verschließen. Vor allem Erfahrungen mit Suiziden im Justizvollzug und die Belastung der Gefangenen durch eine „menschliche Beobachtung“ durch Bedienstete mit kurzen Aufschluss- und Kontrollintervallen im Haftraum lassen eine Videoüberwachung von Hafträumen in eng begrenzten Ausnahmefällen als geeignetes Mittel zur Abwehr von Gefahren vor allem für den Gefangenen selbst erscheinen.

Bei der Änderung der Vollzugsgesetze bestimmte der Gesetzgeber eine gewisse Einschränkung der Videoüberwachung von Hafträumen zumindest in räumlicher Hinsicht – nicht jeder Haftraum sollte potentiell überwacht werden können, sondern nur „dafür vorgesehene Hafträume“.

Eine Einschränkung der Anwendungsvoraussetzung im Vergleich zu anderen besonderen Sicherungsmaßnahmen wurde hingegen nicht vorgenommen. Insoweit setzte ich Hoffnung in das zu diesem Zeitpunkt noch in der Beratung befindliche Sächsische Justizvollzugsdatenschutzgesetz (SächsJVollzDSG), in dessen Entwurf sich eine Regelung fand, nach der die Videoüberwachung von Hafträumen Im Rahmen einer Beobachtung als besonderer Sicherungsmaßnahme zulässig sein sollte, soweit dies „zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben erforderlich“ sein sollte.

Leider wurde diese den Einsatz der Haftraumvideoüberwachung beschränkende Regelung im Gesetzgebungsverfahren gestrichen.

Zwar habe ich meine starken Bedenken dagegen, dass eine so eingriffsintensive Maßnahme in einer Reihe mit und unter denselben Anordnungsvoraussetzungen wie z.B. der Entzug oder die Vorenthaltung von Gegenständen, die Trennung von anderen Gefangenen oder die Beschränkung des Aufenthalts im Freien, auftaucht bzw. angewendet werden soll, wiederholt vorgetragen. Eine Haftraumüberwachung mittels optisch-elektroni-

scher Einrichtungen mit Aufzeichnung der Bilder ist m. E. nur dann eine geeignete, erforderliche und verhältnismäßige Maßnahme, wenn und soweit sie der Abwehr einer gegenwärtigen Gefahr für Leib oder Leben des Gefangenen dient. In diesem Sinne hält auch die Nationale Stelle zur Verhütung von Folter eine Kameraüberwachung nur für zulässig, wenn sie im Einzelfall zum Schutz der Person unerlässlich ist (https://www.nationale-stelle.de/fileadmin/dateiablage/Dokumente/Berichte/Standards/20180613_Standards/20180613_Standards_fuer_Justizvoll-zug.pdf). Auch vor diesem Hintergrund sollte eine Gleichstellung mit Maßnahmen vermieden werden, die der Gefahr der Entweichung oder von Gewalttätigkeiten gegen (andere) Personen oder Sachen entgegenwirken sollen.

Im Ergebnis hat der Gesetzgeber sich aber gegen eine Einschränkung auf Tatbestandsebene der Eingriffsvoraussetzungen entschieden und die Beobachtung von dafür vorgesehenen Hafträumen mit optisch-technischen Hilfsmitteln gewissermaßen gleichrangig in den schon lange bestehenden Katalog besonderer Sicherungsmaßnahmen eingereiht. Nach § 34 Absatz 1 SächsJVollzDSG ist die Beobachtung innerhalb von Hafträumen, Arresträumen und Zimmern mittels optisch-technischer Einrichtungen nunmehr zulässig, soweit eine Rechtsvorschrift dies vorsieht. Solche Rechtsvorschriften finden sich in den Vollzugsgesetzen (s.o.).

§§ 34, 35 SächsJVollzDSG enthalten – das sollte nicht unerwähnt bleiben – Verfahrensregelungen für den Einsatz der Haftraumüberwachung mittels optisch-technischer Einrichtungen, die den Schutz der Gefangenen bezwecken und mit denen das Interesse der Anstalt an der Abwehr von Gefahren und die Belange der Gefangenen in Einklang gebracht werden sollen.

Ich plädiere dafür, dass in der Praxis des Justizvollzugs Gefangene in Hafträumen nur in ganz besonderen Ausnahmesituationen mittels optisch-technischer Einrichtungen überwacht werden und die Maßnahme trotz der gesetzlichen Gleichstellung mit anderen besonderen Sicherungsmaßnahmen nicht zu einer „Standardsicherungsmaßnahme“ wird.

8.5 Erhebung von Verkehrsdaten des Anschlusses eines Rechtsanwalts

Ein in einer sächsischen Großstadt tätiger Rechtsanwalt wandte sich an mich, nachdem er anlässlich einer Akteneinsicht als Strafverteidiger in eine Ermittlungsakte zu einem

gegen seinen Mandanten geführten Verfahren feststellte, dass Verkehrsdaten (im Folgenden auch: Verbindungsdaten) zu seinem anwaltlich genutzten Mobilfunkanschluss aufgeführt waren. Es handelte sich um eine Liste mit Verbindungsdaten, die über einen Zeitraum von über zweieinhalb Jahren im Wege einzelner Telekommunikationsüberwachungsmaßnahmen in verschiedenen Ermittlungsverfahren zu seinem Anschluss erhoben worden waren.

Meine datenschutzrechtliche Prüfung des Sachverhalts zu dem Komplex führte zu einer förmlichen Beanstandung des Landeskriminalamts und der zuständigen örtlichen Staatsanwaltschaft unter Bezug auf strafprozessuale Vorschriften wegen der Verwendung von einem Zeugnisverweigerungsrecht unterliegenden Informationen, nicht erfolgter Löschungen und der Unterlassung von Benachrichtigungen Betroffener.

Im Rahmen strafrechtlicher Ermittlungen in einem bestimmten Deliktsfeld – aus dem auch Vorwürfe gegen Mandanten stammen, die der Rechtsanwalt regelmäßig als Strafverteidiger vertritt – wurden zurückliegend in zahlreichen Fällen auf jeweils richterliche Anordnung bei Providern Verkehrsdaten (§ 96 TKG) erhoben, die zu bestimmten Anschlüssen oder in „Tatort-Funkzellen“ erfasst worden waren.

Die polizeiliche Ermittlungsarbeit erfolgte dabei zentral durch eine Sonderkommission im Landeskriminalamt Sachsen. Die Führung der einzelnen Ermittlungsverfahren oblag der jeweils örtlich zuständigen Staatsanwaltschaft; dabei wurde hauptsächlich die Staatsanwaltschaft der Großstadt tätig, in der sich auch die Kanzlei des Rechtsanwalts befindet.

Die Daten aus zahlreichen Maßnahmen nach § 100g StPO wurden gespeichert und konnten (bzw. können) zentral – durch das Landeskriminalamt Sachsen – ausgewertet werden. Dabei werden bei Auswertungen auch Abgleiche neu erhobener Daten mit dem wachsenden Bestand an Daten aus früheren Erhebungsmaßnahmen durchgeführt, um ermittlungsrelevante Anschlüsse und Kommunikationsverbindungen zu erkennen. Zu Verkehrsdaten bzw. Nummern, die als nicht beweiserheblich bewertet werden, wurden zunächst keine weiteren Ermittlungen angestellt (Bestandsdatenauskunft o.ä.); allerdings wurden diese Daten auch nicht gelöscht, sondern weiterhin gespeichert und bei späteren Auswertungen (Abgleichen) genutzt bzw. einbezogen. Auf diese Weise konnte in einem der Verfahren in einem späteren Jahr in Auswertung von erhobenen Daten und unter Rückgriff auf gespeicherte Verkehrsdaten aus früheren Maßnahmen und anderen Verfahren durch das

Landeskriminalamt eine Liste zu Verbindungen einer bestimmten Telefonnummer erstellt werden, die gespeicherte Verbindungen aus dem Zeitraum April 2013 bis Dezember 2016 aufführt und die zur Akte genommen wurde. Dabei handelte es sich um die Rufnummer des Rechtsanwalts, ohne dass dessen Name zu diesem Zeitpunkt erhoben oder zugeordnet worden war.

Erst im weiteren strafprozesssualen Prozedere erlangte das Landeskriminalamt Kenntnis über die Identität und Eigenschaft als Rechtsanwalt und Strafverteidiger und teilte die umgehend dem zuständigen Staatsanwalt mit. Gleichwohl unterließ es die Staatsanwaltschaft im Folgenden, gegenüber dem Landeskriminalamt die Löschung der zum Anschluss des Rechtsanwalts und Strafverteidigers erhobenen Verkehrsdaten zu verfügen. Ebenso unterblieb eine Mitteilung an den Rechtsanwalt über die Erhebung von Verkehrsdaten des von ihm genutzten Anschlusses. Auch innerhalb der ermittelnden Organisationseinheit des Landeskriminalamts wurde die Information nicht weitergegeben. Daher unterblieben Schritte, um den Datenbestand der Sonderkommission auf das Vorhandensein von Verkehrsdaten zum Anschluss des Rechtsanwalts zu überprüfen und ggf. die jeweils zuständigen Staatsanwaltschaften um unverzügliche Entscheidung über eine Löschung zu ersuchen.

In weiteren Fällen hatte das Landeskriminalamt, wie ich mit meiner Kontrolle feststellte, erforderliche Löschungen nicht durchgeführt und Informationen weiterverwandt. Die Beanstandung des Landeskriminalamt erfolgte wegen des Verstoßes gegen das Verbot der Verwendung von Erkenntnissen über Umstände der Kommunikation eines Rechtsanwalts, die durch nicht gegen ihn gerichtete Ermittlungsmaßnahmen erlangt wurden und über die er das Zeugnis verweigern dürfte (§ 160a Absatz 1 Satz 2 i. V. m. Satz 5 StPO), sowie der unzureichenden Umsetzung von staatsanwaltschaftlichen Löschungsverfügungen nach §§ 101 Absatz 8 und 101a Absatz 3 Satz 4 StPO.

Der mit der gesetzlichen Löschungsverpflichtung bezweckte Grundrechtsschutz wurde den betroffenen Personen vorenthalten, die weitere Verwendung der Verkehrsdaten, die entgegen staatsanwaltschaftlicher Verfügungen nicht gelöscht wurden, erfolgte ohne Rechtsgrundlage. Zudem hätte nach Kenntniserlangung der Rechtsanwalts- bzw. Strafverteidigereigenschaft seitens des Landeskriminalamts eine Überprüfung der im gesamten Ermittlungskomplex akkumulierten Datenbestände im Hinblick auf die Daten des Rechtsanwalts erfolgen müssen.

Die Staatsanwaltschaft habe ich wegen eines Verstoßes gegen das gesetzliche Verbot, eine Ermittlungsmaßnahme gegen einen Rechtsanwalt zu richten, die voraussichtlich Erkenntnisse erbringen würde, über die dieser das Zeugnis verweigern dürfte (§ 160a Absatz 1 Satz 1 StPO), sowie gegen die Pflicht, dennoch erlangte Erkenntnisse unverzüglich zu löschen (§ 160a Absatz 1 Satz 3 StPO), und die Pflicht, Beteiligte der betroffenen Telekommunikation von der Erhebung der Verkehrsdaten nach § 100g StPO zu benachrichtigen (§ 101a Absatz 6 Satz 1 StPO), beanstandet. Die Beanstandung erstreckte sich darüber hinaus auf das Unterlassen der Löschung der Verkehrsdaten des Rechtsanwalts, die in anderen, nicht direkt gegen den Betroffenen gerichteten Maßnahmen erhoben worden waren (§ 160a Absatz 1 Satz 3 i. V. m. Satz 5 StPO).

Ich messe den grundrechtschützenden Verfahrensvorschriften der Strafprozessordnung, die sich auf die besonderen Verhältnisse bei Berufsgeheimnisträgern und auf verdeckte Erhebungsmaßnahmen beziehen, erhebliche datenschutzrechtliche Bedeutung zu. Die Einhaltung dieser Vorschriften erfolgt nicht etwa aus Kulanz der Strafverfolgungsbehörden, sondern ist – ungeachtet der prinzipiellen Bindung staatlicher Stellen an Gesetz und Recht – aus Interessen des Gemeinwohls zwingend geboten. Aufgrund verfassungsgerichtlicher Rechtsprechung und verbindlicher Entscheidungen des Gesetzgebers, in denen sowohl das Strafverfolgungsinteresse des Staates als auch die Belange der betroffenen Grundrechtsträger in Abwägung gebracht wurden, dürfen die Befugnisse der Strafverfolgungsbehörden nicht ohne die flankierenden Verfahrensvorschriften „gedacht“ und angewandt werden. Das Beachten der „befugnisbegleitenden“ Verfahrensvorschriften ist verfassungsrechtlich zwingende Voraussetzung der rechtmäßigen Anwendung der Eingriffsbefugnisse. Darüber hinaus ist die strenge Einhaltung grundrechtsschützender Vorschriften für das Vertrauen in rechtstaatliches Handeln der Strafverfolgungsbehörden unverzichtbar.

Erwähnen möchte ich, dass das Landeskriminalamt und die betroffene Staatsanwaltschaft die Vorgänge zum Anlass genommen haben, die Maßnahmen kritisch auszuwerten, Verfahrensabläufe zu überprüfen und Verbesserungen anzustoßen und ihre Mitarbeiter zu sensibilisieren. Erforderlich erscheinen mir insbesondere Verbesserungen bei der Umsetzung von gesetzlich geforderten Löschungsverpflichtungen, insbesondere bei der Übermittlung der entsprechenden Verfügungen an die Polizei. Hier böte sich, wie etwa die Mitteilung der Staatsanwaltschaft an die Polizei zum Ausgang des Verfahrens, ein standardisierter Benachrichtigungsweg an.

Der Vorgang veranschaulicht besonders deutlich die Gefahren einer umfangreichen Datenerhebung und der Nutzung eines stetig anwachsenden Datenbestandes. Ohne dass Personen auch nur entfernt an Straftaten beteiligt sind, sind sie bei einer Vielzahl von erhobenen Daten, die in einem wachsenden Bestand zusammengefasst und immer wieder untereinander und mit neu hinzukommenden Daten abgeglichen werden, möglicherweise allein durch ihren Aufenthaltsort oder ihre Berufsausübung einem sich stetig erhöhenden Risiko ausgesetzt, (mehrfach) erfasst und allein dadurch zu einer Person von (Ermittlungs-)Interesse zu werden.

8.6 Abschalten der Videoüberwachung der Chemnitzer Innenstadt bei Versammlungen

Im Zuge der Projektierung und Einführung der Videoüberwachung größerer Bereiche der Chemnitzer Innenstadt, über die ich im Tätigkeitsbericht 2018 (4.2.1, 8.1) informiert hatte, diskutierte ich im zweiten Halbjahr 2019 mit dem Sächsischen Staatsministerium des Innern intensiv über das Verhältnis von polizeilichen Eingriffsbefugnissen nach dem Sächsischen Versammlungsgesetz einerseits und dem Sächsischen Polizeigesetz (nun: Sächsisches Polizeivollzugsdienstgesetz) andererseits. Der Kern der Diskussion lag in der Frage, ob bei Versammlungen, die im überwachten öffentlichen Raum der Chemnitzer Innenstadt stattfinden, Bildaufnahmen ausschließlich auf Grundlage von § 20 SächsVersG gefertigt werden dürfen und die permanente Bildaufzeichnung der Kriminalitätsschwerpunkte in diesem Zeitraum deaktiviert werden muss, oder ob die letztere auch während Versammlungen erfolgen dürfe und Versammlungsteilnehmer dies zu dulden haben.

Im April bzw. Anfang Mai 2019 hatte ich der Stadt Chemnitz und der Polizeidirektion meine Auffassung mitgeteilt, dass bei von Artikel 8 GG geschützten Versammlungen allein die Rechtsvorschrift des § 20 SächsVersG bestimmt, unter welchen Voraussetzungen die Polizei Bildaufnahmen von Personen bei oder im Zusammenhang mit einer öffentlichen Versammlung unter freiem Himmel oder einem Aufzug anfertigen darf. Liegen die dort genannten Voraussetzungen nicht vor, sind Bildaufnahmen auch nach polizeigesetzlichen Vorschriften über die Videoüberwachung öffentlichen Raums unzulässig, da die versammlungsrechtliche Vorschrift als speziellere Regelung für Versammlungssituationen die Vorschrift aus dem allgemeinen Polizeigesetz verdrängt. Die Aufnahme und Aufzeichnung von Bildern der als Kriminalitätsschwerpunkt überwachten Bereiche ist daher auszusetzen, die Anlagen sind abzuschalten, soweit und solange dort Versammlungen

stattfinden. In diesem Zeitraum darf allein der Polizeivollzugsdient Bildaufnahmen nur dann fertigen, wenn und solange im Einzelfall die Voraussetzungen von § 20 SächsVersG vorliegen.

Das Sächsische Staatsministerium des Innern hingegen vertrat ausweislich der Antwort der Staatsregierung auf eine parlamentarische Anfrage ebenfalls Ende April 2019 die Auffassung, dass eine allgemeine Aussage zu der Frage, ob Bild- und Tonaufnahmen von Versammlungen an Orten stationärer Videoüberwachung nach § 37 Absatz 2 SächsPolG gegen § 20 SächsVersG verstießen, wenn von der Versammlung selbst kein Anlass zur Anfertigung von Bild- und Tonaufnahmen ausgehe, nicht getroffen werden könne. Es bedürfe einer Prüfung im Einzelfall (Landtagsdrucksache 6/17184).

Im Oktober 2019 kamen die Stadt und die Polizeidirektion Chemnitz in einer gemeinsamen Besprechung überein, dass die Polizei bei Versammlungslagen nicht mehr bzw. nur noch in Ausnahmefällen Kameras abzuschalten, da der Schutzbereich von Artikel 8 GG nicht betroffen sei und auch kein faktischer Eingriff in das Grundrecht auf Versammlungsfreiheit vorliege. Leider erreichte mich diese Information erst im April 2020.

Der Auffassung der Stadt und der Polizeidirektion Chemnitz muss ich entschieden entgegentreten.

Es ist seit Jahren höchstrichterlich geklärt, dass staatliche Eingriffe in das Grundrecht auf Versammlungsfreiheit nach Artikel 8 GG auch dann anzunehmen sind, wenn das staatliche Handeln nicht direkt auf die Versammlung als solche bzw. deren Teilnehmer abzielt, sondern „nur“ mittelbar Auswirkungen auf die Versammlung oder deren – ggf. auch potentielle – Teilnehmer hat. Solche „faktischen Eingriffe“ in den Schutzbereich des Grundrechts liegen dann vor, wenn behördliche Maßnahmen in ihrer Intensität gezielten versammlungsrechtlichen „Maßnahmen gleichstehen und eine abschreckende oder einschüchternde Wirkung entfalten bzw. geeignet sind, die freie Willensbildung und die Entschließungsfreiheit derjenigen Personen zu beeinflussen, die an Versammlungen teilnehmen (wollen)“ (OVG Münster, Beschluss vom 13.03.2020 - 15 B 332/20, mit weiteren Nachweisen, u. a. auf BVerfG vom 7.11.2015 – 2 BvQ 39/15 und vom 11.06.1991 – 1 BvR 772/90). Ob die in Frage stehenden behördlichen Maßnahmen eine solche Wirkung entfalten, bemisst sich nach einem objektiven Beurteilungsmaßstab. Jedenfalls bei einer polizeilichen, aber auch ordnungsbehördlichen permanenten Videoüberwachung des öffentlichen Raums, in dem die Versammlung stattfindet bzw. stattfinden soll, steht eine

potentiell einschüchternde und die Versammlungsfreiheit der (potentiellen) Teilnehmer beeinträchtigende Wirkung außer Frage (vgl. OVG Münster a.a.O.).

Die Videoüberwachung begründet für Teilnehmer an einer Versammlung das Bewusstsein, dass ihre Teilnahme und die Form ihrer Beiträge unabhängig von einem zu verantwortenden Anlass festgehalten werden können und die so gewonnenen Daten über die konkrete Versammlung hinaus verfügbar bleiben. Dabei handelt es sich überdies um sensible Daten. In Frage stehen Aufzeichnungen, die die gesamte - möglicherweise emotionsbehaftete - Interaktion der Teilnehmer optisch fixieren und geeignet sind, Aufschluss über politische Auffassungen sowie weltanschauliche Haltungen zu geben. Das Bewusstsein, dass die Teilnahme an einer Versammlung in dieser Weise festgehalten wird, kann Einschüchterungswirkungen haben, die zugleich auf die Grundlagen der demokratischen Auseinandersetzung zurückwirken. Denn wer damit rechnet, dass die Teilnahme an einer Versammlung behördlich registriert wird und dass ihm dadurch persönliche Risiken entstehen können, wird möglicherweise auf die Ausübung seines Grundrechts verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil die kollektive öffentliche Meinungskundgabe eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten demokratischen und freiheitlichen Gemeinwesens ist (BVerfG, Einstweilige Anordnung vom 17.02.2009 – 1 BvR 2492/08).

Wird öffentlicher Raum als Kriminalitätsschwerpunkt nach polizeigesetzlichen Vorschriften permanent videoüberwacht, greift diese Maßnahme also auch in das Grundrecht auf Versammlungsfreiheit nach Artikel 8 GG ein, wenn in diesem öffentlichen Raum eine Versammlung stattfindet. Unerheblich ist dabei, ob die polizeirechtliche Maßnahme ursprünglich (und eigentlich) einem anderen Zweck dient als der Überwachung einer Versammlung.

Natürlich obliegt dem Staat die Aufgabe, Gefahren für die öffentliche Sicherheit abzuwehren, auch in Versammlungslagen. Der Schutz von Artikel 8 GG ist nicht absolut. Eingriffe sind auf gesetzlicher Grundlage erlaubt; einschlägig sind im Freistaat Sachsen die Vorschriften des Sächsischen Versammlungsgesetzes. Bild- und Tonaufnahmen darf der Polizeivollzugsdienst unter den Voraussetzungen von § 20 SächsVersG anfertigen. Die Intensität der speziellen versammlungsrechtlichen Eingriffe, die der Gesetzgeber mit Blick auf das Grundrecht der Versammlungsfreiheit für erforderlich hält und zulässt, bildet Maßstab und Rahmen auch für andere behördliche Maßnahmen, die zwar nicht die

Versammlung als solche in den Blick nehmen und auf versammlungsrechtliche Vorschriften gestützt werden, die aber – eben im Wege des „faktischen Grundrechtseingriffs“ – geeignet sind, die Rechte der Versammlungsteilnehmer zu beeinträchtigen.

Die Befugnisse des Polizeivollzugsdienstes, personenbezogene Bildaufnahmen einerseits im Rahmen der Überwachung von sog. Kriminalitätsschwerpunkten (§ 57 Absatz 3 Nummer 2 SächsPVDG) und anderseits bei oder im Zusammenhang mit einer öffentlichen Versammlung unter freiem Himmel (§ 20 Absatz 1 SächsVersG) anzufertigen, stehen daher nicht gleichrangig nebeneinander. Im Fall einer Versammlung im Sinne von Artikel 8 GG auf einem nach § 57 Absatz 3 Nummer 2 SächsPVDG überwachten Areal verdrängt § 20 SächsVersG als spezielle und damit vorrangige Rechtsvorschrift die Erhebungsbefugnis aus dem allgemeinen Polizeivollzugsdienstgesetz.

Aufgrund der Spezialität des Versammlungsgesetzes und aufgrund des Grundsatzes der "Polizeifestigkeit" des Versammlungsrechts ist der Rückgriff auf allgemeinere Rechtsgrundlagen für polizeiliche Gefahrenabwehrmaßnahmen während der Versammlung jedenfalls dann von vornherein ausgeschlossen, wenn es eine abschließende und damit speziellere Ermächtigungsgrundlage im Versammlungsgesetz gibt (BVerfG, Beschluss vom 26.10.2004 – 1 BvR 1726/01.

Im Fall des § 57 Absatz 3 Nummer 2 SächsPVDG tritt zur Verdrängung durch § 20 SächsVersG „erschwerend“ hinzu, dass es sich um gar keine echte Gefahrenabwehrmaßnahme handelt, vgl. dazu VGH Baden-Württemberg zur Videoüberwachung in der Innenstadt von Mannheim: „Dabei ist allerdings hervorzuheben, dass es […] um einen polizeirechtlichen Eingriffstatbestand geht, der – abweichend vom ‚klassischen‘ Polizeirecht – nicht an eine konkrete polizeiliche Gefahr für die öffentliche Sicherheit oder Ordnung anknüpft, sondern lediglich an ein gewisses "Gefährdungspotential" bzw. die potentielle Gefährlichkeit des überwachten Ortes.“ (VGH Baden-Württemberg, Urteil vom 21. Juli 2003 – 1 S 377/02 juris). Die Vorschrift zur Videoüberwachung von Kriminalitätsschwerpunkten knüpft also nicht an ein störendes Verhalten Betroffener an, vielmehr werden von der Videokamera unterschiedslos alle Personen erfasst, die sich in ihrer Reichweite aufhalten.

Wenn aber bei Versammlungen Gefahrenabwehrbefugnisse aus dem allgemeinen Polizeigesetz jedenfalls hinter ausdrücklich geregelten Gefahrenabwehrbefugnissen aus dem

Versammlungsrecht zurücktreten müssen (s.o.), dann muss dies erst recht für Maßnahmen aus dem allgemeinen Polizeigesetz gelten, die nicht einmal an eine konkrete Gefahr für die öffentliche Sicherheit oder Ordnung anknüpfen. Auch in diesem Zusammenhang ist allein die spezielle versammlungsrechtliche Eingriffsvoraussetzung entscheidend: § 20 Absatz 1 SächsVersG erlaubt bei oder im Zusammenhang mit einer öffentlichen Versammlung unter freiem Himmel oder einem Aufzug die Anfertigung von Bild- und Tonaufnahmen nur dann, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass von diesen Personen eine erhebliche Gefahr für die öffentliche Sicherheit und Ordnung bei oder im Zusammenhang mit der Versammlung ausgeht. Gefahren unterhalb der Schwelle der erheblichen Gefahr für die öffentliche Sicherheit und Ordnung können damit keinesfalls Bildaufnahmen von Versammlungsteilnehmern rechtfertigen, ganz gleich, welche Rechtsgrundlage herangezogen würde.

Die Verfassungsnormen und einfachgesetzlichen Regelungen sowie die ständige verfassungs- und verwaltungsgerichtliche Rechtsprechung lassen im Ergebnis keine Zweifel daran zu, dass die sächsische Polizei auch im öffentlichen Raum, der als Kriminalitätsschwerpunkt dauerhaft überwacht werden darf, Bildaufnahmen von Versammlungsteilnehmern ausschließlich auf Grundlage und unter den Voraussetzungen von § 20 SächsVersG anfertigen darf. Für die Dauer der Versammlung und soweit diese betroffen ist, ist die Beobachtung des öffentlichen (Versammlungs-)Raums nach § 57 Absatz 3 Nummer 2 SächsPVDG daher auszusetzen.

Der Vorrang versammlungsrechtlicher Eingriffsbefugnisse und der korrespondierende temporäre Ausschluss der Anwendung anderer Eingriffsbefugnisse mit gleicher Wirkung entfalten selbstverständlich nicht nur für den Polizeivollzugsdienst Wirkung, sondern auch für Kommunen als Stellen der öffentlichen Gewalt, soweit sie öffentlichen Raum überwachen, in dem von Artikel 8 GG geschützte Versammlungen stattfinden (sollen). Die obigen Ausführungen zum Verhältnis der Anfertigung von Bildaufnahmen nach § 20 SächsVersG und der Videoüberwachung öffentlichen Raums nach § 57 Absatz 3 Nummer 2 SächsPVDG gelten in gleichem Maße für das Verhältnis von Versammlungsrecht und allgemeinen Befugnissen öffentlicher Stellen (bzw. Ortspolizeibehörden) für Videoüberwachung öffentlichen Raums nach § 13 SächsDSDG oder § 30 SächsPBG. Neben die prinzipielle Verdrängung anderer Vorschriften durch explizite Regelungen des Versammlungsrechts tritt hierbei noch die einfachgesetzliche Bestimmung des § 32 Absatz 2 Nummer 6 SächsVersG, die bestimmt, dass die Zuständigkeit für die Fertigung von Bild- und Tonaufnahmen nach § 20 Absatz 1 und von Übersichtsbildübertragungen nach § 20

Absatz 2 SächsVersG (ausschließlich) beim Polizeivollzugsdienst liegt. Kommunale Polizeibehörden dürfen also selbst dann keine Bildaufnahmen von Versammlungen anfertigen, wenn die Voraussetzungen von § 20 SächsVersG vorliegen.

Für die Videoüberwachung der Chemnitzer Innenstadt hat das zur Folge, dass die Kameras, die den öffentlichen Raum erfassen, in dem eine von Artikel 8 GG geschützte Versammlung stattfindet, für die Zeit der Versammlung abgeschaltet werden müssen. Es ist sicherzustellen, dass keine Bildaufnahmen gefertigt werden, unabhängig davon, ob sie der Live-Beobachtung dienen oder zunächst nur gespeichert werden sollen.

Ausschließlich der Polizeivollzugsdienst darf während der Versammlung nur unter den Voraussetzungen von § 20 Absatz 1 SächsVersG Bild- und Tonaufnahmen anfertigen. Ein Zugriff der Stadt auf diese Bilder ist gesetzlich nicht zulässig.

8.7 Umgang des Landesamtes für Verfassungsschutz mit von Versammlungsbehörden übersandten Versammlungsanzeigen

Im Rahmen der datenschutzrechtlichen Prüfung einer Beschwerde bin ich darauf aufmerksam geworden, dass mindestens eine sächsische Versammlungsbehörde in der Vergangenheit Versammlungsanzeigen (§ 14 Absatz 1 SächsVersG) mit darin enthaltenen personenbezogenen Daten des oder der Anmelder ohne konkreten Anlass, das heißt ohne Anhaltspunkte für ein erhöhtes Gefährdungspotential insbesondere bei vermuteter Beteiligung extremistischer Personen oder Gruppen, an das Landesamt für Verfassungsschutz übermittelt hat. Das Landesamt für Verfassungsschutz wurde also generell über angemeldete Versammlungen informiert, Versammlungsanzeigen wurden gewissermaßen „automatisch durchgereicht“.

Ein solches Vorgehen ist angesichts der Bedeutung der Versammlungsfreiheit (Artikel 8 des Grundgesetzes) für den demokratischen Rechtstaat und des Grundrechts auf informationelle Selbstbestimmung der Anmelder sowie mit Blick auf die einfachgesetzlichen Voraussetzungen für Übermittlungen personenbezogener Daten an das Landesamt für Verfassungsschutz (im Sächsischen Versammlungsgesetz und im Sächsischen Verfassungsschutzgesetz) nicht zulässig. Sowohl versammlungsrechtlich notwendige Gefahrermittlungsmaßnahmen der Versammlungsbehörde, die Anfragen beim Landesamt für Verfassungsschutz rechtfertigen können, als auch Übermittlungsvorschriften bzw. -pflichten

nach dem Verfassungsschutzgesetz setzen der Versammlungsbehörde vorliegende Anhaltspunkte für eine besondere Gefährdung im Zusammenhang mit der angemeldeten Versammlung voraus. Eine nähere datenschutzrechtliche Bewertung dieses Aspekts finden Sie im Beitrag 2.2.9.

Neben der Frage der Rechtmäßigkeit solcher genereller Übermittlungen von Versammlungsanzeigen an das Landesamt für Verfassungsschutz interessierte mich auch der Umgang des Landesamt für Verfassungsschutz mit solchen Meldungen, war doch stark zu vermuten, dass ein nicht unerheblicher Teil der in den von der Versammlungsbehörde übermittelten Anzeigen genannten Anmelder keine extremistischen Bestrebungen verfolgte und sich nicht im gesetzlich bestimmten Beobachtungsfeld des Landesamt für Verfassungsschutz bewegte. Insoweit bestanden selbstverständlich auch nicht abwegige Befürchtungen von betroffenen Versammlungsanmeldern, in Datensammlungen des Verfassungsschutzes aufzutauchen, ohne dafür Anlass gegeben zu haben.

Gegen die mir durch das Landesamt für Verfassungsschutz geschilderte Vorgehensweise hatte ich im Ergebnis keinerlei Einwände:

Das Landesamt für Verfassungsschutz Sachsen prüft gemäß § 14 Absatz 1 SächsVSG unverzüglich, ob die ihm übermittelten personenbezogenen Daten auch für die eigene Aufgabenerfüllung erforderlich sind. Ist dies nicht der Fall, würden die Daten vernichtet. Dies gelte z. B. für Informationen zu Veranstaltungen, bei denen kein Bezug zum Extremismus festgestellt werden könne. Die entsprechenden Unterlagen (Anmeldungen, Bescheide etc.) würden vernichtet.

Stellt das Landesamt für Verfassungsschutz bei einer übermittelten Versammlungsanmeldung allerdings Zusammenhänge mit bereits bestehenden Beobachtungsvorgängen fest, darf es auch personenbezogene Angaben zur durch die Versammlungsbehörde mitgeteilten Versammlungsanmeldung speichern, § 6 Absatz 1 Nummer 1 i. V. m. § 2 Absatz 1 SächsVSG.

Es ist gut zu wissen, dass datenschutzwidriges Handeln einer Stelle nicht unbedingt zu einem dauerhaften und sich möglicherweise sich verstärkenden Grundrechtseingriff bei den betroffenen Personen führt, sondern durch sorgfältige Beachtung gesetzlicher Vorschriften bei anderen beteiligten Stellen „geheilt“ werden kann. Gleichwohl bleibt die exakte Einhaltung gesetzlicher Vorgaben selbstverständlich oberstes Gebot für jede einzelne an Gesetz und Recht gebundene staatliche Stelle.

9 Rechtsprechung zum Datenschutz

9.1 Das Ende des Videoüberwachungsverbesserungsgesetzes im nicht-öffentlichen Bereich – BVerwG, Urteil vom 27. März 2019, 6 C 2/18

Im April 2017 hatte der Bundestag das sogenannte „Videoüberwachungsverbesserungsgesetz“ beschlossen, welches zu einer Änderung des seinerzeitigen § 6b BDSG – nach alter Fassung - führte. Ziel war es, beim Einsatz von „Videoüberwachung in öffentlich zugänglichen großflächigen Anlagen wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen sowie in Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs“ festzuschreiben, „dass der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse gilt". Privaten Betreibern von Videoüberwachungsanlagen sollte es damit erleichtert werden, Videoüberwachungseinrichtungen zu installieren, um auch im öffentlichen Interesse die Sicherheit der Bevölkerung präventiv zu erhöhen , während Datenschützer und Bürgerrechtler die damit bezweckte Ausweitung der Videoüberwachung kritisch betrachteten. Vor dem zeitaktuellen Hintergrund des Amoklaufs in einem Münchner Einkaufszentrum im Juni 2016 mit neun Toten blieben bürgerrechtliche Aufklärungsbemühungen gegenüber den zur Begründung des Gesetzes beschriebene Bedrohungslage, dass Terroristen und Straftäter für Anschläge auch hochfrequentierte öffentlich zugängliche Anlagen in ihren Fokus nehmen, um größtmöglichen Schaden anzurichten und öffentliche Aufmerksamkeit zu erlangen (vgl. Bundestags-Drucksache 8/10941, Seite 1), ohne Erfolg.

Am 25. Mai 2018 ist dann zeitgleich mit der verbindlichen Anwendung der DSGVO auch das grundlegend novellierte Bundesdatenschutzgesetz in Kraft getreten. Dabei waren gerade die oben beschriebenen Regelungen des § 6b BDSG der alten Fassung wortgleich in § 4 BDSG (neue Fassung) übernommen worden. Auch dies war von Anfang an streitig gewesen. Gegenstand der Diskussion war dabei vor allem die für diese nationale Regelung erforderliche Öffnungsklausel in der DSGVO. Einen Regelungsspielraum für die nationalen Gesetzgeber war gemäß Artikel 6 Absatz 2 DSGVO nur für öffentliche Stellen, nicht aber für nicht-öffentliche Stellen, die sich weder auf Artikel 6 Absatz 1 Satz 1 Buchstabe c) noch auf Buchstabe e) der Verordnung stützen können, sondern regelmäßig Buchstabe f) anzuwenden haben, vorgesehen.

Im März 2019 hat das Bundesverwaltungsgericht (BVerwG, Urteil vom 27. März 2019 – 6 C 2/18 –, juris) dann aber das *Videoüberwachungsverbesserungsgesetz* in seiner Geltung für den nicht-öffentlichen Bereich doch noch gestoppt. In dem durch das Bundesverwaltungsgericht zu beurteilenden Fall ging es eigentlich um eine noch auf Grundlage des alten Rechts (BDSG) getroffene Anordnung der *Brandenburgischen Beauftragten für Datenschutz und für das Recht auf Akteneinsicht* zur datenschutzkonformen Ausrichtung der Videoüberwachung in einer Zahnarztpraxis. Ganz am Ende dieser Entscheidung hat sich das Gericht dann aber auch mit der zwischenzeitlich anwendbaren DSGVO auseinandergesetzt und klargestellt, dass die – die Aufsichtsbehörde im Übrigen bestätigende – Entscheidung aber auch nach neuer Rechtslage so Bestand gehabt hätte. In diesem Zusammenhang hat das Bundesverwaltungsgericht insbesondere klar zum Ausdruck gebracht, dass die nationale Regelung des deutschen Gesetzgebers zur Privilegierung der privaten Videoüberwachung in § 4 BDSG europarechtswidrig und im Ergebnis nicht (mehr) anwendbar sei. Die Videoüberwachung durch private Stellen sei stattdessen ausschließlich am europäischen Datenschutzrecht zu messen; die DSGVO regele die Videoüberwachung durch Private abschließend. Nicht-öffentliche Stellen könnten Videokameras daher nur noch auf die Rechtsgrundlage des Artikel 6 Absatz 1 Buchstabe f) DSGVO stützen. Die danach zu erfolgende Güterabwägung sei nicht durch nationales Recht modifizierbar.

Konkret hat das Bundesverwaltungsgericht in Randziffer 47 der Urteilsbegründung ausgeführt, dass die Öffnungsklauseln des Artikel 6 Absätze 2 und 3 DSGVO für Verarbeitungen nach Artikel 6 Absatz 1 Satz 1 Buchstabe e) DSGVO Videoüberwachungen privater Verantwortlicher nicht erfassen. Aufgrund dessen sei kein Raum für eine künftige Anwendung des § 4 Absatz 1 Satz 1 BDSG. Dieser sei an Artikel 6 Absatz 1 Satz 1 Buchstabe f) DSGVO zu messen. Danach muss die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich sein, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Eine nach diesem Maßstab erforderliche Verarbeitung sei zulässig, wenn die Abwägung in dem jeweiligen Einzelfall ergibt, dass berechtigte Interessen des Verantwortlichen höher zu veranschlagen sind als das informationelle Selbstbestimmungsrecht der Betroffenen. Hierfür sei nach Erwägungsgrund 47 zur DSGVO unter anderem bedeutsam, ob die Datenverarbeitung für die Verhinderung von Straftaten unbedingt erforderlich ist, ob sie absehbar, das heißt branchenüblich ist, oder ob die Betroffenen in der konkreten Situation vernünftigerweise damit rechnen müssen, dass ihre Daten verarbeitet werden.

Für Verantwortliche, die ihre Videoüberwachung in der Vergangenheit nicht ausdrücklich auf eine der in § 4 Absatz 1 Satz 2 Nummer 2 und 3 BDSG genannten Voraussetzungen gestützt, sondern § 4 BDSG vielmehr bereits europarechtskonform ausgelegt und die dort enthaltene Interessenabwägung schon im Lichte des Artikel 6 Absatz 1 Satz 1 Buchstabe f) DSGVO durchgeführt haben, sollten die Auswirkungen dieses Urteils überschaubar bleiben. Im Übrigen gilt, dass Verantwortliche sich jetzt jedenfalls nicht mehr unmittelbar auf das Hausrecht (§ 4 Absatz 1 Satz 1 Nummer 2 BDSG) berufen können. Stattdessen müssen sie auch dieses nunmehr als berechtigtes Interesse darstellen. Dies sollte realisierbar sein, zumal sich die Rechtfertigungsgründe "Hausrecht" und "berechtigte Interessen" ohnehin nicht strikt voneinander abgrenzen lassen, sondern inhaltlich überschneiden. Auch dies ist dem Urteil des Bundesverwaltungsgerichts (Randziffer 25) zu entnehmen Das Gericht legt dar, dass das Hausrecht das Mittel ist, das den an einem Raum Berechtigten in die Lage versetzt, darüber zu bestimmen, ob und zu welchem Zweck andere Personen den Raum betreten und sich darin aufhalten dürfen. Der Berechtigte könne zwar aufgrund seines Hausrechts missliebiges Verhalten zum Anlass nehmen, Besuchern "die Tür zu weisen". Allerdings zeige die Regelungssystematik des § 6b Absatz 1 BDSG (alte Fassung) bzw. des § 4 Absatz 1 Satz 1 BDSG (neue Fassung), dass er sich nicht beliebig auf das Hausrecht berufen kann, um eine Videoüberwachung durchzuführen. Vielmehr müsse er sich auf ein berechtigtes Interesse, d. h. auf einen "guten Grund" stützen können. Dies könne jedes subjektive Interesse sein, wenn es grundsätzlich schutzwürdig und objektiv begründbar ist.

In Bezug auf die Kennzeichnung einer Videoüberwachung und die diesbezüglichen Informationspflichten (Hinweisschilder Stufen 1 und 2, [Verweis – Ordnungsnummer vgl. 10.1]) ist somit zu beachten, dass bei den Angaben nach Artikel 13 Absatz 1 Buchstabe c) DSGVO alle Verweise auf § 4 BDSG nunmehr obsolet und folglich zu streichen sind. Ich empfehle Verantwortlichen daher, ihre Hinweisschilder bei passender Gelegenheit auf den aktuellen Stand zu bringen.

9.2 Verwaltungsgerichtliche Entscheidungen in Verfahren unter Beteiligung des Sächsischen Datenschutzbeauftragten

Im Berichtszeitraum ist die Entscheidung in einem noch aus dem Jahr 2017 stammenden Klageverfahren gefallen. Inhaltlich ging es um die Festsetzung zweier Zwangsgelder in einem Auskunftsheranziehungsverfahren.

Ausgangspunkt war die mir angezeigte Videoüberwachung in einer Gaststätte nebst dazugehörigen Spiel-Café in der Leipziger Eisenbahnstraße. Ich hatte den Großteil der für mich wesentlichen Aspekte der – im Ergebnis überwiegend unzulässigen – Videoüberwachung bereits in einer gemeinsam mit der Polizei durchgeführten unangekündigten Anlasskontrolle ermittelt, allerdings waren dabei u. a. wegen der Abwesenheit eines der beiden Geschäftsinhaber noch einige wenige Fragen offen geblieben. Diese Fragen versuchte ich anschließend auf schriftlichem Wege zu klären. Bei den Geschäftsinhabern handelte es sich um zwei Brüder, von denen der bei meiner Kontrolle anwesende behauptet hatte, Betreiber der Videoüberwachungsanlage zu sein.

Nachdem die beiden Geschäftsinhaber auf mein diesbezügliches Anschreiben zunächst nicht reagiert hatten, erließ ich gegen den mir bereits persönlich bekannten Geschäftsinhaber einen Heranziehungsbescheid. Als einzige Reaktion auf diesen Bescheid erhielt ich ein Fax des anderen Geschäftsinhabers, das lediglich die nicht weiter kommentierte Mitteilung enthielt, dass (anders als bisher dargestellt) er die für die den Gewerbebetrieb und damit auch die Videoüberwachung verantwortliche Person sei. Weitere Auskünfte wurden nicht erteilt. Ich sah mich daher gezwungen, nun auch noch gegen den zweiten Geschäftsinhaber einen Heranziehungsbescheid zu erlassen. Nachdem – ohne dass die fehlenden Auskünfte erteilt worden wären – beide Heranziehungsbescheide bestandskräftig geworden waren, habe ich daraufhin – wie in den Bescheiden angekündigt – entsprechende Zwangsgelder festgesetzt. Gegen diese Festsetzungsbescheide hatte dann einer – inzwischen anwaltlich vertretener – der Brüder (im Folgenden: Kläger) dann aber Anfechtungsklage erhoben und die Aufhebung der Festsetzungsbescheide begehrt.

Im weiteren Verlauf hat der Kläger dann seine Klage aber selbst nach mehreren Fristverlängerungsanträgen nicht weiter begründet, sondern stattdessen mit Verweis auf durch mich inzwischen parallel gegen beide Geschäftsinhaber wegen Verstoßes gegen die Auskunftspflichten einerseits und unzulässiger Videoüberwachung andererseits eingeleitete Ordnungswidrigkeitenverfahren gegen über dem Gericht angeregt, gemäß § 173 Satz 1 VwGO in Verbindung mit § 251 ZPO das Ruhen des Verfahrens anzuordnen. Ich habe mich diesem Antrag nicht angeschlossen, sondern dem Ruhen des Verfahrens widersprochen. Auch für ein Ruhen in analoger Anwendung von § 94 VwGO habe ich keinen Raum gesehen. Ist – was hier der Fall war – in dem anderen Verfahren kein Rechtsverhältnis zu klären, sondern stellt sich dort lediglich die gleiche Rechtsfrage, ist eine Vorgreiflichkeit nicht gegeben (BVerwG, Urteil vom 11. Februar 2009, 2 A 7/06, Rz. 34; OVG Lüneburg, Beschluss vom 22. Juli 2013, 5 OB 146/13, Rz. 8, jeweils in: juris).

Daraufhin hat der Kläger dann sowohl das Zwangsgeld bezahlt als auch – dem Verwaltungsgericht gegenüber – die noch offenen Auskünfte erteilt. Damit waren alle Forderungen des streitgegenständlichen Festsetzungsbescheides erfüllt.

Die vom Kläger geforderte Rücknahme des Festsetzungsbescheides habe ich gleichwohl ausgeschlossen. Dieser Bescheid beruhte auf einem bestandskräftigen Heranziehungsbescheid und war (daher) rechtmäßig erlassen worden.

Soweit der Kläger auch den an seinen Bruder adressierten Festsetzungsbescheid angefochten und an das Verwaltungsgericht auch diesbezüglich Auskünfte erteilt hatte, war klarzustellen, dass ihn dieser Bescheid gar nicht in seinen Rechten verletzt hatte, er somit gar nicht klagebefugt war (§ 42 Absatz 2 VwGO). Dieser Festsetzungsbescheid war daher auch schon weit vorher bestandskräftig geworden.

Nach alledem hat der Kläger dann schließlich im Mai 2019 seine Klagerücknahme erklärt. Unmittelbar danach ist durch das Verwaltungsgericht folgerichtig der Beschluss ergangen, dass das Verfahren eingestellt wird (§ 92 Absatz 3 Satz 1 VwGO). Die Verfahrenskosten hatte der Kläger zu tragen (§ 155 Absatz 2 VwGO).

9.3 Zur Frage, ob Betriebsräte eigene Verantwortliche gemäß Artikel 4 Nummer 7 DSGVO sind

In Bezug auf die Frage, ob Interessenvertretungen als Verantwortliche gemäß Artikel 4 Nummer 7 DSGVO anzusehen sind, hatte ich mich bereits in meinem zurückliegenden Tätigkeitsbericht positioniert, vergleiche auch den Beitrag aus dem Tätigkeitsbericht 2017/2018 Teil 2, 2.1.1.

Zwischenzeitlich waren im letzten Berichtszeitraum mehrere Entscheidungen von Landesarbeitsgerichten ergangen. In zwei landesarbeitsgerichtlichen Entscheidungen zu Betriebsräten wurden diese als Verantwortliche im Sinne der DSGVO angesehen: Das Landesarbeitsgericht Sachsen-Anhalt stellte in seiner Entscheidung vom 18. Dezember 2018, Aktenzeichen 4 TaBV 19/17, fest, dass der Betriebsrat ein eigener Verantwortlicher gemäß Artikel 4 Nummer 7 DSGVO sei, Rdnr. 51. Rechtsbeschwerde gegen die Entscheidung wurde eingelegt und über diese wurde noch nicht entschieden. Das Landesarbeits-

gericht Mecklenburg-Vorpommern folgte in einem Beschluss vom 15. Mai 2019, Aktenzeichen 3 TaBV 10/18 auch dieser Auffassung, Rdnr. 21. Rechtsbeschwerde gegen die Entscheidung wurde nicht zugelassen.

Demgegenüber vertrat das Landesarbeitsgericht Niedersachsen in einem Beschluss vom 22. Oktober 2018 gegenteiliges, 12 TaBV 23/18, in dem ausgeführt wurde, dass so solange sich der Betriebsrat im Rahmen der Wahrnehmung seiner gesetzlichen Aufgaben bewegen, es sich nicht um einen „Dritten“ im Sinne von Artikel 4 Nummer 10 DSGVO handele, Rdnr. 46.

Das Bundesarbeitsgericht wiederum ließ in seinem Beschluss vom 7. Mai 2019, Aktenzeichen1 ABR 53/17, die interessierende Frage noch offen, Rdnr. 45.

Meine Dienststelle hat aufgrund der landesarbeitsgerichtlichen Entscheidungen in Sachsen-Anhalt bzw. Mecklenburg-Vorpommern ihre Rechtsmeinung nicht revidiert, dass es sich bei einem Betriebsrat um einen unselbstständigen Teil des Unternehmens handelt, der nicht als Verantwortlicher im Sinne von Artikel 4 Nummer 7 DSGVO anzusehen ist. Der Sächsische Datenschutzbeauftragte sieht sich zudem nicht an die oben aufgeführte landesarbeitsgerichtliche Rechtsprechung gebunden.

Die in der Entscheidung des Landesarbeitsgerichts Sachsen-Anhalt knapp thematisierte Überlassung von Informationen zur Aufgabenwahrnehmung des Betriebsrats als Grund, den Betriebsrat als Verantwortlichen anzusehen, überzeugt nach Auffassung meiner Behörde nicht. Gegenstand waren auch noch Informationen, die die Unternehmensleitung dem Betriebsrat zur Verfügung stellte, die also an anderer Stelle im Unternehmen bereits primär verarbeitet und geschützt aufbewahrt werden. Alleine mit der Überlassung von Informationen zur selbstständigen Aufgabenwahrnehmung kann eine Verantwortlichkeit im Sinne von Artikel 4 Nummer 7 DSGVO nach meiner Überzeugung nicht begründet werden. Der Betriebsrat bleibt insbesondere infrastrukturell bei der personenbezogenen Datenverarbeitung abhängig und datenschutzrechtlich zugeordnet. Da es viele weitere funktionale Stellen innerhalb von Unternehmen gibt, die informationell zwar abgeschottet und weitgehend weisungsfrei agieren, gleichwohl aber institutionell unselbstständig und Teile des Verantwortlichen bleiben, halte ich das Ergebnis auch in seinen möglichen Weiterungen in ähnlich gelagerten Fällen funktionaler Stellen für falsch. Die Annahme

einer Verantwortlichkeit würde im Übrigen auch bedeuten, dass die Betriebs- und Personalräte oder andere funktionale Stellen in gleichgelagerten Fällen eine Benennungspflicht in Bezug auf einen Datenschutzbeauftragten treffen könnte bzw. trifft.

9.4 Verwaltungsaktqualität datenschutzaufsichtlicher Verwarnungen, Artikel 58 Absatz 2 Buchstabe b) DSGVO - Verwarnung als feststellender Verwaltungsakt

In einer Entscheidung des Verwaltungsgerichts Hannover ging es um die Veröffentlichung einer Abbildung durch eine Partei zu Wahlwerbezwecken. Auf dem streitgegenständlichen Foto waren einzelne betroffene Personen erkennbar, die nicht eingewilligt hatten. Hierin erkannte die zuständige unabhängige Datenschutzaufsichtsbehörde des Landes Niedersachsen einen Datenschutzverstoß und sprach dem Verantwortlichen gegenüber eine Verwarnung aus, Artikel 58 Absatz 2 Buchstabe b) DSGVO. Die Entscheidung der Behörde hielt der gerichtlichen Überprüfung stand.

Verfahrensrechtlich war das Urteil vom 27. November 2019, 10 A 820/19, interessant, da es sich wohl um die erste Entscheidung eines deutschen Gerichts zum Rechtscharakter der Verwarnung nach der DSGVO handelte. Das Gericht stellte fest, dass, soweit der Kläger die Aufhebung der Verwarnung begehrt, als die zulässige Klageform die Anfechtungsklage statthaft ist, § 42 Absatz 1, 1. Fall VwGO. Die Verwarnung sei ein feststellender Verwaltungsakt. Diese Einschätzung halte ich für zutreffend, da der Verwarnung als Maßnahme der Datenschutzaufsichtsbehörde sowohl eine Missbilligung oder Beanstandung einer Handlung, als auch ein Verbot gleichartiger zukünftiger Handlungen innewohnt.

In der Sache, bei der es um die ohne Einwilligung erfolgte Veröffentlichung der Abbildung auf einer Internetplattform zu Zwecken der politischen Werbung ging, ließ das Gericht im Übrigen offen, ob die Unzulässigkeit der Verarbeitung personenbezogener Daten aus Artikel 6 Absatz 1 DSGVO oder auch aus § 23 Kunsturheberrechtsgesetz folgt, vergleiche auch den Berichtsbeitrag unter 9.5.

9.5 Verhältnis der DSGVO zum Kunsturheberrechtsgesetz

Nach einer nach dem Berichtszeitraum ergangenen Entscheidung des Bundesgerichtshofs sind die Bestimmungen des Kunsturheberrechtsgesetzes im journalistischen Bereich als

die Öffnungsklausel des Artikel 85 DSGVO ausfüllenden nationalen Gesetzgebung anzusehen, BGH – Urteil vom 7. Juli 2020, Az. VI ZR 246/19. Im Ergebnis zuvor ähnliche Entscheidung waren vom Oberlandesgericht Köln, unter anderem der Beschluss vom 8. Oktober 2018, Aktenzeichen 15 O 110/18, dem Urteil vom 18. Juni 2018, Aktenzeichen 15 W 27/18 sowie dem Urteil vom 10. Oktober 2019, Aktenzeichen 15 O 39/19, aber auch seitens des Landgerichts Frankfurt, Urteil vom 27. September 2018, Aktenzeichen 2-03 O 320/17 und Urteil vom 19. Dezember 2019, Aktenzeichen 2-03 O 6/19 ergangen.

Bisher offen bleibt noch das Verhältnis der DSGVO zum Kunsturheberrechtsgesetz in den Vorgängen, in denen eine Verarbeitung in Form einer Veröffentlichung von Bilddaten nicht zu journalistischen Zwecken erfolgt. Nach der Spruchpraxis meiner Behörde werden die Abwägungen im Rahmen der zumeist vorzunehmenden Abwägungsentscheidung gemäß Artikel 6 Absatz 1 Buchstabe f) DSGVO berücksichtigt. In der Praxis trägt dem unter anderem das Landgericht Frankfurt am Main, Urteil vom 13. September 2018, Aktenzeichen 2-03 O 283/18 und mit Urteil vom 26. September 2019, bei nicht gewerblicher bzw. nicht-journalistischer Verbreitung Rechnung.

Seitens des Bundesgesetzgebers sind mir keine Absichten zu einer weiteren Anpassung des Kunsturheberrechtsgesetzes an die DSGVO bekannt. Eine Auslegung nach den Vorgaben der DSGVO wird daher auf unbestimmte Zeit vorzunehmen sein.

9.6 Der Umfang des Auskunftsanspruchs gemäß Artikel 15 DSGVO, Landgericht Köln

Bereits in meinem letzten Tätigkeitsbericht 2017/2018 Teil 2, 9.6, hatte ich über die Frage des Umfangs des Auskunftsanspruchs anhand einer Entscheidung des Landesarbeitsgerichts Baden-Württemberg erörtert. In einer Entscheidung des Landgerichts Köln vom 18. März 2019, Aktenzeichen 26 O 25/18, wurde der Auskunftsanspruch des Betroffenen gemäß Artikel 15 Absatz 1 DSGVO eher restriktiv gesehen. Das Landgericht erkennt die Vorschrift des Artikel 15 DSGVO als Mittel, um Umfang und Inhalt der gespeicherten personenbezogenen Daten zu beurteilen, jedoch nicht um sämtliche internen Vorgänge beim Verantwortlichen, wie zum Beispiel den vollständigen gewechselten Schriftverkehr als Kopien ausgedruckt und übersandt zu bekommen, vergleiche Artikel 15 Absatz 3 DSGVO, dazu Rdnr. 21 der Entscheidung. Auch erkennt das Landgericht, dass rechtliche Bewertung oder Analysen keine personenbezogenen Daten im Sinne der Verordnung darstellen, Rdnr. 21. Auch meine Behörde neigt zu einer differenzierten Betrachtung.

Die Spruchpraxis der Gerichte zu Artikel 15 DSGVO betrachte ich allerdings noch als uneinheitlich. Eine herrschende Rechtsmeinung hat sich noch nicht herausgebildet.

9.7 Datenschutzrechtliche Zulässigkeit eines Ortungssystems im Beschäftigungsverhältnis, VG Lüneburg, Teilurteil vom 19. März 2019, 4 A 12/19

In meiner datenschutzaufsichtlichen Praxis erreichten mich auch im Berichtszeitraum nicht wenige Anfragen und Beschwerden zu von Arbeitgebern bzw. Dienstherrn eingesetzten Ortungssystemen, die an Betriebsmitteln oder Dienstfahrzeugen angebracht werden.

In einem Fall hatte das Verwaltungsgericht Lüneburg über die datenschutzrechtliche Zulässigkeit des Einsatzes eines Ortungssystems zu entscheiden, 19. März 2019, 4 A 12/19. Die zuständige Datenschutzaufsichtsbehörde des Landes Niedersachsen hatte gegenüber dem Verantwortlichen einen Bescheid auf Grundlage der Rechtslage des Bundesdatenschutzgesetzes alter Fassung erlassen. Das Gericht bestätigte die behördliche Anordnung gegenüber dem Gebäudereinigungsunternehmen, die Erhebung, Verarbeitung und Nutzung von Beschäftigungsdaten durch das Ortungssystem so einzurichten, dass eine personenbezogene Ortung während der ordnungsgemäßen betrieblichen Nutzung der Fahrzeuge nicht erfolgt. Die Behörde hielt die Einrichtung des Ortungssystems nicht für erforderlich und die Verarbeitung auf Einwilligung Basis aufgrund des Abhängigkeitsverhältnisses in der Beschäftigung beim Arbeitgeber für nicht umsetzbar. Das Gericht verneinte ebenso die Erforderlichkeit – Rdnr. 32 ff. – und stellte förmliche Mängel des Einwilligungsverfahrens fest, Rdnr. 57 ff.

Obwohl es sich um eine Entscheidung auf Grundlage der Bundesdatenschutzgesetzes in seiner alten Fassung handelt, hat das Urteil nach meiner Überzeugung seine rechtliche Relevanz, werden doch materiell-rechtlich die wiederkehrenden entscheidenden Fragen, die Erforderlichkeit, die Informiertheit, Fragen der Einwilligung beleuchtet. Verantwortlichen, die den Einsatz von Ortungssystemen planen, ist anzuraten, sich zuvor eingehend rechtlich und fachlich beraten zu lassen. Insbesondere die Schwelle der Erforderlichkeit wird nach meiner Einschätzung, gemessen an dem Umfang, der Tiefe und dem Ausmaß der Datenverarbeitung bei Ortungssystemen, eben gerade nicht niedrig angesetzt werden können.

9.8 Verdeckte Videoaufnahmen zur Aufdeckung von Missständen in Pflegeheimen

Im letzten Berichtszeitraum erreichte mich die Beschwerde, dass ein Hilfsunternehmen verdeckte Videoaufnahmen in einem Pflegeheim und Aufnahmen von Handlungen und in Wort und Bild durchführte und verfremdet publizierte. Die Beschwerdeführer wandten sich auch an meine Dienststelle. In der Sache war ich allerdings aufgrund Rundfunkrechts nicht zuständig, vergleiche auch 7. 1.1. Allerdings hatte sich das Oberlandesgericht Dresden mit Urteil vom 24. September 2019, 4 U 1401/19, mit dem Vorgang auseinanderzusetzen. Das Oberlandesgericht kam unter dem Hinweis, dass Mitarbeiter nicht vergleichbar schutzbedürftig seien, wie Bewohner der Pflegeeinrichtungen zu dem Ergebnis, dass verdeckte bzw. heimliche Bild- und Tonaufnahmen regelmäßig unzulässig seien, aber ein (journalistisches) Interesse, auf einen Missstand hinzuweisen, dem Schutz des Rechts am Bild und am gesprochenen Wort vorrangig sein könne.

9.9 Ansprüche betroffener Personen gegenüber der Aufsichtsbehörde auf konkrete Maßnahmen

Verschiedentlich ergingen im letzten Berichtszeitraum Entscheidungen wegen Ansprüchen betroffener Personen gegen die Aufsichtsbehörde. Gegenstand waren jeweils bestimmte Maßnahmen, die seitens der betroffenen Person von der Aufsichtsbehörde verlangt wurden.

Nach einer Entscheidung des Verwaltungsgerichts Berlin vom 28. Januar 2019, Aktenzeichen 1 L 1.19, hat jede betroffene Person gemäß Artikel 77 Absatz 1 DSGVO das Recht auf Beschwerde bei einer Aufsichtsbehörde, wenn Sie der Auffassung ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt, Rdnr. 5 der Entscheidung. Das Gericht ist der Auffassung, dass das Beschwerderecht nach der DSGVO als Petitionsrecht ausgestaltet worden ist. Demnach käme der Datenschutzaufsichtsbehörde bei der Untersuchung ein weiter Ermessensspielraum zu. Beschwerdeführer hätten keinen Anspruch auf eine bestimmte verfahrensmäßige Behandlung und Entscheidung in der Sache, Rdnr. 5. Mit einer Prüfung und Bescheidung der Beschwerde, so das Gericht, sei die Datenschutzbehörde den an sie gestellten gesetzlichen Anforderungen gerecht geworden. (Nach den Entscheidungsgründen hatte die Datenschutzbehörde (zunächst) von weiteren Untersuchungen abgesehen und wollte den Ausgang des

Ermittlungsverfahrens der Staatsanwaltschaft abwarten, vergleiche Rdnr. 6.) Einen weitergehenden Anspruch habe ein Beschwerdeführer nicht, Rdnr. 6.

In diese Rechtssicht reiht sich auch eine sozialgerichtliche Entscheidung ein. In einem Fall lehnte das Sozialgericht Frankfurt Oder einen Anspruch der betroffenen Person gegen die zuständige Aufsichtsbehörde auf ein Einschreiten gegen behauptete Rechtsverstöße einer Bundesbehörde auf Grundlage der DSGVO ab, Sozialgericht Frankfurt Oder, Bescheid vom 8. Mai 2019, S 49 SF 8/19. Das Gericht wies die Klage als unzulässig ab, da es an einer entsprechenden Anspruchsgrundlage fehle, Rdnr. 21. Aus der DSGVO ergebe sich kein individueller Anspruch einer betroffenen Person auf Vornahme einer bestimmten Maßnahme, Rdnr. 22. Das Gericht erkannte allein in Artikel 77 Absatz 1 DSGVO die Pflicht der Datenschutzaufsichtsbehörde, sich mit der Beschwerde auseinanderzusetzen und den Beschwerdeführer über das Ergebnis der Untersuchung zu unterrichten, Rdnr. 24. Eine weitergehende Verpflichtung bestehe hingegen nicht. Das Beschwerderecht werde als Petitionsrecht verstanden, Rdnr. 24.

Eine differenziertere Ansicht verfolgt das Verwaltungsgericht Ansbach, Urteil vom 8. August 2019, Aktenzeichen AN 14 K 19.00272, das eine Klage als zulässig, aber unbegründet ansah, Rdnr. 15, 33. Zwar lehnt das Gericht ebenso einen Anspruch der betroffenen Person auf die Vornahme bestimmter behördlicher Maßnahmen ab, jedoch räumt das Verwaltungsgericht der betroffenen Person einen Anspruch auf ermessensfehlerfreie Entscheidung der Datenschutzaufsichtsbehörde ein. Bei dem Streitgegenstand ging es um einen geltend gemachten Auskunftsanspruch gemäß Artikel 15 DSGVO der betroffenen Person, vergleiche Rdnr. 3, 40, 42. Das Verwaltungsgericht hielt gegen die Abschlussentscheidungen der Datenschutzaufsichtsbehörden nicht die Anfechtungsklage, sondern eine allgemeine Leistungsklage für statthaft, Rdnr. 17. Das Klagerecht gemäß Artikel 78 Absatz 1 DSGVO erfasse auch die Ablehnung oder Zurückweisung einer Beschwerde gemäß Artikel 77 DSGVO, Rdnr. 24. Das Verwaltungsgericht wandte sich gegen die Ansicht des Verwaltungsgerichts Berlin, wonach es bei Beschwerden nach der DSGVO um Petitionen dienen solle, Rdnr. 25. Die betroffene Person habe nicht nur einen Anspruch auf Verbescheidung, sondern gegebenenfalls ein Anspruch auf Einschreiten der Datenschutzaufsichtsbehörde bei Ermessensreduzierung auf null, ansonsten einen Anspruch auf fehlerfreie Ermessensausübung. Insofern glaubt das Verwaltungsgericht Ansbach, dass ein Anspruch auf Tätigwerden der Datenschutzaufsichtsbehörde besteht, jedoch nicht auf eine konkrete Maßnahme. Auch erkennt das Gericht keinen Anspruch auf konkrete Maßnahmen gemäß Artikel 57 bzw. Artikel 58 DSGVO, Rdnr. 36 ff. Ein Anspruch

auf fehlerfreie Ermessensausübung, auch im Hinblick auf ein Entschließungsermessen und Auswahlermessen wird, abgesehen von den Fällen einer Ermessensreduktion auf null, anerkannt, Rdnr. 41 ff.

In einem Berufungsverfahren hatte das Oberverwaltungsgericht Hamburg über die Frage eines Anspruchs auf datenschutzbehördliches Einschreiten zu entscheiden, Hamburgisches Oberverwaltungsgericht, Urteil vom 7. Oktober 2019, 5 Bf 291/17. In dem Verfahren gegen es um eine betroffene Person, die ein Einschreiten der Datenschutzaufsichtsbehörde in Bezug auf die Löschung von Sie betreffenden Suchmaschinenergebnissen erwartete. Materiell rechtlich erkannte das Gericht, dass sich die Entscheidung der Datenschutzaufsichtsbehörde, nicht einzuschreiten, aus Gründen der Meinung- und Informationsfreiheit als rechtmäßig erwiesen habe, Rdnr. 44 der Entscheidung. Das Gericht sah dem Grunde nach auch eine inhaltliche gerichtliche Befassung mit der Entscheidung der Datenschutzaufsichtsbehörde unter Verweisung auf Literaturquellen als möglich an, vergleiche Rdnr. 74 am Ende, Rdnr. 75 ff. In der Sache erkannte das Oberverwaltungsgericht allerdings, dass es auf diese Frage nicht ankäme, da ein Löschungsanspruch nicht bestanden habe, Rdnr. 78 ff.

Eine gefestigte Rechtsprechung zu der Frage der Ansprüche betroffener Personen auf konkrete datenschutzaufsichtliche Maßnahmen gegenüber den Datenschutzaufsichtsbehörden konnte sich nach alledem noch nicht herausbilden. Auch sind Entscheidungen in Bezug auf (zu treffende) Maßnahmen meiner Behörde seitens der sächsischen oder übergeordneten Verwaltungsgerichtsbarkeit noch nicht erfolgt. Mit sämtlichen vorab dargestellten Auffassungen wäre meine Dienststelle allerdings umzugehen in der Lage.

9.10 Cookies zu Werbezwecken nur mit aktiver Einwilligung – Europäischer Gerichtshof

Der Europäische Gerichtshof entschied mit Urteil vom 1. Oktober 2019, Aktenzeichen C-673/17, dass soweit Anbieter einer Internetpräsenz eine Einwilligung für Cookies benötigen, die Nutzer, diese aktiv zu setzen, imstande zu sein haben. Die Entscheidung hat erhebliche Bedeutung für die Praxis im Bereich von eCommerce und Internetwirtschaft. (Anmerkung: Der Entscheidung ist aufgrund einer nach Ende des Berichtszeitraums ergangenen Entscheidung des Bundesgerichtshofs vom 28. Mai 2020, Aktenzeichen I ZR 7/16, Rechnung zu tragen. Die ordnungsgemäße Umsetzung ist meine Dienststelle als Datenschutzaufsichtsbehörde zu kontrollieren beauftragt.)

Vorausgegangen war eine Klage eines deutschen Verbraucherverbandes wegen Online-Gewinnspielen zu Werbezwecken, bei denen das für die Internetpräsenz verantwortliche Unternehmen ein in der Praxis von Diensteanbietern häufig verwendetes Ankreuzkästchen mit einem voreingestellten Häkchen einsetzte, um Internetnutzer, die an den Gewinnspielen teilnehmen wollten, über eine Einwilligung in das Speichern von Cookies zu Werbezwecken zu gewinnen. Der Bundesgerichtshof, bei dem der Rechtsstreit zu entscheiden war, legte dem Europäischen Gerichtshof Fragen zur Auslegung des Unionsrechts zum Schutz der Privatsphäre in der elektronischen Kommunikation vor. Die Rechtsfragen betrafen im Wesentlichen die Informationspflichten des Diensteanbieters sowie die Wirksamkeit der Einwilligung im Sinne der DSGVO und nach der noch gültigen die ePrivacy-Richtlinie.

Cookies sind Dateien, die von Internetpräsenzen auf dem lokalen Rechner gespeichert und beim erneuten Besuch der Webseite abgerufen werden. Die Dateien speichern Daten über das Verhalten des Nutzers, aber auch Voreinstellungen des Nutzers zur komfortableren Ansicht einer Internetseite. Bei der Beurteilung der Frage hatte sich der europäische Gerichtshof an der Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG, auch ePrivacy-Richtlinie genannt), an der Datenschutzrichtlinie nach alten Recht, Richtlinie 95/46/EG sowie an der wirksam gewordenen DSGVO zu orientieren, da auch die zu beurteilende Rechtsfrage für die Zukunft Gegenstand war.

In seinem Urteil entschied der Gerichtshof, dass die für die Speicherung und den Abruf der Cookies auf dem Gerät des Besuches einer Internetseite erforderliche Einwilligung durch ein voreingestelltes Ankreuzkästchen, das der Nutzer bei Ablehnung einer Einwilligung zu deaktivieren hat, nicht wirksam erteilt wird, u.a. Rdnr. 90, vergleiche auch Ziffer 1 des Tenors. Nach dem Europäischen Gerichtshof ist es dabei nicht entscheidend, ob die Informationen, die im Gerät des Nutzers gespeichert und abgerufen werden können, letztendlich personenbezogen sind oder nicht, Rdnr. 107, vergl. auch Ziffer 2 des Tenors. Der Gerichtshof geht auch noch weiter: Das Unionsrecht soll den Nutzer vor jedem Eingriff in seine Privatsphäre schützen und auch der Gefahr des Eindringens von verdeckten Programmen, von so wörtlich „Hidden Identifiers", Rdnr. 106. Es bedürfe einer Einwilligung für den konkreten Fall, so u. a. Rdnr. 93 der Entscheidung. Eine Betätigung einer Schaltfläche für die Teilnahme an einem Gewinnspiel stelle deshalb noch keine wirksame Einwilligung in die Speicherung von Cookies dar. Darüber hinaus stellte der Gerichtshof

heraus, dass der Diensteanbieter gegenüber dem Nutzer auch Angaben zur Funktionsdauer und zur Zugriffsmöglichkeit Dritter zu machen hat, Rdnr. 91, 113 ff. sowie Ziffer 3 des Tenors.