SACHSEN-ANHALT

XVIII. bis XX.

Tätigkeitsbericht der Landesbeauftragten für den Datenschutz

Telefon: 0391 81803-0
Fax: 0391 81803-33

Internet: https://datenschutz.sachsen-anhalt.de/
E-Mail: poststelle@lfd.sachsen-anhalt.de

Anschrift: Postfach 1947, 39009 Magdeburg
Dienstgebäude: Otto-von-Guericke-Str. 34a, 39104 Magdeburg

Vorwort

Der XVIII., XIX. und XX. Tätigkeitsbericht zum Datenschutz umfasst den Zeitraum vom 1. Januar 2021 bis zum 31. Dezember 2023.

Mit diesem Sammelband über den Berichtszeitraum 2021 bis 2023 gelingt nun der Lückenschluss in der Reihe der Tätigkeitsberichte des Landesbeauftragten für den Datenschutz Sachsen-Anhalt. Sie fallen noch nicht in meine Amtszeit. In dem relevanten Berichtszeitraum oblag die kommissarische Vertretung des Amtes des Landesbeauftragten für den Datenschutz meinem Stellvertreter Albert Cohaus. Ihm gebührt großer Dank für die Zeit der Vertretung und die Leitung der Behörde. Wie den Berichten zu entnehmen ist, stellten sich viele spannende datenschutzrechtliche Fragestellungen, die ich dank des großen Einsatzes der Behörde nun auch vorstellen kann.

Das Berichtsjahr 2021 zeichnet sich insbesondere durch die folgenden Themen aus. Aus Anlass des EuGH Urteils zu Schrems II hatte die DSK ein Rechtsgutachten zur Rechtslage der Kommunikations- und Clouddienstleiter in den USA in Auftrag gegeben. Im Rahmen der Digitalstrategie der EU wurden die Grundlagen für maßgebliche europäische Regelungen geschaffen, wie den Data Governance Act, die EU-Verordnung über künstliche Intelligenz, das Gesetz über digitale Dienste und das Gesetz über digitale Märkte. Beraten wurde zu den Themen BAföG Digital sowie die verschlüsselte Datenübertragung bei Funkmesszählern. Hinzu kam der Abschluss des Staatsvertrages zur Neuregulierung des Glücksspielwesens in Deutschland und der Einrichtung einer zentralen Glücksspielaufsicht (LUGAS) mit Sitz in Sachsen-Anhalt. Natürlich prägte die anhaltende Pandemie die Tätigkeit des Landesbeauftragten. Neben Warn-Apps, Corona-Tests und Erfassung von Testergebnissen spielte auch die Gestaltung des Homeoffice eine Rolle sowie das Beauskunften und Löschen von personenbezogenen Daten.

Im Berichtsjahr 2022 schritt die EU-Digitalgesetzgebung voran und der EDSA führte die öffentliche Konsultation der ersten Fassung der Leitlinien zur Festsetzung von Geldbußen nach der DS-GVO durch. Weitere Themen waren unter anderem Löschkonzepte, Akkreditierung und Zertifizierung, häufige Mängel beim Einsatz von Cookies und Trackingmechanismen, Datenschutz und Forschung, digitale Funkmeldungen des Rettungsdienstes, Beschwerden im Zusammenhang mit dem Zensus 2022, das Mithören von Mitarbeitergesprächen im Rahmen des Beschäftigtendatenschutzes und Datenschutz im Kontext mit Bildaufnahmen von Kindern.

Im Berichtsjahr 2023 prägte das EU-U.S. Data Privacy Framework den internationalen Datenverkehr. Auf nationaler Ebene wurden Themen wie z. B. Chatkontrolle, Google Streetview, Pur-Abo-Modelle, Datenschutz in der Forschung, das Bildungsmanagementsystem an Schulen und Elterneinsicht in WhatsApp-Chatgruppen behandelt. Dazu kamen Themen wie elektronisches Fahrtenbuch für Dienstfahrzeuge, Live-Streams von Ratssitzungen, Auskunft nach Art. 15 DS-GVO, Aushang von Hausverboten, Herausgabe von Aufnahmen einer Videoüberwachung an private Personen sowie Kameradummies und Klingelkameras.

Und das waren noch nicht alle Themen, mit denen sich der Landesbeauftragte befasst hat. Die Arbeit war nicht nur von der Aufsichtstätigkeit geprägt. Eine wichtige Rolle spielten ebenfalls die Information und Sensibilisierung zu datenschutzrechtlichen The-

men. Die Zahl der registrierten Posteingänge ist während des Berichtszeitraums kontinuierlich gestiegen. Die Beschwerdeverfahren und Informations- und Beratungsfälle waren in der Anzahl konstant hoch.

Ein Blick in die Berichte lohnt sich. Sie verdeutlichen, mit welcher Vielfalt an Themen der Landesbeauftragte für den Datenschutz im Laufe eines Berichtsjahres befasst ist und wie wichtig es ist, dass die Behörde sich neben Beschwerden, Informationen und Sensibilisierung gerade auch mit Zukunftsthemen datenschutzrechtlich befasst. Viel Freude bei der Lektüre!

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Magdeburg, den 9. Juli 2025

Maria Christina Rost
Landesbeauftragte für den Datenschutz Sachsen-Anhalt

Inhaltsverzeichnis

XVIII. Tätigkeitsbericht 2021

1 Der Landesbeauftragte 2
1.1 Tätigkeit im Berichtszeitraum 2
1.2 Entwicklung des Arbeitsaufkommens – Fallstatistik 2

2 Weitere europäische und internationale Entwicklungen 3
2.1 Europäischer Datenschutzausschuss 3
2.2 Behandlung grenzüberschreitender Beschwerden – Betroffenheit 5
2.3 Schrems II-Urteil des EuGH – Gutachten zur Reichweite von Zugriffsrechten von U.S.-amerikanischen Sicherheitsbehörden 6
2.4 EU-Datenstrategie 7
2.4.1 Daten-Governance-Rechtsakt (Data Governance Act) 7
2.4.2 Verordnung über Künstliche Intelligenz (KI-VO) 8
2.4.3 Gesetz über digitale Dienste (Digital Services Act) 9
2.4.4 Gesetz über digitale Märkte (Digital Markets Act) 10
2.5 Internationale Datenschutzkonferenz 10

3 Technik und Organisation 11
3.1 BAföG Digital 11
3.2 Verschlüsselte Datenübertragung bei Funkmesszählern 13
3.3 Versehentlicher Erwerb von personenbezogenen Daten 14
3.4 Akkreditierung und Zertifizierung 15
3.5 Informationssicherheit (AG InfoSic Land) 16
3.6 Besonderes elektronisches Behördenpostfach 18

4 Telekommunikation und Medien 19
4.1 Orientierungshilfe für Anbieterinnen und Anbieter von Telemedien 19

5 Öffentliche Sicherheit 20
5.1 Länderübergreifendes Glücksspielaufsichtssystem (LUGAS) 20
5.2 Prüfung der Rechtmäßigkeit von Videoüberwachungsmaßnahmen der Polizeiinspektionen 21
5.3 Einhaltung von Aussonderungsprüf- und Löschfristen beim LKA 21

6 Verkehr 22
6.1 Zeitpunkt der Abfrage des Fahreignungsregisters (FAER) 22

7 Schulwesen 24
7.1 Status der Elternvertretungen 24
7.2 Ausstattung von Schulen mit digitalen Geräten 25
7.3 Zeugnisnoten per E-Mail 27
7.4 Behördliche Datenschutzbeauftragte an Schulen 28
7.5 Fotografieren bei Schulveranstaltungen 29

7.6 BRAFO-KE Berufsorientierung / EU-Verwaltungsbehörde 29

8 Gesundheitswesen 30
8.1 Luca-App/Corona-Warn-App 30
8.2 Corona-Tests an Schulen 31
8.3 Test Schulfremder 33
8.4 Präsenzpflicht an Schulen 34
8.5 Impfstatusabfrage 35
8.6 Atteste zum Mund-Nasen-Schutz 37
8.7 Kontaktdatenerfassungen 38
8.8 Testzentren 39
8.9 Daten des Betriebsarztes 40
8.10 Aufbewahrungsort für Backups 41

9 Sozialwesen 43
9.1 Sozialdaten auf Briefumschlägen 43
9.2 Datenschutz in Kindertagesstätten 44

10 Beschäftigtendatenschutz 44
10.1 Homeoffice 44
10.2 Digitalisierung von Versorgungsakten 45
10.3 Selbstauskunftsbogen der Investitionsbank Sachsen-Anhalt 46

11 Kommunales und Meldewesen 47
11.1 Veröffentlichung in Rats- und Bürgerinformationssystemen 47
11.1.1 Veröffentlichung von Sitzungsvorlagen 47
11.1.2 Veröffentlichung von Beschlüssen 48
11.1.3 Veröffentlichung von Niederschriften 48
11.2 Zuständigkeit der behördlichen Datenschutzbeauftragten der Kommunen für die Kommunalvertretungen 49
11.3 Wahlwerbung 49
11.4 Auskünfte aus dem Liegenschaftskataster 51

12 Wirtschaft 52
12.1 Aktuelle Meldungen von Datenschutzverletzungen 52
12.2 Datenübermittlungen von Versicherungen an Polizeidienststellen 53
12.3 Schutz von Berufsgeheimnissen in E-Mails 54
12.4 Einsicht in die Mitgliederliste einer Genossenschaft 54
12.5 Fotografieren von Wohnräumen und Datenerhebung für das Notariat durch Immobilienmakler 56
12.6 Speicherfrist von 30 Jahren für bestimmte Versicherungsdaten 58
12.7 Erfüllung des Auskunftsanspruchs nach Art. 15 DS-GVO 60
12.8 Dokumentation der Löschung personenbezogener Daten 61
12.9 Verarbeitung von Positivdaten durch Auskunfteien 61
12.10 Erbenermittlung durch Inkassounternehmen 62
12.11 Einholung von umfangreichen Einwilligungserklärungen mithilfe von Vordrucken 63

13 Bußgeldverfahren 64
13.1 Statistik der behördlichen Bußgeldverfahren 64

XIX. Tätigkeitsbericht 2022

14 Der Landesbeauftragte 66
14.1 Tätigkeit im Berichtszeitraum, Entwicklung des Arbeitsaufkommens – Fallstatistik 66

15 Nationales und Europäisches Datenschutzrecht 67
15.1 AK Sanktionen: Evaluierung des § 41 BDSG 67
15.2 Zuständigkeiten nach dem Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG) 67
15.3 EU-Digitalgesetzgebung und Datenschutz 68

16 Weitere europäische und internationale Entwicklungen 70
16.1 Grenzüberschreitende Beschwerden – One-Stop-Shop 70
16.2 Internationale Datenschutzkonferenz 71
16.3 Leitlinien 04/2022 des EDSA zur Berechnung von Geldbußen gemäß der DS-GVO – Version 1.0 für die öffentliche Konsultation 72

17 Technik und Organisation 73
17.1 Was ist ein Löschkonzept? 73
17.2 Besonderes elektronisches Behördenpostfach 74
17.3 Akkreditierung und Zertifizierung 74
17.4 Informationssicherheit (AG InfoSic Land) 76

18 Telekommunikation und Medien 78
18.1 Google Fonts 78
18.2 Kurzgutachten zum Betrieb von Facebook-Fanpages 80
18.3 Häufige Mängel beim Einsatz von Cookies und Tracking-Mechanismen 80

19 Öffentliche Sicherheit 82
19.1 Sichere Videokonferenzen bei der Polizei Sachsen-Anhalts 82
19.2 Ermittlungen gegen Unbeteiligte 83
19.3 Aufnahme neuer Rechtsgrundlagen in das Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt (SOG LSA) 84

20 Forschung 85
20.1 Wissenschaftliche Forschung – selbstverständlich mit Datenschutz 85
20.2 Petersberger Erklärung 85

21 Schulwesen 86
21.1 Datenübermittlung im Rahmen von Zielvereinbarungsgesprächen 86
21.2 Referentenentwurf zur Änderung des Schulgesetzes 86

22 Gesundheitswesen 87
22.1 Info-E-Mail zum Novavax-Impfstoff 87
22.2 Impfterminverarbeitung 87
22.3 3-G-Regel bei Schul- und Hochschulveranstaltungen 88
22.4 Einrichtungsbezogene Impfpflicht 89
22.5 Übermittlung von Gesundheitsdaten mittels WhatsApp 89
22.6 Datenschutzverletzung an der Uniklinik – Meldedatenabruf 91
22.7 Digitale Funkmeldungen des Rettungsdienstes 94
22.8 Datenschutzgrundlagen bei kleineren Leistungserbringern im Gesundheitswesen 95
22.9 Erfüllen der Informationspflichten im Krankentransport und Rettungsdienst 97

23 Beschäftigtendatenschutz 99
23.1 Beschäftigtendatenschutzgesetz 99
23.2 Verarbeitung von Mitarbeiterdaten im Callcenter 99
23.3 Mithören von Telefongesprächen 101

24 Kommunales und Meldewesen 102
24.1 Automatisierte Meldedatenabrufe 102

25 Verwaltung allgemein 103
25.1 Zensus 2022 103
25.2 Zensus 2022 – Beschwerden 104
25.3 Beratungsanfragen Onlinezugangsgesetz (OZG) 105

26 Wirtschaft 105
26.1 Meldungen von Datenschutzverletzungen 105
26.2 Datenschutzrechtliche Verantwortung in Konzernstrukturen 106
26.3 Digitale Schließsysteme in vermieteten Mehrfamilienhäusern 107

27 Videoüberwachung und Fotoaufnahmen 109
27.1 Kinderbilder 109
27.2 Gezieltes Fotografieren Fremder an öffentlichen Plätzen 110

28 Bußgeldverfahren 111
28.1 Statistik der behördlichen Bußgeldverfahren 111
28.2 Bußgelder wegen unzureichender Technikgestaltung beim Web-Tracking nach Art. 25 Abs. 1 DS-GVO 112

XX. Tätigkeitsbericht 2023

29 Der Landesbeauftragte 116
29.1 Tätigkeit im Berichtszeitraum, Entwicklung des Arbeitsaufkommens – Fallstatistik 116

30 Nationales und Europäisches Datenschutzrecht 117
30.1 Wahl einer/eines Landesbeauftragten für den Datenschutz 117

31 Weitere europäische und internationale Entwicklungen 117
31.1 Europäischer Datenschutzausschuss 117
31.2 Grenzüberschreitende Verarbeitungen – One-Stop-Shop 120
31.3 Angemessenheitsbeschluss USA (EU-U.S. Data Privacy Framework) 120
31.4 Angemessenheitsbeschluss Japan (Review) 121
31.5 UAK Extraterritorialer Zugriff 122
31.6 AG „Rechtsgrundlage für die Übermittlung von Gesundheitsdaten und Biomaterialien in Drittstaaten“ 122
31.7 AG „Gemeinsame Handreichung zum EU-U.S. Data Privacy Framework“ 123
31.8 Leitlinien 04/2022 des EDSA für die Berechnung von Geldbußen 123
31.9 Zuständigkeit für die Religionsgemeinschaft Jehovas Zeugen 124

32 Technik und Organisation 124
32.1 Akkreditierung und Zertifizierung 124
32.2 Informationssicherheit (AG InfoSic Land) 126
32.3 Pilotphase „Mein Justizpostfach“ 128
32.4 Angemessene Reaktionen auf gängige Cyberangriffe 129
32.5 Prüfung von Videokonferenzsystemen bei Dataport 130

33 Telekommunikation und Medien 131
33.1 Chatkontrolle 131
33.2 Google Street View 132
33.3 Pur-Abo-Modelle 132
33.4 Beschwerden über den Beitragsservice 133

34 Öffentliche Sicherheit 134
34.1 Einhaltung datenschutzrechtlicher Vorschriften beim Landeskriminalamt und der Verfassungsschutzbehörde 134

35 Rechtspflege und Justizvollzug 134
35.1 Beauftragung von Dienstleistern für den Versand der Gerichtspost 134

36 Forschung 135
36.1 Datenschutz in der Forschung durch einheitliche Maßstäbe stärken 135

36.2 Regulierung gesetzlicher Register 135

37 Schulwesen 136
37.1 Bildungsmanagementsystem 136
37.2 Behördliche Datenschutzbeauftragte der Schulen 136
37.3 Elterneinsicht in WhatsApp-Chatgruppe 137
37.4 WhatsApp in der Schule 137
37.5 Umsetzung des Energiepreispauschalengesetzes 138

38 Gesundheitswesen 139
38.1 Cloudbasierte Gesundheitsanwendungen (Beschluss) 139
38.2 Coronamaßnahmen – Datenlöschung 140
38.3 Datenpannen im Universitätsklinikum 140
38.4 Nutzung der Patiententelefonnummer für private Zwecke 141

39 Beschäftigtendatenschutz 142
39.1 Erhöhter Regelungsbedarf im Beschäftigtendatenschutz 142
39.2 Elektronisches Fahrtenbuch für die Dienstfahrzeuge 143
39.3 Einsatz von WhatsApp zur betrieblichen Kommunikation 144

40 Kommunales und Meldewesen 145
40.1 Live-Streams von Ratssitzungen 145
40.2 Umfang des Auskunftsanspruches gemäß Artikel 15 Datenschutz-Grundverordnung (DS-GVO) 147

41 Verwaltung allgemein 148
41.1 Datenschutzüberprüfung beim Postaustauschzentrum der Landesbehörden 148

42 Wirtschaft 148
42.1 Aktuelle Meldungen von Datenschutzverletzungen 148
42.2 Anruferdatenbank und Datenschutzinformationen eines Taxiunternehmens 149
42.3 Zusammenarbeit mit der Aufsichtsbehörde 150
42.4 Negativauskünfte nach Art. 15 DS-GVO 152
42.5 Vermischung der Daten der Stromanschlussnutzer und Betreiber einer Photovoltaik-Anlage 153
42.6 Feuchtigkeitsmessungen in einer Mietwohnung aufgrund einer Denkmalschutzauflage 155
42.7 Aushang von Hausverboten 156
42.8 Länderübergreifendes Glückspielaufsichtssystem (LUGAS) 156
42.9 Verarbeitung der Daten von Berufsbetreuern bei Banken 157

43 Videoüberwachung und Fotoaufnahmen 157
43.1 Herausgabe von Aufnahmen von Überwachungskameras an private Dritte 157
43.2 Speicherfristen bei Videoüberwachung 159
43.3 Kameradummys – datenschutzgerechte Nichtüberwachung 160

43.4 Ordnungsamt als „Datenschutzaufsicht“ 161
43.5 Klingelkameras 163
43.6 Haushaltsausnahme bei Fotografien von privater Baustelle 165

44 Bußgeldverfahren 167
44.1 Statistik der behördlichen Bußgeldverfahren 167

Anlagenverzeichnis XII

Abkürzungsverzeichnis XIII

Stichwortverzeichnis 169

Anlagenverzeichnis

Anlage 1
Organigramm **168**

Abkürzungsverzeichnis

A

A. ö. R.	Anstalt des öffentlichen Rechts
ABl.	Amtsblatt (der Europäischen Union)
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Amtsgericht
AG	Arbeitsgruppe
AG InfoSic	Arbeitsgruppe Informationssicherheit
AK	Arbeitskreis
AllGO LSA	Allgemeine Gebührenordnung des Landes Sachsen-Anhalt
AO	Abgabenordnung
ArbMedVV	Verordnung zur arbeitsmedizinischen Vorsorge
Art.	Artikel
ASiG	Gesetz über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit (Arbeitssicherheitsgesetz)
ATD	Antiterrordatei
ATDG	Antiterrordateigesetz

B

BAföG	Bundesausbildungsförderungsgesetz
BDBOS	Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben
BDSG	Bundesdatenschutzgesetz
beA	besonderes elektronisches Anwaltspostfach
BeamtStG	Gesetz zur Regelung des Statusrechts der Beamtinnen und Beamten in den Ländern (Beamtenstatusgesetz)
beBPo	besonderes elektronisches Behördenpostfach
beN	besonderes elektronisches Notarpostfach
BfDI	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BITS	Behörden-IT-Sicherheitstraining
BMG	Bundesmeldegesetz
BMG-AG LSA	Ausführungsgesetzes des Landes Sachsen-Anhalt zum Bundesmeldegesetz
BMI	Bundesministerium des Innern, für Bau und Heimat
BRAFO	Landesberufsorientierungsprogramm „BRAFO – Berufswahl Richtig Angehen Frühzeitig Orientieren“
BRAFO-KE	BRAFO Kompetenz- und Interessenerkundung
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStatG	Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz)
bspw.	beispielsweise

BundID	Nutzerkonto Bund, künftig DeutschlandID; Dient der Identifikation und Authentifikation von Bürgern für Online-Verwaltungsleistungen öffentlicher Stellen
BVerfG	Bundesverfassungsgericht
BZRG	Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz)

C

ca.	circa
CEF	Coordinated Enforcement Framework
CEH	Compliance, e-Government und Health Expert Subgroup des EDSA
CI/CD	Continuous Integration – Kontinuierliche Integration/Continuous Delivery oder Continuous Deployment – Kontinuierliche Auslieferung oder Kontinuierliche Bereitstellung (von Software)
CIO	Chief Information Officer, Beauftragter der Landesregierung für Informations- und Kommunikationstechnologie
CISO	Chief Information Security Officer, Informationssicherheitsbeauftragter der unmittelbaren Landesverwaltung/Gesamtverantwortlicher für die Informationssicherheit in einer Organisation
CSA	Concerned Supervisory Authority, betroffene Aufsichtsbehörde

D

d. h.	das heißt
DAkkS	Deutsche Akkreditierungsstelle GmbH
De-Mail	Auf E-Mail-Technik beruhendes Kommunikationsmittel zur sicheren, vertraulichen und nachweisbaren Kommunikation im Internet
DenkmSchG LSA	Denkmalschutzgesetz des Landes Sachsen-Anhalt
DGA	Data Governance Act, Verordnung (EU) 2022/868 des Europäischen Parlamentes und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt)
DiGAV	Digitale Gesundheitsanwendungen-Verordnung
DIN	Deutsches Institut für Normung e. V.
DMA	Digital Markets Act, Verordnung (EU) 2022/1925 des Europäischen Parlamentes und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte, ABl. L 265 vom 12. Oktober 2022, S. 1)
DNA	Desoxyribonukleinsäure
DPF, TADPF	Trans-Atlantic Data Privacy Framework, EU-US Datenschutzrahmen

DSA	Digital Services Act, Verordnung (EU) 2022/2065 des Europäischen Parlamentes und des Rates über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste)
DSAG LSA	Gesetz zur Ausfüllung der Verordnung (EU) 2016/679 und zur Anpassung des allgemeinen Datenschutzrechts in Sachsen-Anhalt (Datenschutz-Grundverordnungs-Ausfüllungsgesetz Sachsen-Anhalt)
DSB	Datenschutzbeauftragter
DSUG LSA	Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz)
DS-GVO, 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

E

eBO	elektronisches Bürger- und Organisationenpostfach
EDSA	Europäischer Datenschutzausschuss
EDSB	Europäischer Datenschutzbeauftragter
EGovG	Gesetz zur Förderung der elektronischen Verwaltung
EEG 2023	Gesetz für den Ausbau erneuerbarer Energien (Erneuerbare-Energien-Gesetz)
EG	Europäische Gemeinschaft
EGMR	Der Europäische Gerichtshof für Menschenrechte
EGVP	Elektronisches Gerichts- und Verwaltungspostfach (Kommunikationsinfrastruktur)
EN	Europäische Norm
EPPSG	Gesetz zur Zahlung einer einmaligen Energiepreispauschale für Studierende, Fachschülerinnen und Fachschüler sowie Berufsfachschülerinnen und Berufsfachschüler in Bildungsgängen mit dem Ziel eines mindestens zweijährigen berufsqualifizierenden Abschlusses (Studierenden-Energiepreispauschalengesetz)
EPPSG-DVO	Verordnung zur Durchführung des Studierenden-Energiepreispauschalengesetzes (EPPSG-Durchführungsverordnung) des Landes
ERV, eRV	Elektronischer Rechtsverkehr
ERVV	Elektronischer-Rechtsverkehr-Verordnung
ESF	Europäischer Sozialfonds
ErwGr	Erwägungsgrund
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EU-KOM	Europäische Kommission
EU-US DPF	siehe DPF
EWR	Europäischer Wirtschaftsraum
e. V.	eingetragener Verein

F

FAER	Fahreignungsregister
FamFG	Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit
FAQ	Frequently Asked Questions, häufig gestellte Fragen
ff.	fortfolgende
FISA	Foreign Intelligence Surveillance Act

G

GDPR	General Data Protection Regulation (dt.: Datenschutz-Grundverordnung, s. DS-GVO)
GenG	Gesetz betreffend die Erwerbs- und Wirtschaftsgenossenschaften (Genossenschaftsgesetz)
GG	Grundgesetz
GGL	Gemeinsame Glücksspielbehörde der Länder
ggf.	gegebenenfalls
ggü.	gegenüber
GlüStV	Glücksspielstaatsvertrag
GPA	Global Privacy Assembly, Internationale Datenschutzkonferenz
GPS	Global Positioning System, satellitengestütztes Ortungssystem
GRCh	Charta der Grundrechte der Europäischen Union
GWB	Gesetz gegen Wettbewerbsbeschränkungen
GWG	Geldwäschegesetz

H

HBDI	Der Hessische Beauftragte für Datenschutz und Informationsfreiheit

I

ICO	Information Commissioner’s Office, Datenschutzaufsichtsbehörde des Vereinigten Königreichs
i. d. R.	in der Regel
IEC	International Electrotechnical Commission
IfSG	Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen (Infektionsschutzgesetz)
IKT	Informations- und Kommunikationstechnik
IMI	Internal Market Information System (Binnenmarkt-Informationssystem)
IMK	Innenministerkonferenz
INPOL	Informationssystem der Polizei
ISB	Informationssicherheitsbeauftragte
ISichG	Gesetz zur Gewährleistung der Informationssicherheit in Sachsen-Anhalt (Informationssicherheitsgesetz ST)
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
ISRL	Informationssicherheitsrichtlinie
IT	Informationstechnik
i. S. d.	im Sinne des

i. S. v.	im Sinne von
i. V. m.	in Verbindung mit

J

JI-Richtlinie	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
JKomG	Justizkommunikationsgesetz

K

KI	Künstliche Intelligenz
KI-VO	Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz und zur Änderung bestimmter Rechtsakte der Union (Verordnung über künstliche Intelligenz)
KMU	kleine und mittelgroße Unternehmen
KRITIS	Kritische Infrastrukturen
KUG	Kunsturhebergesetz
KVG LSA	Kommunalverfassungsgesetz des Landes Sachsen-Anhalt

L

LAG	Länderarbeitsgruppe
LAN	Local Area Network, lokales Netzwerk
LBG LSA	Beamtengesetz des Landes Sachsen-Anhalt (Landesbeamtengesetz
LDA, BayLDA	Das Bayerische Landesamt für Datenschutzaufsicht
LG	Landgericht
LISL LSA	Leitlinie zur Informationssicherheit der unmittelbaren Landesverwaltung Sachsen-Anhalt, Informationssicherheitsleitlinie
lit.	lat. littera (Buchstabe)
LK	Landkreis
LKA	Landeskriminalamt
LSA	Land Sachsen-Anhalt
LSA	Lead Supervisory Authority, federführende Aufsichtsbehörde
LT-Drs.	Landtagsdrucksache
LUGAS	Länderübergreifendes Glücksspielaufsichtssystem
LVermGeo	Landesamt für Vermessung und Geoinformation Sachsen-Anhalt
LVG	Landesverfassungsgericht Sachsen-Anhalt

M

m-RNA	Messenger Ribonucleic Acid (Boten-Ribonukleinsäure)

MDR	Mitteldeutscher Rundfunk
MF	Ministerium der Finanzen
MI	Ministerium für Inneres und Sport
MID	Ministerium für Infrastruktur und Digitales
MsbG	Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz)
MW	Ministerium für Wirtschaft, Tourismus, Landwirtschaft und Forsten

N

Nr.	Nummer
NFC	Near Field Communication, Nahfeldkommunikation

O

o. g.	oben genannt
OH	Orientierungshilfe
OLG	Oberlandesgericht
OWiG	Gesetz über Ordnungswidrigkeiten
OZG	Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz)

P

PAuswG	Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz)
PC	Personal Computer
PGP	Pretty Good Privacy, Software zur Verschlüsselung und zum Unterschreiben von Daten
PKI	Public-Key-Infrastruktur
Pkw	Personenkraftwagen
POCSAG-Protokoll	Post Office Code Standardisation Advisory Group ist ein unidirektionales Funkrufprotokoll.
PPC	japanische Datenschutzbehörde

Q

R

RED	Rechtsextremismusdatei
RED-G	Rechtsextremismus-Datei-Gesetz
RIC-Kennung	Radio Identification Code sind eindeutige Kennungen, die im digitalen Funk zur Adressierung und Alarmierung von Funkmeldeempfängern und Sirenen verwendet werden
RL	Richtlinie
Rn.	Randnummer

S

SAFE	Secure Access to Federated E-Justice/E-Government – sichere elektronische Identitäten in einem föderalen Umfeld, Name einer Software zum Betrieb eines Verzeichnisdienstes und Standard für Verzeichnisdienste (Adressbücher),

	das beBPo kann den SAFE-Verzeichnisdienst der Justiz nutzen
SARS-CoV-2	severe acute respiratory syndrome coronavirus type 2, schweres akutes Atemwegssyndrom Coronavirus Typ 2, umgangssprachlich (neuartiges) Coronavirus
SARS-CoV-2-EindV	Verordnung über die Maßnahmen zur Eindämmung der Ausbreitung des neuartigen Coronavirus SARS-CoV-2 in Sachsen-Anhalt
SBOM	Software Bill of Materials
„Schrems II“-Urteil	Urteil des EuGH, Az. C-311/18
SchulG LSA	Schulgesetz des Landes Sachsen-Anhalt
SGB V	Sozialgesetzbuch Fünftes Buch – Gesetzliche Krankenversicherung
S/MIME	Secure / Multipurpose Internet Mail Extensions, Standard für Verschlüsselung und Signieren von MIME-Objekten durch ein hybrides Kryptosystem
sog.	sogenannte
SOG LSA	Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt
ST	Sachsen-Anhalt
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StRG	Statut der Religionsgemeinschaft Jehovas Zeugen in Deutschland
StVG	Straßenverkehrsgesetz

T

TF	Task Force
TKG	Telekommunikationsgesetz
TLP	Traffic Light Protocol
TTDSG	Telekommunikation-Telemedien-Datenschutzgesetz
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz
TMG	Telemediengesetz

U

UAG	Unterarbeitsgruppe
UAK	Unterarbeitskreis
UK	United Kingdom, Vereinigtes Königreich
US/USA	United States of America, Vereinigte Staaten von Amerika
u. a.	unter anderem
u. U.	unter Umständen

V

VermGeoG LSA	Vermessungs- und Geoinformationsgesetz Sachsen-Anhalt
VG	Verwaltungsgericht
vgl.	vergleiche
VO	Verordnung

VPN	Virtual Private Network, virtuelles privates, in sich geschlossenes Kommunikationsnetzwerk
VS	Verschlusssache
VSB	Verfassungsschutzbehörde
VwGO	Verwaltungsgerichtsordnung
VwKostG LSA	Verwaltungskostengesetz des Landes Sachsen-Anhalt

W

WP	Working Paper, Arbeitspapier
W-LAN	Wireless LAN, drahtloses lokales Netzwerk

X

X.509	Standardformat für digitale Zertifikate

Y

Z

z. B.	zum Beispiel
ZASt	Zentrale Anlaufstelle
ZensAG 2022 LSA	Zensusausführungsgesetz Sachsen-Anhalt 2022
ZensG 2022	Zensusgesetz 2022
ZIdPrüfV	Zahlungskonto-Identitätsprüfungsverordnung
ZMDB-VO LSA	Verordnung zum Zentralen Meldedatenbestand des Landes Sachsen-Anhalt
ZPO	Zivilprozessordnung
ZustVO OWi LSA	Verordnung über sachliche Zuständigkeiten für die Verfolgung und Ahndung von Ordnungswidrigkeiten des Landes Sachsen-Anhalt

SACHSEN-ANHALT

Landesbeauftragte
für den Datenschutz

XVIII. Tätigkeitsbericht
der Landesbeauftragten für den Datenschutz

2021

1 Der Landesbeauftragte

1.1 Tätigkeit im Berichtszeitraum

Die Tätigkeit des Landesbeauftragten war auch im Jahr 2021 noch wesentlich durch Fragen rund um das Pandemiegeschehen geprägt. Unmittelbar auf die Pandemie bezogen befasste sich der Landesbeauftragte mit Themen wie der Impfstatusabfrage (Nr. 8.5), der Kontaktdatenerfassung (Nr. 8.7), den Tests in Schulen (Nr. 8.2) und den Testzentren (Nr. 8.8). Aber auch mittelbar pandemiebedingte Themen wie das Projekt BAföG Digital (Nr. 3.1), welches das Land Sachsen-Anhalt nach dem „Einer-für-alle“-Prinzip für alle Bundesländer umgesetzt hat, beschäftigten den Landesbeauftragten umfassend.

Auch wenn die Pandemie und ihre Auswirkungen das gesellschaftliche Leben weiterhin bestimmten, hatte sich der Landesbeauftragte darüber hinaus mit Themen zu befassen, die davon vollkommen unabhängig waren. So hatte er sich mit dem Status von Elternvertretungen (Nr. 7.3), der Schuldnerermittlung durch Inkassounternehmen (Nr. 13.10) oder auch der Einhaltung von Aussonderungsprüf- und Löschfristen durch das Landeskriminalamt (Nr. 5.3) zu befassen. Es wurden Daten gelöscht, die für die polizeiliche Arbeit weiterhin erforderlich waren. Einen datenschutzrechtlich vertretbaren Weg zur Wiederherstellung der erforderlichen Daten zu finden, war daher gemeinsame Aufgabe von Polizei und Landesbeauftragtem.

1.2 Entwicklung des Arbeitsaufkommens – Fallstatistik

In dieser Rubrik berichtet der Landesbeauftragte regelmäßig über die Anzahl an Posteingängen, um einen möglichst objektiven Eindruck von der Entwicklung des Umfangs seiner Tätigkeit zu vermitteln. Mit dem Inkrafttreten der Datenschutz-Grundverordnung und der JI-Richtlinie im Jahr 2018 hat das Arbeitsaufkommen erheblich zugenommen und hält sich seither auf diesem hohen Niveau.

Anzahl der registrierten Posteingänge:

2016	5.506		
2017	6.737		
2018	9.602	zuzüglich	3.306 Meldungen gem. Art. 37 Abs. 7 DS-GVO
2019	10.941	zuzüglich	746 Meldungen gem. Art. 37 Abs. 7 DS-GVO
2020	13.730	zuzüglich	764 Meldungen gem. Art. 37 Abs. 7 DS-GVO
2021	13.933	zuzüglich	1.351 Meldungen gem. Art. 37 Abs. 7 DS-GVO

Um nachvollziehen zu können, wo Schwerpunkte der Tätigkeit des Landesbeauftragten liegen, führt er für wesentliche Bereiche seiner Tätigkeit eine Geschäftsstatistik. Innerbehördliche Angelegenheiten (Organisation, Personal, Haushalt) sind nicht erfasst, so dass sich aus der Geschäftsstatistik direkt auf seine Aufsichtstätigkeit schließen lässt. Wesentliche aufsichtsbehördliche Aufgabenfelder werden für das Jahr 2021 nachfolgend dargestellt:

Beschwerden und Eingaben	1.028
Informations- und Beratungsfälle	1.206
Meldungen von Datenschutzverletzungen	278
Abhilfemaßnahmen/Anordnungen	32
Eingeleitete Bußgeldverfahren	27
Europäische Verfahren mit eigener Betroffenheit (Kooperation und Kohärenz)	14
Förmliche Begleitung von Rechtsetzungsvorhaben	16

2 Weitere europäische und internationale Entwicklungen

2.1 Europäischer Datenschutzausschuss

Der Europäische Datenschutzausschuss (EDSA) setzt sich aus den Leitungen der nationalen Datenschutzbehörden und dem Europäischen Datenschutzbeauftragten (EDSB) zusammen. Der EDSA ist eine unabhängige europäische Einrichtung, die zur einheitlichen Anwendung der Datenschutzvorschriften im gesamten Europäischen Wirtschaftsraum (EWR) beiträgt und die Zusammenarbeit zwischen den EU-Datenschutzbehörden fördert (vgl. zu dessen Aufgaben XV. Tätigkeitsbericht, Nr. 2.1). Die Aufsichtsbehörden der EWR-Länder (Island, Liechtenstein, Norwegen) sind zwar ebenfalls Mitglieder im EDSA, jedoch ohne Stimmrecht. Die Arbeitssprache im EDSA ist Englisch.

Die Vertretung der deutschen Aufsichtsbehörden im EDSA wird durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und den Leiter einer Aufsichtsbehörde eines Landes (gemeinsamer Vertreter und Stellvertreter nach § 17 Abs. 1 BDSG) wahrgenommen. Der Bundesrat hat in seiner 1006. Sitzung am 25. Juni 2021 den Bayerischen Landesbeauftragten für den Datenschutz, Prof. Dr. Thomas Petri, zum Stellvertreter des gemeinsamen Vertreters im EDSA gewählt.

Im Einklang mit Artikel 29 der EDSA-Geschäftsordnung hat der EDSA sein zweijähriges Arbeitsprogramm für die Jahre 2021 und 2022 auf der Grundlage der EDSA-Strategie 2021-2023 und der Vorschläge seiner Mitglieder entwickelt. Diese Strategie bietet zwar keinen abschließenden Überblick über die Arbeit des EDSA in den kommenden Jahren. Allerdings werden darin die vier tragenden Säulen der strategischen Ziele sowie die wichtigsten Maßnahmen dargelegt, die zur Verwirklichung dieser Ziele beitragen sollen (Säule 1: Förderung der Harmonisierung und Erleichterung der Einhaltung der Vorschriften; Säule 2: Unterstützung einer wirksamen Durchsetzung und einer effizienten Zusammenarbeit zwischen nationalen Aufsichtsbehörden; Säule 3: Ein Grundrechtsansatz für neue Technologien; Säule 4: Die globale Dimension).

Im Rahmen der im Arbeitsprogramm 2021/2022 festgelegten Aufgaben hat der EDSA im Berichtszeitraum zahlreiche Dokumente verabschiedet. Da der Ausschuss gegebenenfalls öffentliche Konsultationen interessierter Kreise gem. Art. 70 Abs. 4 der DS-GVO durchführt, werden einige der Dokumente nochmals nach Abschluss der öffentlichen Konsultation beraten. Von den verabschiedeten Dokumenten (Leitlinien[1] und

[1] https://datenschutz.sachsen-anhalt.de/informationen/datenschutz-grundverordnung/edsa

Empfehlungen[2]) sind vor allem die Nachfolgenden zu nennen. Die Leitlinien nach Art. 70 Abs. 1 DS-GVO stellen dabei einen Schwerpunkt der Tätigkeit des EDSA dar.

- Leitlinien über die gezielte Ansprache von Nutzer:innen sozialer Medien (Guidelines 8/2020 on the targeting of social media users, Version 2.1, adopted on 13 April 2021, amended on 7 July 2021),

- Leitlinien zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DS-GVO (Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, adopted on 7 July 2021 after public consultation),

- Leitlinien zum Zusammenspiel zwischen der Anwendung von Artikel 3 und den Bestimmungen über internationale Übermittlungen gemäß Kapitel V der DS-GVO (Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, adopted on 18 November 2021, version for public consultation) – nur in Englisch,

- Leitlinien zu Beispielen für die Meldung von Datenschutzverletzungen (Guidelines 01/2021 on Examples regarding Data Breach Notification, Version 2.0, adopted on 14 December 2021 after public consultation) – nur in Englisch,

- Leitlinien zu Beschränkungen im Sinne des Art. 23 DS-GVO (Guidelines 10/2020 on restrictions under Art. 23 GDPR, Version 2.0, adopted on 13 October 2021 after public consultation) – nur in Englisch,

- Leitlinien zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen (Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, adopted on 9 March 2021),

- Empfehlungen zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten (Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, adopted on 18 June 2021) – nur in Englisch.

- Erster im Dringlichkeitsverfahren angenommener Beschluss zum Ersuchen der Hamburgischen (deutschen) Aufsichtsbehörde gemäß Art. 66 Abs. 2 der DS-GVO um Anordnung des Erlasses endgültiger Maßnahmen bezüglich Facebook Ireland und der Datenverarbeitung im Zusammenhang mit WhatsApp (Urgent Binding Decision 01/2021 on the request under Article 66(2) GDPR from the Hamburg (German) Supervisory Authority for ordering the adoption of final measures regarding Facebook Ireland Limited, adopted on 12 July 2021)

[2] https://datenschutz.sachsen-anhalt.de/informationen/infopakete/infopaket-drittstaatentransfer/edsa-empfehlungen/

Der Landesbeauftragte bringt sich im Rahmen seiner beschränkten personellen Möglichkeiten mittelbar in den Meinungsbildungsprozess des EDSA über die deutschen Vertreter in den verschiedenen Fachuntergruppen des EDSA (Expert Subgroups) ein. Seit Ende 2021 beteiligt er sich an der Task Force zur Rechtsstudie betreffend die Auslegung der sog. „Haushaltsausnahme“ in Art. 2 Abs. 2 lit. c DS-GVO.

2.2 Behandlung grenzüberschreitender Beschwerden – Betroffenheit

Der Landesbeauftragte prüft jeden Vorgang einer grenzüberschreitenden Verarbeitung, auf seine Betroffenheit nach Art. 4 Nr. 22 DS-GVO. Im Berichtszeitraum betraf dies allein 538 Eingänge zu sogenannten grenzüberschreitenden Beschwerden. Dazu kommen eine Vielzahl statistisch nicht gesondert erfasster Eingänge von anderen Datenschutzaufsichtsbehörden mit grenzüberschreitendem Bezug, bspw. zu Untersuchungen von Amts wegen, Amtshilfeersuchen, Beschlussentwürfen und Beschlüssen sowie Meldungen von Datenschutzverletzungen. Die meisten dieser Vorgänge erreichen den Landesbeauftragten elektronisch über das Internal Market Information System (IMI, vgl. dazu XVI. Tätigkeitsbericht, Nr. 5.2).

Zur administrativen Bearbeitung aller dieser Vorgänge und zur inhaltlichen Bearbeitung aller grenzüberschreitenden Beschwerden, kurz für den Bereich „Europa“, stehen dem Landesbeauftragten 75% einer Vollzeitstelle zur Verfügung. Erschwerend kommt hinzu, dass mangels elektronischer Akte auch alle Vorgänge, die elektronisch beim Landesbeauftragten eingehen, zunächst ausgedruckt und sodann in Papierform bearbeitet und auch veraktet werden müssen. Dies betrifft aufgrund der IMI-Nutzung und des Online-Beschwerdeformulars auf der Homepage des Landesbeauftragten den weit überwiegenden Teil aller Vorgänge.

Vor diesem Hintergrund muss der Landesbeauftragte genau hinterfragen, ob die Meldung als betroffene Aufsichtsbehörde zur Wahrung der Rechte und Freiheiten der Bürger in Sachsen-Anhalt zwingend erfolgen muss. Im Berichtszeitraum hat sich der Landesbeauftragte in 14 Fällen in IMI als betroffene Aufsichtsbehörde gemeldet.

Der Landesbeauftragte meldet sich in jedem Fall als betroffene Aufsichtsbehörde, wenn der Verantwortliche über eine Niederlassung in Sachsen-Anhalt verfügt und/oder wenn sich eine in Sachsen-Anhalt ansässige betroffene Person mit einer Beschwerde, die einen grenzüberschreitenden Bezug aufweist, an ihn wendet (vgl. Art. 4 Nr. 22 lit. a und c DS-GVO).

In allen übrigen Fällen eröffnet Art. 4 Nr. 22 lit. b DS-GVO einen gewissen Auslegungsspielraum hinsichtlich des Merkmals der „erheblichen Auswirkungen auf betroffene Personen“. Wird mit der Beschwerde auch ein struktureller Mangel des Verantwortlichen deutlich, bejaht der Landesbeauftragte in der Regel seine Betroffenheit, wenn das Tätigwerden des Verantwortlichen sich auch auf Bürgerinnen und Bürger in Sachsen-Anhalt auswirkt bzw. auswirken kann.

Bei Vorliegen der nachfolgenden Kriterien lehnt der Landesbeauftragte jedoch in aller Regel seine Meldung als betroffene Aufsichtsbehörde ab. Dabei handelt es sich nicht um zwingende Kriterien. Jeder Einzelfall wird einer individuellen Prüfung und Entscheidung unterzogen:

- Kein Bezug zu Sachsen-Anhalt: Der Verantwortliche verfügt über keine Niederlassung in Sachsen-Anhalt und es ist nicht ersichtlich, dass Bürger aus Sachsen-Anhalt als „Adressaten“ der Datenverarbeitungen des Verantwortlichen in Betracht kommen.

- Einzelfall: Handelt es sich nach den vorliegenden Informationen um einen Einzelfall (also der Gegensatz zum Vorliegen des o. g. strukturellen Mangels), meldet sich der Landesbeauftragte in der Regel nicht als betroffene Aufsichtsbehörde. Das Vorliegen eines Einzelfalls kann dann angenommen werden, wenn in IMI keine weiteren vergleichbaren Beschwerden zu diesem Verantwortlichen vorhanden sind und auch keine weiteren vergleichbaren Beschwerden beim Landesbeauftragten zu diesem Verantwortlichen bekannt geworden sind.

- Fragliche Erfolgsaussichten: Die Erfolgsaussichten der Beschwerde sind nach den vorliegenden Informationen bereits fraglich, weil beispielsweise im Rahmen von Finanzinstituten in der Regel personenbezogene Daten aufgrund der Anti-Geldwäsche-Gesetzgebung nicht sofort gelöscht werden dürfen oder weil der Betroffene seine Rechte ggü. dem Verantwortlichen noch gar nicht geltend gemacht hat.

- Niederlassung in einem anderen Bundesland (Verwaltungsökonomie): Wenn der Verantwortliche über eine Niederlassung in einem anderen Bundesland verfügt, besteht aus Gründen der Verwaltungsökonomie in aller Regel kein Bedarf zur Meldung des Landesbeauftragten als betroffene Aufsichtsbehörde, da nach den Regeln der innerdeutschen Zusammenarbeit nur den Aufsichtsbehörden ein maßgebliches Äußerungsrecht nach außen zukommt, in deren Zuständigkeitsbereich sich eine Niederlassung des Verantwortlichen befindet.

- Datenschutzbeschwerde wird nur als „Vehikel“ und damit missbräuchlich benutzt, während der Hintergrund eine ganz andere Streitigkeit darstellt bzw. ein anderes Ziel verfolgt (bspw. eine zivilrechtliche Streitigkeit, „Jugendschutz“).

- Bei dem geltend gemachten Verstoß handelt es sich um eine Lappalie, die zu keiner erheblichen Auswirkung für Bürgerinnen und Bürger in Sachsen-Anhalt führt bzw. führen kann.

- Der Beschwerdegegenstand hat sich zwischenzeitlich bereits erledigt, da der Verantwortliche dem Begehren des Beschwerdeführers – wenngleich auch verspätet – entsprochen hat.

Der Landesbeauftragte sieht sich in grenzüberschreitenden Verfahren unter anderem nach Art. 4 Nr. 22 lit. b DS-GVO als betroffene Aufsichtsbehörde, wenn eine Einzelfallprüfung „erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Bundesland“ befürchten lässt.

2.3 Schrems II-Urteil des EuGH – Gutachten zur Reichweite von Zugriffsrechten von U.S.-amerikanischen Sicherheitsbehörden

In Folge des „Schrems II-Urteils“ des EuGH gaben die deutschen Datenschutzaufsichtsbehörden ein Gutachten zur Rechtslage der Kommunikations- und Clouddienstleister in den USA bei Herrn Prof. Steven Vladeck (University of Texas) in Auftrag. Das

„Gutachten zum aktuellen Stand des US-Überwachungsrechtes und der Überwachungsbefugnisse“ datiert vom 15. November 2021 ist auf der Homepage der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in englischer und deutscher Sprache abrufbar.[3] Der Gutachter traf nachfolgende wesentliche Feststellungen: Die unbeschränkten Überwachungsbefugnisse der US-Sicherheitsbehörden basieren im Wesentlichen auf dem Abschnitt 702 des US-amerikanischen Foreign Intelligence Surveillance Act (FISA) und der Executive Order 12.333. Der für die Anwendbarkeit von Abschnitt 702 FISA zentrale Begriff „Anbieter elektronischer Kommunikationsdienste“ sei sehr weit. Unter diesen Begriff falle nicht nur klassische IT- und Telekommunikationsunternehmen. Vielmehr könnten auch beispielsweise Banken, Fluggesellschaften, Hotels oder Versanddienstleister dazugehören, wenn sie ihren Beschäftigten einen E-Mail-Dienst bereitstellten.

Der Begriff „Anbieter elektronischer Kommunikationsdienst“ umfasse zudem u. a. auch Anbieter von „Computerspeicher- oder -verarbeitungsdiensten“. Auch wenn ein Unternehmen nur hinsichtlich weniger oder gar nur eines einzelnen Dienstes (etwa E-Mail-Dienst für die Beschäftigten) als „Anbieter elektronischer Kommunikationsdienste“ anzusehen sei, seien die Anordnungsbefugnisse der US-Behörden bezüglich der Herausgabe bestimmter Datenbestände nicht auf Daten im Zusammenhang mit diesem Dienst beschränkt. Vielmehr eröffne die Einordnung als „Anbieter elektronischer Kommunikationsdienste“ aufgrund einer geringfügigen Tätigkeit den Anwendungsbereich von Abschnitt FISA 702 bezüglich sämtlicher Daten im Unternehmen, auch wenn dieser Kommunikationsdienst nichts mit der unternehmerischen Haupttätigkeit zu tun habe. Im Übrigen befasst sich das Gutachten unter anderem mit dem Fall, dass ein selbst nicht als „Anbieter elektronischer Kommunikationsdienste“ anzusehendes Unternehmen Dienste eines solchen in Anspruch nehme, sowie mit Fragen, ob europäische Unternehmen, die in den USA aktiv sind, dem US-Recht unterfallen, und ob Abschnitt FISA 702 extraterritorial anwendbar sei. Außerdem stellt es die Schwierigkeiten für EU-Bürger dar, Rechtsschutz in den USA wegen des Datenzugriffs durch US-Sicherheitsbehörden zu erlangen.

Der Landesbeauftragte beteiligte sich an den Kosten der Erstellung eines Gutachtens zur Reichweite von Zugriffsrechten von U.S.-amerikanischen Sicherheitsbehörden nach dem sog. Königsteiner Schlüssel und wirkte im Rahmen der Task Force Schrems II der DSK an der Auswertung und der Veröffentlichung mit.

2.4 EU-Datenstrategie

2.4.1 Daten-Governance-Rechtsakt (Data Governance Act)

Ende des Jahres 2021 einigten sich die EU-Kommission, der EU-Rat und das EU-Parlament über die endgültige Fassung des Data Governance Act (DGA), mit der die existierenden Datenbestände besser nutzbar gemacht werden sollen. Der Handel mit Daten ist aus Sicht der EU zu schwach ausgebildet; wenig Unternehmen sind bereit ihre Daten zu teilen. Große Herausforderungen, neben der Frage der Datentransformation, sind die Qualität der Daten als auch der Datenschutz. Vertrauensdefizite auf

[3] https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_de.pdf

den Datenmärkten sollen gezielt durch Verhaltensvorgaben für Datenvermittler (Datenintermediäre oder Datentreuhänder) reduziert werden.

Der DGA regelt im Wesentlichen drei unterschiedliche Aspekte der Datennutzung und -weitergabe: Die Wiederverwendung von Daten des öffentlichen Sektors (Art. 3-9 DGA), die Anforderungen an Datenvermittler (Art. 10-15 DGA) und Anforderungen an datenaltruistische Organisationen (Art. 16-25 DGA). Dabei geht es um personen- sowie nichtpersonenbezogene Daten (als codierte bzw. digital strukturierte Informationen). Aus datenschutzrechtlicher Sicht ist besonders der Datenaltruismus nach Art. 16 DGA herausfordernd. Betroffene Personen stellen Daten im Allgemeininteresse als sog. Datenspende zur Verfügung. Für die Bearbeitung naturwissenschaftlicher Fragestellungen ist häufig eine Anonymisierung von Daten hinderlich, weil ein fehlender Personenbezug die Granularität der Daten mindert und die Interpretation der Daten erheblich erschweren kann. Daher ist bei der Datenspende regelmäßig auch die DS-GVO betroffen. Probleme bereiten die Informiertheit der Einwilligung in die Datenverarbeitung und der Bestimmungsgrundsatz in Form der Konkretisierung des Zweckbindungsgrundsatzes. Der Zweck der Forschung kann sich nämlich im laufenden Prozess ändern. Als mögliche Lösung gilt ein „broad consent“ nach dem Erwägungsgrund 33 DS-GVO, danach kann eine Einwilligung rechtskonform für bestimmte Bereiche wissenschaftlicher Forschung erteilt werden (sog. Forschungsprivileg). Probleme ergeben sich aufgrund der Divergenz zwischen den knappen Transparenzpflichten nach Art. 20 DGA im Verhältnis zu den umfassenden Informationspflichten nach Art. 13, 14 DS-GVO. Nach Art. 25 DGA ist die Ausarbeitung eines europäischen Einwilligungsformulars für den Datenaltruismus geplant. Die Datenschutzaufsichtsbehörden sollen über die DS-GVO hinaus ausweislich keine weiteren aufsichtsbehördlichen Zuständigkeiten und Befugnisse erhalten (Erwägungsgrund 44 DGA). Sie haben beratende Funktion gegenüber den durch die Mitgliedstaaten zu bestimmenden Aufsichtsbehörden.

Der DGA wurde als Verordnung (EU) 2022/868 des Europäischen Parlamentes und des Rates über die europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt) am 30. Mai 2022 erlassen und gilt ab dem 23. September 2023 (ABl. L 152, S. 1).

2.4.2 Verordnung über Künstliche Intelligenz (KI-VO)

Am 21. April 2021 legte die EU-KOM einen Vorschlag für eine Verordnung des Europäischen Parlamentes und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz und zur Änderung bestimmter Rechtsakte der Union vor. Künstliche Intelligenz (KI) gilt als Motor von Innovationen bspw. in Bereichen der Gesundheit, Mobilität, Bildung. Um den damit verbundenen Risiken vorzubeugen, sind nach der KI-VO konkrete Anforderungen an die Entwicklung und den Einsatz von KI-Systemen zu stellen. Die VO regelt ein risikoadäquates Maß an Nachvollziehbarkeit und Transparenz. Danach muss eine Kontrollstruktur bestehen, die eine Überprüfbarkeit gewährleistet. Die VO verpflichtet zur präventiven Prüfung von KI-Anwendungen auf bestimmte Rechtsgüter (verschiedene Risikogruppen). KI-Systeme zur Verhaltensmanipulation (sog. Dark Pattern), zur Bewertung sozialen Verhaltens durch Behörden (sog. Social Scoring) oder zur biometrischen Fernidentifizierung, die Bilder, Videos oder Sprachaufnahmen generieren oder manipulieren (sog. Deep Fake) sind verboten. Die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen unterliegt mit Ausnahmen ebenfalls einem Verbot (Art. 5 KI-VO).

Es ist davon auszugehen, dass die Entwicklung und Verwendung von KI-Systemen vielfach mit der Verarbeitung personenbezogener Daten verbunden sein wird, so bspw. im Bereich der Beschäftigung und des Personalmanagements. Um Nachteile für die betroffenen Personen zu vermeiden, klassifiziert die VO solche KI-Systeme als „hochriskant“ mit strengen Zulässigkeitsanforderungen (Art. 6 ff. KI-VO).

Der EDSA und EDSB fordern in der gemeinsamen Stellungnahme vom 18. Juni 2021, dass die Verwendung eines „Social Scoring“ auch durch Privatunternehmen aufgrund seines enormen Diskriminierungspotentials verboten wird. Ferner liegt in der biometrischen Fernidentifizierung im öffentlichen Raum ein hohes Risiko für die Privatsphäre natürlicher Personen. Insofern wird auch ein Verbot der Verwendung von KI zur automatischen Erkennung von personenbezogenen Merkmalen (Gesichtszüge, Fingerabdrücke, DNA, Stimme, Verhaltenssignale) in öffentlich zugänglichen Räumen verlangt. Auch sollen KI-Systeme verboten werden, die natürliche Personen nach biometrischen Merkmalen in Cluster eingruppieren oder zur Emotionserkennung verwenden.

Der EDSA und der EDSB halten es für sinnvoll die Datenschutzbehörden als nationale Aufsichtsbehörden im Sinne des Art. 59 KI-VO zu bestimmen, um so einen einheitlichen Regulierungsansatz zu ermöglichen und dazu beizutragen, dass die Mitgliedstaaten die Datenverarbeitungsvorschriften einheitlich auslegen und Widersprüche in deren Durchsetzung vermeiden. Für grenzüberschreitende Fälle wäre die Zuweisung der Zuständigkeiten unter den nationalen Aufsichtsbehörden erforderlich.

2.4.3 Gesetz über digitale Dienste (Digital Services Act)

Am 15. Dezember 2020 legte die EU-KOM einen Vorschlag zur „Verordnung des Europäischen Parlamentes und des Rates über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG“, den Digital Services Act (DAS), vor. Zusammenfassend regelt der DSA folgendes: Für alle Dienste, die private Kommunikation zwischen Personen anbieten, müssen die Diensteanbieter eine Rechtsvertretung in der EU benennen, auf Anordnungen der Mitgliedstaaten zur Beseitigung illegaler Inhalte reagieren, klare Nutzungsbedingungen haben und Entscheidungen über die Moderation von Inhalten transparent darlegen. Darüber hinaus müssen sie Nutzern eine leicht zugängliche Möglichkeit bieten, illegale Inhalte zu melden, und ihnen Instrumente zur Verfügung stellen, um die Entscheidungen der Plattform anzufechten. Die Mitgliedstaaten benennen Aufsichtsbehörden; eine Behörde ist als unabhängiger „Koordinator für digitale Dienste“ zu bestimmen. Dieser ist für alle Aufsichts- und Vollzugsfragen im Mitgliedstaat verantwortlich und kann genauso wie die EU-KOM sofortige Abhilfemaßnahmen von den Plattformen verlangen und bei Nichtbefolgung die gerichtliche vorübergehende Aussetzung ihres Dienstes beantragen. Der EDSB betont in seiner Stellungnahme (01/2021) vom 10. Februar 2021, dass bei den Aktivitäten der Online-Plattformen regelmäßig die Verarbeitung personenbezogener Daten tangiert sei, so dass der DSA die DS-GVO ergänze. Insofern sei notwendig, die Komplementarität bei der Überwachung und Beaufsichtigung von Online-Plattformen und anderen Hosting-Dienstleistern sicherzustellen. Ferner bewertet der EDSB das Profiling im Zusammenhang mit Online-Werbung und Empfehlungssystemen als hochrisikoreich und fordert höhere Sicherheitsvorkehrungen und Transparenz. Bei der Moderation von Inhalten sollte das Profiling wegen der hohen Risiken der Manipulation verboten werden. Langfristig sollte die gezielte Online-Werbung aufgrund Profilings abgeschafft werden.

Insbesondere fordert der EDSB eine Rechtsgrundlage für eine strukturelle Zusammenarbeit der Aufsichtsbehörden mit den Datenschutzbehörden, den Verbraucherschutzbehörden und den Wettbewerbsbehörden.

Der DSA wurde als Verordnung (EU) 2022/2065 des Europäischen Parlamentes und des Rates über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) am 19. Oktober 2022 erlassen und gilt seit dem 17. Februar 2024 (ABl. L 277, S. 1).

2.4.4 Gesetz über digitale Märkte (Digital Markets Act)

Am 15. Dezember 2020 legte die EU-KOM einen Vorschlag zur „Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor“, den Digital Markets Act (DMA), vor. Mit dem Vorschlag werden Ex-ante-Regulierungsmaßnahmen eingeführt, um sicherzustellen, dass auf Märkten, die von großen Plattformen mit erheblichen Netzwerkeffekten gekennzeichnet sind („Gatekeeper“), Fairness und Wettbewerbsmöglichkeiten sichergestellt bleiben. Aufsichtsbehörde ist die EU-KOM. Der EDSB betont in seiner Stellungnahme (02/2021) vom 10. Februar 2021, dass bei den Aktivitäten der Online-Plattformen regelmäßig die Verarbeitung personenbezogener Daten u. a. in Form des verdeckten Trackings tangiert sei, so dass der DMA die DS-GVO ergänze. Er forderte benutzerfreundliche Einwilligungslösungen und einen höheren Fokus auf die wirksame Anonymisierung personenbezogener Daten.

Der DMA wurde als Verordnung (EU) 2022/1925 des Europäischen Parlamentes und des Rates über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte) am 14. September 2022 erlassen und gilt seit dem 2. Mai 2023 (ABl. L 265, S. 1).

2.5 Internationale Datenschutzkonferenz

Die 43. Internationale Datenschutzkonferenz (Global Privacy Assembly, GPA) fand vom 20. bis 21. Oktober 2021 mit mehr als 150 Mitgliedern als reine Online-Veranstaltung unter der Gastgeberschaft der Datenschutzbehörde Mexicos (National Institute for Transparency, Access to Information and Personal Data Protection of Mexico, INAI) unter dem Motto „Privatsphäre und Datenschutz: Der Mensch im Mittelpunkt“ („Privacy and Data Protection: A human centric approach“) statt. Folgende Top-Themen waren Gegenstand der Diskussionen: Datengestützte Innovation für das Gemeinwohl, Zusammenarbeit bei der Durchsetzung und Förderung der Innovation durch Engagement.

Im Hinblick auf die zukünftige Entwicklung der GPA haben die Mitgliederbehörden beschlossen, dass die Organisation sich auf die praktische und umgehende Beratung für internationale Organisationen, politische Entscheidungsträger und andere Akteure konzentrieren sollte, damit sie auch weiterhin auf internationaler Ebene Gehör findet.

Zudem sollte die GPA auch weiterhin ein Augenmerk auf die Bedeutung des Datenschutzes durch Technik und die Schaffung angemessener Garantien, die in Einklang mit dem internationalen Recht und regulatorischen Rahmen stehen müssen, legen.

Folgende strategische Prioritäten für 2021 bis 2023 wurden bestätigt: Förderung des globalen Datenschutzes im Zeitalter der beschleunigten Digitalisierung, Maximierung der Stimme und des Einflusses der GPA, Ausbau der Expertise der GPA Mitglieder.

Die Konferenz verabschiedete nachfolgende, im Konsens angenommene Entschließungen: zur gemeinsamen Nutzung von Daten für das öffentliche Wohl, zu den digitalen Rechten von Kindern, zum Zugang zu Daten, Privatsphäre und die Rechtsstaatlichkeit: Grundsätze des staatlichen Zugriffs auf personenbezogene Daten für die nationale Sicherheit und die öffentliche Sicherheit. Zudem wurde die Entscheidung der Einrichtung eines durch Mitgliedsbeiträge finanzierten GPA-Sekretariates angenommen.

Die Konferenz hat sich zudem einen neuen Vorsitz gewählt. Blanca Lilia Ibarra Cadena, die Direktorin der Datenschutzbehörde Mexicos, übernimmt den Vorsitz der GPA von Elizabeth Denham, der ehemaligen Chefin der britischen Datenschutzbehörde (Information Commissioner's Office, ICO). Schließlich wurde ein neues Gremium, das „Reference Panel“ geschaffen, das mit Datenschutzexpertinnen und -experten unter dem Vorsitz des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit besetzt ist und u. a. die Berichte und Papiere der Arbeitsgruppen der GPA bei Bedarf fachlich prüfen soll.

Weiterführende Informationen finden sich auf der Webseite der GPA.[4] Das Angebot steht ausschließlich in englischer Sprache zur Verfügung.

3 Technik und Organisation

3.1 BAföG Digital

Das Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz, OZG) verpflichtet Bund, Länder und Kommunen, bis Ende 2022 ihre Verwaltungsleistungen über ein Bund-Länder-Portal auch digital anzubieten. Für die Bereitstellung der Verwaltungsleistungen haben Bund und Länder das „Einer-für-alle-Prinzip“ vereinbart. Nach dieser Vereinbarung ist Sachsen-Anhalt für das Themenfeld Bildung zuständig und betreut in diesem Zusammenhang das Projekt BAföG Digital. Das Ministerium für Wirtschaft, Wissenschaft und Digitalisierung hat dem Landesbeauftragten ein Datenschutzkonzept für den Online-Antragsassistenten BAföG Digital vorgelegt. Der Landesbeauftragte hat das Ministerium hierzu beraten.

Gegenstand des Datenschutzkonzepts ist ein Antragsportal mit einem Online-Antragsassistenten, mit dem online Anträge auf Ausbildungsförderung gestellt werden können. Die Bearbeitung des Antrags erfolgt durch das einzelne für Ausbildungsförderung zuständige Amt mit dem jeweiligen Fachverfahren. Der Antragsassistent unterstützt beim Ausfüllen der Antragsformulare, die bereits für BAföG-online genutzt wurden. Maßgeblich hierfür ist die BAföG-Formblatt-Verwaltungsvorschrift des Bundesministeriums für Bildung und Familie mit Zustimmung des Bundesrates. Basis der Umsetzung dieses „Einer-für-alle-Verfahrens“ ist eine Verwaltungsvereinbarung von Bund

[4] https://globalprivacyassembly.org/

und Ländern, in der das Land Sachsen-Anhalt als Rechteinhaber benannt wird, welches das Ministerium für Wirtschaft, Wissenschaft und Digitalisierung als Verantwortlichen nach Art. 4 Nr. 7 zweiter Halbsatz DS-GVO festlegt. Mit der technischen Unterstützung und für den technischen Support ist der zentrale IT-Dienstleister Dataport A. ö. R. beauftragt.

Das Ministerium hält die Datenverarbeitung durch den Antragsassistenten gem. Art. 6 Abs. 1 lit. e DS-GVO i. V. m. § 4 Satz 1 Nr. 2 DSAG LSA für zulässig (erforderlich zur Erfüllung einer in der Zuständigkeit des Verantwortlichen liegenden Aufgabe, deren Wahrnehmung im öffentlichen Interesse liegt). Nach Art. 4 Nr. 7 zweiter Halbsatz DS-GVO könne der Verantwortliche durch Recht der Mitgliedstaaten vorgegeben werden. Dies seien Normen, die eine Rechtspflicht im mitgliedstaatlichen Recht begründen. Verwaltungsvorschriften und auch die vorgenannte Verwaltungsvereinbarung wären insoweit ausreichend.

Fraglich erschien die Rechtsauffassung, dass der bundesweite Betrieb des Online-Assistenten zur Erfüllung einer in der Zuständigkeit eines sachsen-anhaltischen Ministeriums liegenden Aufgabe erfolge, deren Wahrnehmung im öffentlichen Interesse liege. Eine statthafte Aufgabe bzw. ein öffentliches Interesse daran, dass das Land Sachsen-Anhalt personenbezogene Daten von Menschen verarbeitet, die keinen Bezug zu Sachsen-Anhalt aufweisen, ist nur bedingt erkennbar. Eine Verwaltungsvereinbarung als Zuständigkeitsregelung könnte nicht ausreichend, sondern eine staatsvertragliche Zuweisung der Aufgabe geboten sein. Auch wenn das Recht der Mitgliedstaaten nach Art. 4 Nr. 7 zweiter Halbsatz DS-GVO nicht zwingend ein Parlamentsgesetz fordert, wäre wohl zumindest eine parlamentsgesetzliche Ermächtigung und eine Veröffentlichung in einem außenwirksamen Regelwerk zu fordern.

Weiter wirft die Konzeption die Frage einer gemeinsamen Verantwortlichkeit auf. Diese liegt nach Art. 26 DS-GVO vor, wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung festlegen. Nach dem Datenschutzkonzept entscheidet das Ministerium für Wirtschaft, Wissenschaft und Digitalisierung des Landes Sachsen-Anhalt in Abstimmung mit den teilnehmenden Ländern im Lenkungskreis BAföG Digital über Inhalt, Zweck und Mittel der Verarbeitung von personenbezogenen Daten. Auch in der Verwaltungsvereinbarung werden Zwecke und Mittel der Datenverarbeitung gemeinsam bestimmt. Die strategische und operative Steuerung erfolgt über den gemeinsamen Lenkungskreis. Es liegt eine gewollte und bewusste Zusammenarbeit vor. Die Vertragsparteien nehmen Einfluss bzw. halten sich diesen durch die Verwaltungsvereinbarung offen. Diese Einflussnahme erfolgt auch im eigenen Interesse, da die Länder gehalten sind, Onlinezugänge zu gestalten. Zwar ist es im Fall des Antragsassistenten die Regel, dass fast alle der Beteiligten mit Ausnahme des verarbeitenden Landes Sachsen-Anhalt und des Landes, aus dem der Antragsteller kommt, sowie des Landes in dem die zuständige Fachbehörde sitzt, kein Interesse und auch keine Befugnis haben die Daten des jeweiligen Antragstellers zu verarbeiten. Insoweit ist aber zu berücksichtigen, dass es für die gemeinsame Verantwortlichkeit mehrerer Betreiber für dieselbe Verarbeitung nicht zwingend erforderlich ist, dass jeder Zugang zu den personenbezogenen Daten hat. Insgesamt liegt eine gemeinsame Verarbeitung von Bund und Ländern nahe.

Auch die Frage nach den Rechtsgrundlagen für die Verarbeitung personenbezogener Daten ist problematisch. Insoweit könnte das Ministerium wohl für die landeseigenen Fälle auf § 4 DSAG LSA zurückgreifen. Andere Länder könnten, soweit sie durch den

Wohnsitz des Antragstellers bzw. den Sitz des Amtes für Ausbildungsförderung betroffen sind, ggf. auf ihre allgemeinen datenschutzgesetzlichen Befugnisse zurückgreifen. Es verbliebe dann aber noch die Notwendigkeit, für das Ministerium im Falle seiner Nichtbeteiligung (kein Bürger und kein Amt aus Sachsen-Anhalt) eine Rechtsgrundlage zu finden. Dies könnte wohl nur durch eine Auftragsverarbeitung mit dem jeweiligen Land bzw. der zuständigen Stelle gemäß Art. 28 DS-GVO geschehen, sodass die Tätigkeit insoweit privilegiert wäre.

Der Landesbeauftragte hat das Ministerium umfassend beraten und eine Anpassung der Vereinbarungen und vertraglichen Ausgestaltungen angeregt. Weiter ist beabsichtigt, die Problematik auch in den Kreisen der Datenschutzaufsichtsbehörden zu erörtern. Das Ministerium ist aber zunächst seinem ursprünglichen Konzept gefolgt.

3.2 Verschlüsselte Datenübertragung bei Funkmesszählern

Ein Funkmesszähler ist ein Messgerät, das Verbrauchsdaten für Heizung, Warmwasser oder Strom automatisch erfasst und diese per Funk an ein Auslesegerät oder einen Server übermittelt. Im Gegensatz zu herkömmlichen Zählern, bei denen der Zählerstand von einer Person abgelesen werden muss, ermöglicht der Funkmesszähler eine Fernablesung. Die Verbrauchswerte werden regelmäßig an eine zentrale Einheit übertragen, die bei Bedarf ausgelesen werden kann, ohne dass jemand die Wohnung betreten muss.

Die Daten, die ein Funkmesszähler erfasst und versendet, können als personenbeziehbar betrachtet werden, da sie Auskunft über die Lebensverhältnisse natürlicher Personen geben können. Jedoch sind die Daten technisch kodiert und können nicht ohne professionelle Hilfsmittel erfasst werden. Außerdem sind die Daten pseudonymisiert, denn Sie enthalten keine Namen und Adressen. Lediglich über die Zählernummer können sie in der Abrechnungszentrale einem Vertragspartner und damit einer Person bzw. einem Haushalt zugeordnet werden.

Ein Risiko, dass Unbefugte dieses Signal und damit die Daten empfangen, ist vorhanden, weil die Daten oft in einem lesbaren unverschlüsselten Format und einem offenen Standard mindestens bis zum meist im Hausflur befindlichen Auslesegerät gesendet werden. Das Gesamtrisiko scheint jedoch sehr gering zu sein. Zum einen ist die Eintrittswahrscheinlichkeit, dass Unbefugte mit professionellem technischem Gerät das Signal auffangen gering und zum anderen ist der zu erwartende Schaden niedrig. Bislang sind dem Landesbeauftragten keine Missbrauchsfälle bekannt.

Da die marktführenden Hersteller von Funkmesszählern seit spätestens 2020 Geräte mit verschlüsselter Datenübertragung anbieten, kann das unverschlüsselte Aussenden des Signals nicht länger als Stand der Technik betrachtet werden und muss grundsätzlich nicht mehr hingenommen werden. Es ist daher zu prüfen, ob Geräte mit unverschlüsselter Datenübertragung zeitnah durch verschlüsselte Versionen ersetzt werden können, da die ausgesendeten Daten gem. Art. 32 DS-GVO gegen unbefugte Zugriffe zu schützen sind. Bereits in Nr. 4.11 seines XII. Tätigkeitsberichts sprach der Landesbeauftragte diese Empfehlung aus, noch bevor verschlüsselte Geräte flächendeckend von den Marktführern angeboten wurden.

Insgesamt muss im Rahmen einer Abwägung das Gesamtrisiko unter Berücksichtigung des Standes der Technik den Implementierungskosten gegenübergestellt werden. Die Aufsichtsbehörde wird kaum verlangen können eine Millioneninvestition durchzuführen, um ein nicht nachweisbares vermeintliches Missbrauchsrisiko abzuwenden. Dies gilt z. B. wenn bereits verbaute Funkmesszähler zu einem Zeitpunkt bestellt wurden, als noch keine verschlüsselten Geräte bestellbar waren und dann für die Dauer der Eichfrist von sechs Jahren verbaut bleiben sollten und der organisatorische wie finanzielle Aufwand für den vorfristigen erneuten Austausch der Geräte enorm ist.

3.3 Versehentlicher Erwerb von personenbezogenen Daten

Wenn eine natürliche oder juristische Person ein mobiles Endgerät wie z. B. einen Laptop gebraucht oder refurbished erwirbt und darauf personenbezogene Daten Dritter vorfindet, so muss der Vorgang zunächst als unrechtmäßige Übermittlung durch den Vorbesitzer betrachtet werden. Wenn eine Person im Besitz personenbezogener Daten Dritter – ob rechtmäßig oder unrechtmäßig erhoben – ist, obliegt ihr auch die Verantwortung über den Umgang mit den Daten. Sie kann das Gerät mit den personenbezogenen Daten dann nicht einfach weiter- oder zurückgeben. Als für die Verarbeitung Verantwortliche ist sie verpflichtet, das Gerät zurückzugeben oder die Daten so zu löschen, dass diese später von keinem Unbefugten eingesehen oder rekonstruiert werden können. In jedem Fall sollte der Absender informiert werden.

Beim Löschen reicht es nicht aus, die Daten in den Papierkorb des Betriebssystems zu verschieben, denn von dort können diese sofort wiederhergestellt werden. Auch das dauerhafte Entfernen der Daten, indem z. B. der Papierkorb geleert wird, entspricht noch nicht der irreversiblen Löschung der Daten, denn eigentlich werden die Daten auch dabei noch nicht gelöscht, sondern auf der Festplatte des Gerätes wird nur vermerkt, dass der Speicherbereich, in dem die Daten vorher lagen, nun für das erneute Überschreiben freigegeben ist. Solange allerdings noch keine neuen Daten geschrieben wurden, liegen die alten Daten weiterhin im Speicher vor und können mit Rekonstruktionsprogrammen wiederhergestellt werden.

Das Überschreiben des gesamten freien Speichers einer Festplatte gelingt z. B. unter Verwendung des in Windows enthaltenen Kommandozeilenprogrammes cipher.exe.[5] Es können aber auch Programme anderer Hersteller zum irreversiblen Löschen bzw. Überschreiben freien Speicherplatzes, wie z. B. Secure Eraser[6], Eraser[7] oder Boot and Nuke[8], genutzt werden.

[5] https://www.wintotal.de/tipp/mit-dem-kommandozeilenprogramm-cipher-freien-speicherplatz-sicher-loeschen/

[6] https://www.heise.de/download/product/secure-eraser-standard-edition-11878

[7] https://www.heise.de/download/product/eraser-18980

[8] https://www.heise.de/download/product/dariks-boot-and-nuke-dban-54943

Erst wenn alle personenbezogenen Daten in den Papierkorb gelegt wurden, dieser dann geleert wurde und anschließend noch der gesamte verbleibende freie Festplattenspeicher sicher überschrieben wurde, kann davon ausgegangen werden, dass die Daten nicht ohne extrem hohe forensische Aufwände wiederhergestellt werden können.

3.4 Akkreditierung und Zertifizierung

Jede Zertifizierungsstelle überträgt mit jedem ausgegebenen Zertifikat das in sie gesetzte Vertrauen und entsprechende Qualitätserwartungen auf das hinsichtlich der DS-GVO-Einhaltung geprüfte Produkt oder die geprüfte Dienstleistung. Verlässliche Datenschutzzertifikate und -gütesiegel dienen Verbrauchern als Wegweiser hin zu datenschutzgerechten Produkten und sind ein unübersehbarer Wettbewerbsvorteil. Stellen, die solche Zertifikate für DS-GVO-gerechte Produkte, Dienstleistungen oder Prozesse ausgeben wollen, müssen sich daher im Vorfeld durch die Deutsche Akkreditierungsstelle (DAkkS), in Zusammenarbeit mit der jeweils zuständigen Aufsichtsbehörde, akkreditieren lassen.

In seinem XVI. Tätigkeitsbericht (Nr. 6.6) gab der Landesbeauftragte einen Überblick über die Möglichkeit einer Zertifizierung, die Abläufe und die Notwendigkeit einer vorherigen Akkreditierung durch die DAkkS. Im XVII. Tätigkeitsbericht (Nr. 6.6) wurde auf die der Prüfung zugrunde liegende Norm EN-ISO/IEC 17065/2012 „Konformitätsbewertung – Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren“ eingegangen und es wurde das durch die Aufsichtsbehörden gemeinsam erarbeitete Dokument „Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO i. V. m. DIN EN ISO/IEC 17065“ mit ergänzenden Anforderungen aus dem Datenschutzbereich vorgestellt. Die Anforderungen beider Dokumente sind dauerhaft einzuhalten und nachzuweisen. Auch wurde auf die Norm DIN EN ISO/IEC 17067:2013-12 2 „Konformitätsbewertung – Grundlagen der Produktzertifizierung und Leitlinien für Produktzertifizierungsprogramme (ISO/IEC 17067:2013); Deutsche und Englische Fassung EN ISO/IEC 17067:2013“ verwiesen, welche die Festlegung von Prüfkriterien, -systematik und -methoden erfordert. Datenschutzrechtliche Anforderungen sind daher in einem Prüfkriterienkatalog vorzulegen (Art. 42 DS-GVO), welcher in Form von Zertifizierungskriterien im Zertifizierungsprogramm der Zertifizierungsstelle oder des Programmeigners enthalten ist.

Will eine Stelle oder ein Unternehmen als Zertifizierungsstelle auftreten, müssen Akkreditierungsvoraussetzungen erfüllt werden. Daneben muss der Kriterienkatalog von der Aufsichtsbehörde genehmigt werden. Im Unterarbeitskreis „Prüfkriterien“ des AK Zertifizierung wurde an einem Dokument „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme; Datenschutzrechtliche Prüfkriterien, Prüfsystematik und Prüfmethoden zur Anpassung und Anwendung der technischen Norm DIN EN ISO/IEC 17067 (Programmtyp 6)“[9] zur deutschlandweit einheitlichen Bewertung solcher Prüfkriterienkataloge gearbeitet, welches Anfang 2021 von der DSK verabschiedet worden ist.

[9] https://www.datenschutzkonferenz-online.de/media/ah/DSK_Anwendungshinweis_Zertifizierungskriterien.pdf

Grundlagen für das Papier waren die Vorgaben für Zertifizierungsprogramme aus den EDSA-Leitlinien (vgl. XVII. Tätigkeitsbericht, Nr. 6.6), Art. 43 DS-GVO, die DIN EN ISO/IEC Normen 17065 und 17067 und die Anwendungshinweise „Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO i. V. m. DIN EN ISO/IEC 17065“ der DSK.[10] Neben der Bewertung eines vorgelegten Prüfkriterienkatalogs durch die Datenschutzaufsichtsbehörde dient das Papier aber insbesondere auch dem Antragsteller zur eigenen Vorabüberprüfung der vorgelegten Kriterien.

Entlang der relevanten Artikel der DS-GVO werden die Erwartungen an ein Zertifizierungsprogramm beschrieben. Dabei werden die gesetzlichen Tatbestandsmerkmale, die in den Zertifizierungskriterien zu behandelnden Prüfthemen und deren Umsetzung durch die Kunden der Zertifizierungsstelle und die Art und Weise der Prüfung der Umsetzung durch die Zertifizierungsstelle kurz vorgestellt.

Auf europäischer Ebene werden die Themen Akkreditierung und Zertifizierung in der „Compliance, e-Government und Health Expert Subgroup“ (CEH Expert Subgroup) behandelt. In dieser Arbeitsgruppe wurden die „Guidance on certification criteria assessment“[11] als Nachtrag zu den Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679[12] veröffentlicht.

2021 gibt es in Sachsen-Anhalt noch keine nach Art. 42 und 43 DS-GVO akkreditierte Zertifizierungsstelle.

3.5 Informationssicherheit (AG InfoSic Land)

Die AG InfoSic ist eine Arbeitsgruppe des IT-Planungsrats, die sich mit der Informationssicherheit in der öffentlichen Verwaltung befasst. Sie unterstützt den IT-Planungsrat in Fragen der IT-Sicherheit und fördert die Zusammenarbeit zwischen Bund, Ländern und Kommunen. Auf Landesebene gibt es die AG InfoSic (Land). Diese befasst sich ebenfalls mit dem Thema Informationssicherheit und ergänzt die Aktivitäten der AG InfoSic des IT-Planungsrats und trägt dazu bei, die Informationssicherheit in der öffentlichen Verwaltung in Sachsen-Anhalt umfassend zu stärken. Sie fördert die Zusammenarbeit zwischen verschiedenen Akteuren, darunter Landesbehörden, Kommunen und IT-Dienstleistern und entwickelt und koordiniert konkrete Maßnahmen zur Verbesserung der Informationssicherheit.

---

[10] https://www.datenschutzkonferenz-online.de/media/ah/20201008_din17065_Ergaenzungen_deutsch_nach_opinion.pdf
https://www.datenschutzkonferenz-online.de/media/ah/20201008_german_accreditation17065_eng_nach_opinion.pdf

[11] https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidance-certification-criteria-assessment_de

[12] https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_de

Die Mitglieder der Arbeitsgruppe Informationssicherheit (AG InfoSic) Sachsen-Anhalt sind im Wesentlichen die Informationssicherheitsbeauftragten (ISB) der obersten Landesbehörden unter Leitung des Informationssicherheitsbeauftragten des Landes (CISO). Als Teil des Informations-Sicherheits-Management-Systems (ISMS) des Landes obliegt ihr eine wichtige Schlüsselrolle bei der Umsetzung einer einheitlichen und effizienten Informationssicherheitsstrategie im Land. Die AG InfoSic (Land) als ein Arbeitsgremium mit immer mehr Aufgaben und stetig steigendem Arbeitsaufwand hat sich im Berichtszeitraum eine Geschäftsordnung gegeben, um Sitzungen schnell und geregelt durchführen zu können. Diese regelt die wesentlichen Aspekte der Zusammenarbeit im Gremium. Alle Beschlüsse werden in der AG diskutiert, abgestimmt und abschließend beschlossen, wobei die Wirkung primär intern bleibt. Die Treffen fanden im Berichtsjahr ausschließlich virtuell statt.

Die Landesregierung von Sachsen-Anhalt hat zum 16. September 2021 das Ministerium für Infrastruktur und Digitales des Landes Sachsen-Anhalt (MID) gegründet. Ministerin wurde Dr. Lydia Hüskens. Das MID übernahm das Digitalressort vom Ministerium für Wirtschaft, Tourismus, Landwirtschaft und Forsten (MW) sowie die Zuständigkeit für die Informationssicherheit vom Ministerium der Finanzen (MF). Diese Zusammenführung markierte einen wichtigen Schritt zur Stärkung der Digitalisierung in Sachsen-Anhalt. Unter dem MID wurde eine stärkere Fokussierung auf digitale Themen und IT-Sicherheit möglich.

Die AG InfoSic (Land) wechselte im Zuge der Umstrukturierung ebenfalls vom MF zum MID.

Kurz nach der Regierungsbildung übernahm Staatssekretär Bernd Schlömer die Aufgabe des Beauftragten der Landesregierung für Informations- und Kommunikationstechnologie (CIO). Herr Schlömer sah in der Informationssicherheit eine große Herausforderung und nahm in seiner Funktion als CIO als Gast teil. Die ISB der Ressorts übergaben dem CIO ein Positionspapier, in welchem die Schwerpunkte für die nächsten Aufgaben dargestellt wurden.

Der IT-Kooperationsrat beschloss die Einrichtung einer Unterarbeitsgruppe der AG InfoSic unter der Leitung des MF mit dem Ziel der Einbindung der Kommunen in das ISMS des Landes. Die UAG soll die Zusammenarbeit von Land und Kommunen im Bereich der Informationssicherheit mit dem Schwerpunkt der Entwicklung einer Lösung zum schnellen Informationsaustausch von Warn- und Informationsmeldungen zu Sicherheitslücken sowie bei Sicherheitsvorfällen verbessern.

Im XVII. Tätigkeitsbericht (Kapitel 6.13) wurde über das Inkrafttreten der Leitlinie zur Informationssicherheit der unmittelbaren Landesverwaltung Sachsen-Anhalt (LISL LSA, Informationssicherheitsleitlinie) des Landes und die damit einhergehende beginnende Erstellung belastbarer IT-Sicherheitsrichtlinien (ISRL) berichtet. Die ersten ISRL, die Passwort- und die Telearbeits-RL, befanden sich bereits auf der Zielgeraden und wurden nach Einarbeitung offener Rückmeldungen zügig vollendet. Die ISRL zum „Umgang mit Sicherheitsvorfällen“ wurde finalisiert, Umsetzungshinweise zu den Anforderungen ausgearbeitet. Weitere Arbeiten erfolgten – teils in UAGs – an ISRL und Prozessbeschreibungen betreffend das Dokumentenmanagement, Korrektur- und Vorbeugemaßnahmen, Organisation und Personal, Berichtswesen, Risikomanagement und dem landesweiten Sicherheitsprozess.

Intensiv wurde in der UAG „BITS“ am Behörden-IT-Sicherheitstraining gearbeitet. Ziel war die Anpassung vorhandener Inhalte an die Bedürfnisse der Landesverwaltung. BITS ist ein kostenloses webbasiertes Online-Training, das Beschäftigte in Behörden und öffentlichen Einrichtungen für die Gefahren der IT-Nutzung sensibilisiert. Es vermittelt grundlegende Kenntnisse und Verhaltensweisen, um die Informationssicherheit zu erhöhen und sensible Daten zu schützen.

Im Berichtszeitraum erfolgte ein Cyberangriff auf den Landkreis Anhalt-Bitterfeld. Eine Ransomware legte die IT-Infrastruktur des Landkreises durch Verschlüsselung von Dateien lahm. Der Landkreis rief den Katastrophenfall aus, um schnellere Hilfe von anderen Behörden zu erhalten. Das war das erste Mal, dass in Deutschland aufgrund eines Cyberangriffes der Katastrophenfall ausgerufen wurde. Der CISO unterstützte vor Ort. Es entstand ein erheblicher finanzieller Schaden, hauptsächlich durch die aufgrund von Datenverlusten eingetretene Handlungsunfähigkeit der Verwaltung. Der Vorfall verdeutlichte die Anfälligkeit öffentlicher Verwaltungen für Cyberangriffe und führte zu einem verstärkten Bewusstsein für die Bedeutung von Cybersicherheit in Deutschland. Alle verantwortlichen Stellen sollten aus dem Vorfall lernen, ihre IT-Sicherheitsmaßnahmen und Krisenmanagementpläne auf mögliche Verbesserungen prüfen und diese zügig umsetzen und dauerhaft verbessern.

Bereits im letzten Tätigkeitsbericht wurde darüber informiert, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) Ländern Dienstleistungen anbietet und diese insbesondere bei der Absicherung ihrer IT unterstützen kann. Der Abschluss einer Kooperationsvereinbarung „Zusammenarbeit mit dem BSI auf Bund-Länder Ebene“ wurde angestrebt. Bereits im Jahr 2018 erfolgten erste Gespräche mit dem BSI mit dem Ziel des Abschlusses einer Absichtserklärung. Dem folgte 2019 ein Vorschlag Dataports zu einer Absichtserklärung für eine länderübergreifende Zusammenarbeit mit dem BSI. 2020 erfolgte die Abstimmung einer Absichtserklärung für Sachsen-Anhalt mit dem Verbindungsbüro des BSI. Das Ministerium für Inneres und Sport (MI) erhielt durch die Länderarbeitsgruppe (LAG) Cybersicherheit der IMK den Entwurf einer Kooperationsvereinbarung im Bereich der Cybersicherheit: MI und MF sollten eine gemeinsame Kooperationsvereinbarung für Informations- und Cybersicherheit mit dem BSI für das Land schließen. Nach Diskussionen und rechtlichen Prüfungen wurde nun eine standardisierte Kooperationsvereinbarung im Bereich Cyber- und Informationssicherheit zwischen der LAG Cybersicherheit, der AG InfoSic (Bund) und dem BSI abgestimmt, welche per Umlauf in der AG versandt wurde. Nach landesspezifischen Anpassungen lag sie sodann dem MI zur Stellungnahme vor. Die Unterzeichnung der Kooperationsvereinbarung sollte dann im nächsten Jahr erfolgen.

3.6 Besonderes elektronisches Behördenpostfach

Der Elektronische Rechtsverkehr (ERV) dient dem Austausch elektronischer Dokumente zwischen Behörden, Bürgern und Gerichten. Ein sicherer Austausch allein reichte dazu nicht, notwendig war es auch, dass dieser rechtlich wirksam erfolgt. Bereits ab 2001 wurden u. a. mit dem Formvorschriftenanpassungsgesetz und dem Zustellungsreformgesetz die Vorrausetzungen dafür geschaffen, die Schriftform durch die elektronische Form ersetzen zu können. Durch das Justizkommunikationsgesetz (JKomG) wurden 2005 die rechtlichen Rahmenbedingungen geändert, um den elektronischen Zugang zu Gerichtsakten und den elektronischen Austausch von Dokumenten zu ermöglichen und so Prozessakten elektronisch führen zu können. 2013 folgte

das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten, welches die Nutzung elektronischer Kommunikationsmittel im Rechtsverkehr mit den Gerichten verbessert. 2017 folgte dann die Elektronischer-Rechtsverkehr-Verordnung (ERVV). Sie regelt die technischen Rahmenbedingungen für den elektronischen Rechtsverkehr sowie die Nutzung des besonderen elektronischen Behördenpostfachs. Es folgte im selben Jahr das Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs. Der Name ist hier Programm. Damit waren 2018 die Weichen für die elektronische Übertragung von Dokumenten unter Wahrung der Schriftformerfordernis via Elektronischem Gerichts- und Verwaltungs-Postfach (EGVP) gemäß § 130a Abs. 4 ZPO per sicherem Übermittlungsweg gestellt. Für Behörden und juristische Personen des öffentlichen Rechts bot sich dafür die Einrichtung eines besonderen elektronischen Behördenpostfachs (beBPo) an. Der Landesbeauftragte war ein „Early Adopter“. Die Nutzungshäufigkeit steigt seitdem stetig an.

In seinem XVII. Tätigkeitsbericht für das Jahr 2020 (Nr. 2.4) hatte der Landesbeauftragte noch die Absicht geäußert, zusätzlich zum elektronischen Behördenpostfach auch ein De-Mail-Konto zur Kommunikation mit Bürgerinnen und Bürgern einzurichten. Dazu sollte nur noch der Abschluss eines Rahmenvertrages mit einem Dienstleister durch das Ministerium der Finanzen abgewartet werden. Das hat sich mittlerweile von selbst erledigt: Offenbar gab es zu geringe Nutzerzahlen. Im Berichtszeitraum kündigte die Telekom als großer De-Mail-Anbieter an, dass der Dienst eingestellt werden sollte. Auch der Bundesrechnungshof sah das so und meinte, das Bundesinnenministerium (BMI) sei dabei gescheitert, De-Mail „als elektronisches Pendant zur Briefpost in der Bundesverwaltung zu etablieren“. Der Landesbeauftragte sah daher von einer Einführung eines De-Mail-Zugangs ab.

De-Mail sollte einer „sicheren, vertraulichen und nachweisbaren“ Kommunikation für jedermann im Internet dienen (§ 1 Abs. 1 De-Mail-Gesetz). Aber schnell war klar, dass die Kosten für die Nutzung zwar niedriger als bei der Papierpost, aber dennoch hoch genug waren, um eine umfassende Nutzung zu untergraben. Neben den Gebühren, sorgten dann auch der komplizierte Anmeldeprozess (Identifizierung), fehlende Verbreitung (der Empfänger musste ebenfalls einen Account haben), Konkurrenz (PGP und S/MIME), fehlende Integration in behördliche Kommunikation und Fachverfahren und zu wenig Förderung durch den Staat für fehlende Nutzerzahlen. Bundeseinrichtungen sollten bereits seit 2015 und Gerichte seit 2018 De-Mail nutzen, die Realität sah oft anders aus: Totalverweigerung und Ignoranz. Städte und Gemeinden waren nur optional dabei.

4 Telekommunikation und Medien

4.1 Orientierungshilfe für Anbieterinnen und Anbieter von Telemedien

Cookies und ähnliche Technologien werden beim Betrieb von Telemedien, wie z. B. Webseiten oder Apps, regelmäßig eingesetzt, um das Verhalten der Nutzerinnen und Nutzer im Internet zu verfolgen. Seit Inkrafttreten des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (Telekommunikation-Telemedien-Datenschutzgesetz, TTDSG) am 1. Dezember 2021

können sich Webseiten- und App-Betreiber dabei nicht mehr auf ihr berechtigtes Interesse nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO berufen. Gemäß § 25 Abs. 1 TTDSG ist die Speicherung von Informationen wie z. B. Cookies auf einem Endgerät sowie der Zugriff auf diese Informationen grundsätzlich nur mit vorheriger Einwilligung der Nutzerinnen und Nutzer zulässig.

Nach § 25 Abs. 2 TTDSG kann auf das Einholen einer Einwilligung nur dann verzichtet werden, wenn der Einsatz der Cookies oder ähnlicher Technologien unbedingt erforderlich ist, um einen vom Nutzer ausdrücklich gewünschten Dienst zur Verfügung stellen zu können. Als technisch notwendig können etwa Cookies angesehen werden, die für eine Warenkorbfunktion genutzt werden oder die Spracheinstellung speichern. Auch Cookies, die zur Abwehr von Angriffen eingesetzt werden, sind als technisch notwendige Cookies zu bewerten.

Mit Blick auf die neue Rechtslage hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 20. Dezember 2021 als Hilfestellung die Orientierungshilfe für Anbieterinnen und Anbieter von Telemedien (OH Telemedien 2021) veröffentlicht.[13] Darin finden sich u. a. Hinweise für die Praxis, welche Cookies und ähnliche Technologien unter den Voraussetzungen des TTDSG auch ohne Einwilligung zum Einsatz kommen können. Außerdem sind ausführliche Hinweise zu den Voraussetzungen einer wirksamen Einwilligung enthalten.

5 Öffentliche Sicherheit

5.1 Länderübergreifendes Glücksspielaufsichtssystem (LUGAS)

Der Staatsvertrag zur Neuregulierung des Glücksspielwesens in Deutschland (Staatsvertrag) vom 29. Oktober 2020 dient insbesondere der bundesweiten Legalisierung und Regulierung des Online-Glücksspiels. Zur Wahrnehmung der Glücksspielaufsicht beschlossen die Länder, zum 1. Juli 2021 eine rechtsfähige Anstalt des öffentlichen Rechts als „Gemeinsame Glücksspielbehörde der Länder“ (Aufsichtsbehörde) mit Sitz in Sachsen-Anhalt zu errichten.

Das LUGAS dient der Aufsichtsbehörde als Instrument zur bundesweit einheitlichen Überwachung des Online-Glücksspiels und der Glücksspielanbieter. Dazu ist es erforderlich, die personenbezogenen Daten der Spieler zu verarbeiten. Im Zuge dieser Verarbeitung wird die Aufsichtsbehörde Verantwortlicher im Sinne der Datenschutz-Grundverordnung und dem Landesbeauftragten für den Datenschutz obliegt die datenschutzrechtliche Aufsicht hierüber.

Der Landesbeauftragte für den Datenschutz wurde durch das federführende Ministerium für Inneres und Sport des Landes Sachsen-Anhalt frühzeitig in die Projektgruppe zur Erarbeitung des LUGAS eingebunden. Über die Teilnahme an verschiedenen Projektgruppensitzungen und die Erarbeitung datenschutzrechtlicher Stellungnahmen durch den Landesbeauftragten für den Datenschutz flossen die Belange des Datenschutzes umfassend in die Projektarbeit ein.

[13] https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf

Aufgrund der vertrauensvollen und konstruktiven Zusammenarbeit konnte der Landesbeauftragte für den Datenschutz maßgeblich Einfluss auf die Erarbeitung des LUGAS nehmen und im Ergebnis gewährleisten, dass die Verarbeitung der personenbezogenen Daten innerhalb des LUGAS auf das erforderliche Mindestmaß beschränkt wird.

5.2 Prüfung der Rechtmäßigkeit von Videoüberwachungsmaßnahmen der Polizeiinspektionen

Die Polizei darf gemäß § 16 Abs. 2 Satz 2 i. V. m. § 20 Abs. 2 Nr. 1 oder 3 Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt (SOG LSA) Bild- und Tonaufnahmen und -aufzeichnungen (Videoüberwachung) anfertigen. Videoüberwachungsmaßnahmen, auch der Polizei, stellen immer auch einen Eingriff in die informationelle Selbstbestimmung der Passanten im öffentlichen Raum dar. Neben der o. a. Rechtsgrundlage ist zusätzlich vor deren Einrichtung die Verhältnismäßigkeit der jeweiligen Maßnahme zu betrachten (§ 5 SOG LSA und § 3 Abs. 3 Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt (DSUG LSA)).

Der Landesbeauftragte für den Datenschutz prüfte im Jahr 2021 bei den Polizeiinspektionen des Landes Sachsen-Anhalt die Einhaltung des Datenschutzrechts im Bereich der stationären polizeilichen Videoüberwachung. Hierbei wurden verschiedene Kriterien, wie z. B. Notwendigkeit der Maßnahme, Rechtsgrundlage, Verhältnismäßigkeit, Datenschutzrecht und die Evaluierung betrachtet.

Zum Zeitpunkt der Prüfung erhoben die vier Polizeiinspektionen des Landes insgesamt in 20 Videoüberwachungsmaßnahmen personenbezogene Daten. Im Ergebnis der Prüfung blieben alle Videoüberwachungsmaßnahmen der Polizei beanstandungsfrei. Der Landesbeauftragte gab in einzelnen Fällen Hinweise zur Beschilderung der Überwachungsbereiche.

Da es keine gesetzliche Grundlage für die Anzeige von polizeilichen Videoüberwachungsmaßnahmen gegenüber dem Landesbeauftragten für den Datenschutz gibt, ist inzwischen eine regelmäßige Abfrage zu diesen Videoüberwachungsmaßnahmen vorgesehen. Auf diese Weise soll eine aktuelle Übersicht für die Datenschutzaufsichtsbehörde gewährleistet werden.

Die Prüfung des Landesbeauftragten für den Datenschutz führte zu keinen Beanstandungen. Mangels gesetzlicher Anzeigepflicht haben sich der Landesbeauftragte für den Datenschutz und die Polizeiinspektionen des Landes auf ein Regelabfrageverfahren verständigt, um zukünftig einen stets aktuellen Stand der Aufsichtsbehörde zu gewährleisten.

5.3 Einhaltung von Aussonderungsprüf- und Löschfristen beim LKA

Im § 32a Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt (SOG LSA) sind die nach § 31 Abs. 4 Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt (DSUG LSA) festzulegenden Aussonderungsprüf- und Löschfristen geregelt.

Mit Schreiben vom 23. Februar 2021 teilte das Landeskriminalamt (LKA) mit, dass eine große Anzahl von Daten in den polizeilichen Informationssystemen gelöscht worden

sind. Ein Teil dieser Daten diente der Funktionsfähigkeit von bundesweit genutzten Verbundsystemen.

Die gelöschten Daten waren aus datenschutzrechtlicher Sicht teilweise bereits zu löschen gewesen und teilweise weiterhin für die Polizeiarbeit vorhaltbar. Deshalb musste zwischen dem LKA und dem Landesbeauftragten für den Datenschutz eine Lösung gefunden werden, welche eine Wiederherstellung der verarbeitbaren Daten unter Beachtung des datenschutzrechtlichen Rahmens gewährleistet.

In einer gemeinsamen Besprechung am 4. März 2021 zwischen LKA und dem Landesbeauftragten für den Datenschutz unter Beteiligung des Ministeriums für Inneres und Sport des Landes Sachsen-Anhalt verständigten sich die Beteiligten auf eine entsprechende Vorgehensweise.

Im Ergebnis dieses Verfahrens konnte die datenschutzkonforme Rekonstruktion der Daten in den Informationssystemen der Polizei (INPOL) Sachsen-Anhalt am 7. Mai 2021 abgeschlossen werden. Ab diesem Zeitpunkt standen auch die INPOL-Daten für die bundesweite Recherche im Rahmen der Gefahrenabwehr und Strafverfolgung wieder zur Verfügung.

Der Landesbeauftragte für den Datenschutz regte in diesem Zusammenhang an, dass alle kriminalaktenführenden Polizeibehörden für die verschiedenen polizeilichen Informationssysteme prüfen, ob die bestehenden Aussonderungsprüf- und Löschfristen eingehalten werden. Zur Erleichterung bzw. Unterstützung dieses Verfahrens sollten die genutzten Systeme automatisiert auf die erforderliche Prüfung der vorhandenen Datensätze hinweisen und diese Prüfung ggf. als Bedingung für die weitere Bearbeitung einfordern.

Dieser Anregung folgte die Polizei des Landes Sachsen-Anhalt und konnte dies bereits zum Teil umsetzen. Für die noch fehlenden polizeilichen Informationssysteme soll die automatisierte Prüfung perspektivisch folgen.

Unter Beteiligung des Landesbeauftragten für den Datenschutz konnte eine datenschutzkonforme Rekonstruktion der Daten in den Informationssystemen der Polizei realisiert werden. Der Vorfall wurde zum Anlass genommen, die bestehenden Verfahren zur Prüfung der Aussonderungsprüf- und Löschfristen weiter zu verbessern und zu automatisieren.

6 Verkehr

6.1 Zeitpunkt der Abfrage des Fahreignungsregisters (FAER)

Im Berichtszeitraum gingen bei der Behörde des Landesbeauftragten vier Beschwerden ein, die vor dem Hintergrund unterschiedlicher Sachverhaltskonstellationen kritisierten, dass die Polizeiinspektion Zentrale Dienste bei Durchführung des Bußgeldverfahrens Datenabfragen an das FAER zu früh und damit (noch) nicht erforderlich durchführten.

Das Kraftfahrtbundesamt führt auf Grundlage des Straßenverkehrsgesetzes (§ 28 StVG) das FAER. Die Abfrage von Daten aus dem FAER sind für die zuständigen

Verfolgungsbehörden im Rahmen der Bearbeitung von Verkehrsordnungswidrigkeiten regelmäßig erforderlich, um für die Ahndung der Verstöße festzustellen, ob von der betroffenen Person wiederholt Straftaten oder Ordnungswidrigkeiten begangen werden, die im Zusammenhang mit dem Straßenverkehr stehen.

Die Bußgeldbehörde ist gehalten, die zur Verfügung stehenden Ermittlungsansätze unter Beachtung des Grundsatzes der Verhältnismäßigkeit zu ergreifen (§§ 161, 163 StPO i. V. m. § 46 Abs. 2 OWiG). Der Vergleich des Blitzerfotos mit den Halterdaten (§ 35 Abs. 1 Nr. 3 StVG) ist regelmäßig nur der erste Schritt der Fahrerermittlung. Stimmt das Blitzerfoto mit den Halterdaten hinsichtlich des Geschlechts und des Alters überein, wird dem Halter ein Anhörungsbogen, andernfalls ein Zeugenbefragungsbogen zugesandt. Je nach Rückäußerung des Halters ist die Bußgeldstelle nach §§ 46 OWiG, 161 StPO berechtigt, weitere Ermittlungsmaßnahmen zu ergreifen und z. B. von allen Behörden zum Zweck der Verfolgung von Ordnungswidrigkeiten Auskunft zu verlangen. In Frage kommt die Abfrage der Personalien der beim Halter wohnhaften Familienmitglieder / Mitbewohner beim Einwohnermeldeamt, und auch die Herausgabe eines bei der Meldebehörde hinterlegten Lichtbilds (OLG Rostock, 29. November 2004, 2 Ss OWi 302/04 I 178/04; OLG Bamberg, 2. August 2005, 2 Ss OWi 147/2005). Daneben besteht die Möglichkeit, das Internet auszuwerten (BVerfG, 27. Februar 2008 – 1 BvR 370/07 und 1 BvR 595/07) oder durch Polizeibeamte die Adresse des Halters anfahren zu lassen, um sich beim Halter nach dem Fahrer zu erkundigen oder ggf. die Mitbewohner, Familienangehörige, Mitarbeiter, Geschäftskollegen oder Nachbarn zu befragen.

Die Eintragungen im FAER dürfen nach § 30 Abs. 1 Nr. 2 StVG an die Stellen, die für die Verfolgung von Ordnungswidrigkeiten zuständig sind, übermittelt werden, soweit dies für die Erfüllung der diesen Stellen obliegenden Aufgaben zu den in § 28 Abs. 2 StVG genannten Zwecken jeweils erforderlich ist. § 28 Abs. 2 Nr. 3 StVG definiert diesen Zweck mit der Ahndung der Verstöße von Personen, die wiederholt Straftaten oder Ordnungswidrigkeiten, die im Zusammenhang mit dem Straßenverkehr stehen, begehen.

Die Abfrage des FAER setzt als Vorbereitungsmaßnahme für die Zumessung der Buße voraus, dass sich der Tatverdacht hinsichtlich der Fahrereigenschaft des Betroffenen erhärtet hat und der Erlass des Bußgeldbescheides bevorsteht. Im Unterschied zum Anfangsverdacht setzt die Erhärtung des Tatverdachts z. B. die Anhörung des Betroffenen, ggf. zusätzlich Ermittlungsmaßnahmen und eine Beweiswürdigung aller Umstände voraus. In einem früheren Verfahrensstadium kann von einem erhärteten Tatverdacht insbesondere nur bei Vorliegen einer Zeugenaussage, eines Geständnisses oder bei erfolgreichem Bildabgleich nach Internetrecherche ausgegangen werden. Der Betroffene muss andernfalls vor Einleitung weiterer Ermittlungsmaßnahmen (Lichtbildabgleich mit Ausweisfotos, Anfahren der Adresse, Meldedaten von Familienmitgliedern oder anderen Dritten) mit dem Vorwurf konfrontiert und über das Verfahren informiert werden. Solange er noch keine Gelegenheit hatte, sich zu äußern und ggf. eine andere Person als Fahrer zu benennen, werden die Fahreignungsregisterdaten auf Vorrat bzw. vorzeitig, mithin ohne Erforderlichkeit erhoben. Sie sind darüber hinaus potentiell nicht verwertbar, da immer dann, wenn der Halter nicht der Fahrer war, erneut die Fahreignungsregisterdaten des tatsächlichen Fahrers erhoben werden müssen.

Die Heilung dieses Datenschutzverstoßes auch in den Fällen, in denen sich herausstellt, dass der Halter tatsächlich gefahren ist, kann nicht angenommen werden. Eine Heilung wird allenfalls in Einwilligungskonstellationen und dann nur für die Zukunft für möglich erachtet.

Die verfrühten Abfragen wurden durch einen strukturellen Fehler im in mehreren Bundesländern eingesetzten automatisierten Verfahren verursacht, welches daraufhin technisch geändert wurde. Nach erfolgter Halterauskunft wird nunmehr zunächst nur die Betroffenenanhörung erzeugt. Erst nach einer auf 14 Tage festgelegten Zeitspanne erfolgt eine FAER-Abfrage, sofern diese noch erforderlich ist, d. h., wenn sich der Vorwurf nach der Anhörung bzw. dem Ende der diesbezüglichen Frist noch gegen den angeschriebenen Fahrzeughalter richtet. Den Betroffenen wird im Rahmen der Anhörung die Gelegenheit gegeben, sich binnen einer Woche zu dem Tatvorwurf zu äußern und ggf. den tatsächlichen Fahrzeugführer zu benennen.

Unter Berücksichtigung von Postlaufzeiten erscheint eine FAER-Abfrage im Fachverfahren nunmehr erst 14 Tage nach Auslösung der Betroffenenanhörung als sachgerecht und datenschutzrechtlich vertretbar.

Die Abfrage des Fahreignungsregisters setzt die Erhärtung des Tatverdachts voraus. Dies erfordert z. B. die Anhörung des Betroffenen, ggf. zusätzliche Ermittlungsmaßnahmen und eine Beweiswürdigung aller Umstände. Vorzeitige Abfragen sind nicht erforderlich.

7 Schulwesen

7.1 Status der Elternvertretungen

Aufgrund der bedenklichen Datenverarbeitung eines Schulelternratsvorsitzenden eines Gymnasiums hat der Landesbeauftragte die grundsätzliche Frage der datenschutzrechtlichen Verantwortlichkeit nach Art. 4 Nr. 7 DS-GVO für die Datenverarbeitung von Elternvertretungen geklärt.

Nach Art. 4 Nr. 7 DS-GVO ist Verantwortlicher aus datenschutzrechtlicher Sicht die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Elternvertretungen können nicht frei über die Datenverarbeitung und deren Zwecke entscheiden. Vielmehr sind die Zwecke der Datenverarbeitung durch das SchulG LSA geregelt. Auch über die Mittel der Datenverarbeitung können die Elternvertretungen nicht frei entscheiden. Nach § 63 SchulG LSA sind der notwendige Geschäftsbedarf und die erforderlichen Einrichtungen zur Wahrnehmung der Aufgaben der Elternvertretung vom Schulträger zur Verfügung zu stellen. Die Elternvertretungen können diese dann lediglich nutzen.

Außerdem dürfte es nicht der gesetzgeberische Wille sein, dass Elternvertretungen eigene datenschutzrechtlich Verantwortliche sind. Sinn und Zweck der Definition des Verantwortlichen ist es, klare und umsetzungsstarke Einheiten zur Durchsetzung des Datenschutzrechts zu schaffen. Dies dürfte bei Elternvertretungen nicht der Fall sein.

Wären die Elternvertretungen Verantwortliche, würden sie u. a. alle Betroffenenrechte, wie beispielsweise das Auskunftsrecht selbst treffen und ein eigener Datenschutzbeauftragter müsste bestellt werden. Dies müsste dann in jeder Schule durch jede Klassenelternvertretung und den Schulelternrat gewährleistet werden. Darüber hinaus müssten die Schülervertretungen wohl ähnlich agieren. Diese dann stark zergliederte Organisation Schule, kann nicht die Intention der DS-GVO sein.

Ferner wären datenschutzrechtlich eigenverantwortliche Elternvertretungen wohl keine öffentlichen Stellen i. S. d. § 2 DSAG. Den §§ 55 bis 62, §§ 27 bis 29 SchulG LSA sind keine Rechtsgrundlagen zur personenbezogenen Datenverarbeitung von Elternvertretungen zu entnehmen. Zumeist handelt es sich hier um Aufgabenzuweisungen. Nach § 84a Abs. 8 Satz 2 SchulG sind Datenübermittlungen an Einzelpersonen oder private Einrichtungen allerdings grundsätzlich nur mit Einwilligung zulässig. Damit ist eine personenbezogene Datenübermittlung von der Schule an die Elternvertretung ohne Einwilligung der Betroffenen unzulässig.

Auch nach der Schulverfassung ist davon auszugehen, dass die Elternvertretungen letztlich als unselbständige Organisationseinheiten der Verwaltungseinheit Schule zu betrachten sind. Neben der Schulleitung, der Lehrerkonferenz und der Schulkonferenz gehören auch die Vertretungsorgane der Schüler und Eltern zur „rechtlich verfassten Schule“ (Avenarius/Heckel, Schulrechtskunde, 7. Auflage, Seite 132). Die Mitwirkung in Organen der unmittelbaren Willensbildung der Schule findet durch ihre Repräsentanten statt (Avenarius/Heckel, Seite 147). Auch wenn Elternvertretungen von Weisungen der Schulleitung eine inhaltlich unabhängige Interessenvertretung wahrnehmen können und den Umfang des Engagements frei bestimmen, bleiben sie doch in die Schulorganisation eingebunden und dienen der Vermittlung von schulbezogenen Positionen. So vermitteln sie nicht nur Anregungen aus der Elternschaft an die Schule, sie sollen auch im Interesse der Schule das Verständnis der Öffentlichkeit für die Unterrichts- und Erziehungsarbeit der Schule stärken (§ 55 Abs. 1 SchulG LSA). Ein weiteres Beispiel schulorganisatorischer Einbindung ist, dass der Schulelternrat durchaus Beschlüsse fassen und Anträge an die Gesamtkonferenz stellen darf, die von dieser auch behandelt werden müssen (§ 59 Abs. 3 SchulG LSA).

Die datenschutzrechtliche Verantwortlichkeit hinsichtlich der Datenverarbeitung von Elternvertretungen liegt grundsätzlich bei der Schule.

7.2 Ausstattung von Schulen mit digitalen Geräten

Wie sich Veröffentlichungen entnehmen ließ, u. a. den Antworten der Landesregierung auf Kleine Anfragen (z. B. LT-Drs. 8/127, LT-Drs. 8/194), schritt die Umsetzung des DigitalPakts Schule mit großen Schritten voran. Digitale Endgeräte für Lehrkräfte und Schülerinnen und Schüler stehen in erheblichem Umfang zur Verfügung und sind vielfach bereits verteilt bzw. werden kurzfristig zur Verfügung gestellt. Dabei sollte bedacht werden, dass die Nutzung der Endgeräte mit gängiger außereuropäischer (außerhalb des Anwendungsbereichs der DS-GVO) Software, insbesondere Microsoft Office 365, datenschutzrechtliche Fragen aufwirft. Eine gewisse Sensibilität hierfür ist in den Schulen bereits vorhanden. Den Landesbeauftragten erreichten im Berichtszeitraum einige Anfragen. Leider ist es schon aus Kapazitätsgründen nicht möglich, individuelle Beratungen und Hilfen zur Installation anzubieten. Der Landesbeauftragte hat daher die Schulen zunächst auf die gesetzlich bestimmte eigene Verantwortung hingewiesen.

Sie tragen für die Verarbeitung der Daten der Schülerinnen und Schüler die Verantwortung, sie müssen die datenschutzrechtlichen Vorgaben einhalten. Bei Schülerinnen und Schülern handelt es sich vielfach um Minderjährige, die eines besonderen Schutzes bedürfen. Die DS-GVO betont diesen Schutzbedarf u. a. in den Erwägungsgründen 38, 58, 65, 71 und 75 DS-GVO sowie Art. 8, Art. 12 Abs. 1, Art. 57 Abs. 1 lit. b DS-GVO. Weiter hat der Landesbeauftragte auf die wesentlichen problematischen Fragestellungen hingewiesen, die die Schulen zu klären haben, um in der konkreten Umsetzung vor Ort eine rechtskonforme Verarbeitung der Schülerdaten zu erreichen.

Grundsätzlich ist die Schule befugt, Daten der Schülerinnen und Schüler und Eltern auf Basis des Schulgesetzes insoweit zu verarbeiten, wie dies für die Erfüllung des Bildungs- und Erziehungsauftrags erforderlich ist. Dabei ist es möglich, sich automatisierter Verarbeitung, auch in Auftragsverarbeitung bei einem Dienstleister, zu bedienen. Die Anforderungen der DS-GVO müssen dabei eingehalten werden. Insbesondere sind die Grundsätze der Datenverarbeitung nach Art. 5 DS-GVO (Transparenz, Vertraulichkeit, Datenminimierung, Erforderlichkeit und Zweckbindung) sowie die Anforderungen an technische und organisatorische Vorgaben (Art. 5 Abs. 1 lit. f, Art. 25 Abs. 1, Art. 32 DS-GVO) zu beachten. Dies muss die Schule in eigener Verantwortung prüfen und die Einbindung von geeigneten IT-Dienstleistern datenschutzkonform gewährleisten. Bei einer Umsetzung ist auch zu beachten, dass Softwareprodukte im Auslieferungszustand oft nicht umfassend den Geboten der datenschutzfreundlichen Voreinstellungen (Art. 25 Abs. 2 DS-GVO) entsprechen, sodass insoweit eine Nachjustierung erforderlich werden kann.

Bei einer Verlagerung von personenbezogenen Daten zu einem Dienstleister bedarf es einer Rechtsgrundlage. Ist eine Übermittlung angedacht, wäre grundsätzlich die Regelung des § 84a SchulG LSA einschlägig. Die Übermittlung von personenbezogenen Daten an nichtöffentliche Stellen ist aber sehr stark eingeschränkt (§ 84a Abs. 8 Satz 2 SchulG LSA) und dürfte zudem an der fehlenden Erforderlichkeit scheitern. Übermittlungen von Schülerdaten an nichtöffentliche IT-Dienstleister kommen daher grundsätzlich nicht in Betracht. Es verbleibt deshalb in der Regel nur die Möglichkeit eine derartige Inanspruchnahme eines Dienstleisters im Wege der Auftragsverarbeitung gemäß Art. 28 Abs. 3 DS-GVO vertraglich auszugestalten.

Vor dem Hintergrund der regelmäßigen Unzulässigkeit der Datenübermittlung an einen privaten Dritten ist auch stets zu prüfen, ob über die inhaltliche Nutzung der Softwareprodukte hinaus auf andere Weise Daten übermittelt werden, sei es durch Nutzung anfallender Daten durch den Dienstanbieter für eigene Zwecke oder durch die Notwendigkeit einer persönlichen Anmeldung der Nutzer. Zu betrachten ist weiter, welche der verschiedenen cloudbasierten Online Dienste des Anbieters Verwendung finden sollen, bei denen personenbezogene Datenflüsse entstehen können. Auch bei Standardanwendungen wie Schreib- und E-Mailprogrammen (bei Microsoft Word und Outlook) kommt die Sammlung personenbeziehbarer Daten des Anwenders in Betracht, die über Inhalte hinausgeht (z. B. bezüglich der Verwendung der Rücktaste oder der Worte vor und nach dem in der Rechtschreibüberprüfung geprüften Wort). Durch eine Vielzahl von erfassten Ereignissen können Profile entstehen. Unter anderem können Daten über das genutzte Endgerät, die Adresse des Internetzugangs und Standortdaten personalisiert werden. Dabei ist zu berücksichtigen, dass von einem Personenbezug einer Information bereits ausgegangen werden muss, wenn eine Identifizierbarkeit gegeben ist (siehe dazu Erwägungsgrund 26 DS-GVO). Einfache Pseudonymisierun-

gen als Sicherungsmaßnahmen wären daher gegebenenfalls nicht ausreichend, soweit die Information durch eine Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden können.

Schulen obliegt es, neben der Einhaltung der bereichsspezifischen Vorschriften zur konkreten Datenverarbeitung (§ 84a ff. SchulG LSA) die europarechtlichen Grundsätze (Art. 5 DS-GVO) und Vorgaben, insbesondere in technischer und organisatorischer Hinsicht (Art. 5 Abs. 1 lit. f, Art. 25, Art. 32 DS-GVO) einzuhalten und die Einhaltung auch nachzuweisen (Art. 5 Abs. 2 DS-GVO). Sie müssen daher gem. Art. 32 Abs. 1 DS-GVO Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Kategorien personenbezogener Daten feststellen und basierend darauf die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten betroffener natürlicher Personen beurteilen. Sodann sind geeignete technische und organisatorisch Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Für die Auftragsverarbeitung sind zudem die Voraussetzungen nach Art. 28 DS-GVO zu beachten. Der Verantwortliche hat danach bei der Auswahl eines Auftragsverarbeiters darauf zu achten, dass letzterer hinreichende Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen getroffen wurden und so durchgeführt werden, dass die Verarbeitung dauerhaft im Einklang mit den Anforderungen der DS-GVO erfolgt und damit der Schutz der Rechte der betroffenen Schülerinnen und Schüler gewährleistet ist.

Es erscheint mehr als fraglich, ob es Schulen gelingen kann, eine datenschutzrechtskonforme und damit zulässige Verarbeitung von Schülerdaten bei Nutzung außereuropäischer Software nachzuweisen. Wiederholt haben Beratungen und Prüfungen von Datenschutzaufsichtsbeschwerden erhebliche Bedenken in Bezug auf einen datenschutzkonformen Betrieb von IT-Diensten hervorgebracht. Abschließende Einschätzungen werden zudem dadurch erschwert, dass Produkte unangekündigt geändert werden können und auch die Vertragsbedingungen möglichen Änderungen unterliegen. Infolge mangelnder Transparenz, fehlender Konfigurationsmöglichkeiten und auch offener rechtlicher Fragen bleiben vielfach erheblich Zweifel.

Bisher standen für die Organisation und Gewährleistung eines digitalisierten Betriebs von Schulorganisation und Unterricht gerade in der besonderen Situation der Corona-Pandemie nur wenige Angebote zur Verfügung. Ob trotz vielfältiger Fragen und Bedenken auch weiter davon ausgegangen werden kann, dass Produktnutzungen als alternativlos und damit noch vertretbar anzusehen sind, erscheint fraglich.

7.3 Zeugnisnoten per E-Mail

Eine Schülerin hat sich beim Landesbeauftragten beklagt, dass ihr Oberstufenkoordinator ihre Zeugnisnoten per E-Mail an eine unbekannte Person übermittelt habe. Dies war aufgefallen, als sie den Lehrer auf seiner E-Mailadresse mit ihrem E-Mail-Konto („Marion.Mustermann(at)Anbieter.de“; *Name erfunden*) kontaktierte und um Übermittlung der Notenübersicht bat. Der Oberstufenkoordinator antwortete, dass er doch vor kurzem erst die Noten an ihre E-Mail-Adresse gesandt habe. Zum Beweis habe er der Schülerin seinen E-Mail-Zugang gezeigt, den sie abfotografierte und das Foto als Beweis ihrer Beschwerde beifügte. Bei der verwandten Adresse („Marion.Mustermann(at)Mail.de“) waren zwar Vorname und Name gleich, nicht aber die Domain. Ob und wer also die Zeugnisdaten erhielt, war unbekannt.

Die Schule ließ sich dahin ein, eine E-Mailadresse von Marion Mustermann sei in der Schule nicht gespeichert. Darüber hinaus habe der Oberstufenkoordinator erklärt, sich an eine Beantwortung eines Auskunftsersuchens zu dem genannten Datum der vorgegebenen E-Mail-Versendung nicht erinnern zu können. Auch das Zustandekommen des angeblichen Fotos des E-Mail-Zugangs könne man sich nicht erklären. In der Schule bestehe ein generelles Fotografierverbot, eine Ausnahmegenehmigung sei nicht erteilt worden. Insgesamt gehe man davon aus, dass es sich nicht um eine Fotografie des E-Mailzugangs des Oberstufenkoordinators handele. Das dem Landesbeauftragten vorliegende Foto des E-Mailverkehrs erschien zumindest insoweit unstimmig, als der behauptete Absender unterschiedlich dargestellt wird. Zum Zeitpunkt der ersten Stellungnahme der Schule waren zudem bereits ca. fünf Monate seit dem angeblichen E-Mail-Verkehr vergangen. Aufgrund der regelmäßigen Löschung von bearbeiteten E-Mails auf dem Server der Schule war auch kein älterer E-Mail-Verkehr zu finden. Erfolgversprechende weitere Ermittlungsaussichten waren daher nicht gegeben. Durch das übersandte Foto ließ sich ein tatsächlicher E-Mailverkehr wohl nicht mit hinreichender Sicherheit belegen. Der Landesbeauftragte hat daher die Schulleitung mit der Aufforderung zur schriftlichen Bestätigung des darauf Veranlassten belehrt, dass im Rahmen der Verpflichtungen des Verantwortlichen für die Datenverarbeitungen gemäß Art. 5 Abs. 1 lit. f DS-GVO, Art. 32 DS-GVO geboten ist, durch geeignete technische und organisatorische Maßnahmen die Vertraulichkeit der Daten der Schülerinnen und Schüler sicherzustellen. Dazu gehört insbesondere auch ein hinreichendes Identitätsmanagement, das den Beschäftigten im Rahmen von Beratungen bzw. Fortbildungen zum Datenschutz nahezubringen ist.

7.4 Behördliche Datenschutzbeauftragte an Schulen

Die Absicherung der gesetzlichen Verpflichtung der Schulen zur Benennung von behördlichen Datenschutzbeauftragten war bereits seit Jahren Gegenstand der Beratungen mit dem Bildungsministerium, ohne dass abschließende Lösungen gefunden werden konnten (siehe XI. Tätigkeitsbericht, Nr. 9.3.1; XII. Tätigkeitsbericht, Nr. 9.2.1; XIII./XIV. Tätigkeitsbericht, Nr. 9.2.1; XVII. Tätigkeitsbericht, Nr. 12.2). Der Landesbeauftragte griff die Problematik im Frühjahr 2021 mit einem Schreiben an den Direktor des Landesschulamtes unter Bezugnahme auf die früheren Beratungen und Lösungsmöglichkeiten wieder auf. Ein zentraler Ansatz wäre grundsätzlich denkbar, da Art. 37 Abs. 3 DS-GVO vorsieht, dass eine Oberbehörde einen Datenschutzbeauftragten benennen kann, der die Aufgaben des Datenschutzbeauftragten für nachgeordnete Behörden wahrnimmt. Dies müsse aber unter Berücksichtigung der Größe und Organisationsstruktur der jeweiligen Schulen erfolgen. Die Beauftragten müssten ihren Aufgabenbereich überblicken und ihre Aufgaben vollständig erfüllen können. Umfasst sei der Aufgabenkanon des Art. 39 DS-GVO, der neben der regelmäßigen Beratung auch die Überwachung des jeweiligen Verantwortlichen und damit Besuche vor Ort beinhaltet. Um den zwingenden Vorgaben der DS-GVO hinreichend Rechnung zu tragen, wurde auf die Benennung externer, auf dem freien Markt verfügbarer Datenschutzbeauftragter hingewiesen und angeregt, die hierfür erforderliche Haushaltsvorsorge zu treffen. Der Direktor des Landesschulamtes erläuterte in der Antwort die innere Organisationsstruktur der Schulen und die Gewohnheit, sich in rechtlichen und tatsächlichen Zweifelsfragen an das Landesschulamt zu wenden. Die Beauftragung externer Datenschutzbeauftragter wäre mit einem erheblichen Verwaltungsaufwand verbunden. Mit Verfügung vom 17. Februar 2021 sei daher im Landesschulamt in Magdeburg und in Halle jeweils für den Einzugsbereich Nord und Süd eine Person als behördlicher

Datenschutzbeauftragter für die betroffenen Schulen benannt worden. Die Schulen seien gebeten worden, Ansprechpartner aus der Schulleitung zu benennen, die den engen Kontakt mit den Datenschutzbeauftragten pflegen. Auch wurde auf die unterstützende Handreichung für den Datenschutz an Schulen hingewiesen, die durch das Landesschulamt fortgeschrieben werde. Ob angesichts der Anzahl der Schulen in Sachsen-Anhalt und der bekanntermaßen ohnehin an der Belastungsgrenze arbeitenden Schulleitungen eine den Anforderungen des Art. 37 ff. DS-GVO gerecht werdende Beratung und Kontrolle durch zwei sehr engagierte Personen im Landesschulamt hinreichend Rechnung getragen werden, bleibt zweifelhaft.

7.5 Fotografieren bei Schulveranstaltungen

Immer wieder wurde der Landesbeauftragte zum Fotografieren bei Schulveranstaltungen, insbesondere im Zusammenhang mit Einschulungsveranstaltungen angefragt. So beklagten einige, dass sie wohl fotografiert worden seien, obwohl sie dem nie zugestimmt hätten. Andere, die gerne den ersten Schultag des Nachwuchses für das Familienalbum festgehalten hätten, beklagten, dass Schulleiter das Fotografieren bei Einschulungen verboten hätten, da der Datenschutz dem entgegenstünde. Dies ist aber nicht so. Auch wenn natürlich die Persönlichkeitsrechte der Teilnehmer der Veranstaltungen zu berücksichtigen sind, kann das Fotografieren auf Schulveranstaltungen zulässig sein, wenn die entsprechenden Voraussetzungen vorliegen. Diese können durch organisatorische Maßnahmen hergestellt werden. Hierzu hat der Landesbeauftragte die Hinweise „Fotografieren bei Schulveranstaltungen“ auf seiner Homepage veröffentlicht.[14] Der Datenschutz steht dem Fotografieren bei Schulveranstaltungen demnach nicht entgegen.

7.6 BRAFO-KE Berufsorientierung / EU-Verwaltungsbehörde

Im XIII./XIV. Tätigkeitsbericht (Nr. 9.2.7) hatte der Landesbeauftragte die umfängliche Beratung des Bildungsministeriums im Jahr 2016 zum Berufsorientierungsprojekt BRAFO-KE dargestellt. Im Berichtszeitraum wurde er nunmehr um erneute Beratung bei der Ausgestaltung der Einwilligungserklärungen zu dem Projekt durch das nun weiterführende Ministerium für Arbeit, Soziales, Gesundheit und Gleichstellung gebeten. Der Landesbeauftragte wies u. a. darauf hin, dass Einwilligungen als Rechtsgrundlage mit dem Problem behaftet sind, dass die Rechtsgrundlage für die Verarbeitung entfällt, wenn die Einwilligung widerrufen wird, was jederzeit möglich ist. Vorhandene gesetzliche Grundlagen sollten genutzt werden. Soweit Einwilligungen eingeholt werden sollen, wurde darauf hingewiesen, dass die an den Projekten Teilnehmenden umfassend über die beteiligten Verantwortlichen und die jeweiligen Datenverarbeitungsprozesse informiert werden sollten. Nur damit können Einwilligungen wirksam sein und den Zweck erfüllen, den Erklärenden die Tragweite ihrer Entscheidung vor Augen zu führen. Es sollte klar sein, welche Daten der Projektträger bzw. Durchführende verarbeitet. Die eventuelle Speicherung von Daten im IT-System efREporter3 sollte nachvollziehbar sein. Auch sollte an eine Beteiligung der EU-Verwaltungsbehörde im Finanzministerium gedacht werden, die Daten für den EU-rechtlichen Verwendungsnachweis benötigt. Es müsse differenziert erläutert werden, welche Informationen aufgrund von

[14] https://lsaurl.de/schulvfoto

rechtlich zwingenden Vorgaben erfasst werden müssen, etwa aufgrund von EU-Verordnungen zu Fördermitteln, bzw. welche Informationen rein freiwillig sind.

Im Kontext dieser Beratungen wandte sich Ende des Jahres auch die EU-Verwaltungsbehörde im Ministerium der Finanzen in Bezug auf das Informationsblatt zur Datenverarbeitung an den Landesbeauftragten. Bisher ging dieser davon aus, dass Trägereinrichtungen auf Basis von Art. 6 Abs. 1 lit. f DS-GVO Teilenehmerdaten erheben und weiterleiten müssen, um die Förderungsvorgaben zu erfüllen. Alternativ käme in Betracht, dass die Trägereinrichtungen als Auftragsverarbeiter für die EU-Verwaltungsbehörde gem. Art. 28 DS-GVO agieren. Dies müsste dann transparent gemacht werden und ein Vertrag nach Art. 28 Abs. 3 DS-GVO wäre dann erforderlich. Weiter wäre die eventuelle Einbindung von Evaluatoren und ihre Datenverarbeitung einzubeziehen. Die Speicherung im IT-System efREporter3 sei in den Blick zu nehmen. Auch gegenüber der EU-Verwaltungsbehörde wurde angeregt, eine zentrale, umfassende Darstellung der Verarbeitung von Daten von Teilnehmern in ESF-geförderten Projekten vorzunehmen, damit sich die Beteiligten über ihre Rollen und datenschutzrechtlichen Verpflichtungen klar werden und die Teilnehmer angemessen Transparenz erfahren.

8 Gesundheitswesen

8.1 Luca-App/Corona-Warn-App

Die Luca-App ist eine Anwendung zur Unterstützung der zur Pandemiebekämpfung notwendigen Kontaktnachverfolgung. Die Mehrzahl der Länder der Bundesrepublik Deutschland hat sich, wie auch Sachsen-Anhalt, im Frühjahr 2021 dazu entschieden, mit dem Anbieter der Anwendung Lizenzvereinbarungen zu treffen. Die Luca-App hat eine sehr weite Verbreitung gefunden. Der Landesbeauftragte ist insoweit nicht beteiligt worden. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat dazu in der Stellungnahme vom 26. März 2021 „Kontaktnachverfolgung in Zeiten der Corona-Pandemie – Praxistaugliche Lösungen mit einem hohen Schutz personenbezogener Daten verbinden“ eine erste Bewertung des Systems vorgenommen.[15] Mit der „Stellungnahme zu Kontaktnachverfolgungssystemen – insbesondere zu „Luca“ der cultur4life GmbH“[16] hat die DSK unter Feststellung einer dem Grunde nach tragfähigen Konzeption des Luca-Systems – insbesondere im Bereich der durchgängig verschlüsselten Kontaktdaten – auf Untersuchungen einzelner Aufsichtsbehörden hingewiesen, die Möglichkeiten missbräuchlicher Nutzung aufzeigten. Die DSK hat die Bemühungen des Anbieters um Nachbesserungen und die Kooperationsbereitschaft anerkannt und auf die notwendige zügige weitere Verbesserung gedrängt. Infolge der weiteren Begleitung der Entwicklung der Anwendung durch die für den Anbieter zuständige Berliner Beauftragte für Datenschutz und Informationsfreiheit hat der Landesbeauftragte auf die Anfragen zur Nutzung der Luca-App mitgeteilt, dass gegen die Nutzung zumindest keine durchgreifenden Bedenken bestehen.

[15] https://www.datenschutzkonferenz-online.de/media/st/20210329_DSK_Stellungnahme.pdf

[16] https://www.datenschutzkonferenz-online.de/media/st/20210429_DSK_Stellungnahme_LUCA.pdf

Dabei hat er jedoch regelmäßig darauf hingewiesen, dass auch datenschutzfreundlichere Alternativen geprüft werden sollten, da bei der Nutzung teilweise mit Klardaten (Anmeldedaten beim Anbieter) und pseudonymisierten personenbezogenen Daten gearbeitet wird. Im Zusammenhang mit der Kontaktnachverfolgung sei die Corona-Warn-App des Robert-Koch-Institutes datenschutzfreundlicher ausgestaltet, da sie schnell und ohne personenbezogene Daten nur auf Basis von pseudonymen Bluetooth-Kontakten der Endgeräte feststellt, ob riskante Begegnungen stattgefunden haben und die Betroffenen informiert. Anders als bei der Luca-App würde allerdings nicht das Gesundheitsamt informiert. Die DSK hat mit der Entschließung vom 29. April 2021 „Chancen der Corona-Warn-App 2.0 nutzen“[17] Bund und Ländern nahegelegt, die datensparsamen Möglichkeiten der Corona-Warn-App zu prüfen und empfohlen, sie jedenfalls als ergänzende Möglichkeit der Benachrichtigung potentiell Infizierter zu nutzen und zur Clustererkennung in den Konzepten zur Pandemiebekämpfung zu berücksichtigen.

8.2 Corona-Tests an Schulen

Die Erfahrungen des Jahres 2020 hatten die Notwendigkeit, den Präsenzunterricht an Schulen möglichst aufrecht zu erhalten, deutlich gemacht. Daher mussten Lösungen gefunden werden, den Gefahren einer schnelleren Ausweitung der Corona-Infektionen durch angemessene Maßnahmen zu begegnen. Ein Mittel war die Einführung einer Testpflicht an Schulen, um rechtzeitig Infektionen zu erkennen und ihnen individuell begegnen zu können. Aus datenschutzrechtlicher Sicht war dabei zu berücksichtigen, dass mit der Erfassung des negativen Testergebnisses in der Schule bzw. des Bekanntwerdens eines positiven Testergebnisses durch die Folge der Absonderung der Betroffenen (Isolation, Heimführung) besonders geschützte Gesundheitsdaten (Art. 9 Abs. 1 DS-GVO) betroffen waren. Es handelt sich um personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Die Daten sind auch aktuell sehr sensibel. Kinder und Jugendliche in Gruppen und Gemeinschaftseinrichtungen gehen mit derartigen Informationen auch anders um, als verständige Erwachsene. Die Befürchtungen vieler Eltern, die sich an den Landesbeauftragten wandten, der (unsachgemäße) Umgang mit derartigen Informationen an den Schulen könne zu Stigmatisierungen führen, erschienen zumindest nicht vollständig unbegründet.

Beratung der Schulbehörden

Um den Pandemiegefahren zu begegnen und den Präsenzbetrieb zu sichern ist im Frühjahr 2021 damit begonnen worden, an Schulen Antigen-Selbsttests durchzuführen. Der Landesbeauftragte hat sich infolge besorgter Anfragen beratend an das Ministerium für Bildung und das Landesschulamt gewandt und auf die Sorgen der Eltern in Bezug auf den Umgang mit den Gesundheitsdaten hingewiesen. Thematisiert wurde u. a. die Frage der Rechtsgrundlage der Datenverarbeitung, die mangelnde Pflicht, sich testen zu lassen und der Umgang mit den Ergebnissen (eventuelle Speicherung

[17] https://www.datenschutzkonferenz-online.de/media/en/20210429_DSK_Entschließung_Chancen_der_CWA_2.0_nutzen.pdf

und rechtzeitige Löschung). Das Ministerium hat sodann Anfang April 2021 die Schulen schriftlich dazu verpflichtet, die Schüler vor Schulbeginn zu testen.

Das Ministerium wurde dazu darauf hingewiesen, dass die Verarbeitung von Gesundheitsdaten einer spezifischen, tragfähigen Rechtsgrundlage bedarf. Von einer Einwilligung der teilnehmenden Schüler konnte nicht ausgegangen werden, da die Teilnahme am Präsenzunterricht verweigert worden wäre und die alternativ angebotene „Versorgung mit Lernaufgaben“ nicht als gleichwertiges Erziehungs- und Bildungsangebot angesehen werden konnte. Die nach Art. 7 DS-GVO gebotene Freiwilligkeit war nicht gegeben. Infolge des faktischen Zwangs stellte die ministerielle Vorgabe im Wege des Erlasses ein Anordnungsäquivalent dar. Für eine pauschale Anordnung von körperlichen Untersuchungen „im Vorgriff“ auf eine Vorgabe in der SARS-CoV-2-Eindämmungsverordnung und die damit im Zusammenhang stehend Datenverarbeitung fehlte jedoch die Rechtsgrundlage. Der Landesbeauftragte hat daher den Verzicht auf die Verarbeitung von Gesundheitsdaten bis zur Schaffung einer hinreichenden Rechtsgrundlage empfohlen. Weiter gab er Hinweise für Regelungen zum Umgang mit Daten, die aus einer künftig ggf. rechtskonformen Erhebung stammen.

Testung der Lehrkräfte

Verbunden mit der Testung der Schüler war auch die Testung der Lehrkräfte vorgesehen. Auch dazu hat der Landesbeauftragte das Ministerium für Bildung beraten. Es wurde darauf hingewiesen, dass sich entgegen der Annahme des Ministeriums eine Testpflicht und damit die Befugnis zu Verarbeitung von sensiblen Gesundheitsdaten nicht ohne Weiteres aus der Einschätzung des Arbeitgebers ergibt, dass die Testung von Beschäftigten wohl zur Pandemiebekämpfung notwendig sei. Grundsätzlich gehen den Arbeitgeber Gesundheitsdaten, wie auch der Impf-, Genesungs- oder Teststatus, nichts an (vgl. dazu den Beitrag „Impfstatusabfrage“, Nr. 8.5).

Fehlende Rechtsgrundlage

Das Ministerium für Bildung hat sich wohl entsprechend den Empfehlungen des Landesbeauftragten verhalten. Am gleichen Tag hatte nämlich das Verwaltungsgericht Magdeburg zu den Tests an Schulen entschieden. Es verwies darauf, dass es für Eingriffe in die Rechte der Betroffenen nach dem Vorbehalt des Gesetzes, Art. 20 Abs. 3 GG, einer Rechtsgrundlage bedürfe. Ministerielle Erlasse stellten keine geeignete Rechtsgrundlage dar. Allein die Befugnisse für Ministerien, in der Vierzehnten SARS-CoV-2-Eindämmungsverordnung Näheres zur Ausgestaltung durch Erlass zu regeln, reichten nicht aus. Mit diesen Regelungen könnten nur solche Maßnahmen gemeint sein, die die Landesregierung als Verordnungsgeber selber in den Blick genommen hat. Die Formulierung der Eindämmungsverordnung mache auch deutlich, dass dem Ministerium ein Entscheidungsspielraum für die Berücksichtigung von Besonderheiten eingeräumt werden sollte, nicht jedoch die Befugnis zum Erlass eigener Maßnahmen.

Test in der Eindämmungsverordnung

Mit der Neufassung der SARS-CoV-2-Eindämmungsverordnung am 16. April 2021 wurde die (zweimalig wöchentliche) Testung von nicht geimpften oder genesenen Schülerinnen und Schülern verbindlich vorgegeben. Die Regelungen wurden durch die Landesregierung als Verordnungsgeber auf der Basis von § 32 Satz 1 i. V. m. § 28

Abs. 1, § 28a, § 73 Abs. 1a, § 54 IfSG erlassen. Das Landesverfassungsgericht Sachsen-Anhalt hat mit Beschluss vom 21. Mai 2021 (Az.: LVG 21/21) festgestellt, dass die Anordnung der Testung von Schülerinnen und Schülern den Anforderungen an die Verhältnismäßigkeit von Grundrechtseingriffen genüge. Damit war die Durchführung von Tests normativ geboten. Die Verarbeitung von personenbezogenen Daten der Schülerinnen und Schüler war somit erforderlich im Sinne von § 84a SchulG LSA, § 9 Nr. 4 DSAG LSA i. V. m. Art. 9 Abs. 2 lit. i DS-GVO. Vielen Eltern, die sich weiterhin beim Landesbeauftragten beklagten und Sorgen auch im Hinblick auf die Durchführung der Testungen äußerten, musste der Landesbeauftragte daher mitteilen, dass gegen die mit den Testungen verbundene Datenverarbeitung grundsätzlich keine Bedenken bestehen. Mit steigender Anzahl von Schülerinnen und Schülern, deren Impf- und Genesenenstatus berücksichtigungsfähig war, ließ sich auch nicht immer vermeiden, dass gegebenenfalls aus der Tatsache der Durchführung eines Tests erkennbar wird, dass dort dieser Status nicht vorliegt. Mildernd wirkte insoweit, dass das Ministerium zu Hause durchgeführte Tests akzeptierte. Zudem hatte das Ministerium die Schulleitungen schon frühzeitig zum sensiblen Umgang mit den Testungen aufgefordert und transparente Datenverarbeitungen vorgegeben.

8.3 Test Schulfremder

Aufgrund einer Eingabe von Eltern im Herbst 2021 wurde der Landesbeauftragte darauf aufmerksam, dass Schulleitungen bei der Veranstaltung von Elternabenden beabsichtigen, von den Eltern Testergebnisse abzufragen bzw. alternativ sich Impf- oder Genesenennachweise vorlegen zu lassen. Ein Schulleiter habe auf die Vorgaben des Rahmenplans für die Hygienemaßnahmen, den Infektions- und Arbeitsschutz an Schulen des Ministeriums für Bildung (Rahmenplan-HIA-Schule) hingewiesen. Personen, die sich länger als 10 Minuten an Schulen aufhalten hätten danach eines Test-, Impf- oder Genesenennachweises bedurft. Der Landesbeauftragte hat die Schulbehörde darauf hingewiesen, dass bereits im Frühjahr die Problematik notwendiger Voraussetzungen der Anordnung von Tests im Rahmen der Pandemiebekämpfung erörtert wurde (siehe dazu den Beitrag „Corona-Tests an Schulen“, Nr. 8.2). Die Einführung von Corona-Tests und damit die Verarbeitung von Gesundheitsdaten bedarf einer normativen Grundlage, ein Erlass, wie der Rahmenplan, reicht nicht. In § 14 der seinerzeitigen 14. SARS-CoV-2-Eindämmungsverordnung war nur die Testung von Schülerinnen und Schülern und Schulpersonal vorgesehen.

Auch über die allgemeine Regelung in § 3 Abs. 2, 14. SARS-CoV-2-Eindämmungsverordnung war die Testdurchführung und Datenverarbeitung nicht zu rechtfertigen. Der Landesbeauftragte hatte zu dieser Regelung Kontakt mit dem für die Eindämmungsverordnung zuständigen Ministerium für Gesundheit und Soziales aufgenommen. Dort erhielt er den Hinweis, dass § 3 Abs. 2 14. SARS-CoV-2-EindV zwar entsprechende Vorgaben für Veranstaltungen vorsehen mag, der Veranstaltungsbegriff des § 3 Abs. 2 14. SARS-CoV-2-EindV aber nicht reguläre Veranstaltungen von Schulen und Hochschulen (Elternabend, Vorlesung) erfasse. Erfasst seien nur besondere Veranstaltungen (Sportfest, Chor). Die Regelung zu Veranstaltungen des § 3 Abs. 2 14. SARS-CoV-2-Eindämmungsverordnung betreffe nach der Begründung nicht interne notwendige Zusammenkünfte beim zulässigen Betrieb von Einrichtungen, z. B. Dienstberatungen, Teambesprechungen u. ä. Es fehlte daher die normative Anordnung derartiger Test, die eine demokratisch legitimierte Grundlage für die Erhebung von Gesundheitsdaten ergeben hätte. Daher war die Erhebung zunächst unzulässig.

In der Folge wurde sodann in die nächste geänderte Fassung der Eindämmungsverordnung durch den Normgeber die Testung auch von schulfremden Personen aufgenommen.

8.4 Präsenzpflicht an Schulen

Zum Ende des Jahres 2021 stiegen die Infektionszahlen wieder an. Eine der Schutzmaßnahmen in der SARS-CoV-2-Eindämmungsverordnung sah vor, dass der Betrieb in Schulen in Präsenzunterricht unter Befreiung von der Präsenzpflicht stattfindet. Der Rahmenplan für die Hygienemaßnahmen, den Infektions- und Arbeitsschutz an Schulen des Ministeriums für Bildung (Rahmenplan-HIA-Schule) sah dazu vor, dass die Befreiung von der Präsenzpflicht zwingend einer schriftlichen Erklärung der Erziehungsberechtigten bedarf, die nachvollziehbar durch Belege des Infektionsschutzes begründet sein muss. In der Folge erreichten den Landesbeauftragten Beschwerden. Eine Beschwerde führte aus, dass eine Schulleitung differenzierte medizinische Angaben zu gesundheitlichen Beeinträchtigungen der betroffenen Kinder sowie zur Gesundheit von im Haushalt der Kinder lebenden älteren Personen forderte, zu letzteren einschließlich einer Meldebestätigung. Damit wurde die Verarbeitung von sensiblen, besonders geschützten Gesundheitsdaten angestrebt, und damit auch eine Einschränkung der Befreiung von der Präsenzpflicht vorgenommen.

Dazu wies der Landesbeauftragte das Ministerium für Bildung darauf hin, dass die vorgesehenen Datenverarbeitungen in besonderem Maß grundrechtsrelevant sind (Art. 8 Abs. 1, 2 EU GRCh, Grundrecht auf informationelle Selbstbestimmung, Art. 1 Abs. 1, Art. 2 Abs. 1 GG). Für Eingriffe in die Rechte der Betroffenen bedarf es daher nach Art. 6 Abs. 1 DS-GVO sowie dem Vorbehalt des Gesetzes nach Art. 20 Abs. 3 GG, einer normenklaren Rechtsgrundlage (Art. 5 Abs. 1 lit. a, Art. 6 DS-GVO). § 14 Abs. 2 und 3 15. SARS-CoV-2-Eindämmungsverordnung sah nur vor, an allen Schulen den Präsenzunterricht unter Befreiung von der Präsenzpflicht stattfinden zu lassen. Das Nähere zur Ausgestaltung des Schulbetriebes werde durch Erlass nach § 15 Abs. 3, 15. SARS-CoV-2-Eindämmungsverordnung geregelt. Eine normenklare Rechtsgrundlage für die personenbezogene Erhebung und Verarbeitung von Gesundheitsdaten von Schülerinnen und Schülern sowie ggf. von deren Angehörigen durch Schulen war damit nicht gegeben. Die Verordnung ließ die geltende normative Rechtlage unbestimmt. Aus Regelungen zur Durchführung des Präsenzunterrichts aufgrund eines Erlasses (Rahmenplan-HIA-Schule) als verwaltungsinterne Regelung konnte sich keine Verarbeitungsbefugnis ergeben, da die normative Regelung derartige Maßnahmen nicht im Ansatz vorsah. Das „Ob“ und zumindest grundlegende Kriterien bzw. Maßstäbe für Grundrechtseingriffe bedürfen einer demokratisch legitimierten Festlegung. Auch der Gesetzgebungs- und Beratungsdienst des Landtags von Sachsen-Anhalt hat in einer Ausarbeitung vom 30. November 2021 festgehalten, dass zwar durch Erlass Näheres zur Ausgestaltung geregelt werden darf, sich der Eindämmungsverordnung aber kein Anhaltspunkt dafür entnehmen lasse, die Befreiung von der Präsenzpflicht davon abhängig zu machen, dass diese durch Belange des Infektionsschutzes begründet ist.

Hinter der Regelung stand aber wohl eine durchaus sinnvolle Absicht. Mit der Befreiung Einzelner von der Präsenzpflicht wäre es möglich, besonders Gefährdete, also gesundheitlich vorgeschädigte Schülerinnen und Schüler oder in deren Haushalt lebende ältere oder gesundheitlich vorgeschädigte Personen (z. B. Oma oder Opa) zu schützen. Der Landesbeauftragte empfahl daher, dass, wenn der Verordnungsgeber

eine derartige Regelung für notwendig hielt, grundlegende Kriterien und Maßstäbe in der Eindämmungsverordnung geregelt werden. In der Folge wurde die o. g. Regelung zur Befreiung von der Präsenzpflicht in der Eindämmungsverordnung zunächst gestrichen.

8.5 Impfstatusabfrage

Nachdem Ende 2020 die ersten Impfungen gegen Covid-19 erfolgten, keimte bei Arbeitgebern das Interesse daran auf, sich über den Impfstatus der Beschäftigten zu informieren. Auch in Bezug auf Kunden zeigte die Privatwirtschaft, u. a. in Bezug auf Restaurant- oder Konzertbesuche, Interesse an der Abfrage von Gesundheitsdaten (insbesondere des Impfstatus).

Allgemein wies die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hierzu durch die Entschließung vom 29. März 2021 „Coronavirus: Impfnachweis, Nachweis negativen Testergebnisses und Genesungsnachweis in der Privatwirtschaft und im Beschäftigungsverhältnis gehören gesetzlich geregelt!“[18] darauf hin, dass der Impfstatus und andere Daten, die Rückschlüsse auf die Gesundheit der Betroffenen zulassen, unter besonders strengem Schutz der DS-GVO stehen. Die Privatautonomie gestattet es privaten Veranstaltern zwar grundsätzlich, die Besucher insoweit frei auszuwählen, wie keine gesetzlich verbotene Diskriminierung erfolgt. Für die Datenverarbeitung ist jedoch eine Rechtsgrundlage erforderlich (Art. 5 Abs, 1 lit. a, Art. 6 Abs. 1 DS-GVO). Insoweit ist stets eine Interessenabwägung geboten. Infolge des besonderen Schutzes von Gesundheitsdaten ist somit in aller Regel eine konkrete gesetzliche Regelung erforderlich, die Datenverarbeitungen legitimiert (z. B. § 20 IfSG für die Masernschutzimpfung oder § 23a IfSG für in Krankeneinrichtungen Beschäftigte). Möglicherweise kommt auch eine Einwilligung als Rechtsgrundlage in Betracht. Insoweit sind aber die strengen Anforderungen des Art. 7 und der Erwägungsgrund 32, 42, 43 DS-GVO zu beachten. Die gebotene Freiwilligkeit ist dabei oft fraglich. Es sind stets Einzelfallentscheidungen geboten, die komplex und schwierig sind.

Infolge der Entwicklung des Impfgeschehens und häufiger Anfragen hatte die DSK zunächst den Beschluss „Verarbeitungen des Datums „Impfstatus“ von Beschäftigten durch die Arbeitgeberin oder den Arbeitgeber“ vom 19. Oktober 2021 veröffentlicht.[19] Darin wurde deutlich gemacht, dass der Schutz der Persönlichkeitssphäre der Beschäftigten es erfordert, dass dem Arbeitgeber grundsätzlich keine Gesundheitsdaten zukommen. Auch aus den häufig aufgeführten Gründen des Arbeitsschutzes und der Fürsorgepflicht des Arbeitgebers ergibt sich keine allgemeine Befugnis zur Erhebung von Gesundheitsdaten. Der Arbeitsschutz gebietet nur, sich von Fachkräften beraten zu lassen und ggf. erforderliche Maßnahmen, wie z. B. Hygienemaßnahmen zu treffen. Da der Impfschutz aufgrund der Darstellungen des Robert-Koch-Instituts zunächst auch nur relativen Schutz vor Infektiosität bot, schien auch die Geeignetheit der Kennt-

[18] https://www.datenschutzkonferenz-online.de/media/en/20210331_entschliessung_impfdatenverarbeitung.pdf

[19] https://www.datenschutzkonferenz-online.de/media/dskb/20211025_DSK_Beschluss_Impfstatus_von_Beschäftigten.pdf

nis des Impfstatus als Grundlage von Arbeitgebermaßnahmen fraglich. Zudem bestand Anlass, Beschäftigte vor dem Bekanntwerden des Impfstatus zu schützen, da dies zu Stigmatisierung und ggf. sozialem Druck im Rahmen der gesellschaftlich aufgeheizten Diskussion in Bezug auf Pandemiemaßnahmen führen könnte.

So hat auch die Einführung der Regelungen in § 36 Abs. 3 IfSG im Sommer des Jahres (Abfrage des Impf- und Serostatus durch den Arbeitgeber in bestimmten Einrichtungen, u. a. Gemeinschaftseinrichtungen, Massenunterkünften) nach der vorherigen kontroversen Diskussion in der politischen Öffentlichkeit gezeigt, dass derart sensible Eingriffe in die Persönlichkeitssphäre der Betroffenen einer abgewogenen Entscheidung des Gesetzgebers bedürfen.

Eine weitere häufig auftretende Einzelfrage im Zusammenhang mit dem Impfstatus des Beschäftigten war die Problematik, die sich aus der Erstattung der Verdienstausfallentschädigung nach § 56 Abs. 1 IfSG ergab. Die Arbeitgeber zahlen bei coronabedingter Quarantäne des Beschäftigten i. d. R. den Lohn fort und erhalten vom Gesundheitsamt eine Erstattung (§ 56 Abs. 5 Satz 3 IfSG). Mit Einführung von Satz 5 in § 56 Abs. 1 IfSG erhält der Betroffene keine Entschädigung und somit der Arbeitgeber keine Erstattung, wenn der Betroffenen durch Inanspruchnahme einer Schutzimpfung oder anderen Maßnahme der spezifischen Prophylaxe eine Absonderung hätte vermeiden können. Der Arbeitgeber bedurfte daher vor der Lohnfortzahlung des Nachweises, dass der Beschäftigte geimpft ist. Insoweit war die Erhebung des Impfstatus infolge der gesetzlichen Vorgaben erforderlich und somit datenschutzrechtlich zulässig (§ 26 Abs. 1 BGB, Art. 9 Abs. 2 lit. i DS-GVO). Es besteht aber keine Pflicht zur Mitteilung des Impfstatus, der Beschäftige kann seine Erstattungsansprüche auch selbst gegenüber der zuständigen Behörde geltend machen.

Weitere Fragen ergaben sich durch die Einführung der 3-G-Regelung am Arbeitsplatz mit § 28b IfSG. Leider ließ der Gesetzeswortlaut erheblichen Auslegungsspielraum, sodass die Konferenz der Datenschutzaufsichtsbehörden den Gesetzgeber zum Erlass normenklarer Regelungen aufrief. Grundlegend war jedoch eine Verpflichtung des Arbeitgebers im Abs. 3 zur täglichen Nachweiskontrolle und Dokumentation sowie die Befugnis zur zweckgebundenen Verarbeitung personenbezogene Daten einschließlich Daten zum Impf-, Sero- und Teststatus aufgenommen worden. Weiter wurden Arbeitgeber und Beschäftigte verpflichtet, einen Impfnachweis, einen Genesenennachweis oder einen Testnachweis mit sich führen, zur Kontrolle verfügbar zu halten oder bei dem Arbeitgeber zu hinterlegen. Die teilweise schwierige Umsetzung in der Praxis führte zu vielen Beratungsanfragen beim Landesbeauftragten.

Mit dem Ziel einer länderübergreifenden Rechtsanwendung bei der Pandemiebekämpfung im Bereich des Beschäftigtendatenschutzes veröffentlichte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder im Dezember 2021 die Anwendungshinweise „Häufige Fragestellungen nebst Antworten zur Verarbeitung von Beschäftigtendaten im Zusammenhang mit der Corona-Pandemie“.[20]

[20] https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_dsk_anwendungshilfe.pdf

8.6 Atteste zum Mund-Nasen-Schutz

Beim Landesbeauftragten gingen während des gesamten Berichtszeitraums viele Beschwerden ein, die die Anforderung von medizinischen Informationen im Zusammenhang mit der Befreiung von der Pflicht zum Tragen einer Mund-Nasen-Bedeckung bzw. eines Mund-Nasen-Schutzes betrafen. Die meisten Eingaben betrafen den Schulbereich. Landesrechtlich war aufgrund der 14. SARS-CoV-2-Eindämmungsverordnung (14. SARS-CoV-2-EindV) vorgegeben, in bestimmten Situationen eine Mund-Nasen-Bedeckung bzw. einen Mund-Nasen-Schutz verpflichtend zu tragen. Für Schulen war in § 14 14. SARS-CoV-2-EindV vorgegeben, dass innerhalb des Schulgebäudes grundsätzlich eine Mund-Nasen-Bedeckung zu tragen ist. Dies galt gem. § 1 Abs. 2 Satz 4 der 14. SARS-CoV-2-EindV u. a. nicht für Personen, denen die Verwendung einer Mund-Nasen-Bedeckung wegen einer Behinderung, einer Schwangerschaft oder aus gesundheitlichen Gründen nicht möglich oder unzumutbar ist; dies war in geeigneter Weise (z. B. durch plausible mündliche Erklärung, Schwerbehindertenausweis, ärztliche Bescheinigung) glaubhaft zu machen. Schulleitungen hatten in der Umsetzung vielfach die Anerkennung einfacher ärztlicher Feststellungen, dass das Tragen eines Mund-Nasen-Schutzes aus gesundheitlichen Gründen nicht zumutbar sei, nicht akzeptiert. Vielmehr wurde die Aufführung der gesundheitlichen Gründe gefordert, teilweise sogar die Nennung von Diagnosen. Die Aussage, dass gesundheitliche Gründe vorliegen, reiche nicht. Im Rahmen der Prüfung der Beschwerden durch den Landesbeauftragten wiesen die Schulen und auch das Landesschulamt auf die Vorgaben im Rahmenplan für die Hygienemaßnahmen, den Infektions- und Arbeitsschutz an Schulen (Rahmenplan-HIA-Schule) des Bildungsministeriums hin, der die Benennung gesundheitlicher Beeinträchtigungen erforderte.

Der Landesbeauftragte hatte gegenüber dem Bildungsministerium die erheblichen datenschutzrechtlichen Bedenken dargelegt und eine schnelle Klärung angeregt. Es wurde erläutert, dass es nicht zulässig ist, dass Schulen im Zusammenhang mit der Glaubhaftmachung sensible personenbezogene Gesundheitsdaten erheben. Auf die Veröffentlichung „Hinweise zur Befreiung von der Pflicht zum Tragen von Mund-Nasen-Bedeckungen“ auf der Homepage des Landesbeauftragten wurde hingewiesen. Das Anfordern von näheren Begründungen oder gar ggf. stigmatisierenden Diagnosen im Rahmen der Vorlage eines ärztlichen Attests erscheine in der Regel weder geeignet noch erforderlich und verstoße somit gegen europarechtliche Vorgaben (Grundsatz der Datenminimierung, Art. 5 Abs. 1 lit. c DS-GVO). Bei begründetem Zweifel könne man im besonderen Einzelfall ein amtsärztliches Attest als milderes Mittel verlangen oder bei Verdacht auf Fälschungen die Polizei einschalten. Infolge dessen wurde auch der HIA-Rahmenplan am 26. August 2021 geändert. Die Vorgabe der Erhebung weiterer Begründungen auf ärztlichen Attesten wurde aufgegeben. Da mit Beginn des Schuljahres 2021/2022 weitere Beschwerden eingingen, denen nachzugehen war, hatte der Leiter des Landesschulamtes auf telefonische Nachfrage versichert, dass die Schulleitungen abermals informiert würden, dass in der Regel keine gesonderten Begründungen notwendig sind.

Im Dezember 2021 wurde im Rahmenplan-HIA-Schule wiederaufgenommen, dass dem Attest zu entnehmen sein muss, mit welchen Folgen der Betroffene zu rechnen hätte, wenn er einen Mund-Nasen-Schutz tragen würde. Es gingen weiter Beschwerden und Anfragen ein. Der Landesbeauftragte wies das Bildungsministerium deshalb erneut darauf hin, dass die Rechtsgrundlage fehlt, sodass die Erhebung von Gesundheitsdaten rechtswidrig wäre. Aus § 84a Abs. 2 SchulG LSA in Verbindung mit der 15.

SARS-Co-V2-Eindämmungsverordnung ergab sich ausdrücklich keine diesbezügliche Rechtsgrundlage für die Anforderung sensibler medizinischer Informationen. Grundlage der Befreiung von der Maskenpflicht war § 1 Abs. 2 Nr. 3 15. SARS-Co-V2-EindV. Danach war eine Befreiung gegeben, wenn den Betroffenen aus gesundheitlichen Gründen nicht möglich oder unzumutbar war eine Maske zu verwenden. Dies war in geeigneter Weise, z. B. durch ärztliche Bescheinigung glaubhaft zu machen. Die Begründung machte deutlich, dass keine besonders geschützten Gesundheitsdaten (siehe Art. 9 Abs. 1 DS-GVO) erhoben werden dürfen: „Das Vorliegen der Ausnahmegründe ist in geeigneter Weise glaubhaft zu machen, spezielle ärztliche Atteste oder die Vorlage des Schwerbehindertenausweises sind ausdrücklich nicht erforderlich. Hierfür kann bereits eine plausible Erklärung des Betroffenen ausreichen, … Die Anforderungen an die Glaubhaftmachung sind niedrigschwellig anzusetzen, um die Ausnahmen nicht durch überhöhte Anforderungen bei der Einlasskontrolle faktisch außer Kraft zu setzen.“ Obwohl also die Rechtsnorm, die das Landesrecht für Ausnahmen von Maßnahmen der Pandemiebekämpfung festlegte, ausdrücklich vorgab, dass es nicht als gerechtfertigt angesehen werde, weitere Daten, insbesondere Gesundheitsdaten, zu erheben, setzte sich das Bildungsministerium als an das Recht gebundene Behörde darüber hinweg und ordnete im Erlassweg, also verwaltungsintern, die Datenerhebungen an. Datenschutzrechtlich war problematisch, dass durch die veranlasste Gesundheitsdatenerhebung pandemiebedingt in erheblicher Weise in die Grundrechte der Schüler eingegriffen wurde, obwohl die Rechtsnorm zur Pandemiebekämpfung dies ausdrücklich nicht vorsah.

Hintergrund dieser bedauerlichen Entwicklung mag sein, dass eine Reihe von Obergerichten in Deutschland die Anforderung von Gesundheitsdaten zur Glaubhaftmachung von Ausnahmen in Bezug auf Mund-Nasen-Schutz für vertretbar hielt. Das Bildungsministerium hat in einem Antwortschreiben auch auf einige Entscheidungen verwiesen. Übersehen wurde dabei, dass die Rechtslage in den Ländern eine andere war. Mangels entgegenstehender Begründung der Verordnung wie in Sachen-Anhalt konnte der Text entsprechend ausgelegt werden.

Aufgrund der fragwürdigen Rechtslage waren die weiteren Beschwerden nachvollziehbar. Die Regelung im Rahmenplan-HIA-Schule führte auch zur Verunsicherung bei den Schulleitungen, wie dem Landesbeauftragten durch zahlreiche Telefonate bekannt wurde. Da kurzfristig Lösungen auf dem Rechtsweg angesichts der Situation aber nicht erfolgsversprechend waren, hat der Landesbeauftragte das Bildungsministerium dahingehend beraten, entweder im Regelfall auf die Anforderung von Gesundheitsdaten zu verzichten oder, soweit dies für unerlässlich gehalten wird, auf die Aufnahme in die Eindämmungsverordnung hinzuwirken.

8.7 Kontaktdatenerfassungen

Coronabedingt war die die Nutzung einzelner gewerblicher und kultureller Angebote und Einrichtungen im Berichtszeitraum eingeschränkt. Bedingung für eine Nutzung war nach den seinerzeit geltenden Verordnungen über Maßnahmen zur Eindämmung der Ausbreitung des neuartigen Coronavirus SARS-CoV-2 in Sachsen-Anhalt vielfach die Führung eines Anwesenheitsnachweises durch den Veranstalter, um ggf. die Kontaktnachverfolgung durch die Gesundheitsämter zu ermöglichen. Hierzu wurde in den Verordnungen die Erfassung bestimmter Daten vorgegeben, nämlich Vor- und Familiennamen, die vollständige Anschrift, die Telefonnummer sowie der Zeitraum und der Ort des Aufenthalts der Kunden, Gäste und Veranstaltungsteilnehmer in Textform

(siehe z. B. § 1 Abs. 3 14. SARS-CoV-2-EindV). Die darüberhinausgehende Verarbeitung von Daten der Kunden begegnet durchgreifenden Bedenken.

Die Umsetzung dieser Vorgaben bereitete in der Praxis Schwierigkeiten. Sehr häufig haben die Veranstalter übersehen, dass es sich bei den Kontaktdaten der Kunden um personenbezogene Daten handelt, für deren Übermittlung an Dritte grundsätzlich keine Rechtsgrundlage gegeben ist. Leider wurden die Anwesenheitsdaten bei etlichen Verantwortlichen in Form von für alle Besucher bzw. Gäste einsehbaren Listen geführt. Zwar ist die Verarbeitung dieser Daten in Listenform zulässig, allerdings nur in der Weise, dass die darin enthaltenen Daten nicht von Unberechtigten zur Kenntnis genommen werden können. Mitunter wurden personenbezogene Daten verarbeitet, deren Verarbeitung von den Corona-Verordnungen nicht vorgesehen waren, z. B. Unterschriften und E-Mail-Adressen. Gerade die E-Mail-Adressen wurden in einigen Fällen zudem zweckwidrig für Werbemaßnahmen genutzt. Selbstverständlich ist es auch nicht zulässig, dass sich Mitarbeiter oder Kunden der Daten bedienten, z. B. um sympathische Kundinnen zu kontaktieren. Auch der Zugriff der Polizei auf die Daten ist grundsätzlich nicht zulässig, da die Verwendung strikt zweckgebunden ist (§ 28a Abs. 1 Nr. 17, Abs. 4 IfSG).

Im Falle von Verstößen hat der Landesbeauftragte die Verantwortlichen auf die Einhaltung datenschutzrechtlicher Vorgaben hingewiesen – mitunter war ein gewisser Nachdruck erforderlich. Erfreulich war aber, dass letztendlich alle Verantwortlichen zusagten, sich zukünftig an die Vorgaben zu halten. Auf die Erhebung von Bußgeldern konnte daher – auch unter Berücksichtigung wirtschaftlicher Einbußen im Zusammenhang mit der Pandemie – verzichtet werden.

Der Landesbeauftragte hatte bereits im XVII. Tätigkeitsbericht (Nr. 13.6) auf die Problematik hingewiesen und Hinweise zur Kontaktdatenverfolgung auf der Homepage veröffentlicht. Hinzu kommt noch die Problematik, dass nicht nur die Anwender, sondern auch die Diensteanbieter für digitalisierte Kontakterfassung die datenschutzrechtlichen Rahmenbedingungen beachten müssen. Mit der Stellungnahme „Kontaktnachverfolgung in Zeiten der Corona-Pandemie – Praxistaugliche Lösungen mit einem hohen Schutz personenbezogener Daten verbinden“[21] vom 26. März 2021 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder darauf hingewiesen, dass digitale Verfahren zur Verarbeitung von Kontakt- und Anwesenheitsdaten datenschutzkonform betrieben werden müssen. Weiter hat die DSK die umfängliche Orientierungshilfe „Einsatz von digitalen Diensten zur Kontaktnachverfolgung anlässlich von Veranstaltungs-, Einrichtungs-, Restaurant- und Geschäftsbesuchen zur Verhinderung der Verbreitung von Covid-19“ vom 29. April 2021 veröffentlicht[22] und darin insbesondere die Anforderungen formuliert, die an die technischen und organisatorischen Maßnahmen der Kontaktnachverfolgungssysteme zu stellen sind.

8.8 Testzentren

Die Coronavirus-Testverordnung gewährte den Bürgerinnen und Bürgern einen Anspruch auf einen kostenlosen sog. Bürgertest. In kürzester Zeit sind viele Testzentren

[21] https://www.datenschutzkonferenz-online.de/media/st/20210329_DSK_Stellungnahme.pdf

[22] https://www.datenschutzkonferenz-online.de/media/st/20210429_DSK_Stellungnahme_LUCA.pdf

entstanden und Programme zur Verarbeitung der dort entstehenden Daten entwickelt worden. Für die Datenverarbeitung war zu berücksichtigen, dass die Grundsätze nach Art. 5 DS-GVO zu beachten sind. So dürfen u. a. nicht mehr Daten erhoben werden, als für die Testaufgaben erforderlich (z. B. Kopie des Personalausweises). Die Verantwortlichen müssen angemessene technische und organisatorische Schutzmaßnahmen ergreifen (Art. 25, Art. 32 DS-GVO). Auch sind die Informationspflichten der Betroffenen zu berücksichtigen. Bei Schließungen von Testzentren infolge der gestiegenen Impfquote sind auch die sichere Aufbewahrung und fristgerechte Löschung zu beachten. Die dem Landesbeauftragten bekannt gewordenen Fälle deuteten aber darauf hin, dass das Wissen um die datenschutzrechtlichen Verpflichtungen bei den Testzentrenbetreibern nicht besonders ausgeprägt war. Daher hat der Landesbeauftragte Hinweise zu Testzentren auf seiner Homepage aufgenommen, um zumindest auf grundlegende Verpflichtungen aufmerksam zu machen.[23]

8.9 Daten des Betriebsarztes

Im Berichtszeitraum erreichte den Landesbeauftragten eine Anfrage eines Betriebsarztes zum Umgang mit den bei seiner Tätigkeit anfallenden Daten. In der Antwort wurde zunächst erläutert, dass die Hinweise im IX. Tätigkeitsbericht (Nr. 12.9) infolge gesetzlicher Änderungen nicht mehr aktuell sind. Die Archivierung von Patientenunterlagen bei externen Dienstleistern kann nicht mehr so kritisch bewertet werden. Mit dem Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen hat der Gesetzgeber Ende 2017 den § 203 StGB geändert. Damit ist es auch für Berufsgeheimnisträger möglich, rechtskonforme Auftragsdatenverarbeitungen (Art. 28 DS-GVO) in Bezug auf Patientendaten durchzuführen. Über die berufsmäßig tätigen Gehilfen hinaus können nun auch sog. mitwirkende Personen in die Tätigkeit der schweigepflichtigen Person einbezogen werden. Eine Einbindung in die Sphäre des Berufsgeheimnisträgers wie bei berufsmäßig tätigen Gehilfen (i. d. R. durch ein Beschäftigungsverhältnis) ist dabei nicht notwendig, auch ein Auftragsverarbeitungsvertrag (Art. 28 DS-GVO) kommt in Betracht (auf die Einhaltung der Anforderungen nach § 203 Abs. 3 und 4 StGB ist dabei unbedingt zu achten).

Der interne Betriebsarzt ist grundsätzlich Teil des Betriebes. Bei seiner ärztlichen Tätigkeit in Bezug auf Daten der Beschäftigten aus ihren arbeitsmedizinischen Untersuchungen besteht aber eine Weisungsfreiheit und Schweigepflicht (§ 8 Abs. 1 ASiG). Die Schweigepflicht darf gegenüber dem Arbeitgeber nur bei Einwilligung der Betroffenen oder im Rahmen der engen Grenzen nach § 6 Abs. 3 Nr. 3, Abs. 4 ArbMedVV durchbrochen werden. Einer Übergabe von Unterlagen aus sachbezogenen Beratungen zur Arbeitssicherheit an den Arbeitgeber bzw. einen Nachfolger stehen keine datenschutzrechtlichen Bedenken entgegen. Insoweit handelt es sich um Sachdaten des Betriebes, über die der Betrieb verfügen kann. Anderes gilt in Bezug auf die der Schweigepflicht unterliegenden medizinischen Daten aus den Untersuchungen/Beratungen der Beschäftigten. Insoweit verbleibt es bei der ärztlichen Verantwortung und es wäre die Einwilligung der jeweils Betroffenen erforderlich. Ohne Einwilligung kann der bisherige Betriebsarzt seiner Verantwortung für die ggf. noch notwendige Aufbe-

[23] https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/Informationen/Hinweise/Testzentren.pdf

wahrung (z. B. 10 Jahre nach der Berufsordnung) und die Einhaltung der Schweigepflicht ggf. noch durch die Anwendung des sog. „Zwei-Schränke-Modells“ Rechnung tragen. Grundsätzlich hat der Arzt nach der Berufsordnung dafür Sorge zu tragen, dass die Unterlagen bei Aufgabe der Tätigkeit in gehörige Obhut gegeben werden. Danach kann die Übergabe der zu schützenden Daten an einen ärztlichen Nachfolger möglich sein, wenn die Lagerung der Unterlagen in gesondert verschlossenen Schränken erfolgt und die Zugriffe auf Fälle der vorherigen Einwilligung der Betroffenen vertraglich vereinbart ist. Im Hinblick auf das gebotene Schutzniveau ist die Vereinbarung durch eine angemessene Vertragsstrafe im Fall des Verstoßes zu ergänzen. Weiter sollten die Betroffenen über den Wechsel und die ergriffenen Schutzmaßnahmen informiert werden.

8.10 Aufbewahrungsort für Backups

Aufgrund einer Anfrage prüfte der Landesbeauftragte, unter welchen Voraussetzungen es zulässig sein könnte, dass Beschäftigte, hier einer Arztpraxis, eine vollständige Datensicherung der Praxis mit allen Patientendaten auf verschiedenen mobilen Festplatten in ihren privaten Wohnraum mitnehmen.

Das Anliegen, eine Datensicherung außerhalb der Geschäftsräume aufzubewahren, ist im Interesse der Standortverschiedenheit ausdrücklich erwünscht, da eine Datensicherung, die an einem anderen Ort aufbewahrt wird, bei z. B. Brand oder Hochwasser in den Geschäftsräumen nicht vernichtet werden kann, wodurch die Verfügbarkeit der Daten und die Fähigkeit der raschen Wiederherstellung der Daten gemäß Art. 32 Abs. 1 lit. c DS-GVO sichergestellt wäre.

Werden jedoch Komplettsicherungen einer Datenverarbeitungsanlage gemacht, fallen damit große und umfangreiche Datenmengen vieler betroffener Personen an. Handelt es sich dann auch noch um Patientendaten und damit um Gesundheitsdaten als besondere Kategorien personenbezogener Daten i. S. v. Art. 9 Abs. 1 DS-GVO, so ist von einem hohen Schutzbedarf auszugehen. Entsprechend umfangreich müssen dann die zu treffenden technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO sein.

Werden personenbezogene Daten in diesem Kontext auf transportable Sicherungsmedien kopiert, so sind sowohl die Sicherungsmedien als auch deren Transport und Aufbewahrung durch gesonderte Maßnahmen zu schützen. Nachfolgend werden Maßnahmen genannt, die zusammengenommen dazu geeignet sind, ein hohes Schutzniveau herzustellen.

Technische Maßnahmen:

- Verschlüsselung der Sicherungsdateien nach Stand der Technik (siehe Technische Richtlinie des Bundesamtes für die Sicherheit in der Informationstechnik, BSI TR-2102-1), entweder softwarebasiert oder auf einem hardwareverschlüsselten Medium

- Wahl eines sicheren Passwortes (mindestens 20 Zeichen) bei der Verschlüsselung

- Sicherer Transport

- Aufbewahrung an einem sicheren Ort (z. B. Gebäudebereich ohne Publikumsverkehr, Abgrenzung durch verschlossene Türen ohne Außenzugang, in jedem Fall ohne Zugriff Dritter, auch Haushaltsangehöriger, am Verwahrungsort, auch ohne versehentliche Offenlegung)

- Aufbewahrung in einem gesicherten Behältnis (z. B. Tresor, verschlossener Stahlschrank, verschlossene Geldkassette, innerhalb eines massiven Möbelstückes mit Sicherheitsschloss)

Organisatorische Maßnahmen:

- Ausgabe der Datensicherung nur an vertrauenswürdiges langjähriges Personal

- dokumentierte Belehrung des Personals über das erhöhte Risiko, die zu erfüllenden technischen Vorgaben und die durchzuführenden organisatorischen Handlungen

- Dokumentation der Ausgabe eines Sicherungsmediums (Datum, Uhrzeit, Person, Ort der Aufbewahrung, geplante Rückführung des Sicherungsmediums)

- Dokumentation der Rückführung eines Sicherungsmediums (Datum, Uhrzeit, Person, Ort der Aufbewahrung, Vorkommnisse)

- Transport des Sicherungsmediums auf direktem Weg zum Aufbewahrungsort, ohne Erledigung privater oder dienstlicher Angelegenheiten auf diesem Weg

- Transport des Sicherungsmediums im gesicherten Behältnis (s. o.) jederzeit in unmittelbarer Nähe der transportierenden Person, unter keinen Umständen Zugriff Dritter möglich

- Transport explizit nicht via öffentlicher Verkehrsmittel, wo ein Zugriff Dritter mit erhöhter Wahrscheinlichkeit stattfinden kann

- Verpflichtung des Personals auf die Verschwiegenheit über den Transport und die Aufbewahrung

- Meldung von Vorkommnissen bzgl. des Sicherungsmediums (versuchter Raub, ungewollte Beschädigung) unverzüglich gegenüber dem Verantwortlichen

- regelmäßige Evaluierung der Wirksamkeit durchgeführter Maßnahmen und regelmäßige Mitarbeiterbefragung über die Realisierbarkeit angeordneter Maßnahmen

Darüber hinaus muss gewährleistet sein, dass die Verpflichtung der Beschäftigten zum datenschutzgerechten Transport arbeitsrechtlich wirksam übertragen wurde. Die Beschäftigten gehen hier ein erhebliches Risiko ein. Zudem sind ihre datenschutzrechtlichen Pflichten hier wohl außerhalb ihrer regelmäßigen Arbeitszeit zu erfüllen.

Insbesondere beim Anwendungsfall der Datensicherung aller Patientendaten aus der Arztpraxis, die durch Beschäftigte der Praxis im privaten Wohnraum aufbewahrt werden, kann ein dem hohen Risiko angemessenes Schutzniveau folglich nur durch eine Kombination aus Verschlüsselung, physischem Zugangsschutz und klar und verbindlich festgelegter organisatorischer Rahmenbedingungen erreicht werden.

9 Sozialwesen

9.1 Sozialdaten auf Briefumschlägen

Ein Beschwerdeführer teilte dem Landesbeauftragten mit, vom Jugendamt eines Landkreises Briefe erhalten zu haben, auf deren Umschlägen handschriftlich neben dem Aktenzeichen und dem vollständigen Namen seines Kindes auch die Bezeichnung des Inhaltes („Neuberechnung UH“ und „Auskunft+Verzug“) vermerkt war. Damit sind von außen Sozialdaten sichtbar, die Dritte zur Kenntnis nehmen können.

In einer ersten Stellungnahme teilte der Landkreis mit, dass die Angaben auf den Umschlägen zumindest in Teilen zwingend erforderlich seien. Um zu beweisen, was tatsächlich zugestellt wurde, sei beispielsweise nur das Aktenzeichen auf dem zuzustellenden Schriftstück nicht ausreichend. Hierfür sei eine Konkretisierung erforderlich, sodass die Umschläge darüber hinaus mit der Kurzbezeichnung der Inhalte beschriftet werden müssten. Die Angabe des Kindesnamens sei verzichtbar, da ein Bezug über das Aktenzeichen möglich sei.

Aber auch dieses modifizierte Verfahren begegnete aus hiesiger Sicht weiterhin erheblichen datenschutzrechtlichen Bedenken. Durch die Angabe der Kurzbezeichnung des Inhaltes erfolgte weiterhin eine Übermittlung personenbezogener Daten an Dritte. Eine Rechtsgrundlage hierfür war nicht gegeben. Darüber hinaus war zweifelhaft, inwieweit durch diese Maßnahme konkret nachweisbar sein soll, welcher Inhalt sich im Umschlag befindet. Die Beschriftung des Umschlages mit der Kurzbezeichnung des Inhaltes beweist nicht, dass sich dieser auch im Umschlag befindet. Aus hiesiger Sicht kommt einem entsprechenden Vermerk des Verwaltungsmitarbeiters auf dem Entwurf, der das Schriftstück in den Umschlag steckt, das gleiche Beweispotential zu und bewirkt keine Datenübermittlung an Dritte.

Aufgrund dieses Vorschlags hat der Landkreis sein Verfahren umgestellt. Nunmehr wird auf dem Briefumschlag lediglich das Aktenzeichen vermerkt. Auf der Postzustellungsurkunde wird ein intern festgelegter Code notiert, der intern einen eindeutigen Bezug zum versandten Schreiben herleiten kann.

Eine Übermittlung personenbezogener Daten an Dritte durch Vermerke auf den Briefumschlägen erfolgt auf diese Weise nicht mehr.

Von außen auf Briefumschlägen notierte personenbezogene Sozialdaten führen zu einer unzulässigen Datenübermittlung an Dritte und müssen daher unterbleiben.

9.2 Datenschutz in Kindertagesstätten

Sowohl das Personal von Kitas als auch Eltern haben in der Vergangenheit zahlreiche Fragen an den Landesbeauftragten gestellt oder um konkrete Informationen zur Verarbeitung personenbezogener Daten von in Kitas betreuten Kindern gebeten. Vor diesem Hintergrund hat der Landesbeauftragte die Antworten zu den häufigsten Fragen in den „Hinweisen zum Datenschutz in der Kindertagesstätte“ auf seiner Homepage zusammengestellt und auf seiner Homepage veröffentlicht.[24]

10 Beschäftigtendatenschutz

10.1 Homeoffice

Zunehmend verlagert sich die Verarbeitung von personenbezogenen Daten aus den Büros und Dienststellen in den häuslichen Bereich (siehe hierzu u. a. den Bericht zur Telearbeit in der Landesverwaltung Sachsen-Anhalt, LT-Drs. 7/5474). Infolge der Corona-Pandemie und der verbindlichen Vorgaben für Arbeitgeber, Heimarbeit anzubieten (§ 28b Abs. 4 IfSG), hat die Anzahl der Beschäftigten im Homeoffice nochmals erheblich zugenommen. Dazu wird der häusliche Arbeitsplatz mittels Informations- und Kommunikationstechnologie (IKT) mit dem Büro/der Dienststelle verbunden. Gelegentlich erfolgt auch ortsunabhängiges mobiles Arbeiten unter Einsatz von IKT. Da die Heimarbeit in vielen Fällen mit der Verarbeitung personenbezogener Daten verbunden ist, müssen auch im Hinblick auf den Datenschutz besondere Anforderungen bedacht werden. Durch die Auslagerung der Verarbeitung in den häuslichen oder mobilen Bereich stehen dabei nicht mehr die Sicherheitsvorkehrungen zur Verfügung, wie im betrieblichen/dienstlichen Bereich, sodass eine höhere Gefährdung der Sicherheit der Datenverarbeitung gegeben ist. Der Arbeitgeber/die Dienststelle bleibt aber der für die Einhaltung der datenschutzrechtlichen Anforderungen Verantwortliche(r) nach Art. 4 Nr. 7 DS-GVO, sodass ergänzende technische und organisatorische Maßnahmen (Art. 32 DS-GVO) getroffen werden müssen. Auch besondere Situationen, wie in der Corona-Pandemie, suspendieren nicht von den gesetzlichen Vorgaben, deren Einhaltung gerade in der Krise Stabilität gewährleistet.

Arbeitgeber bzw. Dienststellen müssen sich daher vielen Fragen stellen und viele geänderte bzw. neue Maßnahmen ergreifen, um letztlich auch im Hinblick auf Haftungsrisiken datenschutzkonform zu handeln. Das fängt mit der Prüfung an, ob der Beschäftigte seine Aufgaben ggf. auch ohne oder mit weniger personenbezogenen Daten in Heimarbeit erledigen kann (Grundsatz der Datenminimierung, Art. 5 Abs. 1 lit. c DS-GVO). Wenn die Verwendung personenbezogener Daten notwendig ist, sollte der behördliche Datenschutzbeauftragte beteiligt werden. Dieser könnte auch bei der sinnvollen Ausgestaltung der Heimarbeit in Betriebs- oder Dienstvereinbarungen mitgestalten. Weiter erscheint unumgänglich, für die Beschäftigten einen Handlungsleitfaden herauszugeben und sie besonders zu sensibilisieren, sowie ein Sicherheitskonzept zu erstellen (allgemeine und spezifische Maßnahmen zur Datensicherheit; Festlegungen, wie z. B. zu Hard- und Softwarekomponenten; Verschlüsselung (Ende-zu-

[24] https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/Informationen/Hinweise/Datenschutz_in_der_Kita.pdf

Ende-Verschlüsselung, VPN), aktuelle Protokolle, Sicherheitskopien). Besondere Bedeutung genießen die Aspekte der Sicherheit der Kommunikation und des Transfers der zu verarbeitenden Daten (Netzanbindung oder lokale Speichermedien; kein Liegenlassen von Unterlagen oder PCs im Pkw auf dem Supermarktparkplatz). Den Gefahren des Zugriffs unbefugter Dritter auf die Daten ist zu begegnen. Für den häuslichen Bereich sind auch Sicherungsvorgaben geboten (z. B. Zugangstüren, Schrank, verschließbare Aktentasche, keine „Vernichtung“ im heimischen Papierkorb). Eindeutig zu bevorzugen ist der Einsatz professionell administrierter Technik, die in hohen Maße Datensicherheit, z. B. in Bezug auf Firewall, Virenschutz, Malwareschutz, sichere Verbindungen und Verschlüsselungen gewährleistet. Private Geräte sind oft mit Anwendungen versehen, die sich bei der Installation umfassende Zugriffsrechte haben gewähren lassen. Mit deren Nutzung im privaten Umfeld erhöht sich auch die Gefahr in Bezug auf Schadsoftware. Sind gute Sicherheitsvorkehrungen getroffen, ist zu bedenken, dass sie an Wert verlieren, wenn ihre Einhaltung nicht in angemessenem Umfang geprüft wird. Allerdings darf dabei aus Sicht des Beschäftigtendatenschutzes kein unverhältnismäßiger Überwachungsdruck entstehen. In Bezug auf die genutzten Geräte sind verschiedene Sicherheitsaspekte zu bedenken und zu regeln. Dies gilt u. a. für die sichere und hinreichend passwortgeschützte Anbindung an das dienstliche/betriebliche System. Auch das „Drumherum“ sollte bedacht und gestaltet werden (Verbindung mit privaten Geräten, Ausdruck am heimischen Drucker, private Nutzung dienstlicher Geräte etc.). Soweit mobiles Arbeiten gestattet ist, sind auch insoweit die Besonderheiten auszugestalten (z. B. die Nutzung bzw. das Ausschalten von Verbindungstechnologien (Bluetooth, NFC, öffentliche W-LAN-Hotspots) des genutzten Gerätes. Letztlich muss man sich als Verantwortlicher auch die Frage stellen, ob die Auftragsverarbeiter, die man ggf. eingesetzt hat, Mitarbeiter in Heimarbeit beschäftigen und dabei den gebotenen Sicherheitsanforderungen gerecht werden.

Zur Unterstützung der Arbeitgeber und Dienststellen in Bezug auf die hier nur auszugsweise angesprochenen Fragestellungen, die notwendig mit der Ausgestaltung der Heimarbeit verbunden sind, hat der Landesbeauftragte im Berichtszeitraum umfängliche „Hinweise zum Homeoffice in Behörden und Betrieben“ nebst einer Checkliste zur vereinfachten Umsetzung im Infopaket Homeoffice auf seiner Homepage veröffentlicht.[25]

10.2 Digitalisierung von Versorgungsakten

Eine Anfrage an den Landesbeauftragten galt der Digitalisierung von Versorgungsakten von Beamten durch externe Dienstleister. Grundsätzlich sind Auftragsverarbeitungen durch externe Dienstleister auf der Basis von Art. 28 DS-GVO möglich. Die anfragende Stelle nahm aber Bezug auf eine Entscheidung des Oberverwaltungsgerichts Schleswig-Holstein (vom 27. Juli 2016, Az.: 2 MB 11/16, juris), wonach die Auslagerung des Einscannens von Personalakten an einen externen Dienstleister nicht zulässig sei.

Auch wenn die genannte Entscheidung keine bindende Wirkung in Sachsen-Anhalt begründet, hat der Landesbeauftragte im Hinblick auf die vergleichbare Rechtslage die geäußerten Bedenken bestätigt. Die Herausgabe von Personalaktendaten an Dritte ist

[25] https://datenschutz.sachsen-anhalt.de/informationen/infopakete/infopaket-homeoffice/

durch die Regelungen des Beamtenrechts zum Umgang mit Personalakten beschränkt. Insoweit wurde auf § 50 S. 3, 4 BeamtStG (Vertraulichkeit, begrenzte Verwendungszwecke der Personalverwaltung und Personalwirtschaft) sowie auf die engen Vorgaben des Landesbeamtengesetzes verwiesen (in Sachsen-Anhalt §§ 84 ff LBG LSA). Diese spezielle Ausprägung des Schutzes des Persönlichkeitsrechts der Betroffenen (Personalaktengeheimnis) macht eine Verarbeitung auf der Basis einer allgemeinen datenschutzrechtlichen Basis (Art. 28 DS-GVO, Auftragsverarbeitung) unmöglich. Zudem gebietet dies auch der Grundsatz des Vorrangs bereichsspezifischer Regelungen vor allgemeinem Datenschutzrecht. Auch in § 2 Abs. 5 DSAG LSA findet sich die Regelung des Vorrangs bereichsspezifischer Regelungen sowie zum Vorrang von Berufs- oder besonderen Amtsgeheimnissen (wie z. B. Personalaktengeheimnis). Die Datenschutz-Grundverordnung steht dieser beamtenrechtlichen Gestaltung nicht entgegen (siehe Art. 88 Abs. 1 DS-GVO).

10.3 Selbstauskunftsbogen der Investitionsbank Sachsen-Anhalt

Aufgrund einer Eingabe hat sich der Landesbeauftragte mit einem Selbstauskunftsbogen der Investitionsbank Sachsen-Anhalt befasst. Der Fragebogen diente im Rahmen von Schuldenbereinigungsverfahren dazu, sich über die wirtschaftliche Situation der Schuldner der Investitionsbank ein klares Bild zu machen. Zur Wahrung der haushaltsrechtlich gebotenen Wirtschaftlichkeit und Sparsamkeit muss vor Vergleichsvereinbarungen insbesondere die künftige Fähigkeit, finanzielle Verpflichtungen auch zu bedienen, sorgfältig geprüft werden. Zur Abfrage der entscheidungsrelevanten Aspekte bediente sich die Investitionsbank eines Selbstauskunftsbogens, dessen umfängliche Fragen dem Eingebenden zu weitgehend und zu persönlich erschienen. Der Landesbeauftragte hat daraufhin die Investitionsbank zur Ausgestaltung des Fragebogens mit dem Ziel der Beschränkung der Fragestellungen auf das für die sachgerechte Aufgabenwahrnehmung unbedingt Notwendige beraten.

Bezüglich der Abforderung von Einkommenssteuerbescheiden wurde empfohlen, einige besonders sensible Informationen, insbesondere in Bezug auf Dritte, auszumachen, die den Antragstellern als schwärzbar dargestellt werden können. Weiter wurde angeregt, die Notwendigkeit der Abfrage von Geburtsdatum und Staatsangehörigkeit zu prüfen. Besonders problematisch war die Abforderung der pauschalen Einwilligung, bei Banken, Verbänden, Kammern, Behörden und sonstigen Einrichtungen Daten abzufragen. Dabei war zuzugestehen, dass derartige Einwilligungen vorab eingeholt werden müssen, da Schuldner, mit denen man später im Streit liegt, diese Einwilligung dann nicht mehr abgeben würden. Eine pauschale Einwilligung, bei allen alles abfragen zu dürfen, begegnete aber im Hinblick auf die Bestimmtheit und damit Wirksamkeit erheblichen Bedenken. Daher wurde vorgeschlagen, eine Formulierung zu finden, die zwar vorab noch nicht bekannte Adressaten einbezieht, aber nur, soweit im Einzelfall konkrete Anhaltspunkte dafür vorliegen, dass die Befragung dieser Adressaten unumgänglich ist. Die Investitionsbank hat die Empfehlungen des Landesbeauftragten aufgegriffen und den Selbstauskunftsbogen überarbeitet.

11 Kommunales und Meldewesen

11.1 Veröffentlichung in Rats- und Bürgerinformationssystemen

In einer Vielzahl der Kommunen Sachsen-Anhalts werden mittlerweile automatisierte Rats- oder Bürgerinformationssysteme eingesetzt, die es der Verwaltung ermöglichen, den kommunalen Sitzungsdienst effizient zu steuern und es gleichzeitig den ehrenamtlichen Mandatsträgern und den Bürgern ermöglichen, sich zeitnah über die in den kommunalen Gremien zur Beratung oder Beschlussfassung anstehenden Themen zu informieren. So werden vielfach schon nicht nur die Tagesordnung der kommunalen Gremien, sondern auch bereits die zur Beratung und Beschlussfassung anstehenden Vorlagen sowie die Niederschriften der Sitzungen in das einer breiten Öffentlichkeit zugängliche kommunale Internetangebot eingestellt.

Im zurückliegenden Zeitraum erreichten den Landesbeauftragten immer wieder Beschwerden darüber, dass die Kommunen Unterlagen im Rats- und Bürgerinformationssystem veröffentlicht hatten, die personenbezogenen Daten enthielten.

11.1.1 Veröffentlichung von Sitzungsvorlagen

Die Befugnis zur Weitergabe personenbezogener Daten in Sitzungsvorlagen an die Vertretung ergibt sich in den meisten Fällen aus Art. 6 Abs. 1 lit. e und Abs. 3 DS-GVO i. V. m. § 53 Abs. 4 Kommunalverfassungsgesetz des Landes Sachsen-Anhalt (KVG LSA). Danach sind die für die Verhandlung erforderlichen Unterlagen grundsätzlich beizufügen. Von der Übersendung ist abzusehen, wenn das öffentliche Wohl oder berechtigte Interessen Einzelner dem entgegenstehen. Folglich dürfen der Vertretung personenbezogene Daten – beispielsweise als Anlage zu Beschlussvorlagen – zur Verfügung gestellt werden, soweit dies für die Beschlussvorbereitung oder die Information der Vertretung sowie gegebenenfalls zur späteren Ausführung der Beschlüsse erforderlich ist, es sei denn, das öffentliche Wohl oder berechtigte Interessen Einzelner stehen dem entgegen.

Die Veröffentlichung solcher Sitzungsunterlagen kann sich aus § 28 Abs. 1 KVG LSA ergeben. Danach unterrichtet der Hauptverwaltungsbeamte die betroffenen Einwohnerinnen und Einwohner über die allgemein bedeutsamen Angelegenheiten der Kommune in geeigneter Form. Die Zulässigkeit der gleichzeitigen Veröffentlichung personenbezogener Daten bemisst sich dabei nach dem vorgenannten Grundsatz der Erforderlichkeit zur Information der Einwohnerinnen und Einwohner sowie dem entgegenstehenden öffentlichen Wohl und den berechtigten Interessen Einzelner. Sie ist danach zulässig, sofern ausschließlich die zum Verständnis unbedingt erforderlichen personenbezogenen Daten enthalten sind. Im Einzelfall sind dabei immer die schutzwürdigen Interessen der Betroffenen sorgfältig zu prüfen. Grundsätzlich stellen die Namen betroffener Personen keine Information dar, die für das Verständnis des Sachverhalts erforderlich sind.

Insgesamt wird die Erforderlichkeit, personenbezogene Daten in einem Rats- und Bürgerinformationssystem für die Öffentlichkeit bereitzustellen, nur in wenigen Ausnahmefällen anzuerkennen sein. Bevor Sitzungsunterlagen der Allgemeinheit zur Verfügung gestellt werden, sind personenbezogene Daten deshalb in der Regel zu schwärzen.

11.1.2 Veröffentlichung von Beschlüssen

Aus § 28 Abs. 1 KVG LSA i. V. m. § 52 Abs. 1 und 2 KVG LSA lässt sich ableiten, dass Beschlüsse der Gemeindevertretung zu veröffentlichen sind, soweit nicht im Einzelfall aus Gründen des öffentlichen Wohls oder berechtigter Interessen Einzelner etwas anderes beschlossen wird. Daraus folgt die Pflicht, Beschlüsse vor der Veröffentlichung so weit zu anonymisieren, wie ihr wesentlicher Inhalt, also die Tragweite des Beschlusses, noch erkennbar bleibt. In jedem Fall zu anonymisieren sind personenbezogene Daten in Beschlüssen, zu deren Schutz bereits der Ausschluss der Öffentlichkeit erfolgt war. Die Prüfung, ob ein Beschluss zu anonymisieren ist, ist aber auch dann erforderlich, wenn Beschlüsse in öffentlicher Sitzung getroffen wurden, ausnahmsweise aber personenbezogene Daten enthalten.

11.1.3 Veröffentlichung von Niederschriften

Entsprechend § 58 Abs. 3 KVG LSA ist die Einsichtnahme in die Niederschriften über die öffentlichen Sitzungen zu gestatten. Das Nähere regelt die Geschäftsordnung. Sofern entsprechende Regelungen in der Geschäftsordnung zur Veröffentlichung von Niederschriften im Rats- und Bürgerinformationssystem getroffen wurden, ergibt sich daraus die Grundlage für eine Veröffentlichung der Niederschriften.

Nach § 58 Abs. 1 KVG LSA muss die Niederschrift einer Sitzung der Gemeindevertretung einen gewissen Mindestinhalt aufweisen – beispielsweise die Namen der Teilnehmenden. Dazu gehören jedoch ausschließlich solche Personen mit einem aktiven Teilnahmerecht im kommunalverfassungsrechtlichen Sinn.

Die Veröffentlichung von Niederschriften mit dem beschriebenen (auch personenbezogenen) Mindestinhalt ist im Hinblick auf die Erforderlichkeit für die Aufgabenerfüllung der Kommune (Beteiligung der Einwohnerinnen und Einwohner nach § 28 Abs. 1 KVG LSA) immer zulässig. Dazu gehört auch die Zuordnung der Teilnehmenden zu deren Beiträgen und Wortmeldungen. Nur so können die Interessierten das Handeln der Vertretung sowie der Verwaltung verstehen und ihre Wahlentscheidung entsprechend ausrichten.

Weitere personenbezogene Daten können nur aufgenommen werden, wenn dies zur Beteiligung der Einwohnerinnen und Einwohner im Einzelfall erforderlich ist. In den meisten Fällen ist es das nicht. Beispielsweise spielt es keine Rolle, welche Bürger über die genannten, offiziellen Teilnehmenden hinaus an einer Ratssitzung teilgenommen haben. Entsprechende Anwesenheitslisten dürfen in der Regel nicht Inhalt der Niederschrift werden. Auch ist die namentliche Bezeichnung von Bürgern, die sich im Rahmen einer Einwohnerfragestunde zu Wort gemeldet haben, für das Verständnis der Angelegenheit in aller Regel irrelevant. Soweit die Namen bzw. Anschriften der Fragestellenden für eine spätere Beantwortung erforderlich sein sollten, ist dies separat und nicht in der Niederschrift zu vermerken.

In vielen Fällen hatten es die Gemeinden versäumt, zwischen den Voraussetzungen für die Weiterleitung von personenbezogenen Sitzungsunterlagen an die Vertretung und an die Öffentlichkeit über das Rats- und Bürgerinformationssystem zu unterscheiden. Sie stellten dieselben Dokumente zuerst den Vertretungen und anschließend unverändert der Öffentlichkeit zur Verfügung, ohne zu berücksichtigen, dass für beide Schritte unterschiedliche Voraussetzungen gelten. In den überwiegenden Fällen konnte eine datenschutzgerechte Anonymisierung durch Schwärzung der Unterlagen erfolgen. In Einzelfällen wurden die entsprechenden Unterlagen vollständig aus dem Rats- und Bürgerinformationssystem entfernt, da die jeweiligen Kommunen selbst gar keinen Grund für eine personenbezogene Veröffentlichung sahen.

11.2 Zuständigkeit der behördlichen Datenschutzbeauftragten der Kommunen für die Kommunalvertretungen

Der Landesbeauftragte für den Datenschutz wird regelmäßig mit Anfragen konfrontiert, die die datenschutzrechtliche Verantwortlichkeit eines Gemeinde-, Stadtrates oder Kreistages einschließlich seiner ehrenamtlichen Mitglieder betreffen.

Datenschutzrechtlich Verantwortliche im Sinne des Art. 4 Nr. 7 DS-GVO ist die Kommune als Gebietskörperschaft des öffentlichen Rechts.

Die datenschutzrechtliche Verantwortlichkeit umfasst daher auch die Tätigkeit des Hauptorgans Gemeinde-, Stadtrat bzw. Kreistag, mithin auch die Verarbeitung personenbezogener Daten durch die Ratsmitglieder.

Die Kontrollpflicht und -befugnis des behördlichen Datenschutzbeauftragten umfasst auch die Tätigkeit der Ratsarbeit. Dies stellte sowohl für die Ratsmitglieder als auch für den Datenschutzbeauftragten selbst manchmal eine überraschende Erkenntnis dar.

11.3 Wahlwerbung

Den Landesbeauftragten für den Datenschutz erreichten im Rahmen der anstehenden Landtagswahl Beschwerden von Bürgern zum Erhalt von persönlich adressierter Wahlwerbung. Die Beschwerdeführer vermuteten einen Datenschutzverstoß durch die jeweilige Partei.

Tatsächlich können Parteien solche Adressdaten rechtskonform von den Meldebehörden abfragen. Dabei gelten allerdings enge datenschutzrechtliche Rahmenbedingungen – und dieser Weitergabe kann bürgerseits widersprochen werden.

Die rechtliche Erlaubnis für personalisierte Wahlwerbung ergibt sich aus dem Bundesmeldegesetz (BMG). Danach können die Meldebehörden Parteien im Zusammenhang mit Wahlen Auskünfte aus dem Melderegister erteilen (sogenannte Gruppenauskünfte). Zulässig ist dabei nur die Übermittlung von

- Vor- und Nachname,
- ggf. Doktortitel

- und die derzeitige Wohnanschrift,

nicht aber z. B. das Geburtsdatum. Bei den jeweiligen auf Antrag der Partei erteilten Meldeauskünften gelten zudem folgende gesetzliche Vorgaben, zu denen sich die Parteien schriftlich gegenüber den Behörden verpflichten:

- Die Auskünfte erfolgen nur für den Zeitraum von sechs Monaten vor einer Wahl. Nach der Wahl sind Namen und Adressdaten innerhalb eines Monats von den Verantwortlichen wieder zu löschen.

- Die übermittelten Daten dürfen ausschließlich nur für die Wahlwerbung verwendet werden. Unzulässig wäre die Nutzung der Adressdaten zur Aufnahme in eine „allgemeine Adressdatenbank“ oder zur Mitgliedergewinnung für die Partei.

- Zudem dürfen Auskünfte nur über einzelne Altersgruppen erteilt werden, die Partei muss also bei ihrer Abfrage einen konkreten Altersbereich nennen. So ließen sich zum Beispiel die Adressen aller Erstwählenden oder jungen Erwachsenen ermitteln. Parteien können ihre Wahlwerbung dadurch gezielt an die entsprechende Altersgruppe anpassen.

Halten sich die Empfänger von Meldedaten für Wahlkampfzwecke an diese gesetzlichen Vorgaben, ist deren Verarbeitung aus datenschutzrechtlicher Sicht zulässig. Das Persönlichkeitsrecht der Bürger tritt in diesen Fällen hinter das Recht politischer Parteien oder Organisationen an demokratischer Teilhabe im Rahmen von Wahlen zurück.

Bürger, die keine Wahlwerbung erhalten möchten, haben die Möglichkeit, der Veröffentlichung bzw. der Weitergabe an Dritte zu widersprechen. Für den Widerspruch ist keine besondere Form vorgesehen, er kann in Schriftform, persönlich oder per E-Mail bei der zuständigen Meldebehörde erhoben werden. Wer ihn erhebt, muss weder eine Begründung angeben noch eine Frist beachten. Der Widerspruch ist gebührenfrei und wirkt grundsätzlich auf Dauer, entfaltet für die Vergangenheit jedoch keine Wirkung. Eine Rücknahme des Widerspruchs ist möglich.

Häufig stellen die Gemeinden auf ihren Service-Portalen digitale Widerspruchsformulare zur Verfügung. Auf das Widerspruchsrecht ist zudem einmal jährlich durch ortsübliche Bekanntmachung – also z. B. in einem Mitteilungsblatt – hinzuweisen. Aufgrund des Widerspruchs trägt die Meldebehörde im Melderegister eine Übermittlungssperre für Gruppenauskünfte mit dem Zweck „Wahlwerbung“ ein.

Weiterführende Informationen und Rechtsquellen:

- § 50 Abs. 1 Satz 1 BMG Meldebehörden dürfen Parteien Auskunft aus dem Melderegister geben, jedoch nur, wenn die Wahlberechtigung an eine Altersgrenze geknüpft ist (z. B. 18 Jahre) und nur über einzelne Altersgruppen

- § 44 Abs. 1 Satz 1 BMG listet die Daten auf, die abgefragt werden dürfen

- § 50 Abs. 1 Satz 3 BMG bestimmt eine Löschfrist von einem Monat nach der Wahl

- § 50 Abs. 5 BMG regelt den Widerspruch der Weitergabe

Parteien dürfen im Vorfeld anstehender Wahlen nach Altersgruppen kategorisierte Datensätze von den Meldebehörden abfragen, um diesen Wählergruppen anschließend personalisierte Wahlwerbung zuzusenden. Eine Verwendung der Daten über Wahlwerbung hinaus ist unzulässig. Bürger können jederzeit einer solchen Weitergabe ihrer Daten widersprechen. Die Meldebehörde trägt dann eine entsprechende Übermittlungssperre ein. Die Sperre gilt für die Zukunft und ist unbefristet.

11.4 Auskünfte aus dem Liegenschaftskataster

Wiederholt erreichten den Landesbeauftragten für den Datenschutz Beschwerden von Grundstückseigentümern, die bezüglich ihrer Grundstücke Kaufanfragen erhalten hatten, aber gar nicht an einem Verkauf interessiert waren. Die Kaufinteressenten gaben in der Regel an, die Eigentümerdaten durch ein Auskunftsersuchen aus dem Liegenschaftskataster erhalten zu haben.

Auf Anfrage teilte das zuständige Landesamt für Vermessung und Geoinformation Sachsen-Anhalt (LVermGeo) mit, dass Auskünfte aus dem Liegenschaftskataster generell gem. § 13 Abs. 1 Satz 2 Vermessungs- und Geoinformationsgesetz Sachsen-Anhalt erfolgten. Demnach erhalten – wenn öffentliche Belange dem nicht entgegenstehen – neben den Eigentümern auch solche Personen Auskunft, die ein berechtigtes Interesse daran darlegen.

Weiter teilte das LVermGeo mit, dass das Vorliegen eines berechtigten Interesses in Bezug auf die personenbezogenen Daten des Liegenschaftskatasters im Lichte neuerer katasterrechtlicher Rechtsprechung zu bewerten sei. Danach könne ein berechtigtes Interesse auch dann vorliegen, wenn Eigentümerangaben zur Anbahnung von Verhandlungen bzw. vorgelagert zur Klärung der Verkaufsbereitschaft des jeweiligen Eigentümers benötigt würden. Andernfalls würde ein berechtigtes Interesse voraussetzen, dass bereits Verhandlungen stattgefunden haben bzw. die Verkaufsabsicht des Eigentümers bekannt sei. Dann sei der Eigentümer jedoch bereits bekannt, sodass sich ein Auskunftsersuchen erübrige.

In einigen Fällen wurde bezüglich der Grundstücke der Beschwerdeführer im Geschäftsbuch des LVermGeo kein Eintrag auf mündliche oder schriftliche Auskunft verzeichnet, sodass nicht nachvollziehbar war, wie der Interessent sein berechtigtes Interesse nachgewiesen hatte. Allerdings wurden dort bisher nur kostenpflichtige Anträge registriert. Mündliche Auskünfte unter einer Dauer von 15 Minuten, die kostenfrei sind, wurden nicht im Geschäftsbuch vermerkt.

Aufgrund der Beschwerden hat das LVermGeo seine bisherige Vorgehensweise bei mündlichen Auskünften unter einer Dauer von 15 Minuten dahingehend geändert, dass auch diese entsprechend dokumentiert werden. Dadurch können Grundstückseigentümer zukünftig in ähnlichen Situationen in Erfahrung bringen, wer aufgrund welches berechtigten Interesses Auskunft aus dem Liegenschaftskataster erhalten hat.

12 Wirtschaft

12.1 Aktuelle Meldungen von Datenschutzverletzungen

Die Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden gemäß Art. 33 DS-GVO der Aufsichtsbehörde, es sei denn, dass diese Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Im Berichtszeitraum wurden insbesondere folgende Verletzungen häufig gemeldet:

- Irrtümliche Versendung von Briefpost an Nichtberechtigte,
- Versendung von E-Mails an Nichtberechtigte,
- Abhandenkommen von Datenträgern,
- Kompromittierung von Kundenkonten,
- Unberechtigte Zugriffe von Beschäftigen auf Kundendaten zu privaten Zwecken.

Um Möglichkeiten aufzuzeigen, wie Datenschutzverletzungen verhindert werden und welche Maßnahmen nach einer Verletzung durchgeführt werden können, hat der Landesbeauftragte ein Informationsblatt mit dem Titel „Häufige Ursachen von Datenschutzverletzungen und Abwehrmaßnahmen“ herausgegeben.[26]

Des Öfteren wurde die Meldefrist von 72 Stunden überschritten. Verantwortliche müssen durch technische und organisatorische Maßnahmen sicherstellen, dass die Datenschutzverletzung von dem Unternehmensbereich, in dem die Verletzung festgestellt wurde, zügig an den Bereich, der für die Meldung an die Aufsichtsbehörde zuständig ist, weitergeleitet wird. Wird die Frist von 72 Stunden überschritten, so ist die Verzögerung zu begründen.

Im Falle eines „hohen Risikos“ müssen die betroffenen Personen nach Art. 34 DS-GVO benachrichtigt werden. Dies ist insbesondere der Fall, wenn abgeflossenen Daten ein hohes Missbrauchsrisiko innewohnt. Solche Daten enthalten z. B. Kopien von Ausweisdokumenten und Zahlungsdaten, die für Identitätsdiebstähle oder Phishing verwendet werden können. Ein hohes Risiko liegt auch nahe, wenn Daten i.S.v. Art. 9 Abs. 1 DS-GVO oder detaillierte Beschäftigtendaten Unberechtigten gegenüber offengelegt wurden. Auch eine abgeflossene Telefonabrechnung führt häufig zu einem hohen Risiko. Sie gewährt Aufschluss über das Privatleben und könnte z. B. zu Stalking führen.

Weitere Informationen befinden sich in einem Informationspaket auf der Homepage des Landesbeauftragten.[27]

---

[26] https://lsaurl.de/BspDSVer

[27] https://lsaurl.de/InfopaketKMU

12.2 Datenübermittlungen von Versicherungen an Polizeidienststellen

Aufgrund einer Anfrage hat der Landesbeauftragte geprüft, ob eine Versicherung zur Auskunft gegenüber Polizeidienststellen in strafrechtlichen Ermittlungsverfahren berechtigt oder gar verpflichtet ist, wenn um Auskunft über Daten ersucht wird, die unter die Geheimhaltungspflicht des § 203 StGB fallen. Gemeint sind insbesondere zum persönlichen Lebensbereich gehörende Geheimnisse, die Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung bekannt geworden sind.

Bei polizeilichen Anfragen zum Zwecke der Strafverfolgung wird als datenschutzrechtliche Erlaubnisnorm häufig Art. 6 Abs. 4 DS-GVO i. V. m. § 24 BDSG zu prüfen sein. Denn die bei der Versicherung gespeicherten Daten wurden ursprünglich zum Abschluss und zur Durchführung des Versicherungsvertrages erhoben. Bei der Datenübermittlung an Ermittlungsbehörden zur Strafverfolgung würde es sich somit um eine Weiterverarbeitung der Daten zu anderen Zwecken als dem ursprünglichen Erhebungszweck handeln.

Nach den genannten Vorschriften wäre die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch die Versicherung zulässig, wenn die Verarbeitung zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist, sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen. Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO wäre in diesem Kontext zulässig, wenn die Voraussetzungen des § 24 Abs. 1 BDSG und ein Ausnahmetatbestand nach Art. 9 Abs. 2 DS-GVO oder nach § 22 BDSG vorliegen. Sofern diese Voraussetzungen erfüllt sind, kann sich daraus eine Offenbarungsbefugnis ergeben, auch hinsichtlich der Daten, die der Geheimhaltungspflicht des § 203 StGB unterfallen.

Zu beachten ist dabei, dass eine Auskunftspflicht eines Zeugen nach § 163 Abs. 3 StPO nur gegenüber Ermittlungspersonen der Staatsanwaltschaft besteht oder gegenüber Polizeibeamten, wenn sie von der Staatsanwaltschaft mit den Ermittlungen beauftragt sind (vgl. § 161 Abs. 1 StPO). Ein Zeugnisverweigerungsrecht nach § 53 StPO steht den Beschäftigten der Versicherung i. d. R. nicht zu.

Führt eine Polizeidienststelle aufgrund § 163 Abs. 1 StPO die Vorermittlungen durch (ohne Auftrag der Staatsanwaltschaft), werden Zeugenaussagen freiwillig abgegeben.

Im Spannungsfeld mit § 203 StGB spricht einiges dafür, dass freiwillige Zeugenaussagen gegenüber der Polizei unterbleiben sollten, wenn dies zu einer Offenbarung von Geheimnissen im Sinne des § 203 StGB führt. Die Prüfung der Staatsanwaltschaft kann und sollte sicherstellen, dass der Geheimnisträger nur um die Informationen ersucht wird, die wirklich zur Strafverfolgung erforderlich sind.

In jedem Fall sollte der Inhalt einer Anfrage der Ermittlungsbehörde es der Versicherung ermöglichen, die Voraussetzungen des § 24 BDSG überhaupt zu prüfen (siehe bereits Nr. 13.7 des XIII./XIV. Tätigkeitsberichtes).

Falls aus der Anfrage der Polizeidienststelle hervorgeht, dass wegen möglichen Versicherungsbetrugs ermittelt wird und die Versicherung selbst geschädigt sein könnte, kommt als Erlaubnisnorm für die Übermittlung der Daten neben § 24 BDSG zusätzlich

die Vereinbarkeitsklausel des Art. 6 Abs. 4 DS-GVO in Verbindung mit Art. 6 Abs. 1 Satz 1 lit. b bzw. f DS-GVO (Durchführung des Versicherungsvertrags bzw. eigene berechtigte Interessen der Versicherung) in Betracht. Sofern der Verdacht auf eine Betrugshandlung (zulasten der Versicherung) hinreichend konkret ist, dürften entgegenstehende Interessen des Beschuldigten nicht überwiegen.

Ob eine Versicherung freiwillig gegenüber der Polizeidienststelle Auskunft erteilt oder auf eine vorherige Prüfung und Anfrage durch die Staatsanwaltschaft besteht, könnte davon abhängig gemacht werden, ob sich bei der Versicherung selbst bei genauer Prüfung der vorhandenen Datenlage ein Verdacht auf Versicherungsbetrug zulasten der Versicherung bestätigt. Denn in einem solchen Fall wäre die Versicherung auch ohne Anfrage einer Ermittlungsbehörde zur Übermittlung der Daten berechtigt, die für eine Strafanzeige erforderlich sind. Grundlage wären hier wiederum Art. 6 Abs. 4 i. V. m. Art. 6 Abs. 1 Satz 1 lit. b bzw. f DS-GVO, ggf. zusätzlich Art. 9 Abs. 2 lit. f bzw. g DS-GVO (s. o.).

Notwendig ist zusätzlich stets eine Detailprüfung, ob alle von der Polizeidienststelle angefragten Detailinformationen tatsächlich erforderlich erscheinen. In Zweifelsfällen sollte die Ermittlungsbehörde um Konkretisierung gebeten werden. Soweit Gesundheitsdaten als Daten nach Art. 9 Abs. 1 DS-GVO offengelegt werden sollen, müsste zusätzlich eine Erlaubnisnorm des Art. 9 Abs. 2 DS-GVO oder § 22 BDSG erfüllt sein. In Betracht käme Art. 9 Abs. 2 lit. f bzw. g DS-GVO (Rechtsverteidigung bzw. Spezialnorm im erheblichen öffentlichen Interesse).

12.3 Schutz von Berufsgeheimnissen in E-Mails

Bereits im XVII. Tätigkeitsbericht (Nr. 16.6) hat der Landesbeauftragte die Anforderungen an den Versand von personenbezogenen Daten per E-Mail durch Berufsgeheimnisträger dargestellt. Im Jahr 2021 hat er dazu auch ein Informationsblatt[28] herausgegeben mit dem Ziel, die Anforderungen der Orientierungshilfe der Datenschutzkonferenz „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ (Näheres dazu siehe XVII. Tätigkeitsbericht, Nr. 6.10) für Berufsgeheimnisträger anhand konkreter Anwendungsbeispiele praxisnah auszulegen und organisatorische sowie technische Rahmenbedingungen zu erläutern. Es enthält neben der datenschutzrechtlichen Bewertung eine ganze Reihe praktischer Hinweise, z. B. zur Transportverschlüsselung, zu weiteren Sicherheitsmaßnahmen bei besonders sensiblen Daten, zum Passwort-/Schlüsselmanagement, zum Prüfen der E-Mail-Adresse des Empfängers, zum Schutz des eigenen E-Mail-Einganges sowie auch zu Alternativen zur E-Mail-Kommunikation.

12.4 Einsicht in die Mitgliederliste einer Genossenschaft

Auf eine Anfrage hin hat der Landesbeauftragte geprüft, inwieweit Rechte bestehen, in die Mitgliederliste einer Genossenschaft einzusehen oder Abschriften daraus zu erhalten.

Nach § 31 GenG besteht ein uneingeschränktes Recht der Genossenschaftsmitglieder auf Einsicht in die Mitgliederliste am Sitz der Genossenschaft. Es steht den Mitgliedern zu, damit sie sich über den Mitgliederbestand der Genossenschaft mit allen Angaben

[28] https://lsaurl.de/EMailBerufsgeheimnis

laut § 30 Abs. 1 GenG umfassend informieren können (siehe Begründung des Gesetzgebers in der Bundesrats-Drucksache 360/93, Seite 335). Diese Offenlegung ist somit nach Art. 6 Abs. 1 Satz 1 lit. c DS-GVO datenschutzrechtlich zulässig.

Dass die von der Einsichtnahme betroffenen weiteren Genossenschaftsmitglieder diese Offenlegung ihrer Daten durch eine Erklärung (Widerspruch, Sperre o. ä.) verhindern könnten, ist weder durch das GenG noch durch die DS-GVO vorgesehen. Über diese möglichen Offenlegungen sind alle Mitglieder zu informieren, bestenfalls in den datenschutzrechtlichen Informationen, die sie bei Aufnahme in die Genossenschaft erhalten (Art. 13 Abs. 1 lit. e DS-GVO).

Anders ist es, wenn Dritte die Einsichtnahme in die Mitgliederliste beantragen oder wenn die antragstellende Person auch eine Abschrift der Mitgliederliste wünscht, die über ihre eigenen Daten hinausgeht (als Ausdruck oder auch Fotografie, z. B. mit dem Smartphone). In diesen Fällen muss die antragstellende Person ein berechtigtes Interesse vortragen, z. B. die Absicht, ein Recht nach Maßgabe des § 45 GenG auszuüben (siehe Bundesrats-Drucksache 360/93, Seite 336), und die schutzwürdigen Interessen der von dem Antrag betroffenen Personen dürften demgegenüber nicht überwiegen (§ 31 Abs. 1 GenG, Art. 6 Abs. 1 Satz 1 lit. f DS-GVO).

Diesbezüglich steht den betroffenen Personen (den weiteren Genossenschaftsmitgliedern) ein Widerspruchsrecht zu, wobei sie Gründe geltend machen müssten, die sich aus ihrer besonderen Situation ergeben (Art. 21 Abs. 1 DS-GVO). Auf dieses Widerspruchsrecht sind die betroffenen Personen ausdrücklich hinzuweisen, in einer verständlichen und von anderen Informationen getrennten Form (Art. 21 Abs. 4 DS-GVO) und bestenfalls so rechtzeitig, dass die Betroffenen ihr Widerspruchsrecht ausüben können, bevor die Offenlegung erfolgt.

Ob das Erteilen einer vollständigen Abschrift der Mitgliederliste zulässig ist, ist bei Vorliegen eines entsprechenden Antrags im Einzelfall zu prüfen. Es sind die von der antragstellenden Person vorgetragenen berechtigten Interessen auf der einen Seite gegenüber den generalisierten schutzwürdigen Interessen der betroffenen Mitglieder auf der anderen Seite gegeneinander abzuwägen, ggf. unter Berücksichtigung der individuell von einzelnen Mitgliedern mit einem Widerspruch vorgetragenen Interessen.

Mitglieder einer Genossenschaft haben nach § 31 GenG das Recht, uneingeschränkt in die vollständige Mitgliederliste mit den Angaben laut § 30 Abs. 1 GenG einzusehen. Ein Widerspruchsrecht gegen diese Art der Offenlegung ist gesetzlich nicht vorgesehen.

Anders ist es, wenn Dritte die Einsichtnahme in die Mitgliederliste beantragen oder wenn die antragstellende Person auch eine Abschrift der Mitgliederliste wünscht, die über ihre eigenen Daten hinausgeht. In diesen Fällen muss die antragstellende Person ein berechtigtes Interesse vortragen und die schutzwürdigen Interessen der von dem Antrag betroffenen Personen dürften demgegenüber nicht überwiegen (§ 31 Abs. 1 GenG, Art. 6 Abs. 1 Satz 1 lit. f DS-GVO). Diesbezüglich steht den Betroffenen ein Widerspruchsrecht zu, wobei sie Gründe geltend machen müssten, die sich aus ihrer besonderen Situation ergeben.

12.5 Fotografieren von Wohnräumen und Datenerhebung für das Notariat durch Immobilienmakler

Der Landesbeauftragte war in verschiedenen Vorgängen mit der Frage befasst, in welchem Umfang Immobilienvermittler (Immobilienmakler) personenbezogene Daten verarbeiten dürfen und ob sie für bestimmte Datenverarbeitungen eine Einwilligung der betroffenen Personen benötigen. Zwei Fallkonstellationen seien hier beispielhaft dargestellt.

Immobilienmakler werden auf Auftrag entweder des verkaufswilligen Eigentümers und/oder von Kaufinteressenten tätig. Gegenstand eines Maklervertrages ist üblicherweise der Nachweis der Gelegenheit zum Abschluss eines Kaufvertrags über eine Immobilie oder die Vermittlung eines solchen Vertrags (vgl. § 656a BGB). Dabei kann der Umfang der Tätigkeiten, die der Immobilienmakler übernehmen soll, und damit einhergehend die Rechte und Pflichten beider Vertragsparteien im Maklervertrag unterschiedlich vereinbart werden. Welche Datenverarbeitungen dementsprechend zur Erfüllung des Maklervertrages erforderlich sind (vgl. Art. 6 Abs. 1 Satz 1 lit. b DS-GVO), bestimmt sich stets anhand der individuellen vertraglichen Regelungen.

Ein Kaufinteressent schilderte in seiner Beschwerde beim Landesbeauftragten, dass er, nachdem er sein Interesse am Kauf einer zuvor besichtigten Immobilie bekundet hatte, von dem Immobilienmakler aufgefordert worden sei, per E-Mail weitere personenbezogene Daten anzugeben, damit diese zur Vorbereitung des Kaufvertragsentwurfs an das Notariat weitergeleitet werden könnten. Dazu zählten der vollständige Name und Geburtsname, Anschrift, Geburtsdatum, Berufsbezeichnung, Familienstand und die Steuer-Identifikationsnummer (Steuer-ID). Ihm sei auch auf Nachfrage nicht die Möglichkeit eröffnet worden, seine Daten selbst direkt dem Notariat zur Verfügung zu stellen.

Bei der datenschutzrechtlichen Überprüfung stellte der Landesbeauftragte fest, dass es nicht ausdrücklich vertraglich vereinbart war, dass der Immobilienmakler für die Vorbereitung des Kaufvertragsentwurfes zu sorgen oder die Kommunikation mit dem Notariat zu übernehmen hat. Zwar konnte es sich dabei um einen Service für die Kaufinteressenten handeln, verpflichtend war dies nicht. Alternativ möglich war auch, dass die Kaufinteressenten selbst Kontakt zum Notariat aufnehmen und ihre Daten direkt übermitteln. Das Erheben der Daten durch den Immobilienmakler und das Weiterleiten an das Notariat war daher zur Vertragsabwicklung nicht erforderlich; Art. 6 Abs. 1 Satz 1 lit. b DS-GVO schied als Erlaubnisnorm aus.

Der Immobilienmakler konnte auch nicht nachweisen, dass der Kaufinteressent in die Datenübermittlung wirksam eingewilligt hatte (Art. 6 Abs. 1 Satz 1 lit. a DS-GVO).

Hinzu kam, dass für das Verarbeiten der Steuer-ID § 139b Abs. 2 Satz 2 AO zu beachten ist. Diese Vorschrift regelt die Voraussetzungen, unter denen nichtöffentliche Stellen, wie es ein Immobilienmakler ist, die Steuer-ID verarbeiten dürfen. Dazu gehört, dass die Verarbeitung für Datenübermittlungen zwischen der nichtöffentlichen Stelle und den Finanzbehörden erforderlich ist oder dass eine Rechtsvorschrift die Verarbeitung der Steuer-ID ausdrücklich erlaubt oder anordnet. Sind diese Voraussetzungen nicht erfüllt, wie das hier der Fall war, kann nur eine Einwilligung der betroffenen Person die Verarbeitung legitimieren (§ 139b Abs. 2 Satz 2 Nr. 1 AO).

Daher hat der Landesbeauftragte empfohlen, künftig informierte Einwilligungen in Datenübermittlungen an das Notariat schriftlich oder zumindest in Textform einzuholen. Um dem Merkmal der Freiwilligkeit gerecht zu werden, sollte in den Erläuterungen zur Einwilligung ausdrücklich darauf hingewiesen werden, dass auch die Möglichkeit besteht, die Daten direkt an das Notariat, das namentlich benannt sein müsste, zu übermitteln. Der Immobilienmakler setzte dies um.

In einem weiteren Beschwerdefall ging es um das Anfertigen von Fotografien von vermieteten Wohnräumen durch den Immobilienmakler und deren Weitergabe an Kaufinteressenten. Derartige Fotos sollen den Kaufinteressenten einen Eindruck vom Zustand der Immobilie verschaffen. Häufig dient hierzu schon das Exposé, bevor ein Besichtigungstermin vereinbart wird. Teilweise werden die Fotos auch auf Internetportalen veröffentlicht.

Die Fotografien enthalten in aller Regel personenbezogene Daten, da sie Rückschlüsse auf das private Lebensumfeld der Bewohner der Räumlichkeiten zulassen, etwa auf familiäre Verhältnisse (z. B. durch Fotos an den Wänden, Kleidungsstücke, Kinderspielzeug), auf Gewohnheiten (z. B. Hobbys, Ordnungssinn), ggf. auch auf die finanziellen Verhältnisse (durch den Wert von Einrichtungsgegenständen). Da hier stets die grundrechtlich besonders geschützte Privatsphäre und private Wohnung betroffen sind, ist Voraussetzung für die datenschutzkonforme Verarbeitung der Fotografien regelmäßig eine freiwillige, informierte und jederzeit widerrufliche Einwilligung der betroffenen Personen nach Art. 6 Abs. 1 Satz 1 lit. a DS-GVO. Die Betroffenen können frei von Einflussnahme selbst entscheiden, welche Räumlichkeiten in welchem Zustand auf Fotografien abgebildet werden und ob diese beispielsweise in Inseraten in dem für jedermann zugänglichen Internet veröffentlicht oder nur gegenüber Kaufinteressenten im Einzelfall zugänglich gemacht werden dürfen.

In dem geprüften Einzelfall konnte der Immobilienmakler eine solche Einwilligung der betroffenen Personen nicht nachweisen. Er schilderte zwar, dass die Initiative für das Anfertigen der Fotografien von der Bewohnerin ausging, weil diese in der Pandemie und aufgrund ihrer gesundheitlichen Verfassung Besichtigungstermine vermeiden wollte. Dies allerdings bestritt die Betroffene und legte dar, der Immobilienmakler hätte ihr versichert, die Fotos würden nur zu internen Zwecken angefertigt und nicht an Dritte weitergegeben. Da der Immobilienmakler zudem nicht nachweisen konnte, die Bewohnerin nach Art. 13 DS-GVO über die Datenverarbeitungen informiert zu haben, war ein Verstoß gegen die DS-GVO festzustellen, wegen dem der Landesbeauftragte nach Abwägung der Gesamtumstände eine Verwarnung aussprach.

Für das Erheben und Weitergeben von personenbezogenen Daten von Kaufinteressenten an ein Notariat benötigt ein Immobilienmakler in der Regel eine Einwilligung der betroffenen Personen, es sei denn, dies ist ausdrücklich als vertragliche Pflicht vereinbart. Für das Verarbeiten der Steuer-ID ist § 139b Abs. 2 Satz 2 AO zu beachten und daher stets eine Einwilligung einzuholen.

Auch für das Anfertigen und Weitergeben oder gar Veröffentlichen von Fotografien von vermieteten Wohnräumen bedarf es grundsätzlich einer Einwilligung der betroffenen Personen.

12.6 Speicherfrist von 30 Jahren für bestimmte Versicherungsdaten

Im Jahr 2021 hat der Landesbeauftragte geprüft, ob es zulässig sei, dass personenbezogene Daten von Versicherungsnehmern bei Haftpflichtversicherungen für die Dauer von bis zu 30 Jahren nach Ende des Versicherungsvertrages gespeichert bleiben.

Als Zweck der Speicherfrist wurde vorgetragen, dass die Versicherung vertragliche Ansprüche der Versicherungsnehmer auf ihre Berechtigung prüfen kann. Dabei ging es um Haftpflichtschäden bzw. Ereignisse, die für beide Vertragsparteien nur bedingt vorhersehbar sind, z. B. Gesundheits-, Gebäude- und Umweltschäden, bei denen mehrjährige, zunächst unsichtbare Verläufe durchaus realistisch sind. Derartige Fälle treten zwar nicht häufig, aber in größeren Zeitabständen immer wieder auf und verursachen oft erhebliche Schadenssummen (Streitwerte). Denkbar ist dies im Bereich der Haftpflichtversicherung der planenden, beratenden Berufe (z. B. Architekten, selbständige Bauingenieure), bei der Versicherung der Heilberufe oder Notare, bei Umweltrisiken und teilweise in der Vermögensschadenversicherung.

Als Rechtsgrundlage für die Speicherung war Art. 6 Abs. 1 Satz 1 lit. b DS-GVO zu prüfen. In Betracht kam auch Art. 6 Abs. 1 Satz 1 lit. f DS-GVO. Für die Entscheidung kommt darauf an, ob die Daten zur Durchführung des Versicherungsvertrages für die Dauer von 30 Jahren tatsächlich erforderlich sind oder ob ggf. auch berechtigte Interessen der Versicherung oder eines Dritten (z. B. des vom Versicherungsnehmer Geschädigten) die Speicherung für diese Dauer rechtfertigen können.

Eine besondere Bedeutung kommt dabei dem so genannten Verstoßprinzip zu, das in manchen Versicherungsbedingungen vereinbart ist. Beim Verstoßprinzip ist der Versicherungsfall definiert als „ein während der Wirksamkeit der Versicherung begangener Verstoß, der einen Schaden zur Folge hatte“. Dabei ist ein versicherungsvertraglicher Anspruch auch möglich, wenn der Schaden erst (ggf. weit) nach dem Verstoß und auch nach dem Ende des Versicherungsvertrages entstanden und bekannt geworden ist. Als klassisches Beispiel wurde der Planungsfehler eines Architekten geschildert, der später die Bausubstanz beeinträchtigt und zu einem Schaden beim Bauherren/Eigentümer führt, was allerdings zuweilen erst viele Jahre später sichtbar wird.

Ausgangspunkt der datenschutzrechtlichen Prüfung ist die mögliche Verjährung der vertraglichen Ansprüche des Versicherungsnehmers gegen die Versicherung. Denn innerhalb der Verjährungsfrist kann stets mit der Geltendmachung vertraglicher Ansprüche gerechnet werden. Zu berücksichtigen sind im Dreiecksverhältnis aber auch die Verjährungsfristen der Schadensersatzansprüche des durch den Haftpflichtfall Geschädigten gegen den Versicherungsnehmer. Denn solange der Geschädigte seine Ansprüche noch nicht gegenüber dem Versicherungsnehmer geltend gemacht hat, wird auch der Versicherungsnehmer etwaige Ansprüche gegen die Versicherung noch nicht erheben, bzw. nicht erheben können.

Die regelmäßige Verjährungsfrist beträgt 3 Jahre (§ 195 BGB). Sie beginnt allerdings erst mit dem Schluss des Jahres zu laufen, in dem der Anspruch entstanden ist und der Anspruchsberechtigte von seinem Anspruch Kenntnis erlangt hat (vgl. § 199 Abs. 1 BGB).

Ohne Rücksicht auf die Kenntnis verjähren Schadensersatzansprüche in 10 Jahren von ihrer Entstehung an. Ohne Rücksicht auf Entstehung und Kenntnis verjähren Schadensersatzansprüche in 30 Jahren von der Begehung der Handlung, der Pflichtverletzung oder dem sonstigen, den Schaden auslösenden Ereignis an. Maßgeblich ist die früher endende Frist (§ 199 Abs. 3 BGB).

Gibt es also eine Handlung, Pflichtverletzung oder ein sonstiges schadenauslösendes Ereignis, ist aber dennoch der Schadensersatzanspruch noch nicht entstanden (z. B. weil der Schaden noch nicht eingetreten ist, wie im Falle der Schäden an der Bausubstanz durch einen Architektenfehler) und kann somit der Geschädigte davon auch noch keine Kenntnis erlangt haben, verjährt der Anspruch im extremsten Fall erst nach 30 Jahren nach dem schadenauslösenden Ereignis. Innerhalb dieser Frist könnten folglich Schadensersatzansprüche des Geschädigten gegen den Versicherungsnehmer geltend gemacht werden. Daran schließt sich ggf. eine weitere Frist für die Verjährung oder ggf. Verwirkung der versicherungsvertraglichen Ansprüche des Versicherungsnehmers gegen die Versicherung an, wobei die vertraglichen Obliegenheiten des Versicherungsnehmers zu berücksichtigen sind.

Schadensersatzansprüche, die auf der vorsätzlichen Verletzung (u. a.) des Lebens, des Körpers, der Gesundheit beruhen, verjähren immer in 30 Jahren von der Begehung der Handlung, der Pflichtverletzung oder dem sonstigen, den Schaden auslösenden Ereignis an (§ 197 Abs. 1 Nr. 1, § 199 Abs. 2 BGB). Dies wirkt sich insbesondere bei Haftpflichtversicherungen von medizinischem Personal aus.

Die theoretische Möglichkeit, dass ein Versicherungsnehmer gegenüber der Versicherung auch nach einem längeren Zeitraum als 10 Jahre nach Beendigung des Versicherungsvertrages berechtigterweise vertragliche Ansprüche geltend macht, lässt sich in den beschriebenen Konstellationen nicht gänzlich von der Hand weisen.

Zwar scheint der Eintritt eines solchen Falles nicht sehr wahrscheinlich bzw. häufig aufzutreten. Gleichwohl könnte das finanzielle Risiko für die Versicherung in solchen Einzelfällen hoch sein. Es liegt zudem stets im Interesse der Versicherung, aber auch des Versicherungsnehmers selbst und auch des Geschädigten, dass berechtigte Ansprüche zweifelsfrei festgestellt und reguliert werden können, insbesondere wenn der Versicherungsnehmer in einem Streitfall nach vielen Jahren die notwendigen Unterlagen, um seinen Anspruch nachzuweisen, nicht mehr (lückenlos) vorlegt oder vorlegen kann.

Auf Initiative des Landesbeauftragten hat auch der Arbeitskreis Versicherungswirtschaft der Datenschutzkonferenz diese Fragestellung erörtert und kam zu dem Ergebnis, dass die Speicherung von personenbezogenen Daten für die Dauer von 30 Jahren nach Beendigung des Versicherungsverhältnisses bei nachvollziehbarer Begründung und einzelnen Versicherungsarten als zulässig erachtet werden kann.

Voraussetzung dafür ist, dass nach Ablauf der regulären Speicherfrist von maximal 10 Jahren nur noch die personenbezogenen Daten gespeichert bleiben, die erforderlich sind, um den Zweck der Beweissicherung für späte Haftungsfälle zu verfolgen, und dass die Verarbeitung der Daten auf genau diesen Zweck beschränkt wird. Eine Verarbeitung zu anderen Zwecken (z. B. Werbung für andere Versicherungsprodukte) wäre nur aufgrund einer eigenständigen Rechtsgrundlage zulässig, z. B. einer Einwilligung. Die enge Zweckbindung muss durch angemessene technisch-organisatorische

Maßnahmen umgesetzt werden, z. B. durch stark eingeschränkte Zugriffsberechtigungen.

Die Speicherung von personenbezogenen Daten aus einem Haftpflichtversicherungsvertrag bis zu maximal 30 Jahren nach Beendigung des Versicherungsverhältnisses kann datenschutzrechtlich zulässig sein, soweit im Einzelfall (weitere) vertragliche Ansprüche wegen der Verletzung des Lebens, des Körpers, der Gesundheit oder der Freiheit geltend gemacht werden können (§ 199 Abs. 2 BGB) oder wenn die so genannte Verstoßtheorie vertraglich vereinbart ist. Auch soweit spezialrechtliche Vorschriften entsprechend lange Verjährungsfristen für vertragliche Ansprüche konkret vorsehen, kommt eine längere Aufbewahrungsfrist in Betracht. Die Speicherfrist muss durch angemessene technische und organisatorische Maßnahmen begleitet werden.

12.7 Erfüllung des Auskunftsanspruchs nach Art. 15 DS-GVO

In seinem Urteil vom 15. Juni 2021 (VI ZR 576/19) hat sich der Bundesgerichtshof unter anderem zum Umfang des Auskunftsanspruchs nach Art. 15 DS-GVO geäußert. Ein ebenfalls thematisierter Punkt war die Frage, ob ein Auskunftsanspruch nach Art. 15 DS-GVO auch bei unrichtiger oder unvollständiger Auskunft erfüllt sein kann.

Nach dem Urteil ist der – grundsätzlich weit zu verstehende – Auskunftsanspruch dann erfüllt, wenn der Auskunftsverpflichtete unmissverständlich zum Ausdruck bringt, er habe die Auskunft in dem konkret geschuldeten Umfang vollständig erteilt. Dazu ist es notwendig, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdeckt. Der bloße Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist führt nicht dazu, dass noch weitergehende Auskunft erteilt werden muss. Selbst eine inhaltliche teilweise falsche Auskunft führt nicht automatisch dazu, dass der Anspruch nicht erfüllt wurde.

Das Urteil erscheint auf den ersten Blick vielleicht etwas merkwürdig. Es bedeutet aber weder, dass eine grobe Erteilung von Auskünften genügt, noch, dass die bloße Vermutung einer falschen Auskunft oder geringe Fehler dazu verpflichten, die Beantwortung nachzubessern.

Der Auskunftspflichtige muss genau prüfen, in welchem Umfang die Auskunft berechtigterweise begehrt wird und sich mit jeder Kategorie der Auskunftsgegenstände ernsthaft auseinandersetzen. Wird eine Auskunft erteilt, macht der pauschale Hinweis, weitere personenbezogene Daten des Auskunftsberechtigten würden nicht verarbeitet, eine Auskunft nicht automatisch vollständig.

Eine Ergänzung kann der Auskunftsberechtigte vor allem dann verlangen, wenn sich der Auskunftspflichtige zu bestimmten Punkten gar nicht äußert.

Auskunftsbegehren nach Art. 15 DS-GVO sollten durch den Berechtigten klar formuliert und durch den Verpflichteten sorgfältig beantwortet werden.

12.8 Dokumentation der Löschung personenbezogener Daten

Der Landesbeauftragte wurde gefragt, wie durch einen Verantwortlichen nachgewiesen werden kann, dass eine Löschungsverpflichtung aus Art. 17 DS-GVO erfüllt worden ist. Zu klären war, ob für Nachweiszwecke dasjenige Schreiben gespeichert werden darf, mit dem einer betroffenen Person die Löschung ihrer personenbezogenen Daten bestätigt wird oder ob dadurch unnötigerweise weiterhin Daten der betroffenen Person gespeichert werden.

Der Begriff der Löschung ist in der DS-GVO nicht definiert. Wenn eine betroffene Person die Löschung beantragt, wird jedoch grundsätzlich davon auszugehen sein, dass alle zu ihrer Person vorhandenen Daten unkenntlich gemacht werden sollen. Dies beinhaltet regelmäßig auch die Daten, die im Zuge der Bearbeitung eines Antrags auf Löschung verarbeitet werden. Dem Antrag ist zu entsprechen, wenn die Voraussetzungen des Art. 17 Abs. 1 DS-GVO erfüllt sind.

Im Regelfall kann ein Verantwortlicher den Nachweis der ordnungsgemäßen Löschung personenbezogener Daten durch ein geeignetes Löschkonzept erbringen. In Einzelfällen kann zur Durchsetzung von Betroffenenrechten eine weitere Dokumentation unter vorübergehender Speicherung personenbezogener Daten erforderlich sein, wie z. B. bei der Erteilung von (Negativ-)Auskünften nach Art. 15 DS-GVO. Datenbestände, die der Rechenschaftspflicht oder weiteren Aufbewahrungspflichten unterfallen, sollten dann aber im Produktivsystem nicht mehr verfügbar sein. Sie sind also strukturell vom aktiven Datenbestand getrennt zu halten.

Bei den Anforderungen an die Nachweispflichten muss zwischen der anlassbezogenen Ausübung eines Betroffenenrechts, z. B. in Form eines Löschungsverlangens, und der routinemäßigen Löschung gemäß Löschkonzept unterschieden werden.

Im Regelfall kann ein Verantwortlicher den Nachweis der ordnungsgemäßen Löschung personenbezogener Daten durch ein geeignetes Löschkonzept erbringen.

12.9 Verarbeitung von Positivdaten durch Auskunfteien

Bereits mit Beschluss vom 11. Juni 2018 hatte die DSK festgestellt, dass Handels- und Wirtschaftsauskunfteien sog. Positivdaten zu Privatpersonen grundsätzlich nicht auf Grundlage der Interessenabwägungsklausel des Art. 6 Abs. 1 lit. f DS-GVO erheben können. Positivdaten sind Informationen, die keine negativen Zahlungserfahrungen oder sonstiges nicht vertragsgemäßes Verhalten zum Inhalt haben, sondern zum Beispiel die Informationen über die Tatsache, dass ein Vertrag abgeschlossen wurde. Solche Positivdaten können – je nach Umfang – detaillierte Informationen über die persönliche Lebensgestaltung enthalten, z. B. Vermögen, Neigungen, Hobbys, vertragliche Verpflichtungen etc. Bei diesen Daten überwiegt regelmäßig das schutzwürdige Interesse der betroffenen Personen, selbst über die Verwendung zu bestimmen. Daher ist bereits die Übermittlung von Positivdaten von einem Unternehmen an eine Auskunftei auf der Grundlage des Art. 6 Abs. 1 lit. f DS-GVO regelmäßig unzulässig. Daraus folgt die regelmäßige Unzulässigkeit der Verarbeitung dieser Daten durch die Auskunftei.

Im Berichtszeitraum hatte die DSK zu prüfen, ob für die verbreitete Praxis der Übermittlung und Verarbeitung von Positivdaten zu Verträgen über Mobilfunkdienste und Dauerhandelskonten von Privatpersonen eine andere Bewertung erforderlich ist. Hier geht es um längerfristige Verträge, die Vorausleistungspflichten oder Finanzierungs- bzw. Stundungselemente zu Lasten der Verantwortlichen enthalten, die aber insbesondere keine Zahlungsstörungen der Kunden aufweisen. In der Praxis wurden unter anderem diese Daten bei der Bildung von Scorewerten herangezogen.

Nach der Prüfung von Stellungnahmen von Unternehmen und Verbänden sah die DSK in Ihrem erneuten Beschluss vom 22. September 2021 keinen Grund von Ihrer bisherigen Auffassung abzuweichen.

Eine Ausnahme gilt nur für den Bereich der Kreditwirtschaft, weil hier spezielle Verpflichtungen nach dem Kreditwesengesetz bestehen, die Bonität von Kreditantragstellern zu prüfen. Dies hatte die DSK allerdings auch schon in Ihrem Beschluss vom 11. Juni 2018 festgestellt.[29] Ansonsten bedarf es für die Verarbeitung von Positivdaten grundsätzlich einer informierten und freiwilligen Einwilligung.

Die Übermittlung von Positivdaten von einem Unternehmen an eine Auskunftei auf der Grundlage des Art. 6 Abs. 1 lit. f DS-GVO ist regelmäßig unzulässig. Es bedarf grundsätzlich einer informierten und freiwilligen Einwilligung.

12.10 Erbenermittlung durch Inkassounternehmen

Eine Frau beschwerte sich beim Landesbeauftragten darüber, dass ein Inkassounternehmen gegen sie einen Anspruch geltend machte, der ursprünglich gegen Ihren – inzwischen verstorbenen – Vater gerichtet war. Sie sei nicht Erbin. Es könne nicht sein, dass ein Inkassounternehmen überhaupt ihre Daten verarbeite.

Die Prüfung ergab, dass dem Inkassounternehmen telefonisch nur ein Auftrag zur Erbenermittlung erteilt worden war. Das Inkassounternehmen ging allerdings davon aus, mit der Einziehung der offenen Forderung beauftragt worden zu sein.

Als Rechtsgrundlage für die Ermittlung der Erben eines verstorbenen Schuldners kommt Art. 6 Abs. 1 lit. f DS-GVO in Betracht. Im Erbfall haften die Erben für die Verbindlichkeiten des Verstorbenen, § 1922 BGB.

Allerdings dürfen Daten zur Erbenermittlung nur insoweit verarbeitet werden, als die Verarbeitung erforderlich ist und entgegenstehende Interessen der betroffenen Person nicht überwiegen. Die Verarbeitung von Daten der Nicht-Erben kommt bestenfalls in Betracht, soweit sie zur Ermittlung tatsächlicher Erben erforderlich ist. Grundsätzlich kann der Gläubiger allerdings Dritte mit der Erbenermittlung beauftragen.

Der Inhalt von Aufträgen, zu deren Bearbeitung personenbezogene Daten verarbeitet werden, muss genau verabredet und dokumentiert werden. Dies ergibt sich aus der Rechenschaftspflicht des Art. 5 Abs. 2 DS-GVO. Danach müssen Verantwortliche u. a.

[29] https://www.datenschutzkonferenz-online.de/media/dskb/20180611_dskb_verarbeitung_positivdaten.pdf

die Rechtmäßigkeit und die festgelegten, eindeutigen und legitimen Zwecke der Verarbeitung nachweisen können. Dies war hier nicht der Fall.

12.11 Einholung von umfangreichen Einwilligungserklärungen mithilfe von Vordrucken

Im Berichtszeitraum erteilte der Landesbeauftragte Hinweise zu einer Anfrage, welche Anforderungen an Vordrucke zu stellen seien, mit denen umfangreiche Einwilligungserklärungen einholt werden sollten.

Die Erteilung von Einwilligungen sollte dokumentiert werden. Die DS-GVO enthält insoweit keine Formvorschriften. Die Einwilligung kann nach der DS-GVO sogar grundsätzlich formfrei erfolgen. Allerdings müssen die für eine Verarbeitung Verantwortlichen nach Art. 7 Abs. 1 DS-GVO nachweisen können, dass eine Einwilligung erteilt wurde. Die Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO fordert außerdem allgemein, die Einhaltung der DS-GVO nachweisen zu können. Eine formularmäßig erteilte Einwilligung dürfte ein sicherer Weg sein, entsprechende Nachweise führen zu können.

Von anderen schriftlich niedergelegten Punkten muss die datenschutzrechtliche Einwilligung ganz klar und deutlich zu unterscheiden sein. Hierfür vorformulierte Texte müssen verständlich, in leicht zugänglicher Form und in einer klaren und einfachen Sprache verfasst sein. Missbräuchliche Klauseln sind nach Erwägungsgrund 42 Satz 3 ausdrücklich zu vermeiden.

Außerdem muss die Einwilligungserklärung klar erkennen lassen, worin die jeweilige Person einwilligt, um Freiwilligkeit und Informiertheit zu gewährleisten.

Die Einwilligungserklärung muss ganz deutlich erkennen lassen, dass und in welchem Umfang die jeweilige Person eine datenschutzrechtliche Einwilligung in die Verarbeitung ihrer Daten erteilt. Innerhalb einer Werbeeinwilligung muss beispielsweise deutlich erkennbar sein, für welche konkreten Kategorien von Werbemaßnahmen die Einwilligung gilt.

Pauschale Formulierungen wie z. B. „erklärt sich … aus organisatorischen Gründen …. einverstanden“ sind nicht geeignet. Bei umfangreichen Verarbeitungen von personenbezogenen Daten sind oft mehrere Einwilligungserklärungen erforderlich bzw. eine Einwilligungserklärung mit deutlich voneinander getrennt erkennbaren Verarbeitungszwecken und jeweils separaten Widerrufsmöglichkeiten.

Genügt die Einwilligungserklärung diesen Anforderungen nicht, kann die Einwilligung nach Art. 7 Abs. 2 Satz 2 DS-GVO jedenfalls teilweise unwirksam sein.

13 Bußgeldverfahren

13.1 Statistik der behördlichen Bußgeldverfahren

Datenschutzrechtliche Verstöße kann der Landesbeauftragte mit einer Geldbuße gemäß Art. 83 Abs. 4 bis 6 DS-GVO ahnden (§§ 23 Abs. 5, 31 DSAG LSA i. V. m. § 41 BDSG). In diesem Sinne wurden 27 Bußgeldverfahren eingeleitet, wovon 3 Verfahren eingestellt und 11 Verfahren in 2021 rechtskräftig abgeschlossen wurden.

Vermehrt wurden Ordnungswidrigkeitsverfahren wegen pflichtwidrig unterlassenen technischen und organisatorischen Maßnahmen eingeleitet. Bei der Bemessung der Geldbuße wurde berücksichtigt, dass die Geschäftstätigkeit durch die staatlichen Maßnahmen zur Eindämmung der Ausbreitung des neuartigen Coronavirus SARS-CoV-2 in Sachsen-Anhalt ab März 2020 ganz erheblich beeinträchtigt war.

Die Gesamtsumme der rechtskräftig im Jahr 2021 verhängten Geldbußen aus Verfahren, die auch in Vorjahren begonnen, beläuft sich auf 108.380 Euro:

Tatbestände	Geldbußen insgesamt
Art. 83 Abs. 5 lit. a i. V. m. Art. 6 DS-GVO Unzulässige Datenverarbeitung, verschiedene	23.150 Euro
Art. 83 Abs. 5 lit. a i. V. m. Art. 6 DS-GVO Unzulässige Videoüberwachung (u. a. von Beschäftigten)	60.780 Euro
Art. 83 Abs. 5 lit. b i. V. m. Art. 17 DS-GVO Verspätete Datenlöschung	250 Euro
Art. 83 Abs. 5 lit. c i. V. m. Art. 44 DS-GVO Unzulässiger Datentransfer in ein Drittland	450 Euro
Art. 83 Abs. 4 lit. a i. V. m. Art. 25 Abs. 1 DS-GVO Unzureichender Datenschutz durch Technikgestaltung	22.850 Euro
Art. 83 Abs. 4 lit. a i. V. m. Art. 31, 37 DS-GVO und Unzureichende Zusammenarbeit mit der Aufsichtsbehörde, keine Benennung eines Datenschutzbeauftragten	900 Euro

SACHSEN-ANHALT

Landesbeauftragte
für den Datenschutz

XIX. Tätigkeitsbericht
der Landesbeauftragten für den Datenschutz

2022

14 Der Landesbeauftragte

14.1 Tätigkeit im Berichtszeitraum, Entwicklung des Arbeitsaufkommens – Fallstatistik

Ein besonders medienwirksames Thema im Jahr 2022 war eine Datenschutzverletzungsmeldung durch das Universitätsklinikum Magdeburg (Nr. 23.6). Was zunächst eher harmlos klingt, hat sich als ein massives datenschutzrechtliches Problem herausgestellt. Durch eine Beschäftigte des Universitätsklinikums sollen regelmäßig Meldedaten zu privaten Zwecken abgefragt worden sein; genauer gesagt Meldedaten von Personen, deren politische Orientierung gegensätzlich zu der der Beschäftigten ist. Der Hintergrund des datenschutzrechtlichen Problems ist brisant, der mit der Bewertung verbundene Aufwand beim Landesbeauftragten war enorm.

In der Folge der Ereignisse hat sich der Landesbeauftragte neben dem Einzelfall auch ganz grundsätzlich mit der Frage befasst, wie bei automatisierten Meldedatenabrufen eine effektive datenschutzrechtliche Kontrolle gewährleistet werden kann (Nr. 25). Die Vorstellungen des Landesbeauftragten zur Erhöhung der Sicherheit ließen sich zwar praktisch nicht in Gänze durchsetzen. Mit der erreichten Lösung wurden die gesteigerten Sicherheits- und Datenschutzanforderungen jedoch erfüllt.

Neben der Mitarbeit des Landesbeauftragten in der Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder verfolgt er auch die Entwicklungen auf internationaler Ebene. Die Internationale Datenschutzkonferenz (Global Privacy Assembly) befasste sich in der Türkei unter dem Motto „Rise of Privacy“ („Aufstieg der Privatsphäre“) mit Fragen des Datenschutzes im Zeitalter des raschen technologischen Fortschritts (Nr. 17.2).

In seinen Tätigkeitsberichten stellt der Landesbeauftragte regelmäßig die Anzahl an Posteingängen dar, um einen möglichst objektiven Eindruck von der Entwicklung des Umfangs seiner Tätigkeit zu vermitteln. Auch 2022 war ein Jahr mit stetig hohem Arbeitsaufkommen.

Anzahl der registrierten Posteingänge:

2016	5.506		
2017	6.737		
2018	9.602	zuzüglich	3.306 Meldungen gem. Art. 37 Abs. 7 DS-GVO
2019	10.941	zuzüglich	746 Meldungen gem. Art. 37 Abs. 7 DS-GVO
2020	13.730	zuzüglich	764 Meldungen gem. Art. 37 Abs. 7 DS-GVO
2021	13.933	zuzüglich	1.351 Meldungen gem. Art. 37 Abs. 7 DS-GVO
2022	13.977	zuzüglich	407 Meldungen gem. Art. 37 Abs. 7 DS-GVO

Schwerpunkte seiner Tätigkeit erfasst der Landesbeauftragte über eine Geschäftsstatistik. Innerbehördliche Angelegenheiten (Organisation, Personal, Haushalt) sind nicht erfasst. Wesentliche aufsichtsbehördliche Aufgabenfelder im Jahr 2022 waren:

Beschwerden und Eingaben	971
Informations- und Beratungsfälle	889
Meldungen von Datenschutzverletzungen	305
Abhilfemaßnahmen/Anordnungen	46
Eingeleitete Bußgeldverfahren	3
Europäische Verfahren mit eigener Betroffenheit (Kooperation und Kohärenz)	14
Förmliche Begleitung von Rechtsetzungsvorhaben	14

15 Nationales und Europäisches Datenschutzrecht

15.1 AK Sanktionen: Evaluierung des § 41 BDSG

Mit Schreiben vom 4. Januar 2022 wandte sich das BMI im Zusammenhang mit der Evaluierung des BDSG an den BfDI als seinerzeitigen Vorsitzenden der DSK. Die DSK forderte im BDSG im Abschnitt VII „Haftung und Sanktionen“ „die Befugnisse der Datenschutzaufsichtsbehörden an das deutsche Kartellrecht anzugleichen und die bisherige Regelung des § 41 BDSG um Verweise in das GWB zu ergänzen“. Der derzeitige Verweis auf die analoge Anwendung des OWiG hält für die Verbandshaftung nach der DS-GVO nur unzureichende Haftungs- und Ermittlungsinstrumente vor. Im Rahmen der Evaluierung des BDSG wurde für die Erweiterung des § 41 BDSG u. a. vorgeschlagen, die analoge Anwendung der § 81 c Abs. 5 Satz 2 GWB (Schätzung des Umsatzes), § 82 b i. V. m. § 59 GWB (Herausgabe von Unterlagen zu den wirtschaftlichen Verhältnissen/Umsatz; Durchsuchung und Einsicht in Unterlagen) sowie §§ 81 a ff. GWB (Begriff des funktionalen Unternehmensbegriffes nach Art. 101 und 102 AEUV) aufzunehmen. Auch wurde über die Aufnahme der analogen Anwendung des § 81 h ff. GWB (Kronzeugenregelung bei sehr hohen Geldbußen) sowie des § 53 Abs. 5 GWB (Veröffentlichung von Bußgeldbescheiden nach Abschluss der behördlichen Verfahren ab Bußgeldhöhe von >100.000 € auf der Internetseite der jeweiligen Aufsichtsbehörde) diskutiert. Im Februar 2022 verfasste die Berliner Beauftragte für Datenschutz und Informationsfreiheit als Vorsitzende des AK Sanktionen gegenüber dem BMI in Absprache mit den anderen Aufsichtsbehörden eine Stellungnahme. Der Landesbeauftragte unterstützt ausdrücklich die Forderungen des AK Sanktionen zur Verbesserung der Durchsetzbarkeit der DS-GVO.

Der Landesbeauftragte unterstützt die Forderungen des AK Sanktionen zur Verbesserung der Durchsetzbarkeit der DS-GVO durch Verweise auf das GWB.

15.2 Zuständigkeiten nach dem Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG)

Das TTDSG ist am 1. Dezember 2021 in Kraft getreten. Mit dem Gesetz erfolgte die Anpassung des TKG und des TMG an die DS-GVO und die Umsetzung der RL 2002/58/EG (ePrivacy-RL) zum Schutz der Privatsphäre in nationales Recht. Behördliche Zuständigkeiten und Befugnisse bestimmt das TTDSG für die Bereiche der Telekommunikationsdienste und der Telemedien von Bundesbehörden für den BfDI sowie

für die BNetzA (§§ 1 Abs. 1 Nr. 8 erster Halbsatz, 29, 30 TTDSG). Für Telemedien im Zuständigkeitsbereich der Länder bleibt die Aufsicht durch die nach Landesrecht zuständigen Behörden und § 40 BDSG unberührt (§ 1 Abs. 1 Nr. 8 zweiter Halbsatz TTDSG). Derzeit besteht in Sachsen-Anhalt keine ausdrückliche aufsichtsbehördliche Zuständigkeit für den Schutz der Privatsphäre nach dem TTDSG. Ferner fehlen behördliche Befugnisse zum Vollzug der Vorschriften des TTDSG auf Landesebene. Einige Bundesländer haben bereits ergänzende Regelungen getroffen und Zuständigkeiten ihren Landesbeauftragten zugewiesen. So regte auch der Landesbeauftragte beim MI LSA an, ihm aufsichtsbehördliche Zuständigkeiten nach §§ 19 bis 25 TTDSG unter analoger Anwendung des Art. 58 Abs. 1 bis 5 DS-GVO und verwaltungsbehördliche Zuständigkeiten nach § 28 Abs. 1 Nr. 10 bis 13 TTDSG, § 36 Abs. 1 Nr. 1 OWiG durch Ergänzung des DSAG LSA sowie der ZustVO OWi LSA ausdrücklich zuzuweisen. Betroffen wären damit behördliche Zuständigkeiten und Kompetenzen nicht nur für datenschutzrechtliche Vorschriften des TTDSG, sondern auch für solche zum Schutz der Privatsphäre.

Die Regelungen des TTDSG haben auch in Sachsen-Anhalt erhebliche praktische Bedeutung. Unter den Begriff der Telemedien des TTDSG fallen alle Online-Angebote mit unmittelbarer Bestellmöglichkeit von Waren oder Dienstleistungen, Video-on-Demand-Dienste oder einfache informatorische Webseiten von Unternehmen. Nach Art. 95 DS-GVO sind Regelungen zum Schutz der Privatsphäre vom Datenschutz nach DS-GVO abzugrenzen und vorrangig anzuwenden. Technische Feststellungen zu der Vorfrage, ob z. B. Marketing-Cookies eines Dritten auf einer Webseite eingebunden sind und auf einem Endgerät geladen werden, kann aber nur einheitlich erfolgen. Insofern sollten Sachverhalte mit Bezug zum Schutz der Privatsphäre nach TTDSG und dem Datenschutz nach DS-GVO sinnvollerweise nur durch eine Behörde beaufsichtigt werden. Dies hätte auch den Vorteil, dass eine behördliche Entscheidung auf das TTDSG gestützt werden könnte, wenn es nur mit unverhältnismäßigem technischem Aufwand gelingen könnte, eine datenschutzrechtlich relevante Folgeverarbeitung zum Nachteil einer beschwerdeführenden Person konkret zu beweisen. Wegen der nachteiligen Folgen unzulässigen Trackings für eine Person ist es unabdingbar, unzulässige Praktiken frühzeitig zu erkennen und abzustellen.

Der Landesbeauftragte regt an, ihm aufsichtsbehördliche Zuständigkeiten nach §§ 19 bis 25 TTDSG unter analoger Anwendung des Art. 58 Abs. 1 bis 5 DS-GVO und verwaltungsbehördliche Zuständigkeiten nach § 28 Abs. 1 Nr. 10 bis 13 TTDSG, § 36 Abs. 1 Nr. 1 OWiG durch Ergänzung des DSAG LSA sowie der ZustVO OWi LSA ausdrücklich zuzuweisen.

15.3 EU-Digitalgesetzgebung und Datenschutz

Ziel der EU-Digitalgesetzgebung ist es, die Europäische Union und den europäischen Binnenmarkt auf die digitale Zukunft vorzubereiten. In der europäischen Datenstrategie vom Februar 2020 wurde die Schaffung von Datenräumen in zehn strategischen Bereichen angekündigt. Aus den verschiedenen Datenräumen soll letztlich ein einheitlicher Binnenmarkt für Daten gebildet werden. Die unterschiedlichen Regelwerke müssen in ihrem Zusammenhang untereinander gesehen und angewandt werden. Aus Sicht des Datenschutzes sind Berührungspunkte und Schnittstellen zu analysieren. Hierbei sind Widersprüche zu vermeiden und Unklarheiten auszuräumen.

a) Vor allem der am 23. Juni 2022 in Kraft getretene EU-Data-Governance-Rechtsakt (DGA) soll sektorübergreifend einen Datenaustausch durch Erhöhung der Datenverfügbarkeit und Beseitigung technischer Hindernisse für die Weiterverwendung ermöglichen. Hierzu werden neuartige Datenmittler eingeführt und der Austausch von Daten für altruistische Zwecke gefördert. Die Datennutzung soll mit einem angemessenen Datenschutzniveau einhergehen. Daher ist dort, wo personenbezogene Daten betroffen sind, die DS-GVO vorrangig anwendbar (Art. 1 Abs. 3 DGA). Allerdings werden mit der Weiterverwendung von Daten des öffentlichen Sektors, der Datentreuhand und dem Datenaltruismus materiell-rechtliche Institute eingeführt, die zu Kollisionen mit der DS-GVO führen könnten.

Die Weiterverwendung personenbezogener Daten im Besitz öffentlicher Stellen nach Art. 3 Abs. 1 lit. d DGA kann durch diese öffentlichen Stellen z. B. davon abhängig gemacht werden, dass nach Art. 5 Abs. 3 lit. a i DGA eine Anonymisierung der Daten vorgenommen wurde. Enthält das nationale Recht keine besonderen Schutzvorkehrungen sind die Anordnungen des Art. 5 Abs. 5 DGA anzuwenden, wonach z.B. Reidentifizierungsmaßnahmen verboten werden. Aus diesem Zusammenhang kann abgeleitet werden, dass die öffentlichen Stellen eine Ermächtigungsgrundlage im nationalen Recht benötigen, in der die Rahmenbedingungen der Datenweitergabe geregelt werden.

Die Datenmittler nach Art. 10; 12 DGA ermöglichen den Austausch oder die gemeinsame Nutzung der Daten von Dateninhabern oder betroffenen Personen hin zu Datennutzern. Zu diesem Zweck kann der Datenmittler Daten u. a. aggregieren, anreichern, umwandeln, anpassen, bündeln oder austauschen (Erwägungsgrund 22; Art. 10, 12 DGA). Jeder Verarbeitungsschritt personenbezogener Daten in der Kette erfordert eine datenschutzrechtliche Rechtsgrundlage. Die in Frage kommende Einwilligung begegnet aufgrund der Vielzahl betroffener Personen in großen Datensätzen und aufgrund der Widerruflichkeit praktischen Schwierigkeiten. Diese Probleme korrespondieren mit dem Institut des Datenaltruismusses, der sich in der Regel ebenfalls „auf die Einwilligung der betroffenen Personen im Sinne von Art. 6 Abs. 1 lit. a und Art. 9 Abs. 2 lit. a der Verordnung (EU) 2016/679 [stützt], die den Anforderungen an eine rechtmäßige Einwilligung gemäß den Artikeln 7 und 8 der genannten Verordnung entsprechen sollte“ (Erwägungsgrund 50 DGA). Die Mitgliedstaaten sollen zwar organisatorische und/oder technische Vorkehrungen treffen, mit denen der Datenaltruismus erleichtert würde (Erwägungsgrund 45 DGA). Aufgrund der Widerrufbarkeit der Einwilligung, dem Grundsatz der Speicherbegrenzung und dem Zweckbindungsgrundsatz müssen die Datenspenden an einen konkreten Zweck geknüpft werden, Die personenbezogenen Daten müssen demnach nach einmaliger Verwendung oder nach dem Widerruf der Einwilligung unverzüglich gelöscht werden, was den praktischen Nutzen erheblich einschränkt.

Das berechtigte Interesse dagegen müsste individuell abgewogen und gegenüber der betroffenen Person erläutert werden (Art. 13 DS-GVO). Auch dies stößt bei großen Datensätzen an Grenzen der Praktikabilität. Letztlich scheint nur die frühzeitige Anonymisierung der Daten ein gangbarer Weg der Datenmittlung zu sein.

b) Der Digital Markets Act (DMA), der am 1. November 2022 in Kraft getreten ist, hat das Ziel, die digitale Wirtschaft fairer und wettbewerbsfähiger zu machen. Hierzu werden die großen, marktbeherrschenden digitalen Plattformen, sogenannte Torwächter, reguliert. Bei den Torwächtern handelt es sich unter anderem um Suchmaschinen,

soziale Netzwerke, Betriebssysteme, Webbrowser, Online-Vermittlungsdienste wie z. B. Online-Marktplätze, Video-Sharing-Plattformen, interpersonelle nummernunabhängige Kommunikationsdienste und Cloud-Computing-Dienste. Ihnen wird unter anderem untersagt, eigene Produkte oder Dienste zu bevorzugen oder Suchmaschinenergebnisse zu steuern. Sie müssen gewährleisten, dass zwischen verschiedenen Softwareanwendungen und Diensten gewechselt werden kann. Die Deinstallation vorinstallierter Anwendungen muss möglich sein.

Das Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO wird durch Art. 6 Abs. 9 DMA erweitert, indem die Torwächter den Endnutzern die effektive Übertragbarkeit ihrer Daten ermöglichen müssen, einschließlich der Zur-Verfügung-Stellung kostenloser Instrumente und eines permanenten Echtzeitzuganges. Die Torwächter müssen die Übertragbarkeit anbieten, ohne dass der Endnutzer dies aktiv geltend machen muss. Sie gilt auch außerhalb der DS-GVO Rechtsgrundlagen der Einwilligung und des Vertrages und insbesondere auch für anonyme Daten.

Aus datenschutzrechtlicher Sicht ebenfalls bemerkenswert ist, dass es den Torwächtern nach Art. 5 Abs. 2 DMA untersagt ist, bestimmte Verarbeitungen personenbezogener Daten auf das berechtigte Interesse (Art. 6 Abs. 1 lit. f DS-GVO) zu stützen. Darunter fällt die Nutzung personenbezogener Daten von Drittnutzern zur Online-Werbung und die Zusammenführung oder Weiterverwendung von personenbezogenen Daten aus oder in verschiedenen Diensten.

16 Weitere europäische und internationale Entwicklungen

16.1 Grenzüberschreitende Beschwerden – One-Stop-Shop

Der Landesbeauftragte hat im Berichtszeitraum jeden Eingang zu einer grenzüberschreitenden Verarbeitung auf seine Betroffenheit nach Art. 4 Nr. 22 DS-GVO geprüft. Im Berichtszeitraum betraf dies allein zu sog. grenzüberschreitenden Beschwerden 579 Eingänge, also eine leichte Steigerung ggü. dem Berichtszeitraum 2021 (538 Eingänge). Allein 46 Eingänge betrafen sog. Cookie-Banner Beschwerden. Dazu kommt eine Vielzahl statistisch nicht gesondert erfasster Eingänge anderer Datenschutzaufsichtsbehörden mit grenzüberschreitendem Bezug.

Der Landesbeauftragte hat sich im Berichtszeitraum in 13 grenzüberschreitenden Verfahren als betroffene Aufsichtsbehörde im Internal Market Information System (IMI) gemeldet. Davon beziehen sich 10 Verfahren auf Beschwerden nach Art. 77 DS-GVO und drei Verfahren auf Meldungen von grenzüberschreitenden Datenschutzverletzungen durch andere Datenschutzaufsichtsbehörden. In zwei Fällen sind die Beschwerden beim Landesbeauftragten eingegangen, der diese über das IMI an die für die Hauptniederlassung zuständige Datenschutzaufsichtsbehörde herangetragen hat.

Die grenzüberschreitenden Verfahren sind leider oft sehr langwierig, was von den Betroffenen zu Recht nur schwer nachvollzogen werden kann. Dies liegt einerseits daran, dass bereits im Rahmen der ersten Phase der Ermittlung der für die Hauptniederlassung zuständigen und damit in dem grenzüberschreitenden Verfahren federführenden Aufsichtsbehörde (Lead Supervisory Authority, LSA) oft Monate vergehen können, weil

die vermutete LSA aufgrund eigener Arbeitsüberlastung nicht zeitnah die Federführung übernehmen kann oder die Federführung unter Verweis auf die vermeintliche Erforderlichkeit von Nachermittlungen durch die betroffene Aufsichtsbehörde (Concerned Supervisory Authority, CSA), bei der die Beschwerde eingereicht wurde, an diese „zurückverweist“. Auch die Beschwerdebearbeitung durch die LSA selbst und der im Anschluss erfolgende Abstimmungsprozess mit den CSA bis zur endgültigen Entscheidung nehmen häufig viel Zeit in Anspruch. Im Berichtszeitraum konnte deshalb keine der beim Landesbeauftragten seit Inkrafttreten der DS-GVO eingereichten Beschwerden mit grenzüberschreitendem Bezug abgeschlossen werden.

Zur Vermeidung langwieriger Ermittlungsverfahren versuchen einige Aufsichtsbehörden in Beschwerdefällen, die sich auf die Geltendmachung von Betroffenenrechten beziehen, sog. „Gütliche Einigungen“ zu erzielen, wenn dies nach nationalem Recht möglich ist. Damit lassen sich – je nach Ausgestaltung des nationalen Rechts – viele Verfahren mit vergleichsweise weniger Aufwand für die LSA einer Erledigung zuführen. Diese zulässige Verfahrensweise hat der EDSA auch in einer Leitlinie näher beschrieben. Gleichwohl sieht der Landesbeauftragte diese Verfahren kritisch, wenn erst nach geraumer Zeit, oft nach Ablauf mehrerer Jahre die Beschwerdebearbeitung durch die LSA aufgenommen wird und das Verfahren – freilich in Einklang mit nationalem Recht – bspw. nach unterlassener Rückäußerung durch den Beschwerdeführer im Wege der „gütlichen Einigung“ eingestellt wird. Beschwerdeführer haben oft ein konkretes Problem, für das sie zeitnah eine Lösung suchen. Der Zugang zum gesperrten Konto bei einem Onlineshop oder die Berichtigung einer Eintragung in einem Kundenkonto nach Ablauf mehrerer Jahre bringt den Beschwerdeführern oft nichts mehr. Sie haben sich zwischenzeitlich anderweitig „versorgt“ bzw. das Interesse verloren.

Schließlich haben Mitarbeiter des Landesbeauftragten an einer durch die Zentrale Anlaufstelle (ZASt) angebotenen Grundlagenschulung und an einem Aufbau-Workshop zur Nutzung des IMI teilgenommen. Diese Schulungen sollen zur einheitlichen Auslegung und Anwendung der DS-GVO, hier im Bereich der grenzüberschreitenden Verarbeitungen, beitragen. Die ZASt unterstützt die Datenschutzaufsichtsbehörden des Bundes und der Länder bei ihren Aufgaben, ohne selbst Aufgaben der Datenschutzaufsicht wahrzunehmen. Sie koordiniert die grenzüberschreitende Zusammenarbeit der Datenschutzaufsichtsbehörden des Bundes und der Länder mit den anderen Mitgliedstaaten der Europäischen Union, dem Europäischen Datenschutzausschuss (EDSA) und der Europäischen Kommission.

Der Landesbeauftragte nimmt im Rahmen seiner Betroffenheit nach Art. 4 Nr. 22 DS-GVO an den grenzüberschreitenden Beschwerdeverfahren nach dem One-Stop-Shop teil.

16.2 Internationale Datenschutzkonferenz

Die 44. Internationale Datenschutzkonferenz (Global Privacy Assembly, GPA) fand vom 25. bis 28. Oktober 2022 unter der Gastgeberschaft der Datenschutzbehörde der Türkei (Kişisel Verileri Koruma Kurumu) – erstmals seit der Corona-Pandemie auch wieder als Präsenzveranstaltung – in Istanbul statt.

Das Motto der Konferenz „Rise of Privacy“ („Aufstieg der Privatsphäre“) soll das Hauptthema „A Matter of Balance: Privacy in The Era of Rapid Technological Advancement“

(„Eine Frage des Gleichgewichts: Datenschutz im Zeitalter des raschen technologischen Fortschritts“) ergänzen. Der Mensch braucht von Natur aus Privatsphäre. Daher ist der Schutz der Privatsphäre eine unabdingbare Notwendigkeit in einer sich verändernden Welt. In diesem Zusammenhang gelingt die Lösung der im Hauptthema hervorgehobenen „Frage des Gleichgewichts“ nur unter Beachtung der Bedeutsamkeit der Privatsphäre. In unserem Zeitalter, in dem die Technologie rasch voranschreitet, können verschiedene Probleme bei der Herstellung eines Gleichgewichts zwischen technologischem Nutzen und dem Schutz der Privatsphäre auftreten. Um ein vernünftiges Gleichgewicht herzustellen, sollten Technologien, die auf der Verarbeitung personenbezogener Daten basieren, und der Schutz der Privatsphäre stets zusammen betrachtet werden.

Die Konferenz fasste u. a. folgende Entschließungen:

- zum ständigen Sekretariat der GPA,
- zur Zusammenarbeit zur Bekämpfung unberechtigter Datenzugriffe und Vermeidung diesbezüglicher Schäden für die Betroffenen sowie
- zu Grundsätzen und Vorgaben für Systeme der Gesichtserkennung.

Die zweite Amtszeit des BfDI für den Zeitraum 2022-2024 im Executive Committee (Exekutivkomitee der GPA) wurde bestätigt.

Weiterführende Informationen finden sich auf der Webseite der GPA.[30] Das Angebot steht nur in englischer Sprache zur Verfügung.

16.3 Leitlinien 04/2022 des EDSA zur Berechnung von Geldbußen gemäß der DS-GVO – Version 1.0 für die öffentliche Konsultation

Der EDSA verabschiedete am 12. Mai 2022 die Version 1.0 der Leitlinien zur Berechnung von Geldbußen nach Art. 83 DS-GVO („Guidelines 04/2022 on the calculation of administrative fines under the GDPR“), die in die öffentliche Konsultation gingen. Die Leitlinien wurde am 24. Mai 2023 durch die Version 2.0 ersetzt. Vorausgegangen war eine mehrjährige Vorbereitung und Entwicklung der Leitlinien durch die noch von der Art. 29-Datenschutzgruppe eigens dafür eingerichteten Taskforce Fining Guidelines. Die Leitlinien, mit denen der EDSA seinem Auftrag aus Art. 70 Abs. 1 lit. k DS-GVO nachkommt, soll die Methodik der Aufsichtsbehörden zur Berechnung der Höhe der Bußgelder in der EU sowie dem EWR harmonisieren. Die Leitlinien ergänzen die bereits bestehenden „Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679“ (WP 253), mit denen sich die Aufsichtsbehörden auf die Grundsätze und eine einheitliche Auslegung der Bewertungskriterien nach Art. 83 Abs. 2 DS-GVO verständigt haben. Mit Verabschiedung im EDSA werden die Leitlinien das von der DSK verabschiedete Bußgeldkonzept ablösen.

Die Leitlinie zeigt eine Methodik zur Bußgeldberechnung in fünf Schritten auf. Dabei lässt sie den Aufsichtsbehörden auch noch hinreichende Flexibilität, um eine verhältnismäßige Sanktionierung von Verstößen gegen die DS-GVO zu ermöglichen. Im ersten Schritt ist die Konkurrenz ggf. mehrerer Taten zu bestimmen. Im zweiten Schritt

[30] https://globalprivacyassembly.org/

erfolgt anhand der Schwere der Tat und des Jahresumsatzes des Unternehmens die Festlegung eines Ausgangswertes für die weitere Berechnung der Geldbuße. Im dritten Schritt werden weitere mildernde und erschwerende Umstände berücksichtigt. Im vierten Schritt ist die Geldbuße unter Berücksichtigung des gesetzlichen Höchstbetrages ggf. anzupassen. Im fünften Schritt sind weitere Anpassungen infolge von besonderen Umständen des Einzelfalls möglich, um eine wirksame, abschreckende und verhältnismäßige Geldbuße sicherzustellen.

Zwischenergebnisse der Taskforce Fining Guidelines wurden im AK Sanktionen diskutiert und Vorschläge über die deutschen Vertreter in die Taskforce eingebracht.

17 Technik und Organisation

17.1 Was ist ein Löschkonzept?

Ein Löschkonzept ist eine formale schriftliche Zusammenstellung, die in der Praxis zu implementierende Löschvorgänge theoretisch untermauert. Die DIN-Norm 66398 beschreibt formal den Prozess zur Erstellung eines Löschkonzeptes.[31]

Zunächst müssen dazu alle Verarbeitungsvorgänge, bei denen personenbezogene Daten verarbeitet werden, die einer Löschfrist gem. Art. 17 DS-GVO unterliegen, kategorisch erfasst werden. Dann müssen die einzelnen Datenfelder darunter gelistet werden. Zu jedem Datum muss erfasst werden, welche gesetzliche Aufbewahrungsfrist besteht. Von Vorteil ist dabei die Angabe entsprechender Rechtsgrundlagen. Falls keine gesetzlichen Aufbewahrungsfristen bestehen, muss erfasst werden, zu welchem Zweck die Daten erhoben wurden und wann dieser Zweck erloschen ist, die Daten also nicht mehr erforderlich sind.

Schließlich sollte für jede Datenkategorie beschrieben werden, ob dafür eine automatische, zyklische oder manuell ausgelöste Löschung vorgesehen ist, ob diese ausschließlich digital stattfindet oder auch Akten und Datenträger existieren, die vernichtet werden müssen. Die Angabe einer zuständigen Abteilung bzw. Person erhöht die Nachverfolgbarkeit.

Neben dem Kurzpapier 11 „Recht auf Löschung“[32], welches von der Datenschutzkonferenz veröffentlicht wurde, bieten zahlreiche öffentlich zugängliche Internetseiten eine praktische Anleitung zur Erstellung von Löschkonzepten.[33]

[31] https://www.secorvo.de/publikationen/din-leitlinie-loeschkonzept-hammer-schuler-2012.pdf

[32] https://datenschutzkonferenz-online.de/media/kp/dsk_kpnr_11.pdf

[33] z. B. https://www.datenschutz-praxis.de/fachartikel/schritt-fuer-schritt-zum-loesch-und-sperrkonzept, https://dsgvo-vorlagen.de/muster-fuer-ein-loeschkonzept-nach-dsgvo-in-excel, https://www.datenschutzbeauftragter-info.de/din-norm-66398-die-entwicklung-eines-loeschkonzepts

17.2 Besonderes elektronisches Behördenpostfach

Seit dem 1. Januar 2022 ist die Nutzung des elektronischen Rechtsverkehrs (eRV) für Behörden und juristische Personen des öffentlichen Rechts verpflichtend.[34] Über sogenannte „sichere Übermittlungswege“ ist es möglich, in rechtssicherer Art und Weise elektronische Dokumente zu verschicken. Für Behörden wird die Nutzung des besonderen elektronischen Behördenpostfachs empfohlen, welches einfach und kostenfrei genutzt werden kann.

Für den Landesbeauftragten war es schon immer ein besonderes Anliegen, Bürgerinnen und Bürgern, aber auch Unternehmen und anderen Behörden eine sichere und vertrauliche Kommunikationsmöglichkeit anzubieten. Dazu konnte etwa Verschlüsselung mittels X.509-Zertifikaten oder PGP genutzt werden. Die erforderlichen Schlüssel sind auf der Website des Landesbeauftragten verfügbar. Auch über anonym und verschlüsselt nutzbare Webformulare ist es möglich, die Behörde zu erreichen. Das besondere elektronische Behördenpostfach ist ein weiterer Weg und eröffnet einen sicheren elektronischen Übertragungsweg für elektronische Dokumente. Bisher blieben Bürgerinnen und Bürger von diesem Übermittlungsweg ausgenommen (nur kurze Zeit war die Nutzung kostenfrei möglich, wurde dann aber leider unterbunden).

Im Berichtszeitraum wurde die EGVP-Infrastruktur[35], das Elektronische Gerichts- und Verwaltungspostfach, um ein weiteres besonderes elektronisches Postfach – diesmal für Bürgerinnen und Bürger sowie Organisationen – bereichert. Das elektronische Bürger- und Organisationenpostfach (eBO) ist ein weiterer sicherer Übermittlungsweg, der den schriftformersetzenden Versand und die Zustellung elektronischer Dokumente ermöglicht (§ 130a Abs. 4 Nr. 4 ZPO). Er dient auch der sicheren Übermittlung für nicht formbedürftige Nachrichten im elektronischen Rechtsverkehr. Postfachinhaber werden überprüft und wie bei den anderen Postfächern auch im SAFE-Verzeichnisdienst veröffentlicht. Die Überprüfung erfolgt anhand eines elektronischen Identitätsnachweises, mit Hilfe eines qualifizierten elektronischen Siegels oder in einem manuellen Identifizierungsverfahren mittels in öffentlich beglaubigter Form abgegebener Erklärung (Notar).

Für die Nutzung des eBO wird eine kostenpflichtige Software benötigt. Die ehemals kostenfreie Bereitstellung einer Software ist entfallen. Nutzer werden im Adressbuch des eRV veröffentlicht, aber die Daten können nur von der Justiz, Behörden, Rechtsanwältinnen und Rechtsanwälten, Notarinnen und Notaren sowie Steuerberaterinnen und Steuerberatern eingesehen werden. Auch Inhaber anderer besonderer elektronischer Postfächer (beA, beBPo, beN) können eine Kommunikation aufnehmen. Andere eBO-Postfachinhaberinnen und -inhaber haben darauf keinen Zugriff. Damit wird der Nutzen des Postfachs auf den Justiz-Kontext beschränkt.

17.3 Akkreditierung und Zertifizierung

Im Jahr 2022 konnten in Deutschland und Europa Fortschritte bei der Genehmigung von Zertifizierungskriterien und Akkreditierungsverfahren nach der Datenschutz-Grundverordnung (DS-GVO) erzielt werden. Erste erfolgreiche Akkreditierungen von

---

[34] § 130d ZPO, § 753 Abs. 5 ZPO, § 14b FamFG, § 46g ArbGG, § 65d SGG, § 52d FGO, § 55d VerwGO

[35] https://www.egvp.de/

Zertifizierungsstellen sind absehbar und damit einhergehend werden bereits im nächsten Jahr auch erste Datenschutzzertifizierungen für Produkte und Dienstleistungen erwartet. Bislang liegen in Sachsen-Anhalt noch keine Akkreditierungsanträge vor.

Im Berichtszeitraum wurden im AK Zertifizierung und in dessen UAK Prüfkriterien die Entwicklungen aufmerksam verfolgt und aktiv mitgestaltet. Im AK Zertifizierung treffen sich regelmäßig Vertreter der Datenschutzaufsichtsbehörden und der Deutsche Akkreditierungsstelle GmbH (DAkkS) zum fachlichen Austausch zu aktuellen zertifizierungsrelevanten Themen. Der Austausch erfolgte virtuell mittels Videokonferenzen.

Die Akkreditierung von Zertifizierungsstellen erfordert es, dass diese ein Zertifizierungsprogramm erstellen, das die Umsetzung der datenschutzrechtlichen Anforderungen beschreibt. Diese Programme und die darin enthaltenen Zertifizierungskriterien werden dann von der DAkkS zusammen mit der jeweiligen Aufsichtsbehörde geprüft. Anträge werden zunächst bei der DAkkS gestellt. Diese berät und sorgt für die formale Vollständigkeit, sie nimmt auch eigene Prüfungen vor. Bei der Prüfung der DS-GVO-Kriterien greift die DAkkS jedoch auf Mitarbeitende aus den Aufsichtsbehörden zurück. Dazu werden die Anträge an die jeweils zuständige Aufsichtsbehörde weitergeleitet und dort fachlich geprüft. Zum Schluss erfolgt gegebenenfalls in Abstimmung mit dem Europäischen Datenschutzausschuss die Genehmigung der Kriterien. Erste genehmigte Kriterienkataloge existieren mittlerweile. Nach der Genehmigung des Kriterienkatalogs unterstützen die Fachbegutachtenden der jeweiligen Aufsichtsbehörde die DAkkS auch bei der die Akkreditierung.

Im europäischen Kontext fanden ebenfalls wichtige Entwicklungen statt. Die vielfältigen Meinungen auf der EU-Ebene wurden über den deutschen Vertreter in der „Expert Subgroup“ für Zertifizierung und Akkreditierung in den AK Zertifizierung getragen und umgekehrt vermittelte der AK ein einheitliches Bild der Positionen der unabhängigen deutschen Aufsichtsbehörden in die EU. Diskussionen rund um etwa erste Genehmigungsprozesse für Zertifizierungskriterien auf europäischer Ebene zeigten, dass die Ansprüche und Erwartungen an diese sehr verschieden sein konnten. Die Kooperationsvereinbarung war eine große Hilfe bei der Abstimmung der deutschen Positionen.

Im UAK Prüfkriterien wurde das bereits im Jahr 2021 durch die DSK verabschiedete Dokument „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme – Datenschutzrechtliche Prüfkriterien, Prüfsystematik und Prüfmethoden zur Anpassung und Anwendung der technischen Norm DIN EN ISO/IEC 17067 (Programmtyp 6)“ zur einheitlichen Bewertung von Prüfkriterienkatalogen fortgeschrieben. Die bewährte Struktur wurde beibehalten, neue Themen, etwa zu gemeinsamen Verantwortlichkeiten (Art. 26 DS-GVO) und Anforderungen an die Datenübermittlung in Drittstaaten (Art. 46 DS-GVO), wurden ergänzt. Erste Erfahrungen aus der Praxis wurden eingearbeitet.

Neben der einheitlicheren Bewertung von Prüfkriterien durch die deutschen Datenschutzaufsichtsbehörden dient das Papier auch als Leitfaden für Zertifizierungsprogramme künftiger Zertifizierungsstellen. Zudem soll es auch zur Schaffung einer soliden und europaweit anerkannten Grundlage für die Zertifizierung von Datenschutzprogrammen beitragen. Daher ist diese Version des Katalogs auch in englischer Sprache verfügbar.

17.4 Informationssicherheit (AG InfoSic Land)

Die Leitlinie zur Informationssicherheit (LISL LSA) in der unmittelbaren Landesverwaltung Sachsen-Anhalt bestimmt bei der Nutzung von Informationstechnik (IT), dass ein erforderliches und angemessenes Sicherheitsniveau herzustellen und aufrecht zu erhalten ist sowie verbleibende Restrisiken zu minimieren sind. Sie verlangt den obligatorischen Betrieb eines Informationssicherheitsmanagementsystems (ISMS) gemäß IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) als kontinuierlichen Prozess. Das IT-Grundschutzkompendium gibt die hier zu erfüllenden technischen und organisatorischen Maßnahmen zur Auswahl vor. Der dabei einzuhaltende Mindeststandard wird in den IT-Sicherheitsrichtlinien (ISRL) des Landes festgehalten. Es wurde weiter an den ISRL gearbeitet.

In der UAG „Awareness“ wurde anhand des BSI-Bausteins ORP.3 „Sensibilisierung und Schulung zur Informationssicherheit“ ein Schulungs-, Sensibilisierungs- und Trainingskonzept erstellt. Dieses bildet den Rahmen für die Planung, Durchführung und Strukturierung von Schulungs- und Sensibilisierungsmaßnahmen im Land. Ziel ist die Bereitstellung einer Awareness-Plattform für die unmittelbare Landesverwaltung, die es erlaubt, kontinuierliche Informationssicherheits-Awareness-Kampagnen durchzuführen und auszuwerten. Gedacht ist dabei etwa an Phishing-Simulationen und interaktive bzw. multimediale Nutzersensibilisierungen.

In der UAG „BITS“ wurde in vielen Treffen weiter an den Inhalten für das an die Bedürfnisse des Landes angepasste Behörden-IT-Sicherheitstraining gearbeitet. Es wurde eine an das Land angepasste Version erstellt und von den Stakeholdern auch praktisch erprobt. Neben der Anpassung bestehenden Schulungsmaterials wurden auch neue Lektionen erstellt, etwa zu den Themen Videokonferenzen und Home-Office. Innerhalb der Landesverwaltung musste nun eine technische Plattform für die Nutzung durch die Beschäftigten eingerichtet werden. Die technischen Anforderungen wurden an das MID als Arbeitsauftrag weitergegeben.

Im XVII. Tätigkeitsbericht wurde über das Inkrafttreten der Leitlinie zur Informationssicherheit der unmittelbaren Landesverwaltung Sachsen-Anhalt (LISL LSA, Informationssicherheitsleitlinie) des Landes und die damit einhergehende beginnende Erstellung belastbarer IT-Sicherheitsrichtlinien (ISRL) berichtet. Die ersten ISRL, die Passwort- und die Telearbeits-RL, befanden sich bereits auf der Zielgeraden und wurden nach Einarbeitung offener Rückmeldungen zügig vollendet. Die ISRL zum „Umgang mit Sicherheitsvorfällen“ wurde finalisiert und Umsetzungshinweise zu den Anforderungen ausgearbeitet. Weitere Arbeiten erfolgten – teils in UAGs – an ISRL und Prozessbeschreibungen betreffend Korrektur- und Vorbeugemaßnahmen, Organisation und Personal, Berichtswesen, Risikomanagement und dem Landesweiten Sicherheitsprozess.

Nachdem im letzten Jahr die ISRL „Dokumentenmanagement“, „Passwortrichtlinie" und „Telearbeit“ inhaltlich abgeschlossen und von den ISB der obersten Landesbehörden und dem CISO freigegeben wurden, erfolgte nun auch zum Ende des Jahres die Freigabe durch die Hausleitungen der obersten Landesbehörden und dem CIO. Die Dokumente wurden im Extranet im CISO-Bereich eingestellt.

Gem. Abschnitt 4 LISL LSA tragen die Leitungen der obersten Landesbehörden die Verantwortung für die Informationssicherheit in ihren Zuständigkeitsbereichen. Die

durch Dataport bereitgestellten Sicherheitskonzepte waren, abgesehen vom zertifizierten Rechenzentrumsbetrieb, unzureichend und zu einer fundierten Information der Hausleitungen bezüglich des aktuellen Stands der IT-Sicherheit ungeeignet. Die AG InfoSic (Land) regte eine Überprüfung essentieller Querschnittsdienste bzw. zentral beauftragter Verfahren in Form einer IS-Kurzrevision an. Ziel ist die Gewinnung von Kennzahlen, anhand derer den Hausleitungen in angemessener Form ein Lagebild vermittelt werden kann, damit diese Risiken richtig einschätzen und gegebenenfalls übernehmen können.

Die UAG „Kommunen“ traf sich virtuell per Videokonferenz. Kommunen sollen im Bereich der Informationssicherheit enger an das ISMS Land angebunden werden. Das betrifft insbesondere den Informationsaustausch von Warn- und Informationsmeldungen zu Sicherheitslücken sowie bei Sicherheitsvorfällen. Dazu war eine Meldung von Ansprechpartnern in den Kommunen und deren Einrichtung auf dem Kundenportal des CERT Nord notwendig, damit die dort erstellten Lageberichte und Warnhinweise einen Empfänger finden. Aufgaben des CERT Nord sind der Informationsdienst, ein Warndienst, allgemeine Beratung und die Behandlung von Sicherheitsvorfällen. Dafür steht es in engem Kontakt mit anderen CERTs und dem BSI. Das MID unterstützte das CERT Nord bei der Aufnahme in die E-Mail-Verteiler und die Verpflichtungen der Ansprechpartner nach dem Traffic Light Protocol (TLP). Eine TLP-Verpflichtung ist eine Vereinbarung, die den sicheren Austausch von sensiblen Informationen regelt. Sie verwendet Farbcodes, um den Grad der Vertraulichkeit und die Bedingungen für die Weitergabe eines Dokumentes zu kennzeichnen.

Im Jahr 2021 war die Unterzeichnung einer Kooperationsvereinbarung zwischen dem Land Sachsen-Anhalt und dem BSI geplant. Diese konnte bisher noch nicht erfolgen, da zuvor die Konkretisierung der Handlungsfelder erforderlich ist. Es musste ein zeitlicher Handlungsrahmen festgelegt und ein Arbeitsprogramm für beide Partner entwickelt werden. Die konkreten Kooperationsfelder wurden unter den AG InfoSic-Mitgliedern abgestimmt, um Arbeitsschwerpunkte zu ermitteln. Ziel war es, die wichtigsten Punkte für die nächsten 2 Jahre zu planen und ein konkretes Vorhaben zu entwickeln.

Das MID hatte mit Unterstützung durch das MI die Federführung bei der Erstellung eines Informationssicherheitsgesetzes für das Land Sachsen-Anhalt. Das IT-Sicherheitsgesetz soll die Sicherheit in einem vernetzten Raum wie dem Internet oder dem Landesnetz gewährleisten. Der erste Entwurf sollte bis Ende April 2022 erstellt werden. Im Rahmen der Erstellung wurde der Landesbeauftragte im Juli um eine Prüfung des Abschnitts „Maßnahmen zur Sicherstellung der Informationssicherheit“ ersucht. Gegen den vorgelegten Auszug aus dem Gesetzentwurf bestanden im Grunde keine Bedenken. Es wurden einzelne Defizite erkannt und es konnten sachdienliche Hinweise gegeben werden.

Der gesamte Entwurf des IT-Sicherheitsgesetzes lag leider nicht vor. Das war insofern unglücklich, da ausgehend von den Inhalten der IT-Sicherheitsgesetze anderer Bundesländer angenommen werden konnte, dass weitere Passagen, ggf. auch das Gesetz als Ganzes, datenschutzrelevant sein könnten und bewertet werden sollten.

Das Gesetz wurde mangels Ressourcen und wohl auch entsprechender juristischer Unterstützung bei der Bearbeitung im Berichtszeitraum nicht mehr vollendet. Es wurde jedoch kontinuierlich über Fortschritte in der AG InfoSic (Land) berichtet.

Im Dezember 2021 wurde eine kritische Sicherheitslücke in log4j gefunden. Log4j ist ein Framework für das Logging von Anwendungsmeldungen in Java. Die Lücke war gefährlich, da sie in einer weit verbreiteten Java-Bibliothek vorhanden war und es Angreifern ermöglichte, Schadcode auf betroffenen Systemen auszuführen. Die Schließung der Sicherheitslücke erfolgte rasch, die Umsetzung durch die Softwarehersteller, die log4j integriert hatten, zog sich teilweise über Monate hin. Auch die AG InfoSic (Land) beschäftigte sich mit der Prüfung von Soft- und Hardware und der Ermittlung der eingesetzten Versionen von log4j.

Das führte direkt zum Thema Software Bill of Materials (SBOM). Die SBOM ist eine Liste all jener Komponenten einer Software, die bei der Erstellung der Software als Teil dieser eingebaut wurden. Wünschenswert wäre es, wenn alle eingesetzte Software im Land bekannt und dazu jeweils eine aktuelle SBOM verfügbar wäre. So würde jede Schwachstelle in einer Komponente, die nicht behoben wird, für Kunden und Nutzer sichtbar. Insbesondere bei neuen Produkten sollte eine Information zu allen eingesetzten Komponenten systematisch eingefordert werden. Eine Erstellung einer SBOM durch Dataport wurde bisher aus Kapazitätsgründen abgelehnt. Eine entsprechende Zusammenstellung wird jedoch, insbesondere als Grundlage für Risikoanalysen, für notwendig erachtet. Der Landesbeauftragte befürwortet, dass bei allen Beschaffungen von Software wie Fachanwendungen bereits in den Verträgen entsprechende Bereitstellungen in einem standardisierten Format vorgesehen werden. Mehr noch, es wird angeregt, Hersteller zu bestenfalls kontinuierlichen (CI/CD-basiert), in jedem Fall jedoch bei Sicherheitsvorfällen bzw. auf Nachfrage, zeitnahen Bereitstellungen von aktualisierter Software zu verpflichten.

Im Nachgang zum Sicherheitsvorfall im Landkreis Anhalt-Bitterfeld, wurde dort ein Expertenbeirat ins Leben gerufen. Vorrangig sollen Möglichkeiten zur Schaffung von Fähigkeiten für ein Incident Response bei einem akutem Sicherheitsvorfall identifiziert und bewertet werden. Die Ergebnisse sollen anderen Bedarfsträgern zur Verfügung gestellt werden.

Aufgrund der hohen Bedrohungslage in den Kommunen bot das BSI den Ländern eine „Roadshow Kommunen“ in Form eines Webinars an. Das BSI wollte die Organisation übernehmen, die Länder sollten sich aktiv etwa mit eigenen Vorträgen beteiligen. Sachsen-Anhalt plante, das Angebot anzunehmen und etwa erste Schritte auf dem Weg zum IT-Grundschutz in Form eines „Blaupausen-Fahrplans“ (ISB benennen, Rollen- und Rechte festlegen, …) einzubringen. In einer gemeinsamen Veranstaltung des BSI und dem Ministerium für Infrastruktur und Digitales des Landes Sachsen-Anhalt wurde noch im August 2022 mit Blick auf die aktuelle Bedrohungslage für die Informationssicherheit sensibilisiert und die unterschiedlichen Unterstützungsangebote vorgestellt.

18 Telekommunikation und Medien

18.1 Google Fonts

Den Landesbeauftragten für den Datenschutz erreichten wiederholt Anfragen von Webseitenbetreibern, die aufgrund der Einbindung von Google Fonts Abmahnschreiben von Anwälten erhalten hatten.

Hintergrund ist ein Urteil des Landgerichts München vom 20. Januar 2022 (Az.: 3 O 17493/20), wonach eine Verletzung des Rechts auf informationelle Selbstbestimmung und des allgemeinen Persönlichkeitsrechts vorliegt, wenn beim Aufruf einer Webseite die dynamische IP-Adresse des Webseitennutzers automatisiert und ohne Zustimmung an Google weitergeleitet wird. Der Einsatz von externen Schriftartendiensten könne nicht auf Art. 6 Abs. 1 Satz 1 lit. f DS-GVO (berechtigtes Interesse) gestützt werden, da der Einsatz der Schriftarten auch möglich sei, ohne dass eine Verbindung zu externen Servern hergestellt werde und eine Übertragung der IP-Adresse des Webseitennutzers erfolge. Mit diesem Urteil wurde dem Webseitennutzer ein Schadenersatz in Höhe von 100 € zugesprochen.

Da der Landesbeauftragte nur zu datenschutzrechtlichen Fragen Stellung nehmen kann, war eine Rechtsberatung bezüglich der Frage, wie mit solchen Abmahnschreiben umzugehen ist, nicht möglich. Hier konnte nur auf die eigene Recherche oder auf die Beratung durch einen Rechtsanwalt verwiesen werden. Allerdings hat der Landesbeauftragte hinsichtlich der Einbindung externer Schriftarten folgende Hinweise gegeben:

Um externe Schriftarten datenschutzkonform in Webseiten einzubinden, sollten Webseitenbetreiber die Schriften nicht direkt vom Server des jeweiligen Anbieters laden, sondern diese zunächst herunterladen und lokal auf dem eigenen Server speichern. Von dort können die Schriften datenschutzkonform in die Webseite eingebunden werden, ohne dass eine Verbindung zu externen Servern aufgebaut wird.

Content-Management-Systeme wie z. B. WordPress, die häufig zur Erstellung von Webseiten verwendet werden, binden oft standardmäßig ohne Wissen der Webseitenbetreiber externe Schriftarten ein. Um sicherzugehen, dass auf ihren Webseiten keine externen Schriftarten eingebunden wurden, sollten Webseitenbetreiber die Seiten z. B. mit Hilfe der in allen Webbrowsern enthaltenen Entwicklerwerkzeuge überprüfen.

Der Landesbeauftragte hat außerdem davon abgeraten, für die Einbindung der Schriftarten von externen Servern eine Einwilligung der Webseitenbesucher gem. Art. 6 Abs. 1 lit. a DS-GVO bzw. Art. 49 Abs. 1 Satz 1 lit. a DS-GVO einzuholen. Für eine wirksame Einwilligung müssten vor der Datenerhebung Informationen gem. Art. 12, 13 DS-GVO zur Verfügung stehen, um zu wissen, in welchem Umfang eine Einwilligung erteilt wird. Diese Informationen müssten auch die Risiken im Zuge der Drittlandübermittlung umfassen. Überdies kann in eine Übermittlung in ein unsicheres Drittland gem. Art. 49 Abs. 1 Satz 1 lit. a DS-GVO nur für gelegentliche Übermittlungen eingewilligt werden. Sofern auf einer Webseite Schriftarten von externen Servern geladen und eingebunden werden, sodass bei jedem Aufruf der Webseite die IP-Adresse der Webseitenbesucher an diese Server übermittelt wird, ist von einer systematischen, sich wiederholenden Datenverarbeitung auszugehen. Somit kann die Einwilligung nicht auf Art. 49 Abs. 1 Satz 1 lit. a DS-GVO gestützt werden.

Der Landesbeauftragte für den Datenschutz empfiehlt Webseitenbetreibern die lokale Einbindung von externen Schriftarten wie z. B. Google Fonts.

18.2 Kurzgutachten zum Betrieb von Facebook-Fanpages

Der Europäische Gerichtshof hatte bereits in seinem Urteil vom 5. Juni 2018 (Aktenzeichen C-210/16) festgestellt, dass Betreiber einer Facebook-Fanpage und das Unternehmen Facebook (jetzt: Meta Platforms Inc.) gemeinsame Verantwortliche gemäß Art. 26 DS-GVO sind.

Die sich daraus ergebenden Pflichten wie z. B. die Einhaltung der Grundsätze aus Art. 5 Abs.1 DS-GVO, die Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO und die Informationspflichten aus Art. 13 DS-GVO können von den Fanpage-Betreibern jedoch kaum erfüllt werden, da es hinsichtlich der Datenverarbeitung bei Facebook an der erforderlichen Transparenz fehlt.

Zu diesem Ergebnis kommt auch eine Arbeitsgruppe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), die ein Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages erstellt hat. Demnach ist die Datenverarbeitung, die beim Besuch einer Facebook-Fanpage vorgenommen wird, weder mit der DS-GVO noch mit dem Telekommunikation-Telemedien-Datenschutz-Gesetz vereinbar, weshalb ein datenschutzkonformer Betrieb zurzeit nicht möglich ist.

In ihrem Beschluss vom 23. März 2022 hat die DSK das Kurzgutachten zur Kenntnis genommen und der Bewertung zugestimmt.[36] Weiterhin wurde festgelegt, die obersten Landes- bzw. Bundesbehörden über den Inhalt des Kurzgutachtens zu informieren und darauf hinzuwirken, dass von Landes- bzw. Bundesbehörden betriebene Facebook-Fanpages deaktiviert werden, sofern die Verantwortlichen die datenschutzrechtliche Konformität nicht nachweisen können.

Ziel dieses Vorgehens ist aber kein generelles Verbot von Facebook-Fanpages, sondern der rechtskonforme Betrieb, der jedoch nur mit Änderungen bei der Datenverarbeitung durch Facebook und dessen Mutterkonzern Meta gewährleistet werden könnte.

18.3 Häufige Mängel beim Einsatz von Cookies und Tracking-Mechanismen

Auf vielen Internetseiten werden regelmäßig Cookies gesetzt und ausführbarer Skriptcode von Drittanbietern eingebunden. Beide Technologien können sowohl dazu eingesetzt werden, eine Internetseite datenschutzkonform mit zusätzlichen Funktionalitäten aufzuwerten als auch die Aktivitäten der Seitenbesucher zu verfolgen und seitenübergreifende Profile zu erstellen (Tracking).

Wenn das Anlegen und Auslesen von Cookies für die reine Bereitstellung einer Internetseite nicht unbedingt erforderlich ist, ist gem. § 25 TTDSG (ab 2024 TDDDG) für diese Art der Datenerhebung eine Einwilligung einzuholen. Bei der Datenerhebung durch ausführbaren Skriptcode (z. B. zur Reichweitenanalyse) bzw. Einbindung anderer Inhalte (z. B. Schriftarten, Captcha usw.) wäre Art. 6 Abs. 1 lit. a, b oder f DS-GVO gemäß der Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien vom

[36] https://www.datenschutzkonferenz-online.de/media/dskb/DSK_Beschluss_Facebook_Fanpages.pdf

Dezember 2021[37] anzuwenden und das Urteil des LG München vom 20. Januar 2022 (Az. O 17493/20) zu beachten.

Möglicherweise kann die Anwendung von Skriptcode, der nicht explizit der Profilbildung dient, auch als berechtigtes Interesse des Webseitenbetreibers eingeordnet und im Rahmen der Abwägung ohne Einwilligung zulässig befunden werden. Dies wäre z. B. denkbar bei der Einbindung eines Captcha-Mechanismus zur Erhöhung der Sicherheit einer Webseite ohne Datenübermittlung in unsichere Drittstaaten oder bei der Einbindung eines anonymisierten Statistikwerkzeuges auf der eigenen Webseite. Umgekehrt würde bei der Einbindung von Trackingmechanismen Art. 6 Abs. 1 lit. a DS-GVO anzuwenden sein und eine Einwilligung wäre Voraussetzung und Rechtsgrundlage der Datenverarbeitung (siehe Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 12. Mai 2020 „Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich“[38]).

Zu beachten ist ebenfalls, dass sich die vorgenannte Rechtmäßigkeitsbetrachtung lediglich auf die Verarbeitung der Daten innerhalb des Europäischen Wirtschaftsraums bezieht. Es muss daher auch geprüft werden, ob es bei einer Datenverarbeitung zu einer Übermittlung personenbezogener Daten in Drittländer kommt. Eine Übermittlung von personenbezogenen Daten in Drittländer ohne durch die EU-Kommission anerkanntes Datenschutzniveau (z. B. EU-U.S. Data Privacy Framework[39]) darf nur vorbehaltlich geeigneter Garantien, wie z. B. Standarddatenschutzklauseln, oder bei Vorliegen eines Ausnahmetatbestandes für bestimmte Fälle gemäß Art. 49 DS-GVO erfolgen (siehe Urteil des EuGH vom 16. Juli 2020 Az. C-311/18).

Um bei einem Besuch einer Internetseite eine wirksame Einwilligung einzuholen muss der Besucher vorab zum einen umfassend informiert werden und zum anderen aktiv seine Einwilligung, z. B. durch Klicken auf einen Button „Ich bin einverstanden“, bekunden. Eine rechtmäßige Einwilligung kann auf einer Internetseite durch einen Consent Manager umgesetzt werden. Reine Cookie-Banner, die nur allgemein über das Anlegen von Cookies informieren und mit nur einem Knopf „Bestätigen“ oder „OK“ ausgeblendet werden können, erfüllen nicht die Anforderungen an eine Einwilligung gem. Art. 7 DS-GVO.

Häufig werden auf Internetseiten Consent Manager eingeblendet und obwohl noch gar keine Einwilligung durch den Besucher erteilt wurde, werden bereits Skripte von Drittanbietern wie Google nachgeladen und Cookies durch diese gesetzt. Beides ist unrechtmäßig. Internetseitenbetreiber haben darauf zu achten, das Einbinden einwilligungspflichtiger Cookies und Skripte erst dann aktiv auszuführen, nachdem die Besucher im Consent Manager eingewilligt haben. Ohne Einwilligung sind beim ersten Laden der Internetseite nur solche Cookies erlaubt, die zwingend zum grundlegenden Betrieb der Internetseiten erforderlich sind, so z. B. Sitzungs-Cookies oder Warenkorb-

[37] https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf

[38] https://www.datenschutzkonferenz-online.de/media/dskb/20200526_beschluss_hinweise_zum_einsatz_von_google_analytics.pdf

[39] https://www.dataprivacyframework.gov/

Cookies. Skriptcode Dritter, etwa für Menüfunktionalitäten, sollte lokal gehostet angeboten werden.

Schließlich gilt es ebenfalls zu beachten, dass es durch das Einbinden externer Inhalte ermöglicht wird, dass die Anbieter der Inhalte während des Abrufes durch den Browser der Seitenbesucher deren IP-Adresse, Geolokation, Ursprungswebseite und Zeitstempel erheben und verarbeiten können. Also bereits durch das reine Einbinden von Inhalten Dritter Daten des Besuchers an diese Dritten übermittelt werden. Auch dies bedarf einer Einwilligung, die gemeinsam mit der für Cookies erhoben werden kann.

Wenn Internetseiten mittels Cookies und ausführbarem Skriptcode die Aktivitäten der Seitenbesucher verfolgen sollen oder personenbezogene Daten der Besucher an Dritte übermittelt werden, muss eine Einwilligung der Besucher per Consent Manager eingeholt werden, noch bevor die Cookies und Skripte geladen werden.

19 Öffentliche Sicherheit

19.1 Sichere Videokonferenzen bei der Polizei Sachsen-Anhalts

Mit Schreiben des Ministeriums für Inneres und Sport (MI) im Juli 2022 wurde das Programm „Sachsen-Anhalt digital 2030“ angekündigt. Innerhalb des Teilprojektes „Smart Mobile” begleitete der Landesbeauftragte den Aufbau eines Verschlusssachekonformen Videokonferenzsystems mit Schutzbedarf HOCH zur internen Verwendung im Netz der Polizei des Landes Sachsen-Anhalt. Das Videokonferenzsystem soll zunächst den Lage- und Führungszentren des MI und der Polizeiinspektionen zur Verfügung stehen. Es soll auch die Teilnahme von mobilen Endgeräten über VPN-Tunnel ermöglichen. In der letzten Ausbaustufe sollen auch die Fachhochschule der Polizei und das Landeskriminalamt an das System angebunden werden.

Der Zugriff auf die Plattform soll über die Räume der fünf Lage- und Führungszentren als virtuelle Erweiterung der Leitstellen sowie von dienstlichen Endgeräten und Smartphones aus dem Polizeinetz des Landes erfolgen. Für bundesweite Videokonferenzen soll eine Kopplung an das Videokonferenzsystem der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) über das Netz des Bundes implementiert werden. Dazu wurde ein eigener Netzübergang vom Polizeinetz zum Netz des Bundes beantragt.

Die Realisierung erfolgt durch die Produkte „Meeting Server“ und „WebEx“ der Firma Cisco Systems, Inc., welche autark auf einer eigenen IT-Infrastruktur der Polizei betrieben werden. Die für den Betrieb erforderliche Lizenzvalidierung wird ebenfalls auf Servern der Polizei durchgeführt, so dass keine Verbindung ins Internet erforderlich ist. Die Wartung des Systems wird durch die österreichische Firma Eurofunk, die auch den Digitalfunk der Polizei in Sachsen-Anhalt realisiert hat, erfolgen. Ein Datenabfluss zu Cisco Systems, Inc. ist daher nicht zu erwarten. Seitens der Aufsichtsbehörde wurde darauf hingewiesen, dass auch Wartungsdienstleister mit administrativem Zugang per Auftragsverarbeitung gem. Art. 28 DS-GVO eingebunden werden müssen.

Die Errichtung der Server ist bereits erfolgt und die Ausstattung der Räume mit Endgeräten und Peripherie soll bis Herbst 2022 abgeschlossen sein. Die Installation wird ebenfalls von Eurofunk durchgeführt. Die Polizeiinspektion Zentrale Dienste (ehem. technisches Polizeiamt) fungiert hierbei als interner Dienstleister der Polizei Sachsen-Anhalts.

19.2 Ermittlungen gegen Unbeteiligte

Der Landesbeauftragte hat im Berichtszeitraum die Beschwerde eines Rechtsanwaltes zurückgewiesen, der beanstandete, dass die Bußgeldstelle der Polizei Lichtbildkopien eines von ihm vertretenen Kleinkindes von der Meldebehörde abgefordert habe, obwohl das Kind lediglich auf dem Beifahrersitz eines geblitzten Autos saß und damit als unbeteiligt zu gelten habe. Es sei unzulässig, Ermittlungen gegen Personen anzustrengen, gegen die sich kein Ermittlungsverfahren richte. Aus der Identität des Beifahrers könne auch nicht auf die Identität des Fahrers geschlossen werden. Daher habe auch das Amtsgericht das Verfahren eingestellt.

Die Sachverhaltsermittlung ergab, dass der Halter des geblitzten Pkw der Vater des Kindes war. Der Fahrer war auf dem Blitzerfoto nicht vollständig erfasst. Die mit der Fahrerermittlung beauftragte Polizeidienststelle ermittelte zunächst gegen den Halter, der ausweislich des Melderegisters Vater eines Kindes war. Daraufhin hat die Polizei die Lichtbildkopie des Kinderreisepasses von der zuständigen Meldebehörde abgefordert.

Nach § 4 DSUG LSA in Verbindung mit § 46 Abs. 2 OWiG und §§ 161; 163 b Abs. 2 StPO sind erforderliche Maßnahmen der Identitätsfeststellung auch gegenüber Nichtverdächtigten zulässig, soweit sie zur Aufklärung einer Ordnungswidrigkeit geboten sind. Ein Aufklärungsinteresse besteht, wenn und solange tatsächliche Anhaltspunkte dafür vorliegen, dass der Nichtverdächtigte, im Rahmen des Verfahrens als Zeuge oder Augenscheinsobjekt zur Erforschung des Sachverhaltes beitragen kann.

Der Beifahrer muss gemäß §§ 46 OWiG, 100 h Abs. 3 StPO hinnehmen, dass von ihm im Rahmen der Geschwindigkeitsüberwachung, ein Lichtbild angefertigt wird, obwohl er eine unbeteiligte Person ist (z. B. BVerfG 05.07.2010, BvR 759/10). Grundsätzlich sei zwar jede Anfertigung eines Beweisfotos ein Eingriff in die informationelle Selbstbestimmung der abgebildeten Person. Es ist nach Auffassung der Gerichte aber unvermeidbar, dass bei der Anfertigung eines Fotos im Rahmen der Verkehrsüberwachung auch der Beifahrer mit abgebildet wird. Es bestehe damit in Bezug auf den Beifahrer eine Ermächtigungsgrundlage, die die Anfertigung des Lichtbildes im vollen Umfang abdeckt.

Auch die weiteren Ermittlungshandlungen der Bußgeldbehörde sind rechtmäßig. In der Regel wird der Beifahrer auf dem Blitzerfoto, das an den Betroffenen gesendet wird, unkenntlich gemacht. Intern, d.h. in der Ermittlungsakte, muss der Mitfahrer jedoch nicht unkenntlich gemacht werden. Die Behörde darf einen näheren Blick auf den Beifahrer werfen, ihn identifizieren und ihm gegebenenfalls Fragen stellen oder als Indiz in der Beweisführung verwenden.

Die Ermittlungsbehörden nutzen den Bildabgleich des Blitzerfotos mit hinterlegten Lichtbildern der Meldebehörde, um den Beifahrer zu identifizieren. Für den Fall, dass

es sich bei dem Beifahrer um ein Kleinkind handelt, kann im Rahmen der Beweisführung die Anwesenheit des Kindes im Auto als Teil einer Indizienkette ein Indiz dafür sein, dass ein Elternteil das Fahrzeug geführt hat. Aus der Tatsache, dass das Gericht der Beweisführung im vorliegenden Einzelfall nicht folgen wollte, kann nicht auf die Unzulässigkeit der Datenverarbeitung geschlossen werden. Das gilt sowohl für den Einzelfall als auch für die Geeignetheit der Maßnahme an sich. Der Bildabgleich war auch nicht unverhältnismäßig, die Beiziehung eines Fotos ausschließlich zur Identitätsprüfung ist allenfalls als ein geringfügiger Eingriff zu bewerten und erscheint vor dem Zweck des staatlichen Auftrages, nämlich weitestgehend Verkehrssicherheit zu gewährleisten und Verkehrsverstöße zu sanktionieren, gerechtfertigt.

Voraussetzung für die Herausgabe eines Lichtbildes durch die Meldebehörde ist nach § 24 Abs. 2 Gesetz über Personalausweise und den elektronischen Identitätsnachweis (PAuswG), dass die ersuchende Behörde auf Grund von Gesetzen oder Rechtsverordnungen berechtigt ist, solche Daten zu erhalten, die ersuchende Behörde ohne Kenntnis der Daten nicht in der Lage wäre, eine ihr obliegende Aufgabe zu erfüllen und die ersuchende Behörde die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erheben kann oder wenn nach der Art der Aufgabe, zu deren Erfüllung die Daten erforderlich sind, von einer solchen Datenerhebung abgesehen werden muss. Die gesetzlichen Tatbestandsvoraussetzungen waren erfüllt. § 46 Abs. 2 OWiG und §§ 161 Abs. 1 Satz 1 und 2; 163 b Abs. 2 StPO ermächtigen die Ermittlungsbehörde zur Erhebung von Lichtbildern. Aus dem familiären und gewerblichen Umfeld des Halters unter anderem von Familienangehörigen, Mitbewohnern oder Kollegen. Die Ermittlungstätigkeiten können auch auf Nichtverdächtige ausgeweitet werden. Bei dem Lichtabgleich zum Beifahrer handelt es sich im vorliegenden Fall um einen verbliebenen Ermittlungsansatz, der dem Verhältnismäßigkeitsgrundsatz gerecht wird. Das Anfahren des Wohnsitzes durch Polizeibeamte und Ermittlungen vor Ort in Frage kommende Alternativmaßnahme wäre eingriffsintensiver gewesen, als die Hinzuziehung behördlich gespeicherter Informationen.

19.3 Aufnahme neuer Rechtsgrundlagen in das Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt (SOG LSA)

Im Dezember 2021 wurde der Landesbeauftragte für den Datenschutz gebeten, zu geplanten Rechtsänderungen im SOG LSA Stellung zu nehmen. Als wesentliche Änderungen sollten Rechtsgrundlagen für die Einsatzdokumentation durch Bild- und Tonaufnahmen (Bodycam) und die abschnittsbezogene Geschwindigkeitskontrolle aufgenommen werden.

Im Zuge einer abschnittsbezogenen Geschwindigkeitskontrolle werden zunächst alle Kennzeichen der den Kontrollbereich durchfahrenden Fahrzeuge erfasst und in einem Zwischenspeicher hinterlegt. Alle Daten von Fahrzeugen, die ohne Geschwindigkeitsübertretung den Kontrollbereich durchfahren, werden sofort vollständig gelöscht. Die Kennzeichen, welche einem Verstoß zuzuordnen sind, werden zur Weiterverwendung an die Zentrale Bußgeldstelle übergeben.

Der Einsatz von Bodycam ist bei den Polizeien anderer Bundesländer und des Bundes bereits Alltag, gilt aber als umstritten und ist immer wieder Anlass für Diskussionen. Auch hinsichtlich der geplanten Änderung des SOG LSA hatte der Landesbeauftragte für den Datenschutz kritische Anmerkungen gemacht. Dem Landesgesetzgeber wurde eine Lösung aufgezeigt, welche die bekannten Kritikpunkte aufgreift und eine aus Sicht

der Aufsichtsbehörde vertretbare Regelung darstellen könnte. Leider ist der Landesgesetzgeber den Empfehlungen des Landesbeauftragten für den Datenschutz hier nicht gefolgt.

Durch die Begleitung des Gesetzgebungsverfahrens durch den Landesbeauftragte für den Datenschutz konnte für die abschnittsbezogene Geschwindigkeitskontrolle eine datenschutzkonforme und damit eine mit nur geringfügigen Eingriffen in die informationelle Selbstbestimmung der Bürger verbundene Rechtsgrundlage geschaffen werden. Für den Einsatz von Bodycam ist dies dem Landesbeauftragten für den Datenschutz leider nicht gelungen.

20 Forschung

20.1 Wissenschaftliche Forschung – selbstverständlich mit Datenschutz

Da die Verarbeitung von Daten zu wissenschaftlichen Forschungszwecken immer mehr an Bedeutung gewinnt, hat sich die die Konferenz der Datenschutzbeauftragten des Bundes und der Länder das Thema „Datenschutz bei Forschungsdaten“ zum Arbeitsschwerpunkt für das Jahr 2022 gemacht. Die DSK hob mit ihrer einstimmigen Entschließung vom 23. März 2022 „Wissenschaftliche Forschung – selbstverständlich mit Datenschutz“[40] hervor, dass wissenschaftliche Forschung und Datenschutz miteinander vereinbar sind. So begrüßte diese die Überlegungen der Bundesregierung für ein Forschungsdatengesetz und ein Gesundheitsdatennutzungsgesetz. Darüber hinaus bot sie ihre Unterstützung an, bei der Forschungsdatenverarbeitung den bestmöglichen Schutz der Persönlichkeitsrechte der Bürger zu erreichen.

20.2 Petersberger Erklärung

Auf ihrer 104. Konferenz auf dem Petersberg bei Bonn beschloss die Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) am 23. November 2022 die „Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung“.[41] Die DSK bekräftigte nochmals, dass die Grundlage für eine datenschutzkonforme effektive Gesundheitsdatenforschung sowohl eine weitreichende Transparenz und eine hohe Rechtsklarheit für alle Beteiligten als auch die Sicherstellung des Schutzes personenbezogener Daten ist. Mit dieser Entschließung wurden den Gesetzgebern konkrete Empfehlungen für Regelungen bzgl. der Forschung mit Gesundheitsdaten gegeben.

So wurde u. a. darauf verwiesen, dass es Aufgabe des Gesetzgebers ist, im Allgemeininteresse liegende Forschung mit Gesundheitsdaten zu ermöglichen, aber auch ihre Grenzen festzulegen und die Interessen der betroffenen Personen zu wahren. Sofern eine gesetzliche Regelung Rechtsgrundlage einer Datenverarbeitung zu Forschungszwecken sein soll, muss sie in jedem Fall normenklar wirksam den Schutz des

---

[40] https://www.datenschutzkonferenz-online.de/media/en/DSK_6_Entschliessung_zur_wissenschaftlichen_Forschung_final.pdf

[41] https://www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf

Rechts auf informationelle Selbstbestimmung der betroffenen Personen gewährleisten und die datenschutzrechtlichen Anforderungen des europäischen und nationalen Datenschutzes erfüllen. Soweit der Forschungszweck mit anonymisierten Daten erreicht werden kann, dürfen nur anonymisierte Daten verarbeitet werden.

21 Schulwesen

21.1 Datenübermittlung im Rahmen von Zielvereinbarungsgesprächen

Durch eine Beschwerde wurde der Landesbeauftragte darauf aufmerksam, dass eine Ganztagsschule in Bezug auf mehrere Kinder mit diesen und deren Sorgeberechtigten gemeinsam ein Zielvereinbarungsgespräch geführt hat. Die Beschwerdeführerin habe zu Beginn der Veranstaltung noch auf die Datenschutz-Grundverordnung hingewiesen, dies sei aber mit dem Hinweis darauf, dass „Schüler und Eltern sehen, dass man nicht alleine diese Probleme hat“ ignoriert worden. So wurden im Kreis von Lehrkräften und vier Schülerinnen und Schülern sowie deren Sorgeberechtigten sensible Daten wie einzelne Probleme, Noten und persönliche Einschätzungen zu den Schülern durch Fachlehrer unter Bezug auf die von den Schülern zuvor notierten Zielbenotungen und Zielsetzungen für das Lernverhalten erörtert. Auf Nachfrage verwies die Schule auf einen Beschluss der Gesamtkonferenz, die Zielvereinbarungsgespräche in Kleingruppen durchzuführen. Die Teilnahme sei freiwillig, Einzelgespräche seien möglich. So könne auf Grundlage der Interaktion der Kinder die Gelegenheit gegeben werden, die zurückliegende Etappe zu reflektieren und Eltern können sich über Wichtiges in sozialen Beziehungen austauschen.

Dazu wurde die Schule auf § 84a Abs. 8 Satz 2 SchulG LSA hingewiesen, der die Übermittlung von personenbezogenen Daten der Schülerinnen und Schüler an private Dritte und damit an Mitschüler und deren Eltern grundsätzlich ausschließt. Eine Verarbeitung von sensiblen Schülerdaten in einem solchen gemeinsamen Zielvereinbarungsgespräch kann daher allenfalls auf der Grundlage der Einwilligung der Betroffenen erfolgen. Diese Einwilligung muss den Anforderungen des Art. 7 und der Erwägungsgrund 32, 42 und 43 DS-GVO entsprechen. Insbesondere ist eine umfassende vorherige Information und die Freiwilligkeit geboten. Dies ist von der verantwortlichen Schule nachzuweisen (Art. 5 Abs. 2 DS-GVO). Eine Einwilligung der Beschwerdeführerin, die diesen Anforderungen genügte, konnte die Schule nicht nachweisen. Die Schule hatte daher in erheblichem Umfang gegen die Vorgaben des Schulgesetzes verstoßen und die Persönlichkeitsrechte des betroffenen Kindes missachtet. Der Landesbeauftragte hat daher gegenüber den schulischen Datenschutzbeauftragten im Landesschulamt angeregt, die Schulen auf die Problematik hinzuweisen, um künftig für solche sicher sinnvollen gemeinsamen Zielvereinbarungsgespräche eine sichere Rechtsgrundlage zu schaffen.

21.2 Referentenentwurf zur Änderung des Schulgesetzes

Im Berichtszeitraum hatte der Landesbeauftragte die Gelegenheit, das Ministerium für Bildung zu einem Referentenentwurf zur Änderung datenschutzrechtlicher Regelungen des Schulgesetzes zu beraten. Dabei hat er die Nutzung verschiedener digitaler Lehr- und Lernmittel problematisiert und auf den Regelungsbedarf hingewiesen. Besonders hervorgehoben wurde die Problematik der Nutzung von privaten digitalen

Endgeräten durch Schülerinnen und Schüler. Weiter erörtert wurden u. a. die verschiedenen Grundlagen der Übermittlung von personenbezogenen Daten an Dritte.

22 Gesundheitswesen

22.1 Info-E-Mail zum Novavax-Impfstoff

Die Impfambulanz eines großen Klinikums hatte zu Beginn des Jahres zunächst eine Umfrage unter den Beschäftigten durchgeführt, wer an einer Impfung mit dem Impfstoff Novavax interessiert sei. Der neue Impfstoff Novavax basierte im Unterschied zu den bis dahin verfügbaren Impfstoffen gegen die Covid-19-Infektion nicht auf m-RNA-Basis. Es bestand daher die verbreitete Hoffnung, dass die Personen, die aus Sorge vor negativen Folgen durch die noch nicht umfänglich erforschten m-RNA-Impfstoffe noch nicht geimpft waren, sich nun mit dem neuen Novavax impfen lassen würden, das auf herkömmliche Weise hergestellt wurde. Die weitere Information zum Ablauf von Impfungen und Impfterminen mit Novavax wurde per E-Mail an über 90 Interessenten und drei weitere Stellen der Einrichtung versandt, so, dass alle Adressaten die E-Mailadressen der Empfänger lesen konnten. Erst nach der Versendung war aufgefallen, dass man anhand der E-Mailadressen rückschließen konnte, wer noch nicht geimpft war. Angesichts der kontroversen Diskussionen zum Impfgeschehen hätte diese sensible Gesundheitsinformation jedoch zum Schutz der Betroffenen geheim bleiben müssen. Das Klinikum hat umgehend vorgegeben, dass derartige Informationen künftig als Blindkopie zu versenden sind, um das Erkennen von anderen Empfängern derartig sensibler Informationen zu vermeiden. Diese Reaktion war zu begrüßen. Aus Sicht des Landesbeauftragten wäre aber wichtig, sich bei Massen-E-Mails frühzeitig die notwendigen Gedanken zu machen, insbesondere im Zusammenhang mit sensiblen Gesundheitsdaten.

22.2 Impfterminverarbeitung

Ein Beschwerdeführer beklagte, dass er am 24. Januar 2022 vom Impfzentrum seiner Stadt eine Einladung zur Corona-Impfung am 8. April 2021 per E-Mail bekam. Er ging davon aus, dass der Umgang mit seinen Daten fehlerhaft sei. Der Landesbeauftragte wandte sich daraufhin an das Gesundheitsamt des betroffenen Landkreises. Dieses verwies in seiner Stellungnahme auf die Möglichkeit, Impftermine online über die Webseiten des Landkreises zu buchen. Das Land habe diesen Service, der bei einem IT-Dienstleister lief, bereitgestellt.

Auf die Bitte des Landesbeauftragten um Erläuterungen zur Verantwortlichkeit und Darlegung von technischen Details des Fehlers wurde die verantwortliche Führung der Terminbuchung bestritten und auf den vom Land beauftragten Systemhersteller verwiesen. Der Hersteller des Systems, das in Auftragsverarbeitung bei einem IT-Dienstleister lief, erläuterte, dass den jeweiligen Gesundheitsämtern die in Mandanten abgeschirmte Nutzung eingeräumt worden und die Daten noch gespeichert seien, da das Ministerium für Arbeit, Soziales, Gesundheit und Gleichstellung noch erklären müsse, wie lange sie noch gebraucht würden. Ein Vertrag sei nur mit dem Ministerium zur Bereitstellung des Systems geschlossen worden. Auftragsverarbeitungsverträge mit den jeweiligen Gesundheitsämtern gäbe es nicht. Das Ministerium teilte dazu auf Nachfrage und Hinweis auf die wohl gebotene Löschung mit, dass die erfassten Daten

ausschließlich vom jeweiligen Landkreis in Mandanten verarbeitet würden. Das Ministerium habe das System zur Impfdokumentation und Impfterminvergabe zwar in Auftrag gegeben und zur Verfügung gestellt, es habe aber keinen Zugang zu den Daten. Das Ministerium bestätigte ein Versehen beim IT-Dienstleister. Der Fehler sei behoben.

Die Nutzung des Systemangebots durch die kreisfreien Städte und Landkreise, die Einbindung in den eigenen Internetauftritt sowie die Darstellung des Ministeriums ergab, dass von der Verantwortlichkeit der Kreisebene auszugehen war. Dafür sprach auch die Impfstrategie des Landes, wonach die Impfstofflogistik und das Terminmanagement landeseinheitlich durch das Land beauftragt werden. Die Landkreise und kreisfreien Städte errichten und betreiben die Impfzentren und bestimmen eine organisatorische Leitung. Die Verarbeitung von Impfdaten und die Terminorganisation lag in der Verantwortung der Kreisebene. Die lokalen Gesundheitsämter sind u. a. auch durch § 4 Abs. 1 i. V. m. § 3 Abs. 1 Nr. 1 IfSG in ihrer Verantwortung angesprochen, die Datenübermittlungen für die Impfsurveillance an das Robert Koch-Institut vorzunehmen. So hatte auch der betroffene Landkreis in der verspäteten Benachrichtigung für weitere Fragen auf seine Homepage verwiesen. Durch den Einsatz des Systems hat der jeweilige Kreis bzw. die kreisfreie Stadt die Entscheidung über die Mittel und den Zweck der Verarbeitung getroffen (Art. 4 Nr. 7 DS-GVO) und die Eigenschaft als datenschutzrechtlich Verantwortlicher begründet.

Da die somit für die Verarbeitung ihrer Impfdokumentation und Impfterminierung verantwortliche Kreisebene mit dem Anbieter des Service, dem Systemhersteller, keine Auftragsverarbeitungsverträge geschlossen hatte, stellte sich die Weitergabe der Daten der betroffenen Bürgerinnen und Bürger als eine Übermittlung dar. Dafür war keine Rechtsgrundlage ersichtlich und wurde auch nicht seitens des Landkreises vorgetragen. Der Landesbeauftragte wies daher darauf hin, dass die bisherige Verarbeitung somit als unzulässig anzusehen war und regte dringend an, die Weitergabe von Daten in das System des Herstellers durch Abschluss von Auftragsverarbeitungsverträgen zu legitimieren.

22.3 3-G-Regel bei Schul- und Hochschulveranstaltungen

Dem Landesbeauftragten ist bekannt geworden, dass eine Universität die sog. 3-G-Regelung nicht nur auf Basis des § 28b Infektionsschutzgesetzes (IfSG) für Beschäftigte, sondern auch auf Basis eines Rektoratsbeschlusses auf Lehrveranstaltungen unter Hinweis auf § 3 Abs. 2 Satz 4, 5 15. SARS-CoV-2-EindV anwendet. Danach war der Zugang zu Veranstaltungen in geschlossenen Räumen mit über 50 Personen auf Personen eingeschränkt, die die in Bezug auf die Corona-Erkrankung geimpft, genesen oder getestet waren. Grundsätzlich erschien eine Anwendung dieser Regelung auf Hochschulveranstaltungen, wie Vorlesungen, unter dem Aspekt der Kontaktreduzierung nachvollziehbar. Allerdings war der Veranstaltungsbegriff nach § 3 Abs. 2 Satz 1 15. SARS-CoV-2-EindV offen ausgestaltet. Daher wurde im für die Eindämmungsverordnung zuständigen Ministerium für Arbeit, Soziales, Gesundheit und Gleichstellung nachgefragt und von dort telefonisch bestätigt, dass der Veranstaltungsbegriff des § 3 Abs. 2 15. SARS-Co-V2-EindV nicht auf reguläre Schul- bzw. Hochschulveranstaltungen anwendbar wäre. Der Landesbeauftragte musste daher die Universität darauf hinweisen, dass die Erhebung von Gesundheitsdaten (geimpft, genesen, getestet) auf der Basis von § 3 Abs. 2 Satz 4, 5 15. SARS-CoV-2-EindV gegenüber Teilnehmern von regulären Hochschulveranstaltungen (z. B. Vorlesungen) nicht erfolgen darf. Es

blieb der Universität daher, wie wohl vom für Hochschulen zuständigen Ministerium beabsichtigt, nur die Möglichkeit, im Rahmen der Anwendung von Hygienevorgaben, z. B. durch die Anordnung der Maskenpflicht, der Entwicklung der Infektionsdynamik nach eigenem Ermessen flexibel zu begegnen.

22.4 Einrichtungsbezogene Impfpflicht

Für gesetzlich bestimmte Einrichtungen und Unternehmen aus dem Gesundheitsbereich galt ab dem 15. März 2022 nach § 20a Abs. 1 IfSG eine einrichtungsbezogene Impfpflicht. Seit diesem Zeitpunkt dürfen in diesen Einrichtungen nur Personen tätig sein, die gegen das Coronavirus SARS-CoV-2 geimpft oder von diesem genesen sind oder bei denen einen medizinische Kontraindikation hinsichtlich einer Impfung gegen das Coronavirus SARS-CoV-2 vorliegt. Infolge der hohen Zahl der Betroffenen traten viele Fragen auf, die auch an den Landesbeauftragten gestellt wurden. So wurde u. a. gefragt, für wen die einrichtungsbezogene Impfpflicht genau gilt, welche Nachweise nötig bzw. zulässig sind, gegenüber wem die Pflicht gilt, wann bzw. wie oft der Nachweis geboten ist und wie mit den Daten umzugehen ist. Dazu hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder den Beschluss vom 13. April 2022 „Zur Verarbeitung personenbezogener Daten im Zusammenhang mit der einrichtungsbezogenen Impfpflicht“ gefasst.[42]

22.5 Übermittlung von Gesundheitsdaten mittels WhatsApp

Im Rahmen einer Eingabe wurde dem Landesbeauftragten mitgeteilt, dass alle Mitarbeiter eines Corona-Testzentrums ihre privaten Handys im Rahmen der dienstlichen Tätigkeit nutzen müssen. Im Ergebnis der Sachverhaltsaufklärung war festzustellen, dass Mitarbeiter der verschiedenen Testzentren der Verantwortlichen ihre privaten Mobiltelefone im Rahmen der dienstlichen Tätigkeit genutzt haben. Über eine WhatsApp-Gruppe erfolgte laut der Verantwortlichen eine Versendung von Kundendaten, wenn die Kunden im falschen Testzentrum erschienen waren. Eine Datenübermittlung per WhatsApp wäre ausschließlich aufgrund der Einwilligung der Patienten und zum Zweck der Durchführung des Tests erfolgt. Darüber hinaus teilte die Verantwortliche mit, dass die Nutzung von WhatsApp-Gruppen durch Beschäftigte zu keiner Zeit für dienstliche Zwecke angeordnet wurde, da hierfür dienstliche Telefone zur Verfügung gestanden haben. Aufgrund vorliegender Screenshots aus der WhatsApp-Gruppe konnte die Übermittlung von Namen, Vornamen, Uhrzeiten und Testergebnissen (positiv/negativ) belegt werden. Auch Bilder von Kunden-Mails mit Nachfragen zum Testergebnis, von Kundenlisten mit Datum, Uhrzeit, Vorname, Name, Geburtsdatum, Adresse, Telefonnummer und E-Mail-Adresse sowie von Stapeln von Bestätigungen durchgeführter Tests waren enthalten. Die WhatsApp-Gruppe bestand lt. entsprechendem Screenshot aus 42 Teilnehmern. Die Gruppe wurde von den Leiterinnen des Testzentrums gegründet und die Teilnehmer, einschließlich des Gesellschafters hinzugefügt. Sowohl der Gesellschafter als auch die beiden Leiterinnen des Testzentrums waren Administratoren dieser WhatsApp-Gruppe.

Bei der Versendung von Beschäftigten- und Patientendaten über WhatsApp handelt es sich um eine Verarbeitung personenbezogener Daten, die einer Rechtsgrundlage

[42] https://www.datenschutzkonferenz-online.de/media/dskb/2022_13_04_beschluss_DSK_20a_IfSG.pdf

bedarf (Art. 6 Abs. 1 DS-GVO). Als Rechtsgrundlage gab die Verantwortliche für die Übermittlung der Kundendaten innerhalb der WhatsApp-Gruppe die Einwilligung der Betroffenen an.

Die Anforderungen an eine wirksame Einwilligung finden sich in Art. 4 Nr. 11, 6 Abs. 1 lit. a, 7 und den Erwägungsgründen 32, 42 und 43 DS-GVO. Die zentralen Wirksamkeitsvoraussetzungen sind Freiwilligkeit, Bestimmtheit, Informiertheit und Widerrufbarkeit. Eine Einverständniserklärung ist bestimmt, wenn die betroffene Person die Verarbeitung der sie betreffenden Daten für einen oder mehrere bestimmte Zwecke gegeben hat. Die Bedingung einer informierten Einwilligung erfordert, dass die betroffene Person zum Zeitpunkt der Verarbeitung bereits abschätzen kann, welche Auswirkungen die Erteilung hat. Sie muss die Umstände der Datenverarbeitung sowie die Tragweite der Einwilligung eindeutig und klar erkennen können. Ferner muss die Einwilligung jederzeit ohne Angabe von Gründen widerrufbar sein. Dies bedeutet, dass die Mitarbeiter der Verantwortlichen den betroffenen Patienten nicht nur den genauen Zweck der Datenverarbeitung, sondern vielmehr auch die vorgesehene Nutzung von WhatsApp auf den privaten Handys der Mitarbeiter mit den entsprechenden Auswirkungen für die Sicherheit und den Schutz der personenbezogenen Daten (z. B. Zugriff von Meta Relations, Speicherdauer der Nachricht, Zugriff auf den Chatverlauf durch Dritte (z. B. Familienangehörige)) verständlich gemacht haben müssten. Aufgrund dessen waren zumindest die Bestimmtheit und Informiertheit der Einwilligungen der betroffenen Patienten und damit die Wirksamkeit insgesamt zu verneinen. Darüber hinaus wurden die Einwilligungen der Betroffenen lt. Verantwortlicher ausschließlich mündlich erteilt, sodass auch ein entsprechender Nachweis der Einwilligung durch die Verantwortliche nicht möglich ist. Die Versendung personenbezogener Daten über WhatsApp auf der Grundlage wirksamer Einwilligungen der Betroffenen scheidet damit aus.

Als gesetzliche Grundlage für die Datenverarbeitung kommen Art. 6 Abs. 1 lit. b bzw. f DS-GVO in Betracht. Zum Zweck der Vertragserfüllung bzw. einer verbesserten Arbeitsorganisation ist eine Datenverarbeitung im Wege einer Kontaktierung des anderen Testzentrums auch als berechtigtes Interesse der Verantwortlichen zu werten. Allerdings setzen Art. 6 Abs. 1 lit. b und f DS-GVO auch voraus, dass die Verarbeitung erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen.

Die Erforderlichkeit ist gegeben, wenn die Verarbeitung für die Erreichung des Zwecks, d. h. der Durchführung der Tests geeignet, erforderlich und insgesamt verhältnismäßig ist. Für die Fälle, in denen Kunden nicht in dem Testzentrum erschienen sind, in denen sie vorab den Termin zur Testdurchführung gebucht hatten, wurde zwar anerkannt, dass eine Kontaktaufnahme mit dem anderen Testzentrum hilfreich für eine komplikationslose Absprache des weiteren Vorgehens ist. Allerdings standen hierfür als mildere Mittel dienstliche Telefone zur Verfügung. Die Nutzung privater Smartphones oder einer WhatsApp-Gruppe war daher zwar geeignet, jedoch nicht erforderlich. Darüber hinaus wurden durch die Verwendung der WhatsApp-Gruppe die Daten nicht nur den zu diesem Zeitpunkt für die Durchführung der Tests zuständigen Mitarbeiter des jeweiligen Testzentrums, sondern an alle 42 Mitglieder der Gruppe versandt. Auf diese Weise hat immer auch eine erhebliche Anzahl von Mitarbeitern die personenbezogenen Daten zur Kenntnis erhalten, die nicht im Dienst waren. Für diese Mitarbeiter waren diese Informationen in keinster Weise erforderlich.

In diesem Zusammenhang war besonders zu berücksichtigen, dass es sich bei einer Vielzahl der Informationen um Gesundheitsdaten nach Art. 4 Nr. 15 DS-GVO handelte, die nach Art. 9 DS-GVO einem besonderen Schutz unterliegen. Art. 9 DS-GVO steht der Verarbeitung von Gesundheitsdaten zwar grundsätzlich nicht entgegen. Nach Art. 9 Abs. 2 lit. h DS-GVO unterliegt die Verarbeitung zur medizinischen Diagnostik und zur Versorgung oder Behandlung im Gesundheitsbereich auch dem Erforderlichkeitsgrundsatz. Aufgrund der fehlenden Erforderlichkeit der Datenübermittlung per WhatsApp-Gruppe ergab sich keine Rechtmäßigkeit der Verarbeitung durch Art. 6 Abs. 1 lit. b bzw. lit. f DS-GVO. Die entsprechenden Verarbeitungen waren damit datenschutzrechtlich unzulässig.

Für die weiteren aufgrund der Screenshots erkennbaren Datenübermittlungen (Liste mit Datum, Uhrzeit, Vorname, Name, Geburtsdatum, Adresse, Telefonnummer und E-Mail-Adresse; Stapel von Bestätigungen durchgeführter Tests) war schon kein entsprechender Zweck und damit auch keine Rechtsgrundlage ersichtlich. Aufgrund der festgestellten Rechtsverstöße (mindestens 114 Personen in 21 Fällen) betreffend besonders sensibler Gesundheitsdaten im Zeitraum von ca. einem Jahr wurde gegen die Verantwortliche ein Bußgeld einschließlich Gebühren und Auslagen in Höhe von 28.360,50 Euro erhoben.

22.6 Datenschutzverletzung an der Uniklinik – Meldedatenabruf

Im Oktober 2021 wurde bekannt, dass gegen eine Beschäftigte eines Universitätsklinikums staatsanwaltschaftlich ermittelt wird, da sie über den automatisierten Meldedatenabruf aus privaten Motiven Daten abgerufen haben soll. Im Zusammenhang mit der Körperverletzung einer Person in ihrer Wohnung in Leipzig war die Staatanwaltschaft auf die Abfrage der Meldeadresse durch die Beschäftigte des Uniklinikums gestoßen. Die Beschäftigte soll Gleichgesinnte mit Meldeadressen politischer Gegner versorgt haben. Erst auf Anfrage des Landesbeauftragten sandte das Uniklinikum sodann eine Meldung einer Datenschutzverletzung. Im Weiteren hat das Uniklinikum auf seiner Homepage Erläuterungen zur Sach- und Rechtslage abgegeben und weiterhin auf die Anfragen des Landesbeauftragten mit umfänglichen Stellungnahmen hilfreich reagiert.

Hintergrund des Falls ist die Befugnis von einigen öffentlichen Stellen im Land, Meldeadressen von Personen bundesweit automatisiert abzurufen (§ 38 BMG). Im Rahmen der Recherchen stellte sich heraus, dass das Uniklinikum bereits frühzeitig mit der Problematik befasst war. Bereits im November 2019 gab es gegenüber dem Uniklinikum ein Auskunftsersuchen des Landeskriminalamtes Sachsen zur genutzten dienstlichen E-Mail-Adresse der Beschäftigten. Die Beschäftigte hatte dann im Februar 2020 die Abfrage der Meldeadresse der verletzten Person in Leipzig eingeräumt, aber behauptet, dem hätte eine dienstliche Suche nach einem Schuldner zugrunde gelegen. Ein Durchsuchungsbeschluss vom April 2020 konkretisierte den Verdacht. Weitere Erkenntnisse ergab ein Schreiben des Landeskriminalamtes Sachsen-Anhalt vom Juli 2020 an das Uniklinikum. Das Uniklinikum verwies jedoch darauf, dass erst ein Schreiben des Landeskriminalamtes Sachsen-Anhalt im Oktober 2021 ergeben hätte, dass gegen die Beschäftigte wegen einer Vielzahl von Einzelverfahren ermittelt würde. Erst damit hätte sich der Verdacht einer missbräuchlichen Nutzung des dienstlichen Zugangs zum automatisierten Meldedatenabruf weiter konkretisiert, sodass die Meldung einer Verletzung des Datenschutzes nach Art. 33 Abs. 1 DS-GVO tags darauf rechtzeitig erfolgt sei.

Zur Meldung einer Datenschutzverletzung hatte der Landesbeauftragte zu prüfen, ob die Meldung einer Datenschutzverletzung rechtzeitig erfolgt ist. Dazu verwies das Uniklinikum zunächst darauf, dass die Meldepflicht des Art. 33 Abs. 1 DS-GVO den Verantwortlichen treffe, die abgefragten Personen aber weder Schuldner noch Patienten waren, sodass das Uniklinikum nicht Verantwortlicher sei. Der richtige Gedanke hinter der Erwägung war, dass ggf. ein Mitarbeiterexzess der Beschäftigten dem Arbeitgeber Uniklinikum nicht hätte zugerechnet werden können. Mit dem eingerichteten Abrufsystem wurden aber personenbezogene Daten durch das Uniklinikum verarbeitet und es musste als Verantwortlicher gewährleisten, dass die Nutzung des Systems und die Verarbeitung nur im Rahmen des Erforderlichen erfolgt. Technische und organisatorische Maßnahmen des Verantwortlichen müssen Schutz gegen jegliche Art der datenschutzrechtswidrigen Verarbeitung bieten. Zudem ist auch in § 39 Abs. 1 BMG bestimmt, dass die abrufberechtigte Stelle bei der Einrichtung eines automatisierten Abrufverfahrens durch geeignete technische und organisatorische Maßnahmen nach den Artikeln 24, 25 und 32 DS-GVO sicherzustellen hat, dass Daten nur von hierzu befugten Personen abgerufen werden können. Das Uniklinikum war daher als für die Abrufe seiner Beschäftigten zumindest mit Verantwortlicher zu betrachten und somit zur Meldung einer Datenschutzverletzung verpflichtet.

Voraussetzung der Meldepflicht nach Art. 33 Abs. 1 DS-GVO ist eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt (siehe Art. 4 Nr. 12 DS-GVO). Eine Verletzung der Sicherheit lag vor. Sowohl die allgemeine Vorgabe des Art. 32 DS-GVO als auch die spezifische Bestimmung in § 39 Abs. 1 BMG gebieten eine Datenverarbeitung in einer Weise, die einen hinreichenden Schutz insbesondere in Bezug auf Integrität und Vertraulichkeit der Daten gewährleistet.

Von einer solchen Verletzung der Sicherheit war auszugehen, da hinreichende Anhaltspunkte dafür vorlagen, dass die betroffene Beschäftigte des Uniklinikums automatisierte Abfragen zu nicht dienstlichen Zwecken gestellt hatte. Die Sicherheitsverletzung hatte auch zu einer Schutzverletzung geführt (unbefugter Zugang zu den Daten bzw. unbefugte Offenlegung). Die Beschäftigte selbst war unbefugt an Meldedaten gekommen und hatte sie nach den vorliegenden Erkenntnissen wohl auch an weitere Unbefugte weitergereicht.

Die Verpflichtung zur unverzüglichen Meldung entsteht grundsätzlich mit der Sicherheitsverletzung. Nicht erforderlich ist eine Meldung auf „bloßen“ Verdacht hin. Der Verantwortliche muss hinreichende Kenntnis von der Verletzung haben, nicht jedoch sichere Informationen über alle Details. Nach Berücksichtigung der Stellungnahmen des Klinikums und Einsicht in Schriftverkehr und Dokumente kam der Landesbeauftragte zu der Auffassung, dass das Uniklinikum bereits weit vor dem Oktober 2021 eine hinreichende Kenntnis von der Verletzung des Datenschutzes hatte. Infolge des Verstoßes gegen die Pflicht zur unverzüglichen Meldung einer Datenschutzverletzung nach Art. 34 Abs. 1 Satz 1 DS-GVO hat der Landesbeauftragte mit einem Bußgeld reagiert.

In Bezug auf Maßnahmen gemäß Art. 32 DS-GVO, § 39 Abs. 1 S. 1 BMG hatte das Uniklinikum fachlich qualifiziertes Personal eingesetzt. Die mit dem Abruf Beschäftigten waren belehrt worden (u. a. Hinweise zum rechtskonformen Umgang mit personenbezogenen Daten, auf Strafvorschriften und Schweigepflichten, auf die begrenzte

Weitergabe von Daten). Es fand auch eine Dokumentation der Abrufe statt. Missbräuchliche Abrufe, die von den Handelnden nicht dokumentiert wurden, waren somit allerdings nur feststellbar, wenn der Browserverlauf noch nicht gelöscht war.

Die Sicherungsmaßnahmen wurden nach Auffassung des Landesbeauftragten den Anforderungen von Art. 32 DS-GVO und § 39 Abs. 1 BMG nicht gerecht. Es entspricht der Erfahrung der Datenschutzaufsichtsbehörden, dass dienstliche Zugänge zu Datenbeständen missbraucht werden, um Daten aus persönlichen Motiven zu verarbeiten. Dieser realistischen Gefahr ist mit hinreichenden Maßnahmen zu begegnen. Zwar geht es nur um Daten, die als einfache Melderegisterauskunft jedermann ohne Nachweis eines berechtigten Interesses zugänglich sind (§ 44 Abs. 1 BMG). Gefährdete Personen haben zudem die Möglichkeit, Auskunftssperren zu beantragen (§ 51 BMG). Der vorliegende Fall zeigte aber, dass auch einfache Informationen in erheblicher Weise zu schädigenden Ereignissen missbraucht werden können. Dem Risiko unbefugter Zugriffe wurde nicht hinreichend begegnet. Die individuelle Abrufkennung (E-Mail-Adresse) hilft ebenso wenig wie das Gebot zur Aufzeichnung der Abrufe, da dies im browsergestützten Verfahren umgangen werden kann. Einem automatisierten Abruf per Fax stünden datenschutzrechtliche Bedenken entgegen. Eine Erhöhung der Sicherheit könnte sich aus dem Abruf im Vier-Augen-Prinzip ergeben, was aber einen erheblichen finanziellen und personellen Aufwand erfordern würde.

Um eine sachgerechte und wirksame Sicherung zu erzielen schlug der Landesbeauftragte infolge der Kommunikation mit dem Uniklinikum und dem Ministerium für Inneres und Sport vor, Stichprobenkontrollen mit Abrufprotokollen in Betracht zu ziehen, in einem geringen Umfang, der lediglich dazu dienen soll, durch ein potentielles Entdeckungsrisiko vom Missbrauch dienstlicher Kommunikationstechnik abzuhalten.

Bedenken des Uniklinikums, dem könnte der Beschäftigtendatenschutz entgegenstehen, greifen nicht. Grundsätzlich ist zwar das Persönlichkeitsrecht der Beschäftigten bei der Verarbeitung von Beschäftigtendaten zu berücksichtigen. Eine Überwachung der Nutzung dienstlicher Kommunikationstechnik ist aber durchaus möglich, ausgeschlossen wäre erst eine unverhältnismäßige Verhaltens- oder Leistungskontrolle. Der Rückgriff auf Protokolldaten schien daher eine sinnvolle Lösung. § 40 Abs. 5 Satz 3 BMG sieht auch vor, dass die Verwendung der Protokolldaten für Datenschutzkontrollen möglich ist. Leider teilte das Ministerium für Inneres und Sport dazu mit, dass § 40 Abs. 5 Satz 3 BMG - trotz des klaren Wortlauts - aufgrund von Bedenken des Bundesministeriums des Innern und für Heimat keine regelmäßigen anlasslosen Zugriffe auf Protokolldaten zulasse. Die einzig wirkungsvolle Sicherungsmaßnahme des Abgleichs stichprobenartiger Protokolldaten mit den tatsächlich gegebenen dienstlichen Anlässen durch die abrufenden Stellen ist damit nicht durchführbar.

Die verbleibende Nutzung der Protokolldaten durch die Meldebehörden schützt nicht, da die Meldebehörden nur feststellen könnten, dass eine berechtigte Stelle abgerufen hat, nicht aber, ob ein dienstlicher Anlass dazu gegeben war. Zudem finden diese Prüfungen aufgrund von Vereinbarungen in der Praxis wohl auch gar nicht statt. Alternativ erwogenen Sicherungsmaßnahmen des Ministeriums für Inneres und Sport hatten sich, wie der Vorgang zeigte, als nicht wirksam herausgestellt.

22.7 Digitale Funkmeldungen des Rettungsdienstes

Durch Hinweise und eine Meldung nach Art. 33 DS-GVO ist dem Landesbeauftragten bekannt geworden, dass in zwei Rettungsdienstkreisen die Alarmierungsdaten mit Namen, Adressen, Hinweisen auf Erkrankungen (z. B. Schlaganfall, Schenkelfraktur, Bewusstseinsstörung etc.), Hinweisen auf das Vorliegen von Infektionen und Hinweisen auf die Destination (z. B. Demenzpflegezentrum) zu bis über hundert Vorgängen an einem einzigen Tag im Internet zugänglich auffindbar waren. Offensichtlich wertete jemand die digitalen Einsatzkräfte-Alarmierungen mit einem digitalen Meldeempfänger aus und machte sie über das Internet zugänglich. Es wurde vermutlich die kostenlose Software BosMon verwendet, um die mit dem älteren Pocsag-Protokoll versandten Informationen lesbar zu machen. Die Funkmeldungen waren in einem Rettungdienstkreis nicht einmal verschlüsselt. Zudem bestand der Verdacht, dass Webserver, auf denen die Daten gespeichert waren, über Suchdienste wie Censys wohl leicht auffindbar waren. Eine Rettungsleitstelle erklärte, dass in ihrem Bereich ca. 5000 digitale Meldeempfänger im Einsatz wären, vielfach gefragt in kleineren örtlichen Feuerwehren.

Der Landesbeauftragte hat mit den betroffenen und weiteren Rettungsleitstellen Kontakt aufgenommen, zum Hintergrund recherchiert und diese direkt beraten. Die Problematik des Ausspähens und unbefugter Veröffentlichung von Alarmierungsdaten mit personenbezogenen und insbesondere medizinischen Daten ist seit einigen Jahren bundesweit Gegenstand medialer Aufmerksamkeit. Die bisher ergriffenen technischen und organisatorischen Maßnahmen haben offensichtlich nicht ausgereicht, um ein dem Gebot des Art. 32 DS-GVO angemessenes Maß an Datensicherheit zu gewährleisten. Infolge der flächendeckenden Problematik und des Zusammenwirkens verschiedener Einrichtungen hat der Landesbeauftragte weiter dem zuständigen Ministerium empfohlen, auf Landesebene auf möglichst einheitliche und vor allem sichere Verfahrensweisen hinzuwirken, um datenschutzkonforme Verarbeitungen zu gewährleisten. Dazu hat er auf Folgendes hingewiesen:

Zunächst dürfte es notwendig sein, die Alarmierungsdaten, soweit sie auf Servern gespeichert werden, dort vor unbefugtem Zugriff zu sichern. Dies gilt auch in Bezug auf Rechner in den Einrichtungen, die die Informationen befugt erhalten. Insoweit wäre darauf hinzuwirken, dass auch in Empfängereinrichtungen, wie ggf. kleinen Kommunen oder örtlichen Feuerwehren, eine netzgebundene Speicherung nur erfolgt, wenn diese hinreichend gegen unbefugten Zugriff abgesichert ist. Der Zugriff durch ausschließlich Befugte sollte durch Zugangsschutz (Passwort) bzw. Verschlüsselung gesichert werden.

Da die Verschlüsselung allein offenbar kein hinreichender Sicherheitsgarant war, sollte zur Erhöhung der Wirksamkeit dieser Sicherungsmaßnahme darauf hingewirkt werden, dass Entschlüsselungsschlüssel an so wenige Empfänger wie möglich herausgegeben werden. Der Schlüssel sollte nur durch einzelne Beschäftigte der Leitstelle auf die Empfänger aufgespielt und geschützt werden, sodass Gefahren unbefugter Entschlüsselungen reduziert werden.

Eine weitere Notwendigkeit erschien die Adressierung einzelner digitaler Meldeempfänger durch sog. RIC-Kennungen. Damit kann die Übermittlung der in der Meldung enthaltenen personenbezogenen Daten an eine Vielzahl von Besitzern von digitalen

Meldeempfängern grundsätzlich eingegrenzt werden. Ohne entsprechende Beschränkungen kann dies offensichtlich zu nicht aufklärbaren unbefugten Veröffentlichungen führen.

Auch erschien es notwendig, dass ein regelmäßiger Wechsel der RIC-Kennungen vorgegeben wird. Viele RIC-Kennungen sind einem größeren Personenkreis bekannt. Hierzu gab es Hinweise darauf, dass inzwischen sogar „Listen“ zu den RIC-Kennungen kursieren. Zudem können digitale Meldeempfänger bis zu 50 RIC-Kennungen aufnehmen. Ein regelmäßiger Wechsel grenzt die Kenntnis über die Kennungen in der Breite ein.

Ein wichtiger und besonders wirksamer Ansatz des Schutzes von sensiblen persönlichen Daten ist auch, zu prüfen, ob und inwieweit in bestimmten Meldungen auf personenbezogene Informationen verzichtet werden kann. So könnten die Meldungen an die Feuerwehr ggf. keine personenbezogenen Daten enthalten. Die für den Rettungsdienst notwendigen Daten wie Namen könnten vor unbefugtem Zugriff geschützt werden, indem sie in der Alarmmeldung gar nicht enthalten sind und erst auf Nachfrage per Funk an das Rettungsfahrzeug mitgeteilt werden. Dies sollte weitestgehend auch für medizinische Informationen gelten. Für die meisten Einsatzarten dürfte der ggf. zu beachtende Zeitverlust auf dem Fußweg zum Rettungswagen nicht erheblich sein.

Abschließend sollten die Rettungsleitstellen angehalten sein, in ihrer Verantwortung für die im Rahmen des Rettungsdiensteinsatzes verarbeiteten personenbezogenen Daten auch auf die Empfänger einzuwirken und diese mit Hinweisen bzw. Vorgaben zum datenschutzkonformen Umgang in die Pflicht zu nehmen. Die jeweils handelnden Beschäftigten sollten insoweit regelmäßig sensibilisiert werden.

22.8 Datenschutzgrundlagen bei kleineren Leistungserbringern im Gesundheitswesen

Im Berichtszeitraum häuften sich bei dem Landesbeauftragten Eingaben und Beschwerden gegen die Datenverarbeitungen von kleineren Leistungserbringern im Gesundheitswesen, z. B. Ambulanten Pflegediensten, Rettungsdiensten und Unternehmen, die häusliche Krankenpflege oder Krankenbeförderung anbieten. Dabei machte der Landesbeauftragte immer wieder die Erfahrung, dass häufig grundlegende Anforderungen der DS-GVO nicht bekannt waren oder nicht beachtet wurden.

Insbesondere führten die Unternehmen vielfach kein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DS-GVO, stellten den betroffenen Personen keine Informationen nach Art. 13, 14 DS-GVO zur Verfügung (siehe hierzu auch Nr. 22.9) und hatten teilweise keinen Datenschutzbeauftragten benannt, obwohl sie gemäß Art. 37 DS-GVO dazu verpflichtet waren.

Häufig klärte der Landesbeauftragte über die Grundsatzfragen auf, dass in der Regel auch Papiersammlungen von Unterlagen Datenverarbeitungen darstellen, die in den Anwendungsbereich der DS-GVO fallen. Dies ist immer dann der Fall, wenn es sich um eine nach Kriterien geordnete und recherchierbare, strukturierte Sammlung personenbezogener Daten und damit um ein „Dateisystem“ i. S. d. Art. 2 Abs. 1, Art. 4 Nr. 6 DS-GVO handelt (vgl. auch Erwägungsgrund 15 Satz 3).

Bei den genannten Leistungserbringern wurden beispielsweise Daten in einer personenbezogenen Pflegedokumentation, auf Krankentransportscheinen oder Rettungseinsatzprotokollen erhoben, anschließend (ggf. teilweise) in automatisierten Datenverarbeitungssystemen erfasst und an die Kostenträger (z. B. Krankenkassen) übermittelt (ggf. über Auftragsverarbeiter, Rechenzentren o. ä.) sowie zur Erfüllung von Dokumentations- und Aufbewahrungspflichten für viele Jahre gespeichert, teilweise auch für Qualitätssicherungsmaßnahmen verwendet oder in besonderen Fällen an Dritte übermittelt (z. B. an Herzinfarktregister). Bei allen diesen Vorgängen handelt es sich um Verarbeitungen i. S. v. Art. 4 Nr. 7 DS-GVO. Diese finden auch nicht nur gelegentlich statt, sodass unabhängig von der Anzahl der im Unternehmen beschäftigten Personen ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DS-GVO zu führen ist.

Auch im eigenen Interesse des Unternehmens ist es ratsam, ein vollständiges Verzeichnis von Verarbeitungstätigkeiten zu erstellen. Das Verzeichnis dient als wesentliche Grundlage für eine strukturierte Datenschutzdokumentation und hilft dabei, gemäß Art. 5 Abs. 2 DS-GVO nachzuweisen, dass die Vorgaben aus der DS-GVO eingehalten werden (Rechenschaftspflicht).

Wie eine Reihe von Datenschutzprüfungen ergab, erstellten Unternehmen das Verzeichnis der Verarbeitungstätigkeiten pflichtwidrig erst nach der aufsichtsbehördlichen Anfrage gemäß Art. 30 Abs. 4 DS-GVO. In einem besonders gravierenden Fall verhängte der Landesbeauftragte dafür ein hohes dreistelliges Bußgeld.

Eine Ausnahmeregelung, nach der Leistungserbringer im Gesundheitswesen auf die Erfüllung der Informationspflichten nach Art. 13, 14 DS-GVO verzichten können, ist nicht ersichtlich. Praxisnahe Lösungen sind möglich, auch in Beförderungsfahrzeugen (Näheres hierzu unter Nr. 22.9). Fehlende, unvollständige oder nicht transparente Informationen haben im Berichtszeitraum zu vielfachen aufsichtsbehördlichen Hinweisen geführt. Dies führte in einzelnen Fällen zu einem Bußgeld in dreistelliger Höhe.

Bei der Frage, unter welchen Voraussetzungen, die Unternehmen verpflichtet sind, einen Datenschutzbeauftragten zu benennen, sind im Wesentlichen zwei Voraussetzungen zu prüfen.

Nach Art. 37 Abs. 1 lit. c DS-GVO ist stets ein Datenschutzbeauftragter zu benennen, wenn die Kerntätigkeit des Verantwortlichen in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 DS-GVO, also auch Gesundheitsdaten, besteht. Eine Sonderregelung beinhaltet Erwägungsgrund 91 Satz 4. Danach gilt eine Datenverarbeitung nicht als umfangreich, wenn sie die personenbezogenen Daten von Patienten betrifft und durch einen einzelnen Angehörigen eines Gesundheitsberufes erfolgt. Dies traf allerdings in den geprüften Fällen nicht zu, denn es handelte sich stets um Unternehmen mit einer gewissen Anzahl an Beschäftigten. Auch wenn sie Angehörige von Gesundheitsberufen waren, führten sie die Datenverarbeitung jedenfalls nicht einzeln bzw. allein durch.

Verarbeitungsvorgänge sind umfangreich, wenn sie dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, wenn sie eine große Zahl von Personen betreffen könnten und – beispielsweise aufgrund ihrer Sensibilität – wahrscheinlich ein hohes Risiko mit sich bringen

und bei denen entsprechend dem jeweils aktuellen Stand der Technik in großem Umfang eine neue Technologie eingesetzt wird, sowie wenn sie ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen, insbesondere dann, wenn diese Verarbeitungsvorgänge den betroffenen Personen die Ausübung ihrer Rechte erschweren (Erwägungsgrund 91 Satz 1 zur DS-GVO). Dies lässt sich festmachen an der Anzahl der Betroffenen, der Menge der betroffenen Datensätze bzw. der Vielfalt der Datenverarbeitungsprozesse, der Dauer der Datenverarbeitung und der geographischen Reichweite (vgl. Leitlinien der Artikel-29-Datenschutzgruppe in Bezug auf Datenschutzbeauftragte in der Fassung vom 5. April 2017, WP 243 rev. 01).

Sind die besonderen Voraussetzungen des Art. 37 Abs. 1 DS-GVO nicht erfüllt, müssen Unternehmen dennoch einen Datenschutzbeauftragten benennen, soweit sie in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen (§ 38 Abs. 1 Satz 1 BDSG). Zu diesen Personen zählen alle Personen, auch Mitglieder der Geschäftsleitung, Leiharbeitnehmer, Praktikanten, freiberuflich Mitarbeitende etc. jeweils als „vollwertige“ Person. „Ständig“ heißt hier, dass die Person dauerhaft mit der Tätigkeit betraut ist, gleichwohl ihr nicht in engen Zeitabständen konkret nachgehen muss. Wer bestimmte Datenverarbeitungen z. B. einmal monatlich durchführt, ist ständig mit der Verarbeitung beschäftigt. Wer Tätigkeiten nur vorübergehend als Vertreter ausführt, ist nicht „in der Regel“ damit betraut.

Ein Unternehmen, das im Rettungsdienst und als anerkannte Lehrrettungswache tätig war, hatte beispielsweise 44 Beschäftigte, die allesamt die Daten aus Rettungseinsatzprotokollen in einer Software erfassten und damit auch Gesundheitsdaten automatisiert verarbeiteten. Einen Datenschutzbeauftragten benannte das Unternehmen erst nach mehrmaligen aufsichtsbehördlichen Hinweisen. Dies hat der Landesbeauftragte mit einem vierstelligen Bußgeld sanktioniert.

Leistungserbringer im Gesundheitswesen sind in besonderem Maße den Anforderungen der DS-GVO verpflichtet, da sie häufig in erheblichem Umfang Gesundheitsdaten als besondere Kategorie personenbezogener Daten nach Art. 9 DS-GVO verarbeiten. Dass sie die Grundlagen des Datenschutzmanagements und der Datenschutzdokumentation kennen und beachten, sollte eine Selbstverständlichkeit sein. Dazu gehören insbesondere das stets aktuelle Verzeichnis der Verarbeitungstätigkeiten, transparente Informationen für die betroffenen Personen und das Benennen eines Datenschutzbeauftragten, wenn gesetzlich notwendig, spätestens also, wenn 20 Beschäftigte mit der automatisierten Datenverarbeitung betraut sind.

22.9 Erfüllen der Informationspflichten im Krankentransport und Rettungsdienst

In einer Datenschutzüberprüfung beschäftigte sich der Landesbeauftragte im Jahr 2022 intensiv mit der Frage, wie Beförderungsunternehmen ihre Informationspflichten nach Art. 13, 14 DS-GVO erfüllen können, konkret wie die Informationen den Fahrgästen sinnvollerweise zur Verfügung gestellt werden können. Die Prüfung bezog sich insbesondere auf Unternehmen, die – ausschließlich oder zusätzlich zu Taxifahrten – auch Krankentransportleistungen anbieten oder im Rettungsdienst tätig sind.

Der Landesbeauftragte machte die Erfahrung, dass vor allem die Unternehmensleitungen von Taxi-/Krankentransportunternehmen und dessen (häufig nichtmedizinisches)

Personal sich der Datenverarbeitungen im Detail und deren Sensibilität und Schutzbedürftigkeit vielfach erst durch die aufsichtsbehördliche Anfrage und Beratung bewusstwurden. Ein Unternehmen wandte mit Nachdruck ein, dass die gesetzlichen Anforderungen überzogen seien, da der Gesundheitszustand es für die beförderten Personen vor allem im Rettungsdienst uninteressant oder gar unmöglich mache, die datenschutzrechtlichen Informationen zur Kenntnis zu nehmen. Dieses Unternehmen trug auch vor, dass kein anderes Beförderungsunternehmen die Anforderungen der Art. 13, 14 DS-GVO erfüllen würde. Dies nahm der Landesbeauftragte zum Anlass, seine Auffassung mit den weiteren Datenschutzaufsichtsbehörden in Deutschland, im Arbeitskreis Gesundheit und Soziales der Datenschutzkonferenz, abzustimmen. Dabei erhielt er breite Zustimmung.

Der Landesbeauftragte hält die Informationspflichten nach Art. 13, 14 DS-GVO in den Geschäftsbereichen Krankentransport und Rettungsdienst deshalb für bedeutsam, weil die Beförderungsunternehmen besondere Kategorien personenbezogener Daten nach Art. 9 DS-GVO verarbeiten. Der besonderen, ggf. auch gesundheitlichen Situation bei der Datenerhebung von den transportierten Personen ist selbstverständlich Rechnung zu tragen. Insbesondere darf die Erfüllung der Informationspflichten nicht dazu führen, dass Krankentransporte verzögert, verlängert oder ansonsten für die transportierte Person unangenehmer werden. Allerdings ist keine Ausnahmeregelung ersichtlich, nach der hier auf die Erfüllung der Informationspflichten nach Art. 13, 14 DS-GVO gänzlich verzichtet werden kann. Insbesondere ist dies nicht allein deshalb der Fall, weil die betroffene Person nicht interessiert oder aus gesundheitlichen Gründen nicht in der Lage ist, die Informationen zur Kenntnis zu nehmen. Nach Auffassung des Landesbeauftragten muss daher jedes Unternehmen die Informationen auf irgendeine Weise bereithalten, die, der Situation angemessen, durchaus auch niedrigschwellig sein kann.

Möglich erscheint ein zweistufiges Verfahren, bei dem im Transportfahrzeug Aufkleber, Aushänge oder Kärtchen (ca. DIN A6 oder A7) bereitgehalten werden, auf denen informiert wird über den Verantwortlichen, die Kontaktdaten des Datenschutzbeauftragten, die Zwecke der Verarbeitung und die Rechtsgrundlage sowie die Quelle, unter der die vollständigen Informationen eingesehen werden können (z. B. Hinweis auf eine Internetseite). Aufkleber, Aushänge oder Kärtchen sollten so platziert werden, dass die transportierte Person sie sehen und sich ggf. eines der Kärtchen mitnehmen kann. Nach Möglichkeit sollte ein Hinweis darauf erfolgen.

Aber auch der Volltext der Datenschutzinformationen sollte vorgehalten werden, z. B. als Flyer. Der betroffenen Person sollte dann mitgeteilt werden (telefonisch, mündlich oder auf dem Aufkleber/Aushang/Kärtchen), dass sie sich diese Papierversion im Beförderungsfahrzeug zum Mitnehmen aushändigen lassen kann. Falls die transportierte Person ohnehin Schriftstücke erhält (z. B. das Rettungsdienstprotokoll), sollten ihr die Datenschutzinformationen stets mit ausgehändigt werden.

Dem Argument des geprüften Unternehmens, dass kein anderes Beförderungsunternehmen derartige Anforderungen erfüllen würde, konnte der Landesbeauftragte öffentlich zugängliche Beispielinformationen großer Leistungserbringer im Krankentransport- und Rettungswesen entgegenhalten. Diese können zugleich Formulierungshilfen für die Informationen kleiner Unternehmen bieten.

Es ist nicht zulässig, dass Leistungserbringer im Krankentransport- und Rettungswesen den betroffenen Personen die datenschutzrechtlichen Informationen nach Art. 13, 14 DS-GVO gar nicht bereitstellen. Praxisnahe Lösungen, die den besonderen Zustand der beförderten Personen berücksichtigen, sind möglich.

23 Beschäftigtendatenschutz

23.1 Beschäftigtendatenschutzgesetz

Schon seit den 80er Jahren besteht das Bedürfnis, den Umgang mit Beschäftigtendaten im Arbeitsverhältnis ausgewogen zu regeln, u. a. geltend gemacht vom Bundestag, Bundesrat, den Datenschutzaufsichtsbehörden des Bundes und der Länder und den Gewerkschaften. 2010 wurde ein Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes in den Bundestag eingebracht. Dieser fiel jedoch der Diskontinuität zum Opfer. Inzwischen hat die sich dynamisch entwickelnde Digitalisierung tiefgreifende Veränderungen in der Arbeitswelt bewirkt. Dies führt zu vielfachen datenschutzrechtlichen Fragestellungen, denen die bisherige rechtliche Ausgestaltung nicht mehr gerecht wird. Im Zeitalter der Digitalisierung muss ein hohes Datenschutz-niveau und Rechtsklarheit für alle Akteure der Arbeitswelt gewährleistet werden. Es bedarf eines angemessenen Ausgleichs zwischen den grundrechtlich geschützten Interessen der Arbeitgeberseite sowie dem Grundrecht auf informationelle Selbstbestimmung der Beschäftigten. Auszugestalten wären u. a. die Bereiche des Einsatzes algorithmischer Systeme einschließlich Künstlicher Intelligenz, der Grenzen der Verhaltens- und Leistungskontrolle, der Datenverarbeitungen auf Grundlage von Kollektiv-vereinbarungen und Einwilligungserklärungen, der Datenverarbeitung bei Bewerbungs- und Auswahlverfahren und die Frage des Beweisverwertungsverbots für rechtswidrig verarbeitete Beschäftigtendaten. Auch der Beirat Beschäftigtendatenschutz des Bundesministeriums für Arbeit und Soziales hat den Gesetzgeber aufgerufen, spezifische Regelungen zum Beschäftigtendatenschutz zu schaffen. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat hierzu die Entschließung vom 04. Mai 2022 „Die Zeit für ein Beschäftigtendatenschutzgesetz ist „Jetzt“!“ gefasst.[43]

23.2 Verarbeitung von Mitarbeiterdaten im Callcenter

In einer Eingabe wurde gerügt, dass für die Wohnraumarbeit in einem großen Callcenter vorausgesetzt würde, dass am Bildschirm eine Kamera angeschlossen wird. Zudem finde darüber hinaus über elektronische Tools eine umfassende Überwachung statt. Der Landesbeauftragte hat den Vorgang aufgegriffen und u. a. in sehr umfangreichem Schriftverkehr die Hintergründe zur Kamera am heimischen Arbeitsplatz und die einzelnen Datenerfassungen mit dem Unternehmen erörtert und datenschutzrechtliche Hinweise gegeben.

Das Unternehmen hatte zur Begründung wie folgt argumentiert. Die Videokamera erfasse mit der speziellen Software in einem stundenweisen Rhythmus allein die Identität

[43] https://www.datenschutzkonferenz-online.de/media/en/Entschliessung_Forderungen_zum_Beschaeftigtendatenschutz.pdf

des Beschäftigten, um sicherzustellen, dass keine betriebsfremden Personen Zugriff auf die Firmendaten hätten. Referenzbilder, die in Templates umgewandelt werden, würden auf den Servern der Anbieterfirma gespeichert und zur Authentifizierung abgeglichen. Damit sollten nicht nur die Kundendaten geschützt, sondern auch unberechtigte Transaktionen durch Dritte verhindert werden. Es werde nur die Identität, nicht aber die Arbeitsleistung kontrolliert. Die kameratechnische Überwachung der Authentizität werde von einigen Kunden (u. a. sehr große, europaweit tätige Telekommunikationsunternehmen) verlangt. Zudem sei die Möglichkeit, zu Hause zu arbeiten, nur ein Angebot. Würde nicht in die Kameranutzung eingewilligt, müsse am Arbeitsplatz im Unternehmen gearbeitet werden.

Da die Erfassung von biometrischen Daten einen erheblichen Eingriff in die Persönlichkeitsrechte der Beschäftigten bedeutet wurden mit dem Unternehmen zahlreiche mildere Alternativen erörtert. Insbesondere vermag ein Kundenwunsch grundsätzlich keine datenschutzrechtlich unzulässige Verarbeitung zu rechtfertigen. Allerdings ist die Möglichkeit zu Hause zu arbeiten eine Befreiung von der grundsätzlichen Pflicht, im Unternehmen zu arbeiten und somit ein Vorteil für die Beschäftigten. Zudem waren notwendige Sicherungsmaßnahmen getroffen. Die Nutzung der Videokamera erschien daher noch vertretbar.

Weiter wurden verschiedene Softwareprodukte vom Unternehmen zur Erfassung von Beschäftigtendaten und zur weiteren Auswertung und Verarbeitung eingesetzt. So gab es u. a. ein System zur sekundengenauen Erfassung von Telefongesprächen, u. a. für Abrechnungszwecke. Ein weiteres System diente der Organisation von Schichtplänen sowie der Berechnung von Lohn und Boni. Ein anderes System erfasste Daten nicht für die Personalabteilung, sondern für die Vorgesetzten zu Zwecken der Prozessoptimierung und für Coachingzwecke. Die Systeme waren auch vernetzt, um einzelne Daten aus einem System für Aufgaben in einem anderen System verwenden zu können. Die Verarbeitungen waren in einer Betriebsvereinbarung enthalten und somit schon einer gewissen Prüfung unterzogen. Zu den einzelnen Datenerfassungen konnte das Unternehmen darlegen, für welche konkreten Zwecke diese notwendig sind (z. B. Telefoniezeiten aus einem System für vertraglich vereinbarte zeitgenaue Bearbeitung im Abrechnungssystem, teambezogene Auswertungen für Schulungszwecke). Auch wurde dargelegt, wie letztlich im Interesse der Datenminimierung der zugriffsberechtigte Personenkreis gesteuert wird. Deshalb war es trotz des erheblichen Verarbeitungsumfangs nicht ohne weiteres möglich, von einer unverhältnismäßigen und damit unzulässigen Überwachung auszugehen. Das Unternehmen ist aber auf diverse grenzwertig umfängliche Erfassungen hingewiesen worden, die ggf. in Einzelfällen zu einer unzulässigen Erfassung und Verarbeitung führen könnten. Empfehlungen zur Verbesserung der Zugriffsberechtigungen nach dem Need-to-know-Prinzip wurden gegeben.

Weiter fand ein Monitoring (Aufzeichnung von Gesprächen und deren Auswertung) statt. Je Callcenter-Agent wurden transparent in einer Woche des Monats nur einzelne Tage erfasst und nur wenige Gespräche aufgezeichnet, von denen wiederum nur einzelne zur Auswertung kommen. Im Ergebnis wurden jeweils weniger als ein Prozent der Gespräche ausgewertet. Dagegen bestehen keine Bedenken. Da die Aufzeichnungsphasen in etwa einem Viertel der Jahresarbeitszeit entsprachen wurde aber empfohlen, zumindest die Anzahl der erfassten Arbeitstage zu reduzieren.

23.3 Mithören von Telefongesprächen

Aufgrund einer Presseveröffentlichung wurde dem Landesbeauftragten bekannt, dass eine Bürgermeisterin die IT-Abteilung der Stadt beauftragt habe, eine Vorrichtung zum Mithören von Telefongesprächen der Mitarbeiter einzurichten. Im Ergebnis war hinsichtlich des Sachverhaltes festzustellen, dass ein Verfahren geschaffen werden sollte, die Amtsleiter in dringenden Fällen über die Telefonanlage kontaktieren zu können, während diese Telefongespräche führen. Damit sollte für dringende Fälle die Möglichkeit eröffnet werden, den Amtsleitern während eines Telefonates zu signalisieren, dass seitens der Bürgermeisterin ein sofortiger Gesprächsbedarf bestehe. Eine entsprechende Einwahl in Telefongespräche vom Apparat der Bürgermeisterin aus war grundsätzlich für vier Tage möglich. Nach Äußerung von Bedenken durch den behördlichen Datenschutzbeauftragten wurde die Einwahlmöglichkeit deaktiviert. Die Funktion selber wurde nicht genutzt, da keine vollständige Einweisung erfolgte. Sofern eine Einwahl in ein Gespräch mit zwei internen Teilnehmern erfolgt wäre, wäre eine Telefonkonferenz mit drei Teilnehmern entstanden, die durch optische und akustische Signale auf diese Telefonkonferenz hingewiesen worden wären. Sofern eine Einwahl in ein Gespräch mit einem internen und einem externen Gesprächsteilnehmer erfolgt wäre, wäre der externe Teilnehmer während der Hinzuschaltung der Bürgermeisterin stumm geschaltet worden. Ein Mithören von Telefongesprächen wäre daher vom Apparat der Bürgermeisterin nur bei Telefongesprächen zwischen zwei internen Gesprächsteilnehmern grundsätzlich möglich gewesen. Ob und inwieweit die optischen und akustischen Signale hinreichend vernehmbar waren und wie lange ein Mithören wohl gedauert hätte, war nicht hinreichend klärbar.

Sofern jedoch ein Einwählen erfolgt wäre, hätte hierfür eine Rechtsgrundlage für die Datenverarbeitung vorliegen müssen. Insoweit wäre an Art. 6 Abs. 1 Satz 1 lit. e DS-GVO in Verbindung mit Art. 6 Abs. 3 Satz 1 lit. b DS-GVO und § 4 Satz 1 DSAG LSA zu denken. Dies hätte jedoch stets die Erforderlichkeit der konkreten Maßnahme des Mithörens zur Erfüllung etwaiger öffentlicher Aufgaben der Bürgermeisterin vorausgesetzt. Dies war nicht ersichtlich. Die Erforderlichkeit wäre nicht schon dann gegeben, wenn die Maßnahme irgendwie dienlich oder förderlich gewesen wäre. Voraussetzung ist vielmehr, dass es zur beabsichtigten Art und Weise der Datenverarbeitung keine sinnvolle oder zumutbare Alternative gibt, um die jeweils verfolgte Zielsetzung zu erreichen. Zweifelsohne existieren zur Einwahl in ein laufendes Telefonat alternative Möglichkeiten, um dem jeweils Sprechenden erfolgversprechend zu signalisieren, dass die Bürgermeisterin aktuellen Gesprächsbedarf hat (z. B. lauter Anrufton und Dienstanweisung, dass dies nur von der Bürgermeisterin veranlasst werden darf). Eine Rechtsgrundlage für die Datenverarbeitung im Rahmen des Mithörens von internen Telefongesprächen bestand daher nicht. Sofern eine entsprechende Datenverarbeitung stattgefunden hätte, wäre diese somit rechtswidrig erfolgt.

Aufgrund des kurzen Zeitfensters der Einrichtung und der Tatsache, dass eine Datenverarbeitung durch ein Mithören praktisch nicht erfolgte, hat der Landesbeauftragte keine aufsichtsrechtlichen Maßnahmen ergriffen. Die Bürgermeisterin wurde jedoch nochmals ausdrücklich darauf hingewiesen, dass eine entsprechende Datenverarbeitung rechtswidrig wäre. Der Landesbeauftragte hat daher dringend empfohlen, zukünftig Anweisungen an Beschäftigte, die gegebenenfalls eine personenbezogene Datenverarbeitung von Beschäftigten beinhalten, konkret und schriftlich zu verfassen. Darüber hinaus sollte sichergestellt werden, dass der behördliche Datenschutzbeauftragte

gemäß Art. 37 Abs. 1 lit. a DS-GVO in Verbindung mit § 19 Abs. 1 DSAG LSA frühzeitig einbezogen wird.

24 Kommunales und Meldewesen

24.1 Automatisierte Meldedatenabrufe

Aufgrund eines medienwirksamen Missbrauchsfalles unzulässiger Meldedatenabrufe zu privaten Zwecken hatte sich der Landesbeauftragte mit der Frage zu befassen, wie bei automatisierten Meldedatenabrufen eine effektive datenschutzrechtliche Kontrolle gewährleistet werden kann.

Gemäß § 39 Abs. 3 Bundesmeldegesetz (BMG) ist den in § 34 Abs. 4 Satz 1 BMG genannten Sicherheitsbehörden sowie weiteren durch Bundes- oder Landesrecht bestimmten öffentlichen Stellen zu jeder Zeit der automatisierte Abruf von Meldedaten zu ermöglichen. Gewährleistet wird der länderübergreifende automatisierte Abruf in Sachsen-Anhalt über den zentralen Meldedatenbestand bei Dataport A. ö. R. gemäß § 2 ff. des Ausführungsgesetzes des Landes Sachsen-Anhalt zum Bundesmeldegesetz (BMG-AG LSA) und der Verordnung zum Zentralen Meldedatenbestand des Landes Sachsen-Anhalt (ZMDB-VO LSA). Die Protokollierung für die Meldebehörden gemäß § 40 Abs. 1 BMG übernimmt Dataport A. ö. R. ebenfalls. Länderübergreifende Rechtsgrundlage ist die Verwaltungsvereinbarung zum länderübergreifenden automatisierten Abruf von Meldedaten nach den §§ 38, 39 BMG über zentrale Stellen.

Gemäß § 34a Abs. 2 Satz 1 BMG dürfen alle Daten nach § 34 Abs. 1 Satz 1 abgerufen werden. Die in § 34 Abs. 4 Satz 1 genannten Sicherheitsbehörden dürfen gemäß § 34a Abs. 2 Satz 2 BMG zusätzlich auch die Daten nach § 34 Abs. 1 Satz 2 abrufen. Hierfür können sich alle öffentlichen Stellen des Landes i. S. d. § 2 Abs. 2 Datenschutz-Grundverordnungs-Ausfüllungsgesetz Sachsen-Anhalt (DSAG LSA) registrieren lassen. Über die Berechtigung zum automatisierten Abruf von Meldedaten entscheidet gemäß § 4 Abs. 3 Satz 2 ZMDB-VO LSA das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt.

Für die Kontrolle der Meldedatenabrufe trifft § 39 Abs. 4 Satz 1 BMG eine Verantwortungszuweisung an die abrufende Stelle. Zwar kann auch der Landesbeauftragte für den Datenschutz entsprechende Kontrollen durchführen. Allein die Menge der Abrufe macht eine wirksame Kontrolle durch ihn aber praktisch unmöglich. Die Aufsichtsbehörde hat schlichtweg nicht die personellen Kapazitäten, derartige Kontrollen stichprobenhaft für alle öffentlichen Stellen des Landes durchzuführen. Die Kontrolle muss vorrangig durch die abrufende Stelle selbst stattfinden.

Da der Abruf über eine Webapplikation bereitgestellt wird, mithin über die zur Verfügung gestellten Zugangsdaten jederzeit an jedem Ort möglich ist, stellt die Kontrolle die verantwortliche Stelle vor einige Herausforderungen. Maßnahmen in Bezug auf das tätige Personal (sorgfältige Auswahl, Belehrungen, Dienstanweisungen etc.) dürften daher flankierend einzurichten sein, um einen Missbrauch zu vermeiden.

Der Landesbeauftragte hatte mehrfach mit dem MI erörtert, wie eine effektivere Kontrolle gewährleistet werden könne. Die vom Landesbeauftragten zunächst präferierte

Schaffung einer landesrechtlichen Regelung zum Protokollzugriff für die abrufenden Stellen ließ sich hierbei leider nicht realisieren.

Das MI hat alle Accounts deaktiviert und anschließend unter erheblichen Einschränkungen neu vergeben. Je öffentlicher Stelle wird nur noch ein Administrator-Account und ein Vertreter zugelassen. Damit werde den gesteigerten Sicherheits- und Datenschutzanforderungen Genüge geleistet.

Der Landesbeauftragte wird zunächst die Wirksamkeit der Neuregelung des MI beobachten und bewerten. Als erfolgversprechendstes Mittel wird nach wie vor eine Stichprobenkontrolle der – ohnehin bereits vorhandenen – Protokolldatensätze durch die abrufenden Behörden erachtet. Hierfür bedürfte es allerdings der Schaffung einer landesrechtlichen Regelung. Der Landesbeauftragte selbst hat nicht die personellen Kapazitäten, derartige Kontrollen stichprobenhaft für alle öffentlichen Stellen des Landes durchzuführen.

25 Verwaltung allgemein

25.1 Zensus 2022

Wie bereits im XVII. Tätigkeitsbericht (Nr. 15.1) berichtet, war turnusgemäß für den 16. Mai 2021 ein Zensus – also eine Volks-, Gebäude- und Wohnungszählung – vorgesehen, die aufgrund der Corona-Pandemie jedoch um ein Jahr auf den 15. Mai 2022 verschoben werden musste. Der Zensus 2022 wurde registergestützt durchgeführt und umfasste vier Erhebungsteile (Bevölkerungszählung, Gebäude- und Wohnungszählung, Haushaltebefragung auf Stichprobenbasis, Erhebungen an Anschriften mit Sonderbereichen).

Damit europaweit einheitliche Grunddaten über die Bevölkerung und die Wohnsituation verfügbar sind, sind die Mitgliedstaaten nach der Verordnung (EG) Nr. 763/2008 über Volks- und Wohnungszählungen verpflichtet, alle zehn Jahre einen Zensus durchzuführen. Die nationalen gesetzlichen Regelungen für den Zensus 2022 finden sich im Bundesstatistikgesetz (BStatG) und im Zensusgesetz 2022 (ZensG 2022). Die Auskunftspflicht ergibt sich aus § 15 BStatG i. V. m. § 23 ZensG 2022. Kommen Befragte ihrer Auskunftspflicht nicht nach und verweigern die Teilnahme am Zensus 2022, stellt dies eine Ordnungswidrigkeit dar, die mit einer Geldbuße geahndet werden kann (siehe § 23 Abs. 1 BStatG).

Die beim Zensus 2022 erhobenen Daten unterliegen dem Statistikgeheimnis bzw. der statistischen Geheimhaltung gem. § 16 Abs. 1 BStatG. Alle an der Organisation und Durchführung des Zensus 2022 beteiligten Personen werden auf das Statistikgeheimnis verpflichtet. Verstöße dagegen sind strafbar und werden entsprechend verfolgt.

Außerdem gibt es ein sogenanntes Rückspielverbot. Das bedeutet, dass bearbeitete Einzeldatensätze, die noch einen Personenbezug aufweisen, von den Statistischen Ämtern nicht an die Stellen „zurückgespielt“ werden dürfen, von denen die Ursprungsdaten stammen. Auch eine Weitergabe von Daten mit Personenbezug an sonstige Stellen und Behörden erfolgt nicht. Der Zweckbindungsgrundsatz nach Art. 5 Abs. 1

lit. b DS-GVO verhindert zudem, dass die für den Zensus erhobenen Daten nachträglich für andere Zwecke verwendet werden können. Dies wäre rechtlich unzulässig.

Bei den im Zensus 2022 erhobenen Einzelangaben handelt es sich zunächst um personenbezogene Daten. Deshalb ist es besonders wichtig, die Vertraulichkeit und Integrität dieser Daten zu gewährleisten. Allerdings werden die „Hilfsmerkmale“, wie z. B. Name und Anschrift der Auskunftspflichtigen, von den für die Ergebnisse des Zensus relevanten Daten („Erhebungsmerkmale“) frühestmöglich getrennt. Die Weiterverarbeitung und die Auswertung der Zensus-Ergebnisse erfolgen dann auf Basis der anonymisierten Daten.

Gemäß § 7 Abs. 1 Zensusausführungsgesetz Sachsen-Anhalt 2022 (ZensAG 2022 LSA) haben die örtlichen Erhebungsstellen die für die Durchführung des Zensus 2022 benötigten Erhebungsbeauftragten anzuwerben, auszuwählen, zu bestellen, auf die Wahrung des Statistikgeheimnisses und des Datengeheimnisses schriftlich zu verpflichten und sie über ihre Rechte und Pflichten zu belehren. Die Bestellung eines oder einer Erhebungsbeauftragten darf nicht erfolgen, wenn Tatsachen die Annahme rechtfertigen, dass der oder die Erhebungsbeauftragte nicht die erforderliche Zuverlässigkeit besitzt.

Zur Überprüfung der Zuverlässigkeit kann die örtliche Erhebungsstelle eine unbeschränkte Auskunft nach § 41 Abs. 1 Nr. 9 des Bundeszentralregistergesetzes einholen. Die örtliche Erhebungsstelle kann darüber hinaus eine Stellungnahme der für den Wohnort der Bewerberin oder des Bewerbers zuständigen Behörde der Landespolizei, einer zentralen Polizeidienststelle oder des Landeskriminalamts einholen, soweit dies zur Überprüfung der Zuverlässigkeit erforderlich ist.

Gemäß § 20 Abs. 1 ZensG 2022 dürfen Erhebungsbeauftragte außerdem nicht in der unmittelbaren Nähe ihrer Wohnung eingesetzt werden, um zu vermeiden, dass sie ihnen bekannte Personen befragen.

25.2 Zensus 2022 – Beschwerden

Den Landesbeauftragten erreichten während der Haushaltsbefragung und der Wohnungs- und Gebäudezählung mehrere Beschwerden darüber, dass im Rahmen des Zensus 2022 einige Rechte aus der DS-GVO eingeschränkt wurden und zwar das Auskunftsrecht nach Artikel 15, das Recht auf Berichtigung nach Artikel 16, das Recht auf Einschränkung der Verarbeitung nach Artikel 18 und das Widerspruchsrecht nach Artikel 21 DS-GVO.

Die Petenten wollten wissen, warum ihre Rechte im Rahmen des Zensus 2022 derart eingeschränkt wurden. Außerdem kritisierten sie, dass in Deutschland nur 8 Bundesländer die Betroffenenrechte ausgeschlossen haben und diese in 4 Bundesländern eingeschränkt wurden. Durch die unterschiedlichen Regelungen sahen sie sich als Bewohner des Landes Sachsen-Anhalt deutlich benachteiligt und diskriminiert.

Der Ausschluss der Betroffenenrechte ergibt sich aus § 9 Satz 1 Zensusausführungsgesetz Sachsen-Anhalt 2022 (ZensAG 2022 LSA) i. V. m. Art. 89 Abs. 2 DS-GVO.

Art. 89 Abs. 2 DS-GVO besagt unter anderem, dass bei der Verarbeitung personenbezogener Daten zu statistischen Zwecken im Recht der Mitgliedsstaaten Ausnahmen

von den Rechten gemäß der Art. 15, 16, 18 und 21 vorgesehen werden können, wenn diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind.

Da die genannten Rechte die Durchführung des Zensus 2022 beeinträchtigen würden, wurde in § 9 Satz 1 ZensAG 2022 LSA festgelegt, dass zum Schutz der fristgemäßen und vollständigen Durchführung des Zensus 2022 die Rechte gem. Art. 15, 16, 18 und 21 DS-GVO nicht bestehen.

Basierend auf dem Zensusgesetz 2022 haben die Bundesländer eigene Zensusausführungsgesetze erlassen, wie das in Sachsen-Anhalt mit dem ZensAG 2022 LSA der Fall ist. Da es sich hierbei um Landesrecht handelt, entscheiden die einzelnen Landesparlamente unabhängig über die Gesetzesinhalte, sodass die Regelungen in den Bundesländern unterschiedlich sein können.

25.3 Beratungsanfragen Onlinezugangsgesetz (OZG)

Das Ministerium für Wirtschaft, Wissenschaft und Digitalisierung hatte sich Mitte 2020 mit einem Datenschutzkonzept für einen Online-Antragsassistenten BAföG Digital nebst Entwurf einer Verwaltungsvereinbarung für alle Bundesländer an den Landesbeauftragten mit der Bitte um Prüfung und Abnahme gewandt.

Da dies eine der ersten OZG-Anwendungen war, die für die sogenannte Nachnutzung durch andere Bundesländer vorgesehen war, hatte der Landesbeauftragte die Gründung einer Arbeitsgruppe unter Beteiligung der anderen Aufsichtsbehörden angeregt, im Rahmen derer die datenschutzrechtlichen Problemstellungen gemeinsam besprochen und abgestimmt werden konnten. Insbesondere im Hinblick auf die Zuweisung der datenschutzrechtlichen Verantwortlichkeit gab es erheblichen Klärungsbedarf, der im Ergebnis auf Druck der Aufsichtsbehörden auf Bundesebene zur Einführung einer gesetzlichen Regelung im OZG führen wird.

Der Landesbeauftragte hatte im letzten Jahr eine Vielzahl von Beratungsanfragen aus den obersten Landesbehörden und Kommunen zu verzeichnen, die die Umsetzung weiterer OZG-Projekte in der Nachnutzung betraf. Hierbei stellten sich immer wieder dieselben Fragen hinsichtlich der datenschutzrechtlichen Verantwortlichkeit, der Nutzungsmöglichkeit von Verwaltungsvereinbarungen oder der Notwendigkeit von Auftragsverarbeitungsverträgen einschließlich deren Ausgestaltung.

Der Landesbeauftragte konnte unter Nutzung der Erfahrungen aus der geschaffenen Arbeitsgruppe wesentliche Hilfestellungen leisten. Eine abschließende Rechtssicherheit wird allerdings erst nach der anvisierten Änderung des OZG zu erwarten sein.

26 Wirtschaft

26.1 Meldungen von Datenschutzverletzungen

Die Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden nach bekanntwerden gemäß Art. 33

DS-GVO der Aufsichtsbehörde, es sei denn, dass diese Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Im Berichtszeitraum wurden insbesondere folgende Verletzungen häufig gemeldet:

- Irrtümliche Versendung von Briefpost an Nichtberechtigte,
- Versendung von E-Mails an Nichtberechtigte,
- Kompromittierung von Datenbeständen durch Cyberangriffe,
- Unberechtigte Zugriffe von Beschäftigen auf Kundendaten zu privaten Zwecken.

Die Meldefrist von 72 Stunden wurde häufiger überschritten, teilweise sogar um mehrere Wochen. Verantwortliche müssen durch technische und organisatorische Maßnahmen sicherstellen, dass die Datenschutzverletzung zügig an die Aufsichtsbehörde gemeldet wird. Wird die Frist von 72 Stunden überschritten, so ist die Verzögerung zu begründen.

Nach einem Cyberangriff auf einen Abrechnungsdienstleister waren in Sachsen-Anhalt über 20 Unternehmen betroffen. Die Daten sollen im Darknet veröffentlicht worden sein. Allerdings waren lediglich alte Datenbestände betroffen. Ein hohes Risiko bestand nicht.

Durch eine Bank wurden Zugangsdaten für das Online-Banking per unverschlüsselter E-Mail an einen unberechtigten Dritten versandt, welcher sich als angeblicher Bankkunde ausgegeben hatte. Dieser erhöhte das Online-Banking-Limit und verschaffte sich 20.000 € von dem fremden Konto.

Informationen und Hinweise des Landesbeauftragten zu Datenschutzverletzungen finden sich auf einem Informationsblatt „Häufige Ursachen von Datenschutzverletzungen und Abwehrmaßnahmen“[44] und in dem Informationspaket „Informationen für kleine und mittlere Unternehmen (KMU)“.[45]

26.2 Datenschutzrechtliche Verantwortung in Konzernstrukturen

In einer Datenschutzüberprüfung im Berichtszeitraum war dem Landesbeauftragten bekannt geworden, dass in einer Unternehmensgruppe, einem Konzern, insgesamt neun konzernangehörige Tochtergesellschaften unter der Beherrschung der Muttergesellschaft tätig waren. Es bestand je eine Tochtergesellschaft für die einzelnen Geschäftsfelder des Konzerns. Von Beginn der Geschäftstätigkeit an galt ein Beherrschungs- und Ergebnisabführungsvertrag aller Unternehmen zugunsten der Muttergesellschaft.

Die Geschäftsführung der Muttergesellschaft war mit denen der Tochtergesellschaften weitgehend personenidentisch. Die Tochterunternehmen beschäftigten kaum eigenes

[44] https://lsaurl.de/BspDSVer

[45] https://lsaurl.de/InfopaketKMU

Personal, allenfalls wenige Personen, die spezielle technische Tätigkeiten für den jeweiligen Geschäftsbereich ausübten. Beinahe die gesamte Geschäftstätigkeit für alle Tochterunternehmen führte faktisch das Personal der Muttergesellschaft durch. Dem lag zivilrechtlich ein Dienstleistungsvertrag zugrunde. Die Muttergesellschaft und ihre Beschäftigten waren für sämtliche darin genannten Angelegenheiten bevollmächtigt.

Gleichzeitig war die jeweils zuständige Tochtergesellschaft zivilrechtlich Vertragspartnerin der Kunden für die von ihnen in Anspruch genommene Leistung. Sie wurde auch in den Informationen nach Art. 13 DS-GVO als Verantwortliche nach Art. 4 Nr. 7 DS-GVO benannt. In der Kommunikation mit den betroffenen Personen und auch mit dem Landesbeauftragten trat jedoch nur die Muttergesellschaft in Erscheinung.

Dies führte zu der Nachfrage des Landesbeauftragten, wie die Verantwortlichkeiten für die Datenverarbeitungen im Konzern ausgestaltet sind. Zunächst ging der Konzern von einer Auftragsverarbeitung durch die Muttergesellschaft für die Tochtergesellschaften aus. Dies war jedoch in Anbetracht der sehr weitreichenden eigenen fachlichen Leistungen der Muttergesellschaft, der Auslegungsspielräume in den Verträgen und auch der gesellschaftsrechtlichen Verhältnisse zwischen den beteiligten Unternehmen zweifelhaft. Für eine Auftragsverarbeitung müssten sich auch die Weisungsbefugnisse und Kontrollrechte der Tochtergesellschaften in den tatsächlichen Verhältnissen widerspiegeln.

Nach einer sehr intensiven Prüfung, auch unter Beteiligung eines während dieser Prüfung benannten externen Datenschutzbeauftragten, kam der Konzern zu dem Ergebnis, dass es sich weitgehend um eine gemeinsame Verarbeitung der Tochtergesellschaften mit der Muttergesellschaft handelt. Es war eine Vereinbarung gemäß Art. 26 DS-GVO abzuschließen, aus der die Zwecke der und die Mittel zur Verarbeitung hervorgehen, die die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegelt und die in transparenter Form festlegt, welcher Verantwortliche welche Verpflichtung gemäß der DS-GVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Personen angeht. Der Konzern hat anschließend das wesentliche dieser Vereinbarung nach Art. 26 DS-GVO den betroffenen Personen zur Verfügung gestellt, seine Informationen nach Art. 13 DS-GVO entsprechend angepasst und dabei auch eine Anlaufstelle für die betroffenen Personen angegeben (Art. 26 Abs. 1 Satz 3 DS-GVO).

Im Ergebnis der Datenschutzüberprüfung, bei der auch weitere Verstöße gegen die DS-GVO festgestellt werden mussten, erteilte der Landesbeauftragte der Muttergesellschaft eine Verwarnung nach Art. 58 Abs. 2 lit. b DS-GVO und setzte die Kosten des Verfahrens fest.

26.3 Digitale Schließsysteme in vermieteten Mehrfamilienhäusern

Aufgrund einer Beschwerde prüfte der Landesbeauftragte im Jahr 2022, unter welchen Bedingungen der Einsatz eines digitales Schließsystems in vermieteten Mehrfamilienhäusern auf der Grundlage der Interessenabwägungsklausel des Art. 6 Abs. 1 Satz 1 lit. f DS-GVO datenschutzrechtlich zulässig ist.

Ein Wohnungsunternehmen hatte eine erhebliche Anzahl mutmaßlicher Einbruchsdiebstähle in Keller und Gemeinschaftsräume zu verzeichnen und im Einzelnen dokumentiert. Daraus waren hohe Schäden für das Unternehmen selbst (für Reparatur oder Austausch von Türen, Austausch von Schlüsseln, Schließzylindern oder ganzen Schließanlagen), aber auch für die Mieterschaft entstanden (z. B. durch Diebstahl von Fahrrädern, Werkzeug, Technik). Digitale Schließsysteme sollten zur Vermeidung von Einbrüchen beitragen, denn bei Verlust oder Diebstahl von Transpondern können diese sehr zügig deaktiviert werden, sodass der Zutritt zu den Gebäuden mithilfe dieser Transponder nicht mehr möglich ist. Wenn dennoch ein Einbruch stattgefunden hat, sollten die LOG-Daten aus den Schließzylindern (das Aufzeichnen der Schließvorgänge) zur Aufklärung des Sachverhalts und zur Strafverfolgung beitragen, denn mit ihrer Hilfe sollten ggf. Rückschlüsse gezogen werden auf die beim Einbruch verwendeten Transponder, deren Herkunft und damit auf mögliche (Mit-)Täter oder Mitwisser.

Jeder Transponder konnte mindestens einer Wohneinheit und (ggf. über Zusatzinformationen) letztlich einer Person zugeordnet werden, sodass es sich um eine Verarbeitung personenbezogener Daten handelte.

Zwar sollten nicht die Wohnungseingangstüren, sondern nur die Haustüren, Kellertüren und Türen an Hofausgängen mit der Transpondertechnik ausgestattet werden. Dennoch könnten mithilfe der LOG-Daten Bewegungsprofile entstehen, die Rückschlüsse auf die Aufenthaltszeiten in der Wohnung und damit die privaten Lebensgewohnheiten der Bewohner ermöglichen.

Gleichzeitig gab das Unternehmen an, dass die LOG-Daten ausschließlich dezentral in den Schließzylindern gespeichert und nur dann ausgelesen werden, wenn es zu einem strafrechtlich relevanten Vorfall gekommen ist. Ein anlassloses Auslesen der Zylinder oder eine Auslesung ohne Bezug zum Zweck der Strafverfolgung schloss das Unternehmen mittels interner datenschutzrechtlicher Prüfprozesse aus. Auch der externe Datenschutzbeauftragte hat eine Prüfung der Auslesevorgänge der LOG-Daten in seinen Prüfplan aufgenommen. Ein Auslesen der LOG-Daten durch Unbefugte war durch technische und organisatorische Maßnahmen ausgeschlossen. Das Zusammenführen der Daten zu Bewegungsprofilen war nach Angaben des Unternehmens ausdrücklich nicht Zweck der Datenverarbeitung.

Nach aufsichtsbehördlicher Beratung reduzierte das Unternehmen die Speicherfrist von 90 auf 30 Tage. Angesichts der von dem Unternehmen dokumentierten üblichen Zeitabläufe zwischen einem Einbruch und dem Anfordern der LOG-Daten durch die Strafverfolgungsbehörden hielt der Landesbeauftragte diese Frist für vertretbar, gab dazu allerdings den Hinweis, dass in regelmäßigen Abständen zu prüfen ist, ob die Datenverarbeitung die Rechtmäßigkeitsvoraussetzungen noch immer erfüllt. Insbesondere die Frage der Geeignetheit und Erforderlichkeit - auch von einzelnen Verarbeitungsschritten - sollte periodisch evaluiert werden. Wenn beispielweise das digitale Schließsystem präventiv derart wirksam ist, dass über einen längeren Zeitraum keine weiteren aufklärungsbedürftigen Einbrüche aufgetreten sind bzw. die Strafverfolgungsbehörden keine LOG-Daten angefordert haben, sollte die (repressive) Speicherung der LOG-Daten deaktiviert werden. Denn datenschutzrechtlich wäre dann die Speicherung der LOG-Daten nicht mehr erforderlich im Sinne von Art. 6 Abs. 1 Satz 1 lit. f DS-GVO. Diese regelmäßigen Prüfungen sind zu dokumentieren.

Der Landesbeauftragte betonte, dass die datenschutzrechtliche Bewertung für dieses Unternehmen eine Einzelfallentscheidung darstellte. Die Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO fußte auf der besonderen Vorgeschichte bei diesem Unternehmen und der damit verbundenen Gefahrenprognose. Sollte bei einem anderen Wohnungsunternehmen ohne entsprechende Vorgeschichte ein digitales Schließsystem beispielsweise allein zur Prävention oder aufgrund des allgemeinen technischen Fortschritts eingesetzt werden und dann möglicherweise auch noch die (eingriffsintensiveren) Wohnungseingangstüren mit Transpondern ausgestattet und die Daten über einen längeren Zeitraum gespeichert werden, würde die Prüfung sehr wahrscheinlich zu einem anderen Ergebnis führen.

Im Interesse der Datenminimierung sollte zudem vorrangig stets geprüft werden, ob ein solches Schließsystem technisch auch ohne die Verarbeitung personenbezogener (auch nicht pseudonymisierter) Daten auskommt. In einem solchen Fall stünde dem Einsatz jedenfalls die DS-GVO nicht entgegen.

Der Einsatz digitaler Schließsysteme in vermieteten Immobilien kann mit der Verarbeitung personenbezogener Daten einhergehen, wenn die Schließvorgänge mit einem Transponder ggf. über Zusatzinformationen einer bestimmten Person zugeordnet werden können. Bei der Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO ist ein besonderes Augenmerk darauf zu richten, dass die Bewohner der Wohnungen in ihren privaten Lebensgewohnheiten im Wohnumfeld betroffen sind. Eine solche Datenverarbeitung kann nur datenschutzrechtlich zulässig sein, wenn demgegenüber besonders gewichtige berechtigte Interessen des Vermieters stehen und bei der Auswahl und Einrichtung der technischen und organisatorischen Maßnahmen besondere Sorgfalt darauf verwendet wird, den Umfang der Datenverarbeitung und eventuelle technische Risiken zu minimieren.

27 Videoüberwachung und Fotoaufnahmen

27.1 Kinderbilder

Durch eine Beschwerde wurde dem Landesbeauftragten bekannt, dass ein Medienunternehmen eine Gewinnspielaktion durchführt, bei der Fotos von Babys online veröffentlicht werden. Die Veröffentlichung erfolgte zum Teil mit Angabe von Namen, Wohnort und anderen persönlichen Angaben. Die Fotos wurden von Fotografen angefertigt, mit denen entsprechende Vereinbarungen bestanden. Gegenstand der Beschwerde war insbesondere das Fehlen von Informationen nach Art. 13 DS-GVO bei der Anmeldung zu der Aktion.

Im Laufe des Verfahrens stellte der Landesbeauftragte mehrerer Verstöße gegen Art. 6, Art. 12, 13 und Art. 17 DS-GVO fest. Insbesondere fehlten die wirksamen Einwilligungen der Eltern, wesentliche Teile der Informationen nach Art. 13 DS-GVO und die Löschung der Bilder von den eigenen Internetseiten, mindestens für die zurückliegenden zwei Jahre. Insgesamt waren mehrere hundert Bilder betroffen.

Nach dem Hochladen von Fotos auf „offenen“ Internetseiten kann durch anonyme Nutzer weltweit auf die Fotos zu unbestimmten Zwecken zugegriffen werden. Damit ist schon die Veröffentlichung an sich aus vielen Gründen bedenklich. Die gesetzlichen

Anforderungen an die Einwilligung der Eltern steigen mit der Sensibilität der Daten und der Reichweite der Veröffentlichung.

Der Landesbeauftragte hält es deshalb für geboten, die in die Internetveröffentlichung einwilligenden Eltern auch ausdrücklich darüber zu informieren, dass die gegebene Einwilligung später nur für die Internetseite widerrufen werden kann, auf die sie sich einst bezog. Inzwischen könnte eine Fotografie ihres Kindes aber Inhalt anderer unbekannter Internetseiten oder Informationssammlungen geworden sein, auf die das die Einwilligung anfordernde Unternehmen keinerlei Einflussmöglichkeit besitzt.

Die Veröffentlichung von Kinderbildern im Internet ist grundsätzlich bedenklich und von äußerster Sensibilität. Für die Wirksamkeit der erforderlichen Einwilligung beider Elternteile gelten hohe datenschutzrechtliche Anforderungen.

27.2 Gezieltes Fotografieren Fremder an öffentlichen Plätzen

Die Aufsichtsbehörde erreichten im Rahmen der telefonischen Beratung gelegentlich Anfragen zur datenschutzrechtlichen Bewertung des absichtlichen, zielgerichteten und womöglich auch noch heimlichen Fotografierens unbekannter und unbeteiligter Dritter an öffentlichen Plätzen. Es besteht kein Zweifel daran, dass es sich bei solchen Fotos um personenbezogene Daten i. S. v. Art. 4 Nr. 1 DS-GVO handelt, denn die Fotografierten könnten, selbst wenn sie im Moment der Aufnahme vielleicht noch von der Anonymität gedeckt wären, später jedoch die Personen identifizierbar sind. Die datenschutzrechtlich viel interessantere Frage ist die, ob solche Aufnahmen von der sog. Haushalts- bzw. Privatausnahme nach Art. 2 Abs. 1 lit. c DS-GVO erfasst wären, wonach die DS-GVO keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten findet. Das könnte besonders dann hinterfragt werden, wenn der Fotograf die Aufnahmen, z. B. von besonders auffälligen oder von nach seiner Ansicht besonders schönen Menschen, nur zum Erreichen eigener Ziele und Zwecke betrachten oder anders nutzen möchte und nicht beabsichtigt, die Aufnahmen weiterzugeben.

Doch in solchen Fällen greift die Haushaltsausnahme eben nicht. Schon mit dem gezielten Fotografieren einer sich in der Öffentlichkeit aufhaltenden Person wird der von Art. 2 Abs. 1 lit. c DS-GVO geschützte private Bereich verlassen, schließlich befindet sich die Zielperson der Bestrebungen des Fotografen in der Öffentlichkeit. Nach dem Beschluss des AG Hamburg vom 3. Juli 2020 (Az. 163 Gs 656/20) wird eine in der Öffentlichkeit fotografierte Person durch die Anfertigung eines Bildes auch nicht in die Privatsphäre des Fotografen „hineingezogen“.

Zu unterscheiden sind solche gezielten Personenaufnahmen im Übrigen von Aufnahmen im Stil von Urlaubsbildern, auf denen unbeteiligte Dritte als unvermeidliches Beiwerk neben einer touristischen oder sonstigen Sehenswürdigkeit mitabgebildet werden, was von diesen auch ohne weiteres hinzunehmen ist (vgl. Urteil des BGH vom 25. April 1995 – VI ZR 272/94, Rn. 17). Dies gilt bei alltäglichen Gegebenheiten, nicht aber z. B. im FKK-Bereich am Strand. Der Inhaber des Hausrechts in geschlossenen Räumen (z. B. in einem Museum) bestimmen, ob in seinen Räumen fotografiert werden darf.

Durchaus relevant für die Gesamtbewertung von solchen gezielten Personenfotos ist die Tatsache, dass bei diesen Aufnahmen, besonders bei solchen gegen den Willen

der fotografierten Person, ihre Einwilligung vorab nicht eingeholt worden sein wird. Spätestens an dieser Stelle wird deutlich, dass es sich beim Anfertigen solcher Aufnahmen nicht um ein Kavaliersdelikt handelt. Es könnte nämlich nach Art. 83 Abs. 5 DS-GVO ein bußgeldbewehrter Verstoß gegen die Art. 6 (Rechtmäßigkeit der Verarbeitung), 7 (Bedingungen für die Einwilligung) und 13 (Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person) der DS-GVO vorliegen. Auch wenn die Aufsichtsbehörde in einem konkreten Beschwerdefall den vom europäischen Verordnungsgeber in Art. 83 Abs. 5 DS-GVO gesetzten Bußgeldrahmen von 20.000.000 Euro vielleicht nicht vollständig ausschöpfen würde, so hätte sie nach Art. 83 Abs. 1 DS-GVO doch die Pflicht, sicherzustellen, dass die Verhängung der Geldbuße wirksam, verhältnismäßig und abschreckend ist.

An öffentlichen Plätzen ist nach der DS-GVO das gezielte Fotografieren Fremder ohne deren Einwilligung grundsätzlich unzulässig. Rechte anderer dürfen nicht verletzt werden.

28 Bußgeldverfahren

28.1 Statistik der behördlichen Bußgeldverfahren

Datenschutzrechtliche Verstöße kann der Landesbeauftragte mit einer Geldbuße gemäß Art. 83 Abs. 4 bis 6 DS-GVO ahnden (§§ 23 Abs. 5, 31 DSAG LSA i. V. m. § 41 BDSG). In diesem Sinne wurden 20 Bußgeldverfahren eingeleitet. 6 Verfahren wurden eingestellt. 16 Verfahren wurden in 2022 rechtskräftig abgeschlossen.

Die Gesamtsumme der rechtskräftig im Jahr 2022 verhängten Geldbußen aus Verfahren, die auch in Vorjahren begonnen, beläuft sich auf 200.415 Euro:

Tatbestände	Geldbuße insgesamt
Art. 83 Abs. 5 lit. a i. V. m. Art. 6 DS-GVO unzulässige Datenverarbeitung mittels sozialer Medien	168.165 Euro
Art. 83 Abs. 5 lit. a i. V. m. Art. 6 DS-GVO unzulässige Datenverarbeitung durch Nutzung dienstlicher Datenbanken zu privaten Zwecken	1.050 Euro
Art. 83 Abs. 5 lit. b i. V. m. Art. 12, 15 DS-GVO unzureichende Auskunftserteilung	1.500 Euro
Art. 83 Abs. 4 lit. a i. V. m. Art. 25 Abs. 1 DS-GVO unzureichender Datenschutz durch Technikgestaltung	20.700 Euro
Art. 83 Abs. 4 lit. a i. V. m. Art. 33 DS-GVO verspätete Datenpannenmeldung	9.000 Euro

28.2 Bußgelder wegen unzureichender Technikgestaltung beim Web-Tracking nach Art. 25 Abs. 1 DS-GVO

Der Landesbeauftragte verhängte in 2022 rechtskräftige Bußgelder von 9.900 Euro und 22.000 Euro gegenüber zwei Unternehmen, die Internetshops für Computerspiele betreiben für das Fehlen bzw. unzureichende Konfigurieren von „Cookie-Bannern“. In einem Fall hatten Webseitennutzer keine Option, das eingebundene Web-Tracking durch Google und Meta abzuwählen. In dem anderen wurde das Web-Tracking unabhängig von Optionen des „Cookie-Banners“ bereits bei Aufruf der Webseite geladen. Trotz aufsichtsbehördlicher Maßnahmen vergingen mehrere Monate bis ein rechtskonformer Zustand geschaffen wurde.

Die beiden Unternehmen hatten Web-Trackingmechanismen von Google (u. a. Google Analytics) und Meta (Facebook Connect) auf ihren Webseiten eingebunden. Sie waren dabei ihren Pflichten aus Art. 25 DS-GVO, technische und organisatorische Maßnahmen zu ergreifen, um den Anforderungen der DS-GVO zu genügen und die Rechte der betroffenen Personen zu schützen, nicht im ausreichenden Maße nachgekommen. Der Anwendungsbereich des Art. 25 DS-GVO war eröffnet, da die Unternehmen in gemeinsamer Verantwortlichkeit mit Google und Meta personenbezogene Daten der Webseitennutzer (IP-Adresse, Daten zum Betriebssystem, zum Browser sowie zur Art des Endgerätes) verarbeiteten. Die Verantwortlichen sind zwar selbst nicht in der Lage Nutzer zu identifizieren. Laut EuGH (Urteil vom 19. Oktober 2016, Az. C-582/14 (Breyer)) verfügt aber ein Webseitenbetreiber in Deutschland z. B. im Fall von Cyberattacken über rechtliche Mittel, einen Nutzer anhand der gespeicherten IP-Adressen und weiteren Informationen bestimmen zu lassen, so dass die Voraussetzungen für den Personenbezug nach Art. 4 Nr. 1 DS-GVO gegeben sind. Nach Art. 25 Abs. 1 DS-GVO ist bei dem Aufsetzen und späterem Hochladen einer Webseite eine datenschutzkonforme Technikgestaltung bereits im Stadium der Programmierung zu berücksichtigen. Dies betrifft die eigenen Inhalte sowie die Einbindung Dienste Dritter auf der Webseite.

Laut den EDSA-Leitlinien 4/2019 zu Art. 25 DS-GVO soll ein Verantwortlicher nachweisen können, dass er für die Verarbeitung geeignete Maßnahmen ergriffen und Garantien umgesetzt hat, um die Wirksamkeit der Datenschutzgrundsätze zu gewährleisten. Dazu muss der Verantwortliche eine gültige Rechtsgrundlage für die Verarbeitung personenbezogener Daten festlegen. Die Maßnahmen und Garantien sollten die Anforderungen unterstützen und sicherzustellen, dass der gesamte Verarbeitungslebenszyklus im Einklang mit den entsprechenden Rechtsgrundlagen für die Verarbeitung steht. Art. 25 Abs. 1 DS-GVO gibt nicht vor, welche Maßnahmen im Einzelnen zu treffen sind und wie diese konkret umzusetzen sind, vielmehr werden die datenschutzrechtlichen Anforderungen von dem Risiko abhängig gemacht, das von der konkreten Verarbeitung ausgeht. Die Bewertung und Entscheidung, welche Maßnahmen ergriffen werden, obliegen dem Verantwortlichen. Art. 25 DS-GVO gibt lediglich die bei der Abwägungsentscheidung zu berücksichtigenden Faktoren vor. Als technische und organisatorische Maßnahmen und notwendige Garantien können im weiten Sinne alle Methoden oder Mittel verstanden werden, die ein Verantwortlicher bei der Verarbeitung anwenden kann. Den Webseitenbetreiberinnen standen verschiedene Möglichkeiten zur Verfügung, um das Abfließen von Daten von Webseitennutzern an Google

oder Meta zu verhindern, wie z. B. die Auswahl datenschutzkonformer Analysealternativen oder das serverseitige Tracking, das dem Webseitenbetreiber erlaubt, die Daten vor der Weitergabe an Dritte zu anonymisieren.

Das von den webseitenbetreibenden Unternehmen verfolgte Ziel der Implementierung der Dienste von Google und Meta ließe sich nur realisieren, wenn der Webseitennutzer in das Web-Tracking nach Art. 6 Abs. 1 lit a DS-GVO einwilligt hätte. Die Webseiten hätten so programmiert werden müssen, dass die entsprechenden Skripte von Google und Meta nicht mit dem Aufrufen der Webseite, sondern erst nach Abgabe einer Einwilligung geladen werden. Dies erforderte die Programmierung eines Einwilligungsmanagements einschließlich der notwendigen Informationen und eine entsprechende Dokumentation. Die technische Implementierung eines solchen automatisierten Einwilligungsmanagements im Online-Bereich stellt eine typische Maßnahme nach Art. 25 Abs. 1 DS-GVO dar.

SACHSEN-ANHALT

Landesbeauftragte
für den Datenschutz

XX. Tätigkeitsbericht
der Landesbeauftragten für den Datenschutz

2023

29 Der Landesbeauftragte

29.1 Tätigkeit im Berichtszeitraum, Entwicklung des Arbeitsaufkommens – Fallstatistik

Im Jahr 2023 war die Pandemie vorbei. Bestimmte Arbeitsweisen, die zunächst pandemiebedingt eingeführt wurden, hatten sich zwischenzeitlich jedoch etabliert. Das diese veränderten Arbeitsweisen in einem datenschutzrechtlich vertretbaren Rahmen erfolgen, ist Teil der Aufgaben des Landesbeauftragten. So stellten sich ihm Fragen nach der Zulässigkeit des Livestreams von Ratssitzungen (Nr. 41.1) ebenso wie die Nutzung von WhatsApp in der Schule (Nr. 38.4).

Der Landesbeauftragte hat auch regelmäßig wiederkehrende Aufgaben wahrzunehmen. So hat er z. B. aufgrund gesetzlicher Verpflichtung alle zwei Jahre zu kontrollieren, ob durch das Landeskriminalamt Sachsen-Anhalt und die Verfassungsschutzbehörde die datenschutzrechtlichen Vorschriften bei der Verwendung der Antiterror- und der Rechtsextremismusdatei eingehalten werden (Nr. 35).

Zudem hatte sich der Landesbeauftragte im Jahr 2023 auch mit eher ungewöhnlichen Anfragen bzw. Beschwerden zu befassen. Zum einen war zu klären, ob der Landesbeauftragte für Beschwerden betreffend die Religionsgemeinschaft Jehovas Zeugen zuständig ist (Nr. 32.9). Zum anderen war zu klären, ob die stündliche Messung der Feuchtigkeit in einer Mietwohnung aufgrund einer denkmalrechtlichen Auflage auch dazu führt, dass die Messdaten datenschutzrechtlich rechtmäßig erhoben werden dürfen (Nr. 43.6).

In seinen Tätigkeitsberichten stellt der Landesbeauftragte regelmäßig die Anzahl an Posteingängen dar, um einen möglichst objektiven Eindruck von der Entwicklung des Umfangs seiner Tätigkeit zu vermitteln. Im Jahr 2023 war ein nochmal gesteigertes Aufkommen zu verzeichnen.

Anzahl der registrierten Posteingänge:

2016	5.506		
2017	6.737		
2018	9.602	zuzüglich	3.306 Meldungen gem. Art. 37 Abs. 7 DS-GVO
2019	10.941	zuzüglich	746 Meldungen gem. Art. 37 Abs. 7 DS-GVO
2020	13.730	zuzüglich	764 Meldungen gem. Art. 37 Abs. 7 DS-GVO
2021	13.933	zuzüglich	1.351 Meldungen gem. Art. 37 Abs. 7 DS-GVO
2022	13.977	zuzüglich	407 Meldungen gem. Art. 37 Abs. 7 DS-GVO
2023	14.563	zuzüglich	414 Meldungen gem. Art. 37 Abs. 7 DS-GVO

Schwerpunkte seiner Tätigkeit erfasst der Landesbeauftragte über eine Geschäftsstatistik. Innerbehördliche Angelegenheiten (Organisation, Personal, Haushalt) sind nicht erfasst, so dass sich aus der Geschäftsstatistik direkt auf seine Aufsichtstätigkeit schließen lässt. Wesentliche aufsichtsbehördliche Aufgabenfelder im Jahr 2023 waren:

Beschwerden und Eingaben	1.120
Informations- und Beratungsfälle	1.118
Meldungen von Datenschutzverletzungen	366
Abhilfemaßnahmen/Anordnungen	40
Eingeleitete Bußgeldverfahren	5
Europäische Verfahren mit eigener Betroffenheit (Kooperation und Kohärenz)	12
Förmliche Begleitung von Rechtsetzungsvorhaben	24

30 Nationales und Europäisches Datenschutzrecht

30.1 Wahl einer/eines Landesbeauftragten für den Datenschutz

Der Landesbeauftragte für den Datenschutz hatte sich im Berichtszeitraum an den Präsidenten des Landtags von Sachsen-Anhalt gewandt, da Zweifel dahingehend bestanden, ob die rechtliche Ausgestaltung des Wahlverfahrens zum Landesbeauftragten für den Datenschutz den europarechtlich vorgezeichneten Anforderungen entsprechen.

Diskutiert wurde auch, ob der Landesbeauftragte für den Datenschutz hinsichtlich des „eigenen“ Wahlverfahrens überhaupt aufsichtsrechtliche Befugnisse ausüben kann. Insoweit bestanden zwischen dem Landtag und dem Landesbeauftragten für den Datenschutz unterschiedliche Rechtsauffassungen.

Die landesrechtlichen Regelungen entsprechen den europarechtlichen Vorgaben. Insoweit bedurfte es keiner Beanstandung durch den Landesbeauftragten für den Datenschutz.

31 Weitere europäische und internationale Entwicklungen

31.1 Europäischer Datenschutzausschuss

Im Mai 2023 wurde Anu Talus (Leiterin der finnischen Datenschutzaufsichtsbehörde) zur neuen Vorsitzenden des EDSA gewählt. Ihre Amtszeit beträgt fünf Jahre. Sie tritt die Nachfolge von Andrea Jelinek an, die von 2018 bis 2023 den Vorsitz im EDSA geführt hatte. Irene Loizidou Nicolaidou (zyprische Datenschutzbehörde) wurde zur neuen stellvertretenden Vorsitzenden gewählt und löst damit als Nachfolgerin den aus dem Amt scheidenden stellvertretenden Vorsitzenden Ventsislav Karadjov (Bulgarien) ab.

Der Tätigkeit des EDSA liegt im Berichtszeitraum das zweijährige Arbeitsprogramm für die Jahre 2023 und 2024 zugrunde. Dieses basiert auf der EDSA-Strategie für die Jahre 2021-2023, in der sich der EDSA vier Säulen als Arbeitsschwerpunkte vorgegeben hat: Säule I - Förderung der Harmonisierung und Erleichterung der Einhaltung der Vorschriften, Säule II - Unterstützung einer wirksamen Rechtsdurchsetzung und einer effizienten Zusammenarbeit zwischen nationalen Aufsichtsbehörden, Säule III – Ein Grundrechtsansatz für neue Technologien, Säule IV – Die globale Dimension.

Ein Arbeitsauftrag innerhalb der Säule I bestand in der Entwicklung gemeinsamer Instrumente zur Sensibilisierung eines breiteren Publikums für die DS-GVO, insbesondere durch spezielle Informationen für kleine und mittelgroße Unternehmen (KMU). In Erfüllung dieses Auftrags hat der EDSA im April 2023 seinen Datenschutzleitfaden für kleine Unternehmen veröffentlicht. Dieser steht neben Englisch und Französisch auch in deutscher Sprache zur Verfügung. Hierzu hatte der Landesbeauftragte verschiedene, von ihm erstellte Dokumente und Hinweise an den EDSA übermittelt, der diese im Rahmen des Datenschutzleitfadens auf seiner Webseite eingebunden hat. Die Webseite mit dem Datenschutzleitfaden hat der Landesbeauftragte auch auf seiner Webseite zur Information verlinkt.[46]

Darüber hinaus stellt der Landesbeauftragte auf seiner Webseite im „Infopaket KMU“ noch viele weitere Informationen für kleine und mittelgroße Unternehmen bereit.[47]

In Umsetzung der Säule II hat der EDSA im Rahmen der Durchführung jährlicher koordinierter Maßnahmen sog. Coordinated Enforcement Framework (CEF) zu vordefinierten Themen im Berichtszeitraum das Thema „Benennung und Stellung des Datenschutzbeauftragten“ zugrunde gelegt. Das CEF soll den Aufsichtsbehörden die Möglichkeit geben, gemeinsame Maßnahmen zu dem jeweiligen Thema auf flexible, aber koordinierte Weise durchzuführen. In Auswertung des CEF-Berichts sollten die Datenschutzaufsichtsbehörden mehr Aufklärungsmaßnahmen durchführen und die Organisationen dafür sorgen, dass den Datenschutzbeauftragten ein ausreichendes Schulungsangebot zur Verfügung steht. Der Landesbeauftragte legt die Ergebnisse des Berichts seiner künftigen Aufsichts- und Beratungstätigkeit zugrunde.

Im Berichtszeitraum hat der EDSA auf Bitte der Europäischen Kommission hin einen konsolidierten Beitrag aller Datenschutz-Aufsichtsbehörden zum Bericht der Europäischen Kommission nach Artikel 97 (Evaluation der Datenschutz-Grundverordnung) abgegeben. Hierzu hat auch der Landesbeauftragte seinen Beitrag geleistet.

Im Rahmen der in seinem Arbeitsprogramm 2023/2024 festgelegten Aufgaben hat der EDSA im Berichtszeitraum zudem zahlreiche weitere Stellungnahmen und Dokumente verabschiedet, darunter u. a. zwei neue Leitlinien sowie neun Leitlinien im Anschluss an eine öffentliche Konsultation. Da der Ausschuss gegebenenfalls öffentliche Konsultationen interessierter Kreise gem. Art. 70 Abs. 4 der DS-GVO durchführt, werden dafür bestimmte Dokumente nochmals nach Abschluss einer öffentlichen Konsultation beraten. Von den verabschiedeten Dokumenten sind vor allem die nachfolgenden zu erwähnen, die vornehmlich für Betroffene und verantwortliche Unternehmen relevant sein dürften. Diese Dokumente sind zunächst nur in englischer Sprache verfügbar (die Arbeitssprache im EDSA ist Englisch), werden aber im Nachgang auch in die deutsche Sprache übersetzt. Die Leitlinien nach Art. 70 Abs. 1 DS-GVO stellen dabei einen Schwerpunkt der Tätigkeit des EDSA dar. Folgende Dokumente hat der Landesbeauftragte auch auf seiner Webseite verlinkt:[48]

---

[46] https://datenschutz.sachsen-anhalt.de/informationen/infopakete/infopaket-kmu-1#c403684

[47] https://datenschutz.sachsen-anhalt.de/informationen/infopakete/infopaket-kmu

[48] https://datenschutz.sachsen-anhalt.de/informationen/datenschutz-grundverordnung/edsa

- Leitlinien zu trügerischen Designmustern in den Schnittstellen sozialer Medienplattformen: Wie man sie erkennt und vermeidet (Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: How to recognise and avoid them, Version 2.0 adopted after public consultation), nur in Englisch

- Leitlinien zum technischen Anwendungsbereich von Art. 5(3) der Datenschutzrichtlinie für elektronische Kommunikation (Guidelines 02/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, Version for public consultation), nur in Englisch

- Leitlinien zur Meldung einer Datenschutzverletzung nach der DS-GVO (Guidelines 09/2022 on personal data breach notification under GDPR, Version 2.0 after public consultation), nur in Englisch

- Leitlinien zu den Rechten der betroffenen Person – Auskunftsrecht (Guidelines 01/2022 on data subject rights – Right of access, Version 2.1 adopted after public consultation)

- Leitlinien für die Bestimmung der federführenden Aufsichtsbehörde eines Verantwortlichen oder Auftragsverarbeiters (Guidelines 08/2022 on identifying a controller or processor's lead supervisory authority, Version 2.0 after public consultation) - nur in Englisch

- Leitlinien über die Zertifizierung als Instrument für Übermittlungen (Guidelines 07/2022 on certification as a tool for transfers, Version 2.0 adopted after public consultation)

- Leitlinien über die Zertifizierung als Instrument für Übermittlungen (Guidelines 07/2022 on certification as a tool for transfers, Version 2.0 adopted after public consultation)

- Leitlinien über das Zusammenspiel zwischen der Anwendung des Artikels 3 und der Bestimmungen über internationale Übermittlungen nach Kapitel V DS-GVO (Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, Version 2.0 adopted after public consultation)

- Empfehlungen zum Antrag auf Genehmigung und zu den Bestandteilen und Grundsätzen, die in verbindlichen internen Datenschutzvorschriften für für die Verarbeitung Verantwortliche enthalten sein sollten (Art. 47 DS-GVO) (Recommendations 01/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), Version 2.1 adopted after public consultation).

Da die personellen Möglichkeiten des Landesbeauftragten auch im Berichtszeitraum nach wie vor begrenzt sind, kann er sich bislang grundsätzlich nur mittelbar in den Meinungsbildungsprozess des EDSA über die von anderen Aufsichtsbehörden benannten deutschen Vertreter in den verschiedenen Fachuntergruppen des EDSA (Expert Subgroups) einbringen.

31.2 Grenzüberschreitende Verarbeitungen – One-Stop-Shop

Der Landesbeauftragte hat im Berichtszeitraum jeden Eingang zu einer grenzüberschreitenden Verarbeitung auf seine Betroffenheit nach Art. 4 Nr. 22 DS-GVO geprüft. Im Berichtszeitraum betraf dies allein zu sog. grenzüberschreitenden Beschwerden 633 Eingänge, also eine Steigerung gegenüber dem Berichtszeitraum 2022 (579 Eingänge). Dazu kommt eine Vielzahl statistisch nicht gesondert erfasster Eingänge anderer Datenschutzaufsichtsbehörden mit grenzüberschreitendem Bezug.

Der Landesbeauftragte hat sich im Berichtszeitraum in 12 grenzüberschreitenden Verfahren als betroffene Aufsichtsbehörde im Internal Market Information System (IMI) gemeldet. Davon beziehen sich neun Verfahren auf Beschwerden nach Art. 77 DS-GVO und ein Verfahren auf eine Meldung einer grenzüberschreitenden Datenschutzverletzung durch eine andere Datenschutzaufsichtsbehörde. In zwei Fällen sind die Beschwerden beim Landesbeauftragten eingegangen, der diese über das IMI an die für die Hauptniederlassung zuständige Datenschutzaufsichtsbehörde herangetragen hat. Die grenzüberschreitenden Verfahren sind leider oft sehr langwierig, was von den Betroffenen zu Recht nur schwer nachvollzogen werden kann. Im Berichtszeitraum wurden zwei der beim Landesbeauftragten seit Inkrafttreten der DS-GVO eingereichten Beschwerden mit grenzüberschreitendem Bezug und unter Abgabe an die federführende Aufsichtsbehörde abgeschlossen. Der Landesbeauftragte ist bestrebt, die bei ihm eingereichten Beschwerden mit grenzüberschreitendem Bezug bereits möglichst im Rahmen der sog. vorläufigen Untersuchung (also vor der Einleitung eines Verfahrens in IMI) einer für den Beschwerdeführer akzeptablen Lösung zuzuführen. Dies ist auch in diesem Berichtszeitraum bis auf die o. g. zwei Fälle gelungen.

Schließlich hat der Landesbeauftragte in diesem Berichtszeitraum an dem durch die Zentrale Anlaufstelle (ZASt) angebotenen IMI-Workshop teilgenommen.

31.3 Angemessenheitsbeschluss USA (EU-U.S. Data Privacy Framework)

Mit dem sogenannten Schrems II-Urteil des Europäischen Gerichtshofs (EuGH) vom 16. Juli 2020 (Rs. C-311/18) wurde der Durchführungsbeschluss zum sog. „Privacy Shield“ (nach Art. 45 DS-GVO) für unwirksam erklärt. Da der EuGH keine Übergangsfrist eingeräumt hat, konnten Datenübermittlungen an die USA ab Rechtskraft des Urteils nicht mehr auf dieses Abkommen gestützt werden. Damit fehlte eine sichere Rechtsgrundlage für den Transfer personenbezogener Daten an die USA, wenn – neben den Garantien nach Art. 46 DS-GVO – keine ausreichenden zusätzlichen Maßnahmen getroffen werden konnten und auch keine Ausnahmevorschriften im Einzelfall anwendbar waren. Die EU und die USA einigten sich infolge des Urteils auf den „Transatlantischen Datenschutz-Rahmen“ („Trans-Atlantic Data Privacy Framework“ - TADPF, auch als „EU-US Data Privacy Framework“ bzw. „EU-US Datenschutzrahmen“ bezeichnet). Dabei handelt es sich um eine Selbstverpflichtung der USA zum Schutz der Privatsphäre. Die entsprechende Exekutivanordnung des US-Präsidenten vom 7. Oktober 2022 dient der Umsetzung des EU-US Data Privacy Framework. Durch das EU-US Data Privacy Framework sollen die durch den EuGH mit dem Schrems II-Urteil festgestellten Defizite nunmehr abgestellt und eine neue Rechtsgrundlage für Datentransfers an die USA geschaffen werden. Auf dieser Grundlage hat die Europäische Kommission am 10. Juli 2023 den Angemessenheitsbeschluss für das „EU-US Data Privacy Framework“ (EU-US DPF) angenommen. Seit diesem Tag können unter bestimmten Voraussetzungen wieder personenbezogene Daten aus der EU und dem

EWR an die USA übermittelt werden, ohne dass weitere Übermittlungsinstrumente oder zusätzliche Maßnahmen erforderlich sind. Der Angemessenheitsbeschluss gilt aber nur sektoral, d. h. Datenexporteure in der EU und dem EWR müssen vorab prüfen, ob sich der jeweilige US-Datenimporteur unter den Bedingungen des EU-US DPF zertifiziert hat. Das Department of Commerce veröffentlicht eine Liste mit den zertifizierten US-Organisationen nebst Informationen und weiteren Verlinkungen. Sofern der Datenimporteur nicht auf dieser Liste steht, muss der Datenexporteur die Rechtfertigung seiner Datenübermittlung auf andere geeignete Garantien nach Art. 46 DS-GVO, bspw. auf Standarddatenschutzklauseln, stützen.

Seit dem 10. Juli 2023 können unter bestimmten Voraussetzungen personenbezogene Daten aus der EU bzw. dem EWR an die USA übermittelt werden, ohne dass weitere Übermittlungsinstrumente oder zusätzliche Maßnahmen erforderlich sind.

31.4 Angemessenheitsbeschluss Japan (Review)

Für die erste gemeinsame Überprüfung (Joint Review) des EU-Angemessenheitsbeschlusses zu Japan (Durchführungsbeschluss (EU) 2019/419) vom 23. Januar 2019 durch die EU-Kommission nach Art. 45 Abs. 3 Satz 2 DS-GVO und umgekehrt des Angemessenheitsbeschlusses der japanischen Datenschutzbehörde PPC für die EU und UK fand im Juli 2021 eine Besprechung mit EU-Vertretern und Vertretern der PPC Japan statt. Für die Datenschutzaufsichtsbehörden beteiligten sich federführend die DSB Österreich, das LDA Bayern, der Landesbeauftragte und weitere europäische Behörden. Die PPC erhob von den EU-Aufsichtsbehörden mittels Fragebögen Informationen zur finanziellen und personellen Ausstattung sowie zum praktischen Umgang mit datenschutzrechtlichen Themen. Im November 2022 legte die EU-KOM ihren Bericht zum Joint-Review im Entwurf vor. Dieser umfasste unter anderem Beiträge von den japanischen Behörden sowie relevanten Interessenträgern und öffentlich zugängliches Material. Der EU-Angemessenheitsbeschluss bezieht sich auf das japanische Gesetz über den Schutz personenbezogener Daten („APPI“), nebst den „ergänzenden Vorschriften“ in Anhang I des Beschlusses sowie die in Anhang II des Beschlusses enthaltenen Erklärungen und Zusicherungen. Letztere betreffen die Beschränkungen und Garantien in Bezug auf den Zugang japanischer Behörden zu übermittelten personenbezogenen Daten. Das APPI wurde 2003 in Kraft gesetzt und 2017 erheblich reformiert. Mit der Reform wurden die bestehenden Schutzmaßnahmen gestärkt, aber auch eine Reihe neuer Schutzmaßnahmen eingeführt, wodurch das japanische Datenschutzsystem dem in der EU angenähert wurde. Weitere Ergänzungen erfolgten im Juni 2018, die für japanische Wirtschaftsbeteiligte, die Daten aus der EU importieren, bindend sind und von dem PPC oder direkt von EU-Bürgern vor den japanischen Gerichten durchgesetzt werden können. Mit Änderungen des APPI 2020 und 2021 wurden Aufsichtsbefugnisse des PPC gestärkt. Nach Anhörung der involvierten europäischen Datenschutzaufsichtsbehörden kommt die EU-Kommission in ihren finalen Bericht vom 3. April 2023 zu dem Schluss, dass Japan weiterhin ein angemessenes Schutzniveau für personenbezogene Daten aus der EU gegenüber Unternehmen gewährleistet, die dem APPI sowie den weiteren relevanten Vorschriften unterliegen. Im Übrigen will die EU-KOM von einem Zweijahreszyklus für die Überprüfung in einen Vierjahreszyklus übergehen. Von den japanischen Behörden wird erwartet, dass sie die EU-KOM über wesentliche Entwicklungen informieren, sowohl in Bezug auf die

Verarbeitung personenbezogener Daten durch Unternehmen als auch über die Beschränkungen und Garantien, die für den Zugang von Behörden zu personenbezogenen Daten gelten.

Personenbezogene Daten aus der EU bzw. dem EWR können weiterhin an Japan übermittelt werden, ohne dass weitere Übermittlungsinstrumente oder zusätzliche Maßnahmen erforderlich sind.

31.5 UAK Extraterritorialer Zugriff

Infolge des EuGH-Urteils zu Schrems II konnte die Übermittlung personenbezogener Daten in die USA zunächst nicht mehr auf Basis eines Angemessenheitsbeschlusses nach Art. 45 DS-GVO erfolgen. Es bedurfte nunmehr geeigneter Garantien nach Art. 46 DS-GVO oder einer Ausnahme nach Art. 49 DS-GVO. Nicht jeder Datentransfer ist aber eine Drittlandübermittlung im Sinne der DS-GVO, die den besonderen Anforderungen des Kapitels V genügen muss. Schwierigkeiten der Einordnung ergaben sich im Falle der Auftragsverarbeitung durch eine US-Tochtergesellschaft mit Sitz im EWR, die ggf. den US-Behörden über das Weisungsrecht der Muttergesellschaft Zugriff auf personenbezogene Daten gewähren muss. Die Datenschutzkonferenz (DSK) beauftragte den AK Internationaler Datenverkehr mit der datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten. Der AK Internationaler Datenverkehr richtete den UAK Extraterritorialer Zugriff ein, an dem auch der Landesbeauftragte mitarbeitete und der die Vorlage für den Beschluss der Datenschutzkonferenz vom 31. Januar 2023 lieferte. Danach reicht allein die Gefahr, dass - etwa über gesellschaftsrechtliche Weisungsrechte - die Drittlands-Muttergesellschaft eines EWR-Unternehmens dieses anweisen könnte, oder dass öffentliche Stellen von Drittländern unmittelbar EWR-Unternehmen anweisen könnten, personenbezogene Daten in ein Drittland zu übermitteln, nicht aus, um eine Übermittlung in ein Drittland i. S. d. Art. 44 ff. DS-GVO anzunehmen. Allerdings gelten in diesen Fällen, die keine Drittlandübermittlung darstellen, dennoch die übrigen Anforderungen der DS-GVO, insbesondere an die Sicherheit der Verarbeitung nach Art. 32 DS-GVO.

31.6 AG „Rechtsgrundlage für die Übermittlung von Gesundheitsdaten und Biomaterialien in Drittstaaten“

Mit DSK-Beschluss vom 15. April 2020 wurden Patienten-Einwilligungsdokumente der Medizin-Informatik-Initiative zur Verarbeitung genetischer Daten aus Biomaterialien gebilligt. In 2021 stand eine Neufassung zur Prüfung an. Die DSK traf am 24. und 25. November 2021 Festlegungen zur Einrichtung der „Task Force Forschungsdaten“ unter der Leitung des HBDI und des BfDI. Die fachliche Expertise einiger Arbeitskreise der DSK sollten in der TF mit eingebunden werden. Der Landesbeauftragte beteiligte sich als einer der Vertreter des AK Internationaler Datenverkehr. In dem AK wurde die AG "Rechtsgrundlage für die Übermittlung von Gesundheitsdaten und Biomaterialien in Drittstaaten" gegründet. Die AG war in 2022 und 2023 mit der Prüfung befasst, unter welchen Bedingungen der Datentransfer von Gesundheitsdaten zu Forschungszwecken an Drittländer zulässig sein kann und wie entsprechende datenschutzrechtliche Informationen ausgestaltet werden müssen.

Die Arbeit der AG "Rechtsgrundlage für die Übermittlung von Gesundheitsdaten und Biomaterialien in Drittstaaten" wurde in 2023 noch nicht vollständig abgeschlossen.

31.7 AG „Gemeinsame Handreichung zum EU-U.S. Data Privacy Framework“

Die Europäische Kommission hat am 10. Juli 2023 den Angemessenheitsbeschluss für das „EU-US Data Privacy Framework“ (EU-US DPF) angenommen. Infolge der Komplexität des Beschlusses beauftragte die DSK den AK Internationalen Datenverkehr mit der Fertigung einer Hilfsstellung zum einen für Verantwortliche, die personenbezogene Daten an die USA übermitteln, und zum anderen für betroffene Personen mit Informationen bezüglich ihrer Rechtsschutzmöglichkeiten. An der eigens dazu eingerichteten AG "Gemeinsame Handreichung zum EU-U.S. Data Privacy Framework" arbeitete auch der Landesbeauftragte mit. Die DSK hat am 4. September 2023 die Anwendungshinweise zum Angemessenheitsbeschluss zum EU-US Data Privacy Framework (EU-US DPF) veröffentlicht und dazu eine Pressemitteilung herausgegeben.[49]

31.8 Leitlinien 04/2022 des EDSA für die Berechnung von Geldbußen

Der EDSA verabschiedete am 12. Mai 2022 eine Version 1.0 der Leitlinien für die Berechnung von Geldbußen im Sinne der DS-GVO („Guidelines 04/2022 on the calculation of administrative fines under the GDPR“). Nach öffentlicher Konsultation wurde die Version 2.0 erstellt und am 24. Mai 2023 angenommen.[50] Vorausgegangen war eine mehrjährige Vorbereitung und Entwicklung der Leitlinien durch die noch von der Art. 29-Datenschutzgruppe eigens dafür eingerichteten Taskforce Fining Guidelines. Die Ausarbeitung von Leitlinien zur Harmonisierung der Verhängung von Bußgeldern gehört nach Art. 70 Abs. 1 lit. k DS-GVO zu den Aufgaben des EDSA. Diese Leitlinien ergänzen die bereits bestehenden „Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679“ (WP 253), mit denen sich die Aufsichtsbehörden auf die Grundsätze und einheitliche Auslegung der Bewertungskriterien des Art. 83 DS-GVO verständigt hatten. Die Leitlinien 04/2022 lösen das von der DSK verabschiedete nationale Bußgeldkonzept ab.

Die Leitlinien 04/2022 zeigen eine Methodik zur Bußgeldberechnung in fünf Schritten auf. Dabei lassen sie den Aufsichtsbehörden hinreichenden Ermessenspielraum bei Sanktionierung von Verstößen im Einzelfall. Im ersten Schritt ist die Konkurrenz ggf. mehrerer Verstöße zu bestimmen. Im zweiten Schritt erfolgt anhand der Schwere des Verstoßes und des Jahresumsatzes des verantwortlichen Unternehmens die Festlegung eines Ausgangswertes für die weitere Berechnung der Geldbuße. Im dritten Schritt werden weitere mildernde und erschwerende Umstände berücksichtigt. Im vierten Schritt ist die Geldbuße unter Berücksichtigung des gesetzlichen Höchstbetrages ggf. anzupassen. Im fünften Schritt sind weitere Anpassungen infolge von besonderen

[49] https://www.datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf

[50] https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_en

Umständen des Einzelfalls möglich, um eine wirksame, abschreckende und verhältnismäßige Geldbuße nach Art. 83 Abs. 1 DS-GVO sicherzustellen.

Am 24. Mai 2023 wurden die Leitlinien 04/2022 des EDSA für die Berechnung von Geldbußen im Sinne der DS-GVO angenommen und geringfügig am 29. Juni 2023 für die Version 2.1 geändert.

31.9 Zuständigkeit für die Religionsgemeinschaft Jehovas Zeugen

Der Landesbeauftragte ist für Beschwerden gegen die Verarbeitung personenbezogener Daten durch örtliche Vertreter oder Vereinigungen der Religionsgemeinschaft Jehovas Zeugen zuständig. Es kommen zwei Fallgruppen in Betracht. Zum einen beschweren sich Nichtmitglieder über Zeugen Jehova im Predigtdienst, zum anderen beschweren sich Mitglieder bzw. ehemalige Mitglieder gegen die örtlichen „Versammlungen“.

Die Religionsgemeinschaft Jehovas Zeugen in Deutschland ist eine Körperschaft des öffentlichen Rechts, deren Status als Körperschaft zunächst von Berlin und dann von allen anderen Bundesländern in Zweitbescheidung anerkannt wurde (Art. 140 GG i. V. m. 137 Abs. 5 Satz 2 Weimarer Reichsverfassung; Art. 83 GG). Bei den örtlichen "Versammlungen" handelt es sich um selbstverwaltete, aber rechtlich nicht selbstständige Vereinigungen auf regionaler Ebene, die in ebenfalls rechtlich unselbstständigen "Kreisen" zusammengefasst sind, von dort aber lediglich geistlich betreut werden. Auch ohne eigene Rechtspersönlichkeit gelten die Versammlungen vertreten durch die Ältestenschaft (§ 5 Abs. 1 Versammlungsordnung) als Verantwortliche, wenn sie über die Zwecke und Mittel der Verarbeitung entscheiden (Art. 4 Nr. 7 DS-GVO). Der Predigtdienst an der Haustür und auf öffentlichen Plätzen wird von Zeugen Jehovas im Predigtdienst (Mitglieder) zusammen mit ungetauften Verkündigern in der Ausbildung (keine Mitglieder) durchgeführt. Gemäß § 13 Abs. 2 des Statuts der Religionsgemeinschaft Jehovas Zeugen in Deutschland (StRG) handelt es sich um eine eigenverantwortliche persönliche Glaubensausübung. Nach dem Urteil des EuGH vom 10. Juli 2018 (C-25/17, Rn. 73) besteht jedoch eine gemeinsame Verantwortlichkeit zwischen den Mitgliedern und Verkündigern im Predigtdienst einerseits und den "Versammlungen" andererseits, da die "Versammlungen" an der Organisation und Koordination des Predigtdienstes mitwirken.

Je nach Beschwerdegegenstand ergibt sich die Zuständigkeit des Landesbeauftragten aus § 40 BDSG i. V. m. § 23 Abs. 4 DSAG LSA oder § 23 Abs. 1 DSAG LSA.

32 Technik und Organisation

32.1 Akkreditierung und Zertifizierung

Die Möglichkeit der datenschutzrechtlichen Zertifizierung von Produkten, Prozessen und Dienstleistungen durch akkreditierte Zertifizierungsstellen besteht prinzipiell. In den letzten Jahren wurden die die DS-GVO begleitenden Dokumente und Regelungen rechtlicher, technischer und organisatorischer Art sowohl auf nationaler als auch auf europäischer Ebene erstellt. Im Berichtsjahr lag ein Schwerpunkt erwartungsgemäß

auf der Genehmigung von Zertifizierungsprogrammen und Prüfkriterienkatalogen. Nun könnten eigentlich auch erste Zertifikate durch akkreditierte Zertifizierungsstellen erteilt werden. Tatsächlich werden erste Zertifizierungsprogramme in anderen Bundesländern bereits geprüft, jedoch wird es noch bis ins Jahr 2024 dauern, bis erste deutsche Datenschutzzertifikate die Welt erblicken können.

Die Teilnahme und Mitarbeit im Arbeitskreis Zertifizierung und im Unterarbeitskreis Prüfkriterien erfolgte auch im Berichtszeitraum. Hier werden regelmäßig die jeweils aktuellen Themen rund um Zertifizierung, Kriterienkataloge und diesbezüglich noch offene Punkte besprochen.

Es wurde ein deutlicher Anstieg der Anträge auf die Genehmigung von Zertifizierungskriterien sowie auf die Akkreditierung von Zertifizierungsstellen registriert. Das betraf vor allem einzelne Bundesländer und EU-Mitgliedsstaaten. Verfahren zur Anerkennung von Zertifizierungskriterien in Deutschland und Europa wurden somit ein dauerhafter Tagesordnungspunkt bei den AK-Treffen.

In mehreren Bundesländern liegen erste Anträge zur Anerkennung von Kriterienkatalogen und Akkreditierungen vor. Es gab regen Abstimmungsbedarf, denn die Genehmigung von Kriterienkatalogen ist neben der fachlichen Zuarbeit im Rahmen der Akkreditierung eine der Hauptaufgabe der Datenschutzaufsichtsbehörden in diesen Verfahren.

Im AK Zertifizierung wurde die Reichweite von Zertifizierungen bei grenzüberschreitender Datenverarbeitung thematisiert. Es geht um das Europäische Datenschutzsiegel (Art. 42 Abs. 5 Satz 2 DS-GVO). Zu klären war etwa die Frage, wie mit Zertifikaten einer Zertifizierungsstelle aus einem Mitgliedstaat umgegangen werden soll, die diese für Datenverarbeitungsvorgänge in einem anderen Mitgliedstaat ausstellt. Insbesondere mit Blick auf die ggf. abweichende Einschätzung der Aufsichtsbehörde vor Ort. Die Frage soll auf EU-Ebene behandelt werden.

Bereits im Jahr 2020 wurde eine Kooperationsvereinbarung zwischen den Datenschutzaufsichtsbehörden und der DAkkS geschlossen (XVI. Tätigkeitsbericht, Nr. 6.6). Sie regelt unter anderem die Zusammenarbeit bei der Genehmigung von Zertifizierungskriterien und der Akkreditierung von Zertifizierungsstellen. Im Verlauf der ersten konkreten Verfahren traten noch offene Fragen und ungeregelte Aspekte zu Tage, etwa, wie auch die unbeteiligten deutschen Aufsichtsbehörden in den Genehmigungsprozess der Kriterienkataloge mit eingebunden werden können und was dabei alles zu berücksichtigen ist. Um diese Lücken zu schließen, wurde im November 2023 eine ergänzende Vereinbarung („Addendum zur Kooperationsvereinbarung“) zwischen den Kooperationspartnern geschlossen. Durch eine nun vorgezogene Information sollen – in enger Abstimmung mit dem Antragsteller – die nicht direkt beteiligten Aufsichtsbehörden zeitnaher informiert und in geeigneter Weise in den Prozess einbezogen werden, um zu vermeiden, dass erst kurz vor Ende des Genehmigungsverfahrens oder gar auf EU-Ebene noch Meinungsverschiedenheiten unter den deutschen Aufsichtsbehörden ausgeräumt werden müssen. Das beschleunigt das Genehmigungsverfahren und ermöglicht ein einheitliches Auftreten der deutschen Aufsichtsbehörden.

Das Kurzpapier Nr. 9 „Zertifizierung nach Art. 42 DS-GVO“[51] der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) wurde durch den AK Zertifizierung überarbeitet und durch die DSK freigegeben. Es gibt insbesondere für den nichtöffentlichen Bereich einen Überblick über das Thema Zertifizierungen.

Auch in diesem Jahr wurde das vom UAK Prüfkriterien erstellte Dokument „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme – Datenschutzrechtliche Prüfkriterien, Prüfsystematik und Prüfmethoden zur Anpassung und Anwendung der technischen Norm DIN EN ISO/IEC 17067 (Programmtyp 6)“ zur einheitlichen Bewertung von Prüfkriterienkatalogen fortgeschrieben. Bei den Ergänzungen und Aktualisierungen handelt es sich etwa um Hinweise zu „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ (Art. 25 DS-GVO). Eine Veröffentlichung der aktualisierten Fassung ist geplant.[52] Auch zukünftig soll das Dokument als Orientierungshilfe bei der Erstellung von Zertifizierungsprogrammen und -kriterien dienen.

Bislang liegen in Sachsen-Anhalt noch keine Anträge auf die Genehmigung von Zertifizierungskriterien beziehungsweise auf die Akkreditierung von Zertifizierungsstellen vor.

Insgesamt zeigt sich aber, dass der Bereich der Zertifizierung nach der DS-GVO nun zunehmend an Fahrt gewinnt. Erste aktive Zertifizierungsstellen werden frühestens nächstes Jahr in Deutschland erwartet. Insgesamt sind die Datenschutzaufsichtsbehörden auf einem guten Weg, Datenschutzzertifizierungen mit einer hohen Qualität und Verlässlichkeit nachhaltig zu etablieren.

32.2 Informationssicherheit (AG InfoSic Land)

Die Arbeit in den UAG der AG InfoSic (Land) wurde erfolgreich fortgesetzt, viele Projekte, meist Informationssicherheitsrichtlinien, auch weitgehend abgeschlossen. Sie warten jetzt auf ihre Finalisierung und abschließende Freigabe. Offen blieb lange Zeit, wie die verbindliche Veröffentlichung von ressortübergreifenden Informationssicherheitsrichtlinien derart erfolgen kann, dass die Inhalte nicht öffentlich einsehbar werden und der Schutzbedarf „intern“ gewahrt bleibt. Auch die Art und Weise der Veröffentlichung wurde wiederholt diskutiert. Muss diese über einen gemeinsamen Runderlass erfolgen oder kann sie der CIO wie geplant auf der Grundlage von §13 EGovG veröffentlichen? Ein zum Ministerialblatt alternatives Verfahren soll daher im Informationssicherheitsgesetz festgeschrieben werden. Bereits vom CIO gezeichnete Richtlinien sollen über die Hausleitungen und die ISB in den jeweiligen Ressorts bekannt gegeben werden.

Die UAG „BITS“ wurde in die UAG „Awareness“ migriert. Die im letzten Jahr eingerichtete BITS-Entwicklungsplattform befindet sich jetzt in der dSecureCloud und ist aus dem Landesnetz erreichbar. Es war geplant, eine landeseigene, übergreifende Schulungsplattform (ILIAS) mit Betrieb bei Dataport für alle Ressorts zur Verfügung zu stellen. Diese sollte neben den bereits vorhandenen Inhalten aus der Landesverwaltung

[51] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_9.pdf

[52] https://datenschutzkonferenz-online.de/anwendungshinweise.html

Niedersachsen auch BITS und das Modul „Phishing“ beinhalten. In einer Machbarkeitsstudie sollte ein funktionaler Prototyp der ILIAS-Plattform im MID bereitgestellt werden, um sie genauer evaluieren und beurteilen zu können. Auch mögliche Nutzer anderer Plattformen und Dienstleister sollten so motiviert werden, ILIAS auch zu verwenden. Derweil lehnte Dataport die Bereitstellung der ILIAS-Plattform ab und schlug als Alternative Moodle vor. Auf Nachfrage mehrerer Trägerländer bei Dataport nach dem Betrieb von ILIAS, erfolgte dann doch die Aufnahme in das Produktportfolio.

In der UAG „Cloudnutzung und KI“ entstand im November 2023 das „Merkblatt KI“, welches kurz und prägnant wichtige Hinweise zur Nutzung von KI in der öffentlichen Verwaltung gibt.

Anfang des Jahres 2023 wurde ein erster Entwurf des Informationssicherheitsgesetzes Sachsen-Anhalt durch BSI und MI geprüft, später auch in der Runde der Informationssicherheitsbeauftragten der Ressorts vorgestellt. Es wurde um sehr kurzfristige Stellungnahmen gebeten, die in der zur Verfügung stehenden Zeit nicht möglich waren. Schließlich handelt es sich um ein wichtiges Gesetzesvorhaben, welches unmittelbar die zukünftige Arbeit der ISB betrifft und beeinflusst. So wurde ein gemeinsames Antwortschreiben an den CISO des Landes formuliert, dass die Übersendung als Beginn der fachlichen Diskussion des Entwurfs, mit dem verbindlichen Ziel der Schaffung angemessener rechtlicher Rahmenbedingungen zur nachhaltigen Gewährleistung von Informationssicherheit in der unmittelbaren Landesverwaltung Sachsen-Anhalt, angesehen wird. Auf bereits festgestellte Defizite hinsichtlich der Kompatibilität mit der Landesleitlinie Informationssicherheit wurde hingewiesen.

In den späteren Sitzungen der AG InfoSic (Land) wurden der immense Umfang und die Komplexität des Vorhabens deutlich. Immer mehr Punkte, fast alle aus der NIS-2-Richtlinie resultierend, mussten geregelt und im Gesetz abgedeckt werden. Der CISO informierte stetig und transparent über den Stand des Entwurfs des Informationssicherheitsgesetzes (des Landes) und wies immer wieder auf die Möglichkeit der Übersendung von fachlichen Stellungnahmen und Anmerkungen an das CISO-Team hin. Nach der Bereitstellung eines aktualisierten Entwurfes im Spätsommer 2023 sollte die Ressortbeteiligung erfolgen. Zu klärende Problemfelder und Themen wurden nach und nach durch das MID und den CISO herausgearbeitet. Hinderlich war insbesondere das noch ausstehende und somit fehlende Umsetzungsgesetz des Bundes. Die Umsetzung der aufgrund der NIS-2-Richtlinie geplanten Maßnahmen sollte bis Oktober 2024 erfolgen.

Der Landesbeauftragte unterstützte von Anfang an das Anliegen des CISO, ein handwerklich gutes Gesetz mit sinnvollen Regelungen für das Land vorlegen zu wollen, wissend, dass nicht alle Forderungen Bestand haben werden und erwartend, dass vieles noch geändert oder gestrichen werden wird. Die Landesregierung wird sich an dem, was übrigbleibt, messen lassen müssen.

Im Dezember wurden die ISB der Ressorts zu einem Austausch im Zuge der Erstellung des Informationssicherheitsgesetzes Sachsen-Anhalt allerdings erst im Jahr 2024 eingeladen. Nun sollen die Anforderungen, Wünsche und Empfehlungen zeitnah erörtert und einbezogen werden.

Nach weiteren Abstimmungen fand im Oktober die lange erwartete Unterzeichnung der „Kooperationsvereinbarung im Bereich Cyber- und Informationssicherheit“ zwischen dem Land Sachsen-Anhalt vertreten durch das MID und dem BSI statt. Für das nächste Jahr soll etwa ein IT-Grundschutztag in Sachsen-Anhalt organisiert werden.

32.3 Pilotphase „Mein Justizpostfach“

Gerade noch im Berichtszeitraum wurde der Internetdienst „Mein Justizpostfach“ (MJP) in den Pilotbetrieb überführt.[53] Er soll eine sichere und kostenlose elektronische Kommunikation insbesondere mit der Justiz erlauben. Es ist explizit kein Elektronisches Bürger- und Organisationenpostfach (eBO), sondern nutzt ein OZG-Nutzerkonto Bund mit einer BundID[54] und dem Vertrauensniveau hoch, was den elektronischen Personalausweis voraussetzt. Das MJP dient der rechtswirksamen Einreichung elektronischer Dokumente mit nur einer einfachen Signatur durch Angabe des vollen Namens am Ende des Dokuments. Damit muss keine qualifizierte elektronische Signatur beschafft und verwendet werden. Dennoch ist dies einer der sogenannten „sicheren Übermittlungswege“ (§ 130a Abs. 4 Nr. 5 ZPO). Das MJP ergänzt damit das bestehende Angebot des eBO und bietet damit all jenen einen Zugang zur Justiz, die nicht über ein besonderes elektronisches Postfach verfügen und auch nicht die monatlichen Kosten eines eBO tragen wollen.

Wie bereits beim eBO (siehe Nr. 17.2), gibt es Einschränkungen, die eine allgemeine Verwendung verhindern und den Nutzerkreis auf den der besonderen Postfächer der EGVP-Infrastruktur (ohne eBO) beschränken. So können MJP-Nutzer zwar mit den elektronischen Postfächern des EGVP (beA, beN, beSt und beBPo), aber nicht untereinander und auch nicht mit eBO-Nutzern kommunizieren.

Offenbar ist die Nutzung des MJP mit einer Einwilligung zur Bekanntgabe von Verwaltungsakten über das Postfach des Nutzerkontos (§ 9 Abs. 1 OZG) und den ggf. damit verbundenen Fristen verbunden.

Nutzende des MJP sollten wissen, dass ihre vollständige Privatanschrift für alle EGVP-Teilnehmer, die ein MJP adressieren können, einsehbar ist. Das betrifft auch Personengruppen, die vielleicht eher keine privaten Besuche von unzufriedenen Verfahrensbeteiligten möchten (Schiedspersonen, Gutachter, Sachverständige), aber das MJP zur sicheren Kommunikation mit Anwälten nutzen werden.

Personen, für die im Melderegister eine Auskunftssperre nach dem BMG eingetragen ist, sollten beachten, dass die Daten des MJP aus der BundID und damit dem Melderegister stammen und andere Teilnehmende am elektronischen Rechtsverkehr (Gerichte, Rechtsanwälte, Steuerberater, Behörden, …) in der Lage sind, diese – etwa die Meldeanschrift – einzusehen. Laut FAQ wird daran gearbeitet, dass Sperrvermerke im Melderegister zukünftig beachtet werden und etwa SAFE-Einträge ohne Anschrift möglich werden. Erst im Zuge der Weiterentwicklung des MJP soll die Einrichtung eines Postfachs auch ohne Veröffentlichung der Anschrift ermöglicht werden.

---

[53] https://mjp.justiz.de/

[54] https://id.bund.de/

Es ist wichtig, dass der elektronische Rechtsverkehr DS-GVO-konform realisiert wird. Es sollte technisch möglich sein, in einer Identitätsdatenbank auch solche ohne Postanschrift mitzuführen, zumal deren Sinn ja darin besteht, mit diesen Personen elektronisch Kontakt aufnehmen zu können. Einzig die Prüfung auf zusammengehörige Daten (SAFE-Identität und vorhandene personenbezogene Daten) müsste passend ausgestaltet werden – entweder ohne Anschriften (Name, Geburtsdatum, …) oder mit Anschriften-Matching, aber auch dafür gibt es bereits erprobte Verfahren.

32.4 Angemessene Reaktionen auf gängige Cyberangriffe

Ein Cyberangriff ist ein vorsätzlicher unbefugter Versuch, durch Zugriff auf IT-Systeme Daten zu stehlen oder zu manipulieren oder IT-Systeme zu stören. Die beim Landesbeauftragten am häufigsten gemeldeten Cyberangriffe sind Ransomware-Attacken, Virenbefall und Identitätsdiebstahl durch unbefugten E-Mail-Versand. Cyberangriffe müssen gem. Art. 33 DS-GVO immer dann an die Datenschutzaufsichtsbehörde gemeldet werden, wenn personenbezogene Daten betroffen sind und der Angriff voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Bei Ransomware handelt es sich um spezielle Schadsoftware, die jegliche Daten auf Festplatten und Netzwerkfreigaben verschlüsseln und oft mit einer Lösegeldforderung einhergehen. Nach einem Befall mit Schadsoftware oder Viren ist die Neuinstallation der Systeme und die Wiederherstellung der Daten aus Backups unerlässlich, denn Ransomware und andere Viren laden evtl. weiteren Schadcode aus dem Internet nach. Dieser Schadcode kann sich zunächst unbemerkt und ohne weitere schädliche Auswirkung im System einnisten und später ggf. aktiv werden, obwohl die Datei mit dem ursprünglichen Virus bereits bereinigt bzw. gelöscht wurde. Daher ist es bei Virenbefall dringend geboten, alle Systeme, die mit dem Virus in Kontakt gekommen sind, neu aufzusetzen. Nur eine Neuinstallation betroffener Rechner und Server kann garantieren, dass keine Reste des Virus oder von diesem nachgeladener Schadcode, im System verbleiben und später aktiv werden. Das Bundesamt für Sicherheit in der Informationstechnik gibt umfangreiche Empfehlungen zum Schutz vor und zum Umgang mit Ransomware-Befall.[55]

Zudem sollte bereits präventiv und fortlaufend auf allen Systemen und im Vorfeld der E-Mail-Zustellung auf Viren gescannt werden, noch bevor Schadprogramme Client-PCs erreichen können. Dafür bieten die Hersteller von Antivirensoftware gesonderte Produkte sog. E-Mail-Gateways an. Außerdem sollte das Ausführen von Makros in Office-Produkten weitgehend deaktiviert werden, um zu verhindern, dass Makros in aus E-Mails heraus geöffneten Dokumenten aktiv werden. Im aktuellen Berichtszeitraum kursieren vermehrt Viren (z. B. Emotet), die über E-Mail-Anhänge eingeschleust werden und mittels Makros das Adressbuch eines Nutzers auslesen und dessen E-Mail-Adresse und die Bestands-E-Mails nutzen, um weitere E-Mails mit schädlichen Inhalten zu verschicken. Oft werden auch E-Mail-Server selbst Ziel eines Angriffs, um aus Adressbüchern personenbezogene Daten zu erbeuten, die dann wiederum für den Versand gefälschter, schädlicher E-Mails genutzt werden. Diese Angriffe basieren

[55] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/ransomware-angriffe_node.html

meist auf Sicherheitslücken in den E-Mail-Servern, die aufgrund des Auslassens aktueller Updates noch nicht geschlossen wurden. Daher gilt es, verfügbare Updates stets unverzüglich einzuspielen.

Um Cyberangriffe zu vermeiden sollten Systeme auf dem neusten Stand gehalten, Makros eingeschränkt oder deaktiviert und die Beschäftigten über schadhafte E-Mails aufgeklärt werden. Wenn ein Cyberangriff erfolgt ist, müssen die beteiligten Systeme neu aufgesetzt werden. Das Anlegen und Wiederherstellen von Backups ist in diesem Zusammenhang unerlässlich.

32.5 Prüfung von Videokonferenzsystemen bei Dataport

Dataport A.ö.R. bietet öffentlichen Stellen in den Trägerländern die Dienste dVideokommunikation und Phoenix im Rahmen einer Auftragsverarbeitung gem. Art. 28 DS-GVO an. Die Dienste beinhalten die Zurverfügungstellung von Plattformen, Zugängen und virtuellen Räumen zur Durchführung eigener Videokonferenzen. Dabei werden durch Dataport im eigenen und auch in Rechenzentren von Unterauftragnehmern Bild- und Tondaten aller an einer Videokonferenz teilnehmenden Personen sowie anfallende Verkehrs- und Metadaten verarbeitet. Bei der Zurverfügungstellung der vorgenannten Dienste werden verschiedene Technologien eingesetzt. Bezüglich dVideokommunikation kommt zentral im Rechenzentrum und bei den Verantwortlichen vor Ort Hardware und Software der Firma Cisco Systems zum Einsatz. Im Rahmen des Projektes Phoenix werden Videokonferenzen über die quelloffene Plattform JitsiMeet realisiert.

Verantwortlich für die Datenverarbeitung sind die jeweiligen öffentlichen Stellen, die den Dienst bei Dataport in Anspruch nehmen und damit eigenständig Videokonferenzen durchführen. Da diese allerdings den Dienst in der Ausprägung in Anspruch nehmen müssen, wie Dataport ihn anbietet und die Anzahl der öffentlichen Stellen, die diesen Dienst in Anspruch nehmen, sehr umfangreich ist, wurde die Verarbeitung personenbezogener Daten im Kontext dieses Dienstes direkt beim Auftragsverarbeiter Dataport geprüft, denn gem. Art. 58 Abs. 1 lit. b DS-GVO verfügt jede Aufsichtsbehörde über sämtliche Untersuchungsbefugnisse, die es gestatten beim Auftragsverarbeiter Datenschutzüberprüfungen durchzuführen. Die Prüfung wurde gemeinsam mit den Datenschutzaufsichtsbehörden aus Bremen, Hamburg und Schleswig-Holstein durchgeführt.

Prüfgegenstand war die Feststellung, ob Dataport seinen eigenen Verpflichtungen aus Art. 28 DS-GVO nachkommt und es den Auftragnehmern ermöglicht, die Vorgaben der DS-GVO hinsichtlich der Forderungen aus Art. 5, Art. 13, Art. 25, Art. 28 und Art. 32 zu erfüllen. Dabei wurde insbesondere die Ermöglichung der Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten aus Art. 5 DS-GVO i. V. m. den Anforderungen an technische und organisatorische Maßnahmen aus Art. 25 und 32 DS-GVO geprüft. Außerdem wurde untersucht, ob der Dienstleister sich entsprechend der Vorgaben als Auftragnehmer einer Auftragsverarbeitung gem. Art. 28 Abs. 3 DS-GVO verhält, sich den Weisungen der Auftraggeber unterwirft und die Auftraggeber bei der Erfüllung ihnen obliegender Pflichten nach Art. 13 DS-GVO unterstützt.

So wurden Dataport in einem Anschreiben gemeinsam von den Aufsichtsbehörden erarbeitete Prüffragen gestellt, um das Ausfüllen einer Checkliste zu technischen und organisatorischen Maßnahmen gebeten und für die Videokommunikation wesentliche

Dokumente angefordert. Der Fragenkatalog diente dem Ziel, ein breites Spektrum an Antworten herbeizuführen, welche die Aufsichtsbehörden in die Lage versetzen sollten, gemeinsam mit den übersandten Dokumenten eine möglichst umfassende datenschutzrechtliche Bewertung zum Prüfgegenstand abgeben zu können. Der Fragenkatalog unterteilte sich in die Themenkomplexe Implementation, Leistungsumfang, Unterauftragnehmer und Unterstützung der öffentlichen Auftraggeber.

Dataport lieferte den Großteil der geforderten Dokumente und Antworten. Zur Klärung von Nachfragen fanden mehrere Videokonferenzen statt. Bis auf kleinere Unzulänglichkeiten in der Dokumentation und Unterauftragsvergabe waren durch die Aufsichtsbehörden kaum Mängel festzustellen. Einzig in der Gestaltung des Vertragswerkes gem. Art. 28 DS-GVO sahen die Aufsichtsbehörden mehrere Nachbesserungsbedarfe. In der darauffolgenden Zeit überarbeitete Dataport einen Teil der Standardvertragsmuster für seine Kunden aus dem öffentlichen Bereich der Trägerländer nebst dazugehörigen Anhängen, so dass alle vertragsmäßigen Anforderungen aus der DS-GVO erfüllt waren.

33 Telekommunikation und Medien

33.1 Chatkontrolle

Im Mai 2022 hat die Europäische Kommission einen Vorschlag für eine Verordnung zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern vorgelegt. Der Vorschlag sieht unter anderem vor, dass Anbieter von E-Mail-, Messenger- oder Chat-Diensten dazu verpflichtet werden, die Verbreitung von bekannten oder neuen Darstellungen sexuellen Kindesmissbrauchs oder die Kontaktaufnahme zu Kindern anhand bestimmter Indikatoren zu erkennen.

Selbstverständlich müssen Kinder vor sexuellem Missbrauch geschützt werden. Die Wahl der Mittel ist jedoch äußerst zweifelhaft, denn die digitale Kommunikation sämtlicher Nutzerinnen und Nutzer wäre verdachtsunabhängig von einer solchen Überwachung betroffen und das über alle Lebensbereiche hinweg.

Das Gesetzesvorhaben würde von den Anbietern verlangen, dass die mittlerweile für private Kommunikation weitgehend etablierte Ende-zu-Ende-Verschlüsselung aufgebrochen wird. Im Ergebnis bedeutet dies, dass die Sicherheit beim Austausch digitaler Nachrichten geschwächt wird.

In ihrer Entschließung „Geplante Chatkontrolle führt zu einer unverhältnismäßigen, anlasslosen Massenüberwachung!“[56] vom 17. Oktober 2023 richtet die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) den nachdrücklichen Appell an den EU-Gesetzgeber, bei der beabsichtigten Regulierung die Grenzen der Rechtsstaatlichkeit einzuhalten und insbesondere Erforderlichkeit und Verhältnismäßigkeit zu wahren.

[56] https://www.datenschutzkonferenz-online.de/media/en/20231017DSKEntschliessungChatkontrolle.pdf

Die Datenschutzkonferenz weist in aller Deutlichkeit darauf hin, dass es sich bei der vorgesehenen Chatkontrolle um eine anlasslose Massenüberwachung handelt, die nicht mit den Grundrechten auf Achtung des Privat- und Familienlebens, der Vertraulichkeit der Kommunikation und zum Schutz personenbezogener Daten vereinbar ist.

33.2 Google Street View

Anfang Juni 2023 hat Google wieder damit begonnen, systematisch alle Straßenzüge für seinen Dienst Google Street View zu fotografieren. Dabei kann es passieren, dass neben den Straßenansichten auch Fahrzeuge mit Nummernschildern und Personen auf öffentlichen Flächen oder privaten Grundstücken aufgenommen werden.

Da sich die deutsche Niederlassung von Google in Hamburg befindet, ist der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit für die datenschutzrechtliche Prüfung zuständig und hat dazu auf seiner Webseite einige Informationen bereitgestellt.

Die grundsätzliche datenschutzrechtliche Bewertung solcher Panorama-Aufnahmen von deutschen Städten ergibt sich aus dem Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 12. Mai 2020 „Vorabwidersprüche bei Street View und vergleichbaren Diensten“.[57]

Die Anfertigung und Veröffentlichung von Bildaufnahmen aus dem öffentlichen Straßenraum kann Google auf die Rechtsgrundlage des Art. 6 Abs. 1 lit. f DS-GVO stützen. Dabei dürfen nur Aufnahmen von Bereichen erstellt werden, die vom öffentlichen Raum aus einsehbar sind.

Personenbezogene Daten, die aufgenommen werden, aber nicht für die Straßenansichten erforderlich sind, wie z. B. Gesichter und Kfz-Kennzeichen, müssen vor der Veröffentlichung verpixelt werden.

Betroffene können bereits bevor die Aufnahmen erfolgen, einen Widerspruch gegen die Veröffentlichung der Bilder ihres Hauses bei Google Street View einlegen. Nach Veröffentlichung der Aufnahmen ist ein Widerspruch zusätzlich über das „Problem melden”-Feature von Google Street View möglich.

33.3 Pur-Abo-Modelle

Seit einiger Zeit werden auf den verschiedensten Webseiten sogenannte „Pur-Abo-Modelle“ angeboten. Bei einem „Pur-Abo-Modell“ werden den Besucherinnen und Besuchern einer Webseite über ein Einwilligungsbanner in der Regel zwei Wahlmöglichkeiten gegeben, um die Inhalte der Webseite lesen zu können: Entweder schließen sie ein „Pur-Abo“ ab oder sie willigen ein, dass ihre Daten für profilbasierte und individualisierte Werbung genutzt werden dürfen. Nur bei Wahl eines „Pur-Abos“ sind die Tracking-Mechanismen deaktiviert und die Webseite kann ohne individuelle Profilbildung

[57] https://www.datenschutzkonferenz-online.de/media/dskb/20200526_beschluss_vorabwidersprueche_bei_streetview_und_vergleichbaren_diensten.pdf

und personalisierte Werbung genutzt werden. Die Besucherinnen und Besucher zahlen also nicht für die Inhalte auf der Webseite. Sie verhindern damit vielmehr, dass ihre personenbezogenen Daten durch digitales Marketing monetarisiert werden.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in ihrem Beschluss zur „Bewertung von Pur-Abo-Modellen auf Websites“[58] vom 22. März 2023 die Anforderungen an „Pur-Abo-Modelle“ konkretisiert. Der Beschluss kann in der Praxis als Hilfestellung für die konkrete Ausgestaltung eines „Pur-Abo-Modells“ dienen. Insbesondere stellt die DSK mit dem Beschluss fest, dass die Nachverfolgung von Nutzerverhalten (Tracking) grundsätzlich auf eine Einwilligung gestützt werden kann, wenn alternativ ein trackingfreies Modell angeboten wird, auch wenn dieses bezahlpflichtig ist. Soweit mehrere Verarbeitungszwecke vorliegen, müssen Einwilligungen granular erteilt werden können. Mit dem Beschluss werden die Prüfmaßstäbe der Datenschutzaufsichtsbehörden in Beschwerdeverfahren für die Öffentlichkeit deutlich transparenter.

33.4 Beschwerden über den Beitragsservice

Wiederholt erreichten den Landesbeauftragten für den Datenschutz Beschwerden über den Beitragsservice der öffentlich-rechtlichen Rundfunkanstalten (früher: Gebühreneinzugszentrale). Unter anderem wurde dabei die Rechtmäßigkeit der Datenübermittlung von den Meldebehörden an die jeweilige Rundfunkanstalt bzw. den Beitragsservice in Frage gestellt. Allerdings mussten die Beschwerdeführer an den Rundfunkdatenschutzbeauftragten des Mitteldeutschen Rundfunks (MDR) verwiesen werden, da der Landesbeauftragte aufgrund des Medienprivilegs nicht die zuständige Aufsichtsbehörde für den MDR und den von den öffentlich-rechtlichen Rundfunkanstalten gemeinsam betriebenen Beitragsservice ist.

Gemäß § 42 Abs. 1 MDR-Staatsvertrag hat der MDR einen Rundfunkdatenschutzbeauftragten ernannt, der zuständige Aufsichtsbehörde im Sinne des Art. 51 DS-GVO ist und der die Einhaltung der Datenschutzvorschriften des MDR-Staatsvertrages, des Rundfunkstaatsvertrages, der DS-GVO und anderer Vorschriften über den Datenschutz bei der gesamten Tätigkeit des MDR und seiner Beteiligungsunternehmen überwacht.

Die Beschwerdeführer wurden jedoch darüber informiert, dass im Zusammenhang mit der Erhebung des Rundfunkbeitrags die Datenübermittlung der Meldebehörde an den MDR ohne deren Einwilligung erfolgen kann. Gemäß § 7 Abs. 1 Ausführungsgesetz des Landes Sachsen-Anhalt zum Bundesmeldegesetz (BMG-AG LSA) darf die Meldebehörde dem MDR und dem Beitragsservice zum Zwecke der Erhebung und des Einzugs der Rundfunkbeiträge im Falle der Anmeldung einer alleinigen Wohnung oder Hauptwohnung, einer An- oder Abmeldung einer Nebenwohnung oder des Todes folgende Daten volljähriger Einwohner übermitteln:

1. Familienname,
2. Vornamen,
3. Doktorgrad,

[58] https://www.datenschutzkonferenz-online.de/media/pm/DSK_Beschluss_Bewertung_von_Pur-Abo-Modellen_auf_Websites.pdf

4. Geburtsdatum,
5. derzeitige und letzte frühere Anschrift, Haupt- und Nebenwohnung, bei Zuzug aus dem Ausland auch die letzte Anschrift im Inland,
6. Einzugsdatum, Auszugsdatum,
7. Sterbedatum.

Außerdem dürfen im Falle einer Namensänderung neben dem früheren Namen die Nummern 1 bis 5 übermittelt werden.

34 Öffentliche Sicherheit

34.1 Einhaltung datenschutzrechtlicher Vorschriften beim Landeskriminalamt und der Verfassungsschutzbehörde

Entsprechend der Aufgabenzuweisung in § 23 Abs. 2 Datenschutz-Grundverordnungs-Ausfüllungsgesetz Sachsen-Anhalt (DSAG LSA) kontrollierte der Landesbeauftragte die Einhaltung datenschutzrechtlicher Vorschriften bei der Verwendung der Antiterrordatei (ATD) sowie der Rechtsextremismusdatei (RED) durch das Landeskriminalamt Sachsen-Anhalt (LKA) und die Verfassungsschutzbehörde. Nach den §§ 10 Abs. 2 Antiterrordateigesetz (ATDG) und 11 Abs. 2 Rechtsextremismus-Datei-Gesetz (RED-G) besteht die Verpflichtung zur datenschutzrechtlichen Kontrolle mindestens alle zwei Jahre.

Der Landesbeauftragte führte bei den genannten Behörden die Kontrolle der ATD und der RED anhand repräsentativer Stichproben durch. Insgesamt ergab die Kontrolle in zwei Fällen die Notwendigkeit einer weitergehenden Prüfung durch die kontrollierte Stelle. Die Prüfung führte im Ergebnis zur Löschung der Eintragungen.

Der Landesbeauftragte konnte die Kontrolle ohne förmliche Beanstandungen beenden.

35 Rechtspflege und Justizvollzug

35.1 Beauftragung von Dienstleistern für den Versand der Gerichtspost

Aufgrund einer Beschwerde hatte sich der Landesbeauftragte mit der Beauftragung von Postdienstleistern für die Justiz des Landes Sachsen-Anhalt zu befassen. Hintergrund war das scheinbar häufige Verlorengehen von Gerichtspost durch einen Unterauftragnehmer.

Im Rahmen der Ermittlungen stellte sich tatsächlich heraus, dass der betroffene Dienstleister bei Mängelanzeigen überproportional in Erscheinung tritt, allerdings bewegte sich die Mängelquote insgesamt – es handelte sich um mehrere Millionen Zustellungen – dennoch nur im Promillebereich, so dass ein datenschutzrechtlich relevantes Auswahlverschulden der Justiz des Landes Sachsen-Anhalt nicht festzustellen war.

Die im Beschwerdeverfahren zu Tage getretenen Schwachstellen und die daraus gewonnenen Erkenntnisse konnte die Justiz sogleich für das anstehende neue Ausschreibungsverfahren berücksichtigen, so dass für die Zukunft mit einer weiteren Verringerung der Mängelquote zu rechnen sein wird.

36 Forschung

36.1 Datenschutz in der Forschung durch einheitliche Maßstäbe stärken

Auch im Jahr 2023 hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder intensiv mit dem Datenschutz in der Forschung befasst. Um ein hohes Datenschutzniveau in der medizinischen Forschung zu erreichen wurden Eckpunkte erarbeitet, mit denen sich durch eine aufeinander abgestimmte zeitnahe rechtsklare und systematische Neustrukturierung der entsprechenden rechtlichen Regelungen ein hohes Datenschutzniveau in der medizinischen Forschung erreichen lässt. Die Eckpunkte werden in der Entschließung „Datenschutz in der Forschung durch einheitliche Maßstäbe stärken“[59] vom 23. November 2023 aufgezeigt. Die Unterstützung bei entsprechenden Gesetzesvorhaben bieten die Datenschutzaufsichtsbehörden im Rahmen ihrer Beratungsfunktion an.

36.2 Regulierung gesetzlicher Register

Wissenschaftliche Forschung mit Gesundheitsdaten ist essentiell, um neue Therapien zu entwickeln und bestehende Behandlungsverfahren zu überprüfen und zu verbessern. Neben klinischen Studien gehören die medizinischen Register zu den wichtigsten Datengrundlagen. Mit dem Ziel einer vereinfachten Nutzung von Registerdaten hat das Bundesministerium für Gesundheit begonnen, ein Registergesetz zu erarbeiten. Da in der „Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (vgl. Beitrag „Petersberger Erklärung“, Nr. 20.2) kaum registerbezogene Erwägungen enthalten sind, wurde die Entschließung vom 22. und 23. November 2023 „Rahmenbedingungen und Empfehlungen für die gesetzliche Regulierung medizinischer Register“[60] gefasst. Aufgrund der vielen, sehr unterschiedlichen medizinischen Register wird das Vorhaben der Bundesregierung, einen allgemeinen Rahmen und eine einheitliche Basis zu schaffen, um Daten im öffentlichen Interesse nutzen zu können, aus datenschutzrechtlicher Sicht grundsätzlich begrüßt. Insbesondere sind klare gesetzliche Regelungen hinsichtlich der Übermittlung personenbezogener Daten an das Register zu schaffen, soweit diese nicht durch Einwilligungen gedeckt sind. Die Aufbewahrungsdauer und Löschfristen sind festzulegen. Hinsichtlich der Verarbeitung von Registerdaten, einschließlich der Übermittlung an Dritte, sind konkrete und verhältnismäßige Voraussetzungen zu definieren.

---

[59] https://www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliessung_DS.pdf

[60] https://www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliessung_medRegister.pdf

37 Schulwesen

37.1 Bildungsmanagementsystem

Der Landesbeauftragte begleitet seit Jahren den Aufbau und die Entwicklung des Bildungsmanagementsystems als IT-gestütztes Schulverwaltungsverfahren nach § 87f SchulG LSA (siehe XVI. Tätigkeitsbericht, Nr. 11.2.3). Auch im Berichtszeitraum erfolgten regelmäßig ein Austausch von schriftlichen Ausarbeitungen und Gespräche zu den rechtlichen Ausgestaltungen. So fanden u. a. Abstimmungen über die Ausgestaltung der Hilfe des Bildungsministeriums für die Schulen bei der Datenmigration, die Ausgestaltung des Verzeichnisses der Verarbeitungstätigkeiten und der Datenschutz-Folgenabschätzung, die Frage der beteiligten Verantwortlichen und der insoweit zu schließenden Vereinbarungen sowie einzelne Funktionen des Systems statt. Insbesondere wurde seitens des Landesbeauftragten darauf hingewiesen, dass es infolge des umfangreichen Umgangs mit Schülerdaten dringend eines tragfähigen Datenschutzkonzepts bedarf. Der Landesbeauftragte wird das Bildungsministerium insoweit weiter beraten.

37.2 Behördliche Datenschutzbeauftragte der Schulen

Der Landesbeauftragte wirkt seit vielen Jahren gegenüber dem Bildungsministerium auf eine angemessene Ausstattung der Schulen mit behördlichen Datenschutzbeauftragten ein (siehe dazu XVII. Tätigkeitsbericht, Nr. 12.2). Gemäß der Möglichkeit nach Art. 37 Abs. 3 DS-GVO wurden im Februar 2021 zwei zentrale schulische Datenschutzbeauftragte jeweils für den Schulamtsbereich Nord und Süd eingesetzt. Die Schulen sollten jeweils Ansprechpartner benennen. Zu Beratungszwecken findet mit den beiden behördlichen Datenschutzbeauftragten häufig ein telefonischer oder schriftlicher Austausch statt. Im Berichtszeitraum hat der Landesbeauftragte die beiden Datenschutzbeauftragten besucht.

Zusammenfassend war erkennbar, dass es den beiden Datenschutzbeauftragten möglich ist, auf einzelne Anfragen und Beschwerden zu reagieren, proaktives agieren dagegen nicht. Umfassende Beratungen oder gar die gebotene Wahrnehmung von Kontrollaufgaben vor Ort in den Schulen sind nicht möglich. Regelmäßige flächendeckende Schulungen müssen durch gelegentliche Teilnahme an Schulleiterdienstberatungen und seltene Ergänzungen der „Handreichung Datenschutz an Schulen“ substituiert werden. Für sinnvolle Maßnahmen zentral gesteuerter Beratung, wie z. B. Newsletter, ist keine Kapazität vorhanden. Auch wäre angesichts der fortschreitenden Digitalisierung zielführend, für technische Themen zusätzlich eine entsprechend ausgebildete Person (Informatiker) als behördlichen Datenschutzbeauftragten einzusetzen. Hinzu kommt, dass wohl etwa drei Viertel der Schulen der Aufforderung der Benennung von Ansprechpartnern in der Schulleitung für die schulnahe Kommunikation in Datenschutzfragen bisher nicht nachgekommen sind. Der Landesbeauftragte hat daher dringend angeraten, Haushaltsvorsorge für mindestens zwei weitere behördliche Datenschutzbeauftragte der Schulen zu schaffen und sodann entsprechende Ausschreibungen vorzunehmen.

37.3 Elterneinsicht in WhatsApp-Chatgruppe

Eine Mutter hatte sich an den Landesbeauftragten mit der Frage gewandt, ob es Personensorgeberechtigten erlaubt sei, heimlich und ohne Zustimmung des Kindes dessen WhatsApp-Nachrichten zu lesen, diese abzufotografieren und an Dritte weiterzugeben. Es wurde dargelegt, dass sich Schüler (14 Jahre alt) in einer WhatsApp-Gruppe über mehrere Lehrerkräfte in übelster Weise beleidigend geäußert haben. Von einem Schüler aus der WhatsApp-Gruppe habe dessen Mutter den Chatverlauf abfotografiert und an die Klassenlehrerin weitergegeben, was zu entsprechender Aufarbeitung in der Schule führte.

Der Petentin wurde dazu erläutert, dass Eltern nicht nur das Recht, sondern auch die Pflicht haben, sich um die Pflege und Erziehung zu kümmern (Art. 6 Abs. 2 GG). Die elterliche Pflicht umfasst auch die Aufsicht und Kontrolle der Abwehr möglicher Gefahren bei der Nutzung von digitalen Medien, wie WhatsApp. Überlassen Eltern ihrem minderjährigen Kind ein digitales Gerät (z. B. Smartphone) zur dauernden eigenen Nutzung, entsteht damit auch die Pflicht, die Nutzung zum Schutz des Kindes zu begleiten. Dazu gehört grundsätzlich auch, sich darüber zu informieren, ob und inwieweit Bedarf besteht, das Kind bzw. den Jugendlichen vor Gefahren zu warnen und auf die Notwendigkeit der Achtung der Rechte Dritter hinzuweisen (siehe dazu AG Bad Hersfeld, Beschluss vom 20. März 2016, Az.: F 111/17 EASO, www.openjur.de). Ein Zugriff von Eltern auf Smartphones der minderjährigen Kinder kann daher grundsätzlich zulässig sein. Bei der Frage, ob und wann im Einzelfall ein Zugriff vertretbar ist, ist allerdings auch zu berücksichtigen, dass das Agieren mit dem Smartphone angesichts des heute üblichen Nutzungsumfangs in ganz erheblicher Weise auch die Persönlichkeitsrechte des Kindes bzw. Jugendlichen betrifft. Der Zugriff auf das Handeln und die Selbstdarstellung betrifft das datenschutzrechtliche Grundrecht (Art. 1 Abs. 1 Satz 1 i. V. m. Art. 2 Abs. 1 GG, Art. 8 Abs. 1 EU GRCh) und das Grundrecht auf geschützte Privatsphäre (Art. 7 EU GRCh). Entsprechende Eingriffe sind daher auf ein Minimum zu begrenzen. Hat das Kind einen Grad der Einsichtsfähigkeit erreicht, der es dazu befähigt, selbst verantwortlich zu handeln und seine Persönlichkeitsrechte wahrzunehmen (i. d. R. etwa ab 16 Jahren), dürfte der Schutz des Persönlichkeitsrechts das Recht der Eltern zur Beaufsichtigung überwiegen. Gegen die Übermittlung der Erkenntnisse der Einsicht an die Schule zur Aufarbeitung des Diskussionsniveaus bestanden angesichts der ggf. strafrechtsrelevanten Inhalte des Chats keine Bedenken.

37.4 WhatsApp in der Schule

Eine Schulleiterin hatte sich an den Landesbeauftragten mit der Bitte um Informationen gewandt, ob die Kommunikation über WhatsApp zwischen Schülern, Lehrpersonal und Eltern datenschutzkonform sei. Der Schulleiterin wurde dargelegt, dass gegen den Einsatz von „WhatsApp“ für schulische Zwecke, also zur dienstlichen Kommunikation zwischen Lehrpersonal und Schülern sowie Eltern, erhebliche datenschutzrechtliche Bedenken bestehen. Die Nutzung dieses Kommunikationsmediums kann daher trotz seiner Verbreitung nicht empfohlen werden. Insbesondere wäre der Ausschluss von schulischer Kommunikation für die, die WhatsApp aus nachvollziehbaren Gründen nicht nutzen, zu vermeiden. Bei der Nutzung von WhatsApp werden automatisch Adressbuchdaten aus den Smartphones ausgelesen und an WhatsApp übermittelt. Erfolgt diese Übermittlung ohne, dass die Betroffenen darin eingewilligt haben, liegt ein Verstoß gegen Art. 5 Abs. 1 lit. a, Art. 6 Abs. 1 DS-GVO vor. Für die Verwendung der

Metadaten (wer hat wann mit wem kommuniziert) durch WhatsApp für eigene wirtschaftliche Zwecke und die Weitergabe dieser personenbezogenen Daten innerhalb des Facebook-Konzerns zu allen möglichen Zwecken, existiert keine Rechtsgrundlage. Durch die Zusammenführung dieser Daten können umfangreiche Kontakt- und Kommunikationsprofile erstellt werden. Weiter müsste WhatsApp als Kommunikationsdienstleister wohl datenschutzrechtlich als Auftragsverarbeiter eingebunden werden, um unzulässige Übermittlungen (§ 84a Abs. 8 Satz 2 SchulG LSA) zu vermeiden. Der dazu notwendige Auftragsverarbeitungsvertrag setzt aber nach Art. 28 DS-GVO inhaltliche Vereinbarungen voraus, die mit WhatsApp kaum realisierbar sein dürften. Soweit beabsichtigt wäre, WhatsApp auf der Basis von Einwilligungen zu verwenden, wären die hohen Anforderungen von Art. 7 und Erwägungsgrund 32, 42 und 43 DS-GVO zu beachten, was insbesondere infolge der fraglichen Freiwilligkeit schwierig wäre. Zudem besteht die Gefahr, dass auf privaten Geräten gespeichert und mit privaten Daten vermischt werden.

37.5 Umsetzung des Energiepreispauschalengesetzes

Im Hinblick auf den immensen Anstieg der Energiepreise im Winter 2022/2023 hat der Bundestag das Energiepreispauschalengesetz (EPPSG) im Dezember 2022 verabschiedet und Studierenden und Fachschulbesuchern einen gesetzlichen Anspruch auf eine Zahlung von 200,- € eingeräumt. Anspruchsberechtigt waren ca. 3,5 Millionen Betroffene. In der Zeit von März 2023 bis September 2023 war es gelungen, ca. 2,8 Millionen Auszahlungen vorzunehmen. Die Umsetzung sollte nach dem „Einer für Alle – Verfahren“ durch ein zentrales Antragsportal erfolgen, das die bundesweit Antragsannahme und Prüfung übernimmt und die Anträge an die zuständigen Stellen in den Ländern zur Auszahlung weiterleitet. Infolge der Themenfeldzuständigkeit Sachsen-Anhalts für Bildung im Bereich der Umsetzung des Onlinezugangsrechts bestimmte die Verwaltungsvereinbarung von Bund und Ländern zur Umsetzung des EPPSG das Ministerium für Infrastruktur und Digitales (MID) für die vorgeschaltete Internetseite „Einmalzahlung200.de“ sowie für das Antragssystem als datenschutzrechtlich Verantwortlichen.

Das MID hat den Landesbeauftragten um Beratung gebeten. Unterlagen zu Überlegungen zur Ausgestaltung des Verfahrens, die zwischen den Beteiligten (Bundes- und Länderministerien) beraten wurden, wurden zu Beginn des Jahres 2023 dem Landesbeauftragten überlassen. Das Verfahren sollte digital umgesetzt werden. Dazu sollte auf bewährte Programme zurückgegriffen werden. Zu den rechtlichen Grundlagen wurde frühzeitig mitgeteilt, sich am Projekt BAföG Digital orientieren zu wollen. Seitens des Landesbeauftragten wurde zu der rechtlichen Grundkonstruktion auf bestehende Bedenken hingewiesen, da eine sicher tragfähige Rechtsgrundlage für die umsetzende Stelle von derartigen Einer-für-Alle Verfahren in einer Ergänzung des Onlinezugangsgesetzes aktuell noch in Planung war. Da die jeweiligen Länderministerien auch die für sie zuständigen Aufsichtsbehörden beteiligten hat letztlich auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einem Schreiben an das MID auf einige grundlegende Bedenken hingewiesen.

Weiter gingen einige Beschwerden beim Landesbeauftragten ein, die beklagten, dass ein Zugang zur erfolgreichen Antragstellung nur möglich war, wenn der Antragsteller sich zuvor bei dem Nutzerkonto BundID beim Bundeministerium des Innern und für Heimat registrierte. Die Antragsteller wurden, nachdem sie von ihrer Ausbildungsstelle

einen Zugangsschlüssel und ggf. eine PIN erhalten hatten, vom Antragsportal zunächst zur Registrierung auf die Seiten des Nutzerkontos BundID geleitet. Von dort wurden einige der dort eingetragenen Daten sodann in das Antragsverfahren übernommen. Dies war für die Masse der Antragsteller zu Zwecken der Authentifizierung grundsätzlich sinnvoll, um ein schnelles und sicheres digitales Verfahren zu ermöglichen. Für diejenigen, die ihre persönlichen Daten aber nicht bei BundID eingeben wollten und die sich über das Pin-Verfahren hätten authentifizieren können, gab es keine Alternative. Nach Auffassung des Landesbeauftragten war die Authentifizierung ohne BundID mit Hilfe der PIN möglich und die wenigen von BundID übernommenen Daten hätten auch direkt eigegeben werden können. Die Direkteingabe war für andere Daten (z. B. Bankverbindung) ohnehin eröffnet. Der Landesbeauftragte hat das MID frühzeitig darauf hingewiesen, dass eine Nutzung des Antragsportals auch ohne Einbindung von BundID angeboten werden müsse. Zwar hatte § 7 Abs. 1 EPPSG-DVO LSA wie die übrigen Landesverordnungen zur Umsetzung des EPPSG die Nutzung von BundID vorgegeben und § 6 Satz 2 EPPSG-DVO LSA eine andere Art der Antragstellung ausgeschlossen. Die Verordnung war aber insoweit nicht tragfähig, da die Ermächtigungsnorm des EPPSG lediglich vorsah, dass die Landesverordnungen die zuständigen Stellen bestimmen. Auch war dem Bundesgesetz zu entnehmen, dass es gerade kein spezifisches Verfahren vorgeben wollte. Zudem verstieß die zwingende Einbindung von BundID gegen die bundesrechtlich vorrangige Bestimmung in § 2 Abs. 5 OZG, wonach die Nutzung von BundID freiwillig ist. Wenn man aber den gesetzlich bestehenden Anspruch auf die Einmalzahlung nicht verwirklichen kann, wenn man nicht bei BundID Daten eingibt, kann von Freiwilligkeit keine Rede sein. Das MID hat trotz der Hinweise des Landesbeauftragten bis zum Ende des Verfahrens keine für Antragsteller auffindbare Alternative angeboten und weiter in den Veröffentlichungen (FAQ) auf die Notwendigkeit der Nutzung von BundID verwiesen.

38 Gesundheitswesen

38.1 Cloudbasierte Gesundheitsanwendungen (Beschluss)

Digitale Gesundheitsanwendungen sind bestimmte digitale Medizinprodukte, die bei der Behandlung von Erkrankungen oder dem Ausgleich von Beeinträchtigungen unterstützen können. Da sie häufig als Apps für das Smartphone verfügbar sind, werden sie auch Apps auf Rezept genannt. Es gibt sie jedoch auch als browserbasierte Webanwendungen oder Software zur Verwendung auf Desktop-Rechnern. Seit 2020 ist für die erstattungsfähigen digitalen Gesundheitsanwendungen gemäß § 33a Sozialgesetzbuch V (SGB V) die Digitale Gesundheitsanwendungen-Verordnung (DiGAV) in Kraft. Sie regelt, dass digitale Gesundheitsanwendungen die gesetzlichen Vorgaben des Datenschutzes und die Anforderungen an die Datensicherheit nach dem Stand der Technik unter Berücksichtigung der Art der verarbeiteten Daten und der damit verbundenen Schutzstufen sowie des Schutzbedarfs gewährleisten (§ 4 Abs. 1 DiGAV) müssen.

Neben diesen gesetzlich geregelten digitalen Gesundheitsanwendungen gibt es jedoch eine Vielzahl weiterer, die nicht von diesen Regelungen erfasst sind. Für den Einsatz dieser Anwendungen hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. November 2023 das „Positionspapier zu cloudbasierten

Gesundheitsanwendungen“ beschlossen.[61] Hinsichtlich der datenschutzrechtlichen Verantwortlichkeiten, der Verwendung der Gesundheitsanwendungen, der Nutzung personenbezogener Daten zu Forschungszwecken und zur Qualitätssicherung, der Sicherheit der Verarbeitung, zu den Betroffenenrechten und zu Datenübermittlungen in Drittländer werden ausführliche Hinweise gegeben.

38.2 Coronamaßnahmen – Datenlöschung

Aufgrund der Beendigung von Maßnahmen zur Pandemiebekämpfung ist in Bezug auf die sogenannte 3-G-Regelung am Arbeitsplatz und der Anwesenheitsnachweise, z. B. bei Veranstaltungen, die Rechtsgrundlage für die Datenspeicherung entfallen. Der Landesbeauftragte hat dies zum Anlass genommen, auf die Löschpflicht nach Art. 17 Abs. 1 lit. a DS-GVO hinzuweisen. Die Hinweise „Coronamaßnahmen – Daten löschen nicht vergessen“ sind auf seiner Homepage veröffentlicht.

38.3 Datenpannen im Universitätsklinikum

In den Monaten um den Jahreswechsel gingen beim Landesbeauftragten sechs Meldungen von Datenschutzverletzungen aus einem Universitätsklinikum ein. In den Fällen bestand der Verdacht, dass Beschäftigte unbefugt im Krankenhausinformationssystem (KIS) auf Patientendaten zugegriffen haben. Anlass der Prüfungen in einem sogenannten Patientenschutzverfahren des Universitätsklinikums waren die Anregungen der jeweils betroffenen Patienten, die den Verdacht hegten, es sei auf ihre Daten unbefugt zugegriffen worden. Nachdem die Universitätsklinik im Rahmen der internen Prüfung anhand der Zugriffsprotokolle und durch Nachfragen bei den Beschäftigten den Verdacht bestätigt fand, hat sie gemäß Art. 33 Abs. 1 DS-GVO Meldungen von Datenschutzverletzungen an den Landesbeauftragten gesandt. Der Landebeauftragte hat die Fälle aufgegriffen und anhand angeforderter Unterlagen und Stellungnahmen untersucht.

In einem Fall hatte eine Psychologin Zugriff auf Daten einer ihr bekannten Patientin genommen, die in einer gynäkologischen Klinik behandelt worden war. Um im KIS auf die Daten einen Zugriff zu haben, der für sie nicht hinterlegt war, konnte sie über die Suche des Namens eine sogenannte Datenschutzmaske öffnen. Dort können verschiedene aufgeführte Gründe angeklickt werden, wie z. B. Notfall oder Konsil. Sodann wird der Zugriff technisch gewährt. Eine Benachrichtigung der für die Patienten verantwortlichen Beschäftigten bzw. eine generelle Überprüfung dieser besonderen Zugriffe ist nicht vorgesehen. Die Psychologin hatte den Grund „Konsil“ angeklickt. Die Universitätsklinik hat aber nach Prüfung infolge der Anregung der Betroffenen keinen Konsilgrund feststellen können. Die zugreifende Psychologin fand verschiedene, nicht überzeugende Begründungen, wie z. B. die Suche nach einem gleich- bzw. ähnlichnamigen Patienten. Nach Überprüfung konnte aber festgestellt werden, dass es keinen derartigen Patienten im zeitlichen und fachlichen Zusammenhang gab. Im zweiten Fall griff eine Sekretärin einer chirurgischen Klinik auf Daten einer ihr privat bekannten Patientin einer anderen chirurgischen Klinik aus Neugier zu. Sie verwandte auch die Datenschutzmaske und die Angabe „Konsil“. Im dritten Fall griff eine Pflegekraft aus der

[61] https://www.datenschutzkonferenz-online.de/media/dskb/2023_11_06_Beschluss_cloudbasierte_digitale_Gesundheitsanwendungen.pdf

Zentralen Notaufnahme mit übergreifender Zugriffsbefugnis auf Daten einer befreundeten Patientin in einer gynäkologischen Klinik zu. Im vierten Fall hat eine weitere Pflegekraft mit übergreifenden Zugriffsbefugnissen aus einer anderen Klinik ebenfalls auf die Daten einer befreundeten Patientin in einer gynäkologischen Klinik zugegriffen. Fall fünf betraf eine Pflegekraft mit Leitungsfunktionen, die ebenfalls mit übergreifenden Zugriffsbefugnissen ausgestattet auf die Corona-Testdaten einer Mitarbeiterin zugriff. Zuletzt hat eine Pflegekraft aus einer hämatologischen Klinik, die aus nicht ganz nachvollziehbaren Gründen Zugriffsrechte auf eine chirurgische Klinik hatte, dort Daten einer ihr bekannten Patientin angesehen.

Auch der Landesbeauftragte kam nach seiner Prüfung zu dem Schluss, dass die jeweiligen Beschäftigten im Rahmen eines Mitarbeiterexzesses aus rein privaten Motiven von den faktischen Zugriffsmöglichkeiten Gebrauch machten. Somit wurden unbefugt personenbezogene Patientendaten, die gesetzlich besonders geschützt sind, verarbeitet, ohne dass eine Rechtsgrundlage ersichtlich war. Das Interesse in Bezug auf befreundete oder bekannte Personen kann einen Zugriff nicht rechtfertigen, da der Schutz des Patientengeheimnisses dem klar entgegensteht. Der Landesbeauftragte hat daher Bußgeldverfahren eingeleitet. Lediglich in einem Fall konnte der Zugriff nicht sicher der verdächtigen Person nachgewiesen werden.

Wo Missbrauch möglich ist, findet Missbrauch statt. Die zeitlich nah zusammenliegenden Vorgänge wurden nur entdeckt, weil zufällig die richtigen Betroffenen nachgefragt haben. Sie lassen den Umfang der Dunkelziffer erahnen. Die Zugriffe auf Patientendaten einfach durch Anklicken auf Konsil, Notfall oder ähnliches zuzulassen, ohne dies systematisch zu kontrollieren, wird dem Vertraulichkeitsgebot der Art. 5 Abs. 1 lit. f, Art. 32 DS-GVO wohl nicht gerecht. Seitens eines Datenschutzteams werden in der Universitätsklinik zwar einige, wenige Vorgänge pro Jahr einer Stichprobenprüfung unterzogen. Ob und inwieweit ein angemessener Schutz der Vertraulichkeit der Patientendaten dadurch erreicht wird, erscheint jedoch offensichtlich mehr als fraglich. Dies bedarf einer weiteren Betrachtung.

38.4 Nutzung der Patiententelefonnummer für private Zwecke

Von der Staatsanwaltschaft bekam der Landesbeauftragte einen Vorgang eines eingestellten Ermittlungsverfahrens übersandt. Anlass war die Strafanzeige der Mutter einer Tochter, der von einem Jungen auf dem Rückweg von der Schule ein Bein gestellt wurde, was letztlich wohl dazu führte, dass die Tochter in die Notaufnahme gebracht und später wohl auch operiert wurde. Die Mutter der Tochter hatte Strafanzeige gestellt. Bei der später folgenden Vernehmung der Mutter des Jungen stellte diese ebenfalls einen Strafantrag. Die Mutter der Tochter hatte am Tattag als Mitarbeiterin einer Arztpraxis die Telefonnummer der Mutter des Jungen als Patientin der Praxis verwandt, um letztere anzurufen und über das Vorgefallene zu informieren. Die Erlaubnis der Praxisinhaberin, die Daten für private Zwecke zu nutzen, konnte nicht eindeutig nachgewiesen werden. Die Mutter der Tochter ließ sich dahin ein, dass es lediglich darum gegangen sei, der anderen Mutter in nur einem Anruf die Folgen des Tuns ihres Sohnes zu verdeutlichen. Die Telefonnummer habe sie direkt nach dem Gespräch gelöscht.

Die Telefonnummer war ein personenbezogenes Datum, dass der Praxisinhaberin im Rahmen ihrer beruflichen Tätigkeit bekannt geworden war und damit der ärztlichen Schweigepflicht und der Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO) unterlag. Weiter

war das generelle Interesse der Mutter des Jungen zu berücksichtigen, dass ihre Telefonnummer nicht über den von ihren Zweckbestimmungen begrenzten Bereich hinaus Verwendung findet. Die Mutter der Tochter hatte nur Zugang im Rahmen ihrer Tätigkeit als berufliche Gehilfin, der Zugriff für private Zwecke war daher unbefugt. Eine tragfähige Rechtsgrundlage für die private Nutzung war trotz eines nachvollziehbaren Interesses letztlich nicht ersichtlich. Da über den einen Anruf hinaus kein weiterer Schaden entstanden war, hat es der Landesbeauftragte bei einer Verwarnung der Mutter der Tochter belassen.

39 Beschäftigtendatenschutz

39.1 Erhöhter Regelungsbedarf im Beschäftigtendatenschutz

Der Europäische Gerichtshof (EuGH, 30. März 2023, Rechtssache C-34/21, juris) hatte über die Anforderungen an eine europarechtskonforme Umsetzung des Beschäftigtendatenschutzrechts in Hessen zu entscheiden. In seinem Urteil stellt der EuGH hohe Anforderungen an nationale Vorschriften, die auf der Grundlage der Öffnungsklausel des Art. 88 DS-GVO erlassen werden. Die Entscheidungsgründe legen nahe, dass § 23 Abs. 1 Satz 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes und § 86 Abs. 4 des Hessischen Beamtengesetzes diesen Anforderungen nicht genügen. Die Entscheidung des EuGHs entfaltet bundesweit Bedeutung, weil die Gesetzgeber nun prüfen müssen, ob bestehende Regelungen den Anforderungen des Art. 88 DS-GVO entsprechen. Die Regelungen dürfen nicht nur die Bestimmungen der DS-GVO wiederholen, sondern müssen spezifischer sein (siehe Art. 88 Abs. 1 DS-GVO) und insbesondere nach Art. 88 Abs. 2 DS-GVO grundrechtsschützende Vorgaben enthalten. Nationale Regelungen im Beschäftigtenkontext, die nicht den Vorgaben der DS-GVO entsprechen, müssen dem Urteil nach unangewendet bleiben. Das Bundesarbeitsgericht (BAG 1 ABR 14/22, 9. Mai 2023, juris) hat bereits seine Rechtsprechung aufgegeben, wonach die der hessischen Regelung entsprechende Regelung in § 26 Abs. 1 Satz 1 BDSG (Begründung, Durchführung, Beendigung des Beschäftigungsverhältnisses) den Anforderungen des Art. 88 DS-GVO genüge. Zur Betonung der Dringlichkeit des Regelungsbedarfs hat die DSK am 11. Mai 2023 die Entschließung „Notwendigkeit spezifischer Regelungen zum Beschäftigtendatenschutz! Rechtsprechung des Europäischen Gerichtshofs hat Auswirkungen auf zahlreiche deutsche Vorschriften im Beschäftigungskontext“ gefasst.[62] Zur Rechtfertigung der Verarbeitung von Beschäftigtendaten im nicht-öffentlichen Bereich ist daher derzeit auf Art. 6 Abs. 1 DS-GVO zurückzugreifen. Inwieweit für den öffentlichen Bereich ein Rückgriff auf die bestehenden Normen - allerdings unter Stützung auf die weniger strenge Öffnungsklausel in Art. 6 Abs. 3 Satz 1 Buchstabe b DS-GVO – weiterhin möglich ist, bleibt abzuwarten. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit hat

[62] https://www.datenschutzkonferenz-online.de/media/en/2023-05-11_DSK-Entschliessung_Beschaeftigtendatenschutz.pdf

dazu die „Handreichung zur Verarbeitung personenbezogener Daten von Beschäftigten im Lichte des EuGH-Urteils vom 30. März 2023 Rs. C-34/21“ herausgegeben.[63]

39.2 Elektronisches Fahrtenbuch für die Dienstfahrzeuge

Eine Landesbehörde mit ca. 30 Dienstfahrzeugen, die ausschließlich für dienstliche Fahrten genutzt werden beabsichtigte, zur Erfüllung steuerlicher Dokumentations- und Aufzeichnungspflichten, zur Arbeitsvereinfachung und zur Entlastung der Mitarbeiter ein vollelektronisches und vollautomatisches Fahrtenbuch einzuführen und bat den Landesbeauftragten um Einschätzung. Erfasst werden sollten Start und Endzeit, Orte des Beginns und des Endes der Dienstfahrten sowie zurückgelegte Kilometer. Die Erfassung des Ortes sollte über GPS erfolgen. Geplant war, nur das für die Fahrtenbücher Notwendigste aufnehmen. Die Überwachung der Beschäftigten war ausdrücklich nicht beabsichtigt. Eine Ortung sollte allerdings für Notfälle und Ausnahmesituationen, wie etwa bei Gefahr für Leib und Leben oder wegen eines aufgrund objektiver und nachvollziehbarer Tatsachen begründeten Verdachts einer Straftat, möglich sein.

Auch wenn sich aus dem der Anfrage beigefügten Gutachten bereits die Berücksichtigung vielfältiger Aspekte des Beschäftigtendatenschutzes ergab, hat der Landesbeauftragte ergänzend auf offene Fragen und Bedenken hingewiesen. Zunächst war fraglich, ob das System in alle Fahrzeuge eingebaut werden soll und ob alle diese Fahrzeuge für lohnsteuerrechtlich relevante Fahrten genutzt werden. Reine Dienstfahrten vom Parkplatz des Fuhrparks zum Kunden und zurück zum Parkplatz des Fuhrparks haben keinerlei privaten Charakter, sodass sie lohnsteuerrechtlich wohl nicht relevant sein dürften. Weiter wurde wegen der bekannten Sorge der Auswertung der vorhandenen Daten in Bezug auf Geschwindigkeit(süberschreitungen), Beschleunigungs- und Bremsverhalten, Pausenzeiten und Abweichungen von vorgegebenen Fahrtrouten auf die notwendige, auch technische Einschränkung entsprechender Auswertungsmöglichkeiten hingewiesen. Datenerfassungen müssten durch überwiegende Interessen des Arbeitgebers gerechtfertigt und insgesamt verhältnismäßig sein. Zur Prüfung wäre daher anhand der Systembeschreibung des Betreibers aufzuführen, welche konkreten personenbeziehbaren Daten tatsächlich erfasst werden (Zündung an/aus, Kilometerstand am Tachometer, Fahrtstreckenverlauf, Bewegungsdaten (alle 60 m, alle 600 m), Geschwindigkeit, Drehzahl, Beschleunigung etc.) sowie welche Daten dem Zugriff offenstehen und für welche Zwecke sie verarbeitet werden. Die Hinweise im Konzept auf die Erfassung von Zwischenstopps, die reine Absicht, Überwachungen zu „verunmöglichen“ und die Hinweise auf die Fürsorgepflicht und den Schutz von Leben und Gesundheit der fahrenden Beschäftigten sowie den Zweck der Prävention begründeten auszuräumende Zweifel an den durch konkrete Notwendigkeiten begründeten überwiegenden Interessen der Landesbehörde.

Der Landesbeauftragte konnte aber deutlich machen, dass die Berücksichtigung datenschutzrechtlicher Anforderungen den angestrebten Vereinfachungen aber nicht grundsätzlich entgegenstehen. Es ist grundsätzlich in vielfacher Hinsicht zulässig, Beschäftigtendaten durch Fahrzeugsysteme mit GPS-Daten zu verarbeiten, wenn dies in

[63] https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2023-05/handreichung_beschaeftigtendatenschutz_eugh-urteil.pdf

der konkreten Anwendung erforderlich und verhältnismäßig ist. Die Reduktion auf das Notwendige muss im Blick bleiben. Zielt das GPS-System auf den Diebstahlschutz, dürfte die Erfassung erst eingeschaltet werden, wenn der Verdacht begründet ist, dass das Fahrzeug abhandenkam. Sind aktuelle Dispositionsentscheidungen zu treffen, wie z. B. bei Speditionen, kann durch Einschalten der Ortung kurzfristig festgestellt werden, welches Fahrzeug dem Einsatzort am nächsten ist. Auch in Bezug auf die Einhaltung der vertraglichen Verpflichtungen sind Überwachungen bzw. Leistungs- und Verhaltenskontrollen in Bezug auf Beschäftigte in sehr geringen Umfang datenschutzrechtlich grundsätzlich möglich, z. B. wenn es sich um angemessene Stichproben handelt, die keinen allgemeinen Überwachungsdruck entstehen lassen. Insgesamt konnte der Landesbeauftragte der Landesbehörde zu den einzelnen Zwecküberlegungen differenzierte Hinweise geben, deren Berücksichtigung die Landesbehörde zusagte.

39.3 Einsatz von WhatsApp zur betrieblichen Kommunikation

Ein Beschwerdefall im Berichtszeitraum nahm gleich mehrfach unerwartete Wendungen. Zunächst wandte sich ein Gastronomiebetrieb an den Landesbeauftragten und trug vor, eine ehemalige Beschäftigte habe private Kontaktdaten weiterer Beschäftigter aus einer Akte entnommen, die ausschließlich zum Zweck behördlicher Kontrollmaßnahmen vorgehalten wurde. Die Beschäftigte habe diese Daten im Rahmen einer Strafanzeige genutzt.

Zur Sachverhaltsaufklärung wandte sich der Landesbeauftragte zunächst an diese Beschäftigte, die sich allerdings auf ihr Auskunftsverweigerungsrecht nach § 40 Abs. 4 Satz 2 BDSG berief. Nach dieser Vorschrift kann die Auskunft auf solche Fragen verweigert werden, deren Beantwortung die Auskunftspflichtige selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 ZPO bezeichneten Angehörigen der Gefahr strafrechtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde.

Im Wege der Amtshilfe erhielt der Landesbeauftragte sodann von der zuständigen Staatsanwaltschaft, die die Strafanzeige prüfte, die Information, dass die Beschäftigte die Daten aus einer WhatsApp-Gruppe entnommen hatte, die der Gastronomiebetreiber zur Schichteinteilung nutzte.

Danach eröffnete der Landesbeauftragte eine Datenschutzüberprüfung bei dem Gastronomiebetreiber selbst. Denn die Eröffnung der WhatsApp-Gruppe führte dazu, dass allen Mitgliedern der Gruppe die privaten Telefonnummern aller weiteren Gruppenmitglieder angezeigt wurde, auch wenn diese zuvor nicht im Adressbuch der Gruppenmitglieder gespeichert waren. Dabei handelte es sich um eine Offenlegung und somit eine Datenverarbeitung i. S. d. Art. 4 Nr. 2 DS-GVO, die einer gesetzlichen Erlaubnis bedarf (vgl. Art. 6 Abs. 1 Satz 1 lit. a bis f DS-GVO). Bereits in dem XII. Tätigkeitsbericht des Landesbeauftragten, Nr. 5.10, im XIII. und XIV. Tätigkeitsbericht (Nr. 5.7) sowie im XVII. Tätigkeitsbericht (Nr. 14.1.3) wurden die datenschutzrechtlichen Bedenken bei der Nutzung des Messenger-Dienstes WhatsApp dargelegt.

Auch der Gastronomiebetreiber berief sich zunächst auf das ihm zustehende Auskunftsverweigerungsrecht. Dennoch ist es dem Landesbeauftragten im weiteren Verlauf gelungen, den Verantwortlichen zur Kooperation zu bewegen, intensiv zu beraten und zu einer datenschutzkonformen Lösung beizutragen.

Dabei stellte sich heraus, dass der Geschäftsführer des Unternehmens selbst zwei WhatsApp-Gruppen eröffnet und administriert hatte, eine Gruppe für jede seiner zwei gastronomischen Einrichtungen. Die Gruppe enthielt jeweils alle Beschäftigte, die in dem jeweiligen Lokal tätig waren und WhatsApp auf ihren privaten Endgeräten nutzten. Der Zweck war die interne Kommunikation und Abstimmung zu betrieblichen Abläufen, z. B. Reservierungsinformationen, Dienstplanabstimmung im Krankheitsfall, Vertretungsregelungen, Übermittlung von Einkaufslisten. Einwilligungen der Beschäftigten in die Offenlegung ihrer privaten Telefonnummer gegenüber den Kolleginnen und Kollegen und der weiteren persönlichen Informationen in der Gruppe, z. B. auch der Krankmeldungen, hatte der Geschäftsführer nicht eingeholt, wenn dies überhaupt wirksam möglich gewesen wäre (vgl. § 26 Abs. 2 BDSG).

Nach den aufsichtsbehördlichen Hinweisen stellte das Unternehmen die Nutzung des Messengers WhatsApp ein. Im Ergebnis weiterer eingehender Erörterung hat das Unternehmen letztlich auch alle Schritte unternommen, um die WhatsApp-Gruppen wirksam zu löschen und die Löschung aller aus den Gruppen verbliebenen Daten, auch bei den Beschäftigten, zu veranlassen. Dazu gehörten auch eine betriebliche Anweisung und Belehrung der Beschäftigten, dass sie zu prüfen haben, inwieweit sich auf ihren privaten Endgeräten noch personenbezogene Daten aus den Gruppen befinden, sowie sicherzustellen haben, dass sie berechtigt sind, diese Daten weiterhin zu verarbeiten, oder anderenfalls die Daten zu löschen. Dazu gehörte, dass die Chatverläufe der Gruppen in keinem Backup oder Export erhalten bleiben dürfen, dass keine Medieninhalte aus den Chatverläufen (z. B. Fotos, Videos, Sprachnachrichten usw.) im Speicher des jeweiligen privaten Endgeräts verbleiben (auch nicht in der Fotogalerie oder einem externen Speicher) und auch, dass die Telefonnummern der Gruppenmitglieder aus den Adressbüchern der weiteren Gruppenmitglieder gelöscht werden. Ausnahmen konnten nur zulässig sein, wenn vorher geprüft und festgestellt wurde, dass die weitere Verarbeitung der jeweiligen Daten auf eine gesetzliche Rechtsgrundlage oder eine Einwilligung der jeweils betroffenen Person gestützt werden kann. Zu der Belehrung gehörte auch der Hinweis, dass die Beschäftigten datenschutzrechtlich selbst dafür verantwortlich sind, wenn sie Datenverarbeitungen, die ihren Ursprung in der WhatsApp-Gruppe haben, unzulässigerweise fortführen.

Unternehmen dürfen WhatsApp nicht sorglos zur betrieblichen Kommunikation verwenden, nur weil die Anwendung ohnehin von vielen Beschäftigten auf ihren privaten Endgeräten genutzt wird. Das Einrichten einer WhatsApp-Gruppe mit Beschäftigten als Gruppenmitgliedern führt dazu, dass ihnen untereinander alle privaten Telefonnummern und die Kommunikationsinhalte aus der Gruppe bekannt werden. Dies ist mit gesetzlichen Erlaubnisnormen in der Regel nicht zu rechtfertigen.

40 Kommunales und Meldewesen

40.1 Live-Streams von Ratssitzungen

Der Landesbeauftragte wurde im Berichtszeitraum mehrfach mit Sachverhalten konfrontiert, die die datenschutzrechtliche Beurteilung sogenannter Live-Streams von Sitzungen eines Gemeinde-/Stadtrates oder Kreistages betreffen.

§ 52 Abs. 5 des Kommunalverfassungsgesetzes des Landes Sachsen-Anhalt (KVG LSA) eröffnet grundsätzlich diese Möglichkeit. Es bedarf aber zusätzlich noch einer entsprechenden Regelung in der Geschäftsordnung des Rates bzw. Kreistages.

Nach der Begründung zum Gesetzentwurf (Drucksache 6/2247 vom 04.07.2013) strebte der Landesgesetzgeber mit der Regelung eine ausdrückliche Öffnung über die Saalöffentlichkeit hinaus auf die Medienöffentlichkeit an. Der Landesbeauftragte für den Datenschutz hatte im Gesetzgebungsverfahren diesen gesetzgeberischen Willen anerkannt: Die Übertragung der öffentlichen Sitzungen - auch im Internet - sei ein zeitgemäßes Mittel, um Transparenz und bürgerschaftliche Kontrolle zu gewährleisten. Datenschutzrechtliche Bedenken würden unter dieser Prämisse nicht bestehen, solange das Kunsturhebergesetz (KUG) beachtet würde.

Die Regelung gewährt den Kommunen einen erheblichen Gestaltungsspielraum, schuf gleichzeitig aber auch einige Unsicherheiten. Nach früherer Rechtsprechung konnte man Mitglieder der kommunalen Vertretung als relative Personen der Zeitgeschichte ansehen, die sich ihre Darstellung in der Öffentlichkeit nach §§ 22, 23 Abs. 1 Nr. 1 und 3 KUG gefallen lassen müssten. Die Unterscheidung zwischen absoluten und relativen Personen der Zeitgeschichte musste nach einer Entscheidung des Europäischen Gerichtshofs für Menschenrechte (EGMR) aus dem Jahr 2004 allerdings aufgeben werden und wurde vom Bundesgerichtshof (BGH) durch das abgestufte Schutzkonzept ersetzt. Weil die Regelung des § 52 Abs. 5 Satz 3 KVG LSA sich hierzu nicht verhält, zwang sie das Organ der Kommune, diese Abwägung selbst vorzunehmen.

Mit Einführung der Datenschutz-Grundverordnung (DS-GVO) hat sich die Problemlage etwas aufgelöst, wenn auch beide, DS-GVO und §§ 22, 23 KUG, bis heute ein eher schwieriges Verhältnis pflegen. Problematisch ist, ob und inwieweit seit Geltung der DS-GVO noch Raum für die Anwendung der §§ 22, 23 KUG besteht, da die DS-GVO innerhalb ihres Geltungsbereichs Anwendungsvorrang vor nationalem Recht genießt. Im journalistischen Bereich beispielsweise steht nach der Rechtsprechung des BGH die DS-GVO der Anwendung der §§ 22, 23 KUG als nationale Regelung nicht entgegen. Bei diesen Normen handele es sich um nationale Ausgestaltungen der Öffnungsklausel des Art. 85 Abs. 2 DS-GVO. Für Kommunen stellt sich diese Privilegierungsfrage nicht. Hier ist also von einem Anwendungsvorrang der DS-GVO auszugehen.

Da § 52 Abs. 5 Satz 3 KVG LSA eine Regelung in der Geschäftsordnung bedingt, diese wiederum aber nur das Organ binden kann, wird für Dritte (z. B. die interessierte Öffentlichkeit) hinsichtlich des Live-Streams § 52 Abs. 5 KVG LSA nicht als Verarbeitungsgrundlage in Betracht kommen. Insoweit bedarf es also einer Einwilligung, so denn eine Aufnahme dieses Personenkreises überhaupt in Betracht kommen soll.

Der Landesgesetzgeber hat den Kommunen für einen Live-Stream der Rats- oder Kreistagssitzungen einen nicht unerheblichen Gestaltungsspielraum zur Verfügung gestellt. Dieser führt in der Praxis fast schon zwangsläufig zu einem erhöhten Beratungsbedarf, weil die Aufsichtsbehörde die behördlichen Datenschutzbeauftragten mit der Komplexität der Materie weder allein lassen kann noch möchte. Hierbei zeigte sich erfreulicherweise, dass aufgrund des Bestehens verschiedener Erfahrungsaustauschformate zwischen der Aufsichtsbehörde und den behördlichen Datenschutzbeauftragten keine Hemmschwelle besteht, Sachverhalte auch mal nur zur kurzen Bestätigung resp. Korrektur der eigenen Beurteilung an den Landesbeauftragten heranzutragen. Das versetzt die Aufsichtsbehörde in die günstige Möglichkeit, prophylaktisch agieren zu können und nicht erst im Nachhinein, z. B. im Beschwerdefall, eingreifen zu müssen.

40.2 Umfang des Auskunftsanspruches gemäß Artikel 15 Datenschutz-Grundverordnung (DS-GVO)

Kommunen werden regelmäßig mit Auskunftsansprüchen nach Art. 15 DS-GVO konfrontiert.

Der Anspruch ist gemäß Art. 12 Abs. 3 Satz 1 DS-GVO im Regelfall (kann verlängert werden) binnen eines Monats nach Antragseingang zu beantworten. Neben Fristfragen stellen sich auch immer wieder Fragen zum Umfang des Anspruches. Insbesondere die Frage, ob und, wenn ja, welche Kopien an die Antragsteller herauszugeben sind, steht immer wieder zur Beantwortung an.

Der Europäische Gerichtshof (EuGH) hat in seiner Entscheidung vom 4. Mai 2023 in der Rechtssache C-487/21 nunmehr etwas Klarheit in diese bisher recht umstrittene Frage gebracht.

Der EuGH ordnet hiernach Art. 15 Abs. 3 Satz 1 DS-GVO als Rechtsfolgenbestimmung der in Abs. 1 statuierten Pflicht zur Auskunft über personenbezogene Daten ein. Im Grundsatz erteilt der EuGH der extensiven Auffassung, Abs. 3 Satz 1 verpflichte den Verantwortlichen generell zur Kopie der die Daten enthaltenen Dokumente, eine Absage.

Allerdings kann sich zum Verständnis der bereitgestellten Informationen die Reproduktion von Auszügen aus Dokumenten oder gar von ganzen Dokumenten oder auch von Auszügen aus Datenbanken, die u. a. personenbezogene Daten enthalten, die Gegenstand der Verarbeitung sind, als unerlässlich erweisen, wenn die Kontextualisierung der verarbeiteten Daten erforderlich ist, um ihre Verständlichkeit zu gewährleisten.

Was bedeutet das für die Praxis?

Künftig werden Auskunftsbegehren wohl häufig zweistufig ausfallen können. Auf der ersten Stufe kann mit dem EuGH davon ausgegangen werden, dass kein Anspruch auf eine Kopie von Dokumenten oder Dateien besteht, sondern nur auf Beauskunftung von personenbezogenen Daten des Betroffenen.

Wenn der Betroffene daraufhin allerdings geltend macht, dass der Kontext, in dem seine personenbezogenen Daten verarbeitet werden und damit eine Gesamtschau der

vorliegenden Akte, Dateien und Dokumente, unerlässlich ist, um die Zulässigkeit der Verarbeitung zu überprüfen oder die Unzulässigkeit nachweisen zu können, wird man dem wohl häufig wenig entgegenzusetzen haben und auf der zweiten Stufe dann doch Daten und/oder Dokumente in Kopie herausgeben müssen.

Für die Kommunen (und auch alle anderen Auskunftspflichtigen) bleiben leider auch nach der Entscheidung des EuGH noch Fragen offen. Es bleibt zu hoffen, dass sich der vom EuGH eher als Ausnahme statuierte Fall nicht zur Regel entwickeln wird. Jedenfalls ist abzusehen, dass sich der Landesbeauftragte auch weiterhin mit entsprechenden Sachverhalten auseinanderzusetzen – sei es beratend oder auch im Rahmen der Beschwerdebearbeitung – haben wird.

41 Verwaltung allgemein

41.1 Datenschutzüberprüfung beim Postaustauschzentrum der Landesbehörden

Der zentrale Postaustausch innerhalb der Landesverwaltung findet zu großen Teilen in einem Postaustauschzentrum statt, welches sich in einem Dienstgebäude der Landesverwaltung in Magdeburg befindet. In dem Dienstgebäude wird ein Raum mit Postfächern für den Postaustausch vorgehalten.

In diesem Jahr fand durch den Landesbeauftragten eine anlasslose Datenschutzüberprüfung im Hinblick auf die datenschutzgerechte organisatorische Ausgestaltung des Postaustauschzentrums statt.

Hierbei musste der Landesbeauftragte feststellen, dass keine ausreichenden Kontrolleinrichtungen vorhanden waren, die einen unbefugten Zugang Dritter zum Dienstgebäude sowie zu den Räumlichkeiten und im Weiteren einen unbefugten Zugriff auf die in den Postfächern liegenden Schriftstücke mit personenbezogenen Daten verhinderten. Der Landesbeauftragte hat daher die zuständige Behörde aufgefordert, entsprechende Abhilfemaßnahmen einzuleiten.

Nach Aufforderung zur Beseitigung der festgestellten Verstöße wurden durch die zuständige Behörde entsprechende technisch-organisatorische Maßnahmen zum Ausschluss eines unbefugten Zutritts veranlasst. Der Landesbeauftragte konnte sich im Wege einer unangekündigten Nachprüfung von der Umsetzung der Maßnahmen überzeugen.

42 Wirtschaft

42.1 Aktuelle Meldungen von Datenschutzverletzungen

Die Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden nach bekanntwerden gemäß Art. 33 DS-GVO der Aufsichtsbehörde, es sei denn, dass diese Verletzung voraussichtlich

nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt (siehe auch Nr. 12.1 und 26.1).

Im Berichtszeitraum wurden insbesondere folgende Verletzungen häufig gemeldet:

- Fehlerhafte Adressierung, z. B. bei gleichem Nachnamen,
- Fehlversand von Waren,
- Fehlerhafte Eingabe von E-Mailadressen, auch durch Berufsgeheimnisträger,
- Abhandenkommen von Datenträgern,
- Unberechtigte Datenzugriffe durch Beschäftigte zu privaten Zwecken,
- Angriffe auf zentrale IT-Infrastruktur beim Verantwortlichen oder deren Auftragsverarbeitern, teilweise mit der Folge, dass die gesamte IT für längere Zeit vom Netz genommen werden musste und Leistungen mithilfe des Netzes nicht erbracht werden können.

Auf der Homepage des Landesbeauftragten sind mögliche Abhilfemaßnahmen aufgeführt.[64] Die Homepage des Bundesamtes für Sicherheit in der Informationstechnik enthält weitere Informationen (IT-Sicherheitsvorfall).[65]

42.2 Anruferdatenbank und Datenschutzinformationen eines Taxiunternehmens

Im Jahr 2022 erreichte den Landesbeauftragten eine Beschwerde gegen ein Taxiunternehmen. Darin schilderte der Beschwerdeführer, dass er gelegentlich Fahrgast bei diesem Unternehmen sei und in Telefonaten mit deren Beschäftigten mehrmals auf frühere Fahrziele oder andere Telefonnummern angesprochen worden sei, die er vor ca. drei bis fünf Jahren verwendet hatte. Er fragte den Landesbeauftragten, ob diese Speicherung seiner personenbezogenen Daten zulässig sei.

Im Ergebnis der Sachverhaltsaufklärung hat der Landesbeauftragte festgestellt, dass das Unternehmen die Daten von Anrufern und Fahrgästen tatsächlich zeitlich unbegrenzt in seinem Computersystem gespeichert hatte. Es handelte sich unter anderem um Vornamen, Namen, Anschrift, Telefonnummern sowie Beförderungsdaten. Eine gesetzliche Rechtsgrundlage dafür war nicht ersichtlich. Einwilligungen der betroffenen Personen wurden nicht eingeholt.

Eine zeitlich unbegrenzte Speicherung personenbezogener Daten stellt einen Verstoß gegen den Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c DS-GVO sowie die Löschungsverpflichtung des Verantwortlichen nach Art. 17 DS-GVO dar.

Eine besondere Schwierigkeit lag in diesem Fall darin, dass die Software, die das Unternehmen nutzte, gar keine Möglichkeit vorsah, automatische Löschroutinen für bestimmte Datenarten oder Datenkategorien zu definieren. Das Unternehmen war zwar

[64] https://lsaurl.de/BspDSVer

[65] https://www.bsi.bund.de/DE/Home/home_node.html

gewillt, Löschfristen festzusetzen und einzuhalten. Die Löschzyklen mussten jedoch manuell überwacht und die Löschprozesse manuell durchgeführt werden, was als Dauerlösung einen enormen Aufwand verursacht hätte.

Das Unternehmen gab schließlich an, eine Ergänzung der Software um entsprechende Funktionen in Auftrag gegeben zu haben. Der Landesbeauftragte bewertete es als besonders positives Ergebnis dieser Datenschutzüberprüfung, dass damit eine datenschutzfreundliche Technikgestaltung (vgl. auch Art. 25 DS-GVO) vielen weiteren Nutzern dieser Software zugutekommen könnte.

Ein weiteres Ergebnis der Sachverhaltsaufklärung war, dass das Unternehmen den Anrufern und Fahrgästen nicht die notwendigen Informationen nach Art. 13 DS-GVO zur Verfügung stellte. Eine kurze Bandansage mit dem Hinweis auf die Homepage des Unternehmens genügte nicht, denn auf der Homepage wurden die betroffenen Personen nur über die Datenverarbeitungen mittels der Homepage informiert und nicht über die weiteren Datenverarbeitungen im Unternehmen, insbesondere wenn es zu einer Taxifahrt kam oder gar zu einer Krankenbeförderung mit dem Taxi inklusive anschließender Abrechnung der Leistung gegenüber der Krankenkasse.

Der Landesbeauftragte beriet das Unternehmen zu der ganz praktischen Frage, wie die Datenschutzinformationen bereitgestellt werden können, wenn der Kundenkontakt zuerst telefonisch und dann persönlich im Fahrzeug stattfindet. Die Lösung lag letztlich darin, die Datenschutzinformationen auf der Homepage zu ergänzen und in ausgedruckter Form in den Fahrzeugen zum Lesen und bei Bedarf auch zum Mitnehmen bereitzuhalten [siehe Kapitel 22.9]. Nach anfänglicher Skepsis hat das Unternehmen dies im betrieblichen Alltag integriert.

Da das Unternehmen zusätzlich zu diesen beiden Verstößen auch kein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DS-GVO geführt hatte, erteilte der Landesbeauftragte letztlich eine Verwarnung nach Art. 58 Abs. 2 lit. b DS-GVO und legte dem Verantwortlichen die Kosten des besonders aufwändigen Verfahrens auf [siehe Kapitel 42.3].

Eine zeitlich unbegrenzte Speicherung personenbezogener Daten steht unter keinen Umständen im Einklang mit der DS-GVO. Ein Datenverarbeitungssystem sollte im Sinne des Prinzips „Privacy by Design“ (vgl. Art. 25 DS-GVO) bestenfalls die Möglichkeit bieten, für bestimmte Datenarten Löschzyklen zu definieren und die Löschprozesse automatisiert durchzuführen.

Auch ein Taxiunternehmen muss für alle betroffenen Personen vollständige Informationen nach Art. 13 DS-GVO bereithalten. Wenn das Unternehmen eine Internetseite betreibt, bietet es sich an, die Datenschutzinformationen dort einzustellen und bei dem telefonischen Taxiruf darauf hinzuweisen. Im Beförderungsfahrzeug muss der Fahrgast die Möglichkeit haben, in die Informationen einzusehen und sie bei Bedarf zum späteren Lesen mitzunehmen.

42.3 Zusammenarbeit mit der Aufsichtsbehörde

Nach Art. 31 DS-GVO arbeiten der Verantwortliche und der Auftragsverarbeiter und gegebenenfalls deren Vertreter auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Es handelt sich um eine Pflicht zur Zusammenarbeit.

Art. 31 DS-GVO kann erhebliche Auswirkungen haben. Insbesondere in einer Datenschutzüberprüfung, sowohl anlasslos als auch aufgrund einer Beschwerde einer betroffenen Person (Art. 57 Abs. 1 lit. f DS-GVO, Art. 58 Abs. 1 lit. b DS-GVO), kann es für die Verantwortlichen sinnvoll sein, mit der Aufsichtsbehörde von Beginn an zu kooperieren, z. B. zur Sachverhaltsaufklärung beizutragen, Beratungsangebote anzunehmen, Hinweise möglichst zeitnah umzusetzen bzw. Gegenargumente vorzutragen und Missverständnisse auszuräumen.

Diese Kooperation kann vordergründig dazu führen, die Datenverarbeitungen im Einklang mit der DS-GVO auszugestalten. Hinzu kommt jedoch auch, dass bei festgestellten Verstößen gegen die DS-GVO die Aufsichtsbehörde letztlich stets zu entscheiden hat, welche Maßnahmen daraufhin erforderlich sind. Dabei hat sie alle be- und entlastenden Umstände des Sachverhalts zu berücksichtigen, u. a. auch die Maßnahmen des Verantwortlichen zur Minderung des entstandenen Schadens, die Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, die Einhaltung der gegen den Verantwortlichen angeordneten Maßnahmen, und jeden anderen erschwerenden oder mildernden Umstand (Art. 83 Abs. 2 DS-GVO, Erwägungsgrund 148 Satz 3). Mangelnde Kooperation mit der Aufsichtsbehörde stellt somit nicht nur einen Verstoß gegen Art. 31 DS-GVO dar, der für sich genommen ebenfalls sanktioniert werden kann (Art. 58 Abs. 2 lit. i i. V. m. Art. 83 Abs. 4 lit. a DS-GVO). Sie würde auch bei der Entscheidung über aufsichtsbehördliche Maßnahmen wegen der weiteren festgestellten Verstöße negativ ins Gewicht fallen und so die Wahrscheinlichkeit von z. B. Anweisungen, Zwangsgeldern, Bußgeldern, Verwarnungen erhöhen.

Hinzu kommt, dass mangelnde Kooperation bei der Aufsichtsbehörde häufig den Verwaltungsaufwand erhöht, z. B. für häufige Erinnerungen, Nachfragen oder gar förmliche Anweisungen, die ggf. zwangsweise Durchsetzung von Anweisungen. Stellt die Aufsichtsbehörde im Ergebnis einer besonders aufwändigen Datenschutzüberprüfung einen Datenschutzverstoß fest und ergreift daraufhin eine aufsichtsbehördliche Maßnahme nach Art. 58 Abs. 2 lit. b bis g DS-GVO, muss sie dafür Verwaltungskosten erheben. Rechtsgrundlage dafür ist § 1 VwKostG LSA i. V. m. § 1 AllGO LSA, Kostentarif Nr. 25 Ziff. 2.1 der Anlage zur AllGO LSA. Die Grenze, ab der ein besonderer Verwaltungsaufwand vorliegt, liegt bei 500 EUR und kann schnell überschritten sein. Die Höchstgrenze liegt bei 15.000 EUR. Der Aufsichtsbehörde steht im Verwaltungskostenrecht kein Ermessen zu. Die Gründe, wegen denen die Aufsichtsbehörde von der Festsetzung der Kosten absehen oder sie erlassen, stunden oder ermäßigen kann (Billigkeitsmaßnahmen nach § 12 VwKostG LSA), liegen selten vor.

Im Berichtszeitraum hatte der Landesbeauftragte in verschiedenen Verfahren Anlass, auf diese Kooperationspflicht und die Folgen der Verletzung der Kooperationspflicht besonders hinzuweisen. In einzelnen Verfahren mussten auch tatsächlich Kosten festgesetzt werden, teils im vierstelligen Bereich.

Zwei Fälle von Zwangsgeldfestsetzungen wegen beharrlichen Schweigens auf eine Auskunftsanweisung nach Art. 58 Abs. 1 lit. a DS-GVO ragten besonders heraus.

In einem Fall hatte eine für eine Datenverarbeitung verantwortliche natürliche Person das Beitreiben eines Zwangsgeldes durch Kontenpfändung ignoriert und wurde in der Geschäftsstelle des Landesbeauftragten erst vorstellig, als ein zweites und erhöhtes Zwangsgeld gegen ihn festgesetzt worden war. Dabei war ihm mitgeteilt worden, dass nach § 56 Abs. 1 SOG LSA ein Zwangsgeld bis zu 500.000 EUR schriftlich festgesetzt

und nach § 54 Abs. 3 SOG LSA auch solange gesteigert wiederholt werden kann, bis der Verwaltungsakt befolgt worden ist oder sich auf andere Weise erledigt hat. Durch einen einzigen Satz hatte der Auskunftspflichtige dann die von der Aufsichtsbehörde geforderte Auskunft erteilt, damit die Beitreibung des festgesetzten wiederholten Zwangsgeldes abgewandt und so die Einstellung des Verwaltungsverfahrens ermöglicht.

In einem anderen Fall bezahlte ein Unternehmen das erste und auch das zweite Zwangsgeld, jeweils in niedriger vierstelliger Höhe, und erteilte die zur Sachverhaltsaufklärung notwendigen Auskünfte erst, als das dritte Zwangsgeld, dann in mittlerer vierstelliger Höhe, festgesetzt worden war. Im weiteren Verlauf kam es auch zur Sanktionierung verschiedener Verstöße gegen die DS-GVO durch mehrere Bußgelder in insgesamt mittlerer fünfstelliger Höhe sowie zu einer Verwarnung, woraufhin dem Unternehmen schließlich die Kosten des Verwaltungsverfahrens auferlegt wurden.

Bei einer Datenschutzüberprüfung sind Verantwortliche nach Art. 31 DS-GVO verpflichtet, mit der Aufsichtsbehörde zusammenzuarbeiten. Mangelnde Kooperation kann nicht nur für sich genommen als Verstoß gegen die DS-GVO sanktioniert werden, sondern ist auch deswegen nicht zu empfehlen, weil es die Wahrscheinlichkeit für aufsichtsbehördliche Maßnahmen bei festgestellten Verstößen gegen die DS-GVO erhöht und zu einem erhöhten Verwaltungsaufwand bei der Aufsichtsbehörde führt. Besonderen Verwaltungsaufwand einer Datenschutzüberprüfung hat nach dem Verwaltungskostenrecht des Landes Sachsen-Anhalt unter bestimmten Umständen der Verantwortliche zu tragen.

42.4 Negativauskünfte nach Art. 15 DS-GVO

Im Jahr 2023 erreichten den Landesbeauftragten gehäuft Beschwerden von betroffenen Personen, die bei Unternehmen Auskunftsersuchen nach Art. 15 DS-GVO gestellt hatten und denen die Unternehmen daraufhin entweder gar keine Auskunft erteilten oder – teils erst auf Anfrage des Landesbeauftragten – mitteilten, dass Daten zu dieser Person dort nicht verarbeitet würden (so genannte Negativauskunft). Da die betroffenen Personen allerdings zuvor z. B. ein Schreiben, eine Werbe-E-Mail oder auch einen Anruf des Unternehmens erhalten hatten, für das ihre Daten verwendet worden waren, waren diese Angaben nicht plausibel und aufklärungsbedürftig.

Der Landesbeauftragte beriet die Unternehmen in diesen Verfahren zunächst dahingehend, dass es auch in dem Fall, dass zu einer Person keine Daten auffindbar sind, nicht zulässig ist, auf ein Auskunftsersuchen nach Art. 15 DS-GVO (vgl. Art. 12 und Art. 15 Abs. 1, 1. Halbsatz DS-GVO) gar nicht zu antworten. Auch wenn keine personenbezogenen Daten dieser Person verarbeitet werden oder es Gründe gibt, die einer Auskunft nach Art. 15 DS-GVO entgegenstehen, müssen dieser Umstand und die Gründe dafür der betroffenen Person unverzüglich, auf jeden Fall binnen eines Monats mitgeteilt werden (Art. 12 Absätze 3 und 4 DS-GVO). Auch soweit das Recht auf Erhalt einer Kopie die Rechte und Freiheiten anderer Personen beeinträchtigt (Art. 15 Abs. 4 DS-GVO), darf dies jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird (Erwägungsgrund 63 Satz 6).

Im Ergebnis der teilweise sehr aufwändigen Erörterungen mit den Unternehmen stellte sich in mehreren Fällen heraus, dass die personenbezogenen Daten der Beschwerdeführer von einem Auftragsverarbeiter des Verantwortlichen verarbeitet wurden oder

von einem anderen Unternehmen, mit dem der Verantwortliche zusammenarbeitete, ggf. als gemeinsam Verantwortlicher i. S. d. Art. 26 DS-GVO. Der Verantwortliche hatte sich vor der Auskunftserteilung an die betroffene Person nicht bei dem Auftragsverarbeiter oder dem mit ihm gemeinsam Verantwortlichen erkundigt, ob dort Daten zu dieser Person vorhanden sind. Dies ist allerdings erforderlich.

Denn die Auskunftspflicht trifft auch in diesen Fällen den Verantwortlichen (Art. 15 Abs. 1 DS-GVO). Der Verantwortliche darf sich nicht darauf zurückziehen, dass die Daten nicht in seinen eigenen IT-Systemen gespeichert sind. Hat er den Auftrag für diese Datenverarbeitung erteilt oder trägt dafür eine Mitverantwortung, so ist er verpflichtet, sich von dem Auftragsverarbeiter oder dem weiteren Verantwortlichen Informationen einzuholen. Dazu sind entsprechende Vereinbarungen mit dem Auftragsverarbeiter oder gemeinsam Verantwortlichen abzuschließen (vgl. Art. 26 Abs. 1 Satz 2, Art. 28 Abs. 3 lit. e DS-GVO). Hierauf hat der Landesbeauftragte hingewiesen und hingewirkt.

In einigen weiteren Fällen trugen die Verantwortlichen vor, dass sie eine Fülle personenbezogener Daten verarbeiten und es sehr aufwändig sei, die Daten des jeweiligen Betroffenen herauszufiltern und zu einer Auskunft nach Art. 15 DS-GVO zusammenzustellen. Dieses Argument kann allerdings nicht dazu führen, dass eine Auskunft gänzlich verweigert wird. Denn gerade die Verantwortlichen, deren Datenverarbeitungen in Umfang und Komplexität besonders herausragen, stehen in der Pflicht, über diese Datenverarbeitungen Transparenz herzustellen. Die organisatorischen Prozesse und die Personalausstattung bei dem Verantwortlichen sind darauf auszurichten, dass Anträge der Betroffenen nach der DS-GVO innerhalb der Fristen des Art. 12 Abs. 3 DS-GVO vollständig bearbeitet und beantwortet werden können. Es empfiehlt sich, für die Anträge, die besonders häufig eingehen, jeweils einen standardisierten Prozess einzuführen und hierfür ggf. Formulare oder sogar IT-gestützte Funktionen für die Betroffenen und Bearbeiter beim Verantwortlichen bereitzustellen. Eine Verweigerung einer Auskunft käme allenfalls in Betracht, wenn es sich um einen exzessiven Antrag i. S. v. Art. 12 Abs. 5 Satz 2 DS-GVO handelt, was der Verantwortliche nachweisen können muss. Dies war in den Beschwerdefällen fernliegend.

Bei Auskunftsersuchen nach Art. 15 DS-GVO muss ein Verantwortlicher größtmögliche Sorgfalt darauf verwenden, alle personenbezogenen Daten der anfragenden Person in seinen Datenverarbeitungen und in den Datenverarbeitungen seiner Auftragsverarbeiter und der mit ihm gemeinsam Verantwortlichen zu identifizieren und darüber vollständig Auskunft gemäß Art. 15 DS-GVO zu erteilen. Sollten der anfragenden Person keine Daten zuzuordnen sein, ist fristgerecht eine Negativauskunft nach Art. 15 Abs. 1, 1. Halbsatz DS-GVO zu erteilen. Der Anspruch der betroffenen Person ist mittels einer Anweisung der Aufsichtsbehörde nach Art. 58 Abs. 2 lit. c DS-GVO, aber auch zivilrechtlich durchsetzbar.

42.5 Vermischung der Daten der Stromanschlussnutzer und Betreiber einer Photovoltaik-Anlage

Im Jahr 2023 hatte der Landesbeauftragte eine Beschwerde eines Betreibers einer Photovoltaik-Anlage gegen den Stromnetzbetreiber zu prüfen. Der Beschwerdeführer hatte festgestellt, dass in seinem Datensatz bei dem Netzbetreiber die E-Mail-Adresse eines Dritten eingetragen war. Seinem Berichtigungsantrag sei der Netzbetreiber nicht

nachgekommen. Er äußerte zudem die Befürchtung, dass seine personenbezogenen Daten per E-Mail an den unbefugten Dritten übermittelt wurden.

Es handelte sich um eine Mischnutzung des Stromanschlusses: Der Photovoltaik-Anlagenbetreiber und der Nutzer des Stromanschlusses waren nicht personenidentisch. Dies ist in der Praxis durchaus gängig und könnte bei weiterem Ausbau erneuerbarer Energien künftig häufiger vorkommen. Der Anlagenbetreiber kann der Eigentümer des Objekts sein oder die Dachfläche für die Photovoltaik-Anlage gemietet haben; er erhält die Einspeisevergütung vom Netzbetreiber nach dem EEG 2023. Der Stromanschlussnutzer kann der Mieter sein oder bei Vermietung der Dachfläche auch der Eigentümer des Objekts; er bezieht den Stromverbrauch über einen Energieversorger und meldet die Zählerstände an den Messstellenbetreiber nach dem MsbG. Beide Stromflüsse (Einspeisung in das und Stromverbrauch aus dem Netz) werden über denselben Zähler gemessen.

Das Unternehmen, gegen das sich die Beschwerde richtete, handelte zugleich als Netzbetreiber und Messstellenbetreiber. Es hatte allerdings die Datenhaltung dieser beiden Marktrollen nicht voneinander getrennt. Durch die gemeinsame Zählernummer waren die Datensätze beider Beteiligter miteinander verknüpft. So konnte es dazu kommen, dass der Stromanschlussnutzer bei der Meldung der Zählerstände in einem Onlineportal des Messstellenbetreibers seine E-Mail-Adresse als Kontaktdatum eingegeben hat und diese E-Mail-Adresse in einem gemeinsamen Datensatz mit den personenbezogenen Daten des Photovoltaik-Anlagenbetreibers vermischt wurde.

Das Unternehmen gab an, dass jedoch tatsächlich keine personenbezogenen Daten des Beschwerdeführers unbefugt an diese E-Mail-Adresse übermittelt wurden. Dies war wichtig zu prüfen, auch wenn es sich möglicherweise nur um sehr technische Daten aus dem Zähler handelte. Denn auch diese Daten können personenbeziehbar sein, insbesondere, wenn sie Informationen über den Energieverbrauch oder das Eigentum natürlicher Personen enthalten (z. B. die Leistungsfähigkeit einer Photovoltaik-Anlage).

Im Ergebnis der Erörterungen hat das Unternehmen seine IT-Software angepasst und in seinem Onlineportal das Erfassen von E-Mail-Adressen dauerhaft deaktiviert. Unter Berücksichtigung der gesamten Umstände des Beschwerdefalls beendete der Landesbeauftragte das Verfahren mit einem Hinweis auf einen vermeintlichen Verstoß gegen Art. 5 Abs. 1 lit. f, Art. 25, 32 DS-GVO.

Ist ein Unternehmen gleichzeitig als Netzbetreiber und als Messstellenbetreiber tätig und fallen Anlagenbetreiber und Anschlussnutzer auseinander, darf die gemeinsame Zählernummer nicht dazu führen, dass die Daten verschiedener Personen in einem Datensatz vermischt werden und dadurch ggf. unrichtige Daten oder gar Datenübermittlungen an Unbefugte entstehen. Auf die Festlegung der geeigneten und angemessenen technischen und organisatorischen Maßnahmen ist besondere Sorgfalt zu verwenden. Bestenfalls ist die Datenhaltung der beiden Marktrollen Netzbetreiber und Messstellenbetreiber voneinander zu trennen.

42.6 Feuchtigkeitsmessungen in einer Mietwohnung aufgrund einer Denkmalschutzauflage

Aufgrund einer Anfrage im Jahr 2023 prüfte der Landesbeauftragte folgenden Sachverhalt: Für die Sanierung eines Mehrfamilienhauses hatte die untere Denkmalschutzbehörde ihre denkmalrechtliche Genehmigung gemäß § 14 DenkmSchG LSA mit einer Auflage als Nebenbestimmung versehen. Die Auflage sah vor, dass ein langfristiges Monitoring der Feuchtigkeitsveränderung im Außenmauerwerk (mindestens 3 Jahre) durchzuführen ist. Nach dem Messkonzept befanden sich in Flur, Küche, Wohnzimmer und Schlafzimmer einer bestimmten Wohnung jeweils drei Sensoren (ein Sensor auf der Innenwand und zwei Sensoren im Außenwandbereich), die im Messtakt von einer Stunde jeweils die Lufttemperatur und die relative Luftfeuchte messen sollten. Diese Wohnung sollte zu privaten Wohnzwecken vermietet werden.

Datenschutzrechtlich ergab sich die Frage, ob die Nebenbestimmung zur denkmalrechtlichen Genehmigung eine rechtliche Verpflichtung darstellt, aus der sich für den Vermieter eine Befugnis zur Datenverarbeitung nach Art. 6 Abs. 1 Satz 1 lit. c DS-GVO ergibt. Denn mindestens die Messergebnisse der Sensoren auf der Innenwand dürften bei einem Messtakt von einer Stunde personenbeziehbar sein, da sie Rückschlüsse auf die Lebensgewohnheiten der Bewohner dieser Wohnung zulassen.

Die datenschutzrechtliche Prüfung ergab, dass eine Auflage in einem Verwaltungsakt einer Behörde nicht generell, sondern nur unter bestimmten Bedingungen eine Rechtsverpflichtung i. S. v. Art. 6 Abs. 1 Satz 1 lit. c DS-GVO darstellen kann. Die rechtliche Verpflichtung muss sich gemäß Art. 6 Abs. 3 Satz 1 DS-GVO aus dem Unionsrecht oder aus dem Recht eines Mitgliedstaates ergeben, dem der Verantwortliche unterworfen ist. Eine rechtliche Verpflichtung kann sich aus allen verfassungsmäßigen Regelungen mit normativem Charakter ergeben, wozu alle Gesetze im materiellen Sinn zählen. Nicht nur aus Bundesgesetzen sowie aus den Parlamentsgesetzen der Bundesländer können sich rechtliche Verpflichtungen ergeben, sondern auch aus sich auf gesetzliche Ermächtigungen stützenden Verordnungen sowie aus Satzungen einer Körperschaft, einer Stiftung oder einer Anstalt. Allein ein Verwaltungsakt einer Behörde genügt allerdings nicht, sondern es kommt auf den Regelungsgehalt der materiellen Rechtsnorm an, die dem Verwaltungsakt oder seiner Nebenbestimmung zugrunde liegt.

Bei einer Nebenbestimmung zu einer denkmalrechtlichen Genehmigung handelt es sich nicht um eine rechtliche Verpflichtung in diesem Sinne. Denn § 14 DenkmSchG LSA vermittelt dem Antragsteller im denkmalschutzrechtlichen Genehmigungsverfahren keinerlei konkrete Verpflichtungen zur Datenverarbeitung. Solche sind der gesetzlichen Regelung nicht einmal zwangsläufig immanent, wie sich aus der Genehmigungsfiktion des § 14 Abs. 11 Satz 1 DenkmSchG LSA ergibt.

Der Vermieter musste daher andere Rechtsgrundlagen prüfen. Dies führte zu dem vertretbaren Ergebnis, dass eine Vermietung dieser konkreten Wohnung zu privaten Wohnzwecken nicht im Einklang mit der DS-GVO möglich ist.

Temperatur- und Feuchtigkeitsmesswerte aus einer Wohnung können Rückschlüsse auf die Lebensgewohnheiten der Bewohner zulassen und daher personenbezogene Daten darstellen.

Eine Auflage in einem Verwaltungsakt einer Behörde kann nicht generell, sondern nur unter bestimmten Bedingungen eine Rechtsverpflichtung i. S. v. Art. 6 Abs. 1 Satz 1 lit. c DS-GVO darstellen. Eine Auflage in einer denkmalschutzrechtlichen Genehmigung erfüllt diese Bedingungen in der Regel nicht.

42.7 Aushang von Hausverboten

Den Landesbeauftragten erreichen regelmäßig Beschwerden wegen des öffentlichen Aushangs von Hausverboten. Häufig geht es dabei um Streitigkeiten in Vereinen, bei denen Gespräche oder Verhandlungen zwischen den Beteiligten nicht mehr stattfinden. Manchmal sind bereits Gerichtsverfahren anhängig. Im weiteren Verlauf erteilt der Vorstand einem Vereinsmitglied ein Hausverbot für das Vereinsgelände und hängt dieses in schriftlicher Form in öffentlich zugänglichen Schaukästen aus.

Ein per Computerprogramm gedrucktes Hausverbot mit Angaben zu einer oder mehreren konkreten Personen fällt unter die DS-GVO. Es liegt jedenfalls eine teilweise automatisierte Verarbeitung personenbezogener Daten (Art. 4 Nr. 1 und 2 DS-GVO) vor.

Bei Aushängen in öffentlich zugänglichen Bereichen handelt es sich dann um eine Verarbeitung in Form der Offenlegung, also um eine einfache „Bereitstellung“ gegenüber einer unbestimmten Zahl von Dritten mit der Möglichkeit zur Kenntnisnahme.

Die Verarbeitung personenbezogener Daten nach der DS-GVO ist nur zulässig, wenn eine der in Art. 6 Abs. 1 DS-GVO genannten Bedingungen erfüllt ist. Mangels Einwilligung scheidet Art. 6 Abs. 1 lit. a DS-GVO regelmäßig aus. Art. 6 Abs. 1 lit. b DS-GVO ist hier ebenfalls nicht einschlägig. Somit verbliebe Art. 6 Abs. 1 lit. f DS-GVO.

Häufig ist schon das Bestehen eines berechtigten Interesses i. S. v. Art. 6 Abs. 1 lit. f DS-GVO zu verneinen, da Streitfragen um eine eventuelle Räumung noch nicht gerichtlich geklärt sind und somit auch ein Räumungsurteil noch nicht vollstreckt wurde.

Die durch den öffentlichen Aushang des Hausverbots regelmäßig erzeugte Prangerwirkung führt aber jedenfalls dazu, dass diese Art der Verarbeitung „nicht erforderlich“ i. S. v. Art. 6 Abs. 1 lit. f DS-GVO ist, um etwaige berechtigte Interessen wahrzunehmen. Eine persönliche oder postalische Bekanntgabe dürfte in der Regel ausreichen. Außerdem überwiegen grundsätzlich die Interessen der Betroffenen am Unterbleiben einer Bloßstellung.

Der öffentliche Aushang eines für ein Vereinsgelände erteilten Hausverbots ist nicht zulässig.

42.8 Länderübergreifendes Glückspielaufsichtssystem (LUGAS)

Ein Unternehmen aus dem europäischen Ausland beabsichtigte, virtuelles Automatenspiel in Deutschland online gegenüber Spielern in Deutschland anzubieten. Die hierfür erforderliche glückspielrechtliche Erlaubnis setzte einen Anschluss an das LUGAS-System voraus (§ 4 Abs. 5 Nr. 6 GlüStV 2021).

Das Unternehmen sah eine gemeinsame Verantwortlichkeit i. S. v. Art. 26 DS-GVO zwischen der GGL und sich für den Betrieb und die Nutzung der LUGAS-Dateien.

Der Landesbeauftragte verneinte die gemeinsame Verantwortlichkeit. Das Unternehmen hatte keinen rechtlichen oder tatsächlichen Einfluss auf die Datenverarbeitung im Rahmen des LUGAS-Systems. Es hatte lediglich einige gesetzliche Verpflichtungen in Form der Übermittlung bestimmter personenbezogener Daten an die GGL zu erfüllen. Für die Richtigkeit dieser zu übermittelnden Daten bejahte der Landesbeauftragte eine eigene Verantwortlichkeit (Art. 4 Nr. 7 DS-GVO) des Unternehmens. Im Übrigen bejahte er eine eigene Verantwortlichkeit der GGL.

Werden personenbezogene Daten zur Erfüllung einer gesetzlichen Verpflichtung an eine öffentliche Stelle übermittelt, begründet dies für Datenübermittler und Datenempfänger in aller Regel keine gemeinsame Verantwortlichkeit i. S. v. Art. 26 DS-GVO.

42.9 Verarbeitung der Daten von Berufsbetreuern bei Banken

Beim Landesbeauftragten wurde angefragt, ob Berufsbetreuer mit dem Aufgabenkreis der Vermögenssorge sich bei einer Bank durch Vorlage ihres Betreuerausweises legitimieren können. Laut „Handbuch“ einer Bank sollte es erforderlich sein, zusätzlich zum Betreuerausweis den Beschluss des zuständigen Amtsgerichts (§ 286 FamFG) vorzulegen, mit dem der Betreuer bestellt worden war.

Der Landesbeauftragte teilte hierzu mit, dass die Vorlage des Betreuerausweis genügt. Zwar unterliegen Kreditinstitute gesetzlichen Verpflichtungen zur Identitätsprüfung, beispielsweise nach dem GwG und der ZIdPrüfV. Enthält der Betreuerausweis aber die Angaben nach § 290 FamFG, ist dies als Legitimation in Verbindung mit einem Personalausweis in aller Regel ausreichend. Dabei hat der Landesbeauftragte berücksichtigt, dass Kreditinstitute nur vereinfachte Sorgfaltspflichten erfüllen, soweit sie ein lediglich geringes Risiko der Geldwäsche oder Terrorismusfinanzierung feststellen, was im Betreuungsbereich regelmäßig der Fall sein dürfte.

43 Videoüberwachung und Fotoaufnahmen

43.1 Herausgabe von Aufnahmen von Überwachungskameras an private Dritte

In den letzten Jahren hatten sich im Zuständigkeitsbereich der Aufsichtsbehörde mehrmals Fälle zugetragen, in denen Aufnahmen von Überwachungskameras, die auch die Anwesenheit und das Tun von betroffenen Personen abbildeten, auf Verlangen an Dritte herausgegeben worden waren. Ein besonders dramatisches Ereignis trug sich in einem Supermarkt zu. Dort war einer jungen Kundin durch eine unbekannte Person ihr Mobiltelefon gestohlen worden. Die herbeigeeilte Mutter des Opfers hatte sodann bei der Marktleitung Einsicht in die Aufnahmen der zahlreichen Überwachungskameras begehrt und auch erhalten. Ihr Ziel war, die Diebstahlshandlung zu beobachten und an Aufnahmen des vermeintlichen Täters zu gelangen. Solche Aufnahmen sind dadurch herausgegeben worden, dass die Marktleitung zuließ, dass durch die Familie des Diebstahlsopfers Fotografien von den Bildern auf dem Kontrollmonitor gemacht wurden. Diese Aufnahmen wurden dann zu einer privat motivierten Öffentlichkeitsfahndung in Sozialen Netzen verwendet und weit verbreitet, was auch ungewollte schwere Folgen und einen nachhaltigen Ansehensverlust für die ganze Familie des schnell identifizierten Beschuldigten hatte, welcher auch durch das ca. 6 Monate nach dem

Fahndungsaufruf erfolgte Dementi durch das Diebstahlsopfer nicht mehr ungeschehen gemacht werden konnte (zu Fragen der privat motivierten Öffentlichkeitsfahndung in Sozialen Netzen vgl. XIII./XIV. Tätigkeitsbericht (Nr. 14.1.11)).

Die Betroffenenfamilie wandte sich im Rahmen von Beschwerdeverfahren wegen der Herausgabe der Aufnahmen und deren Verwendung zur Öffentlichkeitsfahndung an die Aufsichtsbehörde. Zumindest das wegen der freizügigen Herausgabe von Überwachungsaufnahmen durch das beteiligte Handelsunternehmen durch die Aufsichtsbehörde eingeleitete Verwaltungsverfahren blieb allerdings fruchtlos, da das Handelsunternehmen kurz nach dem fraglichen Vorfall seinen Geschäftsbetrieb aufgegeben hatte.

Gleichwohl sieht die Aufsichtsbehörde Anlass, auf datenschutzrechtliche Fragen einzugehen, die mit der Gewähr der Einsichtnahme in Überwachungsaufnahmen gegenüber Dritten, der Bereitstellung von Kopien dieser Aufnahmen und dem Zulassen von Fotos, die von Aufnahmen eines Kontrollmonitors gemacht werden, im Zusammenhang stehen.

Wie auch die Videoüberwachung selbst stellt die Einblickgewährung und die Herausgabe von Aufnahmen der Überwachungskameras Vorgänge (oder Phasen oder Arten?) der Verarbeitung personenbezogener Daten dar. Auch bei einer Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung handelt es sich bekanntermaßen um eine Verarbeitung im datenschutzrechtlichen Sinne (vgl. Art. 4 Nr. 2 DS-GVO). Folglich bedurften die Einblickgewährung und die Herausgabe von Aufnahmen der Überwachungskameras als Verarbeitung i. S. v. Art. 6 Abs. 1 DS-GVO einer gesetzlichen Erlaubnisnorm oder der Einwilligung der Betroffenen, wobei im vorliegenden Fall eine Einwilligung i. S. v. Art. 6 Abs. 1 lit. a i. V. m. Art. 7 DS-GVO wegen der Abwesenheit des vermuteten Täters nicht in Frage kam.

Die Aufsichtsbehörde hatte durchgreifende Zweifel daran, ob als gesetzliche Erlaubnisnorm für die Offenlegung der gespeicherten Aufnahmen gegenüber der Familie der geschädigten Kundin Art. 6 Abs. 1 Satz 1 lit. f DS-GVO in Frage kam. Zwar heißt es dort, dass die Verarbeitung u. a. dann rechtmäßig ist, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Ob diese Erforderlichkeit allerdings tatsächlich gegeben war, blieb höchst zweifelhaft. Die Familie der geschädigten Kundin hätte durchaus die Möglichkeit gehabt, bei einer Anzeige des Diebstahles bei der Polizei gegen Unbekannt auf die in dem Markt vorhandene Videoüberwachung hinzuweisen. Allerdings hätte die Gefahr bestanden, dass bis zum zeitlich nicht einzuschätzenden Tätigwerden der Polizei die Videodaten bereits automatisch gelöscht gewesen wären.

Auch das Bestreben der Marktleiterin als Geschäftsfrau und Händlerin, möglichst zufriedene Kunden zu haben und diesen in einer angenommenen Notlage unterstützend zur Seite zu stehen, mag zwar menschlich nachvollziehbar sein, eine Rechtsgrundlage für die Einblickgewährung in die Videoaufzeichnungen gegenüber der Familie der geschädigten Kundin und die damit einhergehende Übermittlung personenbezogener Daten von Dritten vermochte die Aufsichtsbehörde darin jedoch nicht zu erkennen. Anderes gilt im Übrigen, wenn die Polizei im Rahmen von Ermittlungen, z. B. zu einem Diebstahl i. S. v. § 242 StGB, Einsicht in die Videoaufzeichnungen begehrt, um damit den Sachverhalt zu erforschen. Sie könnte sich dabei auf § 160 Abs. 1 und 2 der StPO berufen.

Die Aufsichtsbehörde empfiehlt Marktbetreibern für ähnlich gelagerte Fälle des Begehrens der Einblickgewährung in ihre Videoaufzeichnungen durch private Dritte nachdrücklich, auf die ausschließliche Zuständigkeit der Polizei zu verweisen.

Die Unterstützung eines Marktbetreibers in solchen Fällen dürfte nur so weit gehen, als dass dieser die zeitlich (z. B. 11:03 Uhr bis 11:06 Uhr) und örtlich (z. B. die Regalreihe, in der die Konservendosen stehen) begrenzten Videosequenzen, die vielleicht den Diebstahl und die beteiligten Personen zeigen, durch geeignete Maßnahmen vor dem automatischen Löschen durch sein Videoüberwachungssystem zu schützen.

Die dem Marktbetreiber als für die Videoüberwachung Verantwortlichem obliegende Pflicht, die Videodaten nach einer bestimmten Speicherdauer datenschutzgerecht zu löschen, wenn deren weitere Speicherung nicht bzw. nicht mehr erforderlich ist, bliebe davon unberührt.

Herausgabe von Aufnahmen von Überwachungskameras nur an die Polizei.

43.2 Speicherfristen bei Videoüberwachung

Bekanntermaßen dürfen personenbezogene Daten nur so lange gespeichert werden, wie es zulässig und für die Zwecke, für die sie verarbeitet werden, auch erforderlich ist. Die Grundsätze der Datenminimierung und der Speicherbegrenzung nach Art. 5 Abs. 1 lit. c und e DS-GVO sind auch bei der Frage, ob und wann Aufnahmen von Überwachungskameras gelöscht werden müssten, relevant. Allerdings wird dies, so zeigt sich in der laufenden Kontroll- und Beratungspraxis der Aufsichtsbehörde, von den Verantwortlichen oftmals nicht beachtet. Vielmehr werden Aufnahmen von Überwachungskameras eher erst dann gelöscht, wenn das verwendete Speichermedium an seine Kapazitätsgrenzen stößt.

In den Leitlinien 3/2019 des Europäischen Datenschutzausschusses zur Verarbeitung personenbezogener Daten durch Videogeräte, enthalten im Infopaket Videoüberwachung[66] auf der Homepage der Aufsichtsbehörde, hat sich der Ausschuss eindeutig positioniert. Da einer der am häufigsten vorliegenden legitimen Zwecke der Videoüberwachung der Schutz des Eigentums oder die Sicherung von Beweismitteln ist und in der Regel eingetretene Schäden innerhalb von 72 Stunden erkannt werden können, sollte diese Frist grundsätzlich als maximale Speicherdauer für Aufnahmen von Überwachungskameras ausreichen. Soll diese Frist überschritten werden, müsste bei der Argumentation in Bezug auf die Rechtmäßigkeit des Zwecks der Verarbeitung und der Erforderlichkeit für die längere Speicherung höherer Aufwand betrieben werden. Zu hinterfragen wäre dann neben der Erforderlichkeit auch die Geeignetheit der längerfristigen Speicherung für das Erreichen des beabsichtigten Zweckes.

Die Datenschutzkonferenz hat sich der Empfehlung des Europäischen Datenschutzausschusses zur Löschung von nicht mehr erforderlichen Überwachungsaufnahmen innerhalb von 72 Stunden in ihrer „Orientierungshilfe Videoüberwachung durch nichtöffentliche Stellen“ angeschlossen.[67]

---

[66] https://lsaurl.de/InfopaketVideo

[67] https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_vü_dsk.pdf

Soweit das Kamerabetriebssystem oder die Management-Software des Datenrekorders keine Möglichkeit bieten, eine bestimmte Löschfrist einzustellen, um dadurch das automatische zeitgesteuerte Löschen der Kameraaufnahmen zu initiieren, muss der Verantwortliche durch geeignete organisatorische Maßnahmen die manuelle Löschung der Aufnahmen in dieser Frist veranlassen bzw. dies schlicht selbst tun.

Eher nicht oder höchstens sehr ungenau funktionieren wird ein häufig anzutreffendes Verfahren, bei dem die Kamera bzw. der Datenrekorder so konfiguriert sind, dass die ältesten gespeicherten Bilddaten durch die neuesten überschrieben werden (First In – First Out), wenn Platzbedarf besteht, was nach einer angenommenen Zeit von ca. 72 Stunden vielleicht der Fall sein könnte. Dies genügt aber für einen datenschutzgerechten Betrieb der Videoüberwachung in der Regel nicht. Bliebe bei Kameras, die nur bei erkannter Bewegung im Beobachtungsbereich aufzeichnen, der Bildernachschub wegen schlechten Wetters, eines erneuten Pandemie-Lockdowns oder aus anderen Gründen aus, verhinderte dies die rechtzeitige Löschung der ältesten Bilddaten. Die maximale Speicherfrist könnte dadurch weit überschritten werden, was eine Videoüberwachung in dieser Betriebsweise datenschutzrechtlich zumindest zweifelhaft erscheinen ließe.

Die Speicherfrist von Videoüberwachungsaufnahmen hat in der Regel nach 72 Stunden zu enden.

43.3 Kameradummys – datenschutzgerechte Nichtüberwachung

Es bedarf sicherlich keiner vertieften Betrachtung, dass mit Attrappen von Überwachungskameras, sog. Kameradummys, keine personenbezogenen Daten verarbeitet werden können. Folglich sind auf sie die DS-GVO und auch das BDSG nicht anzuwenden. Damit entfällt bei Attrappen für die Aufsichtsbehörde, soweit die Eigenschaft als Kameraattrappe glaubhaft gemacht worden ist, das Recht, nach Art. 58 Abs. 1 lit. b DS-GVO Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen, und es entfällt für den Eigentümer eines solchen kameraähnlichen Gegenstandes z. B. auch die Informationspflicht nach Art. 13 DS-GVO gegenüber den Betroffenen.

Allerdings, und das sind Sinn und Zweck derartiger „Geräte“, erwecken Kameradummys durchaus den Eindruck, dass durch eine echte Überwachung tatsächlich personenbezogene Daten verarbeitet werden. Es entsteht eine Art angenommener Überwachungsdruck, der durch die provozierte Verhaltenssteuerung und -anpassung durchaus zu einer Beeinträchtigung der Persönlichkeitsrechte der Betroffenen führen kann. Hiergegen sind die Betroffenen mitnichten schutzlos: Sie haben, unabhängig von ihrem Beschwerderecht bei einer Aufsichtsbehörde nach Art. 77 DS-GVO, auch die Möglichkeit, sich auf zivilrechtlichem Wege nach §§ 1004, 823 des BGB gegen eine Videoüberwachung bzw. eine Verletzung des allgemeinen Persönlichkeitsrechts zu wehren. Diese Möglichkeit besteht selbst dann, wenn es sich bei einer wahrgenommenen Überwachungskamera lediglich um eine Attrappe oder eine nicht funktionsfähige bzw. nicht aktivierte Kamera handeln sollte oder soweit die Kamera öffentlich zugängliche Flächen oder Nachbargrundstücke nicht wirklich beobachtet. Dies wird von den Nutzern von Kameradummys häufig übersehen.

Für öffentliche Stellen des Landes Sachsen-Anhalt gibt es allerdings eine durchaus wichtige Einschränkung bei der Verwendung von Kameradummys: Sie findet sich in

§ 8 Abs. 4 DSAG LSA. Nach jener Vorschrift nämlich ist der Einsatz von Kameraattrappen nur unter entsprechender Anwendung von § 8 Abs. 1 und 2 DSAG LSA zulässig. Der Gesetzgeber meint damit, dass nur, wenn auch eine echte Videoüberwachung datenschutzrechtlich erlaubt wäre, durch die öffentliche Stelle auch Kameraattrappen eingesetzt werden dürften.

Auch von Überwachungskamera-Dummys kann eine Beeinträchtigung des allgemeinen Persönlichkeitsrechts ausgehen, was einen Abwehranspruch des Betroffenen zur Folge haben kann.

43.4 Ordnungsamt als „Datenschutzaufsicht“

Der Aufsichtsbehörde ging ein Schreiben eines Ordnungsamtes zu, in dem davon berichtet wurde, dass die dortigen Mitarbeiter mit geübtem Auge auf einem privaten Grundstück eine Überwachungskamera festgestellt hatten. Diese Kamera erwecke aufgrund ihrer Ausrichtung den Eindruck, öffentlich zugängliche Bereiche zu erfassen. Das Ordnungsamt leitete gegen den Grundstückseigentümer prompt ein Bußgeldverfahren ein, weil dieser sich trotz deutlicher Aufforderung durch das Amt weigerte, die Kamera, die nach seinen Angaben nur eine Attrappe sei, zu entfernen. Die Aufsichtsbehörde, von der Gemeinde um Fortsetzung des Verfahrens gebeten, äußerte sich nicht gegenüber dem Grundstückseigentümer, sondern im Rahmen einer Beratung nach § 24 Abs. 4 DSAG LSA gegenüber der Gemeinde, und teilte ihr das Folgende mit:

Im Rahmen der der Aufsichtsbehörde durch die DS-GVO sowie durch nationales Recht zugewiesenen Aufgaben ist nach § 23 Abs. 5 DSAG LSA ausschließlich der Landesbeauftragte zuständige Behörde für die Feststellung und die Verfolgung bzw. Ahndung von Ordnungswidrigkeiten nach dem Datenschutzrecht. Nach Art. 57 Abs. 1 lit. d DS-GVO obliegt es ihm, die Verantwortlichen für die ihnen aus der DS-GVO entstehenden Pflichten zu sensibilisieren und nach Art. 58 Abs. 1 lit. b DS-GVO, Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen.

Adressat aufsichtsbehördlicher Tätigkeiten in Bezug auf die Feststellung und die Verfolgung bzw. Ahndung von Ordnungswidrigkeiten nach dem Datenschutzrecht wäre primär der für die Verarbeitung personenbezogener Daten durch eine vermutete Videoüberwachung datenschutzrechtlich Verantwortliche, der zunächst festgestellt werden müsste. Nicht per se sei dies der Grundstücks- oder Gebäudeeigentümer. Infrage kämen ggf. neben der vom Eigentümer bestellten Verwaltungsgesellschaft auch die Mieter oder Pächter selbst und ferner die sonst an der Liegenschaft Nutzungsberechtigten.

Sodann hätte die Aufsichtsbehörde festzustellen, ob tatsächlich keine funktionsfähige Videoüberwachung vorliegt und andernfalls, in welchem Umfang mittels der Videoüberwachung doch personenbezogene Daten verarbeitet werden. Eine Einschränkung der Betriebszeiten der Kamera, des Erfassungsbereiches oder der Bildqualität oder auch ein teilweises Unkenntlichmachen von Bildbereichen durch Privatzonenmaskierung oder auf anderem Wege, könnte dazu führen, dass die Kamera durch ihre Ausrichtung zwar den äußeren Anschein erweckt, unbeschränkt Daten zu erheben, dass diese Datenerhebung in der Praxis aber durch die technische Ausgestaltung oder die Betriebsart der Kamera beschränkt ist. Nur dieser eingeschränkte Umfang wäre dann für die aufsichtsbehördliche Bewertung relevant.

Auch in Fällen, in denen mit einer Videoüberwachung öffentlich zugängliche Bereiche beobachtet oder mitbeobachtet werden, wäre diese Videoüberwachung nicht immer rechtswidrig, jedoch bedarf die mit einer solchen Überwachung verbundene Verarbeitung der personenbezogenen Daten der Betroffenen einer Rechtsgrundlage. Gemäß Art. 6 Abs. 1 DS-GVO ist eine Datenverarbeitung nur zulässig, wenn die betroffene Person eingewilligt hat oder eine gesetzliche Erlaubnisnorm erfüllt ist. Während eine Einwilligung im Fall einer Videoüberwachung von öffentlich zugänglichen Bereichen eher nicht in Betracht kommt, da allein das Betreten oder Befahren eines videoüberwachten Bereiches keine „eindeutig bestätigende Handlung“ und keine informierte Einwilligung im Sinne von Art. 4 Nr. 11 DS-GVO (vgl. Erwägungsgrund 32 DS-GVO) darstellt, könnte für eine Datenverarbeitung mittels Überwachungskamera Art. 6 Abs. 1 Satz 1 lit. f DS-GVO durchaus eine zutreffende Rechtsgrundlage darstellen, soweit diese Videoüberwachung 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. Das Ergebnis dieser gewissenhaften Interessenabwägung wäre u. U. ein Indiz für die Annahme, ob eine bestimmte Videoüberwachung rechtswidrig sein könnte.

Selbst die gesetzlich geregelten aufsichtsbehördlichen Kompetenzen der Aufsichtsbehörde bei einer Datenschutzüberprüfung nach Art. 58 Abs. 1 lit. b DS-GVO gehen im Fall einer festgestellten rechtswidrigen Videoüberwachung nicht so weit, als dass er als Aufsichtsbehörde letztlich auch den Abbau der Kamera verlangen könnte. Sofern ein Verstoß gegen Datenschutzrecht vorliegen sollte, der zunächst verbindlich festgestellt werden müsste und der nicht bereits durch eine Neuausrichtung der Kamera oder anderweitige Änderungen der Datenverarbeitung beseitigt werden kann, könnte die Aufsichtsbehörde allenfalls eine Beschränkung erwirken bzw. ein Verbot der Nutzung der Videoüberwachungstechnik verhängen. Die Beseitigung der Kamera, also der Hardware selbst, könnte die Aufsichtsbehörde jedoch nach Art. 58 Abs. 2 DS-GVO nicht anweisen.

In Bezug auf die Angabe des Grundstückseigentümers, die Kamera sei nicht funktionsfähig und diene lediglich präventiven Zwecken, hatte die Aufsichtsbehörde ggü. der Kommune außerdem das Folgende mitgeteilt: Mit einer nicht funktionsfähigen Überwachungskamera, also einer Art Attrappe, oder einer doch funktionsfähigen aber nicht aktivierten Überwachungskamera, oder soweit eine Kamera öffentlich zugängliche Flächen oder Nachbargrundstücke tatsächlich nicht beobachtet, findet keine datenschutzrechtlich relevante Verarbeitung personenbezogener Daten möglicher Betroffener statt. Das habe zur Folge, dass der Anwendungsbereich der DS-GVO in diesem Fall nicht eröffnet sei, dass kein Raum für die Aufsichtsbehörde bestünde, aufsichtsbehördliche Abhilfemaßnahmen zu ergreifen, soweit die Wahrhaftigkeit entsprechender Angaben über den „Nicht-Betrieb“ angenommen werden könne.

Bei dieser Einschätzung unbeachtet bliebe, da eine tatsächliche Verarbeitung personenbezogener Daten nicht vorliege, die Tatsache, dass auch von einer Kameraattrappe ein gefühlter Überwachungsdruck auf die von der vermuteten Videoüberwachung Betroffenen ausgeübt und dadurch in deren Persönlichkeitsrechte eingegriffen werde. Sich dessen zu erwehren bliebe möglichen Betroffenen die Äußerung eines Unterlassungsverlangens nach §§ 1004, 823 BGB ggü. dem „Betreiber“ der Überwachungskamera und, bliebe dies erfolglos, letztendlich auch der Zivilrechtsweg.

Anlass, wegen der vermuteten Videoüberwachung des öffentlich zugänglichen Bereiches ein Verwaltungsverfahren einzuleiten, hatte die Aufsichtsbehörde in jenem Fall zunächst nicht gesehen. Gegenüber dem Ordnungsamt wurde durch die Aufsichtsbehörde lediglich die Überprüfung angeregt, ob nicht das wegen der vermuteten Videoüberwachung des öffentlich zugänglichen Bereiches und der Weigerung des Grundstückseigentümers, die „Kamera“ zurückzubauen, eingeleitete Bußgeldverfahren eingestellt werden sollte.

Ausschließlich die Datenschutz-Aufsichtsbehörde ist zuständige Behörde für die Feststellung und die Verfolgung bzw. Ahndung von Ordnungswidrigkeiten nach dem Datenschutzrecht.

43.5 Klingelkameras

Während der an der Haus- oder Wohnungstür läutende und sicherlich willkommene Geldbriefträger einer eher selten anzutreffenden Spezies angehören dürfte, könnte es in bestimmten Situationen doch wünschenswert sein, bei einem Läuten zunächst zu schauen, wer da Einlass begehrt, um dann die Entscheidung darüber zu treffen, ob die Person eingelassen werden soll. Am Markt wird eine Fülle diesen Wunsch erfüllender Geräte angeboten. Sie werden Klingelkamera, Video-Türsprechanlage, Video-Türklingel oder Video-Doorbell genannt.

Diese Geräte haben gemeinsam, dass ihr Betrieb eine datenschutzrechtliche Komponente hat. Durch die optische und akustische Erfassung des Besuchers und seiner unmittelbaren Umgebung kommt es zur Verarbeitung seiner personenbezogenen Daten, was zur Folge hat, dass sich der Betrieb einer solchen Klingelkamera an den Grundsätzen der DS-GVO auszurichten hat. Nach Art. 5 DS-GVO sind die Datenverarbeitung und die Auswahl und Gestaltung der Technik an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten (Grundsätze der Datenminimierung und der Speicherbegrenzung).

Klingelkameras sind nicht per se unzulässig. Folgende Bedingungen müssten aber erfüllt sein, um ein solches Gerät datenschutzrechtlich zulässig zu betreiben:

- Mildere Mittel, wie die Einlasskontrolle durch Öffnen der Tür oder durch einen handelsüblichen Türspion kommen aufgrund einer besonderen baulichen Situation und/oder weiterer Umstände eher nicht in Betracht.

- Die Klingelkamera wird ausschließlich durch das Betätigen des Klingeltasters in Betrieb gesetzt und schaltet sich kurz danach selbstständig wieder aus. Keinesfalls darf eine Klingelkamera in permanent eingeschaltetem Zustand betrieben werden. Die abstrakte allgemeine Befürchtung von Straftaten reicht nicht zur Rechtfertigung des Eingriffs in Persönlichkeitsrechte. (Urteil des VG Oldenburg vom 12. März 2013, 1 A 3850/12 Rn. 14, juris)

- Es ist nur eine Live-Beobachtung möglich, eine Aufzeichnung der Kamerabilder darf nicht stattfinden, nicht auf einer Speicherkarte, nicht auf einem verbundenen Mobilgerät und auch nicht bei einem Cloud-Anbieter.

- Die Kamera darf zur Identifikation der Besucher nur den Bereich direkt vor der Tür beobachten. Sie darf dazu neben dem Hauseingang nur insoweit Teile des öffentlichen Verkehrsraumes mitbeobachten, als dies unvermeidlich ist.

- Den Personen, die eine solche Türklingel betätigen, werden durch ein geeignetes Hinweisschild die in Art. 13 DS-GVO genannten Informationen mitgeteilt, soweit diese zutreffen. Auf der Internetseite der Aufsichtsbehörde werden Empfehlungen gegeben, wie den Betroffenen mittels Hinweisschildes die erforderlichen Informationen zur Verfügung gestellt werden können.[68]

  Das Hinweisschild müsste folgende Angaben enthalten:

  - den Namen und die Kontaktdaten des für die Kamera Verantwortlichen,
  - die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen,
  - die Rechtsgrundlage für die Verarbeitung,
  - die berechtigten Interessen, die von dem Verantwortlichen verfolgt werden.

  Hinzu kommen einige weitere in Art. 13 DS-GVO genannte Angaben.

Bei Klingelkameras an Mehrfamilienhäusern kommt noch die Bedingung dazu, dass das Bild des Besuchers allein in die Wohnung übertragen werden darf, bei der geläutet wurde. Auch nur zu dieser Wohnung darf eine Sprechverbindung aufgebaut werden. Das Zuschalten von Wohnungen, bei denen nicht geläutet wurde, muss ausgeschlossen sein.

Eine permanent eingeschaltete Klingelkamera, die regelmäßig auch mit einem Mikrofon ausgestattet ist, könnte schnell auch strafrechtlich relevant werden. Ein Straftatbestand wäre verwirklicht, wenn jemand unbefugt das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt (§ 201 Abs. 1 Nr. 1 StGB) oder unbefugt das nicht zu seiner Kenntnis bestimmte nichtöffentlich gesprochene Wort eines anderen auch nur mit- oder abhört (§ 201 Abs. 2 Nr. 1 StGB). Opfer einer solchen Straftat könnte der Briefträger beim Einlegen einer Sendung in einen Hausbriefkasten in der Nähe der Klingelkamera sein, wenn er sich währenddessen, in der Annahme, unbeobachtet zu sein, mit einem Dritten unterhält oder telefoniert. Dazu muss er sich nicht einmal im optischen Beobachtungsbereich der Kamera aufhalten, Hörentfernung zur Kamera genügt bereits.

Für die Verfolgung eines solchen mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe sanktionierten Vergehens wäre dann nicht die Datenschutz-Aufsichtsbehörde zuständig, sondern die Staatsanwaltschaft.

---

[68] https://lsaurl.de/InfopaketVideo

Klingelkameras dürfen nicht zur dauerhaften Ausforschung der in den Beobachtungsbereich geratenen Dritten missbraucht werden.

43.6 Haushaltsausnahme bei Fotografien von privater Baustelle

Im Jahr 2023 prüfte der Landesbeauftragte aufgrund einer Anfrage, unter welchen Bedingungen es denkbar wäre, dass eine Baustellendokumentation anhand von Fotografien außerhalb des Anwendungsbereichs der DS-GVO stattfindet. Der private Bauherr gab an, diese Fotos nur zur Dokumentation des Baufortschritts für die persönlichen Erinnerungen anzufertigen, dafür aber eine fest installierte Kamera auf der Baustelle anbringen zu wollen.

Zunächst war grundlegend darauf hinzuweisen, dass Fotografien immer dann personenbezogene Daten enthalten, wenn die Qualität der Aufnahmen (z. B. anhand der Größe der Personen auf der Aufnahme und der Auflösung der Fotografien) es zulässt, eine Person zu erkennen (vgl. Art. 4 Nr. 1 DS-GVO, Erwägungsgrund 26). Dies kann auch der Fall sein, wenn es sich nicht um Nahaufnahmen handelt, z. B. wenn eine Person anhand ihrer Kleidung, Körperhaltung, der ausgeführten Tätigkeiten oder mitgeführten Gegenstände identifizierbar ist. Auch wenn dies nicht der Fokus bei diesen Aufnahmen ist, sondern ggf. unbeabsichtigt erfolgt, bleibt es ein personenbezogenes Datum der betroffenen Person. Falls die Aufnahmen keine personenbezogenen Daten enthalten, ist bereits aus diesem Grund die DS-GVO nicht anwendbar.

Bei Aufnahmen mit Personenbezug lautet die zweite zentrale Frage, unter welchen Bedingungen es sich um eine Datenverarbeitung handelt, die unter die so genannte Haushaltsausnahme des Art. 2 Abs. 2 lit. c DS-GVO fällt. Dies ist nach dem genauen Wortlaut der Fall, wenn natürliche Personen ausschließlich persönliche oder familiäre Tätigkeiten ausüben. Zusammenfassend formulierte der Landesbeauftragte dafür folgende Rahmenbedingungen:

- Es dürfen keine Nachbargrundstücke und keine öffentlich-zugänglichen Bereiche im Erfassungsbereich der Aufnahmen liegen (d. h. keine Bereiche außerhalb der umzäunten Baustelle, auch wenn es sich noch um das Privatgrundstück handelt; vgl. die Rechtsprechung des EuGH z. B. in der Rechtssache C-101/01 „Lindqvist“ und C-212/13 „Ryneš“).

- Die Aufnahmen dürfen nicht dazu geeignet sein, die betroffenen Personen zu überwachen. Dies gilt insbesondere für Personen außerhalb des persönlichen oder familiären Bereichs des Bauherrn. Häufig sind die Beschäftigten der Baufirmen betroffen, die der Bauträger mit den Arbeiten auf der Baustelle beauftragt hat. Die schutzwürdigen Interessen dieser Beschäftigten sind deswegen besonders zu berücksichtigen, weil sie sich in Erfüllung ihrer arbeitsvertraglichen Verpflichtung auf der Baustelle aufhalten und der Fotodokumentation nicht entziehen können. Um eine Überwachung zu vermeiden, sind die folgenden Maßnahmen geeignet:

    - größtmögliches Zeitintervall zwischen den Aufnahmen,

    - Aufnahmezeitpunkt in den generell arbeitsfreien Stunden des Tages oder sogar nur am Sonntag,

- Erfassungsbereich, wenn möglich, nur auf den Baustellen-Bereichen, in denen sich selten Personen aufhalten,

- ggf. zusätzlich eine niedrige Bildauflösung, sodass evtl. Personen nicht mehr identifizierbar sind.

- Die Aufnahmen dürfen nicht in einem Cloud-Speicher abgelegt werden, auf den auch der Cloud-Betreiber zugreifen kann.

- Die Fotos dürfen keinen Dritten außerhalb des persönlich-familiären Kreises (Familie und Freunde) zur Verfügung gestellt und nicht im Internet veröffentlicht werden.

- Die Aufnahmen dürfen nicht auf eventuelle Baumängel analysiert und später als Beweismittel bei einer Geltendmachung von Rechtsansprüchen genutzt werden, z. B. gegen Handwerker, Bauträger, Baufirmen, Architekten usw.

Werden diese Rahmenbedingungen nicht eingehalten, fällt die Datenverarbeitung in den Anwendungsbereich der DS-GVO. Damit hat der Bauherr als Verantwortlicher für die Fotoaufnahmen alle Anforderungen der DS-GVO einzuhalten und die entsprechenden Pflichten zu erfüllen. Dies kann durch den Landesbeauftragten als Aufsichtsbehörde überprüft werden.

Aber auch wenn die DS-GVO, z. B. die Informationspflicht des Art. 13 DS-GVO, nicht anwendbar ist, kann es ratsam sein, gegenüber den betroffenen Personen und dem Bauträger Transparenz herzustellen hinsichtlich der Zwecke und des Umfangs der Fotodokumentation, um Konflikte zu vermeiden. Dazu verwies der Landesbeauftragte auf das Muster für ein Informationsblatt bzw. den Aushang, wie er ihn für eine Verarbeitung von Fotografien nach Art. 13 DS-GVO empfehlen würde.[69]

Der Landesbeauftragte wies auch darauf hin, dass sich die betroffenen Personen gegen Datenverarbeitungen auch zivilrechtlich zur Wehr setzen können. Wegen einer Verletzung des allgemeinen Persönlichkeitsrechts können Beseitigungs- und Unterlassungsansprüche aufgrund der §§ 1004, 823 BGB bestehen. Dies ist zum Beispiel möglich, wenn von einer fest installierten (Video- oder Foto-)Kamera ein Überwachungsdruck ausgeht, auch wenn sie nicht (ständig) aktiv ist. Denn man kann ihr häufig nicht ansehen, wann sie eine Aufnahme anfertigt und wann nicht.

Eine Fotodokumentation vom Baufortschritt für private Erinnerungen des Bauherrn ist nicht generell vom Anwendungsbereich der DS-GVO ausgenommen. Dafür müssen bestimmte Rahmenbedingungen eingehalten werden. Um Rechtsunsicherheit, Konflikte oder gar zivilrechtliche Auseinandersetzungen zu vermeiden, ist es stets ratsam, so wenig wie möglich personenbezogene Daten aufzunehmen.

[69] https://lsaurl.de/InfopflichtFoto

44 Bußgeldverfahren

44.1 Statistik der behördlichen Bußgeldverfahren

Datenschutzrechtliche Verstöße kann der Landesbeauftragte mit einer Geldbuße gemäß Art. 83 Abs. 4 bis 6 DS-GVO ahnden (§§ 23 Abs. 5, 31 DSAG LSA i. V. m. § 41 BDSG). In diesem Sinne wurden 19 Bußgeldverfahren eingeleitet. Drei Verfahren wurden eingestellt. Elf Verfahren wurden in 2023 rechtskräftig abgeschlossen.

Die Gesamtsumme der rechtskräftig im Jahr 2023 verhängten Geldbußen aus Verfahren, die auch in Vorjahren begonnen, beläuft sich auf 16.340 Euro:

Tatbestände	Geldbußen insgesamt
Art. 83 Abs. 5 lit. a i. V. m. Art. 9 DS-GVO unzulässige Verarbeitung von Gesundheitsdaten	400 Euro
Art. 83 Abs. 5 lit. a i. V. m. Art. 6 DS-GVO unzulässige Datenverarbeitung durch Nutzung dienstlicher Datenbanken zu privaten Zwecken	2.740 Euro
Art. 83 Abs. 4 lit. a i. V. m. Art. 25 Abs. 1 DS-GVO unzureichender Datenschutz durch Technikgestaltung	4.000 Euro
Art. 83 Abs. 4 lit. a i. V. m. Art. 30, 31, 37 Abs. 1 DS-GVO unzureichende Zusammenarbeit mit der Aufsichtsbehörde, keine Vorlage eines Verarbeitungsverzeichnisses, keine Benennung eines betrieblichen Datenschutzbeauftragten	9.200 Euro

Anlagen

Anlage 1

Organigramm

Stichwortverzeichnis

3

3-G-Regel 88

A

Abruf von Meldedaten 91
abschnittsbezogene Geschwindigkeitskontrolle 84
Akkreditierung 74, 124
Ambulante Pflegedienste 95
Angemessenheitsbeschluss 120, 121
Anruferdaten 149
Arbeitsaufkommen 66, 116
Arbeitsprogramm 3
Artikel 15 DS-GVO 147
Arztpraxis 41
ATD 134
Auftragsverarbeitung 106, 152
Auskunft 147
Auskunfteien 61
Auskunftsanspruch 60
Auskunftsrecht 147, 152
Auskunftsverweigerungsrecht 144

B

Backup 41
BAföG Digital 11, 105
beBPo 18, 74
Behördliche Datenschutzbeauftragte 28
Beitragsservice 133
Berufsgeheimnisträger/Berufsgeheimnisse 53, 54
Berufsorientierung 29
Beschäftigtendatenschutz 142, 144
Beschäftigtendatenschutzgesetz 99
besondere Kategorien personenbezogener Daten 95, 97
Besonderes elektronisches Behördenpostfach 74, 128
Betreuerausweis 157
Betreuung 157
Betriebsarzt 40
betroffene Aufsichtsbehörde 5
Bildungsmanagementsystem 136
BITS 18
Blindkopie 87
Bodycam 84
BRAFO-KE 29
Briefumschläge 43
BSI 16
BundID 138

C

Callcenter	99
Chatkontrolle	131
Consent Manager	80
Cookie	80
Cookies	19
Corona	34, 35, 37, 38, 39, 87, 88, 89
Coronamaßnahmen	140
Corona-Test	33
Corona-Tests an Schulen	31
Corona-Warn-App	30
Cyberangriffe	129

D

DAkkS	74, 124
Data Governance Act	7
Dataport	130
Datenlöschung	14, 21
Datenminimierung	107, 149
Datenschutzbeauftragte	49, 136
Datenschutzbeauftragter	95
Datenschutzinformationen	149
Datenschutzverletzung	91
Datensicherung	41
Datentrennung	153
Datenübermittlung bei gesetzlicher Verpflichtung	156
Datenübermittlung per E-Mail	54
De-Mail	19
Digitalisierung	45
DIN	73
Drittstaatentransfer	6, 122

E

eBO	74
EDSA	3, 117
EGVP	74, 128
Einsatzdokumentation	84
Einsichtsrechte	54
Einwilligung	63, 110
Einwilligungen	56
Elektronischer Rechtsverkehr	74
elektronisches Bürger- und Organisationenpostfach	74
Elternvertretung	24
E-Mailkonto	27
Empfehlungssysteme	9
Energiepreispauschalengesetz	138
Energiewirtschaft	153
Erbenermittlung	62
Europäischer Datenschutzausschuss	117

EU-US Data Privacy Framework 120, 123

F

Facebook-Fanpages 80
Fahreignungsregister 22
Fahrtenbuch 143
Fallstatistik 66, 116
Forschung 135
Forschungsdaten 85
Fotografien 165
Fotografien von vermieteten Wohnungen 56
Fotografieren 29
Fotografieren Fremder 110
Freiwilligkeit der Einwilligung 63
Funkalarmierung 94
Funkmesszähler 13

G

Gastronomie 144
Gemeinderat 49, 145
Gemeinsame Glücksspielbehörde der Länder 20
gemeinsame Verantwortlichkeit 156
gemeinsame Verantwortung 106, 152
genetische Daten 122
Genossenschaft 54
Gerichtspost 134
Gesundheitsanwendungen 139
Gesundheitsdaten 95, 97
Google Fonts 78
Google Street View 132
GPS 143
Grenzüberschreitende Verfahren 5

H

Haushaltsausnahme 110, 165
Häusliche Krankenpflege 95
Hausverbot 156
Herausgabe von Aufnahmen 157
Homeoffice 44

I

IMI 5
Immobilienmakler/Immobilienvermittler 56
Impfdokumentation 87
Impfpflicht 89
Impfstatus 35
Impfterminsoftware 87
Informationspflichten 95, 97
Informiertheit bei der Einwilligung 63

InfoSic 16
Inkasso 62
INPOL 21
Investitionsbank 46

J

Japan 121

K

Kameraattrappe 160, 161
Kinderbilder 109
Kindertagesstätte 44
KI-VO 8
Klingelkamera 163
Kontaktdatenerfassung 38
Kontrolle 134
Konzern 106
Kooperationspflicht 150
Krankenbeförderung/Krankentransport 95, 97
Kreistag 49, 145
Künstliche Intelligenz 8

L

Länderübergreifendes Glücksspielaufsichtssystem 20
Landeskriminalamt 21, 134
Leitlinien 3
Liegenschaftskataster 51
Live-Stream 145
Löschkonzept 61, 73
Löschung personenbezogener Daten 61
Luca-App 30
LUGAS 20

M

Medizin 135
Mein Justizpostfach 128
Meldedatenabrufe 102
Melderecht 49, 102
Meldungen von Datenschutzverletzungen 52, 105, 148
Messenger-Dienst 144
Messstellenbetreiber 153
Microsoft Office 365 25
MID 17
Mitgliederliste 54
Mithören von Telefongesprächen 101
Mitwirkende Personen 40
Mund- und Nasenschutz 37

N

Nachnutzung 105
Nachweis der Erfüllung der Betroffenenrechte 61
Negativauskunft 152
Netzbetreiber 153

O

Offenlegung 144
öffentlicher Aushang 156
Online-Veröffentlichung von Kinderbildern 109
Online-Werbung 9
Onlinezugang 11
Onlinezugangsgesetz 105
OZG 105, 128, 138

P

Patientendaten 140
Patiententelefonnummer 141
Personenbezug 165
Petersberger Erklärung 85
Photovoltaik 153
Plattformen 10
Polizei 21, 82
Polizeiliche Ermittlungen 53
Positivdaten 61
Postaustausch 148
Postaustauschzentrum 148
Postdienstleister 134
Präsenzpflicht an Schulen 34
Privacy by Design 149
Pur-Abo-Modell 132

R

Ransomware 129
Rats- und Bürgerinformationssysteme 47
Rechenschaftspflicht 62, 63
Recht am eigenen Bild 163
Recht auf Löschung 149
Rechtmäßigkeit 21
RED 134
Register 135
Rettungsdienst 94
Rettungsdienst/Rettungswesen 95, 97
Rundfunkbeitrag 133

S

Schließsystem
digital 107
Schrems II 120, 122

Schulgesetz 86
Schulveranstaltungen 29
Scoring 61
Speicherfristen 58
bei der Videoüberwachung 159
Stadtrat 49, 145
Steuer-ID 56
strafrechtliche Ermittlungen 53

T

Taxiunternehmen 95, 97, 149
technische und organisatorische Maßnahmen 41, 54, 107
Telemedien 19
Testzentren 39
Testzentrum 89
Tracking 80
Transpondertechnik 107
Transportverschlüsselung 13
TTDSG 67

U

Unternehmensgruppe 106
Urlaubsbilder 110
USA 120
US-Recht 6

V

Verfassungsschutzbehörde 134
Verjährung 58
Vermögenssorge 157
Versicherungen 53, 58
Versorgungsakten 45
Verwaltungskosten 150
Verzeichnis der Verarbeitungstätigkeiten 95
Videokonferenz 82
Videokonferenzen 130
Videoüberwachung 21, 157, 159, 161, 163
Viren 129

W

Wahl Landesbeauftragter für den Datenschutz 117
Wahlen 49
Wahlwerbung 49
Werbeeinwilligung 63
WhatsApp 89, 137, 144
Wiederherstellung von INPOL-Daten 21
Wohnungswirtschaft 54, 56, 107

Z

Zensus 2022	104
Zertifizierung	74, 124
Zielvereinbarungsgespräche	86
Zusammenarbeit	150
Zwangsgelder	150