20. Wahlperiode

Drucksache **20/8296**

HESSISCHER LANDTAG

07. 06. 2022

Fünfzigster Tätigkeitsbericht zum Datenschutz und Vierter Bericht zur Informationsfreiheit

Hessischer Beauftragter für Datenschutz und Informationsfreiheit

vorgelegt zum 31. Dezember 2021
vom Hessischen Beauftragten für Datenschutz und
Informationsfreiheit Prof. Dr. Alexander Roßnagel
nach Art. 59 der Verordnung (EU) Nr. 2016/679 i. V. m.
§ 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes und
§ 89 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes

Eingegangen am 7. Juni 2022 · Ausgegeben am 8. Juni 2022
Gestaltung: Satzbüro Peters, Taunusstein · Herstellung: AC Medienhaus, Wiesbaden · Landtagsinformationssystem: www.Hessischer-Landtag.de

DER HESSISCHE BEAUFTRAGTE FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT

LT-Drs. 7/1495 v. 29.3.1972 ▫ LT-Drs. **7/3137** v. 29.3.1973 ▫ LT-Drs. **7/5146** v. 1.4.1974 ▫ LT-Drs. **8/438** v. 26.3.1975 ▫ LT-Drs. **8/2475** v. 30.3.1976 ▫ LT-Drs. **8/3962** v. 11.3.1977 ▫ LT-Drs. **9/67** v. 18.12.1978 ▫ LT-Drs. **9/2740** v. 06.2.1980 ▫ LT-Drs. **9/4032** v. 23.12.1980 ▫ LT-Drs. **9/5873** v. 15.1.1982 ▫ LT-Drs. **10/166** v. 12.1.1983 ▫ LT-Drs. **11/473** v. 19.1.1984 ▫ LT-Drs. **11/3215** ▫ 14.2.1985 ▫ LT-Drs. **11/5232** v. 24.1.1986 ▫ LT-Drs. **12/21** v. 18.2.1987 ▫ LT-Drs. **12/1742** v. 26.2.1988 ▫ LT-Drs. **12/4040** v. 2.2.1989 ▫ LT-Drs. **12/6126** v. 13.2.1990 ▫ LT-Drs. **12/7951** v. 11.2.1991 ▫ LT-Drs. **13/1756** v. 4.3.1992 ▫ LT-Drs. **13/3887** v. 23.2.1993 ▫ LT-Drs. **13/5813** v. 11.2.1994 ▫ LT-Drs. **14/412** v. 21.2.1995 ▫ LT-Drs. **14/1418** v. 22.2.1996 ▫ LT-Drs. **14/2701** v. 24.2.1997 ▫ LT-Drs. **14/3697** v. 5.3.1998 ▫ LT-Drs. **15/23** v. 8.4.1999 ▫ LT-Drs. **15/1101** v. 28.3.2000 ▫ LT-Drs. **15/2500** v. 2.4.2001 ▫ LT-Drs. **15/3705** v. 6.3.2002 ▫ LT-Drs. **15/4790** v. 17.3.2003 ▫ LT-Drs. **16/2352** v. 24.4.2004 ▫ LT-Drs. **16/3746** v. 7.3.2005 ▫ LT-Drs. **16/5359** v. 6.3.2006 ▫ LT-Drs. **16/6929** v. 21.2.2007 ▫ LT-Drs. **16/8377** v. 19.2.2008 ▫ LT-Drs. **18/106** v. 27.2.2009 ▫ LT-Drs. **18/2027** v. 9.3.2010 ▫ **18/3847** v. 18.3.2011 ▫ **18/5409** v. 20.3.2012 ▫ **18/7202** v. 9.4.2013 ▫ **19/289** v. 31.3.2014 ▫ **19/2334** v. 31.8.2015 ▫ **19/3510** v. 22.6.2016 ▫ **19/4762** v. 30.3.2017 ▫ **19/6137** v. 7.5.2018 ▫ **20/704** v. 28.5.2019 ▫ **20/2607** v. 6.4.2020 ▫ **20/5799** v. 27.5.2021 ▫**LT-Drs. 20/8296**

50

50. Tätigkeitsbericht Datenschutz
4. Tätigkeitsbericht Informationsfreiheit

Fünfzigster Tätigkeitsbericht zum Datenschutz
und
Vierter Tätigkeitsbericht zur Informationsfreiheit

des

Hessischen Beauftragten für Datenschutz
und Informationsfreiheit

Professor Dr. Alexander Roßnagel

vorgelegt zum 31. Dezember 2021
gemäß Art. 59 der Verordnung (EU) Nr. 2016/679 i. V. m.
§ 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes
sowie § 89 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes

Beiträge zum Datenschutz und zur Informationsfreiheit
Herausgegeben vom Hessischen Beauftragten für Datenschutz und Informationsfreiheit
Prof. Dr. Alexander Roßnagel
Gustav-Stresemann-Ring 1, 65189 Wiesbaden
Postfach 31 63, 65021 Wiesbaden

Telefon: (06 11) 14 08-0
E-Mail: poststelle@datenschutz.hessen.de
Internet: www.datenschutz.hessen.de

Drucksache des Hessischen Landtags 20/8296

Technisch-organisatorische Betreuung: Frauke Börner (HBDI)
Gestaltung: Satzbüro Peters, www.satzbuero-peters.de
Herstellung: AC medienhaus GmbH, Ostring 13, 65205 Wiesbaden-Nordenstadt

Inhaltsverzeichnis

Kernpunkte IX

Vorwort XIII

I Erster Teil
50. Tätigkeitsbericht zum Datenschutz

1. Neue Aufgaben und Rahmenbedingungen 3

2. Datenschutz während der Corona-Pandemie 13
2.1 War Datenschutz ein Hindernis in der Pandemiebekämpfung? 13
2.2 Datenschutzrechtliche Vorgaben zur Kontaktnachverfolgung 16
2.3 Verstöße gegen die Regeln der Kontaktnachverfolgung 21
2.4 Datenerhebung von Reiserückkehrern durch Kitas 24
2.5 Veröffentlichung von Impfdaten in sozialen Netzwerken 25
2.6 Kein Ausschluss der Betroffenenrechte durch Coronavirus-Schutzverordnung 30

3. Digitale Souveränität 35
3.1 Digitale Souveränität und Datenschutz 35
3.2 Digitale Souveränität und erfolgreiche Digitalisierungsprojekte 45

4. Videokonferenzsysteme 51
4.1 Videokonferenzsysteme – Gekommen um zu bleiben 51
4.2 Einsatz von Videokonferenzsystemen in Schulen und Hochschulen 55

5. Europa, Internationales 63
Zusammenarbeit mit anderen europäischen Aufsichtsbehörden 63

6. Bußgeldverfahren, Gerichtsverfahren 69
6.1 Juridifizierung der Arbeit des HBDI 69
6.2 Entwicklungen zu den Bußgeldern 69
6.3 Bußgeldverfahren 72
6.4 Datenschutzrechtliche Verwaltungsgerichtsverfahren 76

7. Polizei, Justiz 79
7.1 Entwicklungen im Bereich der Sicherheits- und Strafverfolgungsbehörden 79
7.2 Datenschutzkontrollen bei Polizeibehörden und Verfassungsschutz 81
7.3 Videoüberwachung der Hessischen Polizei- und Gefahrenabwehrbehörden 86
7.4 Abfragen im Fahreignungsregister bei der Verfolgung von Verkehrsordnungswidrigkeiten 89

8. Allgemeine Verwaltung, Kommunen 91
8.1 Aktuelle Entwicklungen in der öffentlichen Verwaltung 91
8.2 Live-Streaming von Sitzungen und Veröffentlichung von Protokollen im Internet – Kommunalpolitische Teilhabe in Zeiten der Corona-Pandemie 95

9. Schulen, Hochschulen 99
9.1 Verbesserungen durch die Novelle des Hessischen Schulgesetzes 99
9.2 Elektronische Fernprüfungen an Hochschulen 102
9.3 Unzulässige Datenerhebung einer Schule bei der Ausleihe eines mobilen Endgeräts 104
9.4 Datenschutzprobleme der Software-Anwendung Padlet 106
9.5 Datenschutz leicht gemacht 108
9.6 Auskunftsrecht und die schutzwürdigen Belange Dritter 109
9.7 Erste datenschutzrechtliche Eindrücke zum Schulportal Hessen 114

10. Beratung des Hessischen Landtags 117
10.1 Gilt die DS-GVO für den Hessischen Landtag? 117
10.2 Datenschutz im Petitionsgesetz 121
10.3 Neufassung der Datenschutzordnung des Hessischen Landtags 124

11. Beschäftigtendatenschutz 127
11.1 Aktuelle Entwicklungen im Beschäftigtendatenschutz 127
11.2 Nutzung von digitalen Instrumenten zur Mitarbeiterüberwachung 131
11.3 GPS-Tracking im Beschäftigungsverhältnis 134
11.4 Interessenkonflikte bei Datenschutzbeauftragten 140

12. Internet, Werbung 147
12.1 Es menschelt im Netz – Aus dem bunten Alltag der Beschwerdebearbeitung 147
12.2 Die Cookie-Einwilligung – Fluch und Segen zugleich 150

13. Sozialwesen, Videoüberwachung 155
13.1 Bundesteilhabegesetz: Arbeitshilfe „Datenschutz in der Rehabilitation“ 155
13.2 Videoüberwachung in Einkaufspassagen 157

14. Wirtschaft, Banken, Selbstständige 161
14.1 Selbstauskünfte sind auch bei Verschlüsselung gespeicherter Daten zu erteilen 161
14.2 Auskunftsanspruch vs. Tipping-Off-Verbot 162
14.3 Fehlversand von Kundenanschreiben 166

15. Auskunfteien, Inkassounternehmen 169
15.1 Beauskunftung von Anschriftendaten durch Auskunfteien und Inkassounternehmen 169
15.2 Unzulässigkeit der postlagernden Zustellung einer Datenkopie nach Art. 15 DS-GVO 172

16. Verkehrswesen 177
Fahrzeughalterabfrage zur Durchsetzung von Vertragsstrafen auf privaten Parkplätzen 177

17. Gesundheitswesen 183
17.1 Transparenz der Datenverarbeitung 183
17.2 Rechnungen aus der Apotheke per Mail? 184
17.3 Diskretion in Arztpraxis wiederhergestellt 187
17.4 Aufbewahrungsdauer der Patientenakte in Zahnarztpraxis . . 188

17.5 TeleCOVID Hessen 191
17.6 Datenschutzfragen in Abschlussarbeiten und Promotionen 191

18. Technik und Organisation 193
18.1 Meldungen von Datenschutzverletzungen 193
18.2 Ransomware und Ransomware-Angriffe 201
18.3 Umgang mit Schwachstellen in Internet-Diensten 214
18.4 Verlust von Datenträgern 228
18.5 Phase-Out nicht datenschutzrechtskonformer Technologien am Beispiel Fax 231

19. Arbeitsstatistik Datenschutz 237
19.1 Zahlen und Fakten 237
19.2 Ergänzende Erläuterungen zu Zahlen und Fakten 238

Anhang zu I

1. Ausgewählte Entschließungen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder 247
„Chancen der Corona-Warn-App 2.0 nutzen“ vom 29. April 2021 247

2. Ausgewählte Beschlüsse der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder 249
2.1 „Energieversorgerpool“ darf nicht zu gläsernen Verbraucher*innen führen“ vom 15. März 2021 249
2.2 „Verarbeitung von Positivdaten von Privatpersonen aus Verträgen über Mobilfunkdienste und Dauerhandelskonten durch Auskunfteien“ vom 22. September 2021 250
2.3 „Verarbeitungen des Datums ‚Impfstatus‘ von Beschäftigten durch die Arbeitgeberin oder den Arbeitgeber“ vom 19. Oktober 2021 251

2.4 Zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO auf ausdrücklichen Wunsch betroffener Personen“ vom 24. November 2021 253

3. Ausgewählte Orientierungshilfen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder 255

Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail (Stand 16.06.2021) 255

II Zweiter Teil

4. Tätigkeitsbericht zur Informationsfreiheit

1. Einführung Informationsfreiheit 267

2. „Voraussetzungsloser“ Informationszugang und kommunaler Satzungsvorbehalt 269

3. Weitergabe von Daten der antragstellenden Person 273

4. (Keine) Informationsbeschaffung für den Antragsteller seitens des Informationsfreiheitsbeauftragten 275

5. Kommt Open Data nach Hessen? 279

6. Arbeitsstatistik Informationsfreiheit 285

ANHANG zu II

1. Ausgewählte Entschließungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland 289

1.1 „Mehr Transparenz beim Verfassungsschutz – Vertrauen und Legitimation stärken!“ vom 2. Juni 2021 289

1.2 „Forderungen für die neue Legislaturperiode des Bundes: Ein Transparenzgesetz mit Vorbildfunktion schaffen!“ vom 2. Juni 2021 290

1.3 „Mehr Transparenz durch behördliche Informationsfreiheitsbeauftragte!“ vom 2. Juni 2021 292

1.4 „EU-Richtlinie zum Whistleblowerschutz zeitnah umsetzen! Hinweisgeberinnen und Hinweisgeber umfassend und effektiv schützen!“ vom 3. November 2021 293

1.5 „Umweltinformationen: Beratungs- und Kontrollkompetenz auch auf Landesbeauftragte für Informationsfreiheit übertragen!“ vom 3. November 2021 294

1.6 Tromsø-Konvention ratifizieren und einheitlichen Mindeststandard für den Zugang zu Informationen in ganz Deutschland schaffen! vom 3. November 2021 295

Verzeichnis der Abkürzungen 297

Register der Rechtsvorschriften 303

Sachwortverzeichnis 309

Kernpunkte

1. Für den Datenschutz in Hessen waren im Berichtszeitraum keine schwerwiegenden Verstöße festzustellen – ganz im Gegensatz zur Entwicklung in Deutschland oder in der Welt. In Hessen wurde Datenschutz weitgehend akzeptiert und nicht grundsätzlich in Frage gestellt. Dennoch sind in vielen Bereichen die Anforderungen der Datenschutz-Grundverordnung (DS-GVO) noch immer nicht ausreichend umgesetzt, führen zu Beschwerden, erfordern das Eingreifen der Datenschutzaufsicht sowie Anordnungen und Durchsetzungsmaßnahmen im Einzelfall. Die Digitalisierung vieler Aufgaben und Tätigkeiten verursacht für die Verantwortlichen zusätzliche Pflichten, bringt zusätzliche Anforderungen mit sich und erfordert zusätzliche Aufmerksamkeit (Teil I Ziff. 1).
2. Für die Weiterentwicklung des Datenschutzes in Hessen gewinnen die Europäisierung mit Entscheidungen des Europäischen Gerichtshofs (EuGH) und des Europäischen Datenschutzausschusses (EDSA) (Teil I Ziff. 1 und 5) sowie die Juridifizierung des Datenschutzrechts mit einem deutlichen Anstieg der Bußgeldbescheide (von 2 im Jahr 2020 auf 29 im Jahr 2021) und unter Einbeziehung der Gerichte (Teil I Ziff. 1 und 6) zunehmend an Bedeutung. Dies erfordert stärkere Einflussnahme auf die europäischen Entwicklungen durch engagierte Mitarbeit in Arbeitskreisen des EDSA und den Ausbau des Justiziariats zur Bewältigung der zusätzlichen Prozessverfahren.
3. Die vielfältigen Datenschutzfragen bei der Umsetzung der Corona-Schutzmaßnahmen führten in vielen alltäglichen Lebensbereichen zu datenschutzrechtlichen Beschwerden, Nachfragen und Beratungen von Betroffenen und für die Datenverarbeitung Verantwortlichen (Teil I Ziff. 1 und 2). Außerdem waren zusätzliche Maßnahmen erforderlich, um die zu Beginn der Pandemie getroffenen Entscheidungen zum Umgang mit den neuen Herausforderungen, die in der Situation verständlich, im Ergebnis aber datenschutzwidrig waren, nach und nach zu korrigieren (Teil I Ziff. 1 und 4.2).
4. Nach wie vor war ein zentraler Schwerpunkt der Aufsichtstätigkeit die Bearbeitung von Beschwerden, Nachfragen und Beratungen zur Ausübung von Betroffenenrechten sowie zur Unterstützung von Verantwortlichen. Ihre Zahl stabilisiert sich vier Jahre nach dem Wirksamwerden der DS-GVO auf einem sehr hohen Niveau, qualitativ werden sie anspruchsvoller. Einfachere Fragen, wie etwa zu Informationspflichten und Auskunftsrechten, gehen zurück und mit ihnen telefonische Beratungen (von mehr als 10 Minuten) (von 9.444 auf 6.384). Dagegen nahmen schwierigere

Bearbeitungen und mit ihnen die dokumentierten Eingaben immer noch leicht zu (von 7.991 auf 8.404). Große Digitalisierungsprojekte, wie z. B. die Umsetzung des Onlinezugangsgesetzes oder das Hessische Schulportal, schlagen in der Statistik nicht in dem Ausmaß zu Buche, wie sie meine Behörde tatsächlich beschäftigen (Teil I Ziff. 19).

5. Meldungen von Datenschutzpannen und Datenschutzverletzungen gemäß Art. 33 DS-GVO bilden mittlerweile einen Großteil der reaktiven Tätigkeit meiner Aufsichtsbehörde. Neue Formen von Cyberkriminalität wie Phishing- und Ransomware-Angriffe, das Ausnutzen von Sicherheitsschwachstellen und das Veröffentlichen personenbezogener Daten im Darknet verursachten neue Gefährdungen der betroffenen Personen und der Verantwortlichen und führten zu einem Anstieg der Meldungen (von 1.432 auf 2.016) (Teil 1 Ziff. 17).
6. In den Verwaltungsbehörden des Landes und der Kommunen werden derzeit große und anspruchsvolle Digitalisierungsprojekte konzipiert, geplant und umgesetzt, die eine intensive Beteiligung und kritische Mitarbeit der Datenschutzaufsicht erfordern (Teil I Ziff. 8).
7. Die Schulen und Hochschulen waren vor allem geprägt durch starke Entwicklungen zu mehr Digitalisierung von Unterricht und Prüfungen, Lehre und Lernen. Neben dem Einsatz von Videokonferenzsystemen (Teil I Ziff. 4) betraf dies z. B. Geräteausleihen, Lernhilfen und Fernprüfungen. Im Schulbereich begleitete ich die Entwicklungen des Hessischen Schulportals und beriet zu den datenschutzrechtlichen Vorschriften des neuen Schulgesetzes (Teil I Ziff. 9).
8. Die Digitalisierung der Arbeit führt dazu, dass in Beschäftigtenverhältnissen die Arbeitgeber immer intensiver die Leistung und das Verhalten der Beschäftigten überwachen können. In diesem Bereich musste meine Behörde in mehreren Fällen korrigierend eingreifen (Teil I Ziff. 11).
9. Im Bereich der Videoüberwachung durch Polizei und Gefahrenabwehrbehörden, aber noch mehr durch private Unternehmen und im Nachbarschaftsverhältnis musste meine Behörde immer wieder streitschlichtend eingreifen (Teil I Ziff. 7 und 13).
10. Im Bereich der privaten Wirtschaft musste ich vielen Beschwerden insbesondere zu Rechten betroffener Personen wie dem Auskunftsanspruch (Teil I Ziff. 14) und zur Verarbeitung von Anschriftendaten durch Auskunfteien und Inkassounternehmen (Teil I Ziff. 15) nachgehen.
11. Im Gesundheitswesen war die Datenschutzaufsicht stark durch die Datenverarbeitung im Kontext der Corona-Pandemie belastet (Teil I Ziff. 2). Aber auch Probleme etwa zur Wahrung des Patientengeheimnisses, der

Übermittlung von Patientendaten und der Aufbewahrung von Patientenakten mussten gelöst werden. (Teil I Ziff. 17).

12. Obwohl die Informationsfreiheit in Hessen immer noch nur in der Landesverwaltung und wenigen Gemeinden und Landkreisen gilt, hatte ich als Informationsfreiheitsbeauftragter im Berichtsjahr viele interessante Fragen zur Informationsfreiheit zu beantworten und unterstützte ich viele Bürgerinnen und Bürger bei der Durchsetzung ihrer Ansprüche (Teil II Ziff. 2 und 3). Außerdem beteiligte ich mich an der rechtspolitischen Fortentwicklung der Informationsfreiheit (Teil II Ziff. 5) und arbeitete in der Konferenz der Informationsfreiheitsbeauftragten (IFK) mit (Teil II Anhang).
13. Beschwerden und Beratungen stiegen leicht (von 111 auf 123).

Vorwort

Dies ist der erste von mir verantwortete Tätigkeitsbericht und zugleich der 50. des Hessischen Beauftragten für Datenschutz und Informationsfreiheit. Der erste Tätigkeitsbericht (Landtags-Drucksache 7/1495) stammt vom 29. März 1972. Mit ihm beschrieb der erste Datenschutzbeauftragte Hessens, Willi Birkelbach, die ersten Gehschritte der Datenschutzaufsicht in dem neuen Aufgabenfeld des Datenschutzes. Die Aufgaben des Datenschutzbeauftragten waren damals ohne jedes Vorbild, weil das Hessische Datenschutzgesetz (HDSG) vom 7. Oktober 1970 das erste Datenschutzgesetz der Welt war. Insofern gab es auch noch kein Vorbild für einen solchen Bericht. Es war der erste Datenschutzbericht der Welt.

Der Bericht beschreibt einen „Vorstoß ins Neuland“ des Datenschutzes (S. 10f.). Das Gesetz galt nur für die maschinelle Datenverarbeitung in der öffentlichen Verwaltung des Landes Hessen. Es war eine Reaktion auf die Gründung der Hessischen Zentrale für Datenverarbeitung (HZD) und der Kommunalen Gebietsrechenzentren (KGRZ) (S. 8). Das Datenschutzgesetz galt für alle Daten natürlicher und juristischer Personen, die von Rechenzentren und Behörden der öffentlichen Verwaltung verarbeitet wurden. Es verfolgte drei Ziele: den Schutz vor Eingriffen in die Privat- und Geheimsphäre, die Erhaltung der Gewaltenteilung zwischen Parlament, Regierung und Gemeinden und die Sicherung der Daten und Datenbestände (S. 31). Die Aufgaben des Datenschutzbeauftragten bestanden nach § 10 HDSG darin, die Einhaltung des Gesetzes zu überwachen und die zuständige Aufsichtsbehörde zu unterrichten sowie die Auswirkungen der maschinellen Datenverarbeitung auf die staatliche Gewaltenteilung zu beobachten (S. 11f.). Objekte der Untersuchungen und Beobachtungen waren u.a. Maschinenräume und Datenträgerarchive, Lochkarten und Magnetbänder (S. 20, 31f.). Die Integration von Datenbeständen und die Ferndatenverarbeitung waren am zeitlichen Horizont zu erkennen (S. 33f.). Der Datenschutzbeauftragte wurde nach § 7 Abs. 1 HDSG vom Landtag auf Vorschlag der Landeregierung gewählt und war nach § 8 HDSG frei von Weisungen. Ihm standen zur Erfüllung seiner Aufgaben ein technischer Amtsrat und ein Beamter des höheren Dienstes sowie eine Schreibkraft zur Verfügung (S. 35).

Bemerkenswert für diesen ersten Tätigkeitsbericht sind Erkenntnisse zur Aufgabe des Datenschutzes und der Datenschutzaufsicht, die nach der Erfahrung mit 49 weiteren Tätigkeitsberichten zeitlos erscheinen: Zum einen bemerkt Birkelbach zum Verhältnis von Datenschutzrecht und Informationstechnik, dass bei einer unregulierten Entwicklung der Informationstechnik die Gefahr besteht,

> „dass nicht mehr die Gesetze die Entwicklung der Datenverarbeitung bestimmen, sondern dass sie dem Stand der Datenverarbeitung angepasst werden. Denn wenn man die EDV-Anlagen erst einmal mit hohem finanziellem Aufwand installiert und die Arbeitsstrukturen entsprechend umgestellt hat, dann sind Sachzwänge entstanden, die den Entscheidungsspielraum … einengen. Die nachträgliche Berücksichtigung der für den Datenschutz notwendigen Maßnahmen wäre mit hohem Aufwand verbunden oder gar nicht mehr durchführbar“ (S. 36).

Zum anderen schließt Birkelbach seinen Bericht mit einem Zukunftsblick auf die Herausforderungen des Datenschutzes, der noch heute – in einer Welt der künstlichen Intelligenz, des Big Data und der globalen und allgegenwärtigen Datenverarbeitung – zutreffend ist:

> Die „Entwicklung steht nicht still. Neue Techniken werden vielleicht schon morgen neue Wege zum Fortschritt und zum Wohl des Menschen erschließen; aber sie werden auch neue, unbekannte Gefahren für den Einzelnen und für die freiheitliche Struktur von Staat und Gesellschaft in sich bergen. Diesen Gefahren muss rechtzeitig und wirksam entgegengetreten werden. Stete Wachsamkeit ist notwendig. Auch die Gesellschaft wird ihre Strukturen wandeln. Neue Bedürfnisse und Auffassungen werden auch Fragen des Datenschutzes berühren. Datenschutz ist deshalb keine einmalige, sondern eine permanente Aufgabe, die jeden Tag aufs Neue gestellt wird und die es gilt, jeden Tag neu zu überdenken“ (S. 36).

Dieser Aufgabe stellten sich auch die folgenden 48 Tätigkeitsberichte der Hessischen Datenschutzbeauftragten. Willi Birkelbach (Beauftragter vom 9. Juni 1971 bis 18. Juni 1975) verantwortete auch den zweiten und dritten Bericht. Danach folgten der vierte bis 19. Tätigkeitsbericht, die auf Prof. Dr. Spiros Simitis (Beauftragter vom 18. Juni 1975 bis 22. Oktober 1991) zurückgehen. Danach folgten der 20. bis 24. Tätigkeitsbericht, die Prof. Dr. Winfried Hassemer (Beauftragter vom 22. Oktober 1991 bis 30. Mai 1996) verantwortete, der 25. bis 27. Tätigkeitsbericht, die auf Dr. Rainer Hamm (Beauftragter vom 30. Mai 1996 bis 29. Juni 1999) zurückgehen, danach der 28. bis 31. Tätigkeitsbericht, die Prof. Dr. Friedrich von Zezschwitz (Beauftragter vom 29. Juni 1999 bis 30. September 2003) verfasst hat, und schließlich der 32. bis 49. Tätigkeitsbericht, die Prof. Dr. Michael Ronellenfitsch (Beauftragter vom 1. Oktober 2003 bis 28. Februar 2021) erstellte.

Die Berichte der Hessischen Datenschutzbeauftragten dokumentieren auf beeindruckende Weise die Geschichte des Datenschutzes und des Datenschutzrechts in Hessen, Deutschland und Europa. Denn der Datenschutz in Hessen hat den Datenschutz in Deutschland und in der Europäischen Union beeinflusst und wurde von den Rahmenbedingungen, die von den Datenschutzentwicklungen in Deutschland und Europa ausgingen, geprägt. Zu

denken ist etwa an das Inkrafttreten des Bundesdatenschutzgesetzes zum 1. Januar 1978, an das Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983, die europäische Datenschutzrichtlinie vom 24. Oktober 1995, das Urteil des Europäischen Gerichtshofs vom 10. März 2010, das die Unabhängigkeit der Datenschutzaufsicht forderte, und der Geltungsbeginn der Datenschutz-Grundverordnung in Deutschland am 25. Mai 2018. Hessen hat auf diese Entwicklungen mit fünf Novellen des Datenschutzgesetzes reagiert und zusätzlich mehrfach Regelungen dieses Gesetzes angepasst. Wichtig waren u.a. die Reaktionen auf das Volkszählungsurteil durch rechtsstaatliche Korrekturen zur Verbesserung des Grundrechtsschutzes und die Umsetzung der Datenschutzrichtlinie durch verbesserte Regelungen zum Datenschutz. Auf das Urteil des Europäischen Gerichtshofs hin wurde die Datenschutzaufsicht über den öffentlichen und den nicht öffentlichen Bereich zusammengeführt und die Datenschutzaufsichtsbehörde als unabhängige oberste Landebehörde errichtet. In Anpassung auf die Datenschutz-Grundverordnung beschloss der Hessische Landtag das Hessische Datenschutz- und Informationsfreiheitsgesetz (HDSIG) vom 3. Mai 2018. Die Tätigkeitsberichte der Hessischen Datenschutzaufsicht dokumentieren all diese Entwicklungen und ihre Auswirkungen auf die Praxis des Datenschutzes und die Tätigkeiten der Datenschutzaufsicht.

Der 50. Tätigkeitsbericht, der die Entwicklungen im Jahr 2021 umfasst, beschreibt gegenüber dem ersten Tätigkeitsbericht radikal veränderte Verhältnisse und viele neue Problembereiche und Herausforderungen, von denen vor 50 Jahren noch niemand eine Vorstellung hatte – aber auch noch immer die grundsätzliche Aufgabe, individuelle und gesellschaftliche Selbstbestimmung gegenüber den Mächten, die Datenverarbeitung nutzen, zu verteidigen und Machtungleichgewichte, die durch die Datenverarbeitung entstehen, auszugleichen.

Allerdings sind diese Aufgaben unter ganz neuen Umständen zu erfüllen: Die alltägliche Nutzung von weltweit vernetzter Informationstechnik durch nahezu jeden und jede hat zu einer Explosion personenbezogener Daten geführt. Deren Informationsgehalt ist so reich, dass nahezu jede Lebensregung erfasst und abgebildet werden kann. Meinungen, Werthaltungen, Interessen, Präferenzen, Gewohnheiten, Beziehungen und Bewegungen erscheinen für nahezu jede Person berechenbar. Diese Informationsmenge und neue Auswertungstechniken bieten bisher ungeahnte Möglichkeiten, durch Datenverarbeitung das Verhalten von einzelnen, gesellschaftlichen Gruppen und sogar Staaten vorherzusagen und zu beeinflussen. Risiken und Einschränkungen der individuellen und kollektiven Selbstbestimmung gehen nicht mehr nur von staatlichen Instanzen aus, sondern – vor allem

sogar – von privater Seite, angefangen von der neugierigen Nachbarin bis hin zu weltweit agierenden Großkonzernen.

Noch immer gilt jedoch die Erkenntnis aus dem ersten Tätigkeitsbericht, dass sich die Gefahren für Freiheit und Selbstbestimmung andauernd wandeln, dass wir ihnen aber immer wieder rechtzeitig und wirksam entgegentreten müssen. „Datenschutz ist deshalb keine einmalige, sondern eine permanente Aufgabe, die jeden Tag aufs Neue gestellt wird und die es gilt, jeden Tag neu zu überdenken.“ Und die datenschutzgerechte Gestaltung der Informationstechnik und die Einrichtung von Vorsorge- und Schutzmaßnahmen muss erfolgen, bevor „Sachzwänge entstanden sind, die den Entscheidungsspielraum … einengen. Die nachträgliche Berücksichtigung der für den Datenschutz notwendigen Maßnahmen wäre mit hohem Aufwand verbunden oder gar nicht mehr durchführbar.“

Die Funktion des Tätigkeitsberichts ist geblieben – wie im ersten Tätigkeitsbericht der hessischen Aufsichtsbehörde beschreibt und analysiert der 50. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten die aktuelle Praxis des Datenschutzes in Hessen und die Möglichkeiten der Aufsichtsbehörde, auf diese zugunsten der Grundrechte und der Demokratie Einfluss zu nehmen.

Prof. Dr. Alexander Roßnagel

I

Erster Teil

50. Tätigkeitsbericht zum Datenschutz

1. Neue Aufgaben und Rahmenbedingungen

Der vorliegende Tätigkeitsbericht beschreibt und analysiert den Datenschutz in Hessen im Jahr 4 seit dem Geltungsbeginn der Datenschutz-Grundverordnung am 25. Mai 2018. Viele Unsicherheiten, die der neue, sehr abstrakte Rechtsrahmen für die Praxis des Datenschutzes gebracht hat, sind überwunden. Einige Streitfragen sind inzwischen geklärt, andere sind noch immer in der Diskussion. In manchen Handlungsbereichen ergeben sich erste Routinen. Die Europäisierung des Datenschutzes schreitet voran und verändert zunehmend die Aufgaben und Handlungsmöglichkeiten der Datenschutzaufsicht.

Rechtsprechung des Europäischen Gerichtshofs

Entsprechend steigt die Bedeutung des Europäischen Gerichtshofs und seiner Rechtsprechung für die Fortentwicklung des Datenschutzrechts. Er hat inzwischen einige wichtige Entscheidungen zum Datenschutz und zur Auslegung der Datenschutz-Grundverordnung getroffen und durch sie bestehende Streitfragen geklärt. Aber jede Entscheidung konzentriert sich auf ihren Entscheidungsgegenstand und enthält doch auch immer über ihn hinausweisende Bemerkungen. Dadurch hinterlassen die Entscheidungen viele neue Fragen, über die gestritten wird und die Rechtsunsicherheit für Verantwortliche und Aufsichtsbehörden bewirken. Ein Beispiel ist das „Facebook-Fanpage-Urteil“ vom 5. Juni 2018 (C-210/16), in dem das Gericht festgestellt hat, dass der Betreiber einer „Fanpage“ und Facebook eine gemeinsame Verantwortung für die Verarbeitung der Daten von Personen haben, die die „Fanpage“ besuchen. Seit diesem Urteil wird bei jeder IT-Kooperation zwischen zwei Stellen gefragt, ob sie eine gemeinsame Verantwortung für die Datenverarbeitung tragen. Eine klare, von allen akzeptierte Abgrenzung zur getrennten Verantwortung oder zur Auftragsverarbeitung wurde noch nicht gefunden. Diese Frage hat die Hessische Datenschutzaufsicht in vielen Einzelfällen beschäftigt. Ein weiteres Beispiel ist das „Schrems II-Urteil“ vom 16. Juli 2020 (C-311/18). Es ist sehr verdienstvoll, dass das Gericht klargestellt hat, dass der internationale Datentransfer das durch die Datenschutz-Grundverordnung gewährleistete Schutzniveau für den Grundrechtsschutz nicht untergraben darf. Dementsprechend hat es angesichts der unverhältnismäßigen Überwachungspraktiken von US-amerikanischen Geheimdiensten und des Fehlens jeglichen Rechtsschutzes für US-Ausländer die Entscheidung der Kommission, den Grundrechtsschutz zugunsten ungestörten Datenaustauschs zu reduzieren, für unionsrechtswidrig und nichtig erkannt. Zulässig sind Datentransfers in die USA nur noch, wenn die Verantwortlichen zusätzliche Schutzmaßnah-

men gegen den Zugriff der US-Behörden vorsehen. Viele sich an diese Feststellung anschließende Fragen blieben aber ungeklärt – so z. B. welche zusätzlichen Schutzmaßnahmen für weiteren Datenaustausch erforderlich sind und wie diese angesichts der enormen Abhängigkeit gegenüber IT-Anbietern aus den USA umgesetzt werden können (s. Ziff. 3). Diese Fragen betrafen viele Bemühungen zur Umsetzung des Urteils in Hessen wie etwa hinsichtlich Videokonferenzsystemen (s. Ziff. 4). Ein letztes Beispiel ist das Urteil zum Hessischen Petitionsausschuss vom 9. Juli 2020 (C-272/19). In diesem hat das Gericht festgestellt, dass der Petitionsausschuss im Hessischen Landtag der Datenschutz-Grundverordnung unterliegt. Es hat sich aber ganz eng auf die Einordnung des Petitionsausschusses beschränkt und dadurch Unklarheit hinsichtlich vieler weiterer, wichtiger Fragen hinterlassen, wie etwa zur Frage, ob die Landtage in Deutschland in den Anwendungsbereich der Verordnung fallen. Diese Frage konnte ein Rechtsgutachten, das ich für den Hessischen Landtag erstellt habe, dahingehend klären, dass die Datenverarbeitungen zur Unterstützung der parlamentarischen Tätigkeiten des Landtags, der Landtagsfraktionen und der Landtagsabgeordneten nicht der Datenschutz-Grundverordnung unterfallen (s. Ziff. 10).

Europäische Zusammenarbeit

Die Rahmenbedingungen für die Hessische Datenschutzaufsicht werden zunehmend auch durch die Europäische Datenschutzinfrastruktur bestimmt, von der sie ein Teil ist. Der Europäische Datenschutzausschuss (EDSA) hat inzwischen Tritt gefasst und viele Streitfragen in grenzüberschreitenden Einzelfragen entschieden sowie viele hilfreiche Klarstellungen in Form von Empfehlungen, Leitlinien und Stellungnahmen gegeben.

Der Ausschuss ist damit neben dem Europäischen Gerichtshof die Instanz, die unionsweit festlegt, wie die abstrakten Vorschriften der Datenschutz-Grundverordnung im Praxisvollzug zu verstehen sind. Wer darauf einwirken will, wie der Datenschutz künftig in der Union verstanden und praktiziert wird, muss sich aktiv in die Arbeit des EDSA und seiner Arbeitskreise einbringen (s. Ziff. 5).

Um einen einheitlichen Vollzug des Datenschutzes in der Union sicherzustellen, sieht die Datenschutz-Grundverordnung eine enge grenzüberschreitende Zusammenarbeit der Aufsichtsbehörden in den Mitgliedstaaten vor. Berührt ein Aufsichtsverfahren mehrere Mitgliedstaaten, sollen sich die Aufsichtsbehörden über die erforderlichen Maßnahmen einigen. Kommt keine Einigung zustande, entscheidet der EDSA in dem umstrittenen Aufsichtsverfahren abschließend. Diese von der Datenschutz-Grundverordnung verordnete Zusammenarbeit zwischen den Aufsichtsbehörden erweist sich vor allem deshalb als schwie-

rig und aufwendig, weil ihr die notwendige kulturelle Grundlage fehlt. Alle Mitgliedstaaten entstammen unterschiedlichen Datenschutztraditionen und haben unterschiedliche Verständnisse von Datenschutzaufsicht entwickelt. Daher muss zwischen den Aufsichtsbehörden sehr oft über unterschiedliche Begriffsverständnisse, Vollzugspraktiken und Zielsetzungen in der Rechtsumsetzung verhandelt werden. Hinzu kommen die Sprachprobleme und die umständlichen Verfahren der Zusammenarbeit. Insgesamt setzt die Datenschutz-Grundverordnung einen Kulturwandel der Zusammenarbeit in allen Mitgliedstaaten voraus, den sie nicht selbst gewährleisten kann. Da aber in diesen Verfahren der Zusammenarbeit entschieden wird, wer Einfluss auf das künftige Verständnis des Datenschutzes in der Europäischen Union hat, ist eine intensive Beteiligung notwendig (s. Ziff. 5). Dennoch ist es oft frustrierend, hilflos mitansehen zu müssen, wie die Datenschutzanforderungen, auf die sich alle Aufsichtsbehörden der Union geeinigt haben, für die weltweit agierenden Technologiekonzerne, für die es am wichtigsten wäre, praktisch nicht gelten, weil die zuständige Aufsichtsbehörde diese ihnen gegenüber nicht oder unzureichend durchsetzt.

Juridifizierung der Aufsichtstätigkeit

Die Datenschutz-Grundverordnung hat neue rechtliche Handlungsmöglichkeiten für betroffene Personen und die Aufsichtsbehörden geschaffen, die grundsätzlich zu begrüßen sind, aber zu einer stärkeren Juridifizierung der Aufsichtstätigkeit führen. Zum einen hat jede betroffene Person nach Art. 77 DS-GVO das Recht auf Beschwerde bei einer Aufsichtsbehörde, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die Verordnung verstößt. Ist sie mit der Bearbeitung ihrer Beschwerde nicht einverstanden, kann sie nach Art. 78 DS-GVO beim zuständigen Verwaltungsgericht eine Klage gegen den rechtsverbindlichen Beschluss der Aufsichtsbehörde einlegen. Beide Rechte stärken den Grundrechtsschutz, weil sie der individuellen Rechtsdurchsetzung helfen und individuelle Selbstbestimmung gegenüber mächtigen Datenverarbeitern stärken können. Die Beschwerden sind für die Aufsichtsbehörden auch hilfreiche Mittel, um Erkenntnisse zur Praxis des Datenschutzes zu gewinnen. Zum anderen hat die Datenschutz-Grundverordnung in Art. 58 den Aufsichtsbehörden stärkere Befugnisse gegeben, Datenschutz in der Praxis durchzusetzen. Sie können gegenüber nicht öffentlichen Verantwortlichen Anordnungen zur Datenverarbeitung treffen und bei Verstoß gegen Datenschutzvorschriften empfindliche Bußgelder verhängen. Sowohl die neuen Rechte der betroffenen Personen als auch die größere Eingriffstiefe der neuen Befugnisse der Aufsicht in die Grundrechte von Unternehmen führen dazu, dass es zu einer steigenden Anzahl von Gerichtsprozessen kommt. Die Aussicht, dass ihre

Handlungen zunehmend gerichtlichen Überprüfungen unterzogen werden, prägt in immer stärkerer Weise ihren Aufgabenzuschnitt und den Charakter ihrer Aufsichtstätigkeit. Diese wird förmlicher und umständlicher. Sie wird zunehmend geprägt von Fragen der Verfahrensrechte, der Aktenführung, der Darlegungslast, der Beweisführung und prozesstaktischen Überlegungen. Unvoreingenommene Beratungen und Hilfestellungen gegenüber den Verantwortlichen und den betroffenen Personen, die sehr schnell zum Prozessgegner werden können, werden schwieriger.

Die seit 2018 ansteigende Zahl der Beschwerden führt bei der Ressourcenausstattung der Aufsichtsbehörde zu dem Dilemma, dass die Aufsichtsbehörde der zunehmenden Arbeitslast nur gerecht werden kann, wenn sie Mittel der Arbeitsrationalisierung nutzt. Diese kann aber zur Unzufriedenheit bei den Personen führen, die Beschwerde eingelegt haben, und zu einem Anstieg der Klagen gegen die Aufsichtsbehörde. Diese wiederum erhöhen die Arbeitslast und gefährden das Ansehen der Aufsichtsbehörde als Treuhänder der Grundrechte der betroffenen Personen.

Durch die Juridifizierung der Aufsichtstätigkeit kommt der Rechtsprechung der nationalen Gerichte eine zunehmende Bedeutung für den Datenschutz zu. Allerdings gibt es keine auf Datenschutz spezialisierten Gerichte, Kammern oder Senate. Vielmehr entscheiden die einzelnen Spruchkörper meist zu selten über Datenschutzfragen, als dass sie immer in die spezielle Systematik und Methodik des Datenschutzrechts eingedacht sein könnten. Dies erschwert eine konsistente Rechtsprechung in diesem Bereich. Hinzu kommt, dass durch die Gerichtsentscheidungen an entscheidender Stelle wieder eine von nationalen Rechtsvorstellungen geprägte Sichtweise zur Geltung kommt. Selbst wenn die Aufsichtsbehörden des Bundes und der Länder in ihrer Konferenz (DSK) mühsam eine einheitliche Meinung in einer Rechtsfrage gefunden haben und auch der EDSA sich europaweit auf eine gleiche Sicht der Dinge verständigen konnte, ist es nicht ausgeschlossen, dass ein Gericht erster oder zweiter Instanz eine andere Rechtsauffassung vertritt und die zuständige Aufsichtsbehörde an diese gebunden ist (s. Ziff. 6). Dies erschwert es sehr, zu einer einheitlichen Anwendung der Datenschutz-Grundverordnung in der Europäischen Union zu gelangen. Bis das Bundesverwaltungsgericht für Deutschland oder der Europäische Gerichtshof für die Europäische Union zu einer vereinheitlichenden Sichtweise beitragen, können Jahre vergehen – und dann doch die oben dargestellten offenen Fragen hinterlassen.

Kooperation in Deutschland

Eine weitere wichtige Rahmenbedingung für die Wahrnehmung der Aufsichtsaufgabe besteht in der zunehmenden Notwendigkeit, die Aufsichtstätigkeit in Deutschland zu koordinieren. Die Hessische Aufsichtsbehörde ist Teil der deutschen Datenschutzaufsichtsstruktur. Diese Koordination ist zum einen notwendig, weil innerhalb der Union nur in Deutschland die Datenschutzaufsicht föderalistisch organisiert ist und Deutschland im EDSA nur eine Stimme hat. Die deutschen Aufsichtsbehörden müssen sich daher für die Willensbildung im EDSA auf jeweils eine Meinung verständigen. Zum anderen ist eine Verständigung innerhalb Deutschlands in den Fragen notwendig, in denen es Sachverhalte betrifft, die nicht nur Bedeutung für ein Bundesland haben. Dies ist im nicht öffentlichen Bereich der Datenverarbeitung der Fall und in vielen Bereichen der Bund-Länder-Kooperation oder in der länderübergreifenden Zusammenarbeit. In den meisten Datenschutzfragen ist daher ein bundeseinheitlicher Vollzug von Datenschutzrecht gefragt. Für diesen arbeiten die Aufsichtsbehörden des Bundes und der Länder im Rahmen der DSK zunehmend enger zusammen. Das erfordert immer mehr Abstimmungen im Rahmen der Konferenz, in den fachlichen Arbeitskreisen der Konferenz und in einer steigenden Anzahl von Task Forces zu zeitlich befristeten gemeinsamen Aufgaben. Drittens müssen die Aufsichtsbehörden gemeinsame Konzepte und Strategien entwickeln, um sich gegenüber starken Datenverarbeitern durchsetzen zu können. Nur wenn sie gemeinsam auftreten und ihre Positionen gemeinsam durchfechten, haben sie Chancen, den Datenschutz in Deutschland voranzubringen. Die wichtigsten Entscheidungen fallen daher in den Gremien der DSK. Dementsprechend steigt im Rahmen der Aufsichtstätigkeit die Bedeutung der Mitarbeit in diesen Gremien und verändert damit zunehmend die Arbeitsaufgaben der Beschäftigten in der Aufsichtsbehörde.

Angesichts der Notwendigkeit zunehmender Kooperation hat die DSK einen Arbeitskreis „DSK 2.0“ gegründet, der die derzeitige Zusammenarbeit der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder einschließlich der Arbeitsweise der DSK evaluieren und gegebenenfalls Vorschläge für eine Neugestaltung erarbeiten sollte. Neben ihren halbjährlichen zweitägigen Konferenzen führt die DSK inzwischen zusätzlich circa vier eintägige Zwischenkonferenzen durch. Außerdem hat sie einen wöchentlichen Jour fixe eingerichtet, um sich auch in alltäglichen Fragen gegenseitig zu informieren und sich abzustimmen.

Corona-Pandemie

Auch äußere Einflüsse prägten die Aufsichtstätigkeit im Berichtszeitraum – allen voran die Corona-Pandemie. Zum einen zwang sie zur Aufrechterhaltung der Arbeitsfähigkeit der Aufsichtsbehörde zu einer Aufsichtstätigkeit im Pandemiemodus. Die Beschäftigten arbeiteten überwiegend im Home-Office und in der Dienststelle herrschten strenge Hygienebedingungen. Sie konnten erheblich weniger externe Aufsichtstätigkeiten vor Ort wahrnehmen, waren stärker auf Telefonkontakte und Videokonferenzen angewiesen und nutzten vermehrt schriftliche Verfahren. Zum anderen erzeugten die Pandemie, die Maßnahmen zu ihrer Bekämpfung und die sich immer wieder schnell ändernden Rechtsregelungen für immer neue Aufsichtsaufgaben. Beispiele waren die Datenverarbeitungen bei der Organisation von Impfterminen, im Rahmen von Testverfahren, bei der Kontaktnachverfolgung, bei der Aufrechterhaltung der Funktionen von Kindertagesstätten, Schulen und Hochschulen und der Verarbeitung von Daten des Krankheits- und Immunitätsstatus in Arbeitsverhältnissen (s. Ziff. 2).

Schließlich stand die Aufsichtsbehörde im Berichtszeitraum vor der Aufgabe, die Ausnahmen von datenschutzrechtlichen Vorgaben und die befristeten Duldungen nicht datenschutzgerechter Zustände, die sie zu Beginn der Corona-Pandemie und während des ersten Lockdowns im Frühjahr 2020 zur Bewältigung der damaligen Notsituation akzeptiert hatte, wieder an die datenschutzrechtlichen Anforderungen anzupassen. Hierzu hat sie – beispielsweise bei der Nutzung von Videokonferenzsystemen – zusammen mit den Verantwortlichen nach konstruktiven Korrekturen gesucht und die für die Umstellung notwendige Zeit eingeräumt (s. Ziff. 4).

Aufsichtstätigkeit in einzelnen Bereichen

Das wichtigste Ergebnis der Aufsichtstätigkeit im Jahr 2021 ist, dass für den Datenschutz in Hessen keine schwerwiegenden Verstöße festzustellen waren – ganz im Gegensatz zur Entwicklung in Deutschland oder in der Welt. Dort sind technische, wirtschaftliche und politische Entwicklungen zu beobachten, die die Persönlichkeitsrechte betroffener Personen zunehmend gefährden. Für Hessen ist dagegen festzuhalten, dass Datenschutz im Berichtszeitraum akzeptiert und nicht grundsätzlich in Frage gestellt wurde.

Dennoch sind in vielen Bereichen die Anforderungen der Datenschutz-Grundverordnung noch immer nicht ausreichend umgesetzt, führen zu Beschwerden, erfordern das Eingreifen der Datenschutzaufsicht sowie Anordnungen und Durchsetzungsmaßnahmen im Einzelfall. Die Digitalisierung vieler Aufgaben und Tätigkeiten verursacht für die Verantwortlichen zusätzliche Pflichten, bringt zusätzliche Anforderungen mit sich und erfordert zusätzliche Aufmerksamkeit.

Damit kommen große Unternehmen und Verwaltungen einigermaßen zurecht. Dies kann kleine und mittlere Unternehmen oder Gemeinden aber leicht überfordern. Das Einfordern der Datenschutzpflichten darf aber im Ergebnis nicht zu einer Reduzierung des Datenschutzes führen. Daher bemüht sich meine Behörde immer wieder zusammen mit den Verantwortlichen darum, datenschutzgerechte Lösungen zu finden, die auch Datenschutz in kleinen und mittleren Unternehmen sowie in kleinen Gemeinden gewährleisten.

Zwischen den Entwicklungen der Datenverarbeitung im Bereich der Sicherheits- und Strafverfolgungsbehörden sowie des Verfassungsschutzes und den Anforderungen des Datenschutzes besteht wegen der kontroversen Aufgaben immer ein Spannungsverhältnis, das aber im Berichtszeitraum nur in Einzelfällen zu Forderungen der Datenschutzaufsicht geführt hat, denen die betroffenen Behörden nachgekommen sind (s. Ziff. 7).

In den Verwaltungsbehörden des Landes und der Kommunen werden derzeit große und anspruchsvolle Digitalisierungsprojekte konzipiert, geplant und umgesetzt. Diese sind für eine Verwaltung in einer digitalisierten Welt unverzichtbar, begründen aber an vielen Stellen Herausforderungen für die Wahrung von Persönlichkeitsrechten und Selbstbestimmung der Bürgerinnen und Bürger. Daher ist es erforderlich, dass sich die Datenschutzaufsicht an diesen Digitalisierungsprojekten beteiligt und mit konstruktiven Hinweisen für die Einhaltung der datenschutzrechtlichen Anforderungen beiträgt (s. Ziff. 8).

Die Schulen und Hochschulen waren im Berichtszeitraum vor allem geprägt durch starke Entwicklungen zu mehr Digitalisierung von Unterricht und Prüfungen, Lehre und Lernen. Neben dem Einsatz von Videokonferenzsystemen (s. Ziff. 4) betraf dies z. B. Geräteausleihen, Lernhilfen und Fernprüfungen, für die aufsichtliche Hinweise erforderlich, aber auch willkommen waren. Im Schulbereich begleitete die Aufsichtsbehörde die Entwicklungen des Hessischen Schulportals und beriet das Kultusministerium hinsichtlich der datenschutzrechtlichen Vorschriften des neuen Schulgesetzes (Ziff. 9).

Die Digitalisierung der Arbeit führt dazu, dass in Beschäftigtenverhältnissen immer intensiver die Leistung und das Verhalten der Beschäftigten überwacht werden kann. Hier kommt es darauf an, dass diese Möglichkeiten nur in verhältnismäßigem Umfang und unter Wahrung der Persönlichkeitsrechte der betroffenen Beschäftigten genutzt werden. In dieser Hinsicht musste meine Behörde in mehreren Fällen korrigierend eingreifen (s. Ziff. 11).

Im Internet ist der Einsatz von Cookies vielfach notwendig, um Nutzende wiederzuerkennen und ihnen die gewünschten Leistungen zu bieten. Noch öfter aber werden sie genutzt, um das Surfverhalten der Nutzenden zu tracken, über sie Profile zu erstellen und ihre Interessen, Präferenzen, Gewohnheiten, Verhaltensweisen und Beziehungen zu erkennen und – insbesondere

für Werbemaßnahmen – zu beeinflussen. Um die Selbstbestimmung der Nutzenden zu wahren, ist dies weitgehend nur zulässig, wenn sie in die Verwendung von Cookies eingewilligt haben. Zu diesem Zweck versucht fast jeder Internet-Anbieter in Form von „Cookie-Bannern“ eine solche Einwilligung einzuholen. Durch die ständige Konfrontation mit solchen „Cookie-Bannern“ wirkt eine an sich sinnvolle Maßnahme zum Schutz der Selbstbestimmung im Alltag nur nervig. Hierzu hat jetzt das Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG) zum 1. Dezember 2021 neue Regelungen geschaffen (s. Ziff. 12).

Ein „Dauerbrenner“ der Datenschutzaufsicht bleibt das Thema Videoüberwachung. Durch die Fortschritte der Videotechnik und ein zunehmendes Vorsorge- und Schutzbedürfnis nimmt die Videoüberwachung durch Polizei und Gefahrenabwehrbehörden, aber noch mehr durch private Unternehmen und im Nachbarschaftsverhältnis zu. Dies zwingt die Datenschutzaufsicht immer wieder zu Hinweisen und Korrekturanordnungen, die von Behörden angenommen werden, gegenüber privaten Stellen bisweilen aber durchgesetzt werden müssen (s. Ziff. 13).

Im Bereich der privaten Wirtschaft gab es viele Beschwerden, die sich z. B. mit Fragen der Rechte betroffener Personen, insbesondere mit dem Auskunftsanspruch (s. Ziff. 14), der Verarbeitung von Anschriftendaten durch Auskunfteien und Inkassounternehmen (s. Ziff. 15) und der Abfragen von Fahrzeughalterdaten zur Durchsetzung von Vertragsstrafen beschäftigten (s. Ziff. 16), denen die Beschäftigten meiner Behörden nachgehen mussten.

Im Gesundheitswesen war die Datenschutzaufsicht stark durch die Datenverarbeitung im Kontext der Corona-Pandemie belastet (s. Ziff. 2). Aber auch Probleme etwa zur Wahrung des Patientengeheimnisses, der Übermittlung von Patientendaten und der Aufbewahrung von Patientenakten mussten gelöst werden. (s. Ziff. 17).

Besonders hinzuweisen ist auf die Zunahme von Cyberkriminalität, die auch Auswirkungen auf den Datenschutz hat. Kriminelle verschaffen sich gezielt über Phishing und andere Formen des Social Engineering Zugang zu den IT-Systemen von Verantwortlichen. In anderen Fällen nutzen sie bekannt gewordene Schwachstellen in bestimmten Softwaresystemen und dringen durch diese in IT-Systeme ein. Ihre Schadsoftware verbreitet sich in allen Teilen der Systeme und ziehen – mitunter sehr große Mengen an – Daten ab. Um die Verantwortlichen zu erpressen, laden sie Verschlüsselungssoftware nach, verschlüsseln (alle) Daten und bieten die Schlüssel zum Entschlüsseln gegen hohe Geldsummen an. In anderen Fällen veröffentlichen sie beim Verantwortlichen abgezogene Daten im Darknet und drohen mit weiteren Veröffentlichungen, wenn kein Lösegeld bezahlt wird. Diese zunehmenden

Formen von Cyberkriminalität erfordern stärkere Vorsorgemaßnahmen, schnelle Reaktionen auf bekanntgewordene Schwachstellen und die wiederholte Aufklärung aller Beschäftigten über die Angriffsmöglichkeiten sowie die Maßnahmen, ihnen zu entgehen (s. Ziff. 18).

2. Datenschutz während der Corona-Pandemie

Auch im Berichtszeitraum war die Datenschutzaufsicht stark von den Bedingungen der Corona-Pandemie geprägt. Zum einen brachte die zur Bekämpfung der Pandemie notwendige Verarbeitung personenbezogener Daten viele neue Herausforderungen für den Datenschutz. Diese waren sowohl von immer wieder neuen, der jeweiligen Pandemie-Situation angepassten Regelungen als auch von vielen Reaktionen der Adressaten dieser Regelungen geprägt, die zu immer neuen Formen und Inhalten der Datenverarbeitung führten. Zum anderen war die Arbeit meiner Behörde auch dadurch erschwert, dass ihre Mitarbeiterinnen und Mitarbeiter ihre Aufsichtstätigkeit überwiegend vom Home-Office aus erbringen mussten.

2.1
War Datenschutz ein Hindernis in der Pandemiebekämpfung?

Trotz gegenteiliger Behauptungen war der Datenschutz im Berichtszeitraum kein Hindernis für die Bekämpfung der Corona-Pandemie, sondern eine wirksame Unterstützung, weil er für das Vertrauen in die staatliche Corona-Politik und die einzelnen Maßnahmen staatlicher Stellen eine wichtige Voraussetzung war.

In vielen Leitartikeln, Talkshows und Politikerreden, Online-Beiträgen und Leser-Kommentaren wird behauptet, Datenschutz habe die effektive Bekämpfung der Pandemie behindert. Daher müsse der Datenschutz zurückgestutzt werden. Diese Meinung wird sogar in wissenschaftlichen Kreisen vertreten. Selbst im Ethikrat der Bundesregierung sind diese Behauptungen zu finden. Seine Vorsitzende, Frau Prof. Dr. Alena Buyx, lässt verlauten, der Datenschutz sei das einzige Grundrecht, das in der Pandemie nicht habe zurückstecken müssen. Mit weniger Datenschutz wären in der Pandemiebekämpfung bessere Ergebnisse zu erzielen gewesen (https://www.zdf.de/nachrichten/digitales/coronavirus-warnapp-datenschutz--kritik-100.html). Der frühere Kulturstaatsminister und jetzige stellvertretende Vorsitzende des Ethikrates Prof. Dr. Julian Nida-Rümelin hat diese Vorstellung mit der Behauptung auf die Spitze getrieben: Deutschland habe den scharfen Datenschutz in der Corona Krise mit 70.000 Todesfällen bezahlt. Aus dieser Behauptung leitet er die politische Forderung ab, den Datenschutz stärker einzuschränken (Zeit-Online 26.03.2021).

Diese Behauptungen erschweren den Datenschutz, halten aber keinem Faktencheck stand. Vielmehr ist das Gegenteil richtig: Datenschutz hat sich gegenüber den Anforderungen der Pandemiebekämpfung sehr flexibel gezeigt

und ist sogar eine wichtige Voraussetzung dafür, dass die Bekämpfung des Corona-Virus gelingt.

Das Datenschutzrecht zeigt sich gegenüber Gesundheitsgefahren sehr flexibel und erlaubt ausdrücklich die Datenverarbeitung zur Pandemiebekämpfung. Die dafür erforderliche Datenverarbeitung ist nach Art. 6 Abs. 1 UAbs. 1 lit. d DS-GVO ausdrücklich zulässig, wenn sie erforderlich ist, um „lebenswichtige Interessen“ zu schützen. Als ein Beispiel für ein solches Interesse nennt die DS-GVO in Erwägungsgrund 46 ausdrücklich die „Überwachung von Epidemien“. Das Datenschutzrecht lässt also alle Datenverarbeitungen zu, die zur Pandemiebekämpfung erforderlich sind. Wenn Impfen, Testen und Kontaktverfolgen nicht wie gewünscht funktioniert haben, ist dies also nicht die Schuld des Datenschutzrechts.

Datenschutz hat weder Todesfälle verursacht, noch ist er in der Corona-Krise als einziges Grundrecht ohne Einschränkung geblieben. Vielmehr haben die Datenschutzaufsichtsbehörden in dieser Sondersituation große Flexibilität gezeigt, um Leben zu retten. Datenschutz steht daher der Bewältigung der Corona-Krise nicht entgegen. Vielmehr unterstützt er sie: In einer westlichen Demokratie wie in Deutschland kann Pandemiebekämpfung nur erfolgreich sein, wenn die Bürgerinnen und Bürger den Institutionen des Staates vertrauen. Ein zentraler Vertrauensfaktor ist der Datenschutz. Nur wenn sie erfahren, dass ihre Grundrechte, zu denen der Datenschutz gehört, in guten Händen sind und auch bei einschneidenden Maßnahmen gewahrt werden, können sie das notwendige Vertrauen entwickeln.

Wie war das Verhältnis von Datenschutz und Pandemiebekämpfung im Berichtszeitraum tatsächlich? Im ersten Lockdown im Frühjahr 2020 haben viele Verantwortliche nach den nächstbesten digitalen Möglichkeiten gegriffen, um trotz Abstandsgebots das soziale und berufliche Leben aufrechtzuerhalten. Datenschutz stand da nicht im Vordergrund. Die Datenschutzaufsichtsbehörden konnten viele der angewendeten Videokonferenzsysteme nicht gutheißen, haben sie aber bis heute geduldet oder nicht beanstandet, etwa um die Unterrichtung der Kinder in den Schulen, das Angebot von Lehrveranstaltungen in den Hochschulen, die Durchführung von Besprechungen in Unternehmen und Behörden sowie das Angebot von Veranstaltungen im Kulturbetrieb auch in der Pandemie weiter zu ermöglichen (s. Ziff. 4).

Ähnlich war der Umgang mit der meist überstürzten Verlagerung der Arbeit ins Home-Office und der Ermöglichung von mobilem Arbeiten. In vielen Fällen entsprachen weder die Bedingungen zu Hause den Anforderungen an den sicheren Umgang mit personenbezogenen Daten, noch wurden die technisch-organisatorischen Verfahren zu Anbindungen der Home-Offices an die Datenverarbeitungssysteme der Unternehmen und Behörden den

Anforderungen des Stands der Technik gerecht. Von krassen Ausnahmen der Überwachung der Beschäftigten abgesehen (s. Ziff. 10.2), wurden diese Umstände zumindest in der ersten Zeit nicht moniert.

Ein weiteres Beispiel für eine Einschränkung des Datenschutzes ist der Zwang, z. B. in Restaurants, Geschäften und Veranstaltungen seine Kontaktdaten hinterlegen zu müssen. Dieser tiefe Eingriff in die informationelle Selbstbestimmung, dass alle Bürgerinnen und Bürger eine staatliche Verfolgung der Aufenthalte und Besuche in diesen Stellen und das Treffen mit anderen Menschen dulden müssen, ist für die Kontaktnachverfolgung durch die Gesundheitsämter notwendig und wurde vom Datenschutz konstruktiv begleitet (s. Ziff. 2.2 und 2.3). Das Gleiche gilt für die Apps, die zur Kontaktnachverfolgung anstelle von Papierlisten genutzt wurden. Auch deren Risiken für das Grundrecht wurden von den Datenschutzaufsichtsbehörden akzeptiert. Dieser Digitalisierungsschritt wurde trotz vieler Mängel vom Datenschutz unterstützt und permanent verbessert (s. Ziff. 2.2). Auch die Datenverarbeitung im Impftermin-Management hat die Datenschutzaufsicht trotz Defiziten nicht blockiert.

Ein weiteres Beispiel für das Zurückstecken des Datenschutzes gegenüber den Notwendigkeiten der Pandemiebekämpfung war die Datenverarbeitung zum Schutz der Arbeitsstätten. Die Erfassung der zur Überwachung der 3G-Regel am Arbeitsplatz erforderlichen Immunitätsdaten von Beschäftigen durch ihre Arbeitgeber oder Dienstherren war ein tiefer Eingriff in den Beschäftigtendatenschutz (s. Ziff. 2.6). Dennoch haben die Aufsichtsbehörden die Entstehung dieser Regelungen und ihre Praktizierung am Arbeitsplatz konstruktiv begleitet.

In Coronavirus-Schutzverordnungen der Länder wurden die Rechte der betroffenen Personen vollständig ausgesetzt, um die Anwendung der Kontaktnachverfolgung nicht zu behindern. Die betroffenen Personen konnten dadurch z. B. keine Auskunft über die Verarbeitung ihrer Daten verlangen, keine Berichtigung falscher Daten durchsetzen und keine Löschung nicht mehr erforderlicher Daten verlangen. Erst als ich in Hessen konstruktiv darauf hingewiesen habe, dass diese Einschränkung für die Kontaktnachverfolgung überflüssig ist, wurde sie in der nächsten Fassung der Coronavirus-Schutzverordnungen aufgehoben (s. Ziff. 2.5).

Die Zielsetzung der Corona-Warn-App entstammt nicht dem Datenschutz, sondern dem Wunsch der Gesundheitspolitik, neben den bestehenden Mitteln der Gesundheitsämter ein zusätzliches anonymes Instrument zu etablieren, Infektionen zu bekämpfen. Datenschutzüberlegungen kamen erst danach ins Spiel, als es darum ging, wie dies zu realisieren sei. Frankreich, Australien und Norwegen haben eine Lösung gewählt, die Daten der Infizierten zentral

speichert – mit dem Ergebnis, dass diese Versuche am mangelnden Vertrauen der potenziellen Nutzenden gescheitert sind. Frankreich hat inzwischen seine App überholt und nutzt sie wie die deutsche App. In Deutschland hat der dezentrale Ansatz, der die Identifikationsdaten des Infizierten nicht preisgibt, Vertrauen erzeugt. Er hat zumindest bis zum Ende des Berichtszeitraums dazu geführt, dass etwa 40 Millionen Menschen die App nutzen und über 1.7 Millionen Infizierte ca. 10 Millionen Kontaktpersonen gewarnt und damit Millionen weitere Infektionen verhindert haben (https://www.bundesregierung.de/breg-de/suche/cwa-40-mio-downloads-1994916).

Die Datenschutzaufsichtsbehörden haben auch die weitere Ausweitung der Funktionen der App unterstützt.

Die Erfahrung mit dem Datenschutz in der Pandemie zeigt also: Ein Zurückschrauben des Datenschutzrechts ist nicht notwendig. Im Gegenteil – die Einschränkung des Grundrechts auf Datenschutz wäre kontraproduktiv. In der Krise hat der Datenschutz Flexibilität und Schutzwirkung gleichzeitig erwiesen. Er ist die Grundlage für das Vertrauen der Betroffenen und die Voraussetzung, sie zum Mitmachen zu motivieren.

Nachdem sich im Berichtszeitraum, dem zweiten Jahr der Pandemie, Routine in der Bekämpfung des Corona-Virus eingestellt hatte und die ersten spontanen Reaktionen und Behelfsmaßnahmen im Umgang mit den neuen Herausforderungen überdacht werden konnten, war es erforderlich, die gefundenen Lösungen den datenschutzrechtlichen Vorgaben anzupassen und wieder rechtmäßige Zustände herzustellen. Auch der Datenschutz hatte lange genug unter der Corona-Pandemie gelitten.

2.2
Datenschutzrechtliche Vorgaben zur Kontaktnachverfolgung

Bereits im Laufe des vorangegangen Berichtzeitraumes (siehe 49. Tätigkeitsbericht, Ziff. 11.6) war die coronabedingte Kontaktdatenerfassung ein Schwerpunkt meiner Tätigkeit. Die Datenschutzfragen im Berichtszeitraum zu bearbeiten, war besonders schwierig, weil die Regelungen für die Kontaktnachverfolgung immer wieder dem Pandemiegeschehen angepasst wurden. Auch aus diesem Grund erreichten mich diverse Anfragen und Beschwerden zum Themenbereich Kontaktnachverfolgung.

I. Häufige Änderung der Rechtsgrundlagen

Die Regelungen zur Kontaktdatenerfassung waren im Laufe des Jahres häufigen – oftmals nur kurzfristig geltenden – Änderungen unterworfen. Die

Anwendung in der Praxis war daher insbesondere für die Verpflichteten eine besondere Herausforderung.

Nachdem nicht der Grundversorgung der Bevölkerung dienende Bereiche des Wirtschaftslebens in den Wintermonaten coronabedingt stillgelegt waren, durften ab dem 1. März 2021 zunächst Friseurbetriebe wieder öffnen. Neben der Einhaltung diverser Hygienemaßnahmen waren die Betreiber und Betreiberinnen gemäß § 6 Abs. 3 der Corona-Kontakt- und Betriebsbeschränkungsverordnung (CoKoBeV, Gültigkeit ab 1.März 2021, GVBl. S. 142) verpflichtet, die Kontaktdaten der Kunden und Kundinnen zu erfassen.

Ab dem 8. März 2021 durften zudem Verkaufsstellen des Einzelhandels im Rahmen einer festen Terminvergabe und unter Einhaltung verschiedener Hygieneregeln öffnen („Click and Meet“). Auch hier mussten nach § 3a Abs. 1 S. 2 Nr. 22 CoKoBeV (Gültigkeit ab 8. März 2021, GVBl. S. 142) die Kontaktdaten der Kundinnen und Kunden erfasst werden. Die Regelung entsprach derjenigen für die Friseurbetriebe. Davon ausgenommen waren lediglich die der Grundversorgung der Bevölkerung dienenden Verkaufsstellen nach § 3a Abs. 1 S. 2 Nr. 1-21 CoKoBeV (Lebensmitteleinzelhandel, Apotheken, Drogerien etc.). Bei Mischwarenläden war nach § 3a Abs. 1 S. 3 CoKoBeV der Schwerpunkt im Sortiment entscheidend.

Ab dem 26. April 2021 war die einschlägige Rechtsgrundlage bei den Geschäften des Einzelhandels von der Höhe der Inzidenz abhängig. Die hessischen Regelungen der CoKoBeV galten nur noch bis zu einer Inzidenz von 100 Infizierten auf 100.000 Einwohner. Sofern ein Landkreis oder eine kreisfreie Stadt an drei aufeinander folgenden Tagen eine Inzidenz von 100 überschritten hatte, galten dort nach § 28b IfSG ab dem übernächsten Tag die bundeseinheitlichen Regelungen des Infektionsschutzgesetzes (IfSG, BGBl. I S. 802).

Die hessische Regelung zu der Erfassung der Kontaktdaten im Einzelhandel wurde sodann am 17. Mai 2021 aufgehoben (CoKoBeV, Gültigkeit ab 17. Mai 2021, GVBl. S. 254). Eine Kontaktdatenerfassung im Einzelhandel war nunmehr nur noch ab einer Inzidenz von 100 nach dem Infektionsschutzgesetz geregelt. Bei einer Inzidenz bis 150 durften nach § 28b Abs. 1 S. 1 Nr. 4 IfSG sämtliche Ladengeschäfte für einzelne Kunden nach vorheriger Terminbuchung für einen fest begrenzten Zeitraum öffnen, sofern die Kontaktdaten der Kundinnen und Kunden erhoben wurden.

Ebenfalls ab dem 17. Mai 2021 durften Gaststätten, Cafés o. Ä. wieder einen Vor-Ort-Verzehr (zunächst nur für die Außengastronomie) anbieten. Dabei mussten u. a. auch die Kontaktdaten der Gäste erfasst werden. Die Regelung des § 4 Abs. 1 S. 3 Nr. 3 CoKoBeV entsprach weitgehend derjenigen für Friseurbetriebe und den Einzelhandel.

Die Kontaktdatenerfassung wurde ab dem 25. Juni 2021 im Zuge der Aufhebung der CoKoBeV und des Erlasses der Verordnung zum Schutz der Bevölkerung vor Infektionen mit dem Corona-Virus SARS-CoV 2 (Coronavirus-Schutzverordnung – CoSchuV – Gültigkeit ab 25. Juni 2021, GVBl. S. 282) neu geregelt. Während die Kontaktdatenerfassung bislang in der jeweiligen Norm für die entsprechende Branche geregelt war, wurde diese nunmehr „vor die Klammer“ gezogen und in § 4 CoSchuV im Ersten Teil (Allgemeine Vorschriften) geregelt. Im Zweiten Teil (Besondere Vorschriften) wurde für einzelne Bereiche (Gaststätten, Kulturbetrieb etc.) auf die Kontaktdatenerfassung nach § 4 CoSchuV verwiesen. § 4 CoSchuV selbst verwies wiederum auf die Bundesregelung des § 28a Abs. 4 IfSG (BGBl. I S. 370) und ergänzte diese um einige Maßgaben.

Die CoSchuV verpflichtete ab dem 25. Juni 2021 zunächst diverse Betreiberinnen und Betreiber sowie Veranstalterinnen und Veranstalter zur Kontaktdatenerfassung:

– Fachmessen und Kulturangebote (Theater, Opern, Kinos und Konzerte) nach § 16 CoSchuV,
– Fitnessstudios und ähnliche Einrichtungen nach § 18 Abs. 2 CoSchuV, Spielbanken, Spielhallen und ähnliche Einrichtungen nach § 18 Abs. 4 CoSchuV, Gaststätten, Mensen,
– Hotels, Eisdielen, Eiscafés und andere Gewerbe bei dem Angebot des Verzehrs vor Ort nach § 22 CoSchuV,
– Übernachtungsbetriebe nach § 23 CoSchuV,
– Tanzlokale, Diskotheken, Clubs und ähnliche Einrichtungen nach § 24 CoSchuV,
– Dienstleistungsbetriebe im Bereich der Körperpflege (Friseurbetriebe und ähnliche) nach § 25 CoSchuV sowie Prostitutionsstätten und ähnliche Einrichtungen nach § 26 CoSchuV.

Nachdem die Informationspflicht des Art. 13 DS-GVO sowie die Betroffenenrechte der Art. 15, 18 und 20 DS-GVO gemäß § 4 Nr. 3 CoSchuV (bzw. nach der jeweiligen Regelung der CoKoBeV) seit Beginn der Corona-Pandemie ausgeschlossen waren, wurde dieser Ausschluss auf meine Intervention ab dem 19. August 2021 (CoSchuV, GVBl. S. 386) gestrichen (s. Ziff. 2.5). Seitdem sind die Betroffenenrechte im Rahmen der Kontaktdatenerfassung ohne Einschränkung anwendbar.

Seit dem 16. September 2021 (CoSchuV, GVBl. S. 571) waren große Teile der vormals Verpflichteten von der Kontaktdatenerfassung ausgenommen (insbesondere Gaststätten, Friseurbetriebe, Fitnessstudios und Kulturbetriebe). Verpflichtet blieben jedoch insbesondere Tanzlokale, Diskotheken, Clubs und

ähnliche Einrichtungen nach § 24 CoSchuV sowie Prostitutionsstätten und ähnliche Einrichtungen nach § 26 CoSchuV. Gemäß § 27 Abs. 2 CoSchuV wurde zudem den örtlich zuständigen Behörden die Befugnis eingeräumt, nach den §§ 28 und 28a IfSG auch über die CoSchuV hinausgehende Maßnahmen anzuordnen. Somit konnte seitdem auf kommunaler Ebene auch eine Kontaktdatenerfassung für weitere Einrichtungen (Gaststätten, Friseurbetriebe etc.) angeordnet werden.

Die CoSchuV wurde zum 25. November 2021 (GVBl. S. 742) neu erlassen. Die Regelungen zu der Kontaktdatenerfassung erfuhren lediglich redaktionelle Änderungen, inhaltlich blieben sie jedoch unverändert.

Zum 16. Dezember 2021 wurde § 4 CoSchuV um einen Satz 2 ergänzt. Danach war die Kontaktdatenerfassung nicht erforderlich, wenn die Person, deren Daten zu erfassen wären, die in der Corona-Warn-App des Robert Koch-Institutes enthaltene QR-Code-Registrierung nutzt.

Zum Ende des Berichtszeitraums galt folgende Rechtslage: Die Erfassung der Kontaktdaten stützt sich auf Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO i. V. m. § 4 CoSchuV und der jeweiligen Vorschrift der CoSchuV (z. B. § 24 CoSchuV für Diskotheken).

Aktuelle Hinweise zu den jeweils aktuellen Regelungen der Kontaktdatenerfassung habe ich stets auf meiner Webseite bereitgestellt.

II. Anforderungen an die Kontaktdatenerfassung

Sofern die entsprechende Norm der CoSchuV keine Kontaktdatenerfassung für den jeweiligen Betrieb oder die Veranstaltung (mehr) vorsah, durften keine Kontaktdaten erhoben werden. Aufgrund der mehrfachen Änderung der Verordnung im Laufe des Berichtszeitraumes und der damit einhergehenden Rechtsunsicherheit wurde diese Maßgabe nicht durchweg eingehalten (s. Ziff. 2.3).

Als Kontaktdaten waren Name, Vorname, Anschrift und die Telefonnummer oder E-Mail-Adresse zu erfassen. Andere Daten (etwa eine Unterschrift) durften nicht erhoben werden. Mitunter wurde die Unterzeichnung von Einwilligungserklärungen o. Ä. verlangt. Da die Kontaktdatenerfassung jedoch gesetzlich normiert ist, waren solche „Einwilligungen“ nicht einzuholen. Auch ist die Anfertigung von Kopien der Personalausweise oder der Negativnachweise (Impfnachweis, Genesenennachweis oder Testnachweis, vgl. § 3 CoSchuV) unzulässig. Diese enthalten deutlich mehr personenbezogene Daten (bei Negativnachweisen zudem Gesundheitsdaten im Sinn des Art. 9 DS-GVO) als gesetzlich erhoben werden durften (s. Ziff. 2.3). Die Kontaktdaten waren gemäß § 4 S. 1 Nr. 1 CoSchuV vollständig und wahrheitsgemäß anzugeben.

Offenkundig falsche Angaben (Pseudonyme, „Spaßnamen“) erfüllten nicht die Anforderungen der CoSchuV.

Im Berichtszeitraum kam es immer wieder vor, dass Kontaktdaten zu anderen Zwecken verwendet worden sind (etwa Werbung oder anderweitige Kommunikation mit den Erfassten). Da die Kontaktdaten nach § 28a Abs. 4 S. 3 IfSG nicht zu einem anderen Zweck verwendet werden dürfen, als sie auf Anforderung an die für die Erhebung der Daten zuständigen Stellen auszuhändigen, ist eine solche Verwendung jedoch rechtswidrig.

Die fehlende Erfassung der Kontaktdaten sowie unwahre oder unvollständige Angaben stellen nach § 30 CoSchuV i. V. m. § 73 Abs. 1a Nr. 24 IfSG eine Ordnungswidrigkeit dar, die nach § 73 Abs. 2 IfSG mit einer Geldbuße bis zu 25.000 Euro geahndet werden kann.

Die Erhebung und Verarbeitung der Kontaktdaten sollte gemäß § 4 S. 1 Nr. 2 CoSchuV möglichst in elektronischer Form erfolgen (etwa mittels eines QR-Codes oder einer App). Neben der elektronischen Form ist jedoch auch eine andere Art der Erfassung anzubieten. Sofern die Kontaktdaten papierhaft erfasst wurden, war darauf zu achten, dass die Kontaktdaten nicht öffentlich zugänglich und für andere Personen einsehbar sein durften. Die Kontaktdaten waren händisch vom Personal zu erfassen oder von den Gästen, Kundinnen, Kunden, Teilnehmerinnen oder Teilnehmern auf einzelnen Blättern einzutragen. Wegen Verstößen gegen diese Verpflichtungen kam es auch im Berichtszeitraum immer wieder zu Beschwerden (s. Ziff. 2.3).

Die Verantwortlichen hatten bereits bei der Erhebung der Kontaktdaten insbesondere darüber zu informieren (etwa mittels eines gut sichtbaren Hinweises vor Ort sowie auf den Erfassungsbögen), dass die Kontaktdatenerfassung zum Zweck der Nachverfolgung und Unterbrechung von Infektionsketten mit dem Corona-Virus SARS-CoV-2 auf Grundlage von Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO i. V. m. § 4 CoSchuV und der jeweiligen Vorschrift der CoSchuV (z. B. § 24 CoSchuV für Diskotheken) erfolgt.

Die Verantwortlichen hatten nach § 28a Abs. 4 S. 2 IfSG sicherzustellen, dass eine Kenntnisnahme der erfassten Daten durch Unbefugte ausgeschlossen ist. Diese Maßgabe wurde in einigen mir zur Kenntnis gelangten Fällen nicht durchweg eingehalten (s. Ziff. 2.3). Die Verantwortlichen sollten die erfassten Daten in einem verschlossenen Schrank, Tresor oder Ähnlichem möglichst an dem Ort der Erfassung aufbewahren. Zu diesem sollten möglichst wenige Personen Zugang haben. Das bloße Abheften der Erfassungsbögen in einem (Akten-)Ordner genügte nicht, sofern dieser nicht sicher verwahrt wurde.

Die Kontaktdaten waren nach § 28 Abs. 1 CoSchuV sowie § 28a Abs. 4 S. 4 und 5 IfSG auf Anforderung nur den Gesundheitsämtern (in Eilfällen den

örtlichen Ordnungsbehörden) herauszugeben. Sie durften an keine anderen Stellen übermittelt werden – auch nicht an die Polizei oder Staatsanwaltschaft.

Die Kontaktdaten waren gemäß § 28a Abs. 4 S. 3 IfSG unverzüglich nach Ablauf von vier Wochen nach Erhebung sicher und datenschutzkonform zu löschen oder zu vernichten. Auf Papier erfasste Kontaktdaten durften nicht direkt in dem Papiermüll entsorgt, sondern mussten vorher in einem Aktenvernichter oder Papierschredder vernichtet werden, damit dritte Personen keine Kenntnis von diesen erlangen konnten. Auch hinsichtlich dieser Vorgaben erreichten mich mehrere Beschwerden, nach denen Kontaktdaten (deutlich) länger als gesetzlich erlaubt aufbewahrt wurden (s. Ziff. 2.3).

2.3
Verstöße gegen die Regeln der Kontaktnachverfolgung

Einige konkrete Beispiele aus der Praxis des Berichtsjahres zeigen die aufgetretenen datenschutzrechtlichen Probleme der Kontaktnachverfolgung. Mich erreichten viele Beschwerden, die das öffentlich zugängliche Auslegen der zu führenden Kontaktlisten zum Inhalt hatten. Zudem wurde die unsachgemäße Verwahrung sowie unzulässig lange Speicherung der Kontaktdaten gerügt. In diesen Fällen wurden von mir Maßnahmen ergriffen, um die datenschutzrechtlichen Verstöße zu unterbinden.

Am 5. Juli 2021 erreichte mich eine Beschwerde, die sich gegen einen Tretbootverleih richtete. Dieser hatte zur Kontaktdatennachverfolgung die Benutzung der Luca-App vorgesehen. Im Falle der Nichtbenutzung der Luca-App wurden Personalausweiskopien der Kunden angefertigt. Am Kassenhaus war die Verkaufsklappe von links nach rechts durchgehend geöffnet, ebenso stand die Eingangstür weit offen. In der Nähe des Verkaufstresens stand ein handelsüblicher Kopierer. Neben dem Kopierer lagen die Kopien der Personalausweise vorheriger Kunden. Die oberste Kopie zeigte sichtbar die Vorderseite eines Personalausweises. Das Kassenhaus war nicht durchgehend besetzt, so dass die Kopien weder vor unerlaubter Offenlegung noch vor Verlust geschützt waren. Zwar versuchte der Betreiber des Tretbootverleihs und Verantwortliche für die Datenverarbeitung seiner zum damaligen Zeitpunkt gesetzlich vorgeschriebenen Pflicht zur Kontaktdatenerfassung gemäß § 4 CoSchuV (vom 22. Juni 2021) i. V. m. § 28a Abs. 4 IfSG nachzukommen. Fraglich war jedoch, ob im vorliegenden Fall eine gesetzliche Grundlage zur Anfertigung von Ausweiskopien vorlag. Gemäß Art. 6 DS-GVO ist die Verarbeitung nur rechtmäßig, wenn mindestens einer der in Art. 6 Abs. 1 UAbs. 1 lit. a – f DS-GVO aufgezählten Tatbestände erfüllt ist. Die CoSchuV ordnete zur Kontaktdatenerfassung die Erhebung von Name, Adresse und

Telefonnummer oder E-Mail-Adresse an. Demnach ist Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO einschlägig. Die CoSchuV stellt eine rechtliche Verpflichtung dar, die der Verantwortliche erfüllen muss.

Auf dem Personalausweis werden allerdings darüber hinaus neben Körpergröße und Augenfarbe auch der Geburtsort sowie die Personalausweisnummer angegeben. Aufgrund der Vielzahl der auf dem Personalausweis vermerkten personenbezogenen Daten besteht eine hohe Missbrauchsgefahr. Diese personenbezogenen Daten werden von der CoSchuV nicht erfasst. Da auch keiner der sonstigen Tatbestände des Art. 6 DS-GVO einschlägig ist, mangelt es an einer gesetzlichen Grundlage. Mithin ist die Anfertigung von Personalausweiskopien unzulässig.

Selbst wenn eine gesetzliche Grundlage zur Datenverarbeitung bestanden hätte, wäre die Erfassung mittels Personalausweiskopien trotzdem unzulässig gewesen, da diese gegen den Grundsatz der „Datenminimierung“ nach Art. 5 Abs. 1 lit. c DS-GVO verstoßen würde. Hiernach müssen personenbezogene Daten „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“. Dieses zentrale Prinzip der DS-GVO bedeutet eine in der Regel qualitative und quantitative Begrenzung der Verarbeitung personenbezogener Daten. Das Wort „Minimierung“ deutet zudem auf eine möglichst weitgehende Begrenzung hin. Die Anfertigung von Personalausweiskopien stellt keine sparsame Verarbeitung personenbezogener Daten dar und ist grundsätzlich als unzulässig anzusehen. Von diesem Grundsatz gibt es zwar Ausnahmen, wie beispielsweise § 8 Abs. 2 Geldwäschegesetz oder § 95 Abs. 4 Satz 3 Telekommunikationsgesetz a. F. verdeutlichen. Im vorliegenden Fall handelt es sich allerdings um keine solche Ausnahme.

Die offene Verwahrung der Personalausweiskopien stellt zudem einen Verstoß gegen § 28a Abs. 4 S. 2 IfSG dar, nachdem die Verantwortlichen sicherzustellen haben, dass eine Kenntnisnahme der erfassten Daten durch Unbefugte ausgeschlossen ist.

In der Folge wurde der Verantwortliche zuerst von mir angewiesen, die Anfertigung von Personalausweiskopien zu unterlassen. Er wurde sodann über die rechtlichen Rahmenbedingen von mir aufgeklärt. Sollten demnach die Kunden ihre Kontaktdaten nicht in elektronischer Form (etwa mittels eines QR-Codes oder einer App) erfassen lassen wollen, so war auch eine andere Art der Erfassung anzubieten. Die Kontaktdaten konnten etwa handschriftlich vom Personal erfasst werden oder den Gästen, Kunden und Kundinnen oder Teilnehmerinnen und Teilnehmern konnten einzelne Blätter zum Ausfüllen vorgelegt werden. Überdies wurde der Verantwortliche angewiesen, die

Kontaktdaten in einem verschlossenen Schrank, Tresor oder an einer ähnlich sicheren Verwahrungsstelle aufzuheben.

Am 21. Juli 2021 erreichte mich eine Beschwerde, die sich gegen einen Restaurantbetrieb richtete. Die Beschwerde wurde durch den Kreisausschuss eines Landkreises in Hessen erhoben. Die Ordnungsbehörde des dortigen Kreisausschusses führte in Gastronomiebetrieben Kontrollen zur Einhaltung der CoSchuV durch. Bei dem betroffenen Restaurant wurde festgestellt, dass die Kontaktdatenblätter der Gäste seit Oktober/November 2020 weiterhin aufbewahrt wurden und somit entgegen § 4 CoSchuV i. V. m. § 28a Abs. 4 S. 3 IfSG nicht nach einem Monat gelöscht oder ordnungsgemäß entsorgt worden waren. Auf Nachfrage bestätigte der Restaurantbetreiber und Verantwortliche ein Aufbewahren der Kontaktdaten seit Beginn der Pflicht zur Kontaktdatenerfassung. Er wurde angewiesen unter Aufsicht der Ordnungsbehörde die Kontaktdaten zu vernichten.

Am 24. September 2021 erreichte mich eine Beschwerde, die sich gegen eine Kontaktdatenerfassung in einem Thermalbadbetrieb richtete. Eine solche Kontaktdatenerfassung war weder in § 4 CoSchuV noch in § 28a Abs. 4 IfSG vorgeschrieben. Da es deshalb an einer gesetzlichen Grundlage mangelte, die örtlichen Behörden allerdings gemäß § 27 Abs. 2 CoSchuV i. V. m. §§ 28 und 28a IfSG über die geltende Verordnung hinausgehende Maßnahmen erlassen konnten, forderte ich den Thermalbadbetrieb zur Stellungnahme auf. Hierbei konnte seitens des Beschwerdegegners keine gesetzliche Grundlage genannt werden, nach der die Kontaktdatenerfassung begründet gewesen wäre. In Absprache mit der örtlichen Ordnungsbehörde wurde die Kontaktdatenerfassung umgehend eingestellt und die bereits erhobenen Daten der Vernichtung zugeführt.

Etliche weitere Fälle betrafen vor allem Speisegaststätten. Die CoSchuV vom 22. Juni 2021 in der ab dem 16. September 2021 gültigen Fassung sah für Gaststätten (definiert als: „Gaststätten im Sinne des Hessischen Gaststättengesetzes vom 28. März 2012 (GVBl. S. 50), zuletzt geändert durch Gesetz vom 15. Dezember 2016 (GVBl. S. 294), Mensen, Hotels, Eisdielen, Eiscafés und andere Gewerbe“) keine Kontaktdatenerfassung mehr vor. In den früheren Fassungen war eine Kontaktdatenerfassung in § 22 CoSchuV normiert. Aufgrund der fehlenden gesetzlichen Grundlagen erreichten mich mehrere Eingaben, die eine über den 16. September 2021 hinausgehende Erfassung von Kontaktdaten zum Inhalt hatten. Auch hier wurden von mir Maßnahmen getroffen, um die weitere Erfassung einzustellen. Die Daten wurden anschließend der Vernichtung zugeführt. Bei einer dieser Eingaben wurde neben der Erfassung ohne gesetzliche Grundlage noch ein weiterer Verstoß festgestellt. Die Gäste der Speisegaststätte wurden gebeten, ihre

Daten in ein Formular in einem bereitgestellten Laptop einzutragen. Hierbei konnten bei den einzelnen Eingabefeldern via Autovervollständigung die Daten aller Kunden, die sich in der Vergangenheit dort eingetragen hatten, abgerufen werden. Auch hier wurde der Gaststättenbetreiber angewiesen, die Kontaktdatenerfassung einzustellen, vorhandene Daten zu löschen und im Falle einer erneuten Kontaktdatenerfassungspflicht diese datenschutzkonform durchzuführen.

Einen weiteren Schwerpunkt meiner Aufsichtstätigkeit betraf das Führen von offenen Listen. So erreichte mich beispielsweise am 5. Juli 2021 eine Beschwerde, die sich gegen einen Friseursalon richtete. Dieser war nach der CoSchuV vom 25. Juni 2021 bis 21. Juli 2021 geltenden Fassung als Dienstleistungsbetrieb gemäß § 25 Abs. 2 CoSchuV zur Erfassung von Kontaktdaten verpflichtet. Der Friseursalon kam der Kontaktdatenerfassung nach, stellte allerdings zur Erfassung eine öffentlich und somit für jedermann einsehbare Liste zur Verfügung. Diese Verhaltensweise war auch Inhalt der an mich gerichteten Beschwerde. Öffentlich einsehbare Listen, die Kontaktdaten enthalten, stellten nach Art. 5 Abs. 1 lit. f DS-GVO einen datenschutzrechtlichen Verstoß dar. Aus diesem Grund wurde der Beschwerdegegner von mir angewiesen, die Erfassung mittels einer öffentlichen Liste einzustellen.

2.4
Datenerhebung von Reiserückkehrern durch Kitas

Nach dem Ende der Ferienzeiten durften Kitas keine Angaben zu dem Aufenthalt in SARS-CoV-2 Risikogebieten und der gegebenenfalls anschließenden Quarantäne sowie zu COVID-Symptomen und Testergebnissen zur Überprüfung der Reiserückkehrer abfragen. Eine Rechtsgrundlage für diese Datenerhebungen lag nicht vor. Die Kitas sind für solche Abfragen nicht zuständig. Sie können die Eltern aber durch Informationsschreiben oder im Gespräch über ihre gesetzlichen Pflichten nach der Einreise aus dem Ausland aufklären.

Aufgrund einer Eingabe wurde ich auf ein Formular aufmerksam, dass einige Kitas zur Abfrage von Informationen von „Reiserückkehrern“ nutzen sollten. Der Träger dieser Kitas stellte diesen vor den Sommerferien 2021 ein Formular zur Abfrage zahlreicher personenbezogener Daten der Eltern und Kinder bereit. In dem Formular wurden Informationen über das Auslandsreiseland, eine Quarantäne und die typischen COVID-Symptome sowie zur digitalen Einreisebestätigung und zu einem negativen Testergebnis abgefragt. Den Befragten wurde mitgeteilt, dass eine Betreuung der Kinder nach den Ferien nur nach Vorlage des ausgefüllten Formulars möglich sei.

Es bestand keine Rechtsgrundlage für die verpflichtende Erhebung und Verarbeitung der im Formular genannten Daten durch die Kitas. Bei den Testergebnissen und den COVID-Symptomen handelt es sich um nach Art. 9 Abs. 1 DS-GVO besonders geschützte Gesundheitsdaten, deren Verarbeitung nur unter den strengen Voraussetzungen des Art. 9 Abs. 2 DS-GVO zulässig ist. Diese Voraussetzungen waren nicht erfüllt.

Die Erhebung dieser sensiblen Daten ist nicht Aufgabe der Kitas. Für die Überprüfung von Einreiseanmeldungen und Testnachweisen sind die mit der polizeilichen Kontrolle des grenzüberschreitenden Verkehrs beauftragten Behörden zuständig (§ 7 Abs. 2 der Coronavirus-Einreiseverordnung). Die Abfrage von Informationen der Reiserückkehrer aus Risikogebieten, insbesondere zu COVID-Symptomen und Quarantänen, liegt in der Zuständigkeit der Gesundheitsämter.

Gegebenenfalls könnte die freiwillige Offenlegung der Daten durch eine Einwilligung der betroffenen Personen legitimiert werden. Als datenschutzkonforme Vorgehensweise hat sich aber ein Informationsschreiben zu den Pflichten für Reiserückkehrer sowie die Möglichkeit eines Gesprächsangebots bewährt.

Diese Einschätzung habe ich bereits im Jahr 2020 in einem Beitrag auf meiner Website veröffentlicht, in dem auch die vergleichbaren Überlegungen zum Schulbereich dargestellt sind. Der Website-Beitrag ist unter dem folgenden Link abrufbar: https://datenschutz.hessen.de/datenschutz/gesundheits-und-sozialwesen/gesundheitswesen/was-schulen-und-kindertagesstätten.

Im weiteren Verlauf habe ich mich an den Träger der Kitas gewandt und mitgeteilt, dass die beabsichtigen Datenerhebungen nicht zulässig sind. Nach Aussage des Trägers seien die Kitas noch während der Sommerferien darüber informiert worden, dass das entsprechende Formular aus datenschutzrechtlichen Gründen nicht verwendet werden darf. Die unzulässigen Datenerhebungen wurden somit aufgrund meiner Intervention eingestellt.

2.5
Veröffentlichung von Impfdaten in sozialen Netzwerken

Es besteht die Gefahr, dass Verantwortliche gegen die Bestimmungen des Datenschutzrechts verstoßen, wenn sie im Zusammenhang mit der Corona-Pandemie Informationen zum Gesundheitsstatus ihrer Beschäftigten in sozialen Netzwerken veröffentlichen.

Im Berichtszeitraum erreichte mich eine Beschwerde, bei der es um einen Beitrag (sog. Post) in einer regionalen Chatgruppe ging. In dem Post hatte die Geschäftsführung eines Unternehmens verkündet, dass alle Beschäf-

tigten gegen Covid-19 geimpft seien. Die Geschäftsführung benannte zwar keinen der Beschäftigten namentlich. Aufgrund des regionalen Bezugs war es aber ohne größeren Aufwand möglich, Rückschlüsse auf die Identität der Beschäftigten des Unternehmens zu ziehen.

Die Beschwerde habe ich zum Anlass genommen, den Verantwortlichen zu dem Vorgang anzuhören. Er nahm dies zum Anlass, den entsprechenden Post zu löschen. Zur Verarbeitung des Impfstatus der betroffenen Beschäftigten gab er an, dass für die Covid-19-Schutzimpfung eine Arbeitszeitbefreiung gewährt worden sei, so dass die Beschäftigten durch die Wahrnehmung der Arbeitszeitbefreiung freiwillig den Impfstatus offengelegt hätten. Die Beschäftigten seien über den beabsichtigten Post informiert worden und hätten hierzu mündlich ihr Einverständnis erklärt.

Mit Blick auf den geschilderten Fall ist zu berücksichtigen, dass zwei Datenverarbeitungsvorgänge voneinander zu unterscheiden sind: Zum einen stellt sich die Frage der Rechtmäßigkeit der Erhebung der Impfdaten durch den Arbeitgeber (Abfragen des Impfstatus), zum anderen ist die Offenlegung des Impfstatus der Beschäftigten in einem sozialen Netzwerk (Posten des Impfstatus) zu bewerten.

Bei dem Abfragen des Impfstatus der Beschäftigten handelt es sich um eine „Verarbeitung personenbezogener Daten“. Die Begriffe „personenbezogene Daten“ und „Verarbeitung“ sind in Art. 4 Nr. 1 und 2 DS-GVO definiert.

Art. 4 Nr. 1 und 2 DS-GVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. *„personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;*
2. *„Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;*

(…)

Die mündliche Abfrage des Impfstatus liegt gemäß Art. 2 Abs. 1 DS-GVO grundsätzlich außerhalb des Anwendungsbereichs der DS-GVO, da insoweit weder eine dateigebundene noch eine automatisierte Verarbeitung erfolgt ist. Im Beschäftigungsverhältnis ist jedoch die Regelung des § 26 Abs. 7 BDSG zu berücksichtigen.

§ 26 Abs. 7 BDSG

(…)

(7) Die Absätze 1 bis 6 sind auch anzuwenden, wenn personenbezogene Daten, einschließlich besonderer Kategorien personenbezogener Daten, von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Die Vorschrift weitet die Regelungen des Beschäftigtendatenschutzes auf jede Form der Verarbeitung personenbezogener Daten aus. Auch die mündliche Abfrage des Impf- oder Genesenenstatus durch den Arbeitgeber stellt daher eine Verarbeitung dar, die den Anforderungen des Datenschutzrechts genügen muss.

Zu berücksichtigen ist weiterhin, dass es sich bei Informationen zu einer in Anspruch genommenen Schutzimpfung gegen Covid-19 um Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DS-GVO und damit um besondere Kategorien personenbezogener Daten im Sinn des Art. 9 Abs. 1 DS-GVO handelt.

Art. 4 Nr. 15 DS-GVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck

(…)

15. „Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

(…)

Art. 9 Abs. 1 DS-GVO

Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nach dem Wortlaut des Art. 9 Abs. 1 DS-GVO untersagt. Art. 9 Abs. 2 DS-GVO sieht von diesem Grundsatz Ausnahmen in den abschließend definierten Fällen der lit. a bis j vor. In Betracht kommt hier insbesondere Art. 9 Abs. 2 lit. b DS-GVO i. V. m. § 26 Abs. 3 BDSG.

§ 26 Abs. 3 BDSG

(…)

(3) [1]Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. [2]Absatz 2 gilt auch für die Einwilligung besonderer Kategorien personenbezogener Daten; die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen. [3]§ 22 Absatz 2 gilt entsprechend.

Auch der Post „alle Beschäftigten sind gegen Covid-19 geimpft“ erfüllt die Begriffe „personenbezogene Daten“ und „Verarbeitung“. Obwohl der Arbeitgeber in dem Post keine Beschäftigten namentlich benannte, handelt es sich um personenbezogene Daten im Sinn der DS-GVO. Wie zuvor dargestellt, sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Da über die Daten des Arbeitgebers eine Identifizierung der Beschäftigten möglich war, handelte es sich daher um personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO.

Auch die Voraussetzungen des Art. 4 Nr. 2 DS-GVO waren erfüllt, da unter den Begriff der Verarbeitung auch die Offenlegung personenbezogener Daten fällt. Offenlegung ist hierbei so zu verstehen, dass Dritten die Möglichkeit verschafft wird, die personenbezogenen Daten betroffener Personen zur Kenntnis zu nehmen. Die regionale Gruppe, in der der Post veröffentlicht wurde, hatte zum Zeitpunkt der Veröffentlichung des Posts rund 12.500 Mitglieder.

In die Verarbeitung ihrer Impfdaten können Beschäftigte nur freiwillig einwilligen. Bei Beachtung der Voraussetzungen des § 26 Abs. 2 BDSG können Beschäftigte in die Verarbeitung ihrer personenbezogenen Daten einwilligen. Dies gilt nach § 26 Abs. 3 Satz 2 BDSG auch für die Verarbeitung besonderer Kategorien personenbezogener Daten. Die Voraussetzungen für eine rechtswirksame Einwilligung zur Datenverarbeitung im Beschäftigungsverhältnis sind in § 26 Abs. 2 BDSG geregelt.

§ 26 Abs. 2 BDSG

(2) [1]Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen.

[2]Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Personen gleichgelagerte Interessen verfolgen. [3]Die Einwilligung hat schriftlich oder elektronisch zu erfolgen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. [4]Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Abs. 3 der Verordnung (EU) 2016/679 in Textform aufzuklären.

Entscheidend für die Frage, ob die Einwilligung rechtmäßig war, ist demnach, dass die Beschäftigten freiwillig in die zuvor beschriebenen Datenverarbeitungsvorgänge (Abfragen und Post des Impfstatus) eingewilligt haben. Zu berücksichtigen ist dabei das im Beschäftigungsverhältnis bestehende Über- und Unterordnungsverhältnis zwischen Arbeitgeber und Beschäftigen. Bei Bestehen eines rechtlichen oder wirtschaftlichen Vorteils für die Beschäftigten kann gemäß § 26 Abs. 2 Satz 3 BDSG von der Freiwilligkeit der Einwilligung ausgegangen werden. Da den Beschäftigten für die Wahrnehmung der Impftermine eine Arbeitsfreistellung gewährt wurde, war von der Einholung einer wirksamen Einwilligungserklärung für die Erhebung des Impfstatus auszugehen.

Abweichend war allerdings die Veröffentlichung des Posts in dem sozialen Netzwerk zu bewerten. Hier konnte der Verantwortliche nicht glaubhaft darstellen, dass die Beschäftigten ihre Einwilligung in die Offenlegung der besonderen Kategorien personenbezogener Daten – insbesondere freiwillig – erteilt hatten. Auch waren mit der Offenlegung – im Gegensatz zur ersten Fallkonstellation – keine wirtschaftlichen oder rechtlichen Vorteile für die Beschäftigten verbunden. Die Voraussetzungen einer wirksamen Einwilligung lagen somit nicht vor.

Das Posten der Impfdaten von Beschäftigten verstieß gegen die DS-GVO. Soweit besondere Kategorien personenbezogener Daten in einem sozialen Netzwerk gepostet wurden, ohne dass hierfür eine Rechtsgrundlage im Sinn des Art. 9 Abs. 2 lit. b bis j DS-GVO oder eine wirksame Einwilligungserklärung nach Art. 9 Abs. 2 lit. a oder § 26 Abs. 3 Satz 2 i. V. m. Abs. 2 BDSG vorgelegen hat, verstieß dies gegen den Grundsatz der Rechtmäßigkeit nach Art. 5 Abs. 1 lit. a DS-GVO i. V. m. Art. 9 Abs. 1 DS-GVO.

Art. 5 Abs. 1 Buchstabe a DS-GVO

Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

(…)

2.6
Kein Ausschluss der Betroffenenrechte durch Coronavirus-Schutzverordnung

Beschränkungen der Rechte und Pflichten aus den Art. 12 bis 22 der DS-GVO (Rechte der betroffenen Person) können nach Art. 23 DS-GVO nur unter strengen Voraussetzungen durch nationales Recht vorgenommen werden. Es muss sich um eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme handeln. Dabei müssen die Notwendigkeit und die Verhältnismäßigkeit für jedes beschränkte Betroffenenrecht und für jede Kategorie von Verantwortlichen einzeln betrachtet werden. Ein pauschaler Ausschluss der wesentlichen Betroffenenrechte hinsichtlich eines Verarbeitungsprozesses lässt sich schwer mit den Anforderungen des Art. 23 DS-GVO in Einklang bringen.

Gemäß § 4 Nr. 3 CoSchuV vom 22. Juni 2021 war die Anwendbarkeit der Betroffenenrechte nach Art. 13 (Informationspflicht), 15 (Auskunftsrecht), 18 (Recht auf Einschränkung der Verarbeitung) und 20 (Recht auf Datenübertragbarkeit) DS-GVO im Rahmen der Kontaktdatenerhebung zur Nachverfolgung und Unterbrechung von Infektionsketten ausgeschlossen:

§ 4 Nr. 3. CoSchuV

… die Bestimmungen der Art. 13, 15, 18 und 20 der 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 (Datenschutz-Grundverordnung) vom 27. April 2016 (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72, 2018 Nr. L 127 S. 2) zur Informationspflicht und zum Recht auf Auskunft zu personenbezogenen Daten finden keine Anwendung; die von der Kontaktdatenerfassung Betroffenen sind über diese Beschränkungen zu informieren.

Eine entsprechende Regelung enthielt die Corona-Kontakt- und Betriebsbeschränkungsverordnung (CoKoBeV) auch schon seit Frühjahr 2020.

Hierzu erreichten mich einige Eingaben von Bürgerinnen und Bürgern, die sich über den Ausschluss der Betroffenenrechte beschwerten.

Nach Art. 23 DS-GVO können die Rechte und Pflichten gemäß Art. 12 bis 22 DS-GVO durch Rechtsvorschriften der Mitgliedsstaaten beschränkt werden, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die eines der in Art. 23 Abs. 1 lit. a bis j DS-GVO genannten Ziele sicherstellt.

Eine solche Rechtsvorschrift muss außerdem die in Art. 23 Abs. 2 DS-GVO genannten spezifischen Vorgaben erfüllen.

Der Ausschluss der Betroffenenrechte erfolgte durch eine Rechtsverordnung des Landes. Beschränkungen nach Art. 23 DS-GVO können auch durch Rechtsverordnungen erfolgen, da nach Erwägungsgrund 41 DS-GVO eine „Gesetzgebungsmaßnahme“ nicht notwendigerweise einen von einem Parlament angenommenen Gesetzgebungsakt erfordert.

Auch ein berechtigtes Ziel der Einschränkungen in Form des Schutzes sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses im Bereich der öffentlichen Gesundheit (Art. 23 Abs. 1 lit. e DS-GVO) konnte im Hinblick auf § 4 Nr. 3 CoSchuV angenommen werden. Nach der Begründung der Landesregierung diente der Ausschluss der Betroffenenrechte der effektiven Pandemiebekämpfung, da die Erfüllung dieser Rechte für die Unternehmen und Betriebe, die der Pflicht zur Kontaktdatenerfassung unterlagen, einen erheblichen Aufwand darstellte.

An der Notwendigkeit und der Verhältnismäßigkeit dieser Einschränkungen hatte ich aber erhebliche Zweifel. Gegen die Erforderlichkeit der Einschränkungen sprach zunächst, dass der Bundesgesetzgeber keinen Bedarf für diese Einschränkungen gesehen hatte, obwohl er die Kontaktnachverfolgung in § 28a Abs. 4 IfSG ausführlich geregelt hatte. Insbesondere vor dem Hintergrund der von der CoSchuV favorisierten elektronischen Kontaktdatenerhebung entsprechend § 4 Nr. 3 CoSchuV war auch zweifelhaft, ob die Erfüllung der Betroffenenrechte für die Unternehmen und Betriebe einen Aufwand bedeutete, der die Pandemiebekämpfung spürbar erschwerte. Im Übrigen ließ der pauschale Ausschluss der Betroffenenrechte nach seinem Wortlaut keinen Raum für die Berücksichtigung der Umstände des Einzelfalls und besonderer Situationen.

Die von Art. 23 Abs. 1 DS-GVO geforderte Notwendigkeit und Verhältnismäßigkeit der Einschränkung müssen für jedes beschränkte Betroffenenrecht und für jede Kategorie von Verantwortlichen einzeln betrachtet werden.

Eine entsprechend ausdifferenzierte Regelung enthielt § 4 Nr. 3 CoSchuV jedoch nicht.

Gerade die Informationspflicht nach Art. 13 DS-GVO konnte durch eine elektronische Bereitstellung einer entsprechenden Erklärung ohne größeren Aufwand erfüllt werden. Hierbei konnten Musterdokumente verwendet werden. So stellen z. B. die Betreiber der Luca App ein praktikables Musterdokument für eine Information nach Art. 13 DS-GVO zur Nutzung des Luca Systems zur Verfügung. Auch verschiedene Branchenverbände stellen entsprechende Musterdokumente zur Kontaktnachverfolgung bereit.

Auch der Auskunftsanspruch nach Art. 15 DS-GVO, der eines der elementarsten Betroffenenrechte darstellt, konnte durch die elektronische Kontaktdatenerhebung regelmäßig mit geringem Aufwand erfüllt werden. Beim Einsatz der Luca App hat die zur Kontaktdatenerhebung verpflichtete Stelle ohnehin keinen Zugriff auf die personenbezogenen Daten, da diese verschlüsselt sind. Eine Auskunft zu den Anmeldedaten und den Besuchsdaten kann jedoch durch den Betreiber der Luca App erteilt werden. Auch bei der schriftlichen Kontaktdatenerfassung in Papierform ist eine Auskunft regelmäßig ohne weiteres möglich, insbesondere wenn die betroffene Person Angaben zu der Besuchszeit macht. Stichhaltige Gründe für die grundsätzliche Unanwendbarkeit dieses Rechts waren nicht erkennbar.

Auch die Notwendigkeit und Verhältnismäßigkeit des pauschalen Ausschlusses der Rechte auf Einschränkung der Verarbeitung (Art. 18 DS-GVO) und Datenübertragbarkeit (Art. 20 DS-GVO) waren nicht ersichtlich. Das Recht auf Datenübertragbarkeit war im Rahmen der verpflichtenden Kontaktnachverfolgung gemäß Art. 20 Abs. 1 lit. b DS-GVO ohnehin tatbestandlich nicht anwendbar, da die Verarbeitung nicht auf einer Einwilligung (Art. 6 Abs. 1 lit. a DS-GVO) oder einem Vertrag (Art. 6 Abs. 1 lit. b DS-GVO), sondern auf einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c DS-GVO) beruhte. Eine Notwendigkeit für den Ausschluss dieses Rechts bestand folglich nicht. Den Ausschluss der Betroffenenrechte in § 4 Nr. 3 CoSchuV hielt ich daher nicht für notwendig und verhältnismäßig im Sinne des Art. 23 Abs. 1 DS-GVO.

Aus diesen Gründen habe ich mich gegenüber der Landesregierung für eine Streichung des § 4 Nr. 3 CoSchuV eingesetzt. Die Landesregierung hat meine Bedenken nachvollzogen und aufgegriffen. Mit der Überarbeitung der CoSchuV zum 19. August 2021 hat sie den § 4 Nr. 3 CoSchuV ersatzlos gestrichen. Die Betroffenenrechte nach der DS-GVO waren seitdem auch bei der Kontaktdatenerhebung in Hessen uneingeschränkt anwendbar.

Auf der Website meiner Behörde habe ich zu diesem Vorgang einen Beitrag veröffentlicht, der unter folgendem Link abgerufen werden kann: https://

datenschutz.hessen.de/datenschutz/gesundheits-und-sozialwesen/gesundheitswesen/beschränkungen-der-betroffenenrechte-nach.

3. Digitale Souveränität

Eine wichtige Aufgabe im Berichtszeitraum ergab sich durch die Notwendigkeit, bei vielen Datenverarbeitungssystemen die internationale Verarbeitung personenbezogener Daten zu bewerten und den grundrechtlich gebotenen Datenschutz auch bei Datenverarbeitungen außerhalb der Europäische Union zu gewährleisten. Aktualisiert wurde diese Aufgabe durch die verstärkte Digitalisierung als Reaktion auf die Corona-Pandemie und die Rechtsprechung des Europäischen Gerichtshofs (EuGH) (Ziff. 3.1). Besondere Bedeutung hat digitale Souveränität, wenn datenschutzgerechte Digitalisierungsprojekte erfolgreich umgesetzt werden sollen (Ziff. 3.2). Exemplarisch kulminierte digitale Souveränität am Beispiel der Videokonferenzen (s. Ziff. 4).

3.1
Digitale Souveränität und Datenschutz

Die normative Eigenverpflichtung der Europäischen Union, das Grundrecht auf Schutz der personenbezogenen Daten gemäß Art. 8 Grundrechtecharta (GRCh) zu schützen, kann nur erfüllt werden, wenn die für die Digitalisierung gesellschaftlicher Beziehungen eingesetzten IT-Systeme diesen Schutz gewährleisten und ihn nicht konterkarieren. Nur wenn der zum Schutz verpflichtete Verantwortliche in der Lage ist, diesen Schutz bei seiner Datenverarbeitung zu gewährleisten, kann dieses Grundrecht umgesetzt werden.

Grundrechtsschutz bei der Übermittlung personenbezogener Daten in Drittländer

Seit 2009 gewährleistet die Europäische Union in ihrer Grundrechtecharta in Art. 8 das Grundrecht auf Schutz der personenbezogenen Daten einer jeden betroffenen Person. Seitdem ist es Aufgabe der Europäischen Union und aller Mitgliedstaaten, dieses Grundrecht gegenüber jedem unberechtigten Eingriff zu schützen. Dies gilt auch gegenüber Datenverarbeitungen im Ausland. Daher hat die DS-GVO zum einen in Art. 3 Abs. 2 bestimmt, dass sie – unabhängig vom Ort der Datenverarbeitung – anwendbar ist, wenn die Datenverarbeitung im Zusammenhang damit steht, betroffenen Personen in der Europäischen Union Waren oder Dienstleistungen anzubieten oder sie zu beobachten. Aus dem gleichen Grund hat die DS-GVO in Art. 44 ff. Regelungen dagegen getroffen, dass betroffene Personen ihren Grundrechtsschutz verlieren, wenn ihre personenbezogenen Daten in ein Drittland, also ein Land außerhalb der Europäischen Union, übermittelt werden. Nach Art. 44 S. 2 und Erwägungsgrund 101 S. 3 DS-GVO soll nämlich „das durch diese Verordnung unionsweit gewährleistete Schutzniveau für natürliche Personen

… bei der Übermittlung personenbezogener Daten aus der Union an Verantwortliche, Auftragsverarbeiter oder andere Empfänger in Drittländern … nicht untergraben werden“.

Nach Art. 44 Satz 1 DS-GVO ist eine Übermittlung personenbezogener Daten in ein Drittland grundsätzlich nur zulässig, wenn die in den folgenden Vorschriften festgelegten Bedingungen eingehalten werden. Die erste Bedingung besteht nach Art. 45 DS-GVO darin, dass die Europäische Kommission für das empfangende Drittland anerkannt hat, dass dort ein vergleichbares Datenschutzniveau herrscht wie in der Europäischen Union. Solche Anerkennungen hat die Europäische Kommission bisher für 14 Drittländer getroffen – unter anderem für Argentinien, Uruguay, Kanada, Neuseeland, Japan, Südkorea und Großbritannien. Eine zweite, alternative Bedingung besteht nach Art. 46 DS-GVO darin, dass der übermittelnde Verantwortliche mit dem Empfänger geeignete Garantien vereinbart hat und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Geeignete Garantien können nach Art. 46 Abs. 2 DS-GVO in Verwaltungsvereinbarungen, in verpflichtenden Verhaltensregeln von Konzernen (gemäß Art. 47 DS-GVO), in der Vereinbarung von Standardvertragsklauseln, in genehmigten Verhaltensregeln oder in einem genehmigten Zertifizierungsmechanismus bestehen. Schließlich kann für nicht routinemäßige Übermittlungen eine der Sonderausnahmen greifen, die in Art. 49 DS-GVO aufgelistet sind. Der Sinn dieser Bedingungen und Ausnahmeregelungen besteht darin, dass sie auf alternative Weise sicherstellen, dass die Datenübermittlung nicht zu einem Grundrechtsverlust führt.

Für die Datenübermittlung in die USA hatte die Europäische Kommission seit 2000 Sondervereinbarungen getroffen, um einen Datenaustausch zu ermöglichen (Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. L 215 vom 25. August 2000, S. 7). Dabei war bekannt, dass weder die Rechtsordnung noch die Rechtspraxis in den USA ein Datenschutzniveau bieten, das mit dem in der Europäischen Union vergleichbar ist. Das erste Abkommen mit den USA, „Safe Harbor“ genannt, sah vor, dass datenempfangende Stellen in den USA sich verpflichten konnten, bestimmte Datenschutzregeln einzuhalten, und durch eine Selbstverpflichtung einen sicheren Hafen für die europäischen Daten bilden konnten. Dann galt eine Datenübermittlung als zulässig. Eine effektive Überprüfung dieser Selbstverpflichtungen in den USA erfolgte nie. Mit dem Abkommen wurden somit Grundrechtsverletzungen europäischer betroffener Personen in Kauf genommen. Wenig verwunderlich hat der EuGH

mit seinem Urteil vom 6. Oktober 2015 (C-362/14 – Schrems I) das „Safe Harbor“-Abkommen als rechtswidrig aufgehoben.

Mit Wirkung zum 1. August 2016 hat die Europäische Kommission erneut ein vergleichbares Abkommen mit den USA anerkannt, diesmal „Privacy Shield“ genannt (Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes, ABl. L 207 vom 1. August 2016, S. 1–112). Dieses enthielt nur wenige zusätzliche Regelungen zu „Safe Harbor“, wie etwa eine Selbstzertifizierung der empfangenden Stellen, mit der sie dem „Privacy Shield“ beitreten konnten, und das Versprechen, einen Ombudsman beim US-Außenministerium zu bestellen. Eine Einschränkung der Kompetenzen der zuständigen Nachrichtendienste und Sicherheitsbehörden in den USA fand jedoch nicht statt.

Das Schrems II-Urteil des EuGH

Mit seinem Urteil vom 16. Juli 2020 (C-311/18 – Schrems II) hat der EuGH die Bedeutung der Vorgaben der DS-GVO zur Übermittlung von personenbezogenen Daten in Drittstaaten betont und diese bezogen auf die USA präzisiert. Dabei hat er festgestellt, dass die Vereinbarung „Privacy Shield“ unionsrechtswidrig und nichtig ist. Die Europäische Kommission verstieß gegen die Grundrechtecharta, indem sie diese Vereinbarung mit den USA als Rechtfertigung für Datenübermittlungen anerkannte, obwohl sie dazu führte, dass die betroffenen Personen ihren Grundrechtsschutz verloren. Der EuGH stützte sein Urteil auf zwei zentrale Kritikpunkte an der Rechtslage in den USA. Zum einen sind die Befugnisse der zuständigen Behörden in den USA, auf die übermittelten personenbezogenen Daten zuzugreifen (insbesondere gemäß des Foreign Intelligence Surveillance Act (FISA), 1978, Pub.L. 95–511, Section 702 und der Executive Order 12333 vom 4. Dezember 1981, weitgehend neu gefasst durch Executive Order 13470 vom 30. Juli 2008), unbestimmt und unverhältnismäßig. Zum anderen kritisierte er, dass für US-Ausländer ein adäquater Rechtsweg zur Abwehr solcher Zugriffe ausgeschlossen ist. Zwar sind bilaterale Standarddatenschutzverträge mit Datenempfängern in den USA weiterhin zulässig, aber allein nicht ausreichend. Vielmehr muss der Verantwortliche in der Europäischen Union, der personenbezogene Daten in die USA übermittelt, die Grundrechte der betroffenen Personen durch „zusätzliche Maßnahmen“ davor schützen, dass ein unverhältnismäßiger Zugriff der dortigen staatlichen Stellen erfolgt.

Nach dem Urteil des EuGH ist jeder Verantwortliche, der ein IT-System verwendet, für das er nicht ausschließen kann, dass personenbezogene Daten

in einen Drittstaat übermittelt werden, verpflichtet, die Situation umfassend zu überprüfen. Er muss die Rechtslage und die Datenschutzpraxis in diesem Drittstaat feststellen und, wenn dort kein angemessenes Datenschutzniveau herrscht, die zum Schutz der Grundrechte erforderlichen „zusätzlichen Maßnahmen“ ergreifen. Zum Prüfprogramm des Verantwortlichen vor der Übermittlung personenbezogener Daten in ein Drittland hat der Europäische Datenschutzausschuss (EDSA) eine umfangreiche Empfehlung (1/2020) veröffentlicht. Ebenso hat er in seiner Empfehlung 2/2020 ausführliche Hinweise zu möglichen Bewertungen des Datenschutzniveaus gegeben (s. zu beiden Empfehlungen https://datenschutz.hessen.de/infothek/europ%C3%A4ischer-datenschutzausschuss-artikel-29-datenschutzgruppe).

Wenn der Verantwortliche zu dem erforderlichen Grundrechtsschutz nicht in der Lage ist, hat er die Datenübermittlung und damit meist auch die Nutzung des IT-Systems, das diese erfordert, zu unterlassen. Die datenschutzrechtliche Aufsichtsbehörde ist verpflichtet, diese Forderungen des EuGH durchzusetzen.

Das Urteil des EuGH hatte nur über den Schutz personenbezogener Daten zu entscheiden, die in die USA übermittelt werden. Das gleiche Problem des Grundrechtsschutzes stellt sich aber auch, wenn US-Behörden auf personenbezogene Daten in der Europäischen Union zugreifen. Dies ist nicht nur nach dem FIS-Act, sondern auch nach dem Clarifying Lawful Overseas Use of Data (CLOUD) Act von 2018, Pub.L. 115–141 (H.R. 4943) möglich, der auf eine eindeutige Rechtsgrundlage von US-Behörden für einen weltweiten Datenzugriff zielt.

Verpflichtet sind alle US Telecommunication Provider. Dieser Begriff wird sehr weit verstanden und umfasst in jedem Fall alle Software-, Cloud- und Plattformanbieter. Sie alle sind verpflichtet, alle Daten (Inhalts- und Metadaten) elektronischer Kommunikation auf Antrag zu erfassen und zu speichern sowie alle gespeicherten Informationen den berechtigten US-Behörden zur Verfügung zu stellen, unabhängig davon, wo sie aufbewahrt werden. Dies trifft also auch für europäische Tochterunternehmen von US-Providern zu.

Hiergegen richtet sich Art. 48 DS-GVO. Er verbietet einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten auf Anordnung eines Gerichts oder einer Behörde eines Drittlandes, es sei denn, diese beruhe auf einem internationalen Abkommen. Auch wenn der EuGH den Fall nicht entschieden hat, dass eine staatliche Stelle eines Drittlandes von einem ihr verpflichteten Unternehmen in der Europäischen Union fordert, ihr personenbezogene Daten zu übermitteln, müssen für diesen Fall ebenfalls die Anforderungen des Schrems II-Urteils gelten. Danach dürfen Verantwortliche anderen Unternehmen, insbesondere Auftragnehmern gemäß Art. 28 DS-GVO, personenbezogene Daten nur dann

anvertrauen, wenn diese nicht ausländischen staatlichen Stellen verpflichtet sind, die von ihnen die Herausgabe dieser Daten verlangen können, oder zusätzliche Schutzmaßnahmen eine Herausgabe verhindern.

Digitale Souveränität als Voraussetzung für Datenschutz

Verantwortliche in Deutschland und Europa sind jedoch in hohem Maß von IT-Systemen US-amerikanischer Anbieter abhängig. Diese IT-Systeme sind in der Regel so gestaltet, dass sie personenbezogene Daten in die USA übermitteln. Dort stehen sie einem rechtlich unzureichend kontrollierten Zugriff durch staatliche Stellen offen. Zusätzlich können die berechtigten staatlichen Stellen US-amerikanische Provider zwingen, ihnen personenbezogene Daten aus Europa, auf die sie – direkt oder etwa über Tochterunternehmen – Zugriff nehmen können, zu übergeben. Da betroffene Personen aus Europa als US-Ausländer diese Praxis nicht gerichtlich überprüfen lassen können, verlieren sie durch die Übertragung der Daten ihren Grundrechtsschutz.

Die Vorgaben des Schrems II-Urteils umzusetzen, ist die Aufgabe der Datenschutzaufsichtsbehörden. Diese haben für diese Aufgabe ein Entschließungs- und Auswahlermessen. Sie müssen und können darüber entscheiden, ob sie gegenüber Verantwortlichen, die gegen die Anforderungen des EuGH verstoßen, vorgehen und welche Mittel sie dafür einsetzen. In Ausübung dieses Ermessens müssen sie bei der Übermittlung von Daten in die USA oder der Beauftragung von Auftragnehmern, die in Loyalitätskonflikte geraten können, für die Auswahl ihrer Maßnahmen auch die Grundrechte und verfassungsrechtlichen Aufgaben der Verantwortlichen berücksichtigen. Dabei lassen sich drei Konstellationen unterscheiden:

1. Entwickeln Unternehmen neue Geschäftsmodelle oder digitalisieren Behörden ihre Verwaltungsleistungen, müssen sie von Anfang an berücksichtigen, dass die DS-GVO – in der Auslegung des EuGH – jede Datenübermittlung in die USA verbietet, bei der nicht durch zusätzliche Maßnahmen ausgeschlossen ist, dass US-Behörden grundrechtsverkürzend auf die Daten zugreifen können. Sie müssen ihre IT-Systeme – im Rahmen ihrer Verpflichtung zu Privacy by Design gemäß Art. 25 DS-GVO – so gestalten, dass eine solche Datenübertragung ausgeschlossen ist. Das heißt, dass sie die eingesetzten Hard- und Software-Systeme, Plattformen und Dienstleistungen so auswählen und konfigurieren müssen, dass keine solche Datenübermittlung stattfindet, oder ihre Auftragnehmer so aussuchen, dass sie nicht dem FIS-Act und dem Cloud Act unterliegen.
2. Sind ausländische Systeme und Dienste in die Tätigkeit der Verantwortlichen voll eingebunden und in den Alltag der Mitarbeitenden und Kunden oder Bürger integriert, ist bei Unternehmen zu berücksichtigen, dass durch

ein Untersagen, Daten in ein Drittland mit unzureichendem Datenschutz zu übermitteln, zumindest seine Grundrechte auf Berufsfreiheit und auf Eigentum eingeschränkt werden. Bei öffentlichen Stellen kann es sein, dass sie ohne die ausländischen Dienste oder Software ihre rechtlich übertragenen Aufgaben nicht mehr erfüllen können, etwa die Polizei ihren Schutzauftrag oder Schulen und Hochschulen ihren Bildungsauftrag. Wenn die Wirkungen eines Verbots der Datenübermittlung berücksichtigt werden, ist entscheidend, ob es für den Verantwortlichen geeignete organisatorische und technische Alternativen gibt, um die Funktionen zu erbringen, die mit der Datenübertragung in das Drittland erfüllt werden. Bestehen solche Alternativen, entstehen für den Verantwortlichen nur „Wechselkosten“, es wird aber nicht sein Geschäftsmodell oder die Erfüllung seiner gesetzlichen Aufgaben in Frage gestellt. Solche „Wechselkosten“ können umfangreich sein und umfassen nicht nur die monetären Kosten für neue Hardware, Lizenzen oder Dienste. Sie sind oft auch mit schwierigen organisatorischen Umstellungen oder der Veränderung von Nutzungsgewohnheiten verbunden. Dennoch dürfte in all diesen Fällen regelmäßig der Schutz der Grundrechte der betroffenen Personen das Gewicht der „Wechselkosten“ überwiegen.

3. Fehlen jedoch geeignete organisatorische und technische Alternativen, kann bei Unternehmen ihr grundlegendes Geschäftsmodell und damit ihre wirtschaftliche Existenz in Frage stehen. Bei staatlichen Stellen kann dies dazu führen, dass sie nicht mehr ihre durch Gesetz übertragenen Aufgaben erfüllen können. Droht ein solcher „Funktionsausfall“, erfordert die datenschutzrechtliche Reaktion eine schwierige Abwägung zwischen dem Schutz der Grundrechte vieler betroffener Personen und dem Schutz der Grundrechte des Unternehmens oder den Zielen staatlicher Aufgabenerfüllung. Dies wird noch dadurch erschwert, dass sowohl die Gefährdung der Grundrechte der betroffenen Personen in dem Drittland als auch die negativen Folgen einer Unterlassung der Datenübermittlung oft nur durch schwierige Prognosen erkannt werden können. Um den durch Art. 8 GRCh aufgegebenen Grundrechtsschutz zu gewährleisten, sind aus praktischer Sicht jeweils technisch-organisatorische Alternativen zu den aus dem Drittland – hier den USA – angebotenen Hardware, Software, Diensten und Plattformen erforderlich. Daher fordert das Grundrecht aus Art. 8 GRCh in der Folge des Schrems II-Urteils des EuGH, solche Alternativen zu schaffen und die technische Abhängigkeit von den USA zu durchbrechen.

Für die Umsetzung des Schrems II-Urteils ist also das Bestehen von geeigneten technischen und organisatorischen Alternativen entscheidend. Der EuGH fordert somit indirekt von der Europäischen Union, den Mitgliedstaaten und

den Verantwortlichen, digitale Souveränität herzustellen. Digitale Souveränität als Voraussetzung und Folge digitaler Selbstbehauptung kann je nach Politikfeld unterschiedliche Ziele beinhalten. Für den hier relevanten rechtsstaatlichen Kontext ist Ziel digitaler Souveränität, dass der Verantwortliche seine IT-Systeme so auswählen, gestalten und beherrschen kann, dass er seine datenschutzrechtlichen Pflichten erfüllen kann (s. auch Entschließung der DSK, Digitale Souveränität in der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen, 2020).

Notwendigkeit datenschutzkonformer Alternativen

Die hohe Abhängigkeit von Hard- und Software, Plattformen und Diensten aus den USA ermöglicht den großen global agierenden Anbietern, Zwangssituationen auszunutzen. Im Bereich des Datenschutzes fordern sie z. B. von den Nutzenden, in unbegrenzte und unbestimmte Datenverarbeitungen einzuwilligen. Von den Verantwortlichen verlangen sie, Geschäftsmodellen, die Daten in Drittländer übermitteln, zuzustimmen und Zugriffsmöglichkeiten auf Daten und Datenverarbeitung zu akzeptieren. Und von der Europäischen Kommission fordern sie, in den Datenaustausch mit den USA einzuwilligen, auch wenn dadurch Grundrechte von betroffenen Personen in der Europäischen Union verkürzt werden. Angesichts der hohen Abhängigkeit von IT-Systemen aus den USA sind digitale Souveränität der Verantwortlichen und der geforderte Grundrechtsschutz nur zu erreichen, wenn geeignete alternative datenschutzgerechte IT-Systeme angeboten werden, auf die Verantwortliche wechseln können.

Diese Vielfalt in möglichst vielen Bereichen der Verarbeitung personenbezogener Daten zu erreichen, ist keine Aufgabe der Aufsichtsbehörden, sondern der Politik. Sie zu erfüllen, erfordert Maßnahmen unter anderem der Wirtschafts- und Industrie-, Wettbewerbs-, Forschungs-, Bildungs-, Rechts- und Digitalpolitik in der Europäischen Union und in den Mitgliedstaaten. Diese Aufgabe wird von der Politik auch grundsätzlich anerkannt. Bemühungen um mehr digitale Souveränität finden in Deutschland und in der Europäischen Union seit mehreren Jahren statt. Denn digitale Souveränität ist nicht nur eine Frage des Rechtsstaats und des Grundrechtsschutzes, sondern auch der Wettbewerbsfähigkeit, der politischen Selbstbestimmung und der Innovationskraft. Sie ist nicht nur Voraussetzung für den Schutz der betroffenen Person, sondern auch für den Schutz der Verantwortlichen vor Wettbewerbsnachteilen. Daher bemüht sich die Europäische Union mit verschiedenen Gesetzesvorhaben wie z. B. den Entwürfen für einen Digital Services Act, einen Digital Market Act, einen Digital Governance Act oder einer KI-Verordnung die Kontrolle über Hardware und Software, Daten und

Datenströme, Standards und Protokolle, Prozesse, Dienstleistungen und Infrastruktur zu gewinnen.

Politische Maßnahmen zur Erreichung digitaler Souveränität

Digitale Souveränität erfordert eine Vielfalt geeigneter datenschutzkonformer Alternativen zu IT-Systemen, die eine Datenverarbeitung in einem Drittstaat erzwingen oder einen Datenzugriff aus einem Drittstaat ermöglichen, der kein vergleichbares Datenschutzniveau wie in der Europäischen Union hat. Digitale Souveränität ist erreicht, wenn es ausreichende Wahlmöglichkeiten für IT-Systeme gibt, die die Datenschutzanforderungen einhalten. Um diese Auswahl zu ermöglichen, sind geeignete gesetzliche Rahmenbedingungen in der Europäischen Union und in den Mitgliedstaaten, aber auch vielfältige praktische Maßnahmen der Auswahl, Beschaffung und Nutzung geeigneter IT-Systeme notwendig.

Die konkreten Zielsetzungen digitaler Souveränität differieren nach Abhängigkeiten und nach Handlungsmöglichkeiten in den unterschiedlichen gesellschaftlichen Bereichen der Digitalisierung. Anzustreben sind z. B.

– Eigenentwicklungen von IT-Systemen und das Angebot von eigenen Plattformen und Diensten aus der Europäischen Union,
– der Eigenbetrieb ausländischer IT-Systeme durch europäische Verantwortliche (On-Premise-Lösungen),
– der Vertrieb, Support und Service ausländischer Informationstechnik durch Anbieter aus der Europäischen Union,
– die rechtskonforme Konfiguration ausländischer IT-Systeme unter Ausschluss von Datenübermittlungen in ein Drittland ohne ausreichendes Datenschutzniveau,
– der Einsatz von technisch-rechtlichen Treuhändern, die keinen ausländischen Stellen verpflichtet sind,
– ausreichende Transparenz über die Funktionen der IT-Systeme, insbesondere der erzwungenen Datenübermittlungen, und
– eine ausreichende eigene Bewertungssouveränität über Eigenschaften und Wirkungen von IT-Systemen und deren Risiken.

Welche Zielsetzung als passend und ausreichend angesehen werden kann, ist für das jeweilige politische, wirtschaftliche und technische Handlungsfeld festzulegen.

Der EuGH fordert mit seinem Schrems II-Urteil, dass die Europäische Union und die Mitgliedstaaten ihre politischen Handlungsmöglichkeiten nutzen, um die Voraussetzungen für digitale Souveränität und damit für den Grundrechts-

schutz in der digitalen Welt herzustellen. Wenn es Aufgabe der Union und der Mitgliedstaaten ist, die Grundrechte auch bei der Datenübermittlung in Drittländer zu schützen, dann müssen sie auch die extrem hohe Abhängigkeit von ausländischen IT-Systemen verringern, die nicht die europäischen Grundrechte respektieren. Der durch die Grundrechtecharta, die DS-GVO und das Schrems II-Urteil des EuGH vorgegebene Grundrechtsschutz kann nur erreicht werden, wenn die Verantwortlichen in der Europäischen Union über eine ausreichende digitale Souveränität verfügen. Sowohl auf der Ebene der Europäischen Union als auch vieler Mitgliedstaaten ist digitale Souveränität als zentrales politisches Ziel schon formuliert und in politische Strategien integriert.

Aufgaben der Aufsichtsbehörde

Die datenschutzrechtliche Aufsichtsbehörde hat bei dem gegebenen (geringen) Maß an digitaler Souveränität die Aufgabe, ein möglichst hohes Maß an Grundrechtsschutz zu erreichen. Sie wird mit dieser Aufgabe auf unterschiedlichen Ebenen konfrontiert sein.

Zum einen trifft sie immer wieder auf dieses Problem, wenn sie Beschwerden betroffener Personen nach Art. 77 DS-GVO bearbeiten muss, die sich dagegen wehren, dass ein Verantwortlicher ihr Grundrecht auf Datenschutz dadurch verletzt, dass er ihre personenbezogenen Daten in ein Drittland ohne ausreichendes Datenschutzniveau überträgt. Sie können sich darauf berufen, dass ein Verantwortlicher, der gegen die Vorgaben des Schrems II-Urteils des EuGH verstößt, rechtswidrig handelt. Als Aufsichtsbehörde muss ich der Beschwerde nachgehen und für Abhilfe sorgen. Sollte ich dies nicht in der Weise und in dem Umfang tun, wie die betroffene Person dies erwartet, kann sie ihre Grundrechte nach Art. 78 DS-GVO auch vor dem Verwaltungsgericht durch Klage gegen mich und den Verantwortlichen (als Beigeladenen) geltend machen. Eventuell kann sie auch gegen den Verantwortlichen direkt vor dem Zivilrechtsgericht oder dem Verwaltungsgericht klagen.

Zweitens entstehen der Aufsichtsbehörde durch das Schrems II-Urteil neue Aufklärungs- und Beratungsaufgaben. Sie muss nach Art. 57 Abs. 1 lit. b DS-GVO „die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung sensibilisieren und sie darüber aufklären“ und nach Art. 57 Abs. 1 lit. d DS-GVO „die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus dieser Verordnung entstehenden Pflichten sensibilisieren“. Wenn sie durch ihre Aufklärung und Beratung auch an Lösungen der Datenschutzprobleme mitwirken will, wird sie sich auch auf Fragen nach möglichen technisch-organisatorischen Alternativen und möglichen Gestaltungen der IT-Systeme einlassen müssen. Sie wird

darüber aufklären, dass bei neuen IT-Systemen von Anfang an das Problem des Grundrechtsverlusts durch Datenübertragungen in Drittstaaten berücksichtigt werden muss und dass der Verantwortliche bereits betriebene IT-Systeme daraufhin überprüfen muss, ob er dadurch personenbezogene Daten in Drittländer ohne ausreichendes Datenschutzniveau überträgt und dafür ausreichende zusätzliche Schutzmaßnahme vorsieht. Andernfalls muss er für Abhilfe sorgen.

Drittens muss die Aufsichtsbehörde in Erfüllung ihrer Aufgabe nach Art. 57 Abs. 1 lit. a DS-GVO, „die Anwendung dieser Verordnung (zu) überwachen und durch(zu)setzen“, ein erfolgversprechendes Vorgehen wählen, um bei den Verantwortlichen die Umsetzung der Datenschutzvorgaben zu erreichen. Sie wird bei geplanten IT-Systemen die Verantwortlichen nach Art. 58 Abs. 1 lit. d DS-GVO auf einen möglichen Datenschutzverstoß hinweisen oder sie gar vor einem absehbaren Verstoß warnen müssen. Sie wird bei betriebenen IT-Systemen mit Datenübertragungen in ein unsicheres Drittland von den Verantwortlichen die vom EuGH verlangten Feststellungen zur Rechtslage und zur Datenschutzpraxis in dem empfangenden Drittland einfordern und die zusätzlichen Schutzmaßnahmen gegen einen unverhältnismäßigen Zugriff durch die Behörden des Drittlandes überprüfen. Vom Verantwortlichen wird sie Planungen oder Abwägungen einfordern, welche alternativen IT-Systeme und -Dienste er geprüft hat, welche Maßnahmen er zum Eigenbetrieb ausländischer IT-Systeme durch ihn selbst oder europäische Auftragsverarbeiter er erwogen hat oder welche Konfigurationen er gewählt hat, um Datenübermittlungen in ein Drittland ohne ausreichendes Datenschutzniveau auszuschließen. Um diese Prüfungen durchführen und zu datenschutzgerechten Lösungen gelangen zu können, wird die Aufsichtsbehörde mit kooperationswilligen Verantwortlichen nach geeigneten Alternativen und passenden Konfigurationen der IT-Systeme suchen.

Angesichts der Verbreitung von IT-Systemen mit Datenübertragungen in Drittländer ohne ausreichendes Datenschutzniveau ist die Aufgabe, die Vorgaben des Schrems II-Urteils durchzusetzen, extrem groß. Um dennoch dieser Aufgabe trotz der begrenzten Ressourcen gerecht werden zu können, muss jede Aufsichtsbehörde eine Strategie entwickeln, die Aufgabe und Handlungsmöglichkeiten in Einklang bringt. Ich versuche, dieser Aufgabe vor allem dadurch gerecht zu werden, indem ich auf Aufklärung und Beratung setze und auf die Vorbildwirkung gelungener Beispiele. Lösungen sind vor allem in den Bereichen zu finden, in denen geeignete Alternativen bestehen, die die geforderten Funktionen erbringen, ohne dass personenbezogene Daten in ein unsicheres Drittland übertragen werden müssen. Ein solcher Bereich mit großer Breitenwirkung und vorhandenen Alternativen und Gestaltungsmöglichkeiten sind Videokonferenzsysteme. Vor allem auf diese richtet sich

in einem ersten Schritt mein Blick, wenn es darum geht, die Vorgaben des Schrems II-Urteils umzusetzen (s. Ziff. 4). Andere Bereiche werden folgen.

3.2
Digitale Souveränität und erfolgreiche Digitalisierungsprojekte

Digitale Souveränität bedeutet, dass Verantwortliche die Möglichkeit haben, ihren datenschutzrechtlichen Pflichten nachzukommen. Sie ist somit eine notwendige Voraussetzung für eine datenschutzrechtskonforme Digitalisierung. Die Sicherstellung digitaler Souveränität und die frühzeitige Berücksichtigung des Datenschutzes bilden somit gemeinsame wesentliche Erfolgsfaktoren für erfolgreiche Digitalisierungsprojekte.

Durch die COVID-19-Pandemie kam es zu Beginn des Jahres 2020 zu einer besonderen Ausnahmesituation. Diese führte und führt weiterhin zu tiefgreifenden Veränderungen im täglichen Leben und hat Auswirkungen auf unterschiedlichste Lebensbereiche. Für eine Vielzahl an Herausforderungen mussten kurzfristig Lösungen gefunden, umgesetzt und bereitgestellt werden. Im Kontext von IT-Lösungen wurde der Fokus bei der Realisierung daher in vielen Fällen zunächst auf Schnelligkeit und die Bereitstellung unverzichtbarer Basisfunktionalitäten gelegt. Andere Aspekte wurden diesen Zielen untergeordnet und häufig zurückgestellt. Dies galt insbesondere auch für den Datenschutz.

Insgesamt ist seit Ausbruch der COVID-19-Pandemie ein anhaltender Digitalisierungsschub festzustellen, der sich im Berichtszeitraum fortsetzte. Auch für den kommenden Berichtszeitraum rechne ich mit einer fortschreitenden Digitalisierung. Im öffentlichen Bereich zeigt sich dies in besonderem Maße im Zusammenhang mit der Umsetzung des Onlinezugangsgesetzes (OZG). Dieses verpflichtet den Bund, die Länder und die Kommunen bis zum Ende des Jahres 2022 eine Vielzahl ihrer Verwaltungsleistungen online zur Verfügung zu stellen und somit zu digitalisieren.

Datenschutzfreundliche Digitalisierung

Anders als in der Ausnahmesituation zu Beginn der COVID-19-Pandemie müssen in Digitalisierungsprojekten datenschutzrechtliche Anforderungen von Beginn an durchgängig berücksichtigt und umgesetzt werden. Dies gilt in besonderem Maße für die Planung, die Anforderungsermittlung sowie für etwaige Ausschreibungen. Schließlich werden hier die Grundlagen und somit das Fundament für alle weiteren Projektphasen sowie für den Betrieb, die Wartung, die Nutzung und die Weiterentwicklung der Projektergebnisse gelegt.

Die umfassende Berücksichtigung des Datenschutzes als integraler Bestandteil von Digitalisierungsprojekten begünstigt die Entwicklung datenschutzrechtskonformer Lösungen. So können durch diese Herangehensweise die Grundsätze des Datenschutzes gemäß Art. 5 DS-GVO im Sinne des Datenschutzes durch Systemgestaltung und durch datenschutzfreundliche Voreinstellungen gemäß Art. 25 DS-GVO umgesetzt werden. Diese Herangehensweise bietet die Chance einer datenschutzfreundlichen Digitalisierung und somit der Wahrung der Rechte und Freiheiten der von der Digitalisierung betroffenen Personen in besonderem Maße.

Daher ist eine notwendige Voraussetzung für eine datenschutzfreundliche Digitalisierung die kontinuierliche und konsequente Berücksichtigung datenschutzrechtlicher Fragestellungen in allen Phasen von Digitalisierungsprojekten. Hierzu müssen von Beginn an in ausreichendem Maße kompetente Ressourcen eingeplant und im weiteren Projektverlauf auch bereitgestellt werden. Dies gilt sowohl für die operative als auch für die Lenkungsebene von Projekten.

Demgegenüber birgt eine zu späte Berücksichtigung datenschutzrechtlicher Anforderungen vielfältige Risiken für den Projekterfolg. Dies gilt sowohl für juristische Fragestellungen als auch in technischer Hinsicht. Aus juristischer Perspektive kann beispielsweise die Vertragsgestaltung mit Dienstleistern, die gemäß Art. 28 DS-GVO personenbezogene Daten im Auftrag verarbeiten, problematisch sein. Dies ist etwa der Fall, wenn Dienstleister diese oder weitere im Rahmen der Verarbeitung anfallende personenbezogene Daten auch für eigene Zwecke nutzen wollen. Probleme auf technischer Ebene können etwa auftreten, falls im Rahmen der Softwareentwicklung der Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DS-GVO nur unzureichend umgesetzt oder die Gewährleistung der Betroffenenrechte gemäß Kapitel III DS-GVO technisch nicht unterstützt wird.

Je später derartige Probleme erkannt werden, desto kosten- und zeitintensiver ist in der Regel ihre Behebung, sofern dies überhaupt noch möglich ist. Empfindliche Zeit- und Budgetüberschreitungen sind insbesondere bei einer Erkennung in späten Projektphasen häufig die Folge. Im ungünstigsten Fall kann es hierdurch auch zu Projektabbrüchen kommen. Wird in einem solchen Fall die Verantwortung für das Scheitern eines Projektes „dem Datenschutz“ zugeschrieben, verdeckt dies die tatsächlichen Ursachen und verhindert das Ziehen der erforderlichen Lehren für zukünftige Projekte.

Digitale Souveränität als Grundlage datenschutzfreundlicher Digitalisierung

Eine wesentliche Grundlage einer datenschutzrechtskonformen Digitalisierung ist die digitale Souveränität. Sie ist gegeben, wenn der Verantwortliche IT-Systeme nutzen kann, die ihm ermöglichen, datenschutzrechtliche Anforderungen zu erfüllen (s. Ziff. 3.1).

Hierzu gehört vor allem die Möglichkeit, die Grundsätze des Datenschutzes gemäß Art. 5 DS-GVO im Sinne des Datenschutzes durch Systemgestaltung und durch datenschutzfreundliche Voreinstellungen gemäß Art. 25 DS-GVO umzusetzen und die Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO zu gewährleisten.

Bei der Einführung neuer Verarbeitungstätigkeiten gilt es für Verantwortliche zunächst zu prüfen, ob und in welchem Ausmaß die Möglichkeit besteht, digital souverän zu agieren. Ein Beispiel für das Vorhandensein digitaler Souveränität ist der Bereich der Videokonferenzsysteme (VKS). Hier sind verschiedene Anbieter von VKS-Software und VKS-Diensten am Markt vertreten. Für Verantwortliche, die VKS einsetzen wollen, stehen hierdurch unterschiedliche Angebote für ein breites Spektrum an möglichen Einsatzszenarien zur Verfügung. Verantwortliche sind im Bereich der VKS folglich in der Lage, digital souverän zu agieren (s. Ziff. 4). Ich erwarte, dass Verantwortliche ihre digitale Souveränität in diesem Bereich nutzen, um datenschutzrechtskonforme Lösungen bereitzustellen und einzusetzen.

Einschränkungen können beispielsweise gegeben sein, falls der Markt für Software-Produkte oder IT-Dienste im betroffenen Bereich nur sehr begrenzt ist oder einzelne Anbieter sogar eine (Quasi-)Monopolstellung innehaben. Auch das Bestehen von Wechselbeziehungen oder Abhängigkeiten zu anderen Verarbeitungstätigkeiten kann für einen Verantwortlichen zu einer Einschränkung der digitalen Souveränität führen. Dies gilt häufig in besonderem Maße, falls Lock-in-Effekte zum Tragen kommen. Die Gründe für derartige Effekte können vielfältiger Art sein. Sie können etwa in einer starken Bindung an einzelne Anbieter liegen, falls stark auf deren proprietäre Produkte gesetzt wird. Wurden hierauf aufbauend Anpassungen oder Individualentwicklungen durchgeführt, verstärken diese Investitionen die Bindung zusätzlich. Ferner können sich Mitarbeitende an die eingesetzten Produkte und Dienste gewöhnt haben, sodass ein Wechsel hier auf mehr oder minder starke Vorbehalte stoßen dürfte. Insgesamt dürfte eine Verfestigung des Lock-in zunehmen, je länger er Bestand hat.

Als Folge hieraus ist die Entscheidungsfreiheit eines von einem Lock-in betroffenen Verantwortlichen stark eingeschränkt oder sogar faktisch nicht mehr vorhanden. Falls ein Lock-in-Effekt zu nicht-datenschutzrechtskonformen

Verarbeitungstätigkeiten führt, können Verantwortliche ihren Verpflichtungen gemäß Art. 24 DS-GVO nicht mehr nachkommen. Spätestens in diesem Fall ist ein partieller oder sogar vollständiger Verlust digitaler Souveränität festzustellen.

Verantwortliche sind einem solchen Verlust an digitaler Souveränität nicht machtlos ausgeliefert. Kurzfristig lässt sich ein Lock-in-Effekt allerdings in der Regel nicht signifikant verringern oder gar aufheben. Vielmehr bedarf es hierzu häufig eines längeren Prozesses und nicht unerheblicher Anstrengungen seitens des Verantwortlichen. In einem ersten Schritt sollten bestehende Abhängigkeiten überprüft, evaluiert und bewertet werden. Aufbauend auf der so erlangten Übersicht, können dann Maßnahmen zur Wiedererlangung der digitalen Souveränität umgesetzt werden, etwa durch den gezielten Abbau von Abhängigkeiten. Parallel sollte bei neuen IT-Projekten immer auch deren Einfluss auf die digitale Souveränität des Verantwortlichen mitberücksichtigt werden. So können sich beispielsweise eine bewusste Diversifizierung bei eingesetzten Produkten und IT-Diensten sowie die Verwendung offener Standards positiv auswirken.

Gerade im öffentlichen Bereich setzen die Wiedererlangung digitaler Souveränität und deren Aufrechterhaltung den entsprechenden politischen Willen, die Bereitschaft, diesen umzusetzen, und eine nicht unerhebliche Ausdauer voraus. Hierbei müssen nicht zuletzt auch die Mitarbeiterinnen und Mitarbeiter der öffentlichen Verwaltung mitgenommen werden.

Veraltete Technologie

Die digitale Souveränität Verantwortlicher ist nicht auf die Einführung neuer Verarbeitungstätigkeiten beschränkt. Vielmehr sind auch bei bestehenden Verarbeitungstätigkeiten das Vorliegen und das Fortbestehen digitaler Souveränität sicherzustellen. Dies gilt zuallererst in Bezug auf die Umsetzung der Grundsätze des Datenschutzes gemäß Art. 5 DS-GVO.

In Bezug auf die Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO kommt dem Stand der Technik eine besondere Bedeutung zu. Kommen zur Verarbeitung personenbezogener Daten beispielsweise Software- oder Hardware-Komponenten zum Einsatz, für die keine Updates mehr bereitgestellt werden, so ist in der Regel davon auszugehen, dass diese Komponenten auch nicht mehr dem Stand der Technik entsprechen. Auch können sich die Rahmenbedingungen für den Einsatz von Technologien mit der Zeit stark verändern. Dies kann zur Folge haben, dass eine vormals als datenschutzrechtskonform einsetzbare Technologie nunmehr als nicht mehr dem Stand der Technik entsprechend anzusehen ist. Ein Beispiel hierfür ist

der Einsatz von Telefax für die Übermittlung personenbezogener Daten (s. Ziff. 18.5).

In Art. 32 Abs. 1 lit. d DS-GVO wird hinsichtlich der Sicherheit der Verarbeitung gefordert, dass „ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“ umgesetzt und betrieben werden sollte. Dementsprechend berücksichtigt die DS-GVO hier explizit Veränderungen der Rahmenbedingungen von Verarbeitungstätigkeiten. Hieraus folgt, dass Verantwortliche diesen Veränderungen begegnen und bei Bedarf aktiv Anpassungen an den von ihnen ergriffenen technischen und organisatorischen Maßnahmen (TOM) ergreifen müssen, um die Sicherheit der Verarbeitung auch weiterhin zu gewährleisten. Können für einen erforderlichen Anpassungsbedarf keine entsprechenden Anpassungsmöglichkeiten zur Gewährleistung der Datenschutzrechtskonformität identifiziert werden, so ist für die zugehörige Verarbeitungstätigkeit ein Verlust der digitalen Souveränität festzustellen. Schließlich hat ein Verantwortlicher in diesem Fall keine Wahlmöglichkeiten hinsichtlich der von ihm ergriffenen TOMs mehr.

Beim Einsatz veralteter und nicht mehr datenschutzrechtskonform einsetzbarer Technologien leistet deren Ersatz einen Beitrag zur Wiedererlangung verlorengegangener digitaler Souveränität. Ein solcher Ersatz muss jedoch nicht in allen Fällen zwingend in einem Schritt erfolgen. So könnte der Einsatz veralteter Technologien gegebenenfalls sukzessive reduziert werden. Auch könnte eine veraltete Technologie für verschiedene Verarbeitungstätigkeiten durch unterschiedliche Technologien ersetzt werden. Dies dürfte gerade bei Technologien wie Telefax ein vielversprechender Ansatz sein.

Unterstützung durch meine Behörde

Gerade im öffentlichen Bereich erreichte mich im Berichtszeitraum eine Vielzahl an Anfragen zu unterschiedlichen Digitalisierungsprojekten. Auch im Zusammenhang mit dem Einsatz von veralteter Technologie wurde ich von mehreren Verantwortlichen kontaktiert. Solche Beratungsanfragen erreichten meine Behörde zunehmend in frühen Projektphasen oder sogar noch vor Projektbeginn. Diese Entwicklung begrüße ich sehr, da die Erfolgsaussichten meiner Beratung erheblich steigen, je früher meine Mitarbeiterinnen und Mitarbeiter einbezogen werden.

Sie stehen in Digitalisierungsprojekten gern mit ihrem Fachwissen und ihren Erfahrungen beratend zur Seite. Diese Beratung umfasst jedoch nicht die Übernahme operativer Aufgaben in Projekten, etwa die Zuarbeit für Ausschreibungsunterlagen oder die Erstellung von konkreten Anforderungen.

Auch kann im Rahmen einer Beratung keine Prüfung oder gar Freigabe von Dokumenten erfolgen. Hieraus würden sich Interessenkonflikte mit meiner aufsichtsbehördlichen Aufgabe ergeben. Hinzu kommt, dass eine derartige Unterstützung die kapazitären Möglichkeiten meiner Behörde bei weitem übersteigen würde. Gleiches gilt für eine nicht selten gewünschte offizielle Freigabe von Verarbeitungstätigkeiten als Ganzes. Für eine solche umfassende Bestätigung der Datenschutzkonformität einer Verarbeitungstätigkeit wären datenschutzrechtliche Zertifizierungen gemäß Art. 42 DS-GVO ein geeignetes Mittel.

Beispiele für erfolgreiche Beratungen im Rahmen von Digitalisierungsprojekten finden sich auch in diesem Tätigkeitsbericht (s. Ziff. 4.2, 7.3, 9.7, 13.2 und 17.4). Die in der Vergangenheit erfolgreiche Beratungspraxis möchte ich auch in Zukunft fortsetzen. Gleichzeitig möchte ich Verantwortliche dazu aufrufen, in ihren Digitalisierungsprojekten für ausreichende Kompetenz und Ressourcen im Bereich des Datenschutzes zu sorgen, sofern dies nicht bereits erfolgt.

Fazit

Das Vorhandensein digitaler Souveränität ist ein wesentlicher Erfolgsfaktor für eine datenschutzfreundliche und erfolgreiche Digitalisierung. Hier bildet die digitale Souveränität eine notwendige Voraussetzung für eine datenschutzrechtskonforme Ausgestaltung und Umsetzung von Tätigkeiten zur Verarbeitung personenbezogener Daten. Daher sollten gerade Verantwortliche im öffentlichen Bereich die Herstellung und Aufrechterhaltung ihrer digitalen Souveränität aktiv betreiben und gestalten. Zusätzlich sollten vorhandene Defizite im Bereich der digitalen Souveränität aufgedeckt und behoben werden. Mir ist bewusst, dass diese Aufgaben von den Verantwortlichen andauernde Anstrengungen erfordern und alle Beteiligten vor Herausforderungen stellen. Gleichzeitig sehe ich in der digitalen Souveränität eine unverzichtbare Grundlage für den Schutz der Rechte und Freiheiten der von der Verarbeitung ihrer Daten betroffenen Personen.

Auch in Zukunft ist von einer fortschreitenden Digitalisierung auszugehen. Gerade im öffentlichen Bereich werden im kommenden Berichtszeitraum mehrere Projekte realisiert werden, nicht zuletzt auch im Zusammenhang mit der Umsetzung des OZG. Meine Mitarbeiterinnen und Mitarbeiter werden auch weiterhin tatkräftig beratend unterstützen und hierdurch ihren Beitrag zur erfolgreichen und datenschutzfreundlichen Digitalisierung in Hessen leisten.

4. Videokonferenzsysteme

Soweit die Aufgaben, IT-Systeme zur Bewältigung der Corona-Pandemie zu nutzen (s. Ziff. 2) und in der Nutzung von IT-Systemen eine digitale Souveränität zu erreichen, die den Verantwortlichen ermöglicht, die Vorgaben des Datenschutzrechts zu erfüllen (s. Ziff. 3), in Widerspruch geraten können, wird das Spannungsverhältnis bei der Nutzung von Videokonferenzsystemen (VKS) wie in einem Brennglas in besonderer Weise deutlich. Sie ist für das Ziel, die Funktionen eines Unternehmens oder einer Behörde trotz des Gebots, körperliche Kontakte zu vermeiden, aufrechtzuerhalten, unverzichtbar. Sie führt aber bei vielen weit verbreiteten VKS, die von US-amerikanischen Anbietern stammen, zu Übertragungen von personenbezogenen Daten in die USA und damit zu einem Verlust von Grundrechten der betroffenen Personen (s. Ziff. 3.1). Lösungen für datenschutzkonforme Zustände müssen durch die Auswahl und Gestaltung von VKS gefunden werden. Dieses Kapitel zeigt sowohl die Entwicklung hin zu dem Spannungsverhältnis zwischen rechtlichen Vorgaben, technologischer Abhängigkeit und sozialem Bedarf an Technologienutzung als auch die Möglichkeiten der Problemlösung durch datenschutzkonforme Systemgestaltung.

4.1 Videokonferenzsysteme – Gekommen um zu bleiben

Videokonferenzsysteme (VKS) haben seit Beginn der COVID-19-Pandemie massiv an Bedeutung gewonnen. Während die Zurückstellung datenschutzrechtlicher Fragestellungen zu Beginn der Pandemie vertretbar *erschien, ist nunmehr von Verantwortlichen zu erwarten, dass sie sich nachweisbar auf den Weg hin zum Einsatz datenschutzrechtskonformer Lösungen gemacht haben. Meine Behörde wird zukünftig ein besonderes Augenmerk auf den Datenschutz bei der Nutzung von VKS richten.*

Im beruflichen und privaten Umfeld nutzen wir eine Vielzahl unterschiedlicher Medien zur zwischenmenschlichen Kommunikation. Zu den klassischen Kommunikationsmedien wie Briefpost, Telefon oder E-Mail kamen in der Vergangenheit weitere Kommunikationsformen hinzu, etwa der Einsatz von Messenger-Diensten. Diese sind auf sehr breite Akzeptanz gestoßen und haben sich in sehr kurzer Zeit ihren festen Platz in unserem Kommunikationsverhalten gesichert.

Für den Bereich der direkten Kommunikation können VKS eingesetzt werden. Bei einem VKS handelt es sich um ein Kommunikationsmedium, bei dem sich zwei oder mehr Beteiligte virtuell zu einer Videokonferenz zusammenfinden

und mittels Übertragung von Audio- und Videodaten zeitgleich (synchron) miteinander kommunizieren. Diese Kernfunktionalität wird je nach eingesetztem VKS um weitere Funktionalitäten ergänzt, etwa die Möglichkeit, gemeinsam Präsentationen zu betrachten, Bildschirminhalte zu teilen, kooperativ an einem Whiteboard zu arbeiten oder Textnachrichten auszutauschen. Insgesamt bieten VKS eine Vielzahl an Möglichkeiten für die direkte zwischenmenschliche Kommunikation, auch über große Distanzen hinweg.

Aus datenschutzrechtlicher Perspektive sind beim Einsatz von VKS zunächst die sogenannten „Inhaltsdaten“ von Bedeutung, also beispielsweise Audio- und Videodaten sowie ausgetauschte Nachrichten und Dokumente. Bei diesen ist zu beachten, dass sie nicht nur Konferenzteilnehmende betreffen müssen, sondern sich auch auf Dritte beziehen können. Hinzu kommen personenbezogene Daten, die zur Bereitstellung des VKS und zur Durchführung von Videokonferenzen erforderlich sind, sowie Daten, die im Rahmen der Nutzung generiert werden. All diese Daten sind bei einer datenschutzrechtlichen Betrachtung zu berücksichtigen.

I. VKS in der COVID-19-Pandemie und danach

Mit Beginn der COVID-19-Pandemie sahen sich öffentliche und nichtöffentliche Stellen seit Anfang des Jahres 2020 u. a. mit der Herausforderung konfrontiert, direkte persönliche Kontakte auf ein Minimum zu reduzieren. Dies galt nicht nur für Mitarbeitende, Stichwort „Home-Office“. So mussten beispielsweise Schulen Konzepte für verteilten Unterricht entwickeln und umsetzen, um auf Schulschließungen zu reagieren, Stichwort „Distanzunterricht“ (s. Ziff. 4.2). Als Lösung bot sich vielfach der Einsatz von VKS an. Aufgrund der damaligen Ausnahmesituation und vor allem des dringenden Bedarfs, sehr kurzfristig Lösungen zu etablieren, traten nicht zuletzt auch datenschutzrechtliche Anforderungen in den Hintergrund. Meine Behörde hat diese besonderen Herausforderungen berücksichtigt und entsprechend gehandelt. So wurde beispielsweise eine zeitlich befristete Duldung für die Nutzung von VKS und von weiteren Anwendungen für den Einsatz in Schulen ausgesprochen (s. Ziff. 4.2).

Der übergangsweise Einsatz von datenschutzrechtlich problematischen VKS war vor dem Hintergrund der besonderen Ausnahmesituation gerechtfertigt. Ein solcher Einsatz darf jedoch nicht auf Dauer erfolgen. Dementsprechend mussten und müssen Verantwortliche die Übergangszeit nutzen und sich auf den Weg hin zum Einsatz datenschutzrechtskonformer VKS machen. Mit Fortschreiten der COVID-19-Pandemie wurde zudem absehbar, dass die Nutzung von VKS in vielen Bereichen auch über die Pandemie hinaus erfolgen dürfte. Insofern müssen Verantwortliche nun vom dauerhaften

Einsatz von VKS ausgehen. Diese Erkenntnis verstärkt den Bedarf nach der Bereitstellung datenschutzrechtskonformer Lösungen. Die Umstellung auf ein datenschutzrechtskonformes VKS kann nicht ad hoc erfolgen und bedarf einer gründlichen Vorbereitung sowie einer entsprechenden Umsetzung.

II. Datenschutzgerechte Gestaltung von VKS

Um VKS datenschutzrechtskonform einzusetzen, müssen diese unterschiedliche Anforderungen erfüllen. Diese erstrecken sich von der Planung und Umsetzung eines Projekts zur Bereitstellung eines VKS über den Betrieb und die Wartung eines solchen bis hin zu dessen Nutzung. Diese Anforderungen gelten unabhängig davon, ob öffentliche oder nicht öffentliche Stellen VKS einsetzen.

Als Ausgangspunkt dienen die vorgesehenen Einsatzszenarien eines VKS. Aus datenschutzrechtlicher Sicht muss für jedes Einsatzszenario eine Rechtsgrundlage zur Verarbeitung personenbezogener Daten gemäß Art. 6 Abs. 1 DS-GVO vorliegen. Auch muss gemäß der nach Art. 5 Abs. 1 lit. c DS-GVO erforderlichen Datenminimierung überprüft werden, ob ein zur Zweckerreichung gleichwertiges und aus datenschutzrechtlicher Sicht milderes Mittel verfügbar ist. Sollte ein solches Mittel verfügbar sein, wäre dies dem eines VKS vorzuziehen.

Im Rahmen der Ermittlung alternativer Produkte und IT-Dienste für die Umsetzung eines VKS sollten neben funktionalen Anforderungen, wie die zu unterstützende Teilnehmerzahl oder die Verfügbarkeit bestimmter Funktionalitäten, Aspekte des Datenschutzes umfassend Berücksichtigung finden. Schließlich werden durch die Auswahl das Fundament und die Rahmenbedingungen für das zukünftige VKS und somit für die Möglichkeiten zur datenschutzrechtskonformen Ausgestaltung desselben gelegt. Eine besondere Bedeutung hat hierbei das Betriebsmodell, vom dem maßgebliche datenschutzrechtliche Auswirkungen ausgehen. Zur Auswahl stehen der Selbstbetrieb, der Betrieb durch einen externen Dienstleister und die Nutzung eines Online-Dienstes. Sofern kein vollständiger Selbstbetrieb erfolgt, müssen die datenschutzrechtlichen Anforderungen für die Einbindung von Auftragsverarbeitern erfüllt werden. Hierzu zählt auch der Abschluss eines Vertrags gemäß Art. 28 Abs. 3 DS-GVO. Kommt es darüber hinaus – wie bei vielen verbreiteten VKS – zu einer Übermittlung personenbezogener Daten in Drittländer, so sind zusätzlich die Anforderungen aus Kapitel V der DS-GVO zu erfüllen. Dabei ist insbesondere zu beachten, dass die Anforderungen des EuGH in seiner Entscheidung vom 16. Juli 2020 (Schrems II) zum Datentransfer in die USA eingehalten werden müssen (s. Ziff. 3.1).

Nachdem die Entscheidung für ein Produkt oder einen IT-Dienst und das zugehörige Betriebsmodell getroffen wurde, müssen bei der Realisierung des VKS die Grundsätze für die Verarbeitung personenbezogener Daten gemäß Art. 5 DS-GVO durch entsprechende technische und organisatorische Gestaltung des Systems gemäß Art. 25 DS-GVO umgesetzt werden. Hinzu kommen technische und organisatorische Maßnahmen (TOMs) zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO. Die getroffenen Gestaltungen und die ergriffenen TOMs müssen im Rahmen von Betrieb und Wartung regelmäßig auf ihre Wirksamkeit hin überprüft, bewertet und evaluiert werden, um den datenschutzrechtskonformen Einsatz des VKS dauerhaft sicherzustellen.

Für die datenschutzrechtskonforme Durchführung einer Videokonferenz muss diese zunächst durch deren Veranstalter entsprechend eingerichtet werden. Hierzu zählen beispielsweise die Aktivierung einer Inhaltsverschlüsselung und die Deaktivierung nicht benötigter Funktionalitäten. Ferner müssen die Teilnehmenden vorab mit angemessenen Informationen über die datenschutzrelevanten Rahmenbedingungen der Videokonferenz versorgt werden. Auch müssen gegebenenfalls gemäß Art. 7 DS-GVO wirksame Einwilligungen eingeholt werden. Schließlich muss während der Durchführung einer Videokonferenz die Einhaltung datenschutzrechtlicher Vorgaben sichergestellt werden.

Nähere Informationen zu den Anforderungen an den datenschutzrechtskonformen Einsatz von VKS können der Orientierungshilfe Videokonferenzsysteme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) entnommen werden (DSK, Orientierungshilfe Videokonferenzsysteme, https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/OH-Videokonferenzsysteme.pdf). Ergänzend habe ich auf der Website meiner Behörde allgemeine Informationen zum Einsatz von VKS sowie Informationen für Entscheidungsträger und Nutzende bereitgestellt (Videokonferenzsysteme – Allgemein, https://datenschutz.hessen.de/datenschutz/it-und-datenschutz/allgemein).

III. Auf dem Weg zu datenschutzgerechten VKS

Im kommenden Berichtszeitraum wird meine Behörde ein verstärktes Augenmerk auf die datenschutzkonforme Ausgestaltung von VKS richten. Verantwortliche in Hessen rufe ich daher dazu auf, sich – sofern noch nicht erfolgt – auf den Weg hin zum datenschutzrechtskonformen Einsatz von VKS zu machen. Ich gehe davon aus, dass die bereitgestellten Informationen und Orientierungshilfen auf diesem Weg wertvolle Unterstützung bieten. Darüber hinaus haben meine Mitarbeiterinnen und Mitarbeiter gerade im

Bereich der öffentlichen Verwaltung unterschiedliche Projekte beratend begleitet und werden dies auch weiterhin tun. Der eingeschlagene Weg sollte von Verantwortlichen dokumentiert werden und gegenüber meiner Behörde nachgewiesen werden können.

Abschließend ist festzustellen, dass VKS aller Voraussicht nach über die COVID-19-Pandemie hinaus ihren festen Platz im Portfolio der Kommunikationsmedien vieler Verantwortlicher behalten werden. Auch ist mit einer Weiterentwicklung der zugrunde liegenden Software und IT-Dienste zu rechnen, um den steigenden Anforderungen der Nutzerinnen und Nutzer gerecht zu werden und Lösungen für neue Anwendungsfelder zu bieten. Anbieter von VKS sind hierbei dazu aufgerufen, die Belange des Datenschutzes zu berücksichtigen und so Verantwortliche in die Lage zu versetzen, datenschutzrechtskonforme VKS bereitzustellen und zu nutzen. Ich erwarte, dass insbesondere Anbieter von Online-Diensten in Drittstaaten ihre diesbezüglichen Anstrengungen unvermindert fortsetzen und intensivieren.

4.2
Einsatz von Videokonferenzsystemen in Schulen und Hochschulen

Seit Beginn der Corona-Pandemie Anfang des Jahres 2020 haben, aufgrund von Kontaktbeschränkungen, Videokonferenzsysteme (VKS) stark an Bedeutung in Schulen und Hochschulen gewonnen, um beispielsweise den Unterricht oder die Vorlesungen, aber auch Prüfungen unter pandemischen Bedingungen durchzuführen. Sie in einen datenschutzgerechten Betrieb zu überführen, ohne ihre Funktion für Schulen und Hochschulen zu beeinträchtigen, war im Berichtszeitraum eine zentrale Aufgabe für mich und meine Behörde.

I. Herausforderungen für die Schulen

Am Freitag, den 13. März 2020, änderte sich durch den coronabedingten Lockdown der Unterrichtsalltag für die Schülerinnen und Schüler wie auch die Lehrkräfte an den hessischen Schulen radikal. Das Schulleben, wie es bis zu diesem Zeitpunkt alle kannten und schätzten, wurde von dem einen auf den anderen Tag auf den Kopf gestellt. Als Maßnahme der Kontaktreduzierung zur Eindämmung der Ausbreitung des Corona-Virus blieben die Schulen geschlossen und Lehrkräfte mussten sich Konzepte überlegen, wie die Schülerinnen und Schüler in den eigenen vier Wänden unterrichtet werden können. Viele Schulen suchten nach Möglichkeiten, wie man den Unterricht so, wie er vor Ort in der Schule üblich war, unter den nun gegebenen Bedingungen bestmöglich durchführen kann, und kamen zu dem Ergebnis, dass

dies am besten mit Hilfe von VKS erreicht werden könne. Hierzu benötigten die Schulen ein VKS, das auch bei einem Internetanschluss mit einer niedrigen Bandbreite und Latenz stabil funktioniert, im Umgang selbsterklärend ist, da wenig bis keine Zeit für die Schulung der Lehrkräfte wie auch der Schülerinnen und Schüler blieb, und den nötigen Komfort bietet, damit der Unterricht attraktiv gestaltet werden konnte. Aufgrund der Kürze der Zeit, die für die Auswahl eines geeigneten VKS blieb, wurde der Datenschutz häufig in den Hintergrund gestellt und es wurden oftmals die bereits am Markt etablierten VKS – meist solche mit US-amerikanischen Betreibern – für den Fernunterricht verwendet.

Der HBDI hat im Interesse der Bekämpfung der Corona-Pandemie Ende März 2020 übergangsweise den Einsatz von VKS in Schulen weitgehend für alle zur Verfügung stehenden Anwendungen auf Grundlage von Art. 6 Abs. 1 UAbs. 1 lit. d und e DS-GVO geduldet, auch wenn deren Datenschutzkonformität noch nicht abschließend geklärt war. Damit verbunden war die Aufforderung an das Hessische Kultusministerium (HKM), für eine datenschutzkonforme Lösung bis zum Beginn des Schuljahres 2020/2021 zu sorgen. Als Reaktion hierauf haben sich etliche Personalräte, Lehrkräfte, Eltern wie auch Schülerinnen und Schüler an mich gewandt, die sich darüber besorgt zeigten, dass in Schulen gegebenenfalls VKS zum Einsatz kommen sollen, die den geltenden datenschutzrechtlichen Anforderungen nicht entsprechen können, und haben den datenschutzkonformen Umgang mit ihren im Rahmen der Nutzung des jeweiligen VKS verarbeiteten Daten eingefordert.

In der Folge konnte das HKM die vom HBDI gesetzte Frist nicht einhalten, weil es wegen der Größe des Projekts, für mehr als 2000 Schulen ein zentral vom Land bereitgestelltes VKS (Landes-VKS) zu etablieren, sowie dem Erfordernis, möglicherweise eine europaweite Ausschreibung vornehmen zu müssen, zu zeitlichen Verzögerungen gekommen war. Da zum damaligen Zeitpunkt eine Realisierung des Projekts Landes-VKS erst im ersten Halbjahr 2021 als möglich erschien, ist der HBDI im August 2020 der Bitte des HKM nachgekommen und hat die Duldung der Nutzung möglicherweise nicht datenschutzkonformer VKS bis maximal 31. Juli 2021 verlängert. Die weitere Duldung wurde allerdings mit den Bedingungen verbunden, dass a) jede Schule im konkreten Einzelfall vorab die Erforderlichkeit der Nutzung eines VKS prüft und b) soweit der zuständige Schulträger eine datenschutzkonforme Anwendung als „on premise“-Lösung anbietet, diese zwingend einzusetzen ist.

Weitere Unterstützung bekamen die Schulen vom HBDI Anfang des Jahres 2021, indem dieser Hinweise für einen sicheren Unterricht mit VKS gab und

ein Muster-Formular zur Einwilligung für die Nutzung von VKS in Schulen auf seiner Homepage zur Verfügung stellte.

Ende März 2021 erinnerte ich daran, dass die Duldung des HBDI für die Nutzung insbesondere US-amerikanischer VKS am 31. Juli 2021 ausläuft. Zum damaligen Zeitpunkt war davon auszugehen, dass bis zum Beginn des neuen Schuljahres 2021/2022 mit dem Landes-VKS eine Anwendung zur Verfügung steht, die sowohl den technischen als auch den datenschutzrechtlichen Anforderungen entspricht. Damit wäre der weitere Einsatz nicht datenschutzkonformer VKS weder erforderlich noch datenschutzrechtlich zulässig gewesen. Dieser Hinweis hat die verschiedensten Reaktionen im Kultusbereich hervorgerufen. Viele Beteiligte begrüßten diesen Schritt ausdrücklich, insbesondere dass im Ergebnis eine rechtssichere datenschutzkonforme Unterrichtung der Schülerinnen und Schüler möglich sein soll. Ich sah mich aufgrund der Klarstellung, die Duldung nun tatsächlich auslaufen zu lassen, aber auch starker Kritik ausgesetzt. Insbesondere dass auch das Programm Microsoft Teams hiervon betroffen sein soll, ließ viele Beteiligte aufschrecken. Es machte sich die Sorge unter den Schülerinnen und Schülern, Eltern, Lehrkräften, aber auch Schulträgern breit, dass ohne dieses System an vielen Schulen ein gegebenenfalls notwendig werdender Fernunterricht nicht realisierbar sei. Diese Sorge war insbesondere vor dem Hintergrund zu sehen, dass zu Anfang der Pandemie im sogenannten ersten Lockdown viele schlechte Erfahrungen mit einigen anderen Produkten gemacht worden waren, da es häufig zu Verbindungsabbrüchen während des Fernunterrichts gekommen sei. Außerdem hatten sich die Nutzerinnen und Nutzer nun nach eigenen Angaben mühsam mit einem VKS vertraut gemacht und hatten beispielsweise Microsoft Teams aufgrund seiner vielfältigen technischen Möglichkeiten schätzen gelernt. Auch Schulträger sind an mich herangetreten und haben mich darüber in Kenntnis gesetzt, dass sie viele teure Lizenzen beschafft hätten, die durch die avisierte Vorgehensweise wertlos würden. Die Kritik wurde in verschiedenen Formen an mich herangetragen und reichte von einer Landtagspetition, eingereicht von einem Schüler, über an mich adressierte Schreiben von Schulträgern und verschiedenen Interessenvertretungen, bis hin zu vielfältigen Eingaben besorgter Schülerinnen und Schüler, Eltern und Lehrkräften bei meiner Behörde.

Dieses Unverständnis vieler betroffener Personen sowie der Wunsch, der größten Sorge der Beteiligten entgegenzutreten, dass ein neues, seitens des HKM zu Verfügung gestelltes VKS nicht den Umfang an Funktionen mitbringen würde, wie es beispielsweise Microsoft Teams tut, haben mich veranlasst, Mitte Juni eine Klarstellung zu Microsoft Teams und dem Auslaufen der Duldung zu veröffentlichen. Wie auch in den Schreiben an die Schulträger, die Interessenvertretungen und bei der Beantwortung der Landtagspetition,

habe ich darauf aufmerksam gemacht, dass von dem Auslaufen der Duldung lediglich die Videokonferenzfunktion von Microsoft Teams betroffen ist. Andere Funktionen von MS Teams (z. B. Chatfunktion, Austausch von Dokumenten) und auch die übrigen Teilprodukte von Microsoft 365 können im pädagogischen Bereich durch Schulen zunächst weiterverwendet werden, bis eine Prüfung der Datenschutzkonformität von Microsoft 365 durch die Konferenz der unabhängigen Datenschutzbeauftragten Klarheit gebracht hat. Ich habe in diesem Rahmen aber auch klargestellt, dass seitens des HKM bis zum 31. Juli 2021 ein landesweites VKS zur Verfügung gestellt werden sollte und damit für die Schulen in Hessen die sachliche Grundlage entfällt, andere VKS zu nutzen.

Auch habe ich nochmals auf die aktuelle Rechtslage hingewiesen. Diese wird derzeit insbesondere durch das sog. „Schrems II-Urteil“ des Europäischen Gerichtshofs (EuGH) geprägt. Nach diesem Urteil ist die Übermittlung von personenbezogenen Daten europäischer Bürgerinnen und Bürger in Staaten, die nicht den Datenschutzstandard der DS-GVO garantieren, ohne zusätzliche Schutzvorkehrungen untersagt (s. ausführlich Ziff. 3.1). Mit der Nutzung des Landes-VKS würden hessische Schulen (vorbehaltlich meiner Prüfung) die vom EuGH verlangten Standards erfüllen.

Selbstverständlich war ich mir auch darüber im Klaren, dass es aufgrund schulspezifischer Prozesse in den einzelnen Schulen des Landes zu unterschiedlichen zeitlichen Verläufen bei der Migration kommen könnte. Deshalb war ich bereit, die hieraus resultierenden Verzögerungen mitzutragen, soweit erkennbar ist, dass die Schulen den Weg hin zu einem datenschutzkonformen VKS eingeschlagen haben. Allerdings ging ich zum damaligen Zeitpunkt davon aus, dass die Schulen bis spätestens zum Ende des ersten Schulhalbjahres 2021/22 die Umstellung vollzogen haben.

Anfang Juli 2021 wurde ich nun darüber informiert, dass sich die Einführung des landeseinheitlichen VKS für die Schulen des Landes Hessen voraussichtlich weiter verzögern wird. Die Verzögerung beruht auf einem Nachprüfungsantrag im Vergabeverfahren. Durch die Verzögerung ließ sich der ursprünglich avisierte Termin zur Einführung des Landes-VKS nicht halten. Durch den Umstand, dass das Landes-VKS nicht zum 1. August 2021 in Betrieb genommen werden konnte, hat sich nichts an dem Auslaufen der Duldung für die Nutzung insbesondere US-amerikanischer VKS geändert. Mir ist daran gelegen, einen datenschutzrechtskonformen Zustand in diesem Bereich herzustellen und die andauernde Einschränkung der Grundrechte Betroffener so gering wie möglich zu halten. Genauso wie die hessischen Schulen hatte ich darauf vertraut, dass das Landes-VKS zu Beginn des Schuljahres 2021/2022 zur Verfügung stehen wird und durch die Schulen

genutzt werden kann. Ich habe nun auf die veränderten Umstände reagiert und angekündigt, dass ich keine Maßnahmen gegenüber Schulen ergreifen werde, denen eine Umstellung auf ein datenschutzkonformes Videokonferenzsystem nicht möglich ist, weil das Landes-VKS noch nicht zur Verfügung steht. Sobald die Schulen das Landes-VKS nutzen können, erwarte ich aber, dass eine Umstellung durch die Schulen auf das Landes-VKS zügig erfolgen wird. Auch hier werde ich die Umstände in den einzelnen Schulen berücksichtigen und eine Umstellungsphase ab Zurverfügungstellung des Landes-VKS durch das HKM einräumen.

Am 27. Dezember 2021 hat das Oberlandesgericht Frankfurt festgestellt, dass das Vergabeverfahren fehlerhaft war. Das HKM muss daher erneut ein Vergabeverfahren durchführen. Ein Landes-VKS ist daher wohl erst zum Beginn des Schuljahres 2022/2023 zu erwarten. Dies ändert an meiner grundsätzlichen Haltung jedoch nichts, den Schulen die Zeit einzuräumen, die sie benötigen, um auf ein landesweites, einheitliches und datenschutzkonformes VKS zu wechseln.

II. Herausforderungen für die Hochschulen

Auch die Hochschulen des Landes Hessen wurden Mitte März 2020 mit den Bedingungen der Corona-Pandemie konfrontiert und das Leben der Studierenden und Lehrenden veränderte sich erheblich. Statt in einem vollen Hörsaal gemeinsam mit den Kommilitonen an den Lehrveranstaltungen teilzunehmen, mussten aufgrund der Kontaktbeschränkungen andere Wege gefunden werden, um die erforderliche wissenschaftliche Kommunikation durchzuführen. Wie auch bei den Schulen lag es nahe, VKS einzusetzen, um die Lehrveranstaltungen in die Studierendenwohnungen zu bringen. Auch hier wurde bei der Auswahl der eingesetzten Systeme der Datenschutz oftmals nicht in den Vordergrund gestellt, sondern auf am Markt etablierte Anbieter zurückgegriffen, die einen hohen Komfort und eine stabile Verbindung versprachen.

Seitens des damaligen HBDI wurde im Frühjahr 2020 gegenüber den Hessischen Hochschulen klargestellt, dass die Möglichkeiten, die den Schulen bei der Auswahl eines VKS eingeräumt wurden, auch für den Hochschulbereich gelten. Dies bedeutete, dass im Interesse der flexiblen Bekämpfung der Corona-Pandemie auch in diesem Bereich übergangsweise der Einsatz von VKS auf Grundlage von Art. 6 Abs. 1 UAbs. 1 lit. d und e DS-GVO weitgehend geduldet wurde, auch wenn deren Datenschutzrechtskonformität noch nicht abschließend geklärt war.

In den folgenden Monaten haben mein Vorgänger und ich die Hochschulen und auch das Hessische Ministerium für Wissenschaft und Kunst (HMWK)

zu den Themen des datenschutzkonformen Einsatzes von VKS und auch der datenschutzkonformen Durchführung von Fernprüfungen durch die Hessischen Hochschulen beraten.

Anfang Juli 2021 habe ich mich schließlich mit einem Brief an die Präsidien der Hessischen Hochschulen gewandt und darauf hingewiesen, dass die, nach dem Gleichbehandlungsprinzip auch für die Hessischen Hochschulen geltende, Duldung für den Einsatz von fast allen gängigen VKS in Schulen zum 31. Juli 2021 ausläuft. Auch in Hessischen Hochschulen muss auf Grund der aktuellen Rechtslage für rechtsgemäße Verhältnisse bei der Nutzung von VKS gesorgt werden. VKS sind nach diesen Vorgaben entweder so zu betreiben, dass sichergestellt ist, dass keine personenbezogenen Daten ohne ausreichende Schutzvorkehrungen in unsichere Drittstaaten übertragen werden, oder sie sind durch andere datenschutzrechtskonforme VKS zu ersetzen (s. näher Ziff. 3.1 und 4.1). Außerdem müssen Hochschulen die eingesetzten VKS datenschutzgerecht gestalten. Sie müssen vor allem so gestaltet sein, dass sie den Anforderungen des Art. 25 Abs. 1 DS-GVO nach einer datenschutzgerechten Systemgestaltung gerecht werden, und so konfiguriert sein, dass sie den Anforderungen nach datenschutzfreundlichen Voreinstellungen gemäß Art. 25 Abs. 2 DS-GVO entsprechen. Außerdem müssen sie die Sicherheit der Datenverarbeitung gemäß Art. 32 DS-GVO dauerhaft gewährleisten. Um den hessischen Hochschulen genügend Zeit für die notwendigen Umstellungen und Anpassungen zu geben und um die Planungen und Vorbereitungen für das Wintersemester 2021/2022 nicht zu gefährden, werde ich vor dem Ende des Wintersemesters von mir aus keine Aufsichtsmaßnahmen ergreifen.

Auch in Zukunft werde ich die Hochschulen in den Umstellungsprozessen beraten und unterstützen und damit auf datenschutzkonforme Zustände hinwirken. Hochschulen, die für die Umstellung auf rechtsgemäße Zustände länger benötigen als bis zum Ende des Wintersemesters 2021/22, können sich an mich wenden und wir können gemeinsam nach Möglichkeiten eines DS-GVO-konformen Betriebs geeigneter VKS suchen. Hierbei werden wir auch in der Abwägung zwischen hochschulspezifischen Anforderungen an VKS und den Anforderungen des Grundrechtsschutzes geeignete Lösungen finden. Bereits zum jetzigen Zeitpunkt stehe ich mit dem HMWK und Vertretern der Hochschulen in einem engen Austausch zu der Frage, welche VKS in welcher Ausgestaltung in Zukunft verwendet werden können, um den hohen Anforderungen der Hochschullehre an ein solches System gerecht zu werden, ohne den Datenschutz außer Acht zu lassen.

III. Technische Anforderungen an datenschutzkonforme VKS

Ein VKS, das für den Einsatz an den Schulen und Hochschulen des Landes Hessen geeignet sein soll, muss bestimmte Anforderungen aus technischer Sicht des Datenschutzes erfüllen können. Diese ergeben sich aus den speziellen Bedingungen, die der Einsatz in solchen Institutionen mit sich bringt.

Bei der Verwendung eines VKS werden verschiedene Kategorien personenbezogener Daten verarbeitet, die für die Nutzerinnen und Nutzer nur teilweise direkt erkennbar sind. Während die Verarbeitung von Bild- und Tondaten, die einen Personenbezug zulassen, offensichtlich ist, ist dies bei denjenigen Daten, die „im Hintergrund“ verarbeitet werden, nicht unbedingt der Fall. Dazu gehören solche Daten, deren Verarbeitung unerlässlich ist, damit eine Videokonferenz überhaupt zustande kommen kann, wie z. B. die IP-Adressen der Teilnehmenden oder eine Information darüber, wer mit wem kommuniziert. Aber auch solche Daten, die der Anbieter des VKS aus anderen Gründen verarbeitet, gehören dazu, etwa die sogenannten Telemetriedaten, die dem Anbieter bestimmte Rückschlüsse über das Verhalten des VKS oder über das Endgerät, mit dem das VKS genutzt wird, liefern können.

Inwiefern solche Daten tatsächlich anfallen, einen Personenbezug erlauben oder gar aus Sicht des Datenschutzes problematisch sein können, kommt dabei auf die jeweiligen Umstände an. Zum einen verarbeiten unterschiedliche VKS auch unterschiedliche Daten. Schulen und Hochschulen müssen sich daher bereits bei der Auswahl eines geeigneten Systems Klarheit darüber verschaffen, welche Daten dies sind. Zum anderen werden Art und Menge an Daten auch durch die organisatorischen Umstände der Bereitstellung, des Betriebs und der Wartung des VKS beeinflusst.

Grundsätzlich werden drei Betreibermodelle unterschieden, die vom Verantwortlichen hinsichtlich der an der Datenverarbeitung beteiligten Stellen und der dort jeweils verarbeiteten personenbezogenen Daten berücksichtigt werden müssen:

1. Beim Selbstbetrieb eines VKS beschaffen Verantwortliche (Hochschulen, Schulen oder Schulträger) die zugrunde liegende Software sowie gegebenenfalls ergänzende Services und Dienstleistungen. Installation, Konfiguration, Betrieb und Wartung erfolgen vollständig durch den Verantwortlichen und auf Basis seiner eigenen IT-Systeme.
2. Beim Betrieb eines eigenen, internen VKS durch einen externen Dienstleister wird auf dessen Ressourcen und Expertise zurückgegriffen. Art, Umfang und Ausgestaltung der übernommenen Aufgaben können von Fall zu Fall stark variieren. Je nach Umfang der erbrachten Dienstleistungen und der konkreten Ausgestaltung im Einzelfall kann es sich bei

dem externen Dienstleister dann um einen Auftragsverarbeiter gemäß Art. 4 Abs. 8 DS-GVO handeln, wodurch die Anforderungen des Art. 28 DS-GVO, beispielsweise bezogen auf den Abschluss eines Auftragsverarbeitungsvertrags, zu berücksichtigen sind.

3. Schließlich kann zur Durchführung von Videokonferenzen auf einen Online-Dienst zurückgegriffen werden. Hierbei handelt es sich in der Regel um ein standardisiertes Angebot eines Dienstleisters, der die Videokonferenz entweder als Telekommunikationsanbieter unmittelbar auf dem Markt anbietet oder für die Verantwortlichen als Auftragsverarbeiter gemäß Art. 4 Abs. 8 DS-GVO agiert.

Erfolgt die Bereitstellung und der Betrieb des VKS unter Einsatz eines Auftragsverarbeiters, eines externen Dienstleisters oder eines Online-Dienstes, so muss der Verantwortliche berücksichtigen, welche personenbezogenen Daten der Anbieter des VKS über die technische Ermöglichung der Konferenz hinaus zu eigenen Zwecken verarbeitet. Eine solche Verarbeitung bedarf in jedem Fall einer gesonderten Rechtsgrundlage sowohl seitens des Anbieters wie auch seitens des Verantwortlichen bezogen auf die Übermittlung an den Anbieter. Das Vorliegen einer solchen gesetzlichen Erlaubnis ist für die Verwendung von VKS in Schulen und Hochschulen schwer zu begründen.

Neben der Bereitstellung und dem Betrieb des VKS ist auch die Art der Nutzung zu betrachten. Wird das VKS über ein privates Endgerät der Lernenden und Lehrenden genutzt, so erlaubt dies dem Anbieter des VKS unter Umständen durch zusätzliche Informationen (etwa die Bezeichnung des Geräts oder andere installierte Software) genauere Rückschlüsse über die Identität und das Verhalten der verwendenden Person. Findet eine Nutzung aus dem privaten Netzwerk der Person heraus statt, z. B. im Rahmen des Fernunterrichts, so lassen sich ähnliche Schlüsse gegebenenfalls aus den Verbindungsdaten ziehen, die bei einer Nutzung aus dem Netz der Bildungsinstitution heraus ein höheres Maß an Anonymisierung gewähren würden.

In der Regel kann die Schule oder Hochschule auf die Verarbeitung personenbezogener Daten durch das VKS Einfluss nehmen. Über entsprechende Konfigurationen muss sie sicherstellen, dass die Grundsätze der Verarbeitung personenbezogener Daten gemäß Art. 5 DS-GVO, wie etwa die Datenminimierung, gewährleistet sind. Solche Konfigurationen können beispielsweise die Deaktivierung der Übermittlung nicht benötigter Telemetriedaten an den Anbieter des VKS oder das Ausblenden des Videohintergrunds bei der Videoübertragung aus dem privaten Wohn- und Lebensbereich von Lernenden beinhalten.

S. näher zu den Anforderungen an VKS: https://datenschutz.hessen.de/datenschutz/it-und-datenschutz/allgemein.

5. Europa, Internationales

Zusammenarbeit mit anderen europäischen Aufsichtsbehörden

Mit Inkrafttreten der DS-GVO haben sich, wie bereits im 47., 48. und 49. Tätigkeitsbericht geschildert, zahlreiche Neuerungen für die Zusammenarbeit der Aufsichtsbehörden in Deutschland und Europa ergeben. Die DS-GVO verpflichtet die europäischen Datenschutzaufsichtsbehörden, in Fällen grenzüberschreitender Datenverarbeitungen im Bemühen, einen Konsens zu erzielen (Art. 60 Abs. 1 Satz 1 DS-GVO), eng zu kooperieren. Um den kommunikativen und organisatorischen Mehraufwand zu bewältigen, der sich aus der Intensivierung der Zusammenarbeit ergibt, hat der HBDI im Jahr 2019 die Stabsstelle Europa und Internationales eingerichtet, die als Bindeglied zwischen dem HBDI und verschiedenen Stellen außerhalb Hessens in Deutschland, Europa und der Welt fungiert.

Verfahren der Kooperation und Kohärenz nach Kapitel VII DS-GVO

Alle bei mir eingehenden Beschwerden, Anfragen und Meldungen von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DS-GVO werden in den Fachreferaten zunächst daraufhin überprüft, ob eine grenzüberschreitende Verarbeitung vorliegt, die die Pflicht zur Zusammenarbeit mit anderen europäischen Aufsichtsbehörden auslöst. Eine grenzüberschreitende Verarbeitung liegt gemäß Art. 4 Nr. 23 DS-GVO vor, wenn der Verantwortliche oder der Auftragsverarbeiter in mehreren Mitgliedstaaten niedergelassen ist und die Verarbeitung in mehreren dieser Niederlassungen erfolgt oder wenn es nur eine einzelne Niederlassung in der EU gibt, aber die Verarbeitung erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann.

Nach dem mit der DS-GVO eingeführten Konzept des sog. One-Stop-Shop ist bei grenzüberschreitenden Datenverarbeitungen eine Aufsichtsbehörde – grundsätzlich die Aufsichtsbehörde am Ort der Hauptniederlassung des Verantwortlichen oder Auftragsverarbeiters (Art. 56 Abs. 1 DS-GVO) – als federführende Aufsichtsbehörde einziger Ansprechpartner des Verantwortlichen und Auftragsverarbeiters (Art. 56 Abs. 6 DS-GVO). D. h., ein Unternehmen muss sich wegen ein und derselben Datenverarbeitung nur mit einer Aufsichtsbehörde auseinandersetzen. Dies bedeutet aber nicht, dass die federführende Aufsichtsbehörde alleine entscheidet. Vielmehr wirken neben der federführenden Aufsichtsbehörde auch alle weiteren betroffenen Aufsichtsbehörden an der Entscheidungsfindung mit. „Betroffen“ („concerned“) sind nach Art. 4 Nr. 22 DS-GVO alle Aufsichtsbehörden, in deren Hoheitsgebiet der Verantwortliche oder der Auftragsverarbeiter niedergelassen ist,

individuell betroffene Personen („data subjects“) ihren Wohnsitz haben oder bei denen eine Beschwerde eingereicht wurde.

Die Zusammenarbeit, Abstimmung und Kommunikation in grenzüberschreitenden Verwaltungsverfahren erfolgt elektronisch über das sog. IMI-System (Internal Market Information System, deutsch: Binnenmarkt-Informationssystem). Die Arbeitssprache im IMI-System ist Englisch.

Beschwerden, Meldungen nach Art. 33 DS-GVO und sonstige Anfragen mit grenzüberschreitendem Bezug, die bei den europäischen Datenschutzbehörden eingehen, werden in einem ersten Schritt in einem Verfahren nach Art. 56 DS-GVO zur Feststellung der federführenden und betroffenen Aufsichtsbehörden in das IMI-System eingestellt. Dabei sind der Sachverhalt für die anderen Aufsichtsbehörden aufzubereiten, in englischer Sprache zusammengefasst zu schildern und die mutmaßlich federführende Aufsichtsbehörde sowie die mutmaßlich betroffenen Aufsichtsbehörden anzugeben. Alle Aufsichtsbehörden haben dann Gelegenheit, den Fall zu prüfen und sich als federführende oder betroffene Aufsichtsbehörde zu melden.

Wird im Art. 56-Verfahren festgestellt, dass die europäische Federführung beim HBDI liegt, da z. B. der Verantwortliche in Hessen niedergelassen ist, leitet die Stabsstelle Europa und Internationales die über das IMI-System eingegangene Beschwerde, Anfrage oder Meldung nach Art. 33 DS-GVO nebst weiterer Unterlagen an das jeweilige Fachreferat beim HBDI weiter, das dann nach eingehender Prüfung des Sachverhalts den Kontakt zum Verantwortlichen aufnimmt.

Für den Fall, dass die Federführung für eine beim HBDI eingegangene Beschwerde, Anfrage oder Meldung nach Art. 33 DS-GVO bei einer anderen europäischen Aufsichtsbehörde liegt, übermittelt die Stabsstelle Europa und Internationales diese über das IMI-System zur Bearbeitung an die jeweils federführend zuständige Behörde. Hierzu müssen die Eingabe sowie alle weiteren zur Bearbeitung notwendigen Unterlagen und sachdienlichen Informationen ins Englische übersetzt werden. Als betroffene Aufsichtsbehörde wirkt der HBDI in diesen Verfahren an der Entscheidungsfindung mit und bleibt im sog. One-Stop-Shop Ansprechpartner für die Eingebenden und informiert in regelmäßigen Abständen über den Stand der Bearbeitung.

Die federführende Aufsichtsbehörde und die betroffenen Aufsichtsbehörden arbeiten im Kooperationsverfahren eng zusammen und versuchen, einen Konsens zu erzielen (Art. 60 Abs. 1 DS-GVO). Die federführende Aufsichtsbehörde prüft den Fall und legt den betroffenen Aufsichtsbehörden nach Abschluss der Ermittlungen einen Beschlussentwurf vor (Art. 60 Abs. 3 Satz 2 DS-GVO). Gegen diesen Beschlussentwurf können die betroffenen Aufsichtsbehörden bei Bestehen von Bedenken Einspruch einlegen (Art. 60 Abs. 4 DS-GVO).

Bei unlösbaren Meinungsverschiedenheiten wird die Angelegenheit dem Europäischen Datenschutzausschuss (EDSA) im Kohärenzverfahren nach Art. 63 DS-GVO zur verbindlichen Entscheidung vorgelegt.

Ziel dieser von der DS-GVO vorgesehenen Arbeitsweise ist eine einheitliche Anwendung der DS-GVO durch die Aufsichtsbehörden in ganz Europa. Da die DS-GVO für diesen Mechanismus der europäischen Zusammenarbeit keine Bagatellgrenze vorsieht, greift sie bei einer Vielzahl von alltäglichen Beschwerden, die den HBDI erreichen.

Gestiegene Fallzahlen und erhöhter Prüfungsaufwand

Die Zahl der über das IMI-System gemeldeten Beschwerden, Anfragen, Art. 33-Meldungen und Verfahren der gegenseitigen Amtshilfe stieg im Berichtszeitraum im Vergleich zu den Vorjahren weiter deutlich an.

Europäisches Verfahren	Anzahl 2019	Anzahl 2020	Anzahl 2021
Art. 56-Verfahren gesamt	633	812	1419
Art. 56-Verfahren mit Betroffenheit	17	32	47
Art. 56-Verfahren mit Federführung	4	7	16
Art. 61-Verfahren (Amtshilfe)	65	26	92

Im Berichtszeitraum waren von der Stabsstelle Europa und Internationales insgesamt 1419 im IMI-System eingetragene Art. 56-Verfahren auf eine mögliche Betroffenheit oder Federführung zu prüfen. In 47 dieser Verfahren hat die Stabsstelle Europa und Internationales den HBDI als „betroffen“ gemeldet, sich in der Folge inhaltlich mit der Angelegenheit befasst und an der Entscheidungsfindung mitgewirkt. In weiteren 16 Verfahren hat der HBDI die Bearbeitung der Beschwerde als federführende Aufsichtsbehörde übernommen.

Auch die Zahl der Verfahren der gegenseitigen Amtshilfe nach Art. 61 DS-GVO nimmt weiter zu. Oft betreffen die von einer anderen europäischen Aufsichtsbehörde an mich gestellten Amtshilfeersuchen konkrete grenzüberschreitende Verwaltungsverfahren, in denen ich für die anfragende Behörde gegenüber einem Verantwortlichen oder Auftragsverarbeiter im Hoheitsgebiet tätig werden soll. Vermehrt werden aber auch allgemeine Rechts- und Auslegungsfragen zu DS-GVO-Themen – ohne Bezug zu einem konkreten Fall – an uns herangetragen, die dann im Haus durch die Fachreferate oder

auf nationaler Ebene in entsprechenden Arbeitskreisen koordiniert und beantwortet werden. Es ist zu erwarten, dass sich dieser Trend auch im kommenden Jahr weiter fortsetzt.

Genehmigung von Binding Corporate Rules

Neben den über das IMI-System zu bearbeitenden grenzüberschreitenden Verwaltungsverfahren lag ein weiterer Schwerpunkt der Tätigkeit der Stabsstelle Europa und Internationales im Berichtsjahr in der Prüfung und Genehmigung von Binding Corporate Rules (deutsch: verbindliche interne Datenschutzvorschriften, kurz: BCR) nach Art. 47 DS-GVO, die sich – auch aufgrund des sog. Schrems II-Urteils des EuGH vom 16. Juli 2020 (Rs. C-311/18) und der Unwirksamkeit des EU-US Privacy Shields – als Transferinstrument für Datenübermittlungen in Drittländer wachsender Beliebtheit erfreuen.

BCR sind komplexe Vertragswerke mit Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein multinationaler Konzern verpflichtet, um personenbezogene Daten innerhalb der Unternehmensgruppe in sog. Drittländer (d. h. Länder außerhalb des Europäischen Wirtschaftsraumes) zu übermitteln, die an und für sich kein angemessenes Datenschutzniveau bieten.

BCR werden in einem europaweiten Kooperationsverfahren von Aufsichtsbehörden mehrerer Mitgliedstaaten gemeinsam geprüft. Auch hierbei agiert eine Aufsichtsbehörde als Federführung (sog. BCR Lead) und koordiniert das Verfahren. Eine oder zwei weitere Aufsichtsbehörden werden unterstützend als sog. Co-Prüfer tätig. Zudem müssen seit Inkrafttreten der DS-GVO und in Abkehr vom vorherigen sog. Mutual Recognition-Verfahren alle europäischen Aufsichtsbehörden gemäß dem in Art. 63 DS-GVO festgelegten Konsistenzmechanismus einbezogen werden und Gelegenheit zur Prüfung und Kommentierung der BCR erhalten, bevor der EDSA eine Stellungnahme hierzu abgibt.

Erst wenn diese Stellungnahme positiv ausfällt, also im EDSA eine Mehrheit der Mitgliedstaaten für die Genehmigung der BCR stimmt, kann die federführende Behörde einen Genehmigungsbescheid erlassen, der dann auch für die übrigen Aufsichtsbehörden bindend ist. Alle europäischen Aufsichtsbehörden werden damit stärker in die Verantwortung und Pflicht genommen. Das Ziel der Verfahrensneuerung ist eine stärkere Vereinheitlichung der BCR, womit aber auch ein neuer und erhöhter Prüfungsaufwand für die Aufsichtsbehörden einhergeht.

Da Hessen häufig Standort von großen global agierenden Unternehmensgruppen ist, bin ich sehr häufig in BCR-Genehmigungsverfahren als

Federführung innerhalb Deutschlands beteiligt oder gar europaweit als sog. BCR Lead federführend zuständig. Derzeit sind in Europa knapp 300 Anträge auf Genehmigung von BCR anhängig. Für 13 dieser BCR-Verfahren bin ich europaweit als BCR Lead federführend tätig. Davon wurden fünf BCR-Genehmigungsverfahren infolge des Brexits von der britischen Datenschutzaufsichtsbehörde als neuer BCR Lead übernommen. In 27 weiteren BCR-Verfahren habe ich die Federführung innerhalb Deutschlands übernommen. Damit bin ich deutschlandweit für die meisten BCR-Verfahren zuständig.

Mitarbeit in Gremien der DSK und auf Ebene des EDSA

Neben den Aufgaben in grenzüberschreitenden Verwaltungsverfahren und bei der Prüfung von BCR arbeitet die Stabsstelle Europa und Internationales auf nationaler und europäischer Ebene weiter in verschiedenen Arbeitsgremien der DSK und Arbeitsgruppen des EDSA mit.

Auf europäischer Ebene hat die Stabsstelle die Vertretung Deutschlands in der International Transfers Subgroup fortgeführt. Die Subgroup befasst sich mit internationalen Datenübermittlungen und sämtlichen Themen und Fragen, die sich auf diesem Gebiet stellen. Neben der Teilnahme an regelmäßigen Sitzungen der Subgroup und BCR-Sessions engagiert sich die Stabsstelle Europa und Internationales in diversen Drafting Teams und Task Forces und berichtet gemeinsam mit Kolleginnen und Kollegen des LDA Bayern und des BfDI den deutschen Aufsichtsbehörden stetig über die Arbeit der Subgroup und die Entwicklungen auf dem Gebiet des europäischen und internationalen Datenschutzrechtes. Die Rückmeldungen aus den deutschen Aufsichtsbehörden bringt der HBDI als Ländervertreter dann wiederum in die Diskussionen auf europäischer Ebene ein. So gelingt es z. B., Einfluss auf vom EDSA zu verabschiedende Leitlinien und Empfehlungen zu nehmen, die dann für die spätere aufsichtsbehördliche Tätigkeit maßgeblich und richtungsweisend werden.

Neben den Informationen aus der International Transfers Subgroup sichtet die Stabsstelle Europa und Internationales aber auch sämtliche Posteingänge aus den übrigen Subgroups des EDSA (z. B. Arbeitspapiere und -ergebnisse, Tagesordnungen und Protokolle), die die Stabsstelle zum Teil per E-Mail, aber auch elektronisch über die Web-Plattform Confluence erreichen und an die jeweils zuständigen Fachreferate beim HBDI – sei es zur bloßen Information und Kenntnis oder gegebenenfalls weiteren Veranlassung – weitergeleitet werden müssen. Dies versetzt die Fachreferate in die Lage, sich aktiv und gestaltend in die Arbeiten auf europäischer Ebene einzubringen und z. B. durch Mitarbeit in ad-hoc-Gruppen oder frühzeitige Kommentierung von Pa-

pieren, die sich im Entwurfsstadium befinden, Einfluss auf den europäischen Meinungsbildungsprozess zu nehmen.

Auch auf nationaler Ebene hat die Stabsstelle Europa und Internationales die Mitarbeit in Arbeitsgremien der DSK fortgeführt. So übernimmt die Stabsstelle weiterhin die Leitung des bundesweiten Arbeitskreises Organisation und Struktur. Der Arbeitskreis unterstützt die Arbeit der DSK in wichtigen organisatorischen Fragestellungen und entwickelt Konzepte und Prozesse zur besseren Verzahnung der Arbeit auf deutscher und europäischer Ebene. Ein weiterer Themenkreis, mit dem sich der Arbeitskreis intensiv beschäftigt, sind Fragen, die sich aus der europäischen Zusammenarbeit nach Kapitel VII der DS-GVO ergeben, einschließlich der konkreten Abwicklung dieser Verfahren im IMI-System. Neben der Organisation regelmäßiger Arbeitskreissitzungen hat die Stabsstelle Europa und Internationales hier stetig die Entwicklungen auf nationaler und europäischer Ebene zu beobachten und zu bewerten, um den Kolleginnen und Kollegen der anderen deutschen Aufsichtsbehörden berichten zu können. Daneben nimmt die Stabsstelle Europa und Internationales für den HBDI weiterhin auch an den Sitzungen des Arbeitskreises Internationaler Datenverkehr teil, der Fragen der grenzüberschreitenden Datenübermittlung im Blick hat.

6. Bußgeldverfahren, Gerichtsverfahren

6.1
Juridifizierung der Arbeit des HBDI

Vor dem 25. Mai 2018 war die Arbeit in der Datenschutzaufsichtsbehörde geprägt von Prüfungen, wenigen förmlichen Maßnahmen und einem kleinen Kanon an Bußgeldtatbeständen in mäßiger Höhe. Seit Geltung der DS-GVO steht mit Art. 58 DS-GVO eine breite Palette an Befugnissen zur Verfügung. Deren Wirkungsweise und Zusammenspiel sind inzwischen vertraut, die Datenschutzaufsicht hat unter Segeln Fahrt aufgenommen und den Kurs auf wirkungsvolle Durchsetzung der DS-GVO eingeschlagen.

Trotz aller theoretischer Vorbereitung war im Vorfeld noch nicht in vollem Umfang abzuschätzen, wie die neue Verwaltungspraxis unter der DS-GVO tatsächlich aussehen würde. Die neuen Vorschriften zu Maßnahmen und Sanktionen aus Art. 58 DS-GVO haben das Verwaltungshandeln der Datenschutzaufsicht stark verändert. Neben einer starken Ausweitung der Aufgaben einer Aufsichtsbehörde ist die Verwaltungspraxis förmlicher geworden. Das Aufsichtsverfahren ist heute geprägt vom klassischen Verwaltungshandeln nach dem Verwaltungsverfahrensgesetz. Anhörungen, Bescheide und die Festsetzung von Zwangsgeldern gehören zum Alltag. Ist die Schwelle überschritten und die Entscheidung für die Durchführung eines Bußgeldverfahrens gefallen, kommt noch die neue Komponente des wirksamen, verhältnismäßigen und abschreckenden Bußgeldes in Millionenhöhe hinzu. Das Bußgeldverfahren richtet sich nach den nationalen Normen im OWiG und der StPO, die durch § 40 BDSG ergänzt werden.

Die stärker in Grundrechte eingreifenden Durchsetzungsmaßnahmen und insbesondere die Bußgeldfestsetzungen führen ebenso wie die Verpflichtung, Beschwerden zu bearbeiten und zu bescheiden, zu einem erheblichen Anstieg der Gerichtsverfahren, die sich gegen die Aufsichtsbehörde richten. Dies wiederum wirkt auf die Arbeit der Behörde zurück, die ihre Verfahren so betreiben und dokumentieren und ihre Entscheidungen so begründen muss, dass sie einer gerichtlichen Nachprüfung standhalten. Dies wird im Folgenden am Beispiel der Bußgeldverfahren näher erläutert.

6.2
Entwicklungen zu den Bußgeldern

Der weite Bußgeldrahmen und die zeitgleiche Europäisierung der Verfahren hat neues Interesse und große Aufmerksamkeit an den Entscheidungen der

Aufsicht hervorgerufen. Das betrifft das Interesse der betroffenen Personen und Unternehmen, die den hohen Bußgeldern eine große Aufmerksamkeit schenken, aber auch das durch die Kooperationspflichten nach Kapitel VII der DS-GVO hervorgerufene Interesse der Aufsichtsbehörden anderer Mitgliedstaaten. Hat ein Unternehmen in mehreren Mitgliedstaaten eine Dependance, dann wird die Notwendigkeit einer Harmonisierung der Rechtsanwendung der DS-GVO besonders deutlich. Begleitet wird das Ganze durch ein hohes Interesse der Öffentlichkeit an der Sanktionierung durch Bußgelder.

Gerade im Jahr 2021 haben Bußgeldverfahren nach der DS-GVO durch die Höhe der ausgesprochenen Bußgelder neue Dimensionen erreicht. Aber nicht nur die Höhe der Bußgelder spielt eine große Rolle. Für die Arbeit der Bußgeldstelle in meinem Haus sind zwei weitere Entwicklungen von besonderer Relevanz: die Bedeutung des Kohärenzverfahrens im Bußgeldverfahren sowie Fragen im Zusammenhang mit der Veröffentlichung von Bußgeldern in der Presse.

Das Bußgeld im Streitbeilegungsverfahren

Im Jahr 2021 sind die höchsten Bußgelder wegen Datenschutzverstößen seit der Geltung der DS-GVO verhängt worden. Die luxemburgische Aufsichtsbehörde hat 746 Mio. Euro gegen einen großen Onlinehandel und die irische Aufsichtsbehörde hat 225 Mio. Euro gegen einen Messaging-Dienst verhängt. Beide Verfahren waren grenzüberschreitende Verfahren. Es waren daher die Regelungen der Zusammenarbeit nach Art. 60 ff. DS-GVO zu berücksichtigen.

Die Entscheidungsvorschläge mussten sich der kritischen Prüfung der europaweit betroffenen Aufsichtsbehörden stellen. In dem Bußgeldverfahren gegen den großen Onlinehandel war auch die hessische Bußgeldstelle zur Stellungnahme aufgefordert. Nach Sichtung des über 100 Seiten umfassenden englischsprachigen Entscheidungsvorschlags war zwischen den deutschen Aufsichtsbehörden eine zeitnahe englischsprachige Stellungnahme zu koordinieren, die dann an die federführende Stelle weitergeleitet wurde. Dieser Fall ging nicht ins Kohärenzverfahren.

Bei dem Verfahren gegen den Messaging-Dienst, an dem Hessen selbst nicht beteiligt war, kam es zu einem Streitbeilegungsverfahren vor dem EDSA nach Art. 65 Abs. 1 lit. a DS-GVO i. V. m. Art. 60 Abs. 4 DS-GVO. Es wurden acht Einsprüche verhandelt, denen sich die irische Aufsichtsbehörde nicht angeschlossen hatte. Im Beschluss wurde die irische Aufsichtsbehörde unter anderem angewiesen, das Bußgeld gegen den Messaging-Dienst zu erhöhen. Dem 89-seitigen Streitbeilegungsbeschluss des EDSA sind weitere Einzelheiten zu den Einsprüchen und die Entscheidung zu entnehmen (https://

edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_en.pdf).

Die Entscheidung des EDSA gibt durch seine Veröffentlichung zugleich für den Verantwortlichen den Blick auf das Innere des Kohärenzverfahrens frei. Es macht deutlich, dass die Höhe des Bußgeldes nicht allein von der Entscheidung einer Aufsichtsbehörde abhängig ist.

Für die Praxis der Aufsichtsbehörden bedeutet dies, dass ein Aufsichtsverfahren und das möglicherweise anschließende Bußgeldverfahren einen sehr hohen zeitlichen Aufwand haben bei i. d. R. kurzen Reaktionsfristen. Der Beschlussentwurf der abschließenden Entscheidung muss ins Englische übersetzt werden und so verfasst sein, dass dieser auch ohne Kenntnis der Verfahrensvorschriften im jeweiligen Land verständlich ist. Gerade im Jahr 2021 ist die Tragweite der Veränderung des Verfahrens bei der Datenschutzaufsicht deutlich geworden.

Bußgelder in der Presse

Im Jahr 2021 ist auch die Frage stärker in den Blickpunkt gerückt, ob über ein Bußgeldverfahren in der Öffentlichkeit berichtet werden kann oder sollte, und wenn ja, in welcher Form dies geschehen darf. Die Bußgelder können ihre abschreckende Wirkung auch für Dritte, vom Verfahren nicht Betroffene, nur entfalten, wenn die Öffentlichkeit von ihnen erfährt. Ein Weg der bisherigen Veröffentlichung ist die Aufnahme einer Fallbeschreibung in den jährlichen Tätigkeitsbericht. Dabei handelt es sich um anonymisierte Beschreibungen ausgewählter Fälle.

Bei der neuen Dimension der Bußgelder wurde gerade in der letzten Zeit von einigen Aufsichtsbehörden der Weg der Pressemitteilung als eine weitere Möglichkeit zur Information der Öffentlichkeit diskutiert und genutzt. Eine gesetzliche Regelung hierzu gibt es weder in der DS-GVO noch in den deutschen Vorschriften zum Datenschutz. Daher ist aus meiner Sicht eher Zurückhaltung geboten. Angefeuert wurde die Diskussion um die Veröffentlichung von Bußgeldern in der Presse durch die Entscheidung des OVG Münster im Eilverfahren – Beschluss OVG Münster vom 17. Mai 2021 – Az.: 13 B 333/21. Die Entscheidung befasst sich mit der Zulässigkeit der Veröffentlichung eines Bußgeldes der Bundesnetzagentur.

In einem Eilverfahren hatte das OVG Münster über die Erfolgsaussichten eines geltend gemachten öffentlich-rechtlichen Unterlassungsanspruchs zu entscheiden. Das OVG kommt unter anderem zu dem Ergebnis, dass öffentliche Stellen grundsätzlich ohne besondere Ermächtigung dazu berechtigt sind, im Zusammenhang mit der ihnen jeweils zugewiesenen Sachaufgabe

Presse-, Öffentlichkeits- und Informationsarbeit zu betreiben. Amtliche Äußerungen, die einen unmittelbaren Grundrechtseingriff darstellen oder einem solchen Grundrechtseingriff als funktionales Äquivalent gleichkommen, bedürfen jedoch regelmäßig der Rechtfertigung durch eine gesetzliche oder verfassungsunmittelbare Ermächtigungsgrundlage.

Ob die für Datenschutzfragen zuständigen Verwaltungsgerichte diese Auffassung auf die Situation der Datenschutzaufsichtsbehörden übertragen werden, bleibt abzuwarten. Mit den Aufgaben aus Art. 57 DS-GVO und Art. 58 Abs. 3 lit. b DS-GVO gibt es gute Gründe, zu einem anderen Ergebnis als das OVG im Eilverfahren gegen die Bundesnetzagentur zu kommen.

Wichtig ist aber sicherlich, dass jede Entscheidung über einen Bericht zu einem Bußgeld in einer Einzelfallentscheidung zu treffen ist. Es ist dabei zu berücksichtigen, dass durch die Pressemitteilung eine Prangerwirkung mit erheblich negativen Konsequenzen im Sinne des „name and shame“ ausgelöst werden kann. Auf der anderen Seite hat die Öffentlichkeit aber auch ein Interesse an der Information. Es stellt sich damit die Frage, ob und wie und in welchem Umfang auf ein verhängtes Bußgeld aufmerksam zu machen ist. Meine Behörde entscheidet hierüber im Einzelfall.

Die Tatsache, dass manche Aufsichtsbehörden Bußgelder veröffentlichen und andere wiederum nicht, manch eine Pressemitteilung den Namen des Unternehmens preisgibt, andere wiederum nicht, ergibt eine bunte Landschaft der Veröffentlichungen. Sie wird dadurch noch bunter, dass manches Bußgeld gar nicht bekannt gegeben wird. Diese unterschiedliche Pressearbeit spielt für die Qualität der Fallsammlungen zum Bußgeldverfahren eine tragende Rolle. Die privaten Fallsammlungen, die Anwaltskanzleien, Unternehmensberater und Pressevertreter anfertigen und veröffentlichen, können immer nur ein kleiner Auszug aus der tatsächlichen Arbeit der Aufsichtsbehörden sein.

6.3
Bußgeldverfahren

Die Palette der in den Ordnungswidrigkeitenverfahren des HBDI zu verfolgenden datenschutzrechtlichen Verstöße ist insgesamt breit gefächert. Im Mittelpunkt der bearbeiteten Bußgeldverfahren in Hessen standen unrechtmäßige Datenverarbeitungen durch eigenmächtig handelnde Mitarbeiterinnen und Mitarbeiter.

Überblick und Entwicklungen

Im Berichtszeitraum wurden 86 neue Ordnungswidrigkeitenverfahren eingeleitet. Damit blieb die Anzahl der neu anhängigen Verfahren annähernd auf

dem Niveau des Vorjahres. Der Schwerpunkt der Bearbeitung lag in diesem Jahr im Bereich des Mitarbeiterexzesses (s. u.), wobei häufig Verstöße gegen den Zweckbindungsgrundsatz gemäß Art. 83 Abs. 5 lit. a i. V. m. Art. 5 Abs. 1 lit. b DS-GVO zu prüfen waren. Es wurden jedoch auch Bußgeldverfahren gegen kleine, mittlere und auch größere Unternehmen insbesondere wegen Verstößen gegen die Grundsätze und Zulässigkeit der Verarbeitung (Art. 5, 6 und 9 DS-GVO), die Betroffenenrechte (Art. 12 ff. DS-GVO) sowie die Sicherheit der Verarbeitung (Art. 32 DS-GVO) geführt. Dabei ging es um Sachverhalte aus verschiedensten Themenbereichen, von unerwünschter Werbung ohne erteilte Einwilligung über Videoüberwachungen im öffentlichen Raum bis hin zur rechtswidrigen Verarbeitung von Gesundheitsdaten im Beschäftigtenverhältnis.

Im Ergebnis habe ich im Berichtsjahr 16 Verfahren mit einem Bußgeldbescheid abgeschlossen und Geldbußen in Höhe von insgesamt 47.750 Euro festgesetzt. Die Höhe der Geldbußen habe ich in jedem einzelnen Fall mit Blick auf Art. 83 Abs. 2 DS-GVO unter Berücksichtigung aller maßgeblichen Umstände stets mit Augenmaß bestimmt, was sich in der breiten Spanne der jeweils verhängten Beträge von 100 Euro bis insgesamt 42.000 Euro widerspiegelt.

Mitarbeiterexzess

Wie bereits in früheren Tätigkeitsberichten (s. 48. TB, Ziffer 15.1, 49. TB, Ziffer 16.1) ausführlich beschrieben, stellen eigenmächtige Datenverarbeitungen durch Mitarbeiter, die sich über die dienst- und arbeitsrechtlichen Anweisungen des Arbeitgebers hinwegsetzen und eigene private Zwecke verfolgen, datenschutzrechtliche Verstöße i. S. d. DS-GVO dar (der sogenannte „Mitarbeiterexzess“). Im Berichtsjahr hat meine Behörde eine Vielzahl von Fällen in diesem Kontext geprüft und auch mit einer Geldbuße geahndet. Dabei ging es beispielsweise um Sachverhalte im Zusammenhang mit der zweckwidrigen Datenverwendung aus den sogenannten „Corona-Listen“ in der Gastronomie oder in Corona-Testcentern durch die dortigen Mitarbeiter und um Verstöße durch hessische Polizeibedienstete.

Ausgewählte Fälle

– Ein Polizeibeamter fragte über einen längeren Zeitraum mehrere Personen aus seinem familiären Umfeld ohne dienstlichen Anlass in diversen polizeilichen und der Polizei zur Verfügung stehenden Systemen ab. Die Verstöße habe ich mit Geldbußen in Höhe von insgesamt 1.800,00 Euro geahndet. Der Bußgeldbescheid ist mittlerweile rechtskräftig. Zuvor hatte die Staatsanwaltschaft das strafrechtliche Ermittlungsverfahren wegen

des Verdachts der Verletzung von Privatgeheimnissen (§ 203 StGB) eingestellt, da nicht nachweisbar war, dass die durch die Abfragen erlangten Daten an Dritte weitergegeben wurden.

– In einem anderen Fall versuchte ein Polizeibeamter nach der Trennung von seiner Lebensgefährtin den Kontakt zu dieser wiederherzustellen. Nach mehreren vergeblichen konventionellen Versuchen der Kontaktaufnahme nutzte er das ihm dienstlich zur Verfügung stehende EWO-System, um nach der neuen Anschrift seiner Ex-Freundin zu recherchieren. Auf diese Weise erfuhr er, dass diese mittlerweile in ein anderes Bundesland verzogen war. Der Beamte fuhr schließlich zur neuen Wohnung seiner Ex-Freundin und traf sie vor dem Hauseingang auch tatsächlich an. Dies erschreckte die ehemalige Lebensgefährtin so sehr, dass sie den Sachverhalt bei der örtlichen Polizeistation zur Anzeige brachte. Das Verhalten des Polizeibeamten wurde mit einer Geldbuße von insgesamt 600Euro geahndet. Der Bescheid ist rechtskräftig.

– Gegenstand eines weiteren Verfahrens waren mehrfache Abfragen durch einen Polizeibeamten betreffend Informationen zu einem Kollegen in den polizeilichen Informationssystemen ComVor und POLAS. Hintergrund der Abfragen war keine dienstliche Veranlassung, sondern die private Neugierde aufgrund von aufgekommenen Gerüchten über ein vermeintliches Strafverfahren. Es wurde eine Geldbuße in Höhe von 500 Euro verhängt. Auch hier wurde kein Rechtsmittel gegen die Bußgeldentscheidung eingelegt.

– Ein Polizeioberkommissar kaufte privat auf einer Internet-Plattform ein hochwertiges Notebook. Da sich der Verkäufer im Nachgang auf keine Verhandlungen über die vereinbarte Zahlungsweise einließ, nutzte der Beamte das Auskunftssystem POLAS, um an Informationen über die Person des Verkäufers zu gelangen. Im Anschluss sandte der Polizist dem Verkäufer mehrere Nachrichten, in denen er diesem unter anderem neben dessen Geburtsdatum und -ort auch die aktuelle sowie die vorherigen Wohnadressen nannte. Durch die Nennung der aus den POLAS-Abfragen gewonnenen Informationen wollte der Polizist seiner Forderung nach einer alternative Zahlungsmethode Nachdruck verleihen. Der Verkäufer brachte den Sachverhalt jedoch zu Anzeige. Das Verhalten des Polizeibeamten wurde mit einer Geldbuße von 400 Euro geahndet.

Zweckwidrige Nutzung von Listen zur Kontaktnachverfolgung

In einem weiteren Fall, der sich im Rahmen der wirtschaftlichen Tätigkeit eines Bistros ereignete, beschwerte sich ein Gast über das kalte Essen und ging schließlich, ohne dieses zu bezahlen. Um den Gast ausfindig zu ma-

chen, wurden mehrere Besucher des Bistros telefonisch durch Mitarbeiter des Restaurants kontaktiert. Hierfür wurden die Telefonnummern verwendet, die durch die Gäste als Corona-Kontakte hinterlegt wurden. Mindestens eine Kontaktaufnahme konnte aufgrund der eingereichten Beschwerde bei meiner Behörde nachgewiesen werden.

Die Verwendung der Kontaktnachverfolgungsdaten stellte einen Verstoß gegen den Zweckbindungsgrundsatz gemäß Art. 5 Abs. 1 lit. b DS-GVO dar, der nach Art. 83 Abs. 5 lit. a DS-GVO geahndet werden kann. Personenbezogene Daten der Besucherinnen und Besucher, die mittels der sogenannten „Corona-Listen“ erfasst werden, sind ausschließlich zu dem Zweck zu verwenden, die Kontaktnachverfolgung von Infektionen zu ermöglichen. Die Nutzung dieser Daten zu anderen Zwecken – auch anderweitige Kommunikation mit den Gästen – ist unzulässig.

Das Verfahren endete mit einem Bußgeldbescheid gegen den Inhaber des Bistros in Höhe von 170 Euro. Dabei wurden die durch die Auswirkungen der Corona-Pandemie angeschlagene finanzielle Situation des Unternehmers, die Einsichtigkeit sowie die konstruktive Zusammenarbeit mit der Aufsichtsbehörde deutlich mildernd bei der Bußgeldzumessung berücksichtigt.

Arbeitsgruppe „Datenschutzverstöße bei der hessischen Polizei“

Die datenschutzrechtlichen Verstöße durch hessische Polizeibedienstete wurden zum Anlass genommen, eine gemeinsame Arbeitsgruppe des Landespolizeipräsidiums (LPP), des Projekts Sichere Daten Hessen und meiner Behörde zum Thema „Datenschutzverstöße bei der hessischen Polizei“ zu bilden. Ziel der Arbeitsgruppe war insbesondere die Verbesserung der bestehenden Abläufe bei Meldungen der Verletzung des Schutzes von personenbezogenen Daten (gemäß § 60 HDSIG, Art. 33 DS-GVO oder § 65 BDSG i. V. m. § 500 StPO) und die Beschleunigung der Bearbeitung datenschutzrechtlicher Verstöße durch hessische Polizeibedienstete.

In insgesamt sechs Sitzungen sowie einer Abschlussbesprechung wurden Abstimmungen getroffen, die geeignet sind, die Verfahrensabläufe bei Datenschutzvorfällen sowohl bei der hessischen Polizei als auch bei meiner Behörde zu optimieren. Die Arbeitsgruppe hat unter anderem – teilweise unter Einbindung des Hessischen Ministeriums der Justiz (HMdJ) – Fragen zur Verantwortlichkeit bei der Meldung des Schutzes personenbezogener Daten erörtert, die erhebliche Bedeutung der unverzüglichen Meldung von Datenpannen betont, geeignete Informationswege zur zügigen Aufklärung festgelegt und das Verhältnis von Disziplinar-, Aufsichts- und Bußgeldverfahren geklärt.

Ein weiterer Fokus der Beteiligten lag auf dem Präventionsgedanken. Die Arbeitsgruppe erarbeitete einen Bericht über kürzlich verhängte Geldbußen gegen Bedienstete der hessischen Polizei wegen Datenschutzverletzungen, um auf mögliche empfindliche Folgen eines Mitarbeiterexzesses aufmerksam zu machen. Der Bericht wurde unter dem Titel „Der Hessische Beauftragte für Datenschutz und Informationsfreiheit verhängt Bußgelder bei unrechtmäßigen Datenabfragen – Es kann teuer werden!“ auf der Intrapol-Seite des Projekts Sichere Daten Hessen veröffentlicht.

Im November tagte die Arbeitsgruppe vorerst zum letzten Mal. Alle Beteiligten waren sich einig, dass die erzielten Ergebnisse sehr positiv zu werten sind. Dieser sehr konstruktive Austausch soll fortgeführt werden.

6.4
Datenschutzrechtliche Verwaltungsgerichtsverfahren

Der deutliche Trend der letzten drei Berichtsjahre setzt sich fort. Die Zahl der Verwaltungsgerichtsverfahren steigt weiter an. Hinzugekommen sind Verfahren, die in der zweiten Instanz vor dem Hessischen Verwaltungsgerichtshof geführt werden, und Vorabentscheidungsersuchen nach Art. 267 AEUV vor dem EuGH.

Zur Statistik

Während 2018 noch keine Verfahren nach DS-GVO vor den Verwaltungsgerichten geführt wurden, waren es 21 im Jahr 2019 und 25 im Jahr 2020. Im Berichtsjahr wurden 34 Verfahren rechtshängig. Von den 34 Gerichtsverfahren aus dem Jahr 2021 und den noch offenen Verfahren aus den Jahren 2019 und 2020 konnten sieben zugunsten des HBDI mit klageabweisendem Urteil abgeschlossen werden. Zwei Urteile fielen zu Lasten des HBDI aus. Von den Verfahren wurden im Berichtsjahr acht durch Klagerücknahme beendet und vier durch Einstellung nach übereinstimmender Erledigungserklärung. Ende 2021 waren insgesamt noch 32 Verfahren aus den Jahren 2019, 2020 und 2021 rechtshängig.

Bis auf die Verfahren vor dem EuGH führt mein Justiziariat die Gerichtsprozesse ohne externe anwaltliche Unterstützung.

Verwaltungsgericht Wiesbaden

Im Berichtsjahr wurden sehr viele der rechtshängigen Verfahren vor dem Verwaltungsgericht Wiesbaden verhandelt.

Es kam in verschiedenen Konstellationen zu Klagen gegen meine Behörde. Zum einen waren die Klagen gegen Bescheide gerichtet, in denen Anordnungen oder Anweisungen nach Art. 58 Abs. 2 DS-GVO getroffen worden waren. In anderen Fällen wandten sich Beschwerdeführer gegen die Unterrichtung meiner Behörde über das Ergebnis des Aufsichtsverfahrens. Das geschah vor allem in den Fällen, in denen eine Beschwerde wegen eines vermeintlichen datenschutzrechtlichen Verstoßes eingelegt worden war, aber meine Behörde zu einem anderen Ergebnis kam und ein solcher Verstoß beispielsweise nicht bestätigt wurde.

Angestiegen ist auch die Zahl der Untätigkeitsklagen gegen meine Behörde. Nach Art. 78 Abs. 2 DS-GVO hat jede betroffene Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn die zuständige Aufsichtsbehörde sich nicht mit einer Beschwerde befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der gemäß Art. 77 GS-GVO erhobenen Beschwerde in Kenntnis gesetzt hat.

Diese Handlungsmöglichkeit der betroffenen Personen hat in diesem Jahr zunehmend an Bedeutung gewonnen. Sie haben Untätigkeitsklagen eingelegt, weil sie nicht innerhalb der vorgesehenen Frist von drei Monaten über das Ergebnis oder einen Zwischenstand unterrichtet worden waren. In den meisten Fällen war die Frist von drei Monaten um wenige Tage überschritten. Wegen des starken Anstiegs der Beschwerden bei gleichbleibender personeller Besetzung fällt es immer schwerer, die Beschwerden rechtzeitig zu bearbeiten. Vielfach richteten sich die Klagen gegen eine vermeintliche Untätigkeit, die aber faktisch nicht vorlag. Hier lagen die Voraussetzungen einer Beschwerde nicht vor oder es gab Missverständnisse über den Zweck von Art. 77 und 78 DS-GVO. Häufig beobachtet werden konnte, dass Forderungen, die auf dem Zivilrechtsweg geltend zu machen sind, im Verwaltungsstreitverfahren vorgebracht wurden, wie z. B. Forderungen von Schadensersatz nach Art. 82 DS-GVO oder von Löschungen. In diesen Fällen wurde die Klägerseite in der Regel nicht anwaltlich vertreten.

Fachlich lag der Schwerpunkt der Verwaltungsstreitverfahren im Anwendungsbereich der Art. 13 DS-GVO (Informationspflicht), Art. 15 DS-GVO (Auskunft), Art. 17 DS-GVO (Löschung), Art. 21 DS-GVO (Widerspruch), Art. 22 DS-GVO (Profiling), Art. 33 DS-GVO (Meldung von Datenpannen) und Art. 40 DS-GVO (Verhaltensregeln) sowie § 26 BDSG (Beschäftigtendatenschutz).

Verwaltungsgerichtshof Kassel

Gegen erstinstanzliche Entscheidungen des Verwaltungsgerichts kann die Zulassung der Berufung unter den Voraussetzungen des § 124 VwGO

beantragt werden. In Hessen ist der Verwaltungsgerichtshof in Kassel die Berufungsinstanz in Verwaltungsgerichtsverfahren.

Im Berichtszeitraum wurde in drei Verfahren die Zulassung der Berufung beantragt, in zwei Verfahren durch die Klagenden, in einem durch mich. Bis zum Ende des Jahres wurde ein Verfahren über die Berufungszulassung beendet, weil der Kläger nicht anwaltlich vertreten war. In den anderen Fällen steht die Entscheidung des Verwaltungsgerichtshofs über die Zulassung noch aus.

Vorabentscheidungsersuchen zum EuGH

Zu den Verwaltungsstreitverfahren und den Verfahren zweiter Instanz kommen im vierten Jahr seit Geltung der DS-GVO auch die Klärung von Streitfragen bei der Auslegung der DS-GVO durch den EuGH.

Die Gerichte der Mitgliedstaaten sind die für die Anwendung des Unionsrechts zuständigen Gerichte. Um eine tatsächliche und einheitliche Anwendung des Unionsrechts sicherzustellen und divergierende Auslegungen zu verhindern, können (und müssen mitunter) nationale Gerichte sich an den Gerichtshof wenden und ihn um eine Auslegung des Unionsrechts bitten, um etwa die Vereinbarkeit ihrer nationalen Rechtsvorschriften mit dem vorrangigen Unionsrecht prüfen zu können. Gegenstand des Vorabentscheidungsersuchens kann auch die Prüfung der Gültigkeit eines Rechtsakts der Union sein. Der Gerichtshof antwortet nicht durch ein bloßes Gutachten, sondern durch ein mit Gründen versehenes Urteil oder durch einen entsprechenden Beschluss. Das nationale Gericht, an das das Urteil oder der Beschluss gerichtet ist, muss bei der Entscheidung über den bei ihm anhängigen Rechtsstreit die Auslegung des Gerichtshofs beachten. In gleicher Weise bindet das Urteil des Gerichtshofs andere nationale Gerichte, die mit dem gleichen Problem befasst werden (s. https://curia.europa.eu/jcms/jcms/Jo2_7024/de/). Für die Entwicklung des Datenschutzes sind diese Verfahren von ganz besonderer Relevanz, da sie grundlegende Fragen mit weitreichender Bedeutung für die gesamte Union klären (Ziff. 1). Die Behörde beauftragt daher in diesen Fällen spezialisierte Prozessvertreter, was bei dem Gewicht dieser Verfahren unabdingbar ist, auch wenn es den behördlichen Haushalt finanziell herausfordert.

Mit den Vorabentscheidungsersuchen C-552/21 und C-634/21 sind zwei Verfahren über Ersuchen des VG Wiesbaden beim EuGH eingeleitet. Die Vorlage C-552/21 wurde allerdings ohne Entscheidung beendet. In dem zugrundeliegenden Verwaltungsgerichtsverfahren vor dem VG Wiesbaden wurde die Klage gegen Ende des Berichtsjahres zurückgenommen und damit das Vorabentscheidungsersuchen gegenstandslos.

7. Polizei, Justiz

7.1 Entwicklungen im Bereich der Sicherheits- und Strafverfolgungsbehörden

Wichtige aktuelle Entwicklungen im Bereich der Sicherheits- und Strafverfolgungsbehörden, insbesondere bei der polizeilichen Videoüberwachung und Datenanalyse, sind in einem übergreifenden und europäischen Kontext zu sehen.

Die rasanten technischen Entwicklungen und damit einhergehenden datenschutzrechtlichen Fragestellungen haben in den letzten Jahren auch die Arbeit der Sicherheits- und Strafverfolgungsbehörden geprägt.

So sind die für die Videoüberwachung verwendeten Kameras immer leistungsstärker geworden und nunmehr etwa in der Lage, Videobilder in hoher Auflösung und Schärfe zu produzieren. Damit hat sich auch die Erkennbarkeit von Personen insgesamt und in größerer Ferne deutlich verbessert, was Auswirkungen auf die Anforderungen an die Ausgestaltung der Videoüberwachungsmaßnahmen hat. Eine wesentliche Aufgabe meiner Behörde ist es daher, insbesondere im Rahmen meiner Beratungstätigkeit für die Polizei- und Gefahrenabwehrbehörden, sicherzustellen, dass nur die rechtlich zulässigen Bereiche und diese nur im erforderlichen räumlichen und zeitlichen Umfang überwacht werden.

Zu einem zentralen Thema entwickelt sich zunehmend die Frage nach der Zulässigkeit intelligenter Videoüberwachung – entsprechende gesetzliche Regelungen gibt es vereinzelt bereits in einigen Landespolizeigesetzen. Schwierig gestalten sich hierbei vor allem die verfassungskonforme Ausgestaltung und Formulierung der rechtlichen Grenzen einer solchen Videoüberwachung. Letzteres spielt insbesondere beim Einsatz von Gesichtserkennungssoftware eine große Rolle. Dabei sind auch die Entwicklungen auf europäischer Ebene und die Erfahrungen aus Ländern, die eine solche Technik schon länger einsetzen, für die künftige datenschutzrechtliche Beurteilung relevant.

So haben der Europäische Datenschutzausschuss (EDSA) und der Europäische Datenschutzbeauftragte (EDSB) im Juni 2021 beim Thema künstliche Intelligenz (KI) in einer gemeinsamen Stellungnahme dazu aufgerufen, KI-Systeme zur automatisierten Erkennung menschlicher Merkmale und andere KI-Nutzungen mit Diskriminierungsrisiko zu verbieten (https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_de). Diese Stellungnahme

5/2021 (abrufbar auf Deutsch unter: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_de) erging zum Vorschlag der Europäischen Kommission für eine Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz). EDSA und EDSB verweisen darauf, dass angesichts der extrem hohen Risiken in Verbindung mit der biometrischen Fernidentifizierung von Personen im öffentlichen Raum ein generelles Verbot der Verwendung von KI für die automatisierte Erkennung menschlicher Merkmale im öffentlichen Raum egal in welchem Kontext, darunter die Gesichts-, Gang-, Fingerabdruck-, DNA-, Stimm- und Tippverhaltenserkennung sowie die Erkennung anhand anderer biometrischer oder verhaltensbezogener Charakteristika, erforderlich sei.

Das Thema KI ist jedoch nicht nur auf europäischer Ebene in den Fokus der Datenschutzaufsichtsbehörden und -gremien gerückt. Der Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) etwa hat im Jahr 2021 zum Einsatz künstlicher Intelligenz in der Strafverfolgung und Gefahrenabwehr ein öffentliches Konsultationsverfahren durchgeführt (https://www.bfdi.bund.de/DE/DerBfDI/Inhalte/Konsultationsverfahren/KI-Strafverfolgung/KI-Strafverfolgung-Thesen-BfDI.html).

Bereits im Juni 2020 hatte sich der EDSA kritisch zur Nutzung eines privaten Dienstes im Bereich der Gesichtserkennungstechnologie, wie Clearview AI, durch Strafverfolgungsbehörden in der Europäischen Union geäußert und festgestellt, dass dies nach derzeitigem Stand wahrscheinlich nicht im Einklang mit dem EU-Datenschutzregelwerk steht (https://edpb.europa.eu/news/news/2020/thirty-first-plenary-session-establishment-taskforce-tiktok-response-meps-use_de).

Aktuell arbeitet der EDSA zudem an der Erstellung von Leitlinien zur Nutzung von Gesichtserkennungstechnologie durch Strafverfolgungsbehörden.

Die nationalen Datenschutzaufsichtsbehörden in Deutschland begleiten die Erarbeitung der erwähnten Dokumente auf europäischer Ebene. Für meine Behörde werden sie eine gewichtige Rolle im Rahmen der Bewertung künftiger Projekte hessischer Behörden spielen. Daher sind die hiesigen Sicherheits- und Strafverfolgungsbehörden aufgerufen, sich an diesen europäischen Stellungnahmen und Leitlinien zu orientieren, um datenschutzkonforme Lösungen zu entwickeln.

Aber auch auf Ebene der Datenschutzkonferenz (DSK) findet eine Auseinandersetzung mit aktuellen IT-Entwicklungen etwa im Polizeibereich statt.

So hat die DSK mit ihrer Entschließung „Polizei 2020 – Risiken sehen, Chancen nutzen!“ vom 16. April 2020 (abrufbar unter: https://www.datenschutzkonferenz-

online.de/media/en/Entschlie%C3%9Fung_99_DSK_TOP%2012_final.pdf) zum neuen „Datenhaus“ in Rahmen des Programms Polizei 2020 die Gefahren durch Auswerte- und Rechercheplattformen im Hinblick auf den Zweckbindungsgrundsatz in den Blick genommen. Eine automatisierte Anwendung zur Datenanalyse wird mit hessenDATA für die Datenbestände der Hessischen Polizei bereits genutzt.

Die Verbindung einer Vielzahl von Erkenntnisquellen und Datenbeständen stellt die Polizeibehörden und den Datenschutz gerade im Hinblick auf die erforderliche Trennung zwischen den verschiedenen Verarbeitungszwecken vor besondere Herausforderungen.

Ein Positionspapier des BfDI zum Grundsatz der Zweckbindung in polizeilichen Informationssystemen setzt sich mit dieser Thematik ebenfalls kritisch auseinander (https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2021/Positionspapier_Zweckbindung-Polizei.pdf?__blob=publicationFile&v=1).

Meine Behörde steht gemeinsam mit den anderen deutschen und europäischen Datenschutzaufsichtsbehörden vor großen Herausforderungen mit Blick auf die dargestellten technologischen Entwicklungen und wird die entsprechenden Projekte sowie gesetzgeberischen Aktivitäten in Hessen aufmerksam verfolgen und bietet den Behörden, die solche Systeme planen, einführen und betreiben, ihre Beratung an.

7.2
Datenschutzkontrollen bei Polizeibehörden und Verfassungsschutz

Die gesetzlichen Regelungen sehen vor, dass meine Behörde im Polizeibereich bestimmte Datenschutzkontrollen durchführt. Für das Jahr 2021 waren turnusmäßig die Rechtsextremismus Datei (RED) und erstmals Ausschreibungen im Schengener Informationssystem der zweiten Generation (SIS II) zu prüfen. Des Weiteren fanden Nachprüfungen zu Datenschutzkontrollen der verdeckten Maßnahmen aus dem Vorjahr statt.

Im Jahr 2021 erfolgten verschiedene datenschutzrechtliche Prüfungen bei unterschiedlichen Polizeibehörden und dem Landesamt für Verfassungsschutz in Hessen (LfV Hessen). Alle Prüfungen wurden von den beteiligten Behörden konstruktiv begleitet.

Die ersten Datenschutzkontrollen zu verdeckten Maßnahmen gemäß § 29a HSOG erfolgten durch meine Behörde bei der Hessischen Polizei im Jahr 2020. Seit Erscheinen des letzten Tätigkeitsberichts wurden diese fortgeführt und weiter ausgewertet.

Ein Schwerpunkt der Prüfung lag auf dem Vorliegen der jeweiligen Anordnungsbefugnis. Je nach verdeckter Maßnahme erfolgt die Anordnung durch richterlichen Beschluss oder die Polizeibehörde. Im letzten Fall erfolgt die Anordnung durch die Behördenleitung oder eine oder einen von der Behördenleitung beauftragte Bedienstete oder beauftragten Bediensteten.

§ 15 HSOG

(…)

(3) Außer bei Gefahr im Verzug erfolgt die Anordnung von Maßnahmen nach Abs. 1 Nr. 2 durch die Behördenleitung oder eine von dieser beauftragte Bedienstete oder einen von dieser beauftragten Bediensteten, soweit nicht nach Abs. 5 eine richterliche Anordnung erforderlich ist.

(…)

Im Rahmen der Datenschutzkontrolle wurde festgestellt, dass bei einem Polizeipräsidium in der Dienstanweisung zwei Personen als beauftragte Bedienstete bestimmt waren. Eine Bestimmung zweier Bediensteter ist jedoch mit der Rechtsgrundlage nicht vereinbar. Im Zuge der Nachbereitung der Datenschutzkontrolle passte das betroffene Polizeipräsidium die Dienstanweisung an die gesetzlichen Vorgaben an.

Wie bereits im letzten Tätigkeitsbericht erwähnt, erfolgten Benachrichtigungen der betroffenen Personen nach Abschluss einer verdeckten Maßnahme teilweise nicht in ausreichendem Umfang und genügten inhaltlich nicht immer den gesetzlichen Anforderungen. Auf meine Veranlassung hin wurde ein umfassendes Formular erstellt, dass nunmehr den Vorgaben der §§ 50 und 51 HDSIG entspricht.

§ 50 HDSIG

Der Verantwortliche hat in allgemeiner, verständlicher und leicht zugänglicher Form Informationen in einer klaren und einfachen Sprache zur Verfügung zu stellen über

1. *die Zwecke der von ihm vorgenommenen Verarbeitungen,*
2. *die im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten bestehenden Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung,*
3. *den Namen und die Kontaktdaten des Verantwortlichen und die Kontaktdaten der oder des Datenschutzbeauftragten,*
4. *das Recht, die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten anzurufen, und*
5. *die Erreichbarkeit der oder des Hessischen Datenschutzbeauftragten.*

§ 51 HDSIG

(1) Ist die Benachrichtigung betroffener Personen über die Verarbeitung sie betreffender personenbezogener Daten in speziellen Rechtsvorschriften, insbesondere bei verdeckten Maßnahmen, vorgesehen oder angeordnet, so hat diese Benachrichtigung zumindest die folgenden Angaben zu enthalten:

1. *die in § 50 genannten Angaben,*
2. *die Rechtsgrundlage der Verarbeitung,*
3. *die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,*
4. *gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten, auch der Empfänger in Drittländern oder in internationalen Organisationen, sowie*
5. *erforderlichenfalls weitere Informationen, insbesondere, wenn die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben wurden.*

(…)

Im Berichtszeitraum fanden gemäß § 11 RED-G zudem die gesetzlich vorgeschriebenen, turnusmäßigen Datenschutzkontrollen der Rechtsextremismus-Datei (RED) statt.

§ 11 RED-G

(1) Die Kontrolle der Durchführung des Datenschutzes obliegt nach § 9 Absatz 1 des Bundesdatenschutzgesetzes der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Die von den Ländern in die Rechtsextremismus-Datei eingegebenen Datensätze können auch von den jeweiligen Landesbeauftragten für den Datenschutz im Zusammenhang mit der Wahrnehmung ihrer Prüfungsaufgaben in den Ländern kontrolliert werden, soweit die Länder nach § 9 Absatz 1 verantwortlich sind. Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit arbeitet insoweit mit den Landesbeauftragten für den Datenschutz zusammen.

(2) Die in Absatz 1 genannten Stellen sind im Rahmen ihrer jeweiligen Zuständigkeiten verpflichtet, mindestens alle zwei Jahre die Durchführung des Datenschutzes zu kontrollieren.

(…)

Die RED wurde im Jahr 2021 beim LfV Hessen und einem Polizeipräsidium hinsichtlich der in 2019/2020 neu gespeicherten Personen geprüft.

Im Rahmen der Datenschutzkontrolle beim LfV Hessen habe ich festgestellt, dass die Ausgestaltung der Personenakten in den letzten Jahren verbessert wurde. Aus den nunmehr einheitlich gestalteten Vordrucken lassen sich die Speichervoraussetzungen hinreichend nachvollziehen. Die geprüften Speicherungen entsprachen den datenschutzrechtlichen Vorgaben.

Bei einem Polizeipräsidium erfolgten u. a. Speicherungen von Kontaktpersonen.

§ 3 RED-G

(…)

2) Kontaktpersonen nach Absatz 1 Nummer 1 Buchstabe b Doppelbuchstabe mm sind Personen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie mit den in § 2 Satz 1 Nummer 1 oder Nummer 2 genannten Personen nicht nur flüchtig oder in zufälligem Kontakt in Verbindung stehen und durch sie weiterführende Hinweise für die Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus zu erwarten sind.

(…).

Zur vollständigen Nachvollziehbarkeit einer Speicherung von Kontaktpersonen erfolgten ergänzende Prüfungen beim Hessischen Landeskriminalamt (HLKA). Die polizeilich ausgelösten Speicherungen konnten nachvollzogen werden und waren datenschutzrechtlich nicht zu bemängeln.

Erstmals fand im Jahr 2021 eine Prüfung der Ausschreibungen nach Art. 36 Abs. 2 Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystem der zweiten Generation (SIS II-Beschluss) statt.

Art. 60 Beschluss (Überwachung der N.SIS II)

(1) Jeder Mitgliedstaat gewährleistet, dass eine unabhängige Behörde (nachstehend als „nationale Kontrollinstanz“ bezeichnet) unabhängig die Rechtmäßigkeit der Verarbeitung personenbezogener SIS-II-Daten in ihrem jeweiligen Hoheitsgebiet und deren Übermittlung aus ihrem Hoheitsgebiet und den Austausch und die Weiterverarbeitung von Zusatzinformationen überwacht.

(2) Die nationale Kontrollinstanz gewährleistet, dass die Datenverarbeitungsvorgänge in ihrem N.SIS II mindestens alle vier Jahre nach internationalen Prüfungsstandards überprüft werden.

Die Fragebögen und Vorgaben für diese Datenschutzkontrolle wurden in der zuständigen Koordinierungsgruppe der europäischen Datenschutzaufsichtsbehörden für das SIS II (SIS II SCG, https://edps.europa.eu/data-protection/european-it-systems/schengen-information-system_de) erarbeitet, um eine einheitliche Prüfung in den Mitgliedstaaten des Schengenraums zu ermöglichen. Ausschreibungen nach Art. 36 Abs. 2 SIS II-Beschluss erfolgen bei der Hessischen Polizei zu präventiven (vgl. § 17 HSOG, zur gezielten

Kontrolle oder polizeilichen Beobachtung) oder repressiven Zwecken (vgl. § 163e StPO, zur polizeilichen Beobachtung).

Art. 36 Beschluss (Ausschreibungsziele und -bedingungen)

(…)

(2) Eine Ausschreibung dieser Art ist zulässig zur Strafverfolgung und zur Abwehr von Gefahren für die öffentliche Sicherheit, wenn

a) tatsächliche Anhaltspunkte dafür vorliegen, dass eine Person eine schwere Straftat, z. B. eine der in Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI genannten Straftaten, plant oder begeht, oder

b) die Gesamtbeurteilung einer Person, insbesondere aufgrund der bisher von ihr begangenen Straftaten, erwarten lässt, dass sie auch künftig schwere Straftaten, z. B. eine der in Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI genannten Straftaten, begehen wird.

(…)

§ 17 HSOG

(1) [1]Die Polizeibehörden können die Personalien einer Person sowie das amtliche Kennzeichen und sonstige Merkmale des von ihr benutzten oder eingesetzten Kraftfahrzeugs im polizeilichen Fahndungsbestand zur Polizeilichen Beobachtung oder zur Gezielten Kontrolle ausschreiben. [2]Polizeilicher Fahndungsbestand im Sinne von Satz 1 sind die Fahndungsdateien des beim Bundeskriminalamt nach den Vorschriften des Bundeskriminalamtgesetzes und des beim Hessischen Landeskriminalamt nach den Vorschriften dieses Gesetzes geführten polizeilichen Informationssystems. [3]Die Fahndungsdateien des polizeilichen Informationssystems umfassen auch die nach den Vorschriften des Schengener Durchführungsübereinkommens zulässigen Ausschreibungen im Schengener Informationssystem.

(…)

§ 163e StPO

(1) Die Ausschreibung zur Beobachtung anlässlich von polizeilichen Kontrollen, die die Feststellung der Personalien zulassen, kann angeordnet werden, wenn zureichende tatsächliche Anhaltspunkte dafür vorliegen, dass eine Straftat von erheblicher Bedeutung begangen wurde. Die Anordnung darf sich nur gegen den Beschuldigten richten und nur dann getroffen werden, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre. Gegen andere Personen ist die Maßnahme zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass sie mit dem Täter in Verbindung stehen oder eine solche Verbindung hergestellt wird, dass die Maßnahme zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes des Täters führen wird und dies auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre.

(…)

Stichprobenartig wurden ca. 10% der Ausschreibungen einer Prüfung unterzogen, wobei aufgrund der Häufigkeit mehr Ausschreibungen zur Polizeilichen Beobachtung als zur Gezielten Kontrolle geprüft wurden. Die Datenschutzkontrolle der Ausschreibungen nach Art. 36 Abs. 2 SIS II-Beschluss dauerte bis zum Redaktionsschluss dieses Tätigkeitsberichts noch an.

Im nächsten Tätigkeitsbericht werde ich über diese Datenschutzkontrollen weiter informieren.

7.3
Videoüberwachung der Hessischen Polizei- und Gefahrenabwehrbehörden

Bei der Beratung von Projekten zur Videoüberwachung der Polizei- und Gefahrenabwehrbehörden auf Grundlage von § 14 Abs. 3 HSOG wende ich insbesondere die folgenden Kriterien und Maßstäbe an, um die Zulässigkeit solcher Videoüberwachungsmaßnahmen an öffentlich zugänglichen Orten zu prüfen.

Im Berichtszeitraum – wie auch schon in den Jahren zuvor – wurde meine Behörde regelmäßig zu verschiedenen Videoüberwachungsmaßnahmen der Polizei- und Gefahrenabwehrbehörden konsultiert. Videoüberwachungen auf Grundlage von § 14 Abs. 3 HSOG machen hier einen Großteil meiner Beratungstätigkeit aus.

§ 14 Abs. 3 HSOG

(…)

(3) Die Gefahrenabwehr- und die Polizeibehörden können zur Abwehr einer Gefahr oder wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Straftaten drohen, öffentlich zugängliche Orte mittels Bildübertragung offen beobachten und aufzeichnen. Der Umstand der Überwachung sowie der Name und die Kontaktdaten der oder des Verantwortlichen sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen. Fest installierte Anlagen sind alle zwei Jahre daraufhin zu überprüfen, ob die Voraussetzungen für ihren Betrieb weiterhin vorliegen. Abs. 1 Satz 2 und 3 gilt entsprechend.

(…)

Im Hinblick auf die Konzipierung und Neuausrichtung von Videoüberwachungsmaßnahmen verweise ich regelmäßig auf folgende Grundsätze und konnte hierzu bei den betroffenen Behörden entsprechend einwirken:

Meine Behörde wird in diesen Fällen in einer beratenden Funktion tätig, da keine gesetzliche Verpflichtung zur Prüfung und Abnahme vor der Inbetriebnahme von Videoüberwachungsanlagen besteht. Die Einhaltung der rechtlichen Vorgaben ist seitens der verantwortlichen öffentlichen Stellen sicherzustellen. Allerdings wenden sich die öffentlichen Stellen in der Regel an meine Behörde und lassen sich bezüglich der konkreten Ausgestaltung der jeweiligen Videoüberwachungsanlage beraten. Im Rahmen dieser Beratung werden u. a. die für die jeweilige Örtlichkeit vorzunehmende Kriminalitätsanalyse, Privatzonenausblendungen (einschließlich Außengastronomie), versammlungsrechtliche Einschränkungen, Beschilderung und die Speicherdauer thematisiert. Eine Prüfung der in Betrieb genommenen Anlage kann dann jederzeit auch ohne Ankündigung durch meine Behörde erfolgen.

Voraussetzung für eine Videoüberwachungsmaßnahme ist zunächst, dass eine Kriminalitätsanalyse die Erforderlichkeit der Maßnahme stützt. Dies ist nur dann der Fall, wenn es sich um einen Kriminalitätsschwerpunkt mit typischer Straßenkriminalität handelt. Der gefahrenabwehrrechtliche Zweck der Videoüberwachung ist hierbei insbesondere, die Kriminalität durch ein erhöhtes Entdeckungs- und Verfolgungsrisiko in den videoüberwachten Bereichen zu reduzieren.

Es ist zudem darauf zu achten, dass bei der Videoüberwachung die erforderlichen Privatzonenausblendungen vorgenommen werden, damit beispielsweise Wohnräume, Innenräume von Geschäften, aber auch Außenbereiche von Restaurants und Cafés, soweit sie für mehr als einen kurzen Verbleib gedacht sind, nicht von der Videoüberwachung erfasst werden. Hierfür ist die Videoüberwachung so zu gestalten, dass die betroffenen Bereiche gar nicht erst von den Kameras aufgenommen werden.

Im Übrigen sind die Voraussetzungen von Aufnahmen bei Versammlungen im Versammlungsgesetz (VersammlG) speziell geregelt und eingeschränkt (§§ 12a, 19a VersammlG). Soweit die Videoüberwachung bei einer Versammlung nicht zulässig ist, sollte die Abschaltung der Kameras für die Versammlungsteilnehmer erkennbar sein. Dies kann etwa durch sichtbare Abdeckungen der Kameras oder durch technische Vorkehrungen, wie beispielsweise durch sog. Versammlungsjalousien, die an den Kameras montiert sind und dann bei Versammlungen sichtbar vor die Objektive heruntergefahren werden, erfolgen.

§ 12a Abs. 1 VersammlG

(1) Die Polizei darf Bild- und Tonaufnahmen von Teilnehmern bei oder im Zusammenhang mit öffentlichen Versammlungen nur anfertigen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass von ihnen erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen. Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(…)

Die Beschilderung der videoüberwachten Bereiche ist so vorzunehmen, dass sie für die betroffenen Personen hinreichend erkennbar und wahrnehmbar ist. Daher sollten die Hinweisschilder so angebracht werden, dass gut sichtbar ist, welchen Bereich die Videoüberwachung umfasst sowie wer die verantwortlichen Stellen sind und wie diese kontaktiert werden können. Weiterführende Hinweise und Informationen auf den Beschilderungen werden aus datenschutzrechtlichen Erwägungen von meiner Behörde im Rahmen der Beratungen ausdrücklich empfohlen.

Schließlich muss auch die Speicherdauer der Videoaufnahmen verhältnismäßig ausgestaltet sein. In § 14 Abs. 1 Satz 2 HSOG, auf den in § 14 Abs. 3 Satz 4 HSOG verwiesen wird, findet sich nur eine Regelung, die die Vernichtung von Unterlagen nach spätestens zwei Monaten vorsieht.

§ 14 Abs. 1 HSOG

(1) Die Polizeibehörden können personenbezogene Daten auch über andere als die in den §§ 6 und 7 genannten Personen bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen erheben, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass bei oder im Zusammenhang mit der Veranstaltung oder Ansammlung Straftaten oder nicht geringfügige Ordnungswidrigkeiten drohen. Die Unterlagen sind spätestens zwei Monate nach Beendigung der Veranstaltung oder Ansammlung zu vernichten, soweit sie nicht zur Abwehr einer Gefahr, zur Verfolgung einer Straftat oder Ordnungswidrigkeit oder zur Strafvollstreckung benötigt werden. Eine Verarbeitung für andere Zwecke ist unzulässig. § 20 Abs. 8 bleibt unberührt.

(…)

Unter Beachtung des Grundsatzes der Verhältnismäßigkeit erachtet meine Behörde grundsätzlich eine Speicherdauer für derartige Videoaufnahmen auf Grundlage von § 14 Abs. 3 HSOG von maximal 14 Tagen – sofern sie nicht für konkrete Verfahren benötigt werden – als zulässig und berät die zuständigen Behörden auch dahingehend. Folglich sollten die Videoüberwachungsanlagen technisch so ausgestaltet werden, dass die Aufzeichnungen nach Ablauf der zulässigen Speicherdauer automatisch gelöscht werden.

7.4
Abfragen im Fahreignungsregister bei der Verfolgung von Verkehrsordnungswidrigkeiten

Im Berichtszeitraum erreichten meine Behörde mehrere Beschwerden zu verfrühten Datenabfragen im Fahreignungsregister im Rahmen der Bearbeitung von Verkehrsordnungswidrigkeiten. Hier konnte in Zusammenarbeit mit dem Regierungspräsidium Kassel, Zentrale Bußgeldstelle, eine grundsätzliche Änderung im Verfahrensablauf erzielt werden.

Das Kraftfahrtbundesamt führt auf Grundlage des Straßenverkehrsgesetzes (§ 28 StVG) das Fahreignungsregister (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. Bezüglich der Frage des rechtlich zulässigen Zeitpunktes einer Abfrage im FAER im Rahmen der Bearbeitung von Verkehrsordnungswidrigkeiten durch das Regierungspräsidium Kassel, Zentrale Bußgeldstelle (ZBS), gingen im Berichtszeitraum mehrere Beschwerden ein.

Im FAER werden Informationen über Verkehrsteilnehmer, die im Straßenverkehr auffällig geworden sind, gespeichert, soweit die begangene Zuwiderhandlung nach dem Fahreignungs-Bewertungssystem mit Punkten bewertet ist. Konkret wurde von den Beschwerdeführern jeweils vorgebracht, dass Anfragen seitens der ZBS an das FAER zu einem Zeitpunkt erfolgt sind, als noch kein zugrundeliegendes Erfordernis vorlag. Da die Informationen aus dem FAER erst für die individuelle Sanktion im korrespondierenden Verkehrsordnungswidrigkeitenverfahren benötigt werden, ist ein Erfordernis zur diesbezüglichen Datenerhebung nach Auffassung meiner Behörde erst dann gegeben, wenn sich das Verfahren nach Würdigung der vorliegenden Informationen gegen einen konkreten Fahrzeugführer richtet.

Die ursprüngliche Verfahrensweise sah eine FAER-Abfrage beim KBA bereits zu einem Zeitpunkt vor, zu dem nach summarischer Prüfung des Sachverhaltes und erfolgter Halterauskunft die Anhörung der oder des Betroffenen ausgelöst wurde. Zu diesem Zeitpunkt hat der Adressat des Vorwurfs jedoch noch keine Möglichkeit gehabt, sich zu diesem zu äußern und gegebenenfalls eine andere Person als verantwortlichen Fahrzeugführer zu benennen oder sonstige Gründe anzugeben, die eine weitere Verfolgung der Verkehrsordnungswidrigkeit hemmen oder die Verfolgungsbehörde im Rahmen der Anwendung des Opportunitätsprinzips von der weiteren Verfolgung absehen

lassen. Diese Verfahrensweise war demnach geeignet, Datenerhebungen auszulösen, die zu diesem Zeitpunkt (noch) nicht erforderlich und damit als datenschutzrechtlich nicht zulässig zu bewerten waren.

Nachdem meine Behörde diese Problematik mit der ZBS erörtert hat, wurde nunmehr eine Änderung des betreffenden Fachverfahrens ausgelöst. Sofern nach Halterauskunft und summarischer Prüfung eine Anhörung als Betroffene oder Betroffener erfolgt, wird zunächst keine FAER-Abfrage vorgenommen. Eine solche Abfrage erfolgt nunmehr erst nach einer Zeitspanne, die die siebentägige Rückäußerungsfrist im Hinblick auf die Betroffenenanhörung sowie Postlaufzeiten berücksichtigt. Voraussetzung dafür ist jedoch auch zu diesem Zeitpunkt die Erforderlichkeit der Abfrage, d. h., dass sich der Vorwurf nach der Anhörung oder dem Ende der diesbezüglichen Frist noch gegen diesen Betroffenen richtet.

8. Allgemeine Verwaltung, Kommunen

8.1 Aktuelle Entwicklungen in der öffentlichen Verwaltung

Mit drei Klicks zum Antrag auf Erteilung einer Fahrerlaubnis – Datenschutzrechtliche Herausforderungen der Verwaltungsmodernisierung

Schneller, effizienter, nutzerfreundlicher und auch noch kostengünstiger? Die Leistungserbringung der Verwaltung gegenüber Bürgerinnen, Bürgern und Unternehmen soll durch den Einsatz von E-Government-Verfahren modernisiert werden. Ein vielfältiges und komplexes Unterfangen, wie etwa das beigefügte Schaubild ausgezeichnet verdeutlicht. Auch mit Blick auf das Datenschutzrecht stellen sich viele knifflige Fragen. Der nachfolgende Beitrag gibt einen Überblick über die Entwicklungen 2021 aus datenschutzrechtlicher Perspektive.

Endspurt für die Umsetzung des OZG

Wesentlicher Baustein der Umsetzung einer modernen Verwaltung ist das 2017 verabschiedete Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG). Das Gesetz verpflichtet Bund, Länder und Kommunen, bis Ende 2022 ihre Verwaltungsleistungen – beispielsweise den Antrag auf Erteilung einer Fahrerlaubnis – über Verwaltungsportale auch digital anzubieten. Betroffen hiervon ist die Digitalisierung von 575 Verwaltungsleistungen.

Um dieses Mammutprojekt im vorgesehenen Zeitraum zu realisieren, wurde u. a. das sogenannte „Einer für Alle“ (EfA)-Prinzip entwickelt. Dem EfA-Prinzip liegt der Gedanke einer effizienten und kostenschonenden Verwaltungsdigitalisierung zugrunde. Wenn etwa das Land Hessen den Antrag auf Erteilung einer Fahrerlaubnis als Verwaltungsleistung digitalisiert, sollen die Behörden anderer Bundesländer sich der Lösung anschließen und diese ebenfalls nutzen können.

Soweit es die Bereitstellung von Portallösungen oder auch die Realisierung digitaler Verwaltungsleistungen unter Nutzung des EfA-Prinzips betrifft, stellen sich aus datenschutzrechtlicher Sicht gleich mehrere schwierige Rechtsfragen, z. B.:

– Welche Verantwortlichkeiten im Sinne der DS-GVO (Verantwortlichkeit, Gemeinsame Verantwortlichkeit, Auftragsverarbeitung) entstehen zwi-

schen den unterschiedlichen, am Digitalisierungsverfahren beteiligten Akteuren – z. B. die das System entwickelnde Einheit (Land A), die betreibende Einheit (IT-Dienstleister) und die nachnutzende Einheit (Land B, Bund, Kommune)?

– Wie können die hieran anknüpfenden Rechtsfolgen effizient realisiert werden? Bedarf es der Schaffung neuer gesetzlicher Grundlagen oder sind Verträge abzuschließen?
– Müssen für die Verarbeitung personenbezogener Daten im OZG-Kontext neue Rechtsgrundlagen geschaffen werden oder genügen die bereits vorhandenen Rechtsgrundlagen?
– Sofern gesetzgeberisches Handeln notwendig ist, wer muss gesetzgeberisch tätig werden, der Bund oder die Länder?
– Welche technischen und organisatorischen Anforderungen sind an ein Verwaltungsportal und an eine digitalisierte Verwaltungsleistung zu stellen?

Für diese und weitere Themen gilt es – trotz des äußert knappen Umsetzungszeitraums – datenschutzrechtskonforme und in der Praxis handhabbare Lösungen zu entwickeln.

Meine Behörde steht hierzu in einem regelmäßigen und engen Austausch mit den Datenschutzbeauftragten des Bundes und der Länder, den OZG-Koordinatorinnen des Landes Hessen, Projektverantwortlichen für die Digitalisierung einzelner Verwaltungsleistungen, den zentralen hessischen Dienstleistern für Informations- und Kommunikationstechnik und der Föderalen IT-Kooperation.

Startschuss für die Registermodernisierung

Um die Nutzung digitaler Verwaltungsleistungen für Bürgerinnen, Bürger und Organisationen weiter zu verbessern, sollen zusätzlich auch die vielen öffentlichen Register angepasst werden. Im April 2021 wurde daher das Gesetz zur Einführung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz – RegMoG) verkündet. Durch die neu geschaffenen Regelungen sollen einfache, nachweisfreie Verwaltungsleistungen unterstützt werden. Die Umsetzung folgt dabei dem Gedanken des Once-Only-Prinzips: Bürgerinnen, Bürger und Organisationen sollen notwendige Angaben nur ein einziges Mal an die Verwaltung übermitteln müssen. Mit dem Einverständnis der Nutzerinnen und Nutzer sollen die Daten wiederverwendet und mit anderen Behörden einfach und sicher ausgetauscht werden können.

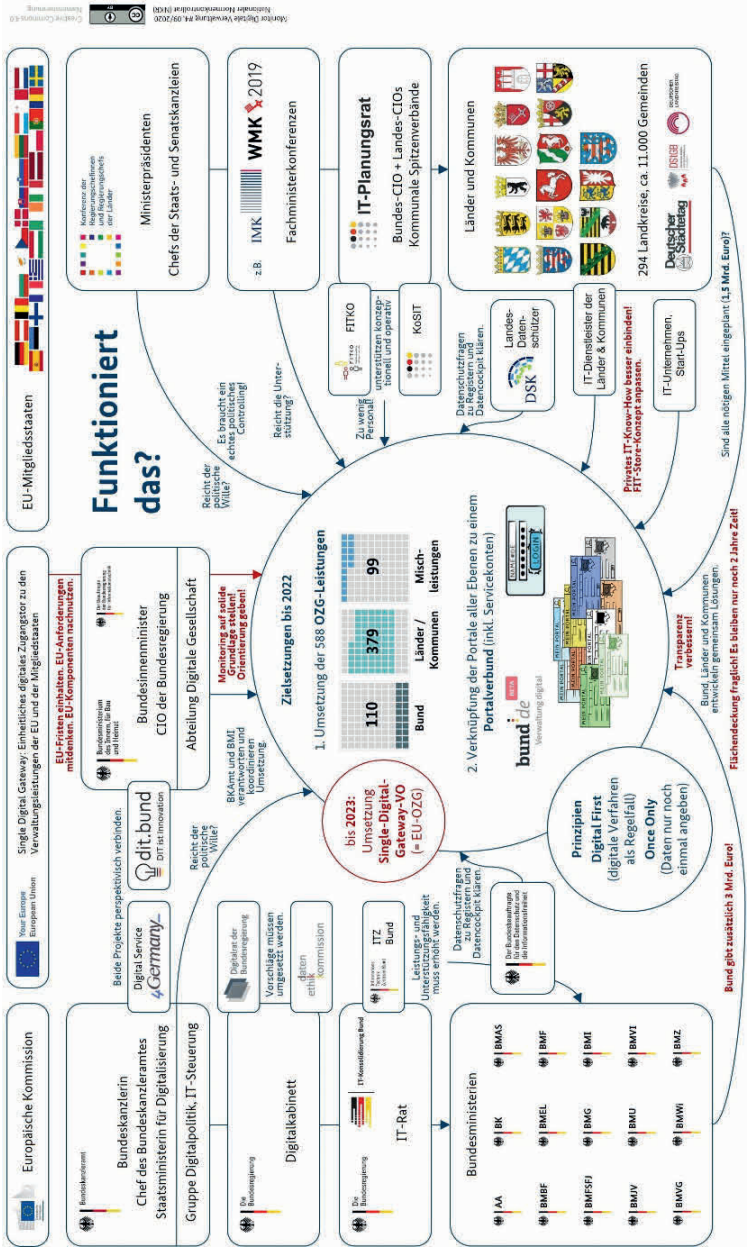
Notwendige Voraussetzung hierfür ist die eindeutige Identifizierung von Personen sowie ein registerübergreifendes Identifikationsmanagement. Damit Daten einer natürlichen Person in einem Verwaltungsverfahren eindeutig

zugeordnet und die Qualität der Daten verbessert werden können sowie die erneute Beibringung von bereits vorhandenen Daten nicht mehr erforderlich ist, soll nach dem RegMoG die Steuer-ID als registerübergreifendes Identifikationsmerkmal genutzt werden. Im Falle des Antrags auf Erteilung einer Fahrerlaubnis könnte die Steuer-ID etwa für Anfragen beim Fahreignungsregister oder beim Zentralen Fahrerlaubnisregister genutzt werden.

Die Thematik hat nicht nur eine nationale, sondern auch eine europäische Dimension. Ausgewählte Verwaltungsverfahren sollen online grenzüberschreitend und vollständig medienbruchfrei abgewickelt werden können (Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates vom 2. Oktober 2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012 – SDG-VO).

Aus datenschutzrechtlicher Perspektive birgt die Verwendung eines registerübergreifenden Identifikationsmerkmals die Gefahr, dass personenbezogene Daten in großem Maße leicht verknüpft und zu einem umfassenden Persönlichkeitsprofil vervollständigt werden können. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierauf bereits in ihrer Entschließung vom 26. August 2020 „Registermodernisierung verfassungskonform umsetzen!“ hingewiesen (https://www.datenschutzkonferenz-online.de/entschliessungen.html). Verdeutlicht wird das Gefährdungspotenzial, wenn man sich die Dimensionen der Registermodernisierung vor Augen führt: 51 Register werden durch die Steuer-ID als Identifikationsmerkmal miteinander verknüpft.

So wünschenswert und wichtig eine schnellere, effektivere und moderne Verwaltung auch ist – Aufgabe der Datenschutzbehörden ist es, dafür Sorge zu tragen, dass bei aller Euphorie und allem Innovationseifer das Recht auf informationelle Selbstbestimmung nicht aus dem Blickfeld gerät. Notwendig hierfür sind transparente Verfahrensweisen, die Einhaltung hoher Datenschutzstandards und eine technisch sichere Ausgestaltung.


Europäische Kommission
Bundeskanzlerin
Chef des Bundeskanzleramtes
Staatsministerin für Digitalisierung
Gruppe Digitalpolitik, IT-Steuerung
Digitalkabinett
IT-Rat
Bundesministerien
BK
BMAS
BMF
BMI
BMJV
BMVI
BMVg
BMWi
BMZ
Beide Projekte perspektivisch verbinden.
Digital Service 4Germany
dit.bund
Single Digital Gateway: Einheitliches digitales Zugangstor zu den Verwaltungsleistungen der EU und der Mitgliedsstaaten
EU-Fristen einhalten. EU-Anforderungen mitdenken. EU-Komponenten nachnutzen.
Bundesministerin
CIO der Bundesregierung
Abteilung Digitale Gesellschaft
Monitoring auf valide Grundlage stellen! Orientierung geben!
BKAmt und BMI verantworten und koordinieren Umsetzung
Zielsetzungen bis 2022
1. Umsetzung der 588 OZG-Leistungen
110
379
99
Bund
Länder / Kommunen
Misch-leistungen
bis 2023: Umsetzung Single-Digital-Gateway-VO (= EU-OZG)
2. Verknüpfung der Portale aller Ebenen zu einem Portalverbund (inkl. Servicekonten)
bund.de
Verwaltung digital
Prinzipien
Digital First (digitale Verfahren als Regelfall)
Once Only (Daten nur noch einmal angeben)
Transparenz verbessern!
Bund, Länder und Kommunen entwickeln gemeinsam Lösungen.
Flächendeckung fraglich! Es bleiben nur noch 2 Jahre Zeit!
Bund gibt zusätzlich 3 Mrd. Euro!
Sind alle nötigen Mittel eingeplant (1,5 Mrd. Euro)?
Prüfstes IT-Kisay-How besser einbinden! FIT-Start-Konzept anpassen.
Datenschutzfragen zu Registern und Datencockpit klären.
Leistungs- und Unterstützungsfähigkeit muss erhöht werden.
Vorschläge müssen umgesetzt werden.
Reicht der politische Wille?
Funktioniert das?
EU-Mitgliedstaaten
Ministerpräsidenten
Chefs der Staats- und Senatskanzleien
z.B. IMK WMK 2019
Fachministerkonferenzen
IT-Planungsrat
Bundes-CIO + Landes-CIOs
Kommunale Spitzenverbände
FITKO
KoSIT
unterstützen Konzeptionell und operativ
Zu wenig Personal!
Es braucht ein echtes politisches Controlling!
Reicht die Unterstützung?
Länder und Kommunen
Landes-Daten-schützer
DSK
IT-Dienstleister der Länder & Kommunen
IT-Unternehmen, Start-Ups
294 Landkreise, ca. 11.000 Gemeinden
Deutscher Städtetag
Deutscher Landkreistag
Monitor Digitale Verwaltung #4, 09/2020
Nationaler Normenkontrollrat (NKR)
Creative Commons 4.0
Namensnennung

8.2
Live-Streaming von Sitzungen und Veröffentlichung von Protokollen im Internet – Kommunalpolitische Teilhabe in Zeiten der Corona-Pandemie

Die Teilhabe an kommunalpolitischen Entscheidungsprozessen – etwa durch die Verfolgung von Sitzungen der Gemeindevertretung oder des Zugriffs auf Sitzungsprotokolle – ist unter Beachtung datenschutzrechtlicher Grundsätze trotz pandemiebedingter Einschränkungen möglich.

Vor dem Hintergrund der Corona-Pandemie erreichten mich vermehrt Anfragen von Bürgern und Kommunen, die die Frage der Übertragung von Sitzungen und die Veröffentlichung von Sitzungsprotokollen (Niederschriften) der Gemeindevertretung im Internet zum Gegenstand hatten. Das Informationsinteresse der Allgemeinheit sowie die Gestaltung eines transparenten politischen Willens- und Meinungsbildungsprozesses stehen hier dem Recht auf informationelle Selbstbestimmung der von der Veröffentlichung betroffenen Personen gegenüber und müssen in einen interessengerechten Ausgleich gebracht werden. Nachfolgend möchte ich daher vertiefend auf die rechtlichen Möglichkeiten und die datenschutzrechtlichen Aspekte eingehen.

I. Veröffentlichung von Bild- und Tonaufnahmen von Sitzungen der Gemeindevertretung im Internet

Für Hessische Kommunen schafft § 52 Abs. 3 der Hessischen Gemeindeordnung (HGO) eine gesetzliche Regelung für die Fertigung von Bild- und Tonaufnahmen in öffentlichen Sitzungen.

> *§ 52 HGO*
>
> *(1) Die Gemeindevertretung fasst ihre Beschlüsse in öffentlichen Sitzungen. Sie kann für einzelne Angelegenheiten die Öffentlichkeit ausschließen. Anträge auf Ausschluss der Öffentlichkeit werden in nicht öffentlicher Sitzung begründet, beraten und entschieden; die Entscheidung kann in öffentlicher Sitzung getroffen werden, wenn keine besondere Begründung oder Beratung erforderlich ist. Der Vorsitzende kann im Einvernehmen mit dem Bürgermeister Gemeindebedienstete zu den nicht öffentlichen Sitzungen beiziehen.*
>
> *(2) Beschlüsse, welche in nicht öffentlicher Sitzung gefasst worden sind, sollen, soweit dies angängig ist, nach Wiederherstellung der Öffentlichkeit bekanntgegeben werden.*
>
> *(3) Die Hauptsatzung kann bestimmen, dass in öffentlichen Sitzungen Film- und Tonaufnahmen durch die Medien mit dem Ziel der Veröffentlichung zulässig sind.*

Die Vorschrift legt die Entscheidungskompetenz über die Veröffentlichung von Film- und Tonaufnahmen öffentlicher Sitzungen in die Hand der Gemein-

devertretung, die in der Hauptsatzung bestimmen kann, dass in öffentlichen Sitzungen Film- und Tonaufnahmen durch die Medien mit dem Ziel der Veröffentlichung zulässig sind. Hiervon umfasst ist auch die Möglichkeit, entsprechende Aufnahmen auf der eigenen kommunalen Internetseite zu publizieren.

Soweit die Hauptsatzung eine entsprechende Regelung beinhaltet, sind jedoch ergänzende datenschutzrechtliche Erwägungen geboten. So sollten Rednerinnen und Redner verlangen können, dass die Aufnahme ihres Redebeitrages oder die Veröffentlichung der Aufnahme unterbleibt (Widerspruchsrecht). Auch sollte vor jeder Sitzung ein Hinweis auf die Fertigung von Bild- und Tonaufnahmen erfolgen (siehe hierzu auch das Kurzpapier Nr. 10 der DSK zu Informationspflichten bei Dritt- und Direkterhebung, abrufbar über https://datenschutz.hessen.de/infothek/kurzpapiere-der-dsk).

Die Stadt Frankfurt am Main hat in § 11 der Hauptsatzung und § 48 Abs. 2 der Geschäftsordnung der Stadtverordnetenversammlung beispielsweise folgende Regelung getroffen:

§ 11 Hauptsatzung der Stadt Frankfurt am Main

Die öffentlichen Sitzungen der Stadtverordnetenversammlung können im Internet als Tonübertragung zugänglich gemacht werden. Näheres regelt die Geschäftsordnung der Stadtverordnetenversammlung.

§ 48 Abs. 3 Geschäftsordnung der Stadtverordnetenversammlung

Die Stadtverordnetenvorsteherin/der Stadtverordnetenvorsteher veranlasst eine zeitgleiche Tonübertragung der Redebeiträge im Internet. Die Tonübertragung ist von der Stadtverordnetenvorsteherin/dem Stadtverordnetenvorsteher zu Beginn der Sitzung anzukündigen. Rednerinnen oder Redner, die einer Tonübertragung widersprechen, haben dies der Stadtverordnetenvorsteherin/dem Stadtverordnetenvorsteher anzuzeigen. In diesem Fall werden Redebeiträge der oder des Widersprechenden, die auf vorheriger schriftlicher Wortmeldung beruhen, nicht übertragen.

In Abgrenzung zu Mandatsträgern müssen Bedienstete und Sitzungsbesucher aufgrund der Satzungsregelung nicht hinnehmen, dass sie Teil von Bild- und Tonaufnahmen sind. Hier sind die Einstellungen so zu wählen, dass Aufzeichnungen einzeln identifizierbarer Personen möglichst unterbleiben. Andernfalls müssen in der Regel Einwilligungen der Betroffenen eingeholt werden. In diesem Zusammenhang ist bei Einwilligungen zu beachten, dass nach einem Widerruf der Einwilligung nicht gewährleistet werden kann, dass einmal im Internet verfügbare Inhalte global gelöscht werden. Lediglich der Abruf auf

der kommunalen Internetseite kann beim Widerruf der Einwilligungserklärung unterbunden und damit seitens der Verantwortlichen zugesichert werden.

Eine transparente Einwilligungserklärung sollte dies berücksichtigen und möglichst konkret, in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache formuliert sein. Daneben muss dem Merkmal der Freiwilligkeit der Einwilligungserklärung ausreichend Rechnung getragen werden (siehe hierzu auch das Kurzpapier Nr. 20 der DSK zur Einwilligung nach der DS-GVO, abrufbar über https://datenschutz.hessen.de/infothek/kurzpapiere-der-dsk).

II. Veröffentlichung von Sitzungsprotokollen

Neben der virtuellen Teilnahme an öffentlichen Sitzungen spielt auch die Online-Zurverfügungstellung von Sitzungsprotokollen vor dem Hintergrund der pandemiebedingten Kontakteinschränkungen eine zunehmend größere Rolle. Eine Regelung zu Niederschriften findet sich in § 61 HGO:

§ 61 HGO

(1) Über den wesentlichen Inhalt der Verhandlungen der Gemeindevertretung ist eine Niederschrift zu fertigen. Aus der Niederschrift muss ersichtlich sein, wer in der Sitzung anwesend war, welche Gegenstände verhandelt, welche Beschlüsse gefasst und welche Wahlen vollzogen worden sind. Die Abstimmungs- und Wahlergebnisse sind festzuhalten. Jedes Mitglied der Gemeindevertretung kann verlangen, dass seine Abstimmung in der Niederschrift festgehalten wird.

(2) Die Niederschrift ist von dem Vorsitzenden und dem Schriftführer zu unterzeichnen. Zu Schriftführern können Gemeindevertreter oder Gemeindebedienstete – und zwar auch solche, die ihren Wohnsitz nicht in der Gemeinde haben – oder Bürger gewählt werden.

(3) Eine Kopie der Niederschrift ist innerhalb eines in der Geschäftsordnung festzulegenden Zeitraumes an alle Gemeindevertreter schriftlich oder elektronisch zu übersenden. Über Einwendungen gegen die Niederschrift entscheidet die Gemeindevertretung.

Adressaten der Niederschriften sind der Gemeindevorstand und die Gemeindevertretung. Den Gremien soll auf diesem Wege die Information und Kontrolle ermöglicht werden. Die Allgemeinheit hat grundsätzlich keinen Anspruch auf Einsicht in die Niederschriften. Es spricht jedoch nichts dagegen, dass Niederschriften, die sich auf den öffentlichen Teil einer Sitzung beziehen, auch anderen Personen zugänglich gemacht werden.

Bei der Veröffentlichung sollte allerdings darauf geachtet werden, ob die Niederschriften personenbezogene oder personenbeziehbare Daten enthalten. Eine mittelbare Personenbeziehbarkeit war bereits mehrfach Gegenstand von Bürgerbeschwerden, die sich als Beschwerdeführer, Käufer oder Verkäufer

von Grundstücken nach entsprechenden, nur sachbezogenen Veröffentlichungen, identifiziert sahen. Insbesondere in kleinen Kommunen ist eine nachvollziehbare Abwägung zwischen kommunalpolitischer Transparenz, dem Informationsbedürfnis der Bürger sowie dem individuellen Recht auf informationelle Selbstbestimmung von Bedeutung. Zu beachten ist in diesem Zusammenhang auch, dass die Allgemeinheit grundsätzlich keinen Anspruch auf die Veröffentlichung von Niederschriften hat.

Da der Kreis der Adressaten bei einer Internetveröffentlichung nicht begrenzbar ist, müssen die Inhalte entsprechend dem Erfordernis angepasst oder geschwärzt werden. Ein datensparsamer Umgang mit personenbezogenen Daten ist dabei auch vor dem Hintergrund etwaiger Geltendmachung von Betroffenenrechten sinnvoll: Macht ein Betroffener z. B. von seinem Recht auf Löschung nach Art. 17 DS-GVO Gebrauch, kann dies zur Folge haben, dass die entsprechende Niederschrift entfernt oder umfangreich überarbeitet werden muss, um sie um die individuellen personenbezogenen Daten des Betroffenen zu bereinigen.

9. Schulen, Hochschulen

9.1 Verbesserungen durch die Novelle des Hessischen Schulgesetzes

Die 12. Änderung des Hessischen Schulgesetzes (HSchG) soll eine Reihe datenschutzrechtlicher Verbesserungen erzielen. So werden Schulen für die digitale Datenverarbeitung keine Einwilligung der Schülerinnen und Schüler sowie der Lehrkräfte mehr benötigen. Eine neue gesetzliche Regelung (§ 83a Abs. 1 Ziff. 2 HSchG) soll es den Schulen ermöglichen, in eigener Verantwortung ihre Digitalisierungsprozesse zu bestimmen. Gleichzeitig werden die Schulen aber auch gefordert sein, Datenschutz und die Sicherheit der Datenverarbeitung zu gewährleisten. Allerdings wird es voraussichtlich bis in den Herbst 2022 andauern, ehe nach vielfältigen Beratungen das Gesetz verabschiedet werden kann.

Die Rechtsgrundlage der schulischen Datenverarbeitung vor der Gesetzesnovelle

Bislang müssen Schulen, die ein digitales Werkzeug im pädagogischen Bereich ihrer Tätigkeit einsetzen wollten, sich der Einwilligung der Betroffenen bedienen, da es für diese Art der Datenverarbeitung keine gesetzliche Grundlage gibt.

Die schulische Datenverarbeitung stützt sich auf die Rechtsgrundlagen des Art. 6 Abs. 1 UAbs. 1 lit. a und e DS-GVO sowie den derzeit gültigen § 83 Abs. 1 HSchG.

Art. 6 Abs. 1 UAbs. 1 lit. a und e DS-GVO

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) die betroffene Person hat ihre Einwilligung zur Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben, …

(…)

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

§ 83 Abs. 1 HSchG:

Schulen dürfen personenbezogene Daten von Schülerinnen und Schülern, deren Eltern, künftig schulpflichtig werdenden oder vom Schulbesuch zurückgestellten Kindern und deren Eltern und Lehrerinnen und Lehrern verarbeiten, soweit dies zur rechtmäßigen Erfüllung des Bildungs- und Erziehungsauftrags der Schule und für einen jeweils damit verbundenen Zweck oder zur Durchführung schulorganisatorischer Maßnahmen erforderlich ist. (…)

Die Notwendigkeit, die Einwilligung der Betroffenen einzuholen, gilt insbesondere für Bilder und Videos von Schülerinnen und Schülern, die im schulischen Kontext verwendet werden. Rechtsgrundlage hierfür ist Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO.

Auch die digitale Datenverarbeitung unterliegt bislang dem Vorbehalt der Einwilligung der Betroffenen. Allerdings soll sich die staatliche Datenverarbeitung (Schule = Staat) grundsätzlich auf gesetzliche Regelungen stützen und das Rechtsinstitut der Einwilligung ausschließlich in Ausnahmefällen (zum Beispiel für Bildaufnahmen) nutzen.

Erwägungsgrund 43 DS-GVO

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

EG 43 betrachtet die Freiwilligkeit der Einwilligung in einem tatsächlichen oder vermuteten Unterordnungsverhältnis von Eltern oder Schülerinnen und Schülern zu Schule und Schulverwaltung, so dass eine zweifelsfreie Einwilligung auf der Grundlage einer freien Entscheidung der Betroffenen in Frage steht.

Die Neuregelung des § 83a HSchG

In regelmäßigen Abständen habe ich in der Vergangenheit wiederholt auf das Erfordernis hingewiesen, die digitale Verarbeitung personenbezogener Daten durch die Schulen auf Grundlage einer rechtlichen Legitimation zu ermöglichen. Dem will das Hessische Kultusministerium (HKM) Rechnung tragen und den § 83a neu fassen.

§ 83a HSchG

(1) Die Verarbeitung personenbezogener Daten, die im Rahmen der Aufgabenstellung von Schulen nach § 83 Abs. 1 zulässig ist, darf auch im Rahmen digitaler Anwendungen erfolgen, wenn

1. *diese durch das Kultusministerium oder eine von diesem beauftragte Stelle geprüft und den Schulen zur Anwendung zur Verfügung gestellt wird, oder*
2. *die Schule selbstständig im Rahmen ihrer Aufgabenstellung digitale Anwendungen einführt und als Verantwortliche die Einhaltung der datenschutzrechtlichen Bestimmungen und die Sicherheit der Datenverarbeitung gewährleistet.*

(2) Den Schulen können zentrale landeseigene elektronische Schulverwaltungsverfahren bereitgestellt werden. Die Nutzung einzelner Verfahren kann für verpflichtend erklärt werden.

(3) Nähere Einzelheiten werden durch Rechtsverordnung geregelt.

Die Schule soll durch § 83a Abs. 1 Ziff. 2 HSchG ermächtigt werden, selbstständig im Rahmen ihrer Aufgabenstellung als Verantwortliche digitale Anwendungen einzuführen. Ein Vorbehalt gilt der Einhaltung datenschutzrechtlicher Bestimmungen und der Gewährleistung der Sicherheit der Datenverarbeitung.

Den Schulen wird damit ermöglicht, im Rahmen ihres pädagogischen Auftrags Art und Umfang digitaler Datenverarbeitung sowohl für pädagogische Zwecke als auch für Zwecke der Schulverwaltung selbst zu bestimmen. Auch hier wird künftig eine Einwilligung der Betroffenen in die Datenverarbeitung obsolet.

Allerdings trifft die Schulen damit auch eine besondere Verpflichtung hinsichtlich der Datenschutzkonformität der Datenverarbeitung. Dies stellt eine dauerhafte und herausfordernde Aufgabe dar, die Schulen nicht ohne zusätzliche Ressourcen werden stemmen können. Deshalb müssen das Ministerium, die Staatlichen Schulämter sowie die Lehrkräfteakademie und die Medienzentren ausreichende Ressourcen für die Unterstützung der Schulen bereithalten.

Die Möglichkeit, den Schulen landeseigene elektronische Verfahren (§ 83a Abs. 2 HSchG) zur Verfügung zu stellen und deren Nutzung im Einzelfall verpflichtend vorzuschreiben, ist grundsätzlich zu begrüßen. Diese Verfahren des HKM und anderer müssen auf deren Datenschutzkonformität geprüft worden sein.

Ist diese sichergestellt, so erscheint es mehr als konsequent, diese durch eine verpflichtende Nutzung in den Schulen zu etablieren. Die Lehrer- und Schüler-Datenbank, die von den Schulen nach § 1 Abs. 2 der Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen vom 4. Februar 2009 (ABl. 2009, S. 131) verpflichtend zu nutzen ist, kann hierfür beispielhaft genannt werden.

Soweit künftig unter diese Vorschrift auch das Schulportal Hessen (SPH) oder das geplante landesweite- und einheitliche Videokonferenzsystem fallen sollten, ist dies datenschutzrechtlich ebenso ein Mehrwert, soweit deren Datenschutzkonformität durch die Prüfung des HBDI festgestellt werden kann.

9.2
Elektronische Fernprüfungen an Hochschulen

Elektronische Fernprüfungen sind eine probate Alternative für Präsenzprüfungen. Allerdings müssen hierfür rechtliche, technische und organisatorische Rahmenbedingungen geschaffen werden, um einem Anspruch der Vergleichbarkeit der Prüfumstände und Kontrollen sowie dem Schutz der Grundrechte der betroffenen Studierenden gerecht zu werden.

Rechtliche Grundlagen

Die Hessische Landesregierung hat das Hessische Hochschulgesetz novelliert. In diesem Zusammenhang wurde in dem neuen § 23 eine gesetzliche Regelung für die Möglichkeit geschaffen, elektronischer Fernprüfungen auch unabhängig der aktuellen Pandemie durchführen zu können. Mit dieser Regelung hat der Gesetzgeber „eine dauerhafte, tragfähige Rechtsgrundlage für elektronische Fernprüfungen“ geschaffen.

Nach § 23 Abs. 6 HHG sollen die Regelungen in § 23 Abs. 1 bis 5 HHG nicht durch eine Verordnung, sondern durch Satzungen der Hochschulen konkretisiert werden, in denen sie das Nähere insbesondere

– zur Ausgestaltung der elektronischen Fernprüfung,
– zur Verarbeitung personenbezogener Daten sowie
– zum Umgang mit technischen Störungen und Täuschungsversuchen

regeln.

Die Hochschulen sind in ihren Satzungen nicht auf diese drei Sachverhalte beschränkt. Vielmehr sieht § 23 HHG in seinen Regelungen vor, dass die Hochschulen in ihren Satzungen in sich geschlossene systematische Vollregelungen zu den Fragen elektronischer Fernprüfungen treffen können.

Inhaltliche Regelungen

Elektronische Fernprüfungen können für alle Beteiligten Erleichterungen bringen. Sie müssen aber eine schwierige Balance zwischen der Chancengleichheit der zu Prüfenden und dem Schutz ihrer Persönlichkeitsrechte und ihrer informationellen Selbstbestimmung einhalten.

Um dies zu erreichen, sieht das Regelungskonzept des § 23 HHG vor, dass elektronische Fernprüfungen nur „zusätzlich zu entsprechenden Präsenzprüfungen angeboten werden“ können (§ 23 Abs. 1 Satz 2 HHG). Elektronische Fernprüfungen sind also immer ein Zusatzangebot, das auch ausgeschlagen werden kann.

Um sich entscheiden zu können, welche Prüfungsform sie wählen, sollen die Studierenden „die Möglichkeit erhalten, die Prüfungssituation in Bezug auf die Technik, die Ausstattung und die räumliche Umgebung im Vorfeld der Prüfung zu erproben“ (§ 23 Abs. 1 Satz 2 HHG).

Die Teilnahme an einer elektronischen Fernprüfung soll somit immer auf dem Grundsatz der Freiwilligkeit beruhen. Bezogen auf den Ausdruck der Freiwilligkeit sieht § 23 HHG ein zweistufiges Verfahren vor:

– Die **Freiwilligkeit der Teilnahme** kommt im Regelfall dadurch zum Ausdruck, dass die zu Prüfenden daran teilnehmen, obwohl zeitgleich eine Präsenzprüfung angeboten wird, die sie auch hätten wählen können (§ 23 Abs. 5 HHG).
– Wollen sie an einer elektronischen Fernprüfung mit automatisierter Aufsicht teilnehmen, darf diese nur erfolgen, wenn sie in diese **ausdrücklich schriftlich eingewilligt** haben.

Die Datenverarbeitung bei elektronischen Fernprüfungen beruht somit grundsätzlich auf einer gesetzlichen Erlaubnis. Diese stellt die Bedingung für eine freiwillige Teilnahme durch ein Alternativangebot sicher. Dem intensiveren Grundrechtseingriff auf Grundlage einer Erlaubnis zur automatisierten Auswertung wird durch umfassende Information und eine ausdrückliche, schriftliche Einwilligung der jeweils teilnehmenden Studierenden Rechnung getragen.

Das von Erwägungsgrund 43 Satz 1 DS-GVO angesprochene Problem, dass eine Einwilligung keine gültige Rechtsgrundlage liefern kann, wenn „es sich bei dem Verantwortlichen um eine Behörde handelt und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde“, besteht hier nicht.

Zum einen beruht die Datenverarbeitung bei elektronischen Fernprüfungen und der grundsätzlich vorgesehenen Aufsicht nicht auf einer Einwilligung, sondern einer gesetzlichen Grundlage, die allerdings die Freiwilligkeit der Teilnahme durch ein zeitgleiches Alternativangebot sicherstellt.

Zum anderen gilt dieses Alternativangebot bei einer automatisierten Auswertung, die von einer ausdrücklichen schriftlichen Einwilligung abhängig gemacht wird. Für diese Einwilligung besteht daher trotz des Machtungleichgewichts zwischen Hochschule und zu prüfender Person „in Anbetracht aller Umstände

in dem speziellen Fall“ eine berechtigte Vermutung, dass die Einwilligung freiwillig gegeben wurde.

Diese Grundkonzeption des hessischen Gesetzgebers und ihre gesetzliche Regelung sind nach Art. 6 Abs. 2 und 3 in Verbindung mit Art. 6 Abs. 1 UAbs. 1 lit. e DS-GVO sowie Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO unionsrechtlich zulässig. § 23 HHG-neu regelt entsprechend dem Wesentlichkeitsprinzip die Grundrechtseingriffe durch Gesetz. Sie enthält eine verfassungsrechtlich zulässige Abwägung zwischen dem Gebot der Chancengleichheit und dem Schutz der Freiheitsrechte der betroffenen Personen.

Bei der Durchführung der elektronischen Fernprüfungen müssen die Grundsätze der Datenverarbeitung nach Art. 5 DS-GVO wie Transparenz, Zweckbindung, Datenminimierung, Datenrichtigkeit, Speicherbegrenzung und Systemdatenschutz beachtet werden. Die Regelungen des § 23 HHG berücksichtigen dies oder stehen der Erfüllung dieser Grundsätze nicht im Wege.

Als schwierig in der Umsetzung erweist sich der Grundsatz der Verhältnismäßigkeit. Dieser erfordert insbesondere, dass für unterschiedliche Prüfungsgegenstände differenzierte Prüfungsmodalitäten umgesetzt und die Überwachungsmaßnahmen an die jeweiligen Prüfungsmodalitäten angepasst werden.

So müssen und dürfen bei Open-Book-Arbeiten, bei denen die Nutzung von Hilfsmitteln weitgehend zulässig ist, wesentlich weniger Überwachungsmaßnahmen durchgeführt werden als bei Prüfungen mit streng reglementierten Hilfsmitteln.

Deshalb ist es je nach Prüfungsmaterie erforderlich, die Prüfungsmodalitäten dem jeweiligen Kontext der Prüfung anzupassen, was einen differenzierten Umfang von Überwachungsmaßnahmen zur Folge haben kann.

Das Prinzip der Verhältnismäßigkeit greift auch bei der differenzierten Betrachtung technischer und organisatorischer Prüfungsbedingungen, etwa bei der Auswahl einer möglichst eingriffsarmen Software oder bei der Differenzierung zwischen in der Privatwohnung oder an der Hochschule durchgeführten elektronischen Fernprüfungen.

9.3
Unzulässige Datenerhebung einer Schule bei der Ausleihe eines mobilen Endgeräts

Eltern müssen für die Ausleihe eines schulischen Endgeräts wie z. B. eines Laptops einen Antrag stellen. Viele Schulen haben für den Prozess der Ausleihe und Rückgabe der Geräte eigene Vorlagen entwickelt, die von den Eltern zu

unterschreiben waren. Zuständig hierfür sind jedoch die Schulträger. Im Fall einer Schule geriet das aber datenschutzrechtlich vollkommen daneben. Die Schule erhob bei Eltern eine Fülle von Daten, die weder rechtlich abgefragt werden durften noch für den Zweck der Ausleihe inhaltlich geeignet waren.

Die Datenerhebung durch die Schule

Durch die Beschwerde betroffener Eltern wurde ich darauf aufmerksam gemacht, dass die Schule eine Fülle personenbezogener Daten erhob, wie sie klassisch im Bereich der Antragstellung von Sozialleistungen üblich ist.

Der Antrag war im Original folgendermaßen gestaltet:

Antrag auf Ausleihe eines Leihlaptops
für Schülerinnen und Schüler

_____
Antragsteller/in (Nachname, Vorname)

_____ _____
Anschrift (PLZ, Wohnort, Straße, Hausnummer) Tel. (tagsüber erreichbar)

A.
Ich beantrage die Ausleihe eines Leihlaptops für meine Tochter/meinen Sohn:

Nachname Schüler/in:	Vorname Schüler/in:	Klasse:

B.
Folgende Geschwisterkinder besuchen die Alexander-von-Humboldt-Schule:

	Nachname Schüler/in:	Vorname Schüler/in:	Klasse:
1.			
2.			
3.			
4.			

Alle folgenden Angaben müssen schriftlich belegt werden.

Erhalten Sie laufende Leistungen zum Lebensunterhalt nach dem zwölften Buch Sozialgesetzbuch („Sozialhilfe", „Neue Wege").

☐ nein ☐ ja* und zwar in Höhe von: _____ €
(* falls ja entfallen die weiteren Angaben C – G)

C.
Ich habe monatliche Einkünfte in Höhe von brutto: _____€, netto: _____€

☐ mein Ehegatte/Ehegattin bzw. mein eingetragener Lebenspartner/in hat

monatliche Einkünfte von netto: _____€

D.
Die Wohnkosten betragen monatlich insgesamt _____€. Ich zahle davon _____€.

E.

Welchen Angehörigen gewähren Sie Unterhalt? Unterhalt kann in Form von Geldzahlungen, aber auch durch Gewährung von Unterkunft, Verpflegung etc. erfolgen. Bitte nennen Sie hier Name, Vorname dieser Angehörigen (Anschrift, nur, wenn sie vorn Ihrer Anschrift abweicht).	Wenn Sie den Unterhalt ausschließlich durch Zahlung leisten. Ich zahle mtl. Euro

Stand: 10.11.2020

Rechtliche Bewertung

Die schulische Datenverarbeitung richtet sich nach Art. 6 Abs. 1 UAbs. 1 lit. e DS-GVO sowie § 83 HSchG (s. auch Beitrag unter Ziff. 9.1 – Novellierung des Hessischen Schulgesetzes). Die Schule ist dazu befugt, jene personenbezogenen Daten von Schülerinnen und Schülern zu verarbeiten, die zur Erfüllung des Bildungs- und Erziehungsauftrags erforderlich sind.

Ohne Zweifel wurden von der Schule zunächst Daten erhoben, die mit dem eigentlichen Zweck, nämlich berechtigten Personen ein Laptop über einen bestimmten Zeitraum auszuleihen, nicht in Verbindung stehen. Fragen nach z. B. Einkommensverhältnissen oder Bankguthaben sind weit über das Ziel hinausgeschossen.

Auch im Hinblick auf Art. 5 Abs. 1 lit. b (Zweckbindung) und c (Datenminimierung) war die Verwendung des Antragsformulars unzulässig. Im Übrigen hatte das Hessische Kultusministerium ein Musterformular für die Schulträger (es handelte sich um Geräte des Schulträgers) entwickelt und diesen zur Verfügung gestellt: Vertrag über die Leihe eines mobilen Endgeräts für Schülerinnen und Schüler, abrufbar unter https://digitale-schule.hessen.de/sites/digitale-schule.hessen.de/files/Endger%C3%A4te_Leihvertrag_Muster.docx.

In ihrer Erklärung mir gegenüber teilte die Schulleitung mit, dass man sich auf die Expertise von Eltern verlassen habe. Die nicht reflektierte und unkritische Übernahme dieser Vorschläge muss sich die Schule vorhalten lassen.

Rücknahme des Antragformulars und Löschung der Daten

Nach meiner Intervention gegenüber der Schule, die auch das zuständige Staatliche Schulamt auf den Plan rief und auch ein Presseecho hervorrief, zog die Schule das Formular zurück. Die bereits erhobenen Daten wurden von der Schule, wie mir die Schulleitung schriftlich versicherte, gelöscht.

9.4
Datenschutzprobleme der Software-Anwendung Padlet

Im Berichtsjahr musste ich mich mit dem Einsatz der Software-Anwendung „Padlet“ im schulischen Bereich beschäftigen. Dabei bin ich zu dem Ergebnis gekommen, dass die Nutzung in der oder für die Schule, soweit private Endgeräte eingesetzt werden, nicht datenschutzkonform erfolgen kann. Ich habe daraufhin die Schulen aufgefordert, die Verwendung bis zum Ende des Schuljahres 2020/21 einzustellen. Gleichzeitig habe ich auf datenschutzkonforme Alternativen hingewiesen.

Nutzung digitaler Instrumente

Mehr denn je setzen die Schulen in Zeiten der Corona-Pandemie auf den Einsatz digitaler Werkzeuge, um den Distanzunterricht bewerkstelligen zu können. Auch das sogenannte „Padlet“ ist ein Werkzeug, das in Form einer digitalen Pinnwand genutzt wird. In Echtzeit kann eine Klasse z. B. gemeinsam Videos anschauen, Texte schreiben, Sprachnachrichten versenden oder andere Informationen austauschen.

Beim Einsatz digitaler Instrumente sind allerdings auch datenschutzrechtliche Fragestellungen zu berücksichtigen. Das gilt ebenso für den Einsatz von Padlet. Zunächst lässt sich positiv festhalten, dass sich Nutzerinnen und Nutzer der Pinnwand nicht registrieren müssen; sie können sich mit einem Gast-Account anmelden. Damit wird die mögliche Erstellung eines Profils vermieden.

Die Plattform Padlet

Padlet wird von einem US-Unternehmen betrieben. Da in den Vereinigten Staaten die DS-GVO nicht gilt, können personenbeziehbare Daten durch das Unternehmen selbst oder Drittanbieter gespeichert und verarbeitet werden. Das können neben den geteilten Inhalten auch die IP-Adressen der Nutzerinnen und Nutzer sein oder auch Bewegungsprofile, da Padlet bei der Benutzung Daten mit Drittanbietern wie z. B. Google teilt. Die genauen Inhalte dieser Daten sind dabei bislang weitgehend unbekannt.

Auch die Datenschutzbestimmungen, die der Plattform zugrunde liegen, entsprechen nicht den Vorgaben der DS-GVO, da diese nur auf Englisch abgefasst und zudem unpräzise sind.

Padlet kann sowohl mobil auf Endgeräten mit Android und iOS mittels App als auch im Browser als Web-App genutzt werden. Nutzen Schulen Padlet ausschließlich auf schulischen Rechnern, ohne einen Account auf dem Rechner für das jeweilige Kind anzulegen, bleiben die Kinder und ihr Nutzungsverhalten anonym. Nicht geklärt ist allerdings, welche Daten vom Plattformbetreiber erhoben werden, wenn mit einem schulischen Endgerät über den privaten Internetanschluss auf Padlet zugegriffen wird. Sobald aber Kinder, Lehrkräfte oder Eltern ihre privaten Endgeräte einsetzen, sind sie grundsätzlich identifizierbar, weil durch den Anbieter personalisierte Daten gespeichert werden können.

Eine datenschutzrechtlich unproblematische Nutzung von Padlet kann nur dann erzielt werden, wenn die Nutzung ausschließlich auf schulischen Rechnern stattfindet. Werden private Geräte eingesetzt, ist eine datenschutzkonforme Anwendung kaum mehr möglich. Auch mit der Einwilligung der Betroffenen

und hinreichenden Informationen zur Datenverarbeitung, soweit diese überhaupt gegeben werden können, ist eine datenschutzkonforme Nutzung der Plattform Padlet im schulischen Kontext nicht möglich.

Es gibt datenschutzkonforme Alternativen

Der Einsatz digitaler Werkzeuge und Anwendungen im schulischen Kontext ist unter Berücksichtigung der datenschutzrechtlichen Anforderungen hilfreich und pädagogisch geboten. Mein Haus hat in der Vergangenheit in vielen Fällen durch Beratung und aktive Unterstützung die Umsetzung digitaler Projekte ermöglicht. Digitalisierung und Datenschutz schließen einander nicht aus; vielmehr ermöglicht der Datenschutz die Sicherheit der Datenverarbeitung in der digitalen Welt und erzeugt das notwendige Vertrauen für die breite Nutzung digitaler Angebote. Gerade auch deshalb haben meine Mitarbeiter die Suche nach Alternativen unterstützt und befördert. Dabei wurde Kontakt zur pädagogischen Hochschule Schwyz in der Schweiz aufgenommen, die eine ähnlich gestaltete Anwendung entwickelt hat und für eine Nutzung anbietet. Zudem hat die Technische Hochschule Mittelhessen ein digitales Produkt entwickelt, das auf Open-Source basiert und auf den ersten Blick einen hinreichend datenschutzkonformen Eindruck gemacht hat. Erste Testanwendungen laufen an einigen hessischen Schulen erfolgreich. Auch unter dem Aspekt der „digitalen Souveränität“, also die Unabhängigkeit von großen, digitalen Dienstleistern, ist die Eigenentwicklung von Software sowie deren Einsatz unter anderem im schulischen Bereich zu begrüßen.

9.5
Datenschutz leicht gemacht

Datenschutz wird von Schülerinnen und Schülern oft als ein Hemmnis wahrgenommen. Die vielfältigen gesetzlichen Regelungen sind wenig ansprechend aufbereitet, nicht nur für Jugendliche. Mir ist daran gelegen, jungen Menschen bereits in der Schule oder in der Ausbildung einfache Mechanismen und rechtliche Regelungen im Umgang mit dem Datenschutz zu vermitteln. Eigene Gestaltungsmöglichkeiten und der eigenverantwortliche Umgang mit den eigenen Daten und den Daten anderer sind eine gute Voraussetzung für einen verantwortungsbewussten Umgang mit den vielfältigen digitalen Werkzeugen, die Kindern und Jugendlichen zur Verfügung stehen.

Im Rahmen zunehmender Digitalisierung motivieren Medien wie Videoclips Jugendliche, sich auf Fragestellungen des Datenschutzes einzulassen. Die Initiative „Datenschutz geht zur Schule“ des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) entwickelte im Jahr 2020 mit Unterstützung

einiger Aufsichtsbehörden der Länder digitale Lehr- und Lernmaterialien zum Datenschutz für den Einsatz im Unterricht.

Hessen unterstützte das Projekt mit der Erstellung von drei Videoclips. Die Außenaufnahmen wurden mit Schülerinnen und Schülern der Immanuel-Kant-Schule (Gymnasium) in Rüsselsheim und mit Unterstützung des Staatlichen Schulamtes für den Landkreis Groß-Gerau und den Main-Taunus-Kreis umgesetzt. Die Expertengespräche wurden in Frankfurt aufgenommen. Ziel war es, bei der Drehbuchgestaltung die Fragestellungen des Datenschutzes mit Hilfe von praxisnahen Szenen für die Schülerinnen und Schüler der Sekundarstufe I didaktisch aufzuarbeiten.

Eng verknüpft mit dem Recht auf „informationelle Selbstbestimmung“ als Persönlichkeitsrecht ist das „Recht am eigenen Bild“. Die Unterscheidung ist nicht immer direkt erkennbar. Die Schülerinnen und Schüler erleben, wie sie im Sportunterricht mit einer Kamera oder einer Drohne aufgenommen werden. Die Videoclips sind so aufgebaut, das Aspekte des Datenschutzes (DS-GVO), des Urheberrechts (UrhG) oder des Drohnenrechts (EU: Drohnenverordnung) szenisch aufgegriffen werden. In Expertengesprächen mit Mitarbeitern der Aufsichtsbehörden und der Initiative „Datenschutz geht zur Schule (BvD)“ werden die Szenen diskutiert und mit Hilfe von einfachen Fragestellungen wie „mein Ich gehört mir“ oder „gehört das Foto, auf dem ich abgebildet bin, wirklich mir“ besprochen. Am Beispiel der Drohnenaufnahme wird verdeutlicht, dass nicht alles, was gefilmt werden kann, auch gefilmt werden darf.

Links
https://www.bvdnet.de/datenschutz-geht-zur-schule/lehrerhandout/
https://www.bvdnet.de/datenschutz-geht-zur-schule/

9.6
Auskunftsrecht und die schutzwürdigen Belange Dritter

Das Recht auf Auskunft nach Art. 15 DS-GVO ist als umfassend zu sehen, wie der Bundesgerichtshof (BGH) und einige Oberlandesgerichte (OLG) in der Vergangenheit geurteilt haben. Allerdings ist das Auskunftsrecht des Einzelnen nicht schrankenlos. Bei der Gewährung der Auskunft müssen z. B. gemäß Art. 15 Abs. 4 DS-GVO die Rechte und Freiheiten anderer Personen beachtet werden. Damit werden in erster Linie die personenbezogenen Daten Dritter oder Betriebs- und Geschäftsgeheimnisse geschützt.

Was beinhaltet das Auskunftsrecht?

Mit dem Auskunftsrecht schafft Art. 15 DS-GVO eine Grundlage dafür, dass andere Betroffenenrechte (wie das Recht auf Berichtigung, Löschung, Einschränkung der Verarbeitung, aber auch das Widerspruchsrecht) überhaupt gezielt geltend gemacht werden können.

Art. 15 DS-GVO:

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

a) die Verarbeitungszwecke;

b) die Kategorien personenbezogener Daten, die verarbeitet werden;

c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;

d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;

f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;

h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(2) Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 46 im Zusammenhang mit der Übermittlung unterrichtet zu werden.

(3) [1]Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. [2]Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. [3]Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts Anderes angibt.

(4) Das Recht auf Erhalt einer Kopie gemäß Absatz 3 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Erwägungsgrund 63 DS-GVO

Eine betroffene Person sollte ein Auskunftsrecht hinsichtlich der sie betreffenden personenbezogenen Daten, die erhoben worden sind, besitzen und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können. Dies schließt das Recht betroffener Personen auf Auskunft über ihre eigenen gesundheitsbezogenen Daten ein, etwa Daten in ihren Patientenakten, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten. Jede betroffene Person sollte daher ein Anrecht darauf haben zu wissen und zu erfahren, insbesondere zu welchen Zwecken die personenbezogenen Daten verarbeitet werden und, wenn möglich, wie lange sie gespeichert werden, wer die Empfänger der personenbezogenen Daten sind, nach welcher Logik die automatische Verarbeitung personenbezogener Daten erfolgt und welche Folgen eine solche Verarbeitung haben kann, zumindest in Fällen, in denen die Verarbeitung auf Profiling beruht. Nach Möglichkeit sollte der Verantwortliche den Fernzugang zu einem sicheren System bereitstellen können, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen würde. Dieses Recht sollte die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, nicht beeinträchtigen. Dies darf jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird. Verarbeitet der Verantwortliche eine große Menge von Informationen über die betroffene Person, so sollte er verlangen können, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht, bevor er ihr Auskunft erteilt.

Art. 15 DS-GVO ermöglicht, vom Verantwortlichen eine Auskunft darüber zu erhalten, ob dieser überhaupt auf die eigene Person bezogene Daten verarbeitet und wenn ja, welche. Aus Erwägungsgrund (ErwG) 63 ergibt sich, dass Betroffene durch die Ausübung des Auskunftsrechts Bewusstsein über die Verarbeitung ihrer personenbezogenen Daten erlangen und in die Lage versetzt werden sollen, die Rechtmäßigkeit der Datenverarbeitung überprüfen zu können.

Hiervon umfasst sind alle Daten und Informationen mit Bezug zur Person (Art. 4 Nr. 1 DS-GVO), die beim Verantwortlichen vorhanden sind. Das Auskunftsrecht bezieht sich also nicht nur auf sogenannte Stammdaten wie etwa Name, Adresse und Geburtsdatum, sondern beispielsweise auch auf die mit ihnen geführte Kommunikation. Häufig ergeben sich Inhalt und Sinn von Informationen, die sich auf eine betroffene Person beziehen, auch erst aus dem Verarbeitungskontext (Beispiel: Korrespondenz zwischen Verantwortlichem und betroffener Person). In diesem Fall sind in der Regel die entsprechenden Dokumente auf Antrag vollständig (in Kopie) herauszugeben.

Die Inanspruchnahme des Auskunftsrechts ist grundsätzlich kostenlos. Wird dem Betroffenen eine Kopie der verarbeiteten Daten übermittelt, gilt dies allerdings nur für die erste Kopie (Art. 15 Abs. 3 Satz 2 DS-GVO). Nach Art. 12

Abs. 5 DSGVO darf nur bei offenkundig unbegründeten oder exzessiven Anfragen entweder ein Entgelt verlangt oder die Erteilung einer Auskunft verweigert werden. Exzessiv können Anträge insbesondere im Falle häufiger Wiederholung sein. An das Merkmal „häufige Wiederholung“ sind dabei strenge Maßstäbe anzulegen.

Grenzen des Auskunftsanspruchs

Auch das Recht aus Auskunft nach Art. 15 DS-GVO wird nicht grenzenlos gewährt. Bei der Gewährung der Auskunft müssen z. B. gemäß Art. 15 Abs. 4 DS-GVO die Rechte und Freiheiten anderer Personen beachtet werden. Damit werden in erster Linie die personenbezogenen Daten Dritter oder Betriebs- und Geschäftsgeheimnisse geschützt. Der Verantwortliche darf die Auskunft regelmäßig aber nicht vollständig verweigern, sondern muss beispielsweise die Namen dritter Personen in Dokumenten schwärzen, um ihre Identität nicht zu offenbaren.

Ein berechtigtes Interesse eines Dritten kann ebenfalls eine Begrenzung des Auskunftsanspruchs rechtfertigen. Es muss nicht notwendig durch eine Geheimhaltungsvorschrift geschützt sein. Zu denken ist hier insbesondere an den Fall, dass der Verantwortliche Informationen über die betroffene Person von einer oder einem Anderen – unter Umständen gegen eine Zusage vertraulicher Behandlung – erhalten hat, die oder der ein z. B. behördliches Einschreiten gegen einen Missstand erreichen möchte. Der Verantwortliche müsste hier nach Art. 15 Abs. 1 Halbsatz 2 lit. g DS-GVO grundsätzlich auch „alle verfügbaren Informationen über die Herkunft der Daten“ bereitstellen. Das Interesse der anderen Person an einer Geheimhaltung ihrer Identität als „Quelle“ überwiegt gegenüber dem Auskunftsinteresse jedenfalls solange, wie Anhaltspunkte dafürsprechen, dass die Offenbarung der Identität der Informantin oder des Informanten zu rechtlichen oder tatsächlichen Benachteiligungen der „Quelle“ führen könnten. Dies gilt umso mehr, soweit es sich um personenbezogene Angaben von Kindern oder Jugendlichen handelt.

Auskunftsanspruch einer Trainerin hat Grenzen

Im 47. Tätigkeitsbericht (Ziff. 4.1.1) wurde zum Auskunftsanspruch nach Art. 15 DS-GVO u. a. folgende Auffassung vertreten:

> „Die Bereitstellung einer strukturierten Zusammenfassung entspricht auch dem Ziel der DS-GVO, natürliche Personen bei der Verarbeitung ihrer personenbezogenen Daten zu schützen (vgl. Art. 1 Abs. 1 DS-GVO). Wird der Kopie-Begriff des Art. 15 Abs. 3 DS-GVO grundsätzlich weit ausgelegt, so besteht die Gefahr, dass das Auskunftsrecht des Art. 15 DS-GVO als allgemeines Recht auf Zugang zu Informationen oder als Akteneinsichtsrecht verstanden wird, mit der Folge, dass die

Geltendmachung von Art. 15 DSGVO nicht zur Verfolgung von Datenschutzzielen im Sinne der DS-GVO, sondern zur Verwirklichung anderer Ziele missbraucht wird."

Allerdings hat die jüngste Rechtsprechung des BGH vom 15. Juni 2021 (VI ZR 576/19) den Auskunftsanspruch sehr weitgehend gefasst. In der gleichen Weise haben das OLG München I in seinem Urteil vom 6. April 2019 (3 O 909/19) und das OLG Köln (Urteil vom 26. Juli 2019 – 20U 75/18) geurteilt.

In dem mir zur datenschutzrechtlichen Beurteilung vorgelegten Fall ging es um eine Turnsport-Trainerin, die bei einem Bundesleistungszentrum angestellt war. Diese sah sich Vorwürfen der dort trainierenden Jugendlichen ausgesetzt, u. a. psychische Gewalt ausgeübt und medizinisch unautorisiert Medikamente an die Trainierenden ausgegeben zu haben. Die Vorwürfe wurden vom verantwortlichen Deutschen Turner Bund (DTB) durch eine externe Rechtsanwaltskanzlei aufgearbeitet. In diesem Zusammenhang wurden die Jugendlichen interviewt und ihnen Vertraulichkeit zugesichert. Ein mehr als 100 Seiten starker Abschlussbericht wurde erstellt und dem DTB übergeben. In der Folge verlangte der Anwalt der Trainerin die Aushändigung des Berichts und berief sich dabei auf Art. 15 DS-GVO. Der DTB übermittelte daraufhin den Bericht, schwärzte jedoch die Passagen, die Rückschlüsse auf die Identität der interviewten Jugendlichen ermöglichten. Hiergegen legte der Anwalt Beschwerde bei mir ein.

Zunächst konnte ich feststellen, dass der DTB bereit war, dem Auskunftsersuchen grundsätzlich nachzukommen. Die erfolgten Schwärzungen erscheinen folgerichtig, geht es doch um die Aussagen der jungen Turnerinnen zum Verhalten der Trainerin gegenüber ihnen und anderen. Eine Anonymisierung der Angaben, also die Entfernung des Namens der Turnerinnen, konnte nicht greifen, da viele der von diesen geschilderten Sachverhalte und Situationen individuell und damit personenbeziehbar nachvollzogen werden konnten.

Zum Datenschutz bei der Verarbeitung von personenbezogenen Daten von Kindern enthält die DS-GVO leider keine allgemeinen Regelungen. Nur für die Datenverarbeitung im Zusammenhang mit einem Angebot von Diensten der Informationsgesellschaft gegenüber Kindern enthält Art. 8 DS-GVO Regelungen. Im ErwG 38 der DS-GVO wird jedoch die besondere Schutzbedürftigkeit von Kindern betont.

Erwägungsgrund 38 DS-GVO

Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind. Ein solcher besonderer Schutz sollte insbesondere die Verwendung personenbezogener Daten von Kindern für

Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden, betreffen. Die Einwilligung des Trägers der elterlichen Verantwortung sollte im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden, nicht erforderlich sein.

Der Auskunftsanspruch der Trainerin steht hier in Konkurrenz zum Recht der betroffenen Turnerinnen auf Schutz ihrer personenbezogenen Daten, die im Bericht in Form von Interviews enthalten sind. Zudem wurde den Betroffenen die Vertraulichkeit ihrer Aussagen zugesichert. Die Interessen der Jugendlichen wurden von mir in diesem Fall gegenüber dem Auskunftsanspruch der Trainerin als höherrangig eingeordnet. Im Übrigen wurde der Bericht, wenn auch nicht die von mir beschriebenen Passagen betreffend, dem Anwalt der Trainerin zugänglich gemacht.

Im Ergebnis hatte das Ansinnen des Rechtsanwaltes und seiner Mandantin, das ungeschwärzte Gutachten zur Kenntnis nehmen zu können, keine Aussicht auf Erfolg.

9.7
Erste datenschutzrechtliche Eindrücke zum Schulportal Hessen

Seit Beginn der Corona-Pandemie Anfang des Jahres 2020 erfreut sich das Schulportal Hessen (SPH) eines stetigen Zuwachses an Nutzerinnen und Nutzern. Während vor der Pandemie nur wenige hessische Schulen an das Schulportal angebunden waren, ist es mittlerweile der überwiegende Teil der Schulen in Hessen, der das Portal nutzt. Dies erscheint vor dem Hintergrund, dass viele Schülerinnen und Schüler in den Jahren 2020 und 2021 lange Zeit zu Hause beschult werden mussten und dass das SPH den Schulen vom Land Hessen kostenlos zur Verfügung gestellt wird, mehr als verständlich. Deshalb ist es umso wichtiger, dass das SPH den datenschutzrechtlichen Vorschriften entspricht.

Das Schulportal und der Datenschutz

Schon vor dem Ausbruch der Pandemie haben ich und das Hessische Kultusministerium (HKM) gemeinsam damit begonnen, die datenschutzrechtlichen Fragestellungen im Zusammenhang mit dem SPH zu erörtern. Aus den zum damaligen Zeitpunkt gesichteten Unterlagen konnte eine vorsichtige Tendenz herausgelesen werden, dass die Datenschutzkonformität der Plattform dem Anschein nach gewährleistet ist. So ist das SPH beispielsweise auf Open Source-Systemen aufgebaut, die in Deutschland gehostet werden, so dass

keine kritische Verarbeitung der Daten der Schülerinnen und Schüler wie auch der Lehrkräfte in einem unsicheren Drittland erfolgt. Eine abschließende datenschutzrechtliche Beratung und Bewertung war im Berichtszeitraum aufgrund der Größe des Projekts noch nicht möglich.

Mit Ausbruch der Pandemie und dem explosiven Wachstum der Zahl der Nutzerinnen und Nutzer des SPH erhielt die Frage nach der Datenschutzkonformität des Portals immer mehr Gewicht. Aus diesem Grund entschied ich im Rahmen der zur Verfügung stehenden Ressourcen, meine Beratungsleistung in diesem Bereich weiter zu erhöhen. So sollte die Erstellung eines vollständigen Datenschutzkonzepts sowie sämtlicher datenschutzrechtlich relevanter Unterlagen zum SPH beschleunigt werden.

Daraus folgten etliche Beratungstermine zwischen dem HKM und mir. Diese fanden sowohl auf der Arbeits- als auch auf der Leitungsebene statt und dienten dazu, die bereits vorliegende datenschutzrechtliche Dokumentation zum SPH gemeinsam zu besprechen und ihr Verbesserungspotenzial herauszuarbeiten.

Ein Ausblick in die Zukunft

Die Pandemie forderte einen großen Schritt in der Digitalisierung der Schulen, der in jedem Aspekt wichtige Datenschutzfragen hervorruft. Um diese zu lösen, habe ich eine umfassende Beratungsaufgabe. Aufgrund der fruchtbaren Zusammenarbeit zwischen dem HKM und mit ist bereits eine umfassende datenschutzrechtliche Dokumentation zum SPH entstanden, auf die im Jahr 2022 aufgebaut werden kann. Es ist mithin davon auszugehen, dass es mir in naher Zukunft möglich sein wird, das Portal abschließend zu bewerten.

Neben dem SPH gibt es noch weitere Projekte im schulischen Bereich, die ich derzeit beratend begleitet. Zum einen handelt es sich hierbei um einen geplanten einheitlichen Schulzugang. Dieser soll Einstiegsbarrieren bei der Nutzung von IT-Verfahren beseitigen. Es soll eine zentrale Zugangsseite eingerichtet werden, von der perspektivisch alle Anwendungen ohne erneute Anmeldung erreichbar sind. Dies bedeutet, dass beispielsweise der Zugang zum Schulportal, zur E-Mail für Lehrkräfte und zu den Portalen der Schulträger über eine Schul-ID und ein Passwort ermöglicht werden soll. Zum anderen möchte das Land Hessen ein landeseinheitliches Videokonferenzsystem für Schulen implementieren. Mit diesem soll den Schulen ein datenschutzkonformer Umgang mit Videokonferenzen ermöglicht werden.

10. Beratung des Hessischen Landtags

Eine wichtige Aufgabe der datenschutzrechtlichen Aufsichtsbehörde ist nach Art. 57 Abs. 1 lit. c DS-GVO, „im Einklang mit dem Recht des Mitgliedstaats das nationale Parlament … über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung (zu) beraten". Im Berichtszeitraum waren drei Beratungen des Hessischen Landtags von besonderer Bedeutung: zur Geltung der DS-GVO für die Datenverarbeitung im Landtag (Ziff. 10.1), zu einem neuen Petitionsgesetz für den Landtag (Ziff. 10.2) und zur Überarbeitung der Datenschutzordnung des Landtags (Ziff. 10.3).

10.1
Gilt die DS-GVO für den Hessischen Landtag?

Die DS-GVO gilt bezogen auf die Verarbeitung personenbezogener Daten im Hessischen Landtag nur für den administrativen Bereich. Zu diesem zählt auch die administrative Bearbeitung von Petitionen, nicht jedoch die Bearbeitung einer Petition durch ein Mitglied des Landtags als Berichterstatter und auch nicht die Beratung im Petitionsausschuss sowie die abschließende Entscheidung über die Petition durch das Landtagsplenum. Keine Geltung hat die DS-GVO für die legislativen und parlamentarischen Tätigkeiten des Landtags, der Fraktionen und der Abgeordneten.

Seit Inkrafttreten der DS-GVO ist umstritten, ob sie auch die Verarbeitung personenbezogener Daten in den Parlamenten der Mitgliedstaaten erfasst. Zwar hat der EuGH (C-272/19) durch Urteil vom 9. Juli 2020 festgestellt, dass der Petitionsausschuss des Hessischen Landtags (HLT) der DS-GVO unterliegt und ihn als Verantwortlichen nach Art. 4 Nr. 7 DS-GVO angesehen. Mit diesem Urteil hat er aber die entscheidende Frage nicht entschieden, ob dies auch für die parlamentarischen Tätigkeiten des Landtags gilt. Zu dieser Frage erbat der Präsident des Hessischen Landtags von mir ein Rechtsgutachten (s. auch Roßnagel/Rost, Ist die Datenschutz-Grundverordnung auch in den Landtagen anwendbar? Demokratische Souveränität und Unionsdatenschutz, NVwZ 2021, 1641).

I. Anwendungsbereich der DSGVO

Entscheidend für die Frage, ob der Anwendungsbereich der DS-GVO die parlamentarische Tätigkeit der Landtage, durch die die Landtagsabgeordneten

vor allem politische und legislative Ziele verfolgen, erfasst oder ausnimmt, ist die Vorschrift des Art. 2 Abs. 1 und 2 lit. a DS-GVO.

Art. 2 DS-GVO

(1) Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(2) Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten

a) im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt,

(…)

Art. 2 Abs. 1 bestimmt den sachlichen Anwendungsbereich der DS-GVO sehr weit. Soweit der HLT personenbezogene Daten verarbeitet, unterfallen auch sie diesem Tatbestand. Nach Art. 2 Abs. 2 lit. a DS-GVO findet die Verordnung jedoch „keine Anwendung auf die Verarbeitung personenbezogener Daten … im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt“.

Zur Frage, ob die Datenverarbeitung im Rahmen der parlamentarisch-legislativen Tätigkeit einer demokratisch gewählten Volksvertretung in Deutschland in den Anwendungsbereich des Unionsrechts und damit auch der DS-GVO fällt, gab es bis zum Urteil des EuGH keine Rechtsprechung. In der Literatur war die Antwort umstritten.

II. Entscheidung des EuGH vom 9. Juli 2020

Auf ein Vorabentscheidungsersuchen des VG Wiesbaden nach Art. 267 Abs. 1 AEUV hat der EuGH in seinem Urteil (C-272/19) vom 9. Juli 2020 festgestellt, „dass der Petitionsausschuss … insoweit, als dieser Ausschuss allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet, als ‚Verantwortlicher‘ im Sinne (des Art. 4 Abs. 7 DSGVO) einzustufen ist, so dass die von einem solchen Ausschuss vorgenommene Verarbeitung personenbezogener Daten in den Anwendungsbereich dieser Verordnung … fällt“.

In seiner Begründung fokussiert der EuGH stark auf die Tätigkeit des Petitionsausschusses und trifft keine grundlegenden Aussagen zur parlamentarischen Tätigkeit des HLT. Er weist dem Petitionsausschuss im Verhältnis zum HLT eine „Sonderrolle“ zu. Aus Sicht des EuGH ist er ein Gremium, das nur „mittelbar zur parlamentarischen Tätigkeit beiträgt“ und dessen Tätigkeiten „politischer und administrativer Natur“ sind. Für ihn nimmt er keine originär parlamentarische Aufgabe wahr, sondern ist ein „Verwaltungskontrollorgan“,

das eher einer Beschwerdekammer oder einer Ombudsperson entspricht. Ein Präjudiz für die Anwendbarkeit der DS-GVO für die allgemeinen parlamentarischen Aufgaben des HLT ergibt sich aus dem Urteil daher nicht unmittelbar.

III. Ausnahme des Art. 2 lit. a DSGVO

Die Frage nach dem Anwendungsbereich der DS-GVO ist daher direkt aus Art. 2 Abs. 2 lit. a DS-GVO zu beantworten. Danach ist entscheidend, ob die parlamentarischen Tätigkeiten des HLT und die politisch-legislativen Tätigkeiten der Abgeordneten in den Anwendungsbereich des Unionsrechts fallen.

Da die Verträge der Europäischen Union nur bestimmte Hoheitsrechte von den Mitgliedstaaten auf die Union übertragen, ist der Anwendungsbereich des Unionsrechts jeweils positiv zu bestimmen. Nach dem Grundsatz der beschränkten Einzelermächtigung gemäß Art. 5 Abs. 2 EUV kann die Union nur innerhalb der Grenzen der Zuständigkeiten tätig werden, die die Mitgliedstaaten ihr in den Verträgen zur Verwirklichung der darin niedergelegten Ziele übertragen haben. Demnach wäre der „Anwendungsbereich des Unionsrechts“ mit den Bereichen, für die der Union Gesetzgebungskompetenzen eingeräumt worden sind, gleichzusetzen. Dies ist für den Bereich der parlamentarisch-legislativen Tätigkeiten der Mitgliedstaaten nicht der Fall.

Doch selbst wenn vertreten würde, dass der „Anwendungsbereich des Unionsrechts“ weiter zu fassen sei als der Bereich, für den Gesetzgebungskompetenzen der Union bestehen, könnte dieser Anwendungsbereich nur so verstanden werden, dass er alle unionsrechtlich geregelten Sachverhalte umfasst, für die die Mitgliedstaaten unionsrechtliche Vorgaben zu beachten haben. Dies ist anzunehmen, wenn der Mitgliedstaat in dem jeweiligen Tätigkeitsbereich Unionsrecht zu vollziehen oder durchzuführen hat oder bei Vollzug oder Durchführung des Unionsrechts die Ausübung oder tatsächliche Verwirklichung der Grundfreiheiten der Unionsbürger zu beachten hat. Der Anwendungsbereich des Unionsrechts wäre dann eröffnet, wenn der Tätigkeitsbereich Gegenstand einer sekundärrechtlichen Regelung ist. Für die parlamentarischen Tätigkeiten des HLT gibt es keine spezifischen unionsrechtlichen Vorgaben. Auch erfassen die Grundfreiheiten diesen begrenzten Tätigkeitsbereich nicht.

Hinzu kommt, dass das Unionsrecht die nationale Souveränität der Mitgliedstaaten zu beachten hat. Aus Art. 4 Abs. 2 Satz 1 EUV ergibt sich die Rechtspflicht der Union, die jeweilige nationale Identität eines jeden Mitgliedstaats zu achten, die in ihren grundlegenden politischen und verfassungsmäßigen Strukturen einschließlich der regionalen und lokalen Selbstverwaltung zum Ausdruck kommt. Diese grundlegenden politischen und verfassungsmäßigen Strukturen und die Tätigkeitsbereiche, in denen diese zum Ausdruck

kommen, bestimmen die nationale Identität, die eine „äußerste Grenze für ein Tätigwerden der Union“ darstellt. In Deutschland deckt sich nach der Rechtsprechung des BVerfG der Begriff der verfassungsmäßigen Strukturen in Art. 4 Abs. 2 Satz 1 EUV mit der Verfassungsidentität, die über Art. 23 Abs. 1 Satz 3 i. V. m. Art. 79 Abs. 3 GG definiert wird. Die Identität der Bundesrepublik Deutschland bestimmt das BVerfG vor allem in seiner Lissabon-Entscheidung vom 30. Juni 2009 (BVerfGE 123, 267). Zur unionsrechtlich nicht antastbaren Verfassungsidentität gehören die „politischen Entscheidungen, die in besonderer Weise auf kulturelle, historische und sprachliche Vorverständnisse angewiesen sind, die sich im parteipolitisch und parlamentarisch organisierten Raum einer politischen Öffentlichkeit diskursiv entfalten“ (Rn. 247). Das Unionsrecht muss daher die Funktionsweise der politisch-parlamentarischen Demokratie in Hessen gemäß Art. 4 Abs. 2 Satz 1 EUV als Teil der nationalen Identität, die in ihren grundlegenden politischen und verfassungsgemäßen Strukturen zum Ausdruck kommt, respektieren. Die parlamentarischen Tätigkeitsbereiche des HLT liegen damit außerhalb der Regelungskompetenz des Unionsrechts und seiner Anwendung und damit auch außerhalb des Anwendungsbereichs der DS-GVO.

Dies gilt zum einen für die Tätigkeit der Volksvertretung und ihre Aufgaben als Gesetzgeber. Datenverarbeitungen im Rahmen des Gesetzgebungsverfahrens im engeren Sinne werden allein durch nationale Datenschutzvorschriften erlaubt und geregelt. Hierzu gehört auch die den Parlamentsbetrieb ordnende Tätigkeit des Präsidiums und des Ältestenrats des HLT sowie der Ausschusssekretariate. Zum anderen erfasst das Unionsrecht auch nicht die Wahl in Staatsämter durch den HLT. Drittens fallen aber auch die parlamentarisch-politische Willensbildung des HLT und die darauf bezogenen Tätigkeiten der Abgeordneten und der Fraktionen im Wettbewerb von Regierung und Opposition nicht in den Anwendungsbereich des Unionsrechts. Diese parlamentarisch-politischen Willensbildungsprozesse umfassen auch die Entwicklung eigener politischer Standpunkte, Initiativen und Konzepte, die Zusammenarbeit mit anderen Parlamenten, Kontakte zu anderen politischen Entscheidungsträgern und zu Interessengruppen sowie die Öffentlichkeitsarbeit des HLT, der Fraktionen und der Abgeordneten. Nicht unter die DS-GVO fällt viertens die politische Kontrolle der Regierung durch den HLT, die er insbesondere durch seine regulären Ausschüsse und durch temporäre Untersuchungsausschüsse ausübt. Diese ermöglichen insbesondere der politischen Opposition, das Handeln der Regierung zu untersuchen und zu bewerten sowie politische Alternativen darzustellen. Schließlich fällt die Bewilligung des Staatshaushalts nicht in den Anwendungsbereich des Unionsrechts.

Der Umstand, dass der HLT als Staatsorgan an das Grundrecht auf Datenschutz nach Art. 8 GRCh gebunden ist, bedeutet nicht, dass für ihn auch die DS-GVO anwendbar ist. Denn die DS-GVO ist nur eine von mehreren gesetzlichen Konkretisierungen des Grundrechtsschutzes, die miteinander konkurrieren, so dass von der Grundrechtsbindung nicht unmittelbar auf die Anwendbarkeit der DS-GVO geschlossen werden kann. Vielmehr konkretisiert der HLT im Rahmen seiner Parlamentsautonomie diese Bindung selbst, indem er sich eine seiner verfassungsrechtlichen Stellung entsprechende Datenschutzordnung gegeben hat (s. Ziff. 10.3).

IV. Anwendung der DSGVO auf den Verwaltungsbereich

Die besondere Bedeutung des HLT für den politisch-demokratischen Prozess und für die Identitätsbildung des Landes Hessen gilt jedoch nur für ihren politisch-legislativen-parlamentarischen Tätigkeitsbereich. Sie gilt nicht für seine verwaltenden Funktionen. Als Organisation mit personellen, sächlichen und finanziellen Ressourcen ist der HLT Verwaltungsbehörde. Daher wird seine verwaltende Tätigkeit vom Anwendungsbereich der DS-GVO erfasst. Dementsprechend regelt auch § 30 HDSIG (über die Öffnungsklausel des Art. 6 Abs. 2 DS-GVO) die Datenverarbeitung des HLT als Verwaltungsbehörde und unterstellt diese meiner Kontrolle.

10.2
Datenschutz im Petitionsgesetz

Im Berichtszeitraum erörterte der HLT einen Gesetzentwurf der Fraktionen der CDU, von BÜNDNIS 90/DIE GRÜNEN, der SPD und der FDP vom 11. Mai 2021 zu einem Gesetz über die Behandlung von Petitionen an den Hessischen Landtag (LT-Drs. 20/5734) und einen Entwurf der Fraktion DIE LINKE für ein Gesetz zur Regelung des Petitionsverfahrens im Hessischen Landtag (Hessisches Petitionsgesetz) (LT-Drs. 20/5743) und führte zu beiden Entwürfen am 9. September 2021 eine öffentliche Anhörung durch. Zu den Datenschutzregelungen dieser Gesetzentwürfe habe ich mit den Obleuten aller Fraktionen einen Vorschlag für eine Neufassung besprochen und zusammen mit der Landtagsverwaltung einen Regelungsvorschlag erarbeitet und in der öffentlichen Anhörung vorgestellt. Dieser wurde weitgehend vom HTL in das Hessische Petitionsgesetz vom 19. Dezember 2021 (GVBl. 2021, 926) übernommen.

Für die Regelung des Datenschutzes im Rahmen des Petitionsverfahrens musste das Urteil des EuGH vom 9. Juli 2020 zum Petitionsausschuss des HLT beachtet werden. Da der Petitionsausschuss nach diesem Urteil „Tätigkeiten … behördlicher Art“ ausübt, gilt für ihn die DS-GVO und er ist als Verantwortlicher nach Art. 4 Nr. 7 DS-GVO anzusehen. An dieses Urteil ist der HLT als Partei des EuGH-Verfahrens gebunden. Allerdings ist nach den Ergebnissen meines Gutachtens zur Geltung der DS-GVO für den HLT (s. Ziff. 10.1) zwischen der administrativen Bearbeitung von Petitionen durch die Landtagsverwaltung und ihrer Bearbeitung durch ein Mitglied des HLT als Berichterstatter und durch das Landtagsplenum zu unterscheiden. Nur soweit der Petitionsausschuss administrative Funktionen ausübt, gilt die DS-GVO. Soweit der HLT parlamentarische Tätigkeiten ausübt, gelten die Hessische Verfassung sowie die Geschäftsordnung und die Datenschutzordnung (DSO) des HLT. Für die Kontrolle der Datenverarbeitung für administrative Tätigkeiten bin ich, für die Kontrolle der Datenverarbeitung für parlamentarische Tätigkeiten ist das Datenschutzgremium nach § 11 DSO zuständig.

Im Hessischen Petitionsgesetz ist der Datenschutz in § 10 geregelt. Diese Vorschrift hat folgenden Wortlaut

§ 10 HPetG

(1) Daten zur Person der Petentin oder des Petenten und zum Gegenstand der Petition dürfen nur für Zwecke der Durchführung von Petitionsverfahren verarbeitet werden.

(2) Der Ausschuss ist im Rahmen der Wahrnehmung seiner Rechte befugt, personenbezogene Daten an die Landesregierung und andere öffentliche Stellen zu übermitteln.

(3) Es besteht kein Anspruch auf Einsicht in Petitionsakten des Landtages. Das Recht auf Auskunft und Kopie der personenbezogenen Daten nach Art. 15 der 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 (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72, 2018 Nr. L S. 2, 2021 Nr. L 74 S. 35) wird insoweit eingeschränkt, als

1. *der Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses des Landes Hessen das Interesse der betroffenen Person an Auskunft und Kopie überwiegt,*
2. *durch die Erteilung einer Auskunft oder Kopie der Schutz der betroffenen Person oder die Rechte und Freiheiten andere Personen beeinträchtigt werden oder*
3. *durch die Auskunft oder Kopie Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten geheim gehalten werden müssen.*

(4) Ab dem Zeitpunkt der Überweisung der Petition in den Ausschuss obliegt die Aufsicht über die Verarbeitung personenbezogener Daten dem Datenschutzgremium des Hessischen Landtages.

Absatz 1 erlaubt die Verarbeitung personenbezogener Daten, soweit sie für die Durchführung von Petitionsverfahren erforderlich sind. Dieser Erlaubnistatbestand ist trotz der Geltung der DS-GVO und ihres Anwendungsvorrangs zulässig, weil das Land Hessen die Öffnungsklausel des Art. 6 Abs. 1 UAbs. 1 lit. e und Abs. 3 DS-GVO nutzen und die Rechtsgrundlage für die Verarbeitungen festlegen kann und muss. Die Zweckfestlegung „nur zum Zweck der Petition“ begründet eine strenge Zweckbindung und stellt indirekt klar, wann die Daten nach Art. 17 Abs. 1 lit. a DS-GVO gelöscht werden müssen.

Gleiches gilt für den Erlaubnistatbestand des Absatzes 2, nach dem der Petitionsausschuss befugt ist, im Rahmen der Wahrnehmung seiner Anhörungs- und Untersuchungsrechte personenbezogene Daten an die Landesregierung und andere öffentliche Stellen zu übermitteln, die von der Petition betroffen sind. Auch diese Daten unterliegen einer entsprechenden Zweckbindung.

Absatz 3 schließt den verwaltungsrechtlichen Anspruch auf Akteneinsicht aus. Er schränkt aber auch das Recht auf Auskunft und Kopie der personenbezogenen Daten nach Art. 15 DS-GVO aus den drei genannten Gründen ein. Diese Einschränkungen der von der DS-GVO vorgesehenen Rechte der betroffenen Person sind sachlich geboten und nach Art. 23 DS-GVO zulässig.

Absatz 4 berücksichtigt die oben geforderte Differenzierung zwischen der Kontrolle durch mich über die administrative Bearbeitung der Petitionen und die parlamentarische Behandlung der Petitionen durch die Abgeordneten als Berichterstatter, durch den Ausschuss in seiner parlamentarisch politischen Funktion und durch das Landtagsplenum als abschließend politisch bewertende und entscheidende Stelle.

Der Schutz der Grundrechte der Petenten fordert grundsätzliche eine starke Aufsicht über die Verarbeitung ihrer Daten. Soweit die Landtagsverwaltung die Datenverarbeitung vornimmt und damit der DS-GVO unterliegt, ist diese Aufsicht durch mich mit Hilfe der Befugnisse nach Art. 58 DS-GVO und § 14 HDSIG gegeben. Dies betrifft im Wesentlichen die geschäftsführende Tätigkeit des Petitionsausschusses, vor allem etwa die Vorbereitung der Behandlung der Petition und die Ausführung der Entscheidungen der Petitionen. Diese Aufsicht muss im Petitionsgesetz nicht geregelt werden, sondern ergibt sich bereits aus dem HDSIG.

Keine Aufsicht durch mich besteht aber über die Abgeordneten als Berichterstatter, deren freie Entscheidung verfassungsrechtlich durch Art. 77, 95, 96 und 97 Hessische Verfassung gewährleistet wird. Die Datenverarbeitung durch Abgeordnete unterliegt vielmehr der Eigenkontrolle des Landtags, die er dem Datenschutzgremium nach § 11 DSO übertragen hat. Dieses Gremium und der Ältestenrat haben die Aufgabe und verfügen über die notwendigen Mög-

lichkeiten, in parlamentarischen Verfahren zu geeigneten Problemlösungen zu gelangen. Diese Ausnahme für Abgeordnete, den Petitionsausschuss und das Plenum wird durch Absatz 4 geregelt. Er überträgt die Aufsicht über die Verarbeitung personenbezogener Daten ab dem Zeitpunkt der Überweisung der Petition in den Ausschuss dem Datenschutzgremium des HLT.

10.3
Neufassung der Datenschutzordnung des Hessischen Landtags

Soweit die DS-GVO nicht für die parlamentarischen Tätigkeiten des Landtags gilt, muss der HLT die Gewährleistung des Grundrechts auf Datenschutz nach Art. 8 GRCh selbst regeln und die Aufsicht über die Einhaltung dieser eigenen Datenschutzregelungen selbst organisieren. Dies erfolgt durch die Datenschutzordnung (DSO) des HLT als Anhang 4 zur Geschäftsordnung des Landtags, bislang noch in der Fassung vom 18. Januar 2014. Auch wenn die DS-GVO für die parlamentarischen Tätigkeiten nicht gilt, ist die DSO den Begriffen und den Strukturen der DS-GVO anzupassen, um zu diesen anschlussfähig zu sein. Dabei sind die Erkenntnisse aus meinem Gutachten zur Nichtgeltung der DS-GVO zu berücksichtigen.

Zusammen mit der Landtagsverwaltung habe ich die Neufassung der DSO durch einen Entwurf der Regelungen unterstützt. Dieser berücksichtigt den auf parlamentarische Tätigkeiten des HLT eingeschränkten Anwendungsbereich der DSO. Obwohl die DS-GVO für diesen Anwendungsbereich nicht gilt, übernimmt der Entwurf Begriffsbestimmungen aus der DS-GVO, um mit diesen kompatibel zu sein. In einem allgemeinen Erlaubnistatbestand wird die Verarbeitung personenbezogener Daten bei der Wahrnehmung parlamentarischer Aufgaben für zulässig erklärt, soweit sie zur Erfüllung parlamentarischer Interessen erforderlich ist und überwiegende schutzwürdige Interessen der Betroffenen nicht entgegenstehen. Sonderregelungen bestehen für die Übermittlung personenbezogener Daten für nicht parlamentarische Zwecke, für die Datennutzung für den Zweck gemeinsamer parlamentarischer Tätigkeit von Abgeordneten und Fraktionen, für die elektronische Datenverarbeitung bei Petitionen sowie die Parlamentsdokumentation. Eigene Regelungen erfuhren auch die Rechte der betroffenen Personen auf Auskunft, auf Berichtigung, auf Löschung und auf Speicherbegrenzung von Daten. Die Zusammenarbeit mit Auftragsverarbeitern fand eine an Art. 28 DS-GVO angelehnte ausführliche Regelung. Neu aufgenommen wurden auch Regelungen zu einem Verzeichnis von Verarbeitungstätigkeiten und zu notwendigen technischen und organisatorischen Maßnahmen, um die personenbezogenen Daten ausreichend zu schützen. Schließlich wurde

im Entwurf die bisherige Regelung zum Datenschutzgremium des HLT als eigenständiges Datenschutzaufsichtsorgan übernommen.

Eine neue DSO des HLT war zum Ende des Berichtszeitraums noch nicht beschlossen, wurde aber am 23. Februar 2022 vom HLT verabschiedet.

11. Beschäftigtendatenschutz

Die Bedingungen des Datenschutzes von Beschäftigten werden sich massiv durch die Digitalisierung des Arbeitslebens, die Virtualisierung von Arbeitskontakten und Arbeitsabläufen (s. zu Home-Office Ziff. 11.2) und die Verbreitung smarter Geräte als Arbeitsmittel oder in der Arbeitsumgebung (s. zu GPS Ziff. 11.3) verändern. Dies ermöglicht, das Verhalten und die Leistung von Beschäftigen leichter, tiefer und umfassender zu erfassen. Diese Entwicklung hat durch die Corona-Pandemie einen zusätzlichen Schub erhalten, weil die Arbeitsleistung oft nur noch unter Verwendung von Informations- und Kommunikationstechnik erbracht werden konnte.

11.1 Aktuelle Entwicklungen im Beschäftigtendatenschutz

Zutrittskontrollen, Kontaktnachverfolgung, Testpflicht und Arbeiten im Home-Office – gerade in Beschäftigungsverhältnissen hat die Corona-Pandemie aber auch neue, eigenständige datenschutzrechtliche Fragestellungen hervorgerufen. So aktuell und wichtig das Thema ist – die fortschreitende Digitalisierung der Arbeitswelt und die hieran anknüpfenden Probleme des Beschäftigtendatenschutzes dürfen dabei nicht in Vergessenheit geraten.

Corona und Beschäftigtendatenschutz

Mit der Ausweitung von Testkapazitäten, der Möglichkeit des Impfens und mit den Sonderregelungen für geimpfte, getestete und genesene Personen wuchs im Frühjahr 2021 verständlich auch das Interesse von Arbeitgeberinnen und Arbeitgebern, die Impf-, Genesenen- und Testdaten ihrer Beschäftigten zu verarbeiten.

Zwangsläufig führte dies zu der Frage, auf welcher Rechtsgrundlage die Verarbeitung der Gesundheitsdaten im Beschäftigungsverhältnis erfolgen könne. Die Konferenz der Datenschutzbeauftragten der unabhängigen Aufsichtsbehörden des Bundes und der Länder (DSK) hatte in ihrer Entschließung vom 29. März 2021 „Corona-Virus: Impfnachweis, Nachweis negativen Testergebnisses und Genesungsnachweis in der Privatwirtschaft und im Beschäftigungsverhältnis gehören gesetzlich geregelt!“ (https://www.datenschutzkonferenz-online.de) bereits frühzeitig auf die Notwendigkeit hingewiesen, gesetzliche Regelungen zu treffen. Da – vor dem Hintergrund der anstehenden Bundestagswahl – keine entsprechenden Gesetzesvorhaben erkennbar waren und sich zeitgleich Anfragen von Unternehmen und Beschäftigten häuften, habe ich im Sommer eine Handreichung zum Thema

„Ist die Verarbeitung des Impf- und Genesenenstatus von Beschäftigten durch Arbeitgeber zulässig?“ veröffentlicht.

Am 24. November 2021 trat schließlich die Vorschrift des § 28b IfSG in Kraft. Sie macht den Zutritt zu Arbeitsstätten, in denen physische Kontakte nicht ausgeschlossen werden können, von der Einhaltung der 3-G-Regel (Abfrage des Impf-, Genesenen- oder Teststatus) abhängig und gestattet damit – bei Beachtung bestimmter Voraussetzungen – die Verarbeitung der im Rahmen der 3-G-Kontrolle anfallenden Gesundheitsdaten. Ich habe diese Entwicklung begrüßt, da hiermit den Forderungen der Datenschutzaufsichtsbehörden Rechnung getragen wurde. Da meine Behörde zur konkreten Umsetzung im Arbeitsalltag gleichwohl viele Anfragen erreichten, habe ich am 25. November 2021 auf meiner Webseite Empfehlungen zur datenschutzkonformen Umsetzung der 3-G-Regel am Arbeitsplatz veröffentlicht (https://datenschutz.hessen.de/datenschutz/arbeitgeber-und-besch%C3%A4ftigte/empfehlungen-zur-datenschutzkonformen-umsetzung-der-3-g).

Auch die DSK sah die Notwendigkeit der Klarstellung dieser und weiterer datenschutzrechtlicher Fragen im Zusammenhang mit der Corona Pandemie. Am 20. Dezember 2021 wurde daher die Anwendungshilfe „Häufige Fragestellungen nebst Antworten zur Verarbeitung von Beschäftigtendaten im Zusammenhang mit der Corona-Pandemie“ (https://www.datenschutzkonferenz-online.de/orientierungshilfen.html) veröffentlicht.

Neben der Frage, welche Daten zum Impf-, Genesenen- oder Teststatus der Beschäftigten der Arbeitgeber abfragen und verarbeiten darf, stellten sich auch Fragen danach, inwieweit er diese Daten kommunizieren darf. Denn der Impf-, Genesenen- oder Teststatus der Beschäftigten ist ja möglicherweise eine Grundlage für das Vertrauen in das Unternehmen bei persönlichen Kontakten nach außen oder bei Besuchen des Unternehmens. Dabei ist vor allem zu beachten, dass die Daten zum Impf-, Genesenen- oder Teststatus der Beschäftigten Gesundheitsdaten nach Art. 4 Nr. 15 DS-GVO sind, die einen besonderen Schutz erfordern. Daher ist die Veröffentlichung solcher Daten durch den Arbeitgeber über das Internet unzulässig (s. Ziff. 2.6).

Aufgrund der dynamischen Entwicklungen im Zusammenhang mit der Corona-Pandemie ist davon auszugehen, dass auch im Jahr 2022 datenschutzrechtliche Fragestellungen rund um diesen Themenkomplex nicht ausgehen werden.

Digitalisierung der Arbeitswelt

Auch wenn die Corona-Pandemie nicht ursächlich für die Digitalisierung der Arbeitswelt ist, hat sie den Prozess in mancher Hinsicht beschleunigt. Die

Kontaktvermeidung als wirksamstes Mittel der Infektionsbekämpfung hat zu einem signifikanten Anstieg etwa des Arbeitens im Home-Office sowie der Nutzung von Videokonferenzsystemen und Kollaborationsplattformen geführt. Da aus Arbeitgeberperspektive die Kontrolle der Arbeitsleistung oftmals nicht als gleichwertig mit den Möglichkeiten im Präsenzbetrieb angesehen wird, etablieren sich zunehmend neue Instrumente der Mitarbeiterüberwachung.

Bereits die genannten Themenkomplexe weisen eine Vielzahl datenschutzrechtlicher Fragestellungen auf, hier einige Beispiele:

– Wie kann ein sicherer Umgang mit personenbezogenen Daten, die Beschäftigte im Home-Office verarbeiten, gewährleistet werden? (s. Ziff. 11.2)
– Welche Anforderungen sind an einen datenschutzkonformen Einsatz von Videokonferenzsystemen und Kollaborationsplattformen, auch vor dem Hintergrund etwaiger Übermittlungen personenbezogener Daten an Drittländer, zu stellen? (s. Ziff. 4.2)
– Inwieweit ist die Überwachung der Arbeitsleistung von Beschäftigten unter Einsatz elektronischer Systeme im Home-Office zulässig und wo sind hier die Grenzen?

Als besondere Ausprägung der Überwachung der Arbeitsleistung haben mich im Berichtszeitraum die Themen Videotechnik, Geolokalisierung und Auswertung von Fahrverhaltensdaten in der Logistikbranche beschäftigt. Die Mitarbeiter und Mitarbeiterinnen gleich mehrerer Logistikunternehmen haben sich etwa mit folgenden Fragen an uns gewandt (s. Ziff. 11.3):

– Ist es zulässig, wenn die in einem Fahrzeug verbaute Technik das Verkehrsgeschehen überwacht und zusätzlich Bild- und Tonaufnahmen vom Innenraum der Fahrzeugkabine gefertigt werden?
– Dürfen die zur Routenplanung verarbeiteten GPS-Daten auch zu anderen Zwecken (z. B. zur Arbeitszeiterfassung oder zum Nachweis eines Arbeitszeitbetruges) genutzt werden?
– Ist die Verarbeitung von Fahrverhaltens- und Fahrzeugdaten durch Arbeitgeberinnen und Arbeitgeber zulässig?

Insgesamt zeigt sich an Hand des Beispiels der Logistikbranche, dass der digitale Wandel der Arbeitswelt in manchen Branchen bereits deutlich vorangeschritten ist. Dabei ist mit dem Einsatz von Videotechnik und GPS bei Weitem nicht das „Ende der Fahnenstange“ erreicht: Der steigende Einsatz von Informations- und Kommunikationstechnik über alle Arten von Beschäftigungsverhältnissen hinaus führt zu einer immer größer werdenden Menge von Beschäftigtendaten. Gleichzeitig werden die Möglichkeiten der Datenanalyse weiter verbessert und der Einsatz algorithmenbasierter

Entscheidungsunterstützungssysteme – etwa im Bewerbungsverfahren – ist schon heute Realität.

Bereits die alte Bundesregierung hat den hieraus erwachsenden Regelungsbedarf erkannt und den Beirat zum Beschäftigtendatenschutz damit beauftragt zu prüfen, ob es eines eigenständigen Gesetzes zum Beschäftigtendatenschutz bedarf. Im Januar 2022 hat der Beirat seinen Bericht mit Thesen und Empfehlungen unter https://www.denkfabrik-bmas.de/schwerpunkte/beschaeftigtendatenschutz veröffentlicht.

Die neue Bundesregierung beabsichtigt in ihrem Koalitionsvertrag nun ausdrücklich, neue Regelungen zum Beschäftigtendatenschutz zu treffen, und wird hierbei sicher auch die Ergebnisse des Beirats berücksichtigen. Mit Blick auf ein neues Gesetzgebungsverfahren könnte dabei auch die Bewertung des EuGHs zu der vom VG Wiesbaden vorgelegten Frage relevant sein, ob die hessische Vorschrift zum Beschäftigtendatenschutz in § 23 HDSIG den Anforderungen des Art. 88 DS-GVO genügt (VG Wiesbaden, Beschluss vom 21. Dezember 2020 – 23 K 1360/20.WI.PV, ZD 2021, 393).

Die Notwendigkeit der Fortentwicklung des Beschäftigtendatenschutzrechts ist kein neues Thema. Schon bei der Novellierung des Bundesdatenschutzgesetzes 2009 und der Regulierung einzelner Fragen des Beschäftigtendatenschutzes in § 32 BDSG-alt wurde im Gesetzgebungsverfahren festgestellt: „§ 32 enthält eine allgemeine Regelung zum Schutz personenbezogener Daten von Beschäftigten, die die von der Rechtsprechung erarbeiteten Grundsätze des Datenschutzes im Beschäftigungsverhältnis nicht ändern, sondern lediglich zusammenfassen und ein Arbeitnehmerdatenschutzgesetz weder entbehrlich machen noch inhaltlich präjudizieren soll.“ (Drucksache 16/13657, Seite 20) Ein erster Anlauf wurde 2010 mit dem Verfahren „Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes“ initiiert. Das Vorhaben scheiterte allerdings – nach viel Kritik – im Jahr 2013.

Die eingeleiteten Schritte zur Regelung eines Beschäftigtendatenschutzes unterstütze ich ausdrücklich. Wie der Bericht des Beirats zum Beschäftigtendatenschutz treffend herausgearbeitet hat, obliegt dem Gesetzgeber dabei die herausfordernde Aufgabe, das „Spannungsverhältnis zwischen den durch die Menschenwürde und den grundrechtlich geschützten Persönlichkeitsrechten und Interessen der Beschäftigten sowie den ebenfalls grundrechtlich geschützten Rechten und Interessen der Arbeitgeber durch ausgewogene Vorgaben zu regeln, um den verbindlich vorgegebenen Schutz der Beschäftigten durch ein wirksames Datenschutzrecht zu gewährleisten und auch bei einer weiterhin dynamisch fortschreitenden Digitalisierung der Arbeitswelt einen fairen Interessenausgleich herbeizuführen“ (Bericht des Beirats zum Beschäftigtendatenschutz, Seite 4 Ziffer II).

11.2
Nutzung von digitalen Instrumenten zur Mitarbeiterüberwachung

Im Berichtsjahr erreichten mich Beschwerden, in denen Beschäftigte angaben, durch Software-Anwendungen auf ihren dienstlichen Geräten von ihren Arbeitgebern überwacht zu werden. Solche Anwendungen sind in der Regel datenschutzrechtlich unzulässig.

Spätestens seit Beginn der Corona-Pandemie ist das Arbeiten im „Home-Office“ weit verbreitet. Zur Vermeidung von Kontakten gehen viele Menschen ihrer Bürotätigkeit von Zuhause aus nach. Das ermöglicht den Beschäftigten, ihre Kontakte zu reduzieren und Infektionen zu vermeiden. Für Arbeitgeberinnen und Arbeitgeber kann sich die Frage stellen, ob ihre Beschäftigten die übertragenen Aufgaben auch im Home-Office erledigen oder die Arbeitszeit auch für private Angelegenheiten nutzen.

Vor diesem Hintergrund gibt es einen wachsenden Markt zur digitalen Überwachung von Beschäftigten z. B. mittels Software-Anwendungen, die für diese Zwecke auf Dienstrechnern installiert werden. Um Leistungs- und Verhaltenskontrollen von Beschäftigten zu ermöglichen, nutzen solche Anwendungen eine Reihe möglicher Daten, die bei der ganz normalen Benutzung von IT-Geräten entstehen. Beginnend bei einfach zu erhebenden Informationen – wie etwa wann ein Mitarbeiter sich auf einem Gerät eingeloggt hat oder der Bildschirmschoner wegen Inaktivität aktiviert wurde –, können auch die Anzahl der Anschläge der Tastatur, die Dauer der sich im Fokus befindlichen, benutzten Anwendungen, die aufgerufenen Websites im Webbrowser bis hin zu regelmäßigen Screenshots aufgezeichnet werden. Bei mobilen Geräten wie beispielsweise Smartphones können zusätzlich auch GPS-Positionen und Bewegungsdaten verarbeitet werden.

Bei Nutzung von Software-as-a-Service-Angeboten (SaaS) werden die ermittelten Daten häufig direkt auf die IT-Systeme der Anbieter übertragen, dort aggregiert und ausgewertet. Den Arbeitgebern wird sodann oftmals der direkte Zugriff auf die Leistungs- und Verhaltensdaten der Beschäftigten ermöglicht. In Fällen, in denen Beschäftigte auch ihre privaten Endgeräte zur dienstlichen Aufgabenerledigung nutzen, oder wenn die private Nutzung von E-Mail und anderen Internetdiensten mittels der dienstlichen Geräte zugelassen ist, ist es zudem nicht unwahrscheinlich, dass auch die private Kommunikation und Aktivität der Beschäftigten erfasst und ausgewertet wird.

Vor dem Hintergrund der technischen Möglichkeiten und dem legitimen Interesse von Arbeitgebern, unter Beachtung der Persönlichkeitsrechte der Beschäftigten Leistungs- und Verhaltenskontrollen durchführen zu können, stellt sich somit die Frage, inwieweit die Überwachung der Arbeitsleistung von

Beschäftigten unter Nutzung elektronischer Systeme datenschutzrechtlich zulässig ist.

Der Einsatz jeglicher Instrumente zur Überwachung Beschäftigter ist an den datenschutzrechtlichen Anforderungen des § 26 Abs. 1 Satz 1 BDSG zu messen.

§ 26 Abs. 1 Satz 1 BDSG

[1]Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

Danach ist eine Verarbeitung personenbezogener Daten im Beschäftigtenverhältnis zulässig, wenn sie zur Durchführung des Beschäftigtenverhältnisses erforderlich ist. Eine solche Erforderlichkeit wird etwa für die Arbeitszeiterfassung angenommen. Nach § 16 Abs. 2 ArbZG sind Arbeitgeber dazu verpflichtet, die Arbeitszeit ihrer Beschäftigten zu erfassen, wenn diese über die in § 3 ArbZG festgelegte Arbeitszeit von acht Stunden pro Tag hinausgeht. Eine Anwendung, die die Arbeitszeiterfassung im Home-Office ermöglicht und darüber hinaus keine personenbezogenen Daten der Beschäftigten verarbeitet, ist daher als datenschutzrechtlich zulässig zu betrachten.

Anders ist die Rechtslage zu beurteilen, wenn eine Software weitergehende Datenverarbeitungsvorgänge betreibt. Einige Produkte, die als Software zur Arbeitszeiterfassung beworben werden, ermitteln die Anzahl der Tastaturanschläge oder fertigen regelmäßig Screenshots des Bildschirms an. Dies ist in aller Regel datenschutzrechtlich unzulässig, da solche Datenverarbeitungsvorgänge einen erheblichen Eingriff in das Recht der Beschäftigten auf informationelle Selbstbestimmung darstellen, der durch den Überwachungszweck nicht gerechtfertigt werden kann (BAG, Urteil vom 27.07.2017, 2 AZR 681/16, Rn. 21 ff).

Sofern es um Überwachungsmaßnahmen zur Aufdeckung von im Beschäftigungsverhältnis begangenen Straftaten geht, sind die strengen Voraussetzungen des § 26 Abs. 1 Satz 2 BDSG zu beachten.

§ 26 Abs. 1 Satz 2 BDSG

[2]Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigtenverhältnis eine Straftat begangen hat, die Verarbeitung erforderlich ist und das schutzbedürftige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Die Überwachung der Beschäftigten muss hiernach zur Aufdeckung von Straftaten erforderlich sein. Dabei gilt, dass keine sogenannte Ermittlung „ins Blaue hinein“ erfolgen darf, sondern bereits tatsächliche Anhaltspunkte für das Begehen einer Straftat im Beschäftigtenverhältnis vorliegen müssen. Diese sind zu dokumentieren. Zudem muss die Datenverarbeitung auch tatsächlich für die Aufdeckung der Straftat erforderlich sein und es ist eine Interessenabwägung durchzuführen.

Keinesfalls ist es datenschutzrechtlich zulässig, alle Beschäftigten unter Generalverdacht zu stellen und von vornherein präventiv zu überwachen. Genau eine solche verdachtsunabhängige und lückenlose Datenverarbeitung erfolgt aber je nach Konfiguration durch die meist angebotene Software zur Mitarbeiterüberwachung, so dass deren Einsatz auch nach § 26 Abs. 1 Satz 2 BDSG nur in seltenen Fällen zulässig sein dürfte. Der bloße Verdacht, dass Beschäftigte im Home-Office private Angelegenheiten erledigen, legitimiert nicht deren lückenlose Überwachung. Selbst wenn von Fällen des Arbeitszeitbetrugs auszugehen ist, wird die Nutzung der beschriebenen digitalen Überwachungsinstrumente regelmäßig schon nicht das mildeste Mittel sein, um den Verdacht der Straftat zu erhärten.

Nutzen Arbeitgeber Produkte zur Mitarbeiterüberwachung, die datenschutzrechtlich unzulässige Verarbeitungsvorgänge durchführen, so muss mit der Verhängung von Maßnahmen nach Art. 58 Abs. 2 DS-GVO gerechnet werden. Je nach Schwere des Verstoßes kann eine Verwarnung, eine Anweisung, die Datenverarbeitung in Einklang mit den Bestimmungen des Datenschutzrechts zu bringen, oder auch ein Verbot der Nutzung der eingesetzten Software in Betracht kommen.

Außerdem ist in solchen Fällen die Einleitung eines Bußgeldverfahrens zu erwägen, wobei Arbeitgeber sich im Rahmen eines Bußgeldverfahrens nicht durch den Einwand exkulpieren können, dass das eingesetzte Produkt mit dem Zusatz „DS-GVO-konform“ beworben wird. Als Verantwortliche im Sinn des Art. 4 Nr. 7 DS-GVO sind Arbeitgeber nach Art. 5 Abs. 2 DS-GVO für die Einhaltung der Grundsätze der Verarbeitung verantwortlich und rechenschaftspflichtig. Anwendungen, die geeignet sind, eine lückenlose Überwa-

chung der Beschäftigten zu ermöglichen, sind daher so zu konfigurieren, dass unzulässige Überwachungsmaßnahmen von vornherein ausgeschlossen sind.

Abschließend ist darauf hinzuweisen, dass Betriebsräte bei der Einführung und Anwendung von technischen Einrichtungen, die dazu geeignet sind, das Verhalten und die Leistung von Beschäftigten zu überwachen, nach § 87 Abs. 1 Nr. 6 BetrVG ein Mitbestimmungsrecht haben. Auch ist die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, nach § 26 Abs. 4 BDSG auf der Grundlage von Kollektivvereinbarungen zulässig. In Unternehmen, in denen ein Betriebs- oder Personalrat existiert, sollten daher vor der Einführung solcher Anwendungen Betriebsvereinbarungen abgeschlossen werden.

11.3
GPS-Tracking im Beschäftigungsverhältnis

Zunehmend wird GPS von Arbeitgebern zum Tracking von Dienstfahrzeugen und damit auch von Beschäftigten eingesetzt. Wo liegen die datenschutzrechtlichen Grenzen einer solchen Überwachung? Wie kann eine Ortung von Beschäftigten mittels GPS-Tracking datenschutzkonform gestaltet werden? Es kann datenschutzrechtlich zulässig sein, soweit die Interessen des Arbeitgebers und das Persönlichkeitsrecht der Beschäftigten in einen angemessenen Ausgleich gebracht werden und es auf das erforderliche Maß beschränkt ist.

Im Berichtszeitraum haben mich mehrere Anfragen und Beschwerden erreicht, die sich mit der Rechtmäßigkeit der Verarbeitung personenbezogener Daten mittels GPS-Tracking befassen.

GPS bedeutet Global Positioning System (globales Positionsbestimmungssystem). Die Technologie beruht auf einem globalen Navigationssatellitensystem und wird zur exakten Navigation oder Ortsbestimmung eingesetzt. Im hier betrachteten Zusammenhang wird ein GPS-Sender an Fahrzeugen angebracht und dient dazu, deren genauen Standort zu ermitteln.

Zu Beginn des Jahres wurde eine Beschwerde gegen ein international tätiges Transportunternehmen eingereicht. Der Beschwerdeführer berichtete, dass GPS-Tracker in die dort genutzten Fahrzeuge eingebaut worden seien.

Zur Begründung sei gegenüber den Beschäftigten ausgeführt worden, dass der Einbau der GPS-Tracker der Diebstahlsicherung, der Effizienzsteigerung, der Verbesserung der Dienstleistung, der Kontrolle unerlaubter Privatnutzung und der Sicherheit der Fahrerinnen und Fahrer sowie der Fahrzeuge

diene. Nach Auskunft des Beschwerdeführers würden die GPS-Daten der Fahrzeuge für sechs Monate gespeichert.

Als Ergebnis meiner Anhörung zu den Kategorien personenbezogener Daten, den Zwecken und Rechtsgrundlagen des Datenverarbeitungsverfahrens stellte sich der Sachverhalt wie folgt dar:

Das Unternehmen verarbeitete folgende Daten: Name des Fahrzeugbenutzers, den aktuellen Standort des Fahrzeuges, die aktuelle Geschwindigkeit des Fahrzeuges und die aktuellen Can-Bus-Daten (d. h. Zündung, Kilometerzähler, Kraftstoffverbrauch, Füllstand, Motorumdrehungen).

Zu den Verarbeitungszwecken wurde von dem Transportunternehmen ausgeführt, dass das GPS-Tracking:

– der schnellen Störungsbehebung und Effizienzsteigerung in der Routenplanung,
– der Sicherstellung der Einhaltung steuerrechtlicher Vorschriften,
– der Sicherheit der Fahrer (Unfall/Pannenhilfe),
– der Sicherheit der Fahrzeuge (Diebstahlschutz),
– der Effizienzsteigerung in der Fahrzeugbeschaffung (Qualität/Abnutzung der Fahrzeuge) und
– der Sicherstellung der Einhaltung arbeitsrechtlicher Vorgaben (Missbrauch der Tankkarte)

diene.

Als Rechtsgrundlagen für das Verarbeitungsverfahren wurden vom Verantwortlichen § 26 Abs. 1 und 2 BDSG sowie Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO genannt. Die Speicherdauer der erhobenen GPS-Daten wurde mit sechs Monaten angegeben. Zusätzlich teilte das verantwortliche Unternehmen mit, dass die Privatnutzung der Firmenfahrzeuge untersagt sei.

Meine rechtliche Bewertung ergab Folgendes:

Während des Prüfverfahrens zeigte sich, dass der Einsatz der GPS-Tracker in der beschriebenen Ausgestaltung gegen die Bestimmungen der DS-GVO verstößt. Ich habe dem Unternehmen meine Zweifel an der Rechtmäßigkeit der Datenverarbeitung mitgeteilt und insbesondere darauf hingewiesen, dass das GPS-Tracking von Dienstfahrzeugen datenschutzrechtlich zulässig sein kann, soweit es auf betriebliche Erfordernisse gestützt werden kann. Vor dem Hintergrund, dass durch GPS-Ortung die Rahmenbedingungen für unzulässige Leistungs- und Verhaltenskontrollen der Beschäftigten geschaffen werden können und für die Beschäftigten ein permanenter Leistungs- und

Kontrolldruck entstehen kann, ist an die Prüfung der Erforderlichkeit ein hoher Maßstab anzulegen.

Im Einzelnen ist zu den vorgetragenen Zwecken zur Datenverarbeitung mittels GPS-Tracking festzuhalten:

Schnelle Störungsbehebung und Effizienzsteigerung bei der Routenplanung

Die Verarbeitung personenbezogener Daten ist grundsätzlich dann zulässig, wenn sie auf eine der in Art. 6 Abs. 1 UAbs. 1 lit. a bis f DS-GVO genannten Erlaubnistatbestände gestützt werden kann. Aufgrund der Öffnungsklausel des Art. 88 DS-GVO ist die Datenverarbeitung im Beschäftigungsverhältnis an § 26 BDSG zu messen (dessen Unionsrechtskonformität wird derzeit in einem Vorabentscheidungsverfahren vom EuGH überprüft).

Bezüglich des GPS-Tracking sowie der hiermit einhergehenden Speicherung der personenbezogenen Daten der Fahrer kommen als mögliche Rechtsgrundlagen insbesondere Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO, spezifiziert durch § 26 Abs. 1 Satz 1 BDSG („Durchführung des Beschäftigungsverhältnisses“), in Betracht.

Beide Vorschriften verlangen, dass die Datenverarbeitung zur Erreichung des verfolgten Zwecks erforderlich ist. Insbesondere wenn es um die Verarbeitung von Beschäftigtendaten geht, sind im Rahmen der Erforderlichkeitsprüfung die betroffenen Grundrechtspositionen und widerstreitenden Interessen zur Herstellung praktischer Konkordanz abzuwägen und zu einem Ausgleich zu bringen, der die Interessen der Beschäftigten und des Arbeitgebers möglichst weitgehend berücksichtigt (BT-Drs. 18/11325, 98). Gefordert wird hierfür eine Prüfung am Maßstab des Verhältnismäßigkeitsgrundsatzes, was wiederum voraussetzt, dass der Verantwortliche einen legitimen Zweck verfolgt, das Verarbeitungsverfahren für die Verwirklichung dieses Zwecks geeignet ist und es sich um das mildeste aller gleich effektiv zur Verfügung stehenden Mittel handelt (vgl. BAG, Beschluss vom 9. April 2019 – 1 ABR 51/17, Rn. 39, NZA 2019, 1055 (1059)). Darüber hinaus muss es auch unter Abwägung der Umstände des Einzelfalles angemessen sein.

In dem zugrundeliegenden Fall habe ich festgestellt, dass die Störungsbehebung und Effizienzsteigerung bei der Routenplanung einen legitimen Zweck gem. § 26 Abs. 1 BDSG darstellt. Zur Verwirklichung des genannten Zwecks ist eine flüchtige Momentaufnahme (d. h., es stehen nur aktuelle GPS-Tracking-Daten zur Verfügung) aber ausreichend. Einer Speicherung der Daten bedarf es zur Erfüllung der verfolgten Zwecke hingegen nicht, sodass

die Speicherung für einen Zeitraum von sechs Monaten nicht erforderlich und damit unzulässig ist.

Einhaltung steuerrechtlicher Vorschriften

Nach allgemeiner Lebenserfahrung werden dienstliche Fahrzeuge, die auch zu privaten Zwecken zur Verfügung stehen, auch tatsächlich privat genutzt. Dafür spricht der Beweis des ersten Anscheins (BFH, Urteil vom 4. Dezember 2012 – VIII R 42/09). Ein privater Nutzungsanteil für einen Firmenwagen wird von der Finanzverwaltung nicht angesetzt, wenn der Verantwortliche nachweist, dass der Wagen nicht privat genutzt wird. Als Nachweis können vertraglich fixierte Nutzungsverbote gelten. Auch die Einführung eines GPS-Tracking Tools kann ein wirksames Mittel zur Nachweiserbringung gegenüber Steuerbehörden sein. Da die Privatnutzung der Firmenfahrzeuge aber von vornherein untersagt war, war nicht erkennbar, warum das GPS-Tracking zur Sicherstellung der Einhaltung steuerrechtlicher Vorschriften erforderlich gewesen sein sollte. Der Verantwortliche konnte auch nicht darlegen, dass es seitens der Steuerbehörden eine entsprechende Vorgabe gegenüber dem Unternehmen gegeben hätte. Aus datenschutzrechtlicher Sicht war die Speicherung daher nicht verhältnismäßig und somit unzulässig. Die Verhältnismäßigkeitsprüfung bezogen auf das Informationsinteresse des Arbeitgebers und das Persönlichkeitsrecht des Arbeitnehmers fiel daher zu Lasten des Arbeitgebers aus.

Sicherheit der Fahrer (Unfall/Pannenhilfe)

Die Erhebung und Speicherung der GPS-Tracking-Daten, um bei einem Unfall oder einer Panne schnelle Hilfe zu gewährleisten, ist als Maßnahme des Arbeitsschutzes zu qualifizieren und nach § 26 Abs. 1 Satz 1 BDSG in Verbindung mit den Bestimmungen des Arbeitsschutzgesetzes zu bewerten. Auch hier gilt der Erforderlichkeitsgrundsatz. Im konkreten Fall wurde bereits die Geeignetheit der Maßnahme von mir bezweifelt, da die im Falle eines Unfalls zur Verfügung stehenden Instrumente (Pannenhilfe, Notruf) für die Sicherheit der Fahrer geeigneter sein dürften. Jedenfalls die dauerhafte Speicherung der GPS-Daten der Fahrzeuge ist für diesen Zweck nicht erforderlich.

Sicherheit der Fahrzeuge (Diebstahlschutz)

Soweit vorgetragen wurde, dass das GPS-Tracking (auch) dem Zweck des Diebstahlschutzes und des Wiederauffindens der Fahrzeuge dient, habe ich kein Erfordernis einer ständigen Erfassung der Fahrzeugposition und einer Speicherung hierzu festgestellt. Für das Wiederauffinden eines entwendeten

Firmenfahrzeugs reicht die anlassbezogene Erhebung des Standorts des Fahrzeugs im Falle eines festgestellten Fahrzeugverlustes aus (so auch VG Lüneburg 4. Kammer, Teilurteil vom 19. März 2019, 4 A 12/19, Rn 39 f.).

Effizienzsteigerung in der Beschaffung (Qualität, Abnutzung der Fahrzeuge)

Durch die Datenverarbeitung mittels GPS-Tracking können effiziente und geeignete Fahrzeugtypen identifiziert werden. In der Beschaffung ermöglicht das Fahrzeugtracking ein Optimierungspotenzial, das sich etwa in Kosteneinsparungen realisieren ließe. Durch die Erhebung und Speicherung der Live Can Bus-Daten (Zündung, Kilometerzähler, Kraftstoffverbrauch, Füllstand und Motorumdrehungen) kann die Leistung der Fahrzeuge bewertet werden und damit auch entschieden werden, ob der Fahrzeugtyp für den verwendeten Zweck geeignet ist: So können Daten zum Verbrauch genutzt werden, um Fahrzeuge anzuschaffen, die einen geringeren Verbrauch aufweisen. Darüber hinaus kann auch relevant sein, ob Maximalkilometervorgaben eingehalten werden, die gemäß den jeweils anwendbaren Leasingverträgen berücksichtigt werden müssen.

Im Verhältnis zu den hierfür erhobenen Daten dürfte jedoch das Persönlichkeitsschutzinteresse der Beschäftigten überwiegen, da es sich um eine Speicherung von massenhaft erhobenen Daten der Betroffenen handelt.

Ich habe daher vorgeschlagen, die Live Can Bus-Daten zu pseudonymisieren und deren Speicherung auf drei Monate zu begrenzen. Nach drei Monaten kann eine Aggregation der Daten erfolgen, in welcher die durchschnittliche Effizienz der eingesetzten Fahrzeuge bestimmt wird.

Ferner habe ich die Abgabe einer freiwilligen Selbstverpflichtung darüber gefordert, dass die erhobenen Daten nicht mit anderen Mitarbeiterdaten zusammengeführt und nicht zu Leistungs- und Verhaltenskontrollen verwendet werden. Dieser Aufforderung ist das verantwortliche Unternehmen nachgekommen.

Sicherstellung der Einhaltung arbeitsrechtlicher Vorgaben (Missbrauch der Tankkarte)

Zu unterscheiden sind anlasslose präventive Kontrollmaßnahmen zur Überprüfung der Einhaltung von bestehenden arbeitsrechtlichen Pflichten und anlassbezogene repressive Mitarbeiterkontrollen bei einem konkret zu dokumentierenden Anfangsverdacht.

Anlasslose präventive Kontrollmaßnahmen zur Überprüfung der Einhaltung von bestehenden arbeitsrechtlichen Pflichten

Präventive Compliance-Kontrollen, die nicht auf einem personenbezogenen einfachen Anfangsverdacht einer Pflichtverletzung oder einer Straftat beruhen, können unter bestimmten Voraussetzungen nach der Rechtsprechung des Bundesarbeitsgerichts auf § 26 Abs. 1 Satz 1 oder 2 BDSG gestützt werden (BAG, Beschluss vom 9. Juli 2013 – 1 ABR 2/13, Rn. 20 ff.). Dies gilt vor allem für nach abstrakten Kriterien durchgeführte, keinen Arbeitnehmer besonders unter Verdacht stellende, offene, temporäre und stichprobenartige Überwachungsmaßnahmen, die der Verhinderung von Pflichtverletzungen oder Straftaten dienen sollen und ohne deren Durchführung keine verhaltenslenkende Wirkung entfaltet werden kann. Eine solche Maßnahme ist anzukündigen.

Anlassbezogene repressive Mitarbeiterkontrolle bei konkretem zu dokumentierendem Anfangsverdacht

Damit ein Ortungssystem zur Aufdeckung einer Straftat zulässig eingesetzt werden kann, ist es nach § 26 Abs. 1 Satz 2 BDSG notwendig, dass ein konkreter Anfangsverdacht einer Straftat vorliegt. Die repressive Mitarbeiterkontrolle greift erheblich in die Persönlichkeitssphäre ein, da eine gezielte Überwachung stattfindet.

Durch das Zulässigkeitserfordernis eines konkreten Tatverdachts wird verhindert, dass die gezielte Überwachung schrankenlos eingesetzt werden kann. Damit ein konkreter Tatverdacht vorliegt, müssen Tatsachen gegeben sein, die als Indizien für das Vorliegen einer Straftat gelten können. Es muss in persönlicher und räumlicher Hinsicht der objektiv begründete Anfangsverdacht einer Straftat bestehen.

Da § 26 Abs. 1 Satz 2 BDSG nur Straftaten im Beschäftigungsverhältnis regelt, trifft den Arbeitgeber eine Nachweispflicht, dass eine Straftat im Beschäftigungsverhältnis verübt wurde und der Einsatz eines Ortungssystems das wirkungsvollste Mittel zur Aufklärung darstellt. Zudem muss sich der konkrete Verdacht auf einen abgrenzbaren Kreis an Arbeitnehmern beziehen. Es ist nicht erforderlich, dass sich der Verdacht ausschließlich gegen eine Person richtet. Denkbar wäre ein Fahrerpool, welcher näher zu untersuchen wäre. Nicht zulässig wäre hingegen, alle Mitarbeiter unter einen Generalverdacht zu stellen.

Auch bei einer repressiven Ortung muss ein berechtigtes Interesse des Arbeitgebers an der Kontrollmaßnahme vorliegen. Im Rahmen einer Verhältnismäßigkeitsprüfung muss das Interesse des Arbeitgebers an der

Aufdeckung der Straftat den schutzwürdigen Arbeitnehmerinteressen an der Wahrung des Persönlichkeitsschutzes überwiegen. Im Rahmen der Interessenabwägung werden vor allem die Art und Schwere der Straftat, der Grad des Tatverdachts und die Schwere des Eingriffs in das Persönlichkeitsrecht berücksichtigt. An der Verhältnismäßigkeit kann es aufgrund des erheblichen Eingriffs in das Persönlichkeitsrecht bei Bagatelldelikten fehlen. Zudem ist die Ortung zu repressiven Zwecken zeitlich zu begrenzen. Sobald der Verdacht aufgeklärt ist oder es sich zeigt, dass die Straftat nicht aufgedeckt werden kann und die Maßnahme damit wirkungslos bleibt, ist die Ortung der Mitarbeiter einzustellen. Andernfalls erfolgt die Maßnahme unverhältnismäßig und damit unzulässig (s. a. Byers in Weth/Herberger/Wächter/Sorge, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl. 2019, Rn. 11 ff.).

Sowohl präventive als auch repressive Maßnahmen erlauben keine dauerhafte und umfassende Ortung der Mitarbeiter. Eine begrenzte Speicherung habe ich bei Vorliegen der oben genannten Fallkonstellationen für zulässig erachtet.

Das Unternehmen zeigte seine umfassende Bereitschaft, sich künftig datenschutzkonform zu verhalten, namentlich wie oben näher ausgeführt zu verfahren. Zu Gunsten des Unternehmens wirkte sich aus, dass eine komplette Dokumentation einschließlich einer Datenschutzfolgenabschätzung zum GPS-Tracking vorgelegt wurde und die Löschung der gespeicherten GPS-Tracking Daten nach Kenntnis der Unzulässigkeit ihrer Speicherung bestätigt wurde. Anzumerken ist ferner, dass die im Verstoßzeitraum gespeicherten Daten nicht zu Mitarbeiterkontrollen genutzt wurden. Die Beschäftigten wurden umfassend über die umgesetzten Maßnahmen informiert.

In Ausübung meines Ermessens habe ich daher von der Abgabe des Verfahrens an das Justiziariat meines Hauses zur Einleitung eines Bußgeldverfahrens abgesehen.

11.4
Interessenkonflikte bei Datenschutzbeauftragten

Die Vereinbarkeit der Tätigkeit als Datenschutzbeauftragter mit anderen Tätigkeiten im Unternehmen oder bei der öffentlichen Stelle ist immer wieder Gegenstand von Anfragen oder Beschwerden bei meiner Behörde. Nachfolgend werden einige relevante Konstellationen aufgezeigt.

Die DS-GVO enthält zu Interessenkonflikten bei Datenschutzbeauftragten in Art. 38 Abs. 6 DS-GVO lediglich eine kurze Regelung. Nähere Maßgaben

enthält die Verordnung nicht. Dementsprechend ist die praktische Anwendung der Norm mit einigen Unsicherheiten verbunden.

Art. 38 DS-GVO

(…)

(6) [1]Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. [2]Der Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

Grundsätzlich können Datenschutzbeauftragte neben den mit der Benennung einhergehenden Aufgaben, vgl. Art. 39 Abs. 1 DS-GVO, auch andere Aufgaben und Pflichten wahrnehmen, sofern diese sonstigen Tätigkeiten nicht zu einem Interessenkonflikt führen. Die Abwesenheit von Interessenkonflikten steht im engen Zusammenhang mit dem Erfordernis einer unabhängigen Tätigkeit, vgl. Art. 38 Abs. 3 Satz 1 DS-GVO. Es handelt sich sowohl um eine Benennungsvoraussetzung als auch – nach der Benennung – um eine Organisationspflicht des Verantwortlichen und des Auftragsverarbeiters.

Art. 38 DS-GVO

(…)

(3) [1]Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. [2]Der Datenschutzbeauftragte darf von dem Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. [3]Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters.

(…)

Datenschutzbeauftragte dürfen innerhalb des Unternehmens keine Position innehaben, bei der sie über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheiden. Um dies sicherzustellen, ist aufgrund der strukturellen Unterschiede des jeweiligen Unternehmens oder der jeweiligen Branche stets eine Einzelfallbetrachtung vorzunehmen. Gleichwohl lassen sich einige Leitlinien herausarbeiten.

Interessenkonflikte können sich regelmäßig aus der Stellung im Unternehmen ergeben (Inhaber, Mitglieder der Geschäftsführung oder des Vorstandes). Diese Personen sind originär für die Rechtmäßigkeit der Datenverarbeitung beim Verantwortlichen oder beim Auftragsverarbeiter verantwortlich und können sich nicht wirksam selbst kontrollieren (siehe auch Art. 38 Abs. 3 Satz 3

DS-GVO, nach dem der Datenschutzbeauftragte unmittelbar der höchsten Managementebene berichtet). Ferner ist in der Regel die Benennung von Leitungspersonen nicht zulässig: Dies gilt insbesondere für die Leitung der Personalabteilung (aufgrund der damit einhergehenden Verantwortung für den Umgang mit Beschäftigtendaten), die Leitung der IT-Abteilung (wegen der mit dieser Funktion einhergehenden Verantwortung für die technisch-organisatorischen Maßnahmen) sowie die Leitung der Marketing- oder Vertriebsabteilung (wegen der Verantwortung für den Umgang mit Kundendaten).

Auch ist eine Benennung bei hierarchisch nachgeordneten Positionen wie etwa Beschäftigte der IT- (insbesondere mit Administratorenrechten) oder Personal-Abteilung regelmäßig unzulässig, sofern diese in der Lage sind, Datenverarbeitungsprozesse zu bestimmen oder wesentlich zu beeinflussen.

Des Weiteren ist die Benennung eines Datenschutzbeauftragten regelmäßig unzulässig, sofern dieser ein besonderes wirtschaftliches Interesse an dem Unternehmenserfolg hat (etwa Gesellschafter sowie Familienangehörige der Geschäftsleitung).

Bei einem IT-Sicherheitsbeauftragten ist häufig ein die Benennung als Datenschutzbeauftragter ausschließender Interessenkonflikt anzunehmen. Die IT-Sicherheit ist zwecks Entdeckung von Missbrauch an umfassenden Sammlungen personenbezogener Daten interessiert. Ein Interessenkonflikt ist noch offensichtlicher, sofern der IT-Sicherheitsbeauftragte Aufgaben der Umsetzung (mit Budgetverantwortung) innehat.

Auch bei Compliance-Beauftragten sowie bei den Leitern der Rechtsabteilung ist häufig ein Interessenkonflikt anzunehmen. Diese sind oftmals in die unternehmensinternen Geschäftsprozesse derart eingebunden, dass sie aufgrund dieser weitergehenden Aufgabenwahrnehmung nicht mehr über die notwendige Unabhängigkeit in der Bewertung einzelner Datenverarbeitungsprozesse verfügen. Ferner ist ihre Tätigkeit mit der Sammlung möglichst vieler personenbezogener Daten verbunden. Gleichwohl kann dies je nach der Aufgabenwahrnehmung im Einzelfall auch anders zu bewerten sein (siehe dazu Bergt, in: Kühling/Buchner, Art. 38 Rn. 42; sowie abwägend Heberlein, in: Ehmann/Selmayr, Art. 38 Rn. 23).

Eher kritisch ist die Benennung eines Datenschutzbeauftragten zu bewerten, der zugleich Mitglied oder sogar Vorsitzende oder Vorsitzender des Betriebsrates ist. Die Kontrollbefugnis des Datenschutzbeauftragten umfasst auch die Datenverarbeitung durch den Betriebsrat, vgl. Art. 39 Abs. 1 lit. b DS-GVO, welche im Rahmen der Mitwirkungs- und Mitbestimmungsrechte auch Beschäftigtendaten einschließen kann (siehe dazu Heberlein, in: Ehmann/Selmayr, Art. 38 Rn. 24; Bergt, in: Kühling/Buchner, Art. 38 Rn. 45: „nicht

empfehlenswert“). Infolge einer Vorlage des BAG (ZD 2021, 701, 703 f.) an den EuGH wird dieser demnächst über diese Streitfrage entscheiden.

Interessenkonflikte können des Weiteren sogar bei externen Datenschutzbeauftragten auftreten. Insofern muss der Verantwortliche oder der Auftragsverarbeiter vertraglich mit dem externen Dienstleister regeln, dass dieser keine anderen Tätigkeiten übernimmt, die zu einem Interessenkonflikt mit den Aufgaben des Datenschutzbeauftragten für diesen Verantwortlichen oder Auftragsverarbeiter führen. Dies kommt insbesondere in Betracht, sofern der Datenschutzbeauftragte neben seiner Tätigkeit für das betreffende Unternehmen beruflich in demselben Geschäftsbereich tätig ist.

Ein unzulässiger Interessenkonflikt läge auch vor, wenn der externe Datenschutzbeauftragte gleichzeitig IT-Dienstleistungen erbringt oder den Verantwortlichen oder den Auftragsverarbeiter in datenschutzrelevanten Rechtsstreitigkeiten vor Gericht vertritt.

Zwecks Vermeidung von Interessenkonflikten sollten je nach Tätigkeiten, Größe und Struktur der Einrichtung einige Maßgaben durch Verantwortliche und Auftragsverarbeiter berücksichtigt werden. Insbesondere bei größeren Unternehmen ist die strukturelle Organisation mit den jeweiligen Aufgaben und Kompetenzen innerhalb einer internen Richtlinie eindeutig festzulegen, so dass das Bewusstsein für etwaige Interessenkonflikte gestärkt wird und diese möglichst von vornherein ersichtlich sind (siehe dazu näher Artikel-29-Datenschutzgruppe, Working Paper 243 – Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“), S. 19 f.).

Im Falle eines Interessenkonfliktes stehen mir verschiedene aufsichtsrechtliche Maßnahmen zur Verfügung. Neben dem Hinweis auf einen Verstoß gegen die DS-GVO gegenüber dem Verantwortlichen oder dem Auftragsverarbeiter gemäß Art. 58 Abs. 1 lit. d DS-GVO kann ich nach § 40 Abs. 6 Satz 2 BDSG die Abberufung des Datenschutzbeauftragten verlangen, wenn ein „schwerwiegender Interessenkonflikt“ vorliegt, vgl. Art. 58 Abs. 6 DS-GVO. Allerdings rechtfertigt nicht jeder Interessenkonflikt die Abberufung, vielmehr muss dieser offenkundig sein (etwa bei dem Leiter der IT-Abteilung) (siehe Dix, in: Kühling/Buchner, § 40 Rn. 17 m. w. N. auch zu der Frage der Europarechtskonformität der Regelung). Des Weiteren sind Verstöße gegen die Vermeidung von Interessenkonflikten nach Art. 83 Abs. 4 lit. a DS-GVO bußgeldbewehrt.

Art. 58 DS-GVO

Jede Aufsichtsbehörde verfügt über sämtliche folgenden Untersuchungsbefugnisse, die es ihr gestatten,

(…)

d) den Verantwortlichen oder den Auftragsverarbeiter auf einen vermeintlichen Verstoß gegen diese Verordnung hinzuweisen,

(…)

(6) [1]Jeder Mitgliedstaat kann durch Rechtsvorschriften vorsehen, dass seine Aufsichtsbehörde neben den in den Absätzen 1, 2 und 3 aufgeführten Befugnissen über zusätzliche Befugnisse verfügt. [2]Die Ausübung dieser Befugnisse darf nicht die effektive Durchführung des Kapitels VII beeinträchtigen.

§ 40 BDSG

(…)

(6) [1]Die Aufsichtsbehörden beraten und unterstützen die Datenschutzbeauftragten mit Rücksicht auf deren typische Bedürfnisse. [2]Sie können die Abberufung der oder des Datenschutzbeauftragten verlangen, wenn sie oder er die zur Erfüllung ihrer oder seiner Aufgaben erforderliche Fachkunde nicht besitzt oder im Fall des Artikels 38 Absatz 6 der Verordnung (EU) 2016/679 ein schwerwiegender Interessenkonflikt vorliegt.

(…)

Art. 83 DS-GVO

(…)

(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;

(…)

Für hessische öffentliche Stellen übernimmt § 7 Abs. 2 HDSIG die Vorschrift des Art. 38 Abs. 6 DS-GVO.

§ 7 HDSIG

(…)

(2) [1]Die oder der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. [2]Die öffentliche Stelle stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

(…)

Ein Interessenkonflikt bei behördlichen Datenschutzbeauftragten besteht ähnlich wie im nicht öffentlichen Bereich regelmäßig bei der Behördenleitung, bei dem Bürgermeister einer Gemeinde sowie bei herausgehobenen Leitungstätigkeiten (insbesondere bei der Leitung der Personalabteilung und bei der Leitung der IT-Abteilung). Die Benennung von Mitgliedern des Personalrates ist aufgrund der Kontrollpflichten des behördlichen Datenschutzbeauftragten gegenüber dem Personalrat kritisch zu bewerten. Grundsätzlich zulässig ist die Tätigkeit im Justiziariat ohne Leitungsfunktion sowie die Leitung des Rechnungsprüfungsamtes.

Die Sanktionsmöglichkeiten meiner Behörde sind bei behördlichen Datenschutzbeauftragten merklich eingeschränkt. Insofern kann ich gemäß Art. 58 Abs. 1 lit. d DS-GVO i. V. m. § 14 Abs. 1 HDSIG die öffentliche Stelle auf einen Verstoß hinweisen. Im Falle eines nicht behebbaren Interessenkonfliktes hat eine Abberufung zu erfolgen, vgl. § 6 Abs. 3 Satz 3 HDSIG.

§ 14 HDSIG

(1) [1]Die oder der Hessische Datenschutzbeauftragte nimmt im Anwendungsbereich der Verordnung (EU) Nr. 2016/679 die Befugnisse nach Art. 58 der Verordnung (EU) Nr. 2016/679 wahr. [2]Kommt die oder der Hessische Datenschutzbeauftragte zu dem Ergebnis, dass Verstöße gegen die Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten vorliegen, teilt sie oder er dies der öffentlichen Stelle mit und gibt dieser vor der Ausübung der Befugnisse des Art. 58 Abs. 2 Buchst. b bis g, i und j der Verordnung (EU) Nr. 2016/679 Gelegenheit zur Stellungnahme innerhalb einer angemessenen Frist. [3]Von der Einräumung der Gelegenheit zur Stellungnahme kann abgesehen werden, wenn eine sofortige Entscheidung wegen Gefahr im Verzug oder im öffentlichen Interesse notwendig erscheint oder ihr ein zwingendes öffentliches Interesse entgegensteht. [4]Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Mitteilung der oder des Hessischen Datenschutzbeauftragten getroffen worden sind. [5]Die Ausübung der Befugnisse nach Art. 58 Abs. 2 Buchst. b bis g, i und j der Verordnung (EU) Nr. 2016/679 teilt die oder der Hessische Datenschutzbeauftragte der jeweils zuständigen Rechts- und Fachaufsichtsbehörde mit.

(…)

§ 6 HDSIG

(…)

(3) [1]Die öffentliche Stelle stellt sicher, dass die oder der Datenschutzbeauftragte bei der Erfüllung ihrer oder seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. [2]Die oder der Datenschutzbeauftragte untersteht und berichtet unmittelbar der höchsten Leitungsebene der öffentlichen Stelle. [3]Die oder der Datenschutzbeauftragte darf von der öffentlichen Stelle wegen der Erfüllung ihrer oder seiner Aufgaben nicht abberufen oder benachteiligt werden.

(…)

Sollten gleichwohl Unsicherheiten über etwaige Interessenkonflikte bestehen, kann meine Behörde gerne zur weiteren Erörterung kontaktiert werden.

Abschließend ist noch einmal darauf hinzuweisen, dass die Kontaktdaten des Datenschutzbeauftragten meiner Behörde mitzuteilen sind, Art. 37 Abs. 7 DS-GVO. Dafür steht auf meiner Webseite ein Meldeformular zur Verfügung.

Art. 37 DS-GVO

(…)

(7) Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

12. Internet, Werbung

12.1
Es menschelt im Netz – Aus dem bunten Alltag der Beschwerdebearbeitung

Als Aufsichtsbehörde stehe ich beim Schutz des Persönlichkeitsrechts in der ersten Reihe und erfülle eine Vielzahl wichtiger, gesetzlich zugewiesener Aufgaben. Gerade dadurch werde ich aber nicht nur mit bedeutenden und grundlegenden Fragen des Datenschutzrechts konfrontiert, sondern häufig auch mit allzu menschlichen, kleineren und größeren Sorgen des digitalen Alltags.

Als unabhängige Datenschutz-Aufsichtsbehörde ist mir ein umfangreicher Katalog an Aufgaben zugewiesen, u. a. in Art. 57 DS-GVO, § 40 BDSG und § 13 HDSIG. Die Bearbeitung von Beschwerden nimmt dabei einen besonderen Stellenwert und einen erheblichen Anteil der täglichen Arbeit der Behörde ein (Ziff. 1).

Der Gesetzgeber hat dem Recht auf Beschwerde bei einer Datenschutz-Aufsichtsbehörde eine große Bedeutung eingeräumt. Nach Art. 57 Abs. 1 lit. f DS-GVO müssen sich die Aufsichtsbehörden mit Beschwerden vor allem von betroffenen Personen befassen, den Gegenstand der jeweiligen Beschwerde in angemessenem Umfang untersuchen und die jeweiligen Beschwerdeführerinnen und Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung unterrichten. Die Beschwerde ist ohne Form- und Fristerfordernisse möglich und ohne dass dabei Kosten für die sich Beschwerenden entstehen. Auch sollen ihnen aufgrund ihrer Beschwerde keine Nachteile durch die verantwortliche Stelle erwachsen.

Tatsächlich ist die Beschwerde ein gut geeignetes Mittel, mit dem Betroffene die zuständige Aufsichtsbehörde auf ein konkretes datenschutzrechtliches Problem aufmerksam machen und so individuelle Hilfe im Einzelfall erhalten können. Gleichzeitig kann die Aufsichtsbehörde auf diese Weise systematische Mängel bei Verantwortlichen aufdecken und abstellen.

Allerdings wird leider nicht jede Beschwerde auch diesen hehren Ansprüchen und Zielen gerecht. Immer wieder sind meine Mitarbeiterinnen und Mitarbeiter auch mit inhaltlich fragwürdigen, skurrilen, missbräuchlichen und gelegentlich sehr amüsanten Fällen konfrontiert, mit denen wir uns als Aufsichtsbehörde nichtsdestotrotz inhaltlich befassen müssen.

Es ist dem Persönlichkeitsrecht immanent, dass bei (vermeintlichen) Verletzungen eine individuelle und persönliche Betroffenheit vorliegt oder zumindest subjektiv wahrgenommen wird. Insofern sind nicht wenige Be-

schwerdeführerinnen und Beschwerdeführer beim Verfassen der Beschwerde erkennbar emotional aufgewühlt. Gerade bei datenschutzrechtlichen Problemen im Zusammenhang mit dem Internet ist das E-Mail-Programm oder das Beschwerdeformular auf meiner Website nur wenige Klicks von der Website oder App entfernt, die den Anlass für die Beschwerde gab. Nicht selten erwecken entsprechende Beschwerden den Eindruck, dass bei der Beschwerdeführerin oder dem Beschwerdeführer das Bedürfnis bestand, sich mit einer Beschwerde kurzfristig Genugtuung gegenüber einer soeben empfundenen Verletzung oder Benachteiligung zu verschaffen.

Diese steht allerdings nicht immer auch originär im Zusammenhang mit der Verarbeitung von personenbezogenen Daten. Nicht selten wird das Beschwerderecht offensichtlich dazu genutzt, einen „Nebenkriegsschauplatz“ für bereits bestehende, anderweitige Streitigkeiten zu eröffnen und bei der Aufsichtsbehörde vermeintliche Verstöße der Gegenseite anzuzeigen. So erreichen mich nicht selten Beschwerden z. B. von unzufriedenen Kunden, die ihrem Ärger über eine unglücklich verlaufene Geschäftsbeziehung mit einer Beschwerde über Cookies oder Datenschutzhinweise auf der Unternehmenswebsite Luft machen. Auch gehen immer wieder Beschwerden gegen die Websites von geschäftlichen Mitbewerbern oder gegen Privatpersonen ein, mit denen der Beschwerdeführer anderweitige persönliche oder familiäre Streitigkeiten hat.

So musste ich im Berichtszeitraum beispielsweise der Beschwerde eines Vaters gegen seinen eigenen, volljährigen Sohn nachgehen, der auf seiner privaten Website als Hobby-Genealoge den Familienstammbaum und damit auch die Lebensdaten seiner Eltern veröffentlicht hatte. Der datenschutzrechtlich ausgefochtene Familienstreit erzeugte neben dem üblichen, vorbereitenden Schriftverkehr zwei förmliche Bescheide, ein Eil- und ein Hauptsacheverfahren vor dem Verwaltungsgericht, eine Petition beim Hessischen Landtag des Vaters und eine weitere des Sohnes sowie eine Dienstaufsichtsbeschwerde gegen den Bearbeiter des Falles. Die Website ist inzwischen immerhin offline.

Vor allem kurz nach Inkrafttreten der DS-GVO, vereinzelt aber noch heute, kann auch der missverstandene Hinweis auf das Beschwerderecht bei der Aufsichtsbehörde deren Arbeit erschweren. Datenschutzinformationen nach Art. 13 DS-GVO, die bei jeder Datenverarbeitung zu erteilen sind, müssen immer auch einen Hinweis auf das Beschwerderecht bei der Aufsichtsbehörde enthalten. Die darin häufig angegebenen Kontaktdaten des HBDI werden immer wieder mit den Kontaktdaten der eigentlich zuständigen Stelle verwechselt. Gelegentlich wird das datenschutzrechtliche Beschwerderecht sogar als allgemeines Beschwerderecht gegen jegliche Entscheidung des Verantwortlichen missverstanden, unabhängig davon, ob diese mit der Verarbeitung

von personenbezogenen Daten im Zusammenhang steht. So erreichten mich beispielsweise zahlreiche Widersprüche gegen Bußgeldbescheide wegen Geschwindigkeitsübertretungen oder Beschwerden gegen die Festsetzung von Rundfunkbeiträgen ohne jeglichen Bezug zum Datenschutzrecht.

Auch unerwartete rechtliche Hürden können bei der Bearbeitung von Beschwerden auftauchen. So sieht das Datenschutzrecht nicht vor, dass Verantwortliche, die über die jeweiligen Datenverarbeitungsvorgänge entscheiden und diese damit auch rechtlich zu vertreten haben, volljährig sein müssen. Ein 11-jähriges Kind, das personenbezogene Daten eines anderen in einem sozialen Netzwerk weltweit verbreitet, ist somit ebenfalls Verantwortlicher. Genau dieser Fall wurde im Wege einer Beschwerde an mich herangetragen. Schon die Ermittlung eines Erziehungsberechtigten oder die Formulierung eines für einen 11-Jährigen verständlichen Anschreibens wäre in diesem Fall schwierig geworden. Glücklicherweise stellte sich der Hintergrund des Falls aber als Missverständnis beim Beschwerdeführer heraus, so dass dieser die Beschwerde zurückzog und tiefere Recherchen zum Schutz minderjähriger Verantwortlicher im Datenschutzrecht entbehrlich wurden.

Gelegentlich offenbaren sich in Beschwerden und an mich herangetragenen Anliegen auch völlig falsche und nicht selten amüsante Vorstellungen vom Datenschutz und von den Aufgaben und Kompetenzen einer Aufsichtsbehörde. So ist der HBDI weder technisch in der Lage noch rechtlich befugt, alle weltweit über eine bestimmte Person gespeicherten Daten zusammenzutragen und zu beauskunften oder gar zu löschen. Auch führt der HBDI keine geheimdienstlichen Operationen aus, kann nicht der gefühlten Verfolgung durch vermeintlich verwanzte Haushaltsgegenstände abhelfen, Anfragenden personenbezogene Daten von Dritten verschaffen, unerwünschte Apps auf dem Handy einer Beschwerdeführerin löschen, eine Entgeltpflicht für den Versand von E-Mails einführen oder die Zahlungspflicht des Rundfunkbeitrags aussetzen, da ein gefiedertes Haustier mit seinen Ausscheidungen den Fernseher unbrauchbar gemacht hat.

Datenschutzrechtliche Beschwerden entstammen dem prallen Leben und ihre Bearbeitung erfordert neben datenschutzrechtlichem Sachverstand oft auch Humor, Empathie oder auch die Beschäftigung mit Websites, die ansonsten von dienstlichen Rechnern nicht aufgerufen werden sollten. Bei berechtigten Beschwerden kann den Beschwerdeführerinnen und Beschwerdeführern gut geholfen und Datenverarbeitungsverfahren verbessert und sicherer gemacht werden. Andererseits werden aber leider auch eine Vielzahl unerfreulicher, querulatorischer oder augenscheinlich missbräuchlicher Beschwerden erhoben. Da die Beschwerdeführerinnen und Beschwerdeführer gerade bei solchen Beschwerden nicht selten besonders nachdrücklich auf die gesetz-

lich geschuldete Bearbeitung ihres Anliegens drängen, müssen auch diese, teilweise unter hohem Arbeits- und Zeitaufwand und Zurückstellung anderer Aufgaben, bearbeitet werden.

12.2
Die Cookie-Einwilligung – Fluch und Segen zugleich

Unzählige Beschwerden betreffen die Nutzung von Cookies und das Einbinden von datenschutzrechtlich relevanten Diensten auf Websites. In den meisten Fällen benötigen die Websitebetreiber eine Einwilligung der Nutzer, um Cookies setzen und damit Tracking-Daten verarbeiten zu können. Oftmals können oder möchten die Nutzer sich jedoch gar nicht vor jedem Besuch einer Website ausführlich mit diesem Thema beschäftigen.

Cookies sind bei der Internetnutzung allgegenwärtig. Während manche Cookies technisch erforderlich sind, um die jeweilige Grundfunktion einer Website zur Verfügung zu stellen, werden andere dazu verwendet, Nutzerdaten zu erheben und Nutzerprofile anzulegen, die der Webanalyse und insbesondere der Vermarktung von zielgruppenorientierter Werbung dienen. Vor allem letzteres birgt erhebliche Risiken für das Persönlichkeitsrecht der Nutzer, da es mit der Erstellung und Verarbeitung umfangreicher Persönlichkeitsprofile einhergeht (s. auch Ziff. 13.2. im 48. TB und Ziff. 13.1 im 49. TB).

Bereits seit 2009 gibt es europarechtliche Vorgaben für das Setzen von Cookies und für die Nutzung vergleichbarer Technologien, die im Dezember 2021 im neuen Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) umgesetzt wurden. So sieht § 25 TTDSG vor, dass Cookies grundsätzlich nur mit Einwilligung des Nutzers auf dessen Endgerät (PC, Smartphone etc.) gespeichert und von dort ausgelesen werden dürfen. Ausnahmen gelten lediglich dann, wenn das Setzen und Auslesen des Cookies unbedingt erforderlich ist, um einen vom Nutzer ausdrücklich gewünschten Dienst zur Verfügung zu stellen. Diese Regelung dient allerdings primär der Integrität des genutzten Endgeräts, mit dem ein bestimmter Dienst aufgerufen wird, und nur mittelbar dem Schutz des Persönlichkeitsrechts. So soll vor allem verhindert werden, dass Diensteanbieter ohne Wissen und ohne Zustimmung der Nutzer Cookies oder andere Daten auf deren Geräten speichern und auslesen und die Endgeräte somit zur eigenen Datenverarbeitung nutzen.

Das TTDSG regelt allerdings nicht, was mit gesetzten Cookies und vergleichbaren Technologien gemacht werden darf und für welche Zwecke und in welchem Umfang damit Nutzerdaten erhoben und verarbeitet werden dürfen. Dies soll in einer europäischen ePrivacy-Verordnung geregelt werden, die ursprünglich gemeinsam mit der DS-GVO im Jahr 2018 in Kraft treten sollte.

Da das Gesetzgebungsverfahren dazu jedoch noch immer nicht abgeschlossen ist, gelten derzeit auch für die Datenverarbeitung mittels Cookies die allgemeinen Regeln der DS-GVO. Danach können zwar bestimmte Datenverarbeitungen im Zusammenhang mit Cookies, die wenig Auswirkungen auf das Persönlichkeitsrecht haben (beispielsweise bei technisch erforderlichen First-Party-Cookies), ausnahmsweise auch ohne Einwilligung der Nutzer zulässig sein. Im Regelfall ist aber, insbesondere wenn es um Tracking geht oder weitere Dienstleister involviert sind, für die Erhebung und Verarbeitung von Daten mittels Cookies eine Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO erforderlich. Diese kann mit der nach § 25 TTDSG erforderlichen Einwilligung zum Setzen von Cookies verbunden werden.

Letztlich benötigen Anbieter somit in allen Fällen, in denen Cookies und vergleichbare Technologien nicht allein für technisch erforderliche, vom Nutzer gewünschte und gleichzeitig persönlichkeitsrechtlich unbedenkliche Zwecke eingesetzt werden, eine Einwilligung der Nutzer in das Setzen von Cookies sowie in die darauffolgende Datenverarbeitung mit diesen. Um diese einzuholen, nutzen die meisten Websitebetreiber ein sog. Cookie-Banner, das bei der ersten Nutzung der Website eingeblendet wird, diese optisch überlagert und mehr oder weniger ausführliche Informationen zu Cookies sowie Buttons enthält, mit denen die Einwilligung erteilt werden kann.

Die Erfahrung zeigt allerdings, dass die meisten Nutzer wenig Interesse haben und sich oftmals nicht die Zeit nehmen können oder wollen, vor dem Besuch einer Website ausführliche Informationen zu einem abstrakten Thema zu lesen und anhand dessen eine bewusste und differenzierte Entscheidung über den Einsatz von teilweise dutzenden Cookies zu treffen. Erschwerend kommt hinzu, dass es für Laien, selbst wenn die Anbieter ausführlich und transparent darüber informieren, kaum möglich ist, die komplexen rechtlichen und technischen Hintergründe der Datenverarbeitung mit Cookies nachzuvollziehen und deren persönlichkeitsrechtliche Auswirkungen einzuschätzen. Aus diesen nachvollziehbaren Gründen versuchen die meisten Nutzer die „Bearbeitung“ von Cookie-Bannern auf die schnellstmögliche Variante zu erledigen. Wohlwissend bieten die Websitebetreiber dazu in aller Regel eine prominente Möglichkeit an, mit einem einzelnen Klick eine Einwilligung zu erteilen und damit gleichzeitig den Cookie-Banner auszublenden, da dies auch ihren geschäftlichen Interessen entspricht.

Vor diesem Hintergrund ist es besonders wichtig, dass die Anbieter beim Einholen von Einwilligungen zumindest den rechtlichen Anforderungen gerecht werden und den Nutzern ermöglichen, eine echte, unbeeinflusste und freiwillige Entscheidung zu treffen. So muss beispielsweise neben einer einfachen Möglichkeit zum Erteilen der Einwilligung eine ebenso komfortable

Möglichkeit angeboten werden, die Einwilligung nicht zu erteilen und das Setzen von Cookies und die damit verbundene Datenverarbeitung abzulehnen.

Hinsichtlich der Ausgestaltung von datenschutzkonformen Cookie-Einwilligungen bestehen angesichts der wenig konkreten rechtlichen Regeln viele Unklarheiten. Unter anderem deshalb stimmt die Praxis der Anbieter in sehr vielen Fällen auch noch nicht mit den geltenden rechtlichen Anforderungen überein. Um diese verständlicher zu machen, hat die Datenschutzkonferenz im Dezember 2021 die Orientierungshilfe der Aufsichtsbehörden für Anbieterinnen und Anbieter von Telemedien ab dem 1. Dezember 2021 (OH Telemedien 2021) veröffentlicht (https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/DSK102_OH-Telemedien_20.12.2021.pdf), mit der die gleichnamige Orientierungshilfe aus dem Jahr 2019 aktualisiert wurde. Darin finden sich ausführliche und präzise Hinweise, welche genauen datenschutzrechtlichen Anforderungen beim Einholen von Cookie-Einwilligungen gelten.

Der Bundesgesetzgeber hat in § 26 TTDSG ein mögliches neues System angelegt, mit dem das Einholen und Erteilen von Cookie-Einwilligungen in Zukunft sowohl für die Anbieter als auch für die Nutzer vereinfacht werden soll. Dazu sollen neutrale Stellen (sog. PIMS – Personal Information Management Services) treuhänderisch das Management von Einwilligungen übernehmen und zwischen Nutzern und Anbietern vermitteln. So soll den Nutzern ermöglicht werden, an zentraler Stelle Entscheidungen zum jeweils gewünschten Umfang der Datenverarbeitung zu treffen, an die die verschiedenen Anbieter gleichermaßen gebunden sind. Die Entscheidung wird somit zeitlich vorverlegt und sowohl Nutzer als auch Anbieter würden von der Bürde befreit, unmittelbar vor jeder Nutzung einer neuen Website eine Einwilligung einfordern bzw. erteilen zu müssen. Vor der möglichen Etablierung von PIMS bedarf es jedoch zunächst noch einer konkretisierenden Rechtsverordnung durch die Bundesregierung. Es wird also noch einige Zeit vergehen, bis sich zeigt, ob PIMS tatsächlich die erhoffte Vereinfachung beim Erteilen von Einwilligungen mit sich bringen werden. Angesichts der unterschiedlichen Interessen der Beteiligten sowie fehlender wirtschaftlicher Anreize zur Umsetzung bestehen daran allerdings gewisse Zweifel.

Bis der Gesetzgeber spezielle Regeln für die Datenverarbeitung mit Cookies und vergleichbaren Technologien schafft und/oder sich durch die Etablierung von PIMS zumindest Vereinfachungen in der Praxis ergeben, obliegt jedem einzelnen Anbieter von Telemedien beim Einsatz einwilligungsbedürftiger Dienste die Aufgabe, rechtlich wirksame Einwilligungen der Nutzer einzuholen. Dabei alle rechtlichen Anforderungen zu beachten und die Nutzer ausführlich und verständlich zu informieren, ohne sie gleichzeitig zu überfordern oder abzuschrecken, ist eine herausfordernde und schwierige Aufgabe.

Dabei darf allerdings nicht vergessen werden, dass die Anbieter es selbst in der Hand haben, über die in ihren Angeboten eingebundenen Dienste und damit die Anzahl und Qualität der eingesetzten Cookies zu entscheiden. Je weniger datenschutzrechtlich problematische Dienste genutzt werden, desto weniger Aufwand muss der Anbieter beim Einholen der dafür erforderlichen Einwilligungen betreiben. Nicht zuletzt aus diesem Grund sollten die Anbieter von Telemedien die in ihren Websites und Apps eingebundenen Dienste hinterfragen und prüfen, ob sie tatsächlich benötigt werden oder nicht vielleicht doch verzichtbar sind bzw. zumindest durch datenschutzfreundlichere Alternativen ersetzt werden können.

13. Sozialwesen, Videoüberwachung

13.1 Bundesteilhabegesetz: Arbeitshilfe „Datenschutz in der Rehabilitation“

Nachdem bereits im Sommer 2019 ein Projekt „Datenschutz im trägerübergreifenden Reha-Prozess“ bei der Bundesarbeitsgemeinschaft für Rehabilitation (BAR) in Frankfurt am Main erfolgreich beendet wurde, war ich erneut als Vertreter der Bundesländer in einem darauf aufbauenden Folgeprojekt Mitglied einer Projektgruppe zur Ausarbeitung einer Arbeitshilfe zu dem oben genannten Thema. Rechtlicher Hintergrund für das Bestreben nach einer solchen weiteren, deutschlandweit verwendbaren Arbeitshilfe war die Neustrukturierung des SGB IX im Zuge des Bundesteilhabegesetzes (BTHG). Auch dieses Projekt konnte im Sommer 2021 mit einem guten Ergebnis beendet werden.

Im Herbst 2019 trat die BAR nach der erfolgreichen Beendigung eines (ersten) Projekts, der Erstellung einer Arbeitshilfe zum Themenkomplex „Datenschutz im trägerübergreifenden Reha-Prozess“ (vgl. meinen Beitrag im 48. TB, 6.4), erneut an die Mitglieder dieser Projektgruppe heran, um das komplexe Thema „Datenschutz in der Rehabilitation“ in einem weiteren (Folge-) Projekt aufzugreifen und zu vertiefen.

Gemeinsam gesetztes Ziel der Projektgruppe war es hier, noch nicht vertieft betrachtete Datenschutzaspekte bei der praktischen Zusammenarbeit im Reha-Prozess aufzugreifen. Konkret sollte es dabei insbesondere um die Zusammenarbeit der Reha-Träger mit Leistungserbringern, die Prozessphasen „Bedarfserkennung“, „Leistungsdurchführung“ und „Aktivitäten zum und nach Ende einer Leistung“ sowie die Querschnittsthematiken „Gutachten“ und „Entlassungsberichte“ gehen.

Neben dem BfDI, HBDI und Vertretern der BAR waren Teilnehmer dieser Projektgruppe erneut Vertreterinnen und Vertreter u. a. von

– Bundesministerium für Arbeit und Soziales,
– Bundesministerium für Gesundheit,
– Deutsche Rentenversicherung Bund,
– Deutsche Gesetzliche Unfallversicherung (DGUV),
– Bundesagentur für Arbeit,
– GKV-Spitzenverband,

– für die Bundesländer: Ministerium für Arbeit, Gesundheit und Soziales NRW,
– für die Integrationsämter: Zentrum für Familie und Soziales Bayern.

Der Kreis der beteiligten Akteure wurde, auch um deren Perspektive mit einbinden zu können, darüber hinaus um Vertreterinnen und Vertreter aus der praktischen Erbringung von Reha-Leistungen erweitert. Dazu gehörten z. B. die Bereiche Leistungserbringer oder Verbände von Menschen mit Behinderungen.

An insgesamt neun von der BAR in Frankfurt am Main organisierten Videokonferenz-Terminen im Zeitraum Dezember 2019 bis Juli 2021 wurde in ganztägigen Arbeitssitzungen das Projektthema durch die Teilnehmerinnen und Teilnehmer auf- und ausgearbeitet. Hinzu kamen zahlreiche bi- oder multilaterale Fachaustausche, Themenaufarbeitungen oder Abstimmungen zwischen unterschiedlichen Projektbeteiligten. Wie im vorherigen Projekt auch verliefen die Diskussionen der Vertreterinnen und Vertreter der verschiedenen Institutionen stets rücksichtsvoll mit Blick auf die jeweiligen Belange und waren konstruktiv wie pragmatisch orientiert. So war die Zusammenarbeit für alle Beteiligten, fachlich wie zwischenmenschlich, erneut angenehm und fruchtbar.

In der letzten Sitzung der Projektgruppe im Sommer 2021 konnte die Arbeitshilfe „Datenschutz in der Rehabilitation“ einstimmig verabschiedet werden. Das gemeinsam erarbeitete Ergebnis kann sich aus meiner Perspektive gut sehen lassen:

– Auf über 60 Seiten wird das Thema in seinen zahlreichen Facetten (nicht zuletzt auch aus der Perspektive des Datenschutzes) ausgearbeitet, inhaltlich dargestellt und erläutert sowie rechtlich eingeordnet.
– Sodann werden in veranschaulichenden Darstellungen auf über 20 Seiten Beispiele für zulässige Datenerhebungen und -übermittlungen in der Rehabilitation aufgeführt.
– Schließlich enthält die Arbeitshilfe noch zahlreiche Musterformulare, die auf nochmals über zehn Seiten integriert wurden.

Insgesamt ist so eine Arbeitshilfe mit über 100 Seiten entstanden.

Sie wurde im Herbst 2021 seitens der BAR in ihrem finalen Stand zunächst der Projektgruppe übersandt und in der Folge publik gemacht. Sie steht nunmehr auf der Internetpräsenz der BAR zum Download unter https://www.bar-frankfurt.de/fileadmin/dateiliste/_publikationen/reha_grundlagen/pdfs/AH_Datenschutz_II_final_barrierearm.pdf bereit und kann auch als gebundene Broschüre dort bezogen werden.

Für die Belange des Datenschutzes kann ich wie im vorlaufenden Projekt erneut bilanzieren, dass BfDI und HBDI in erfreulichem Sinn mitgestaltend Einfluss nehmen konnten und nunmehr ein Ergebnis miterzielt haben, das die Datenschutzperspektiven in den herausfordernden und schwierigen Sachzusammenhängen der unterschiedlichen Rehabilitationsphasen gut berücksichtigt.

13.2
Videoüberwachung in Einkaufspassagen

Unabhängig von den Eigentumsverhältnissen handelt es sich bei einer Einkaufspassage um einen öffentlich zugänglichen Raum. Eine Überwachung muss sich an den entsprechenden Rechtmäßigkeitsvoraussetzungen messen lassen.

Im Jahr 2019 erreichten mich gleich mehrere Beschwerden zur Videoüberwachung in und um eine Einkaufspassage mit angrenzender Wohnbebauung auf einer Liegenschaft in Innenstadtlage. Die Beschwerden erfolgten unabhängig voneinander durch zwei Privatpersonen sowie eine Bürgerrechtsgruppe.

Darstellung des Standortes

Im Einzelnen bestand die Einkaufspassage aus zehn Ladengeschäften, drei Gastronomiebetrieben und einem Theater. Das Untergeschoss bot Parkmöglichkeiten in einer öffentlichen Tiefgarage. Der angrenzende Wohnkomplex (mit über 200 Wohnungen) bestand aus mehreren Gebäuden, mit 14 überwiegend öffentlich zugänglichen Eingängen und Treppenhäusern. In unmittelbarer Nachbarschaft zu der Anlage befand sich eine Parkanlage sowie eine Drogensubstitutionseinrichtung, die im Rahmen einer bundesweiten Heroinstudie eingerichtet wurde.

Der Kamerabetreiber wurde von mir um Auskunft gemäß Art. 31 DS-GVO gebeten. Die Mitwirkung verlief zunächst mit Verzug, was sich jedoch nach Zwangsgeldandrohung änderte.

Der Kamerabetreiber teilte mit, dass sich in der Liegenschaft in der Vergangenheit zahlreiche Fälle von Drogenkriminalität, Drogenkonsum, Sachbeschädigung, Einbrüchen in Wohnungen und Kellern, Diebstahl sowie körperliche Übergriffe gegen Passanten und Beschäftigte mit zum Teil schweren Verletzungsfolgen zugetragen hätten. Auch aufgrund der in der Nachbarschaft liegenden Drogensubstitutionseinrichtung halte sich ein „problembehaftetes Milieu“ in der Passage und dem angrenzenden Wohngebäudekomplex auf. Treppenaufgänge und Nischen würden zum Übernachten, Drogenhandel und

-konsum genutzt. Im Wege der Wahrnehmung des Hausrechts würde die Überwachung zur Gefahrenabwehr, zur Abschreckung sowie zur Sicherung von Beweismaterial durchgeführt.

Überprüfung der Videoüberwachung

Gegenstand der Prüfung waren die Videoüberwachung des öffentlichen und privaten Raumes, die technische und organisatorische Gestaltung der Überwachung sowie die Erfüllung der Transparenzpflichten. Bei der Prüfung wurde unterschieden zwischen der Videoüberwachung im Wohngebäudekomplex und der Überwachung in und um die Einkaufspassage.

Wohnkomplex

Bei der Videoüberwachung im Wohnkomplex wurde noch vor dem aufsichtsbehördlichen Prüfverfahren zivilgerichtlich entschieden, dass ein Anspruch auf Entfernung der Kamera gemäß § 823 Abs. 1 BGB i. V. m. § 1004 Abs. 1 BGB i. V. m. dem aus Art. 2 Abs. 1 GG hergeleiteten Persönlichkeitsrecht nicht bestehe. Die Klage eines ehemaligen Bewohners der Wohnanlage gegen den Betreiber der Kamera, der gleichzeitig Eigentümer des Wohnkomplexes war, blieb in der Sache deshalb ohne Erfolg. Ein Anspruch auf die Entfernung der streitgegenständlichen Kameras bestand – unter Würdigung aller Umstände des Einzelfalls und nach umfassender Güter- und Interessenabwägung der Beteiligten – also nicht.

Im Rahmen einer Vor-Ort-Prüfung konnte zudem festgestellt werden, dass keine privaten Bereiche (wie Wohnungen oder Balkons) von der Überwachung umfasst waren. Die Überwachung erfolgte im Außenbereich, in den gemeinschaftlich genutzten, schwer einsehbaren Treppenaufgängen und Nischen, in denen es wiederkehrend zu Straftaten kam.

Anpassungen waren hier lediglich insofern notwendig, als die Mieter umfassend über die Überwachung zu informieren waren. Dies erfolgte mittels eines Rundschreibens.

Passage

Innerhalb der Einkaufspassage wurde die Videoüberwachung anhand von in der Prüfpraxis gängigen Prüfkriterien geprüft. Hierzu gehörte die Wahrung der berechtigten Interessen, der Erforderlichkeit für eine Überwachung und eine Interessensabwägung. Bei der Prüfung der berechtigten Interessen war zu berücksichtigen, dass ein Drittinteresse gem. Art. 4 Nr. 10 DS-GVO in Betracht kam, da hier eine typische Konstellation bei Einkaufszentren

vorlag, bei der der Vermieter die Überwachung auch im Interesse seiner Ladenmieter betrieb.

Der Kamerabetreiber gab an, dass die Überwachung der Passage ausschließlich innerhalb der Liegenschaft des Betreibers, also im privaten Bereich, stattfinde. Daher war zunächst zu prüfen, ob die Einkaufspassage als öffentlicher Raum gilt.

Öffentlich zugänglich sind Räume, wenn sie dem öffentlichen Verkehr gewidmet sind oder nach dem erkennbaren Willen des Berechtigten von jedermann genutzt oder betreten werden können.

Bei einer Einkaufspassage will der Betreiber, dass diese auch im Außenbereich (z. B. an Schaufenstern) von jedermann genutzt oder betreten werden kann. Die Eigentumsverhältnisse am Beobachtungsobjekt sind zunächst unbeachtlich. Entscheidend ist allein die durch den Berechtigten eröffnete tatsächliche Nutzungsmöglichkeit durch die Allgemeinheit, d. h. einen unbestimmten Personenkreis. Hierunter fallen z. B. Ausstellungsräume eines Museums, Verkaufsräume eines Warenhauses, ein jedem Besucher geöffneter Treppenaufgang zu einer Arztpraxis oder Anwaltskanzlei, Schalterhallen eines Bahnhofs ebenso wie der Bahnsteig oder der Bahnhofsvorplatz. Auch der vorherige Erwerb einer Eintrittskarte oder die Notwendigkeit einer Anmeldung steht dem nicht entgegen, wenn die Möglichkeit jedem eröffnet ist.

So verhielt es sich auch bei dieser Einkaufspassage. Bestimmter Zugangsvoraussetzungen bedurfte es nicht, so dass hier von einem öffentlich zugänglichen Raum auszugehen war.

Der Einsatz der Videoüberwachungseinrichtung in den Innenbereichen der Passage, bei den Lieferanteneingängen, in der Tiefgarage sowie der Tiefgaragenzufahrt und dem Müllplatz war überwiegend nicht zu beanstanden. Der Kamerabetreiber konnte weitreichende Informationen und konkrete Dokumentationen zu Ordnungswidrigkeiten und Straftaten vorlegen, die ein erhöhtes Schutzbedürfnis des Eigentums vor Vandalismusschäden begründeten. In der Abwägung der Belange überwogen hier die Interessen des Kamerabetreibers gegenüber allgemeinen Persönlichkeitsrechten der Passagebesucher.

Überwachung der Umgebung

Die im Außenbereich der Passage angebrachten Kameras waren so ausgerichtet, dass sie von der Außenhaut der Liegenschaft in den öffentlichen Raum (Straße / Gehweg) hinein zeigten. Die Grundstücksgrenze war dabei nicht gekennzeichnet und übergangslos gepflastert. Für Außenstehende war nicht ersichtlich, wo sich überwachte Bereiche befinden und ob gegebe-

nenfalls Bildbereiche geschwärzt sind. Alle Passanten, die an der Passage entlanggingen, sowie Menschen, die die angrenzende Bahnunterführung und den angrenzenden Verkehrsraum nutzten, mussten von einer weitreichenden Videoüberwachung ausgehen.

Im Rahmen der Erforderlichkeitsprüfung war zu klären, ob die Videoüberwachung zur Zweckerreichung geeignet war und ob alternative Maßnahmen, die nicht oder weniger tief in das Persönlichkeitsrecht eingreifen, im konkreten Einzelfall vorzuziehen waren. Vorgetragen wurden diverse Zwecke (Gefahrenabwehr, Abschreckung, Sicherung von Beweismaterial, Sicherheit von Beschäftigten). Für die an der Außenhaut der Passage installierten und in den öffentlichen Raum gerichteten Videokameras konnte jedoch keine Erforderlichkeit und keine hinreichende Zweckbegründung vorgetragen werden, so dass acht Kameras demontiert wurden.

Hinweisbeschilderung

Auf der Grundlage des Art. 13 Abs. 1 und 2 DS-GVO muss bei einer Videoüberwachung öffentlich zugänglicher Räume auf dem vorgelagerten Hinweisschild auf Folgendes hingewiesen werden:

– Umstand der Beobachtung – Piktogramm, Kamerasymbol,
– Identität des Verantwortlichen sowie gegebenenfalls seines Vertreters (nach Art. 27 DS-GVO), Name einschließlich Kontaktdaten,
– Kontaktdaten des betrieblichen Datenschutzbeauftragten – soweit benannt, dann aber zwingend,
– Verarbeitungszwecke und Rechtsgrundlage in Schlagworten,
– Angabe des berechtigten Interesses (soweit die Verarbeitung auf Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO beruht),
– gegebenenfalls Dauer der Speicherung,
– Hinweis auf die weiteren Pflichtinformationen (insbesondere Auskunftsrecht, Beschwerderecht, gegebenenfalls Empfänger der Daten) und den Zugang hierzu.

Die Hinweisbeschilderung wurde im Verfahren verordnungskonform angepasst.

14. Wirtschaft, Banken, Selbstständige

14.1
Selbstauskünfte sind auch bei Verschlüsselung gespeicherter Daten zu erteilen

Personenbezogene Daten werden aus Sicherheitsgründen häufig verschlüsselt gespeichert. Werden diese zur Verarbeitung entschlüsselt und erlangt der Verantwortliche hierdurch Zugriff auf die Daten, steht die Verschlüsselung einer Auskunftserteilung nicht entgegen.

Zum 13. Januar 2018 wurde in Deutschland die neue EU-Zahlungsdiensterichtlinie Payment Services Directive 2 (PSD2) in nationales Recht umgesetzt. Durch die Umsetzung sind für Verbraucher diverse Verbesserungen in Kraft getreten. Vor allem aber wurden zwei neue Dienste etabliert, die Verbraucher unabhängig von Kreditinstituten nutzen können. Bei diesen Diensten handelt es sich um die Zahlungsauslösedienste und die Kontoinformationsdienste.

Ein Zahlungsauslösedienst kann von einem Zahler beauftragt werden, um zu Lasten seines Bankkontos eine Überweisung auszulösen, z. B. um im Onlinehandel einen Bezahlvorgang vorzunehmen. Kontoinformationsdienste stellen einem Kontoinhaber konsolidierte Informationen zu einem oder mehreren Bankkonten zur Verfügung und können Dritten daraus gewonnene Informationen zur Bonitätsbeurteilung liefern. Beide Dienste können zur Durchführung von Zahlungen auch miteinander kombiniert werden.

Beide Dienste erfordern den Zugriff auf das Bankkonto und die dadurch erkennbaren Buchungen in Form von Zahlungen und Zahlungseingängen. Die Nutzung dieser Dienste schafft daher auch einen umfassenden Einblick der Dienstleister in die Vermögensverhältnisse sowie in die Konsum- und Zahlungsgewohnheiten des Nutzers und Kontoinhabers.

Allerdings unterfallen alle Leistungen nach der PSD2 und damit auch die Leistungen der vorgenannten Dienstleister der DS-GVO. Sie müssen daher datenschutzgerecht erbracht werden. Dies erfordert vor allem eine Begrenzung der Datenverarbeitung auf den beauftragten Zweck des Dienstes. Eine Datenverarbeitung ohne entsprechende Beauftragung darf nicht stattfinden.

Wird jedoch ein entsprechend umfangreicher Auftrag erteilt, ist auch eine entsprechend umfangreiche Datenverarbeitung zulässig. Schon deshalb empfehle ich eine sorgfältige Prüfung des Umfangs eines derartigen Dienstes vor Erteilung eines Auftrags und eine sparsame Nutzung dieser Dienste. Der Nutzen und die mit der Nutzung des Dienstes vorhandenen Einbußen an Privatsphäre sollten sorgfältig gegeneinander abgewogen werden.

Aufgrund der Anwendung der DS-GVO auf diese Dienste, unabhängig von ihrer datenschutzrechtlichen Zulässigkeit, ist auch eine Beachtung der Rechte von betroffenen Personen durch die Dienstleister erforderlich. In einem Beschwerdefall wurde die Erteilung einer Selbstauskunft gem. Art. 15 DS-GVO nicht durchgeführt. Der Dienstleister berief sich hierbei auf die aus Sicherheitsgründen verschlüsselten Daten. Die Verschlüsselung der Daten führe zu ihrer Anonymisierung. Eine Verarbeitung von personenbezogenen Daten, über die Auskunft erteilt werden könne, läge deshalb nicht vor. Dem entsprach zum Teil auch die verwendete Datenschutzerklärung. In dieser wurde ebenfalls auf die Verschlüsselung und darauf hingewiesen, dass die Daten nur von der betroffenen Person und unter Nutzung des hierfür erforderlichen Schlüssels abgerufen werden könnten. Dieser Schlüssel läge dem Dienstleister nicht vor. Er könne daher weder auf die Daten zugreifen, noch eine Auskunft gem. Art. 15 DS-GVO erteilen.

Dem widersprach jedoch der Inhalt des Dienstes. Dieser sah eine umfangreiche Verarbeitung und Auswertung der gespeicherten personenbezogenen Daten vor. Eine derartige Verarbeitung ohne vorherige Entschlüsselung der Daten war nicht plausibel. Dies erkannte der Dienstleister nach meinen Hinweisen auch und änderte daraufhin seine Datenschutzerklärung. Diese weist nun explizit auf die Prozesse hin, durch die auch der Dienstleister die personenbezogenen Daten entschlüsselt verarbeitet und diese auch durch Mitarbeiter gelesen werden können. Alle Prozesse waren vom Zweck der Verarbeitung umfasst, so dass keine unzulässige Verarbeitung vorlag. Der Umfang der Verarbeitung war lediglich in der Datenschutzerklärung fehlerhaft dargestellt, was bei betroffenen Personen und Mitarbeitern des Dienstleisters zu Missverständnissen und zur Verweigerung der Auskunft geführt hatte.

Auf meine Hinweise hin wurde auch die begehrte Auskunft erteilt. Zusätzlich wurden die internen Prozesse so umgestaltet, dass auch spätere Auskunftsanfragen datenschutzkonform erteilt werden. Zukünftig beabsichtigt der Dienstleister die automatisierte Erteilung von Auskünften nach Art. 15 DS-GVO.

14.2
Auskunftsanspruch vs. Tipping-Off-Verbot

Trotz Bestehens eines Anspruchs auf Auskunft nach Art. 15 DS-GVO dürfen Banken unter bestimmten Voraussetzungen zur Person gespeicherte Daten gegenüber den Betroffenen nicht beauskunften.

Das Thema „Umfang des Auskunftsanspruchs nach Art. 15 DS-GVO“ im Zusammenhang mit Kontokündigungen oder Ablehnungen von Vertragsabschlüssen ist immer wieder Inhalt von Beschwerden, die mich erreichen.

Gegenstand dieser Beschwerden ist oftmals, dass eine Bank die Geschäftsbeziehung mit der beschwerdeführenden Person ohne Angabe von Gründen einseitig gekündigt hat. Auf Nachfrage nach dem Grund der Kündigung beruft sich die Bank dann, zumindest zivilrechtlich auch zu Recht, oftmals auf die Regelungen aus den AGB, das Vertragsverhältnis ohne Angabe von Gründen kündigen zu können.

Datenschutzrechtlich ist bei der Bewertung derartiger Sachverhalte der Umfang des Auskunftsanspruchs nach Art. 15 DS-GVO zu berücksichtigen. Nach Art. 15 DS-GVO ist gegenüber Betroffenen die Auskunft zu erteilen, welche Daten zur Person gespeichert sind. Das bedeutet, dass ein im System der Bank kundenbezogen gespeicherter Grund für die ausgesprochene Kündigung auch dann in einer Auskunft nach Art. 15 DS-GVO enthalten sein muss, wenn zivilrechtlich eine Angabe von Gründen nicht erforderlich ist. Zivilrechtlich mag eine Kündigung auch ohne Angabe von Gründen wirksam sein. Dies ändert jedoch nichts am Umfang der Auskunftspflicht nach Art. 15 DS-GVO.

Allerdings ist der Auskunftsanspruch grundsächlich gegenüber dem Verantwortlichen geltend zu machen. Die bloße Nachfrage auf die Kündigung, aus welchen Gründen die Bank das Vertragsverhältnis gekündigt hat, ist in der Regel nicht als Auskunftsersuchen nach Art. 15 DS-GVO oder gar als Konkretisierung eines bereits vorliegenden Auskunftsersuchens im Sinne des Satzes 7 des Erwägungsgrunds 63 DS-GVO auszulegen, sofern diese Nachfrage ohne Bezugnahme auf das Auskunftsrecht erfolgt.

Erwägungsgrund 63 Satz 7 DS-GVO

Verarbeitet der Verantwortliche eine große Menge von Informationen über die betroffene Person, so sollte er verlangen können, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht, bevor er ihr Auskunft erteilt.

Wenn jedoch im Rahmen der Konkretisierung des Auskunftsersuchens nach Art. 15 DS-GVO explizit nach dem Grund der Kündigung gefragt wird, ist dieser in der Regel durch die Bank gegenüber dem Betroffenen, sofern gespeichert, auch zu beauskunften. Der Grund für die Kündigung würde damit dem Betroffenen zur Kenntnis gebracht. Gründe für eine einseitige Kündigung durch die Bank sind oftmals die fehlende Rentabilität der Geschäftsbeziehung oder eine nachhaltige Störung des Vertrauensverhältnisses zwischen Bank und Kunde.

Allerdings gibt es im Zusammenhang mit der Erfüllung des Auskunftsanspruchs auch Fallkonstellationen, in denen der Kündigungsgrund, selbst wenn dieser

gespeichert ist, nicht Bestandteil der Auskunft nach Art. 15 DS-GVO sein darf. Das ist zum Beispiel dann der Fall, wenn es gesetzliche Regelungen gibt, die den Verantwortlichen untersagen, bestimmte Informationen an die Betroffenen zu übermitteln.

Eine Norm, die bei dieser Fallkonstellation oftmals zum Tragen kommt, findet sich in § 47 Geldwäschegesetz (GWG), das sogenannte „Tipping-Off-Verbot“.

§ 47 GWG

(1) Ein Verpflichteter darf den Vertragspartner, den Auftraggeber der Transaktion und sonstige Dritte nicht in Kenntnis setzen von

1. *einer beabsichtigten oder erstatteten Meldung nach § 43 Absatz 1,*
2. *einem Ermittlungsverfahren, das aufgrund einer Meldung nach § 43 Absatz 1 eingeleitet worden ist, und*
3. *einem Auskunftsverlangen nach § 30 Absatz 3 Satz 1.*

Das „Tipping-Off-Verbot“ untersagt einem Verpflichteten nach § 2 GWG, u. a. den Vertragspartner (hier den gekündigten, ehemaligen Kunden) darüber zu informieren, dass gemäß § 43 Abs. 1 GWG eine Meldung über einen Sachverhalt an die Zentralstelle für Finanztransaktionsuntersuchungen (FIU) erfolgt ist. In der Regel handelt es sich bei derartigen Meldungen um sog. „Geldwäsche-Verdachtsmeldungen“.

Sofern also durch Nennung des Kündigungsgrunds gegenüber dem Betroffenen offenbart würde, dass eine solche Meldung seitens der Bank an die FIU abgesetzt worden ist, sind die Regelungen des § 47 GWG entsprechend zu beachten. Nach § 47 GWG i. V. m. Art. 23 Abs. 1 lit. e DS-GVO und § 29 Abs. 1 Satz 2 BDSG wäre die Beauskunftung des gespeicherten Datums „Kündigungsgrund“ in dieser Fallkonstellation somit ausdrücklich verboten.

Um derartige nationale Regelungen zu ermöglichen, hat der Verordnungsgeber mit dem Art. 23 DS-GVO eine Öffnungsklausel geschaffen. Art. 23 Abs. 1 DS-GVO ermöglicht den Mitgliedstaaten, unter bestimmten Voraussetzungen u. a. den Auskunftsanspruch nach Art. 15 DS-GVO zu beschränken.

Art. 23 DS-GVO

(1) Durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche oder der Auftragsverarbeiter unterliegt, können die Pflichten und Rechte gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5, insofern dessen Bestimmungen den in den Artikeln 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen, im Wege von Gesetzgebungsmaßnahmen beschränkt werden, sofern eine solche Beschränkung den

Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die Folgendes sicherstellt:

a) die nationale Sicherheit;

b) die Landesverteidigung;

c) die öffentliche Sicherheit;

d) die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit;

e) ***den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit;***

f) den Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren;

g) die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe;

h) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben a bis e und g genannten Zwecke verbunden sind;

i) den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen;

j) die Durchsetzung zivilrechtlicher Ansprüche.

Nach Erwägungsgrund 73 DS-GVO kann eine Beschränkung etwa dann erfolgen, wenn diese zur Aufdeckung und Verfolgung von Straftaten notwendig und verhältnismäßig ist. Nach § 261 StGB handelt es sich bei Geldwäsche um einen ebensolchen Straftatbestand.

Erwägungsgrund 73 DS-GVO

[1]Im Recht der Union oder der Mitgliedstaaten können Beschränkungen hinsichtlich bestimmter Grundsätze und hinsichtlich des Rechts auf Unterrichtung, Auskunft zu und Berichtigung oder Löschung personenbezogener Daten, des Rechts auf Datenübertragbarkeit und Widerspruch, Entscheidungen, die auf der Erstellung von Profilen beruhen, sowie Mitteilungen über eine Verletzung des Schutzes personenbezogener Daten an eine betroffene Person und bestimmten damit zusammenhängenden Pflichten der Verantwortlichen vorgesehen werden, soweit dies in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, um die öffentliche Sicherheit aufrechtzuerhalten, wozu unter anderem der Schutz von Menschenleben insbesondere bei Naturkatastrophen oder vom Menschen verursachten Katastrophen, die Verhütung, ***Aufdeckung und Verfolgung von Straftaten oder die Strafvollstreckung*** *– was auch den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt – oder die Verhütung, Aufdeckung und Verfolgung von Verstößen gegen Berufsstandsregeln bei reglementierten Berufen, das Führen öffentlicher Register aus Gründen des allgemeinen öffentlichen Interesses sowie die Weiterverarbeitung von*

archivierten personenbezogenen Daten zur Bereitstellung spezifischer Informationen im Zusammenhang mit dem politischen Verhalten unter ehemaligen totalitären Regimen gehört, und zum Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, etwa wichtige wirtschaftliche oder finanzielle Interessen, oder die betroffene Person und die Rechte und Freiheiten anderer Personen, einschließlich in den Bereichen soziale Sicherheit, öffentliche Gesundheit und humanitäre Hilfe, zu schützen. [2]Diese Beschränkungen sollten mit der Charta und mit der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten im Einklang stehen.

Der Gesetzgeber hat daher von der Öffnungsklausel Gebrauch gemacht und in § 29 Abs. 1 Satz 2 BDSG eine entsprechende einschränkende Regelung bezüglich des Auskunftsanspruchs nach Art. 15 DS-GVO geschaffen.

§ 29 BDSG

(1) [2]Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht nicht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.

Die Pflicht zur Erteilung einer Auskunft nach Art. 15 DS-GVO besteht also nicht, wenn die in Rede stehenden Informationen aufgrund einer Rechtsvorschrift geheim gehalten werden muss. Mithin finden die den Auskunftsanspruch beschränkenden Regelungen des § 47 GWG i. V. m. Art. 23 Abs. 1 lit. e DS-GVO und § 29 Abs. 1 Satz 2 BDSG auf den Kündigungsgrund Anwendung, sofern hiermit die Übermittlung einer Verdachtsanzeige durch die Bank an die FIU offenbart würde.

In derartigen Fällen ist die Bank folglich dazu verpflichtet, die Auskunft entsprechend zu beschränken, auch wenn die erteilte Geldwäscheverdachtsanzeige den Kündigungsgrund darstellt und dieser in den Systemen der Bank personenbezogen gespeichert ist. Die Auskunft ist dann dennoch als vollständig zu betrachten, auch wenn der Kündigungsgrund nicht genannt wird. Besteht neben der erteilten Geldwäscheverdachtsanzeige allerdings noch ein weiterer Kündigungsgrund, ist dieser in die Auskunft aufzunehmen.

14.3
Fehlversand von Kundenanschreiben

Der Fehlversand von Kundenanschreiben ist eine der am häufigsten von Verantwortlichen an die Aufsichtsbehörde gemeldeten Datenschutzverstöße. Nicht immer löst der Fehlversand die Meldepflicht nach Art. 33 DS-GVO aus.

Um über die Meldepflicht nach Art. 33 DS-GVO entscheiden zu können, ist jedoch in jedem Einzelfall eine entsprechende Risikobeurteilung vorzunehmen. Sofern Unsicherheiten bestehen, empfiehlt es sich, bei der Aufsichtsbehörde in Hessen, dem HBDI, nachzufragen.

Ein Fehlversand von Kundenanschreiben kann durch die fehlerhafte Adressierung eines Schreibens erfolgen. In diesem Fall kann sich aus dem weiteren Inhalt des Schreibens der eigentlich vorgesehene Adressat und der diesem zuzuordnende Sachverhalt ergeben. Ein Fehlversand kann sich aber auch daraus ergeben, dass einem richtig adressierten Schreiben Seiten hinzugefügt wurden, die nicht für den Kunden bestimmt waren, an den das Schreiben adressiert wurde. Auch hier können je nach Inhalt der falsch zugeordneten Seiten Informationen zu einer Person enthalten sein, die nicht den Empfänger des Schreibens betreffen. Selbst dann, wenn es sich bei dem Fehlversand um einen Serienbrief handelt, kann sich aus der Nennung einer weiteren Person ein Hinweis auf eine bestehende Kundenbeziehung ergeben. Auch hierbei handelt es sich um personenbezogene Daten. Der Fehlversand von Kundenanschreiben stellt daher grundsätzlich eine Datenschutzverletzung dar. Dennoch ist nicht jeder Fehlversand meldepflichtig im Sinne des Art. 33 DS-GVO. Eine Ausnahme besteht dann, wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Person führt.

Art. 33 DS-GVO

(1) [1]Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. [2]Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Maßgeblich für die Frage, ob eine Meldung nach Art. 33 DS-GVO erfolgen muss, ist also die Bewertung des Risikos, die aus der Datenschutzverletzung voraussichtlich entstehen kann. Das bedeutet, dass ein Verantwortlicher eine entsprechende Risikobeurteilung in dem jeweiligen Einzelfall vornehmen muss.

Bei einem Fehlversand von Unterlagen sind in dieser Risikobeurteilung insbesondere folgende Parameter zu berücksichtigen:

– Inhalt des Schreibens,

– Empfänger des Schreibens,
– betroffene Person.

Bei der Bewertung des Inhaltes des Schreibens ist in erster Linie auf die daraus zu entnehmenden Daten abzustellen. So wird eine Risikobeurteilung bei einer fehlerhaft versandten Terminbestätigung, aus der z. B. lediglich der Name der betroffenen Person und die bestehende oder sich anbahnende Geschäftsbeziehung zur verantwortlichen Stelle offenbart wird, anders ausfallen, als wenn dieses Schreiben auch noch Daten wie IBAN, Geburtsdaten, -ort und Anschriftendaten oder gar Vermögensaufstellungen oder Gesundheitsdaten enthielte. Diese Umstände würden sicherlich zu einer Meldepflicht führen.

Genau wie der Inhalt des Schreibens ist auch die Person des Empfängers bei der Beurteilung des Risikos von großer Bedeutung. Meldet sich beispielsweise der Empfänger selbst bei der verantwortlichen Stelle und händigt die zu Unrecht erhaltenen Unterlagen aus und bestätigt idealerweise zusätzlich, keine Kopien angefertigt zu haben, kann der Verzicht auf eine Meldung nach Art. 33 DS-GVO durchaus gut vertreten werden. Ist aber der Empfänger nicht zu ermitteln oder reagiert nicht auf Nachfragen und kann daher ein Risiko für die betroffene Person nicht ausgeschlossen werden, hat eine Meldung an die Aufsichtsbehörde nach Art. 33 DS-GVO zu erfolgen.

Neben dem Inhalt und dem Empfänger ist aber auch die betroffene Person selbst bei der Beurteilung des Risikos zu berücksichtigen. Wenn beispielsweise eine Person stark in der Öffentlichkeit steht und die zu Unrecht übermittelten Daten bei Bekanntwerden gegebenenfalls negative Auswirkungen, wie z. B. auf die öffentliche Wahrnehmung zur Person, haben könnten, sollte dieses ebenfalls in die Risikoabwägung mit einfließen.

15. Auskunfteien, Inkassounternehmen

15.1
Beauskunftung von Anschriftendaten durch Auskunfteien und Inkassounternehmen

Die Durchführung einer Adressrecherche seitens einer Gläubigerin sowie eines mandatierten Inkassounternehmens (IKU) im Rahmen einer Forderungsbeitreibung und die in diesem Zusammenhang erteilte Auskunft von aktualisierten Anschriftendaten des Schuldners oder der Schuldnerin seitens einer Auskunftei an diese sind aus datenschutzrechtlicher Sicht jeweils grundsätzlich zulässig. Jedoch kann im individuellen Einzelfall eine gesonderte Prüfung vor Auskunftserteilung erforderlich sein.

Im vorliegenden Fall war eine Schuldnerin während des Inkassoverfahrens umgezogen und hatte der Gläubigerin bzw. dem Inkassounternehmen (IKU) ihre aktuelle Anschrift nicht mitgeteilt. Zusätzlich hatte die Schuldnerin bei den zuständigen Meldebehörden ihres ehemaligen sowie neuen Wohnorts eine Auskunftssperre nach § 51 Bundesmeldegesetz (BMG) im Melderegister eintragen lassen. Um die Schuldnerin im Rahmen des Forderungsmanagements postalisch kontaktieren zu können, führte das mandatierte IKU eine Adressrecherche bei der SCHUFA Holding AG (SCHUFA) durch. Daraufhin übermittelte die SCHUFA diesem die neuen Anschriftendaten der Schuldnerin. Hierbei hatte die SCHUFA jedoch keine Kenntnis vom Vorliegen einer Auskunftssperre nach § 51 BMG; hierüber hatte sie die Schuldnerin nicht informiert. Die Schuldnerin bestritt mir gegenüber nicht das Bestehen der Forderung. Sie vertrat jedoch die Ansicht, die vorliegenden Datenübermittlungen (Anfrage des IKU sowie die Beauskunftung seitens der SCHUFA) seien aufgrund der eingetragenen Auskunftssperre jeweils unzulässig erfolgt. Konkrete Ausführungen zu den Gründen der eingetragenen Auskunftssperre machte die Schuldnerin mir gegenüber nicht.

Die vorliegende Datenverarbeitung ist jedoch in Fällen, in denen der Gläubigerin oder dem IKU die aktuelle Anschrift der Schuldnerin nicht mehr bekannt ist (beispielsweise aufgrund von im Rubrum des Titels ausgewiesener, bereits veralteter Anschriftendaten oder aufgrund eines Umzugs der Schuldnerin während des laufenden Inkassoverfahrens), auf Grundlage von Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO zur Durchsetzung der schuldnerseitigen Erfüllung des Vertrages mit der Gläubigerin sowie auf Grundlage von Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO zur Wahrung berechtigter Interessen des IKU grundsätzlich zulässig.

Art. 6 Abs. 1 UAbs. 1 DS-GVO lautet hinsichtlich der beiden Erlaubnistatbestände wie folgt:

Art. 6 DS-GVO

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

(…)

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Hinsichtlich der Einzelheiten bezüglich der grundsätzlichen Zulässigkeit der Datenverarbeitung durch IKU verweise ich zunächst auf meine Erläuterungen im Rahmen meines 49. Tätigkeitsberichts (Ziff. 12.3).

Eine Auskunftei darf demnach bei Vorliegen eines hierfür erforderlichen berechtigten Interesses ihrer Vertragspartnerin (hier: Gläubigerin oder IKU) Auskunft über Adressdaten der Schuldnerin oder des Schuldners im Rahmen des Forderungsmanagements erteilen. Die Realisierung der geschuldeten Forderung gegenüber der Schuldnerin oder dem Schuldner stellt grundsätzlich ein berechtigtes Interesse dar. Etwaige entgegenstehende überwiegende Interessen der Schuldnerin oder des Schuldners an einer Unterlassung dieser Auskunftserteilung sind grundsätzlich zunächst nicht ersichtlich.

Liegen Tatsachen vor, die die Annahme rechtfertigen, dass der betroffenen oder einer anderen Person durch eine Melderegisterauskunft eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen erwachsen kann, hat die Meldebehörde auf deren Antrag oder von Amts wegen gemäß § 51 BMG eine Auskunftssperre im Melderegister einzutragen.

§ 51 BMG lautet wie folgt:

§ 51 BMG

(1) Liegen Tatsachen vor, die die Annahme rechtfertigen, dass der betroffenen oder einer anderen Person durch eine Melderegisterauskunft eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen erwachsen kann, hat die Meldebehörde auf Antrag oder von Amts wegen unentgeltlich eine Auskunftssperre im Melderegister einzutragen. Ein ähnliches schutzwürdiges Interesse ist insbesondere der Schutz der betroffenen oder einer anderen Person vor Bedrohungen, Beleidigungen sowie unbefugten Nachstellungen. Bei der Feststellung, ob Tatsachen im Sinne des Satzes 1 vorliegen, ist auch zu berücksichtigen, ob die betroffene oder eine andere Person einem Personenkreis angehört, der sich auf Grund seiner beruflichen oder ehrenamtlich ausgeübten Tätigkeit allgemein in verstärktem Maße Anfeindungen oder sonstigen Angriffen ausgesetzt sieht.

(2) Sofern nach Anhörung der betroffenen Person eine Gefahr nach Absatz 1 nicht ausgeschlossen werden kann, ist eine Melderegisterauskunft nicht zulässig. Ist die betroffene Person nicht erreichbar, ist in den Fällen, in denen eine Auskunftssperre auf Veranlassung einer in § 34 Absatz 4 Satz 1 Nummer 1 bis 4, 6 bis 9 und 11 genannten Behörde von Amts wegen eingetragen wurde, die veranlassende Stelle anzuhören. Sofern eine Auskunft nicht erteilt wird, erhält die ersuchende Person oder Stelle eine Mitteilung, die keine Rückschlüsse darauf zulassen darf, ob zu der betroffenen Person keine Daten vorhanden sind oder eine Auskunftssperre besteht.

(3) Wurde eine Auskunftssperre eingetragen, sind die betroffene Person und, sofern die Eintragung auf Veranlassung einer in § 34 Absatz 4 Satz 1 Nummer 1 bis 4, 6 bis 9 und 11 genannten Behörde von Amts wegen erfolgte, zusätzlich die veranlassende Stelle über jedes Ersuchen um eine Melderegisterauskunft unverzüglich zu unterrichten.

(4) Die Auskunftssperre wird auf zwei Jahre befristet. Sie kann auf Antrag oder von Amts wegen verlängert werden. Die betroffene Person ist vor Aufhebung der Sperre zu unterrichten, soweit sie erreichbar ist. Wurde die Sperre von einer in § 34 Absatz 4 Satz 1 Nummer 1 bis 4, 6 bis 9 und 11 genannten Behörde veranlasst, ist diese zu unterrichten, wenn die betroffene Person nicht erreichbar ist.

(5) Die Melderegisterauskunft ist ferner nicht zulässig,

1. *soweit die Einsicht in ein Personenstandsregister nach § 63 des Personenstandsgesetzes nicht gestattet werden darf und*
2. *in den Fällen des § 1758 des Bürgerlichen Gesetzbuchs.*

Diese Auskunftssperre nach § 51 BMG erstreckt sich jedoch ausschließlich auf Auskünfte der Meldebehörde. Die Meldebehörde unterrichtet die Auskunfteien in Deutschland auch nicht präventiv über die Eintragung von Auskunftssperren im Melderegister zu den betroffenen Personen. Eine solche Datenübermittlung wäre bereits deshalb unzulässig, weil hierfür keine gesetzliche Grundlage besteht.

Folglich hat eine Auskunftei hiervon zunächst keine Kenntnis – es sei denn, die Auskunftei wurde seitens des Schuldners oder der Schuldnerin über diesen Sachverhalt in Kenntnis gesetzt.

Sofern also die Auskunftei keine Kenntnis von der Einrichtung einer Auskunftssperre hinsichtlich des Schuldners oder der Schuldnerin hat, ist eine Auskunftserteilung der aktuellen Anschriftendaten zu dieser Person an eine Gläubigerin nicht zu beanstanden.

Auch für den Fall, dass die betroffene Person die Auskunftei über die eingetragene Auskunftssperre nach § 51 BMG informiert, wäre im Falle einer Anfrage der Gläubigerin oder eines IKU, die offenkundig ausschließlich der Realisierung einer offenen Forderung dient, eine Beauskunftung ihrer aktuellen Anschriftendaten grundsätzlich zulässig. Schließlich dient die Eintragung einer Auskunftssperre im Melderegister nicht dem Zweck, dass sich ein Schuldner oder eine Schuldnerin hierdurch der Geltendmachung berechtigter zivilrechtlicher Ansprüche entziehen.

Gleichwohl hat die Auskunftei in einem solchen Falle – durch Implementierung geeigneter Prozesse – dafür Sorge dafür zu tragen, dass durch eine solche Auskunftserteilung eine Gefährdungssituation für die betroffene Person ausgeschlossen werden kann. Ein solcher Prozess kann beispielsweise individuelle Rückfragen bei der betroffenen Person beinhalten, ob eine Auskunftserteilung an die anfragende Vertragspartnerin für diese gefahrlos ist (etwa weil die gefährdende Person nicht bei dieser tätig ist). Alternativ kann auch ein Vermerk zum Datensatz der betroffenen Person aufgenommen werden, an welche Vertragspartner gegebenenfalls nicht zu beauskunften ist, oder mit einem ähnlichen Hinweis. Grundsätzlich darf die SCHUFA davon ausgehen, dass ihre Vertragspartner seriös sind und von ihnen durch die Kenntnisnahme der aktuellen Anschrift der betroffenen Person keine Gefahr für diese ausgeht. Lediglich bei dieser Annahme widersprechenden Anhaltspunkten müsste eine Auskunftei gegebenenfalls ein entgegenstehendes überwiegendes Interesse der betroffenen Person an der Auskunftserteilung hinsichtlich ihrer Anschriftendaten annehmen und eine Auskunftserteilung unterlassen.

15.2
Unzulässigkeit der postlagernden Zustellung einer Datenkopie nach Art. 15 DS-GVO

Die Erteilung einer Auskunft nach Art. 15 DS-GVO mit der Adressierung „postlagernd“ an eine Filiale der Deutschen Post AG ist aus datenschutzrechtlicher Sicht grundsätzlich unzulässig. Die richtige und vollständige Auskunftserteilung kann bei einer entsprechenden Beantragung einer Selbstauskunft für die Auskunftei so erschwert sein, dass die Unterlassung einer Auskunftserteilung nicht zu bemängeln ist.

Im vorliegenden Fall bemängelte der Beschwerdeführer, die SCHUFA Holding AG weigere sich, diesem eine Auskunft nach Art. 15 DS-GVO zu erteilen. Hierzu führte er aus, in nächster Zeit einige Reisen sowie Segeltörns zu unternehmen bzw. sich generell im Ausland aufzuhalten. Daher begehre er die Erteilung der Auskunft postlagernd an eine seinerseits konkret benannte Filiale der Deutschen Post AG in Deutschland. Eine aktuelle Anschrift im Ausland oder eine etwaige Voranschrift in Deutschland teilte der Beschwerdeführer nicht mit.

Grundsätzlich hat eine Auskunftei gemäß Art. 15 DS-GVO der betroffenen Person Auskunft über die dort zu ihrer Person gespeicherten Daten zu erteilen:

> *Art. 15 DS-GVO*
>
> *(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:*
>
> *(…)*

Hierbei hat die Auskunftei als verantwortliche Stelle zu gewährleisten, Auskünfte nach Art. 15 DS-GVO ausschließlich an die betroffene Person, zu der die Auskunftei einen Auskunfteien-Datensatz führt, zu erteilen. Eine fahrlässige Übermittlung der personenbezogenen Daten der auskunftsersuchenden Person an eine unzutreffende dritte Person wäre aus datenschutzrechtlicher Sicht unzulässig.

Um dieser Verpflichtung zur Auskunftserteilung nach Art. 15 DS-GVO ordnungsgemäß nachkommen zu können, muss die Auskunftei jedoch in die Lage versetzt werden, die auskunftsersuchende Person zunächst zweifelsfrei zu identifizieren, um sodann den entsprechenden Auskunfteien-Datensatz (sofern ein solcher existiert) dieser Person korrekt zuordnen zu können. Hinsichtlich der weiteren Einzelheiten zur Art und Weise dieser Identifizierung im Rahmen des Prozesses der Auskunftserteilung durch Auskunfteien nehme ich Bezug auf die Erläuterungen hierzu im Rahmen meines 45. Tätigkeitsberichts (Ziff. 4.2.2.1.1). Zwar beziehen sich die dortigen Ausführungen auf die seinerzeit geltende Rechtslage (Auskunft nach § 34 BDSG a. F.), jedoch haben sich die diesbezüglich erläuterten Grundsätze und das entsprechende Verfahren durch das Wirksamwerden der DS-GVO am 25. Mai 2018 nicht geändert; vielmehr bestehen diese unverändert fort.

Grundsätzlich erfolgt die Identifizierung einer auskunftsersuchenden Person anhand der von ihr mitgeteilten Personalien: Vorname(n), Name, Anschrift und Geburtsdatum.

Unterlässt es die auskunftsersuchende Person, der Auskunftei im Rahmen eines Auskunftsersuchens eine Anschrift mitzuteilen, ist es der Auskunftei bereits aufgrund dieser unvollständigen Personalien in tatsächlicher Hinsicht nicht möglich, die Person zu identifizieren oder dieser einen ggf. dort geführten Datensatz zweifelsfrei zuzuordnen. Darüber hinaus ist es der Auskunftei bei einer derartigen Fallkonstellation auch nicht möglich, entsprechende Rückfragen bei der auskunftsersuchenden Person zu stellen, um die fehlenden Daten bei dieser zu ermitteln. Insofern kann bei der Notwendigkeit einer Rückfrage die Unterlassung einer Auskunftserteilung seitens einer Auskunftei bereits aufgrund der tatsächlichen Unmöglichkeit der richtigen und vollständigen Auskunftserteilung aus datenschutzrechtlicher Sicht nicht zu beanstanden sein.

Selbst wenn im Rahmen des Auskunftsbegehrens der Auskunftei die zuletzt zutreffende (Vor-)Anschrift des Betroffenen in Deutschland mitgeteilt worden wäre und hierdurch ein in Frage kommender Datensatz seitens der Auskunftei zu ermitteln gewesen wäre, käme eine postlagernde Zustellung der entsprechenden Datenkopie nach Art. 15 DS-GVO aufgrund des mit der Zustellungsart verbundenen Missbrauchsrisikos nicht in Betracht. Schließlich kann die Auskunftei bei dieser Form der Zustellung nicht ausschließen, dass die erteilte Auskunft nicht doch in die Hände eines unbefugten Dritten gelangt, der gegebenenfalls missbräuchlich unter Nennung der zutreffenden Personalien der betroffenen Person eine Auskunftserteilung an eine von ihm bezeichnete Filiale der Deutschen Post AG begehrt.

Die postlagernde Zusendung eines einzelnen bestimmten Schreibens (hier: Datenkopie nach Art. 15 DS-GVO) erfolgt – nach Angaben der Deutschen Post AG – dergestalt, dass die Absenderin (hier: die Auskunftei) im Adressfeld des Schreibens lediglich den Namen des Adressaten oder der Adressatin, den Zusatz „postlagernd“ sowie die Anschrift der gewählten Postfiliale angibt. Alternativ zum Namen des Empfängers oder der Empfängerin kann auch ein zwischen der Absenderin (vorliegend Auskunftei) und dem Empfänger oder der Empfängerin vereinbartes Kennwort ausgewiesen werden. Demnach wären dem Adressfeld beispielsweise folgende Daten zu entnehmen: Max Mustermann oder Kennwort: „Fliege32“, postlagernd, Poststraße 1, 12345 Wunschhausen. Das an diese Filiale der Deutschen Post AG gesandte Schriftstück wird dort für einen Zeitraum von sieben Tagen aufbewahrt. Innerhalb dieses Zeitraums besteht für den Empfänger oder die Empfängerin die Möglichkeit, das Schriftstück unter Vorlage eines Ausweises oder

Mitteilung des vereinbarten Kennworts in Empfang zu nehmen. Im Rahmen der Aushändigung dieses Schriftstücks erfolgt seitens des Mitarbeiters oder der Mitarbeiterin der Deutschen Post AG lediglich ein Abgleich der Daten der Absenderin, die der Empfänger oder die Empfängerin mitgeteilt hat, sowie des angegebenen Namens des Empfängers oder der Empfängerin oder alternativ des vereinbarten Kennworts. Hierbei ist es dem aushändigenden Mitarbeiter oder der Mitarbeiterin der Deutschen Post AG nicht möglich, eine zweifelsfreie Identifizierung des Empfängers als zutreffende betroffene Person des entsprechenden Auskunfteien-Datensatzes anhand der im Adressfeld angegebenen Daten vorzunehmen. Überdies ist dies auch nicht deren Aufgabe. Vielmehr bleibt der tatsächliche Empfänger oder die tatsächliche Empfängerin bei der Verwendung eines Kennworts für den Mitarbeiter oder die Mitarbeiterin der Deutschen Post AG im Ergebnis anonym.

Folglich ist auch für einen solchen Fall die Unterlassung einer Auskunftserteilung mittels postlagernder Übermittlung seitens einer Auskunftei aus datenschutzrechtlicher Sicht nicht nur nicht zu beanstanden, sondern vielmehr geboten.

16. Verkehrswesen

Fahrzeughalterabfrage zur Durchsetzung von Vertragsstrafen auf privaten Parkplätzen

Die Erhebung von Fahrzeughalterdaten im Wege einer einfachen Registerauskunft durch Betreiber von privaten Parkplätzen oder von ihnen beauftragten Unternehmen ist zulässig, wenn ein Rechtsanspruch im Zusammenhang mit dem Betrieb des Fahrzeuges plausibel geltend gemacht werden kann. Es ist jedoch weder meine Aufgabe noch fällt es in meinen Zuständigkeitsbereich zu überprüfen, ob das verfolgte Geschäftsmodell des Parkplatzbetreibers oder des von ihm beauftragten Unternehmens legal ist.

Geschäftsinhaberinnen und -inhaber von Kundenparkplätzen und auch Betreiber privater Stellplätze engagieren immer häufiger private Parkraumüberwachungsunternehmen, die die ordnungsgemäße Nutzung der Parkplätze kontrollieren. In diesem Zusammenhang erreichen mich regelmäßig Beschwerden von Bürgerinnen und Bürgern, die eine Zahlungsaufforderung erhalten, weil sie offenbar unzulässig auf einem Parkplatz geparkt haben. Dabei stellt sich für die Beschwerdeführerinnen und Beschwerdeführer die Frage, woher das Unternehmen ihre Kontaktdaten erhalten hat und ob die Datenerhebung rechtmäßig ist.

Bei der von den privaten Parkraumüberwachungsunternehmen versandten Zahlungsaufforderungen handelt es sich nicht wie vielfach angenommen um Bußgelder, sondern vielmehr um Vertragsstrafen. Bußgelder für „Falschparker“ werden ausschließlich von Behörden (z. B. den örtlichen Ordnungsämtern) erhoben, während die gegenständlichen Zahlungsaufforderungen ausschließlich von privaten Unternehmen versandt werden.

Mit dem Abstellen des Fahrzeugs geht der Fahrer einen Vertrag ein, mit dem er die Allgemeinen Geschäfts- und Nutzungsbedingungen akzeptiert. Diese sind in der Regel auf Hinweisschildern auf dem Parkplatz abgedruckt und regeln auch die Zahlung von Vertragsstrafen bei entsprechender Missachtung. Die Frage, ob die Forderung des Unternehmens begründet ist, kann im Wege einer Beschwerde bei meiner Behörde nicht geklärt, sondern muss gegebenenfalls zivilgerichtlich entschieden werden. Meine Behörde kann lediglich die Rechtmäßigkeit der Datenerhebung prüfen.

Diesbezüglich besteht für den Eigentümer des Parkraums oder das von ihm beauftragte Unternehmen die Möglichkeit, die KFZ-Halterdaten über die Zulassungsbehörden oder das Kraftfahrtbundesamt zu ermitteln. Denn diese sind gemäß § 31 StVG als zuständige Registerbehörden verpflichtet, das

örtliche Fahrzeugregister (bei den Zulassungsbehörden) bzw. das Zentrale Fahrzeugregister (beim Kraftfahrt-Bundesamtes) zu führen.

Dabei ist zu beachten, dass die Fahrzeugregister den Zweck verfolgen, die im öffentlichen Straßenverkehr zugelassenen Fahrzeuge und deren Halter zu erfassen und diese Daten für verkehrsbezogene Angelegenheiten zur Verfügung zu stellen (s. § 32 StVG).

Gemäß Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO i. V. m. § 39 Abs. 1 StVG hat die Zulassungsbehörde oder das Kraftfahrt-Bundesamt demnach eine einfache Registerauskunft demjenigen zu übermitteln, der unter Angabe des betreffenden Kennzeichens oder der betreffenden Fahrzeug-Identifizierungsnummer darlegt, dass er die Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt.

Dabei reicht es aus, wenn der Rechtsanspruch auf Auskunft durch den Interessenten plausibel dargelegt wird (s. BT-Drs. 10/5343 vom 17. April 1986, S. 74).

Sofern die Voraussetzungen des § 39 Abs. 1 StVG erfüllt sind, erhält der Anfragende seitens der Behörden eine einfache Registerauskunft über den Halter des benannten Fahrzeugs und somit auch dessen Kontaktdaten. Die einfache Registerauskunft nach § 39 Abs. 1 StVG stellt dabei eine der häufigsten Formen der Registerauskunft dar (s. BT-Drs. 10/5343 vom 17. April 1986, S. 74).

§ 39 StVG

(1) Von den nach § 33 Abs. 1 gespeicherten Fahrzeugdaten und Halterdaten sind

1. *Familienname (bei juristischen Personen, Behörden oder Vereinigungen: Name oder Bezeichnung),*
2. *Vornamen,*
3. *Ordens- und Künstlername,*
4. *Anschrift,*
5. *Art, Hersteller und Typ des Fahrzeugs,*
6. *Name und Anschrift des Versicherers,*
7. *Nummer des Versicherungsscheins, oder, falls diese noch nicht gespeichert ist, Nummer der Versicherungsbestätigung,*
8. *gegebenenfalls Zeitpunkt der Beendigung des Versicherungsverhältnisses,*
9. *gegebenenfalls Befreiung von der gesetzlichen Versicherungspflicht,*
10. *Zeitpunkt der Zuteilung oder Ausgabe des Kennzeichens für den Halter sowie*
11. *Kraftfahrzeugkennzeichen*

durch die Zulassungsbehörde oder durch das Kraftfahrt-Bundesamt zu übermitteln, wenn der Empfänger unter Angabe des betreffenden Kennzeichens oder der betreffenden Fahrzeug-Identifizierungsnummer darlegt, dass er die Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt (einfache Registerauskunft).

Sofern der Parkverstoß nicht vom Halter selbst verursacht wurde, sondern von einem anderen Fahrer, ist die Einholung der einfachen Registerauskunft dennoch datenschutzrechtlich zulässig, da der Parkplatzbetreiber die Möglichkeit haben muss, den Vertragspartner zu ermitteln. Das Parken auf einem privaten Parkplatz erfolgt jedoch regelmäßig anonym, ohne dass der Betreiber Kontakt zu seinem Vertragspartner erhält. Die aktuelle Rechtsprechung des Bundesgerichtshofs spricht dem Fahrzeughalter daher eine sekundäre Darlegungslast hinsichtlich der Fahrereigenschaft zu (s. BGH, Urteil vom 18. Dezember 2019 – XII ZR 13/19). So entschied der Bundesgerichtshof, dass der Betreiber privater Parkplätze auch vom Fahrzeughalter ein erhöhtes Parkentgelt verlangen kann, wenn dieser seine Fahrereigenschaft nur pauschal bestreitet, ohne mitzuteilen, wer als Fahrer und somit als Vertragspartner zum fraglichen Zeitpunkt in Betracht kommt.

17. Gesundheitswesen

Auch die Datenschutzfragen in den Bereichen der Gesundheitsversorgung und der Gesundheitsforschung waren im Berichtszeitraum stark durch das Corona-Virus geprägt. Beispiele hierfür sind z. B. datenschutzrechtliche Hinweise zum Einsatz der Luca App in Hessen (https://datenschutz.hessen.de/datenschutz/gesundheits-und-sozialwesen/gesundheitswesen/datenschutzrechtliche-hinweise-zum-einsatz) zur hessischen Impfkampagne (https://datenschutz.hessen.de/datenschutz/gesundheits-und-sozialwesen/gesundheitswesen/h%C3%A4ufig-gestellte-fragen-im-zusammenhang-mit) oder zu SARS-CoV-2-Schnelltests (https://datenschutz.hessen.de/datenschutz/gesundheits-und-sozialwesen/gesundheitswesen/datenschutz-bei-sars-cov-2-schnelltests). Aber auch für viele bekannte Datenschutzprobleme bestehen gerade in diesen Bereichen noch viele Unsicherheiten, die Beratungen und Interventionen durch mich erforderlich gemacht haben.

17.1 Transparenz der Datenverarbeitung

Im vergangenen Berichtszeitraum gab es leider wieder vermehrt Eingaben zum Thema nicht gewährte Akteneinsicht gemäß § 630g BGB sowie Auskunft gemäß Art. 15 DS-GVO durch Behandlerinnen und Behandler. Dies betraf sowohl Arztpraxen als auch Krankenhäuser. Bedauerlicherweise ist hier oftmals noch eine Intervention nötig, um Patientinnen und Patienten zu den ihnen zustehenden Rechten auf Einsicht und Auskunft zu verhelfen.

Häufig gab es hierzu auch Beratungsanfragen von Ärztinnen und Ärzten, die mich bei der Erfüllung des Auskunftsanspruchs gemäß Art. 15 DS-GVO um Hilfe gebeten haben. Der Auskunftsanspruch nach Art. 15 DS-GVO ist ein gegenüber der Akteneinsicht nach § 630g BGB unabhängiger Anspruch mit anderem Inhalt und anderem Zweck. Der Antrag auf Datenauskunft muss weder begründet werden, noch ist er an eine bestimmte Form gebunden. Bei offenkundig unbegründeten oder exzessiven Anträgen kann die Arztpraxis entweder ein angemessenes Entgelt verlangen oder die Auskunft verweigern.

Die Auskunft muss der Patientin oder dem Patienten unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung gestellt werden. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Hierüber ist die betroffene Person innerhalb eines Monats zu informieren.

Die Auskunftserteilung kann grundsätzlich je nach Wunsch der betroffenen Person schriftlich, elektronisch oder mündlich erfolgen. Die erhöhten Sicherheitsanforderungen bei der Übermittlung der besonders geschützten Gesundheitsdaten müssen aber erfüllt werden (s. Ziff. 17.2). Die betroffene Person kann auch eine Kopie der sie betreffenden gespeicherten Daten verlangen. Die Auskunft ist unentgeltlich zu erteilen. Nur für weitere, über die erste Auskunft hinausgehende Kopien darf die Arztpraxis ein angemessenes Entgelt verlangen.

Sollten Zweifel an der Identität der anfragenden Person bestehen (z. B. bei Wohnortwechsel), muss die Arztpraxis zum Schutz der schützenswerten Gesundheitsdaten weitere Informationen zur Legitimierung anfordern, z. B. die Übersendung einer Kopie des Personalausweises. Die nicht erforderlichen persönlichen Daten auf der Kopie des Ausweises (wie Augenfarbe, Größe, Personalausweisnummer) dürfen dabei von den Patienten geschwärzt werden.

Die Auskunft ist nach § 29 Abs. 1 Satz 2 BDSG auf die Daten der anfragenden Person zu beschränken. Daten Dritter, insbesondere von Familienangehörigen, dürfen grundsätzlich nur mit deren Einwilligung und Schweigepflichtsentbindung mitgeteilt werden.

Zur Unterstützung von Arztpraxen habe ich ein entsprechendes Muster für Auskünfte nach Art. 15 DS-GVO auf meiner Homepage zur Verfügung gestellt: https://datenschutz.hessen.de/datenschutz/gesundheits-und-sozialwesen/gesundheitswesen/auskunft-nach-art-15-ds-gvo-f%C3%BCr-arztpraxen.

17.2
Rechnungen aus der Apotheke per Mail?

Bei der Übermittlung von Apothekenrechnungen per E-Mail ist zum Schutz der hier betroffenen Gesundheitsdaten eine Inhaltsverschlüsselung („Ende-zu-Ende-Verschlüsselung“) erforderlich. Als datenschutzkonforme Lösungen kommen Verschlüsselungsstandards S/MIME oder OpenPGP, Portallösungen oder gegebenenfalls passwortgeschützte ZIP-Dateien in Betracht.

Die Landesapothekerkammer Hessen bat mich um eine Einschätzung, wie grundsätzlich bei dem Versand von Rechnungen per E-Mail zu verfahren sei. Vorangegangen war eine Eingabe bezüglich des unverschlüsselten E-Mail-Versands von Apothekenrechnungen an ein Pflegeheim. Hier hatte ich durchgesetzt, dass die Apotheke diese Vorgehensweise einstellt.

Gemäß Art. 5 Abs. 1 lit. f DS-GVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Durch geeignete technische und

organisatorische Maßnahmen ist der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung sicherzustellen („Integrität und Vertraulichkeit“).

Nach Art. 32 DS-GVO hat der Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Je sensibler die personenbezogenen Daten sind, desto größer ist auch der Schutzbedarf, der bei der Auswahl der zu treffenden Maßnahmen zugrunde zu legen ist.

Die Rechnungen von Apotheken enthalten regelmäßig Informationen, die Rückschlüsse auf den Gesundheitszustand der Kundinnen und Kunden zulassen. Insbesondere bei verschreibungspflichtigen Medikamenten kann die voraussichtliche Einnahme eines Medikaments auch einer konkreten Person zugeordnet werden. Es sind daher die nach Art. 9 Abs. 1 DS-GVO besonders geschützten Gesundheitsdaten betroffen.

Bei der Versendung von E-Mails mit Gesundheitsdaten ist eine Transportverschlüsselung grundsätzlich nicht ausreichend. Vielmehr ist hier zum Schutz der Gesundheitsdaten bei Berücksichtigung des Standes der Technik zusätzlich zur Transportverschlüsselung auch eine Inhaltsverschlüsselung („Ende-zu-Ende-Verschlüsselung“) erforderlich.

Durch Nutzung der gängigen Verschlüsselungsstandards S/MIME oder OpenPGP kann z. B. eine Inhaltsverschlüsselung von E-Mails erreicht werden. Dafür müssten die Empfängerinnen und Empfänger der Rechnungen aber über entsprechende Kenntnisse und technische Möglichkeiten verfügen.

Eine andere datenschutzkonforme Variante kann in der Bereitstellung der Rechnungen über einen externen IT-Anbieter bestehen (Portallösung). Hierbei werden die Kundinnen und Kunden per E-Mail darüber benachrichtigt, dass sie ihre Rechnung über ein personalisiertes und passwortgeschütztes Login von einem Server des IT-Anbieters herunterladen können. Bei dieser Variante muss sichergestellt werden, dass der IT-Anbieter die erhöhten Anforderungen an die IT-Sicherheit beim Umgang mit Gesundheitsdaten erfüllt. Die Daten müssen dazu auch verschlüsselt auf dem Server des Anbieters abgelegt werden, so dass dieser keinen Zugriff auf die Daten erhält.

Alternativ dazu dürfen Apothekenrechnungen unter den folgenden Bedingungen auch als passwortgeschützte ZIP- oder PDF-Datei im Anhang einer E-Mail versendet werden:

– Die E-Mail selbst darf im Betreff, im Text und im Namen des Anhangs keine Gesundheitsdaten enthalten.
– Das Passwort muss ausreichend komplex sein und darf sich nicht aus der Kommunikationsbeziehung ableiten lassen (z. B. Geburtsdatum oder Kundennummer).
– Bei der Verschlüsselung muss durch entsprechende Einstellungen unter Berücksichtigung des Stands der Technik ein angemessenes Schutzniveau erreicht werden (Art. 25 DS-GVO). Dazu gehört beispielsweise, dass die eingesetzte Software sichere Verschlüsselungsalgorithmen unterstützt (z. B. AES-256) und keine Zugriffsmöglichkeiten (sog. „Backdoors“) für den Anbieter der Software vorsieht.
– Das Passwort muss auf einem alternativen Kommunikationsweg übermittelt werden (z. B. persönlich, telefonisch, SMS) und sollte nicht über einen längeren Zeitraum verwendet werden.

Voraussetzung für diese datenschutzkonformen Lösungen zur elektronischen Übermittlung der Rechnungen ist, dass die Empfänger tatsächlich in der Lage sind, die verschlüsselten Nachrichten zu öffnen. Daher ist regelmäßig im Vorfeld der Übermittlung eine Abstimmung zu geeigneten Lösungen und Formaten erforderlich.

Der routinemäßige unverschlüsselte Versand von Rechnungen per E-Mail auf Basis einer Einwilligung der Kundinnen und Kunden ist nicht zulässig. Die gesetzlichen Vorgaben der Art. 5 Abs. 1 lit. f und 32 DS-GVO stehen dem entgegen und verpflichten die Apotheken, unabhängig von Willensbekundungen ihrer Kundinnen und Kunden entsprechende Vorkehrungen zum Schutz der personenbezogenen Daten zu treffen.

Auch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat mit Beschluss vom 24. November 2021 klargestellt, dass ein Verzicht auf die vom Verantwortlichen vorzuhaltenden technischen und organisatorischen Maßnahmen oder die Absenkung des gesetzlich vorgeschriebenen Standards auf der Basis einer Einwilligung grundsätzlich nicht zulässig ist (s. Anhang 1 Ziff. 2.4).

Im Ergebnis habe ich die Landesapothekerkammer Hessen darüber informiert, dass die oben angeführten Anforderungen für den Versand von Rechnungen per E-Mail gelten.

Die Landesapothekerkammer Hessen kann nunmehr ihre Mitglieder rechtssicher beraten und diesen die genannten, datenschutzkonformen Lösungsansätze aufzeigen.

17.3
Diskretion in Arztpraxis wiederhergestellt

Arztpraxen müssen sicherstellen, dass die nötige Diskretion in den Räumlichkeiten der Praxis gewahrt wird. Vertrauliche Gespräche am Praxisempfang dürfen grundsätzlich nicht im Wartezimmer hörbar sein. Gegebenenfalls hat die Arztpraxis Schutzmaßnahmen technischer oder organisatorischer Art, z. B. bauliche Maßnahmen, zu treffen, um die Diskretion in den Praxisräumen zu gewährleisten.

Durch eine anonyme Eingabe wurde ich darauf aufmerksam gemacht, dass die nötige Vertraulichkeit und Diskretion in einer hessischen Arztpraxis nicht gegeben sei. Die von der Arztpraxis bereitgestellten Fotos der Praxis zeigten die folgende Situation vor Ort:

Die Arztpraxis war baulich offen gestaltet. Es gab eine Trennwand zwischen Wartezimmer und Empfangsbereich mit einem offenen Durchgang ohne eine verschließbare Tür. Auch nach oben waren die Räumlichkeiten nicht mit einer Decke abgegrenzt, sondern sie waren zur sehr hohen Gebäudedecke offen belassen.Vertrauliche Gespräche am Empfang konnten daher von Patienten im Wartezimmer vernommen werden.

In Gesprächen am Empfang legen Patientinnen und Patienten besonders sensible Gesundheitsdaten offen. Diese werden regelmäßig vom Praxispersonal in der Patientenakte als Dateisystem nach Art. 2 Abs. 1 Alt. 2 DS-GVO gespeichert, so dass der Anwendungsbereich der DS-GVO eröffnet ist.

Die Arztpraxis ist nach Art. 5 Abs. 1 lit. f DS-GVO gesetzlich dazu verpflichtet, personenbezogene Daten in einer Weise zu verarbeiten, die eine angemessene Sicherheit dieser Daten gewährleistet, einschließlich den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung („Integrität und Vertraulichkeit“).

Daher muss die Praxis dafür Sorge tragen, dass die Kenntnisnahme unberechtigter Dritter soweit wie möglich verhindert wird. Auch die ärztliche Schweigepflicht nach § 203 Abs. 1 Nr. 1 StGB erfordert eine besondere Diskretion in den Räumlichkeiten der Praxis.

Ich habe die Arztpraxis auf die mangelnde Diskretion hingewiesen und verlangt, dass sie angemessene technische und organisatorische Maßnahmen, wie insbesondere bauliche Veränderungen und ergänzende Schallschutzmaßnahmen, trifft.

Die Praxis hat verschiedene Maßnahmen geprüft. So wurde das Einfügen einer zusätzlichen Schallschutzwand sowie das Abhängen des Deckenbereichs mit schallabsorbierenden Segeln angedacht. Am Ende entschied sich die Praxis für eine räumliche Trennung von Wartezimmer und Empfangsbereich. Der Empfangsbereich wurde baulich zu einem geschlossenen Raum umgestaltet, so dass die dortigen Gespräche zwischen Beschäftigen der Praxis und Patientinnen und Patienten nicht mehr im Wartebereich mitgehört werden können.

17.4
Aufbewahrungsdauer der Patientenakte in Zahnarztpraxis

Eine Aufbewahrung der Patientendaten einer Zahnarztpraxis nach Ablauf der gesetzlichen zehnjährigen Aufbewahrungsfrist (§ 630f Abs. 3 BGB) ist grundsätzlich nicht zulässig. Auch die zivilrechtlichen Verjährungsfristen von Schadensersatzansprüchen rechtfertigen regelmäßig keine längere Aufbewahrung der Daten durch die Zahnarztpraxis.

Eine längere Aufbewahrung ist vielmehr nur im Einzelfall zulässig, soweit hierfür besondere medizinische Gründe bestehen oder konkrete Anhaltspunkte für eine rechtliche Auseinandersetzung vorliegen. In diesen Fällen hat die Zahnarztpraxis die Begründung der längeren Aufbewahrung zu dokumentieren.

Anlässlich einer Eingabe habe ich das Verfahrensverzeichnis einer Zahnarztpraxis geprüft. Im Verfahrensverzeichnis war vorgesehen, dass die Patientendaten auch nach Ablauf der zehnjährigen Aufbewahrungsfrist noch archiviert aufbewahrt werden.

Die Zahnarztpraxis teilte mir mit, dass die Patientendaten bis zu 30 Jahre nach Beendigung des Behandlungsverhältnisses aufbewahrt würden. Diese lange Aufbewahrung sei aufgrund der späten Verjährung entsprechender Schadensersatzansprüche erforderlich. Nach § 199 Abs. 2 BGB beträgt die Höchstfrist der Verjährung von Schadensersatzansprüche wegen der Verletzung des Lebens, des Körpers oder der Gesundheit 30 Jahre.

Grundsätzlich sind personenbezogene Daten nach den Prinzipien der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) und Speicherbegrenzung (Art. 5 Abs. 1 lit. e DS-GVO) zu löschen, wenn die Zwecke der Datenverarbeitung erreicht sind (Art. 17 Abs. 1 lit. a DS-GVO) und keine gesetzlichen Aufbewahrungspflichten gemäß Art. 17 Abs. 3 lit. b DS-GVO eine längere Speicherung verlangen. In der Regel sind daher die Patientendaten mit dem Ende der folgenden Aufbewahrungsfristen nach zehn Jahren zu löschen.

Nach 630f Abs. 3 BGB und § 12 Abs. 1 der Berufsordnung für hessische Zahnärztinnen und Zahnärzte sind die Patientenakten für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach anderen Vorschriften andere Aufbewahrungsfristen bestehen.

Der Beginn der Aufbewahrungsfrist setzt den Abschluss der Behandlung voraus. Dabei ist zu differenzieren, ob es sich um einen einzelnen abgeschlossenen Behandlungsvorgang wegen eines konkreten Leidens handelt oder um eine Dauerbehandlung z. B. wegen einer chronischen Erkrankung.

Bei Einzelerkrankungen beginnt die Aufbewahrungsfrist mit Abschluss des konkreten Behandlungsvorgangs.

Bei einer dauerhaften oder zeitlich gestreckten Behandlung kommt es auf den Tag an, an dem der Patient letztmalig zu diesem Krankheitsvorgang behandelt wurde (Rehborn/Kern in: Laufs/Kern/Rehborn Handbuch des Arztrechts, 5. Auflage 2019, § 61, Rn. 31). Dies ist der erste Tag der 10-Jahres-Frist. Der letzte Patientenkontakt, der aus einem anderen Grunde erfolgt, ist demgegenüber nicht maßgeblich (Spickhoff in: Spickhoff, Medizinrecht, 3. Aufl. 2018, BGB § 630f Rn. 7).

Nach § 85 Abs. 2 Satz 1 Nr. 2 Strahlenschutzgesetz (StrlSchG) sind Aufzeichnungen sowie Röntgenbilder, digitale Bilddaten und sonstige Untersuchungsdaten bei einer volljährigen Person für eine Dauer von zehn Jahren (a) und bei einer bei einer minderjährigen Person bis zur Vollendung ihres 28. Lebensjahres (b) aufzubewahren. Eine 30-jährige Aufbewahrungsfrist gilt für diese Unterlagen nur im Falle von Behandlungen mit ionisierender Strahlung oder radioaktiven Stoffen (§ 85 Abs. 2 Satz 1 Nr. 1 StrlSchG).

Im Einzelfall können für Zahnarztpraxen weitere spezialgesetzliche Aufbewahrungspflichten gelten, die dann für die betreffenden Daten zu berücksichtigen sind.

Sollte für die Erreichung des Zwecks, für den die Patientendaten erhoben wurden, die Aufbewahrung noch notwendig sein, müssen diese nicht gelöscht werden (vgl. Art. 17 Abs. 1 lit. a DS-GVO). Dies kann insbesondere dann der Fall sein, wenn die Gesundheitsdaten wichtige Informationen enthalten, bezüglich derer davon ausgegangen werden kann, dass auch nach Ablauf gesetzlicher Aufbewahrungsfristen das Interesse des Patienten an der Speicherung das Interesse an der Löschung überwiegt (z. B. wenn es sich im Verlauf der Behandlung abzeichnet, dass die längere Aufbewahrung der Patientenunterlagen zur zukünftigen Behandlung eines Patienten besonders wichtig ist).

Dies ist aber nicht der Regelfall, sondern kann nur bei besonderen medizinischen Gründen im Einzelfall gelten. In einem Löschkonzept sind über

die Aufbewahrungsfristen hinausgehende Löschfristen entsprechend zu begründen und zu dokumentieren.

Eine pauschale Aufbewahrung der personenbezogenen Patientendaten über die Frist des § 630f Abs. 3 BGB hinaus aufgrund der 30-jährigen Verjährungshöchstfrist des § 199 Abs. 2 BGB ist nicht zulässig.

Nach Art. 17 Abs. 3 lit. e DS-GVO gilt die Löschpflicht nach Art. 17 Abs. 1 DS-GVO nicht, wenn die Verarbeitung der Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. Dies setzt aber voraus, dass ein Streitfall schon besteht oder konkret absehbar ist. Eine generelle vorsorgliche Anwendung für den Fall, dass theoretisch noch ein Anspruch gegen den Behandelnden geltend gemacht werden könnte, ist nicht zulässig.

Eine Aufbewahrung der Patientendaten nach Ablauf der zehnjährigen Aufbewahrungsfrist kann mithin im Einzelfall zulässig sein, wenn die Zahnarztpraxis nach einer Abwägung der widerstreitenden Interessen (Wahrscheinlichkeit der Geltendmachung von Rechtsansprüchen gegenüber dem anhaltenden Grundrechtseingriff durch Speicherung) zu dem entsprechenden Ergebnis kommt.

Auch die Beweislastumkehr nach § 630h Abs. 3 BGB führt zu keiner anderen Bewertung. Diese Beweislastumkehr im Falle fehlender Behandlungsdokumentation gilt nicht mehr, wenn die zehnjährige Aufbewahrungspflicht des § 630f Abs. 3 BGB abgelaufen ist (vgl. Gesetzesbegründung „Entwurf eines Gesetzes zur Verbesserung der Rechte von Patientinnen und Patienten“ vom 15.08.2012, BT-Drs. 17/10488, S. 30).

Den Behandelnden trifft insoweit nach Ablauf der zehnjährigen Frist des § 630f Abs. 3 BGB aus dem Nichtvorhandensein der Dokumentation kein Nachteil. Löscht oder vernichtet er die Dokumentation der Behandlung nach Ablauf der Frist, greift die Beweislastregelung des § 630h Abs. 3 BGB nicht mehr.

Aufgrund regelmäßiger Anfragen zu diesem Themenkomplex habe ich die Bundeszahnärztekammer und die Landeszahnärztekammer Hessen um Stellungnahme gebeten. Beide Kammern sehen ebenfalls bei Zahnärzten keine Erforderlichkeit für eine Aufbewahrung, die über zehn Jahre hinausgeht. Die Landeszahnärztekammer Hessen hat klargestellt, dass auch sie im Einzelfall, bei entsprechender Behandlungsrelevanz, eine längere Aufbewahrung aus medizinischen Gründen als zulässig ansieht.

Ich habe die Zahnarztpraxis über die Rechtslage informiert und zur Anpassung der Löschprozesse aufgefordert. Daraufhin hat mir die Zahnarztpraxis mitgeteilt, dass sie ihre Löschfristen hinsichtlich der Patientendaten entsprechend anpasst.

17.5
TeleCOVID Hessen

Über die TeleCOVID Hessen App können Krankenhäuser mit kleinerer Intensivkapazität zu einer COVID-Behandlung eine Zweitmeinung einer Intensivmedizinerin oder eines Intensivmediziners größerer Krankenhäuser einholen. Per Videotelefonie können sich die Krankenhäuser vernetzen und Befunde sowie Behandlungsdaten verschlüsselt übermitteln. So können auch vor einer Verlegung in ein anderes Krankenhaus wichtige Informationen ausgetauscht werden.

Die Nutzung der App kann den bisherigen Informationsaustausch zwischen den Intensivstationen über Telefon, Fax und E-Mail vereinfachen und fachlich verbessern. Rund 80 Krankenhäuser in Hessen sind bereits angebunden und können die App nutzen.

Bei der Entwicklung und der Einführung der TeleCOVID Hessen App war ich von Anfang an eingebunden. In regelmäßigen Gesprächen haben alle Beteiligten konstruktiv zusammengearbeitet. Meine Hinweise und Anmerkungen zur Gestaltung des Systems wurden umgesetzt und die beteiligten Krankenhäuser wurden in diese Diskussion miteinbezogen. Durch die frühzeitige Einbeziehung konnten zahlreiche datenschutzrelevante Konzepte und Dokumente bereits im Vorfeld abgestimmt werden.

Hier hat sich erneut gezeigt, dass durch meine Einbeziehung vor Projektstart regelmäßig die richtigen Weichen rechtzeitig gestellt werden können und projektverzögernde Nachbesserungen zur Herstellung der Datenschutzkonformität nicht erforderlich werden.

17.6
Datenschutzfragen in Abschlussarbeiten und Promotionen

Werden im Rahmen von Forschungsvorhaben personenbezogene Daten verarbeitet, bedarf es stets einer Rechtgrundlage für diese Verarbeitung. Der Regelfall wird hier die Datenverarbeitung aufgrund einer Einwilligung sein.

Auch ohne Einwilligung ist nach § 24 Abs. 1 Satz 1 HDSIG die Verarbeitung besonderer Kategorien personenbezogener Daten, dies sind insbesondere Gesundheitsdaten, im Sinn des Art. 9 Abs. 1 DS-GVO für wissenschaftliche Forschungszwecke zulässig, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung überwiegen.

§ 24 Abs. 1 Satz 1 HDSIG ist nur für öffentliche Stellen in Hessen, also insbesondere Hochschulen, anwendbar und gilt daher nur für Forschungsvorhaben unter der Verantwortlichkeit einer Hochschule des Landes Hessen. Für private Hochschulen ist nicht das HDSIG, sondern § 27 BDSG anwendbar.

Der Begriff der wissenschaftlichen Forschungszwecke ist nach Erwägungsgrund 159 Satz 2 der DS-GVO weit auszulegen. Auch Forschungsvorhaben im Rahmen von akademischen Abschlussarbeiten (z. B. Bachelor- oder Masterarbeit) oder Promotionsvorhaben sind regelmäßig davon umfasst.

Basiert die Datenverarbeitung auf der Rechtsgrundlage des § 24 Abs. 1 Satz 1 HDSIG, ist vor dem Beginn des Forschungsvorhabens gemäß § 24 Abs. 1 Satz 3 HDSIG zwingend ein Datenschutzkonzept zu erstellen, das der zuständigen Aufsichtsbehörde auf Nachfrage vorzulegen ist.

Werden ausschließlich anonyme Daten verwendet, liegen keine personenbezogenen Daten vor, die DS-GVO ist nach Art. 2 Abs. 1 DS-GVO dann nicht anwendbar. Es empfiehlt sich aber auch hier, ein Datenschutzkonzept zu erstellen, in dem vor allem die Anonymität der Daten und der Schutz ihrer Anonymität dargelegt wird. Es handelt sich jedoch nur dann um anonyme Daten, wenn die Daten – auch mit erreichbarem Zusatzwissen – keinen identifizierten oder identifizierbaren natürlichen Personen zugeordnet werden können.

Auf meiner Website habe ich ein Muster für ein solches Datenschutzkonzept bereitgestellt, das insbesondere für Forschungsvorhaben im Zusammenhang mit akademischen Abschlussarbeiten (z. B. Bachelor- oder Masterarbeiten) oder Promotionsvorhaben in Hessen verwendet werden kann (https://datenschutz.hessen.de/datenschutz/statistik-und-wissenschaft/wissenschaft/datenschutzkonzepte-f%C3%BCr-akademische).

Vor allem bei den oben genannten „kleineren“ Forschungsvorhaben besteht die Gefahr, dass die Erstellung eines vollständigen Datenschutzkonzepts mangels personeller und fachlicher Ressourcen das Vorhaben zum Erliegen bringt. Mit diesem Muster möchte ich Studierenden und Promovierenden eine Hilfestellung bei der Erfüllung der datenschutzrechtlichen Pflichten geben, damit diese Forschungsprojekte nicht an dem datenschutzrechtlichen Prüfungs- und Dokumentationsaufwand scheitern.

18. Technik und Organisation

Wichtige Themen, in denen in besonderer Weise die technische und organisatorische Kompetenz in der Aufsichtsbehörde gefragt war, betrafen z. B. Videokonferenzsysteme (Ziff. 4), Verwaltungssysteme (Ziff. 8) und große IT-Anwendungen im Schulbereich (Ziff. 10). Aber auch die Zunahme der Cyberkriminalität sowie Fehler und Nachrüstungen in Netzwerkkomponenten erforderten viel Aufmerksamkeit. Eine hohe Grundlast verursachten die zunehmenden Meldungen von Datenschutzverletzungen, die zu prüfen und zu bewältigen waren. Eine weitere wichtige Aufgabe ist es, die technologische Entwicklung zu beobachten und zu erkennen, wo neue Risiken entstehen, aber auch wo alte Schutzmechanismen keinen Datenschutz mehr bieten. Ein plastisches Beispiel hierfür bietet die Notwendigkeit, das Fax durch digitale datenschutzrechtskonforme Alternativen zu ersetzen.

18.1 Meldungen von Datenschutzverletzungen

Die Zahl der Meldungen von Datenschutzverletzungen erreichte im Berichtsjahr einen neuen Rekord. Verantwortliche Stellen haben auch weiterhin Beratungsbedarf zu grundlegenden Fragen im Kontext von Datenschutzvorfällen sowie den Voraussetzungen der Meldepflicht.

Überblick und Entwicklungen

Im Berichtszeitraum gingen bei meiner Behörde insgesamt 2.016 Meldungen von Datenschutzverletzungen nach Art. 33 DS-GVO, § 65 BDSG i. V. m. § 500 StPO und § 60 HDSIG aus dem öffentlichen und nicht öffentlichen Bereich ein. Im Vergleich zum Vorjahr ist die Zahl der angezeigten Datenschutzvorfälle um 571 Meldungen und somit um mehr als 40 % gestiegen. Die folgende Abbildung stellt eine Gesamtentwicklung der gemeldeten Datenschutzverletzung beim HBDI seit dem Wirksamwerden der DS-GVO am 25. Mai 2018 dar.

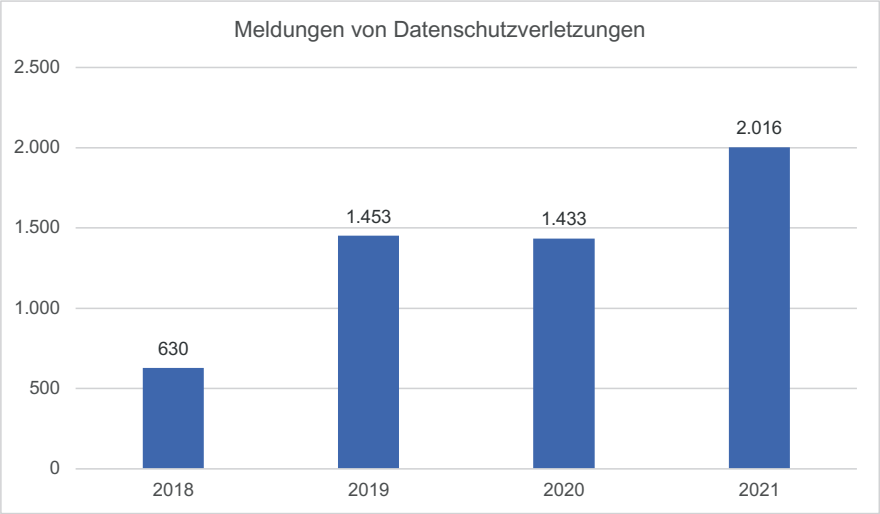


Abb. 1 Entwicklung der Anzahl der Meldungen von Datenschutzverletzungen beim HBDI seit Wirksamwerden der DS-GVO

Die Verpflichtung der verantwortlichen Stellen, Verletzungen des Schutzes personenbezogener Daten an die Datenschutzaufsichtsbehörde zu melden, ergibt sich aus Art. 33 DS-GVO.

Art. 33 DS-GVO

[1]Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. [2]Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.

Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(1) Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

(2) [1]Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. [2]Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.

Den mir gemeldeten Verletzungen des Schutzes personenbezogener Daten liegen unterschiedlichste Sachverhalte und Ursachen zugrunde. Wie bereits in den letzten Jahren dominierten jedoch auch 2021 Datenschutzverletzungen, die strafbare Hackerangriffe, Fehlversand (s. auch Ziff. 14.3) sowie Verlust (s. auch Ziff. 2 und 18.4) oder Diebstahl von Daten zum Gegenstand hatten. Die Branchen Kreditwirtschaft, Handel und Gewerbe, der Themenbereich Beschäftigtendatenschutz sowie der Gesundheitssektor waren erneut am stärksten betroffen.

Anstieg der Cyberkriminalität

Besonders negativ hervorzuheben ist, dass im Jahr 2021 die Meldungen im Zusammenhang mit kriminellen Cyberangriffen deutlich angestiegen sind. Im Vergleich zum Vorjahr verdreifachte sich die Zahl der gemeldeten Angriffe von 184 auf 628 Vorfälle. Diese sehr ernst zu nehmende Entwicklung lässt sich aus meiner Sicht unter anderem auf mehrere im Verlaufe des Jahres eingetretene oder bekanntgewordene größere Ereignisse zurückführen.

Zum einen sorgte die Nachricht über die Zerschlagung des Emotet-Botnetzes durch international kooperierende Strafverfolgungsbehörden für zahlreiche Meldungen von Unternehmen, Kommunen und anderen Organisationen an meine Behörde. In diesem Zusammenhang wurde nämlich festgestellt, dass zuvor mehrere Systeme – unter anderem auch einiger in Hessen ansässiger Verantwortlicher – kompromittiert worden waren. Die jeweiligen Verantwortlichen wurden von den zuständigen Strafverfolgungsbehörden hierüber informiert und meldeten mir die dadurch bekanntgewordenen Datenschutzverletzungen.

Zum anderen waren von den in der Öffentlichkeit stark diskutierten kritischen Schwachstellen in Microsoft Exchange-Servern und deren Ausnutzung durch die Gruppierung namens „Hafnium“ auch zahlreiche hessische Unternehmen und andere Institutionen betroffen. Allein zu diesem Sachverhalt gingen über 260 Meldungen nach Art. 33 DS-GVO innerhalb kürzester Zeit bei meiner Behörde ein, was zu einem enormen zusätzlichen Aufwand führte und hierdurch zeitliche und personelle Kapazitäten in einem erheblichen Umfang band. Um die Bearbeitung dieser Fälle möglichst effizient zu gestalten, wurden bestehende Praktiken beim Bearbeiten von Datenpannenmeldungen optimiert sowie zusätzliche neue Formulare und Fragenkataloge erarbeitet. Der Großteil dieser Meldungen konnte somit bereits geprüft und abgeschlossen werden (s. Ziff. 18.3).

Darüber hinaus erreichten mich im Laufe des Jahres zahlreiche Meldungen über sogenannte Ransomware-Attacken. „Ransomware“ steht in Fachkreisen für „Erpressungssoftware“. Dabei handelt es sich um schädliche Programme, die von kriminellen Angreifern auf Systeme von verantwortlichen Stellen aufgespielt werden. In der Regel werden die Daten anschließend verschlüsselt und die Angriffsopfer mit einer Geldforderung erpresst (s. Ziff. 18.2). Als besonders kritisch ist in diesem Zusammenhang zu beobachten, dass immer häufiger auch kleinere Unternehmen oder z. B. Arztpraxen Opfer solcher Angriffe werden.

Ein weiterer Vorfall, der zu der negativen Statistik beigetragen hat, ereignete sich bei einem hessischen Auftragsverarbeiter. Dieser bietet für diverse Städte und Gemeinden eine Plattform an, auf der sich Bürger mit einer E-Mail-Adresse zwecks Erhalts eines aktuellen Abfallkalenders registrieren können. Beim Versand der Jahresabfallkalender wurde von Cyberkriminellen eine vierstellige Zahl von E-Mail-Adressen abgefangen und zum Teil für Phishing-Mails verwendet. Insgesamt waren von dem Vorfall 51 hessische Kommunen betroffen. Der Auftragsverarbeiter reagierte bei einem ersten Verdacht eines Datenabflusses schnell und informierte sowohl die betroffenen Kommunen als auch die Aufsichtsbehörde. Alle betroffenen Bürgerinnen und Bürger wurden ebenfalls umgehend benachrichtigt. Insgesamt waren die vom Auftragsverarbeiter eingeleiteten Maßnahmen erforderlich und angemessen, um den Schaden gering zu halten und die Risiken eines erneuten Vorkommens dieses Sachverhaltes zu minimieren.

Pandemiebedingte Meldungen

Wie auch bereits im Vorjahr hatte das andauernde Pandemiegeschehen im Berichtsjahr einige Datenschutzverletzungen zur Folge. Während es im Jahr 2020 tendenziell um Offenlegungen einer bestehenden Covid-19-Erkran-

kung sowie diverse Home-Office-Problematiken ging (s. 49. TB, Ziff. 15.1), erreichten mich in diesem Jahr verstärkt Meldungen im Zusammenhang mit der Corona-Impfung, aber auch mit verwechselten Testergebnissen und Impfnachweisen.

Zum Ende des Jahres 2021 kamen einzelne Datenpannenmeldungen im Zusammenhang mit der Umsetzung der sogenannten „3G-Regelung“ am Arbeitsplatz hinzu. So versandten z. B. mehrere verantwortliche Stellen im Rahmen der Organisation der 3G-Kontrollen Listen mit Beschäftigtendaten an (interne) falsche Adressaten. Gesundheitsdaten, wie z. B. der Impfstatus, waren bei diesen Fallkonstellationen in der Regel nicht direkt betroffen. Aus dem Kontext konnten jedoch entsprechende Indizien hergeleitet werden.

Bei der hohen Anzahl an gemeldeten Datenschutzverletzungen überrascht es nicht, dass verantwortliche Stellen, aber auch Auftragsverarbeiter, einen umfangreichen Beratungs- und Unterstützungsbedarf im Umgang mit Datenschutzvorfällen haben und regelmäßig Fragen an meine Behörde herantragen. So erreichten mich im Berichtszeitraum mehrere Anfragen in Bezug auf den zeitlichen Ablauf der Meldung und die Berechnung der Meldefrist.

Wie wird die 72-Stunden-Frist genau berechnet?

Einige wesentliche Fragen, die oft an mich gerichtet wurden und für die Praxis von enormer Bedeutung sind, beziehen sich auf die Berechnung der Frist zur Meldung von Verletzungen des Schutzes personenbezogener Daten. Insbesondere war es für die Verantwortlichen fraglich, ob die Frist auch an Wochenenden und Feiertagen weiterläuft oder bis zum nächsten Arbeitstag ausgesetzt ist.

Es sei an dieser Stelle nochmals darauf hingewiesen, dass bei den Meldungen von Datenschutzverletzungen die besondere Dringlichkeit im Vordergrund steht und diese gemäß Art. 33 Abs. 1 Satz 1 DS-GVO „unverzüglich“, möglichst innerhalb von 72 Stunden zu erfolgen haben.

Darüber hinaus weise ich in diesem Zusammenhang darauf hin, dass die Fristenberechnung gemäß der Verordnung (EWG, Euratom) 1182/71 des Rates vom 3. Juni 1971 zur Festlegung der Regeln für die Fristen, Daten und Termine (FristenVO) erfolgt. Die nationalen Vorschriften aus §§ 186 ff. BGB können als nachrangiges Recht nicht herangezogen werden. Die relevanten Regelungen sind in Art. 3 der FristenVO enthalten.

Artikel 3 FristenVO

(1) Ist für den Anfang einer nach Stunden bemessenen Frist der Zeitpunkt maßgebend, in welchem ein Ereignis eintritt oder eine Handlung vorgenommen wird, so wird bei der Berechnung dieser Frist die Stunde nicht mitgerechnet, in die das Ereignis oder die Handlung fällt. Ist für den Anfang einer nach Tagen, Wochen, Monaten oder Jahren bemessenen Frist der Zeitpunkt maßgebend, in welchem ein Ereignis eintritt oder eine Handlung vorgenommen wird, so wird bei der Berechnung dieser Frist der Tag nicht mitgerechnet, in den das Ereignis oder die Handlung fällt.

(2) Vorbehaltlich der Absätze 1 und 4 gilt folgendes:

a) Eine nach Stunden bemessene Frist beginnt am Anfang der ersten Stunde und endet mit Ablauf der letzten Stunde der Frist.

b) Eine nach Tagen bemessene Frist beginnt am Anfang der ersten Stunde des ersten Tages und endet mit Ablauf der letzten Stunde des letzten Tages der Frist.

c) Eine nach Wochen, Monaten oder Jahren bemessene Frist beginnt am Anfang der ersten Stunde des ersten Tages der Frist und endet mit Ablauf der letzten Stunde des Tages der letzten Woche, des letzten Monats oder des letzten Jahres, der dieselbe Bezeichnung oder dieselbe Zahl wie der Tag des Fristbeginns trägt. Fehlt bei einer nach Monaten oder Jahren bemessenen Frist im letzten Monat der für ihren Ablauf maßgebende Tag, so endet die Frist mit Ablauf der letzten Stunde des letzten Tages dieses Monats.

d) Umfasst eine Frist Monatsbruchteile, so wird bei der Berechnung der Monatsbruchteile ein Monat von dreißig Tagen zugrunde gelegt.

(3) Die Fristen umfassen die Feiertage, die Sonntage und die Sonnabende, soweit diese nicht ausdrücklich ausgenommen oder die Fristen nach Arbeitstagen bemessen sind.

(4) Fällt der letzte Tag einer nicht nach Stunden bemessenen Frist auf einen Feiertag, einen Sonntag oder einen Sonnabend, so endet die Frist mit Ablauf der letzten Stunde des folgenden Arbeitstags.

Diese Bestimmung gilt nicht für Fristen, die von einem bestimmten Datum oder einem bestimmten Ereignis an rückwirkend berechnet werden.

(5) Jede Frist von zwei oder mehr Tagen umfasst mindestens zwei Arbeitstage.

Nach Art. 3 Abs. 1 Satz 1 der FristenVO beginnt die Meldefrist zur nächsten vollen Stunde ab positiver Kenntnis der Datenschutzverletzung. Diese endet gemäß Art. 3 Abs. 2 lit. a FristenVO mit Ablauf der letzten Stunde der Frist.

Für die Frage, ob bei der Berechnung auch die Wochenenden sowie die Feiertage berücksichtigt werden, ist die Auslegung des Art. 3 Abs. 5 FristenVO und die Frage seiner Anwendbarkeit auf die 72-Stunden-Frist von Bedeutung. Art. 3 Abs. 5 FristenVO enthält eine Vorschrift bezüglich aller Fristen „von zwei oder mehr Tagen“. Diese Fristen umfassen danach mindestens zwei Arbeitstage. Da die Frist zur Meldung von Datenschutzverletzungen eine 72-Stunden- und keine 3-Tagesfrist ist, ist Art. 3 Abs. 5 FristenVO nicht anwendbar. Daher ist hier von einer strengen Fristenberechnung auszugehen. Aufgrund eines bei Datenschutzverletzungen anzunehmenden unmittelbaren

Handlungsbedarfs ist eine „unverzügliche“ Meldung geboten. Dies kann nicht bedeuten, dass die Frist aufgrund eines Wochenendes um weitere zwei Tage verlängert werden kann. Zusammenfassend ist also festzuhalten, dass die Frist zur Meldung von Datenschutzverletzungen auch am Wochenende und an Feiertagen ablaufen kann.

Auch die Benachrichtigung von betroffenen Personen gemäß Art. 34 DS-GVO muss unverzüglich und somit „ohne schuldhaftes Zögern“ i. S. v. § 121 BGB erfolgen. Eine feste Frist wurde vom Verordnungsgeber hierzu nicht definiert.

Art. 34 Abs. 1 DS-GVO

(1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

Darüber hinaus ist in diesem Zusammenhang wichtig, dass eine Meldung erst dann befreiende Wirkung hat, wenn sie bei der *zuständigen* Aufsichtsbehörde erfolgt. Anderenfalls könnte die Meldung verfristet sein. Die Aufsichtsbehörden arbeiten zwar zusammen und leiten die Meldungen bei Bedarf an die zuständige Aufsichtsbehörde weiter. Es ist jedoch essenziell wichtig, dass die verantwortlichen Stellen sich bereits im Vorfeld Klarheit darüber verschaffen, welche Datenschutzaufsichtsbehörde für sie zuständig ist, und nicht erst dann, wenn sich ein Datenschutzvorfall ereignet hat.

Wann ist eine schrittweise Meldung notwendig?

Insbesondere bei technisch beeinflussten Fallkonstellationen ist die Informationslage im Zeitpunkt der Kenntniserlangung des Vorfalls oft relativ dürftig oder lückenhaft. Für den Verantwortlichen stellt sich daher die Frage, ob die Meldung bereits zu diesem Zeitpunkt oder erst bei Vorlage weiterer Erkenntnisse zu erfolgen hat.

Maßgeblich für die Bestimmung des Fristbeginns ist gemäß Art. 33 Abs. 1 Satz 1 DS-GVO die Kenntnis des Verantwortlichen von der Verletzung des Schutzes personenbezogener Daten. Bei einer Meldung nach Ablauf von 72 Stunden muss die Verzögerung gemäß Art. 33 Abs. 1 Satz 2 DS-GVO begründet werden. Im Übrigen ermöglicht es Art. 33 Abs. 4 DS-GVO den Verantwortlichen in bestimmten Fällen, die Aufsichtsbehörde schrittweise zu informieren.

Die Anwendung dieser beiden Regelungen wird jedoch manchmal missverstanden. Verzögerte Meldungen mit einer Begründung sollen eine absolute

Ausnahme bleiben. Art. 33 Abs. 4 DS-GVO betont die Notwendigkeit einer unverzüglichen Meldung in allen anzeigepflichtigen Fällen. Darunter fallen auch Sachverhalte, bei denen eine qualitative Meldung mit allen erforderlichen Inhalten innerhalb der Frist nicht ohne weiteres möglich ist. Die Verantwortlichen dürfen also nicht mit der Meldung solange zuwarten, bis der Sachverhalt komplett ermittelt ist, und die Verzögerung dann begründen. Vielmehr muss der Verantwortliche unverzüglich eine Meldung abgeben und nach Vorlage weiterer Erkenntnisse unaufgefordert und ohne unangemessene weitere Verzögerung detailliertere Informationen sukzessive der Aufsichtsbehörde zur Verfügung stellen.

In diesem Zusammenhang weise ich noch einmal nachdrücklich auf den Schutzzweck der Melde- und Benachrichtigungspflicht der Art. 33 und 34 DS-GVO hin, der tendenziell weit zu interpretieren ist. Vor allem geht es darum, die personenbezogenen Daten von Betroffenen zu schützen, mögliche Schäden abzuwenden oder zu verringern und weitere Nachteile für betroffene Personen möglichst zu vermeiden. Die Aufsichtsbehörde wird informiert, um beratend tätig zu werden und gegebenenfalls einschreiten zu können. Daher ist es wichtig, bereits in einem frühen Stadium einer möglichen Datenschutzverletzung die Aufsichtsbehörde einzubeziehen. Betroffene Personen werden benachrichtigt, um diese für die Gefahren, denen sie ausgesetzt sein könnten, zu sensibilisieren und ihnen frühzeitig die Möglichkeit zu geben, Gegenmaßnahmen zu treffen.

Fazit

Im Berichtsjahr wurde insgesamt ein signifikanter Anstieg an Meldungen von Verletzungen des Schutzes personenbezogener Daten, insbesondere verursacht durch kriminelle Cyberangriffe, festgestellt. Die Zusammenarbeit der verantwortlichen Stellen mit der Aufsichtsbehörde gestaltet sich in den meisten Fällen konstruktiv. Sofern die Voraussetzungen des Art. 34 DS-GVO vorliegen, werden die Betroffenen in der Regel informiert. In vielen Fällen unterrichten die verantwortlichen Stellen die betroffenen Personen eigeninitiativ zum Zwecke der Transparenz und eines besseren Schutzes, auch wenn kein hohes Risiko für deren Rechte und Freiheiten vorliegt.

Insgesamt musste ich im Jahr 2021 verhältnismäßig wenig Verstöße im Zusammenhang mit der Melde- und Benachrichtigungspflicht der Verantwortlichen gemäß Art. 33 und 34 DS-GVO feststellen. Verspätete und unterbliebene Meldungen, fehlende Dokumentation der Verletzung sowie nicht erfolgte Benachrichtigungen von Betroffenen blieben Einzelfälle. Diese Vorgänge werden aktuell in Bezug auf weitergehende datenschutzrechtliche Maßnahmen und Sanktionen meinerseits geprüft.

18.2
Ransomware und Ransomware-Angriffe

Cyber-Angriffe mit Ransomware haben in den vergangenen Jahren dramatisch zugenommen und zählen gegenwärtig zu den größten Bedrohungen aus dem Bereich der Cyber-Kriminalität für Organisationen und Unternehmen. Die Auswirkungen auf die Sicherheit personenbezogener Daten sind erheblich und fordern von den Verantwortlichen erhöhte Aufmerksamkeit.

Ransomware und Ransomware-Angriffe

Der Begriff „Ransomware“ bedeutet „Erpressungssoftware“. Er setzt sich aus den englischen Worten „ransom“ für „Lösegeld“ und „ware“ als Kurzform für „Software“ zusammen. In diesem Zusammenhang ist zwischen der Ransomware als Schadsoftware und dem Ransomware-Angriff als Vorgehen des Angreifers zu unterscheiden. Während es sich bei Ransomware als Schadsoftware im Wesentlichen um hocheffiziente Verschlüsselungsprogramme handelt, werden im Rahmen des Ransomware-Angriffs zusätzlich weitere Werkzeuge eingesetzt, z. B. zum Infiltrieren und Auskundschaften des IT-Netzwerks des Opfers. Dabei handelt es sich um unterschiedlich stark automatisierte Angriffe, bei denen der Angreifer direkt im IT-Netzwerk des Opfers operiert. Im Laufe eines erfolgreichen Ransomware-Angriffs werden die Daten auf den betroffenen IT-Systemen des Opfers verschlüsselt und die ursprünglichen Daten gelöscht. Hierdurch wird erreicht, dass die Opfer nicht mehr auf ihre Daten zugreifen können. Erst gegen die Zahlung von Lösegeld wird die Entschlüsselung und damit die Wiederherstellung der Verfügbarkeit der Daten in Aussicht gestellt. Wurde keine geeignete Vorsorge getroffen, können die Daten nicht oder nur mit hohem zeitlichem und finanziellem Aufwand wiederhergestellt werden. In zunehmendem Maße exfiltrieren die Angreifer zusätzlich Daten des Opfers und drohen mit der Veröffentlichung oder der Versteigerung von Daten. Sind durch den Ransomware-Angriff personenbezogene Daten betroffen, kommt es mindestens zur Verletzung der gemäß Art. 32 Abs. 1 lit. b DS-GVO vom Verantwortlichen zu gewährleistenden Vertraulichkeit und Verfügbarkeit. Abhängig vom daraus resultierenden Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen kann dies u. a. eine Meldung von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DS-GVO bei meiner Behörde sowie eine Information der betroffenen Personen gemäß Art. 34 DS-GVO erforderlich machen. In jedem Fall muss eine Dokumentation des Vorfalls gemäß Art. 33 Abs. 5 DS-GVO erfolgen.

Die Entwicklung von Ransomware

Die Anfänge der Ransomware gehen auf die späten 1990er Jahre zurück. Der in Abbildung 2 gezeigte zeitliche Verlauf der Entwicklung (BSI, Ransomware – Bedrohungslage, Prävention & Reaktion 2021, Kapitel 8.1, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf) benennt exemplarisch einzelne Ransomware oder für Ransomware-Angriffe zusätzlich verwendete Schadsoftware.

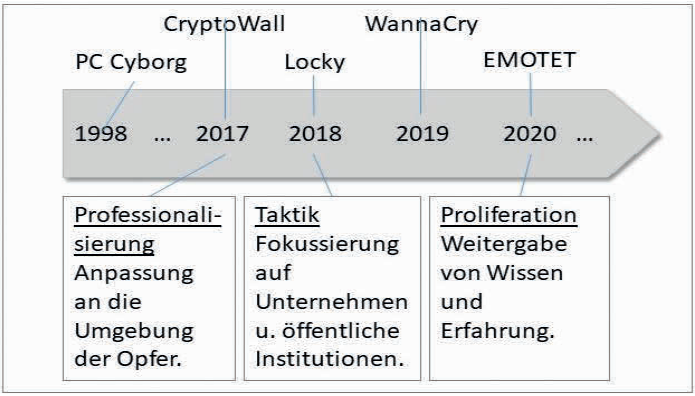


Abb. 2 Zeitlicher Verlauf der Ransomware-Entwicklung

Bis zum Jahr 2017 entwickelten sich die Ransomware-Varianten zunehmend schneller. Mit WannaCry setzte ein Wandel ein, indem effizientere Verbreitungsmethoden verwendet wurden. Es begann eine zunehmende Professionalisierung der Angreifer, was zu einem veränderten taktischen Vorgehen führte. Mit gezielten und methodisch fortgeschrittenen Angriffen rückten Unternehmen und Organisationen in den Fokus. Der damit verbundene größere Aufwand wurde durch ein höheres Schadenspotenzial und deutlich höhere Lösegeldforderungen aufgewogen. Dieser Effekt ist als einer der Motoren der bedrohlich schnell zunehmenden Fallzahlen anzusehen.

Eine Umfrage in Deutschland aus dem Jahr 2019 ergab, dass ca. 30 Prozent der befragten Unternehmen mit einem Umsatz von bis zu 3 Milliarden Euro bereits von einem Ransomware-Angriff betroffen waren (Statista, War Ihr Unternehmen schon einmal von einem Ransomware-Angriff betroffen? https://de.statista.com/statistik/daten/studie/1038985/umfrage/betroffenheit-durch-ransomware-nach-umsatzgroessenklasse-der-unternehmen-in-deutschland/). Das Bundesamt für Sicherheit in der Informationstechnik (BSI) geht davon aus, dass Ransomware-Angriffe weiter zunehmen werden. Die technischen

Fähigkeiten der Angreifer sowie das taktische Vorgehen der Erpresser werden sich weiterentwickeln und neue Angreifer-Gruppen werden dazukommen. Ein zusätzlicher Motor dieser Entwicklung ist das zunehmende Teilen von Wissen zwischen den Angreifern.

Vorgehensweise bei Ransomware-Angriffen

Aus Meldungen nach Art. 33 DS-GVO aufgrund von Ransomware-Angriffen lässt sich in abstrahierter Form folgende Vorgehensweise ableiten (BSI, Die Lage der IT-Sicherheit in Deutschland 2021, Kap. 1.2.2, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf).

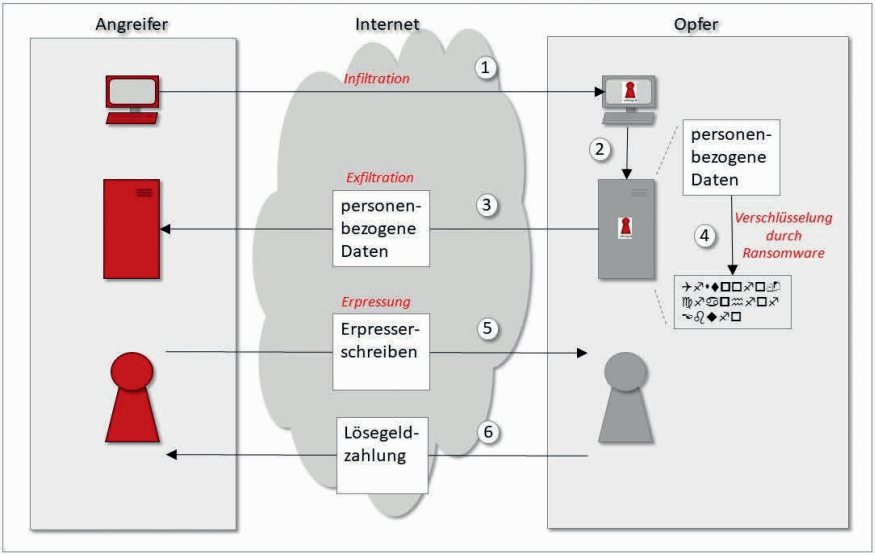


Abb. 3 Taktische Vorgehensweise bei Ransomware

In Schritt 1 werden die IT-Netze des Opfers beispielsweise über E-Mail-Anhänge, Fernzugriffe wie VPN-Verbindungen oder Wartungszugänge infiltriert. Abhängig von den kompromittierten Benutzerkonten des Opfers verfügt der Angreifer über erweiterte Zugriffsrechte, die den Angriff erleichtern. In Form einer lateralen Ausbreitung im Netz des Opfers dringt der Angreifer im zweiten Schritt mit Hilfe erweiterter Zugriffsrechte, entsprechender Schadsoftware und Werkzeugen in weitere IT-Systeme ein. Im dritten Schritt werden personenbezogene Daten des Opfers exfiltriert. Dieser Schritt ist häufig aber

kein zwingender Bestandteil des Angriffs. Im vierten Schritt werden Daten durch die Ransomware verschlüsselt und durch anschließende Löschung der Ursprungsdaten für das Opfer unzugänglich gemacht. Eine Kontaktaufnahme mit dem Opfer in Form eines Erpresserschreibens mit den Lösegeldforderungen und der Androhung, die gegebenenfalls abgezogenen Daten zu veröffentlichen oder zu versteigern, erfolgt im fünften Schritt des Angriffs. Von der Zahlung des Lösegeldes, wie es im sechsten Schritt dargestellt wurde, rät das BSI ab und empfiehlt unverzüglich bei der Polizei Anzeige zu erstatten (BSI, Die Lage der IT-Sicherheit in Deutschland 2021, Kap. 1.2.2).

Notwendiger Umgang mit Ransomware-Angriffen

Mit Blick auf die Sicherheit der Verarbeitung personenbezogener Daten nach Art. 32 DS-GVO müssen Ransomware-Angriffe als erhebliche Gefährdung angesehen werden. Deshalb gilt es für den Verantwortlichen, für diese Gefährdung im Sinne eines Datenschutzmanagements zur Prävention angemessene technische und organisatorische Maßnahmen zu ergreifen. Als Folge der hierzu erforderlichen Risikoanalyse müssen hierbei zusammen mit dem Informationssicherheitsmanagement auch über den konkreten Bereich der Verarbeitungstätigkeit hinaus übergreifende Maßnahmen identifiziert, bewertet und umgesetzt werden. Im Rahmen des Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der ergriffenen Maßnahmen gemäß Art. 32 Abs. 1 lit. d DS-GVO müssen Veränderungen der Gefährdungslage durch Ransomware-Angriffe explizit berücksichtigt werden.

Sollte es zu einem Ransomware-Angriff gekommen sein, ist die datenschutzrechtliche Bewertung des Vorfalls nicht ausschließlich auf die exfiltrierten oder verschlüsselten Daten beschränkt. Vielmehr müssen zunächst alle IT-Systeme als potenziell kompromittiert angesehen werden. Insbesondere ist zu berücksichtigen, dass verschlüsselte Daten trotz einer etwaigen Entschlüsselung z. B. nach Zahlung von Lösegeldern grundsätzlich als kompromittiert betrachtet werden müssen. Die Zahlung von Lösegeldern an die organisierte Kriminalität im Cyberspace leistet weiteren Ransomware-Angriffen Vorschub und garantiert keine Entschlüsselung oder Nicht-Veröffentlichung. Sollten personenbezogene Daten betroffen sein, ist risikoabhängig an eine rechtzeitige Meldung nach Art. 33 DS-GVO und an eine Benachrichtigung der Betroffenen gemäß Art. 34 DS-GVO zu denken (BSI, Die Lage der IT-Sicherheit in Deutschland 2021, Kap. 1.2.2).

Ransomware-Vorfall mit Veröffentlichung personenbezogener Daten im „Darknet“

Unter Umständen erfolgt bei einem Ransomware-Angriff auch eine Veröffentlichung der abgeflossenen Daten durch die Angreifer, um zusätzlichen Druck zur Bezahlung des „Lösegelds“ aufzubauen. Handelt es sich um eine große Datenmenge, so stehen Verantwortliche vor der Herausforderung zu identifizieren, welche Personen davon betroffen sind, und diese gegebenenfalls unverzüglich zu benachrichtigen.

I. Angriff auf einen Versicherungsverein

Ein hessischer Versicherungsverein verarbeitet personenbezogene Daten seiner Versicherungsnehmerinnen und Versicherungsnehmer als Verantwortlicher gemäß Art. 4 Nr. 7 DS-GVO. In der Nacht vom 9. auf den 10. Juli 2021 kam es zu einem Angriff auf die IT-Systeme des Verantwortlichen, bei dem auch Ransomware zum Einsatz kam. Durch diese Schadsoftware wurden personenbezogene Daten von Versicherungsnehmerinnen und Versicherungsnehmern verschlüsselt und so dem Zugriff des Verantwortlichen entzogen. Zusätzlich kam es zu einem Abfluss und einer nachgelagerten Veröffentlichung von Teilen der personenbezogenen Daten. Somit waren die Vertraulichkeit und die Verfügbarkeit der betroffenen personenbezogenen Daten nicht mehr gewährleistet.

II. Meldung gem. Art. 33 DS-GVO

Der Verantwortliche gab gegenüber meiner Behörde am 10. Juli 2021 eine erste Meldung über diese Verletzung des Schutzes personenbezogener Daten ab. Hierzu war er gemäß Art. 33 Abs. 1 Satz 1 DS-GVO binnen 72 Stunden verpflichtet, da mindestens von einem Risiko für Rechte und Freiheiten der betroffenen Personen auszugehen war. Grundsätzlich muss eine solche Meldung an die zuständige Aufsichtsbehörde gemäß den Vorgaben des Art. 33 Abs. 3 DS-GVO auch Informationen zu Art und Umfang der betroffenen personenbezogenen Daten, den Kategorien der betroffenen Personen sowie den möglichen Folgen für die betroffenen Personen enthalten. Da ihm zu diesem Zeitpunkt die entsprechenden Erkenntnisse jedoch noch nicht vorlagen, handelte es sich bei dieser ersten Meldung des Verantwortlichen um eine initiale Mitteilung, die meine Behörde über den Vorfall an sich in Kenntnis setzte. In den folgenden Tagen und Wochen ergänzte der Verantwortliche diese erste Meldung mehrmals um zusätzliche Informationen, die im Zuge seiner Analyse des Vorfalls bekannt wurden. Die Möglichkeit, die notwendigen Informationen der zuständigen Aufsichtsbehörde schrittweise zur Verfügung zu stellen, ist in Art. 33 Abs. 4 DS-GVO vorgesehen und trägt

dem Umstand Rechnung, dass gerade bei Vorfällen, bei denen komplexe IT-Systeme involviert sind, oft erst eine darauf ausgerichtete Analyse Klarheit darüber verschaffen kann, welche Verarbeitungstätigkeiten auf welche Art und in welchem Umfang betroffen sind (s. Ziff. 18.1). Im vorliegenden Fall ist der Verantwortliche seiner Pflicht zur Meldung gegenüber meiner Behörde sowohl fristwahrend als auch inhaltlich nachgekommen.

Der Verantwortliche muss die während der folgenden Analyse entstehenden Erkenntnisse, die im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehen und ihre Auswirkungen und die ergriffenen Abhilfemaßnahmen betreffen, in seine Dokumentation gemäß Art. 33 Abs. 5 Satz 1 DS-GVO aufnehmen. Dies gilt auch für Fälle, in denen es voraussichtlich zu keinem Risiko für Rechte und Freiheiten betroffener Personen gekommen ist. Bei der Bearbeitung von Meldungen gemäß Art. 33 DS-GVO und auch darüber hinaus macht meine Behörde regelmäßig von der Möglichkeit aus Art. 33 Abs. 5 Satz 2 DS-GVO Gebrauch, diese Dokumentation vollumfänglich anzufordern, um insbesondere den Hergang eines Vorfalls nachzuvollziehen und die Angemessenheit und Wirksamkeit der vom Verantwortlichen geplanten und ergriffenen Abhilfemaßnahmen zu überprüfen.

III. Veröffentlichung personenbezogener Daten im „Darknet“

Am 6. August 2021 erlangte ich davon Kenntnis, dass im Rahmen des Vorfalls abgeflossene personenbezogene Daten im sogenannten „Darknet“ veröffentlicht worden waren. Entsprechende Mitteilungen erreichten mich am selben Tag sowohl durch den Verantwortlichen selbst wie auch durch die Datenschutzaufsichtsbehörde eines anderen Bundeslandes, die von der Veröffentlichung Kenntnis erlangte hatte. Da ich selbst ein IT-Laboratorium betreibe, um informationstechnische Sachverhalte mit konkretem Datenschutzbezug überprüfen zu können, konnte ich mich davon überzeugen, dass sich unter den im „Darknet“ veröffentlichten Daten tatsächlich auch personenbezogene Daten aus dem Verantwortlichkeitsbereich dieses Versicherungsvereins befanden.

Bei einer möglichen, angedrohten oder erfolgten Veröffentlichung personenbezogener Daten sind alle Erkenntnisse zu berücksichtigen und müssen sich auch in der Risikobewertung des Verantwortlichen wiederfinden. Dabei ist insbesondere die Frage, ob eine unbefugte Veröffentlichung erfolgt ist oder inwiefern diese anzunehmen ist, für die Bewertung der Eintrittswahrscheinlichkeit eines Risikos für Rechte und Freiheiten der betroffenen Personen relevant. Eine solche Bewertung ist insbesondere dann zu überprüfen und anzupassen, wenn neue Erkenntnisse vorliegen, etwa wenn im Rahmen

eines Vorfalls die Veröffentlichung personenbezogener Daten vom Angreifer angedroht wird oder eine solche Veröffentlichung tatsächlich erfolgt ist.

Die Abschätzung der Schwere des Risikos wiederum wird maßgeblich dadurch beeinflusst,

– durch welchen Personenkreis eine unbefugte Kenntnisnahme voraussichtlich möglich ist,
– welche Kategorien von Personen betroffen sind,
– welche Kategorien personenbezogener Daten betroffen sind, insbesondere unter Berücksichtigung von besonderen Kategorien personenbezogener Daten gemäß Art. 9 DS-GVO,
– welche Anzahl von Personen und Datensätzen betroffen ist,
– welche technischen und organisatorischen Maßnahmen ergriffen werden, um die Folgen der unbefugten Veröffentlichung abzumildern.

Auch hier ist bei neuen Erkenntnissen eine Anpassung der Abschätzung erforderlich, z. B. im Rahmen der Analyse etwaiger Veröffentlichungen personenbezogener Daten durch den Angreifer.

Die große Anzahl abgeflossener und veröffentlichter Daten in diesem Vorfall erforderte es, dass der Verantwortliche für die Auswertung der Veröffentlichung ein externes Unternehmen einband und diesem unter anderem auch die Aufgabe übertrug, in den veröffentlichten Daten personenbezogene Daten auszumachen und die betroffenen Personen zu identifizieren.

IV. Risikobewertung

Für die Risikobewertung waren im vorliegenden Fall die folgenden Kriterien von besonderer Bedeutung:

Möglichkeit der Kenntnisnahme durch Unbefugte

Die aus den IT-Systemen des Verantwortlichen abgeflossenen Dateien wurden durch die Verursacher des Vorfalls auf ihrer „Darknet“-Webseite frei zugänglich veröffentlicht. Die Hürde für weitere unbefugte Zugriffe ist dadurch als niedrig zu bewerten und der Personenkreis derjenigen, die auf diese Daten zugreifen können, ist nahezu unbeschränkt. Dadurch wird die Wahrscheinlichkeit des Eintritts eines Schadens und damit das Risiko für die betroffenen Personen erhöht.

Kategorien betroffener Personen

Bei dem hier beschriebenen Vorfall waren sowohl Versicherungsnehmerinnen und Versicherungsnehmer als auch Mitarbeitende und Geschäftspartner betroffen. Verschiedene Gruppen betroffener Personen können jeweils eine eigene Risikoabwägung erforderlich machen, je nachdem welche Kategorien personenbezogener Daten in ihrem Fall betroffen waren. Da die Gruppe der betroffenen Versicherungsnehmenden die größte der drei genannten bildete, werde ich mich bei der Darstellung der folgenden Aspekte auf diese Gruppe konzentrieren.

Kategorien personenbezogener Daten

Personenbezogene Daten der Versicherungsnehmenden waren überwiegend Adress- und Bankverbindungsdaten. Insbesondere die Bankverbindungsdaten stellten aufgrund der Besonderheiten der unternehmerischen Tätigkeit des Verantwortlichen eine Herausforderung dar. Da die Person, mit der ein Versicherungsverhältnis besteht, in einzelnen Fällen von der Person, die Zahlungen zu diesem Vertrag leistet, abweichen kann, konnten Bankverbindungen nicht in jedem Fall zweifelsfrei einer Versicherungsnehmerin oder einem Versicherungsnehmer mit einer bekannten Kontaktmöglichkeit zugeordnet werden. Die betroffenen Kategorien personenbezogener Daten sind von besonderer Bedeutung für die Beurteilung der Schwere des Risikos für Rechte und Freiheiten der betroffenen Personen. Der Verantwortliche muss dabei die möglichen Folgen einer missbräuchlichen Verwendung dieser Daten durch Unbefugte für Rechte und Freiheiten der betroffenen Personen bewerten. Im Falle der *Adressdaten* ist dabei zuerst an mögliche Betrugsversuche zu denken. Dabei wären sowohl ungerichtete Szenarien (massenweiser Versand von betrügerischen Schreiben oder Weiterverkauf zu Werbezwecken) als auch ein gezieltes Vorgehen möglich. Im vorliegenden Fall war ein persönliches Aufsuchen der betroffenen Personen hingegen unwahrscheinlich. Gleiches galt für eine etwaige akute Gefährdungslage für diese. Eine konkrete Gefährdung ist nicht zuletzt auch aufgrund der großen Anzahl gleichartiger Datensätze weniger wahrscheinlich. Bezogen auf *Bankverbindungsdaten* sind zunächst Zahlungs- und Bankbetrugs-Versuche zu berücksichtigen. Ein Beispiel dafür ist der Lastschriftbetrug, in dessen Rahmen unerlaubte Abbuchungen unter Vortäuschung einer genehmigten Lastschrift vorgenommen werden könnten.

Anzahl betroffener Datensätze

Durch die Verursacher des Vorfalls wurden ca. 25.000 Dateien im „Darknet“ veröffentlicht. Nicht jede dieser Dateien enthielt auch personenbezogene

Daten. Gerade bezogen auf die Bankverbindungsdaten waren es einige wenige Dateien, die einen Großteil entsprechender Datensätze enthielten. In etwa einem Dutzend Dateien fanden sich im weiteren Verlauf der Untersuchungen allein 180.000 Kontoverbindungsdaten. Da mögliche Folgen also auf eine sehr große Anzahl von Personen zutreffen könnten, war auch das damit verbundene Risiko entsprechend hoch zu bewerten.

Folgen unbefugter Veröffentlichung

Das Besondere an der hier vorgefallenen unbefugten Veröffentlichung personenbezogener Daten ist, dass sie im „Darknet“ erfolgte. Im Gegensatz zu üblichen Webseiten, die nahezu jedermann tagtäglich aufruft, ist aufgrund der für „Darknet“-Seiten zusätzlich zum Einsatz kommenden Anonymisierungs-Infrastruktur der Betreiber einer solchen Seite bei deren Besuch nicht ersichtlich, sofern er sich nicht selbst zu erkennen gibt. Dementsprechend finden auch übliche Maßnahmen der Strafverfolgungsbehörden, die etwa Veröffentlichungen auf bestimmten Social Media-Kanälen oder anderen Webseiten unterbinden können, bei „Darknet“-Seiten keinen vergleichbaren Ansatzpunkt. Verantwortliche müssen also damit rechnen, dass eine einmal im „Darknet“ erfolgte Veröffentlichung über längere Zeit bestehen und für Unbefugte abrufbar bleibt. Hinzu kommt, dass veröffentlichte Inhalte abgerufen, kopiert und weiterverbreitet werden können. Auch eine erfolgreiche Entfernung der Veröffentlichung bietet keinen wirksamen Schutz vor einer Weiterverbreitung oder erneuten Veröffentlichung. Dementsprechend wirkt sich eine Veröffentlichung in jedem Fall dauerhaft stark risikoerhöhend aus.

V. Benachrichtigung betroffener Personen gemäß Art. 34 DS-GVO

In der Zusammenschau der relevanten Fakten kommt der Verantwortliche hinsichtlich des Risikos zu einer Gesamtbewertung. Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten betroffener Personen zur Folge, so benachrichtigt der Verantwortliche die betroffenen Personen gemäß Art. 34 Abs. 1 DS-GVO unverzüglich von der Verletzung.

Bei dem hier beschriebenen Vorfall kam der Verantwortliche zu dem Ergebnis, dass er die betroffenen Personen benachrichtigen muss. Grundsätzlich muss diese Benachrichtigung *unverzüglich*, d. h. ohne schuldhaftes Zögern des Verantwortlichen erfolgen. Ob eine entstehende Verzögerung durch ein Verschulden des Verantwortlichen begründet ist, muss anhand der jeweiligen Umstände beurteilt werden. Im vorliegenden Fall sind dem Verantwortlichen die tatsächlich betroffenen Personen erst mit einigem zeitlichen Abstand be-

kannt geworden, da die Auswertung der großen abgeflossenen Datenmenge eine entsprechende Zeit in Anspruch nahm.

In solchen Fällen, in denen eine Benachrichtigung der betroffenen Personen auf direktem Wege mit einem unverhältnismäßigen Aufwand verbunden ist – zum Beispiel auch, weil diese Personen nicht genau ermittelt werden können –, hat die Benachrichtigung stattdessen gemäß Art. 34 Abs. 3 lit. c DS-GVO in Form einer öffentlichen Bekanntmachung oder durch eine ähnliche Maßnahme zu erfolgen. Auch dem Begriff der Öffentlichkeit einer solchen Bekanntmachung ist besonderes Augenmerk zu schenken. Eine Bekanntmachung auf der unternehmenseigenen Webseite des Verantwortlichen erfolgte im vorliegenden Fall bereits zu einem sehr frühen Zeitpunkt. Der Verantwortliche musste jedoch davon ausgehen, dass seine Kundinnen und Kunden üblicherweise die Webseite des Versicherungsvereins nicht regelmäßig aufsuchen. Daher entschied er sich zu einem späteren Zeitpunkt, die Bekanntmachung auch in zwei auflagenstarken Tageszeitungen veröffentlichen zu lassen. Nachdem ihm die betroffenen Personen bekannt geworden waren, erfolgte schließlich auch noch eine persönliche Benachrichtigung auf dem Postweg.

In bestimmten Fallkonstellationen ist es denkbar, dass eine Benachrichtigung per Serienbrief nicht ausreicht, weil Einzelfälle gesonderte Benachrichtigungsinhalte erforderlich machen, damit der Verantwortliche seiner Pflicht aus Art. 34 DS-GVO vollumfänglich nachkommen kann. Daran ist insbesondere dann zu denken, wenn einzelne Datensätze aus den übrigen dadurch hervorstechen, dass sie die Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen in besonderer Weise nahelegen. Ein Beispiel hierfür wäre etwa, wenn neben einer großen Zahl gleichartiger Kontodaten auch noch bestimmte Datensätze existieren würden, die auf Details einzelner Versicherungsverhältnisse eingingen. Davon betroffene Personen wären dann durch entsprechend angepasste Benachrichtigungen zu informieren. Gegebenenfalls kann der Verantwortliche eine Gruppenbildung vornehmen, um bestimmte Fallgruppen betroffener Personen zu unterscheiden und diese jeweils angemessen zu benachrichtigen.

VI. Beratung betroffener Person durch meine Behörde

Im Nachgang insbesondere der postalischen Benachrichtigungen durch den Verantwortlichen erreichten meine Behörde etwa 50 schriftliche Eingaben betroffener Personen – einige davon als Beschwerden gemäß Art. 77 Abs. 1 DS-GVO – sowie eine Vielzahl telefonischer Anfragen. Die Beschwerdesachverhalte zielten dabei hauptsächlich auf die Frage der Unverzüglichkeit der Benachrichtigung ab.

Darüber hinaus wandten sich betroffene Personen mit der Frage an mich, wie sie sich verhalten sollten, um mögliche Folgen aus der Veröffentlichung ihrer personenbezogenen Daten abzuwehren. Vor dem Hintergrund der zuvor dargestellten Risiken informierte ich die Anfragenden in solchen Fällen darüber, dass sie sich der Möglichkeit verschiedentlicher Betrugsversuche infolge der Bekanntgabe ihrer Adress- oder Kontodaten bewusst sein sollten. Mit Blick auf die betroffenen Kontodaten fanden viele der Betroffenen kompetente Hilfe bei den für sie zuständigen Banken und Sparkassen. Diese rieten ihnen beispielsweise dazu, ihre Kontoauszüge regelmäßig auf unbefugte Abbuchungen zu überprüfen und in solchen Fällen aktiv zu werden.

VII. Betreuung der verantwortlichen Stelle

Mit dem betroffenen Versicherungsverein stand ich bereits früh in regelmäßigem Austausch. Da der Schwerpunkt meiner Arbeit dabei auf den datenschutzrechtlichen Fragestellungen lag, fand der Verantwortliche insbesondere in Fragen der IT-Sicherheit sowie der strafrechtlichen Aspekte an anderer Stelle einen weiteren kompetenten Anlaufpunkt: Die zentrale Anlaufstelle Cybercrime beim Hessischen Landeskriminalamt bündelt personelle und fachliche Ressourcen bei der Aufklärung von Straftaten im digitalen Raum und vermittelt den Kontakt zu Stellen, die bei der Verbesserung der unternehmenseigenen IT-Sicherheit beraten und unterstützen können. Im Land Hessen kommt dabei regelmäßig dem Hessen CyberCompetenceCenter eine besondere Bedeutung zu, da dieses für öffentliche Stellen sowie für kleine und mittlere Unternehmen der Privatwirtschaft bei der Bearbeitung konkreter Cybersicherheitsvorfälle auf Anfrage tätig wird. Sofern eine Kontaktaufnahme zu meiner Behörde erfolgt, bevor eine Betreuung mit Blick auf die IT-Sicherheit der meldenden Stelle sichergestellt ist, empfehle ich Verantwortlichen in der Regel, diese Unterstützungsangebote wahrzunehmen.

IT-Notstand im Unternehmen durch einen Ransomware-Angriff

Nicht immer muss ein Ransomware-Angriff zu einer Verschlüsselung der IT-Systeme eines Opfers führen. Auch wenn solche Angriffe entdeckt und vor der Verschlüsselung unterbunden werden, stellt die Bewältigung des Angriffs Unternehmen vor große Herausforderungen, insbesondere wenn sich bereits durch eine Ausleitung und Veröffentlichung von Daten durch die Angreifer schwerwiegende Verletzungen des Schutzes personenbezogener Daten ergeben haben. Was soll ein Unternehmen tun, wenn nichts mehr geht und doch schnell reagiert werden muss?

In dem hier zu berichtenden Fall wurde mir zunächst nur ein Angriff auf das Unternehmensnetzwerk gemeldet, bei dem Daten abgezogen und im sogenannten „Darknet“ veröffentlicht wurden. Genauere Details zum Sachverhalt enthielt die Meldung nicht. Eine weitere Sachverhaltsaufklärung ergab, dass eine bekannte Ransomware-Gruppe mit dem Vorfall im Zusammenhang stand, da aus dem IT-Netzwerk des Verantwortlichen exfiltrierte Daten auf der Darknet-Site dieser Gruppe veröffentlicht wurden.

Der Ablauf des Angriffs folgte dem bekannten Vorgehen bei Ransomware-Angriffen. Über einen initialen Zugang (vermutlich über Phishing oder eine andere Form des Social-Engineering) zu einem IT-System des Opfers breiteten sich die Angreifer lateral in der IT-Infrastruktur des Verantwortlichen aus und versuchten hierbei u. a., auch ihre Zugriffsrechte auf weitere IT-Systeme und -Dienste auszuweiten. Mitarbeitende des Verantwortlichen stellten im Verlauf des Angriffs ein ungewöhnliches Verhalten in der IT-Infrastruktur fest und meldeten dies der IT-Abteilung. Diese reagierte umgehend und konnte den Angreifern den Zugriff auf die IT-Infrastruktur entziehen, bevor diese IT-Systeme und Daten verschlüsseln konnten. Allerdings war es zu diesem Zeitpunkt bereits zu einer Exfiltration von Daten gekommen. Die Angreifer versuchten daraufhin, Lösegeld für die Nichtveröffentlichung der Daten zu erpressen. Letztendlich kam es zu der angedrohten Veröffentlichung der Daten auf der Darknet-Site der Ransomware-Gruppe.

Auch wenn es bei dem Angriff zu keiner Verschlüsselung der IT-Systeme gekommen war und damit nicht zu einem unmittelbaren Betriebsstillstand, stellte die Bewältigung des Vorfalls den Verantwortlichen vor große Herausforderungen. Nachdem sichergestellt wurde, dass den Angreifern der Zugriff entzogen worden war, mussten auf Grund der möglichen lateralen Ausbreitung der Angreifer alle IT-Systeme zunächst als potenziell kompromittiert angesehen und entsprechend behandelt werden. Um das Ausmaß des Angriffs abschätzen und eingrenzen zu können, waren IT-forensische Untersuchungen notwendig, für die ein externer IT-Sicherheitsdienstleister hinzugezogen wurde. Abhängig von den Ergebnissen der forensischen Untersuchung wurden die betroffenen IT-Systeme bereinigt und wiederhergestellt oder mussten vollständig neu aufgesetzt werden.

Weiterhin unterzogen der Verantwortliche und der beauftragte IT-Sicherheitsdienstleister die im Darknet veröffentlichten Unternehmensdaten einer systematischen Analyse. Ziel war es dabei, den Umfang der Verletzungen des Schutzes personenbezogener Daten und die betroffenen Personen zu ermitteln, um diese gemäß Art. 34 DS-GVO benachrichtigen zu können. Die Untersuchung ergab, dass neben personenbezogenen Daten von Beschäftigten des Verantwortlichen auch Beschäftigtendaten von weiteren Unterneh-

men, wie Kunden, Kooperationspartnern, Zulieferern o. Ä. betroffen waren. Soweit Daten im Auftrag verarbeitet wurden, konnten die entsprechenden Verantwortlichen informiert werden. Auf Grund der außerordentlichen Komplexität der im Darknet veröffentlichten Daten war die Analyse nicht kurzfristig möglich, erfolgte jedoch in angemessener Zeit.

In Folge der Benachrichtigung der anderen betroffenen Unternehmen kam es zu weiteren Meldungen gemäß Art. 33 DS-GVO bei Datenschutzaufsichtsbehörden in anderen Bundesländern und Ländern des EWR. Diese stellten dann vereinzelt auch bei mir Rückfragen zu dem Vorfall.

Die Verpflichtung des Verantwortlichen, eine Verletzung des Schutzes personenbezogener Daten innerhalb von 72 Stunden zu melden, ergibt sich aus Art. 33 Abs. 1 DS-GVO, falls mindestens von einem Risiko für die Rechte und Freiheiten natürlicher Personen ausgegangen werden muss. In komplexen Vorfällen besteht für Verantwortliche die Möglichkeit, gemäß Art. 33 Abs. 4 DS-GVO Informationen schrittweise zur Verfügung zu stellen. Dies muss aktiv durch den Verantwortlichen und ohne unangemessene weitere Verzögerung erfolgen.

Für den Auftragsverarbeiter ergibt sich aus Art. 33 Abs. 2 DS-GVO die Verpflichtung, eine Verletzung des Schutzes personenbezogener Daten unverzüglich nach Bekanntwerden dem jeweiligen Verantwortlichen anzuzeigen. Konkret bedeutet dies, dass der Auftragnehmer den Verantwortlichen umgehend informieren muss, wenn seine Ermittlungen ergeben haben, dass personenbezogene Daten, die in den Verantwortungsbereich des Verantwortlichen fallen, betroffen sind. Auf Grund der in diesem konkreten Fall aufwendigen und damit langwierigen Analyse der Daten war dies erst nach mehreren Wochen möglich, weil erst dann festgestellt werden konnte, welche Verantwortliche betroffen waren.

Die vom betroffenen Unternehmen als Verantwortlichem und als Auftragsverarbeiter ergriffenen technischen und organisatorischen Maßnahmen als Reaktion auf den Vorfall waren angemessen und hinreichend, um den Vorfall zu beenden und eine Wiederholung zu verhindern.

Der beschriebene Vorfall zeigt, dass ein Ransomware-Angriff in der Regel zu Verletzungen des Schutzes personenbezogener Daten führt. Insbesondere muss bei einer Exfiltration von personenbezogenen Daten durch die Angreifer auch geprüft werden, ob von einem hohen Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen ausgegangen werden muss. Dies dürfte häufig der Fall sein. Gemäß Art. 34 DS-GVO ist in solchen Fällen eine Benachrichtigung der von den Verletzungen betroffenen Personen erforderlich. Kommt es zur Veröffentlichung von Daten durch die Angreifer, erhöht sich grundsätzlich das Risiko signifikant, da mit der allgemeinen Verfügbarkeit die

Wahrscheinlichkeit, dass diese Daten von Dritten genutzt oder missbraucht werden, entsprechend steigt. Im vorliegenden Fall war eine detaillierte Analyse der veröffentlichten Daten erforderlich, um sowohl Verantwortliche als auch betroffene Personen zu identifizieren und das konkrete Risiko für deren Rechte und Freiheiten individuell abschätzen zu können.

Ein häufiges Problem bei der Exfiltration von Daten durch Angreifer ist, dass es Verantwortlichen im Nachhinein schwerfällt oder nicht möglich ist festzustellen, welche konkreten Daten die Angreifer erbeutet haben. Hierzu wäre eine feingranulare Protokollierung von Ereignissen, Zugriffen, aufgebauten Internetverbindungen und übertragenen Datenmengen auf allen IT-Systemen und -Diensten notwendig. Auch müsste diese den vollständigen Zeitraum des Angriffs abdecken. Angreifer sind bei dieser Art von Angriffen jedoch oftmals mehrere Tage, Wochen oder sogar Monate im IT-Netzwerk der Opfer aktiv, ohne entdeckt zu werden. Für konkrete Aussagen bleibt Verantwortlichen oftmals nur die Möglichkeit, sich zumindest teilweise auf Angaben zu stützen, die die Angreifer preisgeben. Das heißt, sie müssen sowohl die veröffentlichten Daten analysieren, als auch die von Angreifern bereitgestellten Nachweise in Form von Dateilisten o. Ä. auswerten. Ein Verantwortlicher kann hieraus aber nicht schließen, dass nicht noch weitere Daten exfiltriert wurden. Auch kann eine zukünftige Nutzung der Daten ebenso wenig ausgeschlossen werden wie eine Nutzung heruntergeladener Daten durch weitere Akteure. Auch zeigen sich Tendenzen, dass Ransomware-Gruppen Daten im Darknet zum Kauf anbieten. Die konkrete Risikobewertung hängt daher von jedem Einzelfall, dem Kontext und gegebenenfalls auch gesammelten Erfahrungen mit bestimmten Angreifergruppen ab.

Der Vorfall zeigt auch, dass hohe Anstrengungen der Vorsorge gegen solche Angriffe unternommen werden müssen. Sie erfolgen meist durch Social-Engineering. Mitarbeitende eines Unternehmens oder einer Behörde werden beispielsweise dazu verleitet, auf Links in E-Mails oder Internetseiten zu klicken, über die dann die Angriffssoftware in das System des Verantwortlichen übertragen wird. Diese Schwachstelle zu reduzieren, ist im Vergleich zu dem möglichen Schaden eines gelungenen Angriffs immer rentabel. Diese Risikominimierung fordert immer wieder gezielte Maßnahmen der Aufklärung und Bewusstseinsbildung.

18.3
Umgang mit Schwachstellen in Internet-Diensten

Sicherheitskritische Schwachstellen in Software können es Angreifern ermöglichen, IT-Systeme zu kompromittieren. Die Auswirkungen auf den

Datenschutz zeigten sich eindrucksvoll mit den im März 2021 bekannt gewordenen Schwachstellen in der weitverbreiteten Software Microsoft Exchange.

Schwachstellen in Software

Software ohne Fehler gibt es offenbar nicht. Eine für die Sicherheit der Verarbeitung von personenbezogenen Daten besonders relevante Kategorie von Fehlern in Software sind die sogenannten „Schwachstellen“. Diese Art von sicherheitsrelevanten Fehlern kann dazu führen, dass IT-Systeme oder -Dienste anfällig für Bedrohungen werden und somit eine konkrete Gefährdung entsteht. Aus Sicht des Datenschutzes kann die erfolgreiche Ausnutzung von Schwachstellen durch Angreifer zu Verletzungen der in Art. 32 Abs. 1 lit. b DS-GVO geforderten Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit führen.

Um Schwachstellen einheitlich referenzieren zu können, wird in der Regel das „Common Vulnerabilities and Exposures“-System (CVE) (The Mitre Corporation, About the CVE Program, https://www.cve.org/About/Overview) und für die Bewertung der Kritikalität der Industriestandard „Common Vulnerability Scoring System“ (CVSS) (Forum of Incident Response and Security Teams (FIRST), Common Vulnerability Scoring System SIG, https://www.first.org/cvss/) verwendet.

Zur Beseitigung von Schwachstellen ist es notwendig, dass die Hersteller der entsprechenden Software Sicherheits-Updates entwickeln und bereitstellen. Wenn Angreifern Schwachstellen in Software bekannt werden, bevor entsprechende Software-Updates entwickelt und bereitgestellt werden können, entsteht ein besonders großes Risiko für IT-Systeme oder -Dienste. Werden diese Schwachstellen ausgenutzt, spricht man auch von sogenannten „Zero-Day“-Angriffen, da die Entwickler vor dem Beginn der Angriffe 0 Tage Zeit haben, die Schwachstellen zu beheben.

Besonders gefährdet sind in der Regel IT-Systeme oder -Dienste, bei denen Schwachstellen von Angreifern direkt über das Internet ausgenutzt werden können. Betreiber solcher IT-Systeme oder -Dienste müssen diese daher besonders schützen, um die Sicherheit der Verarbeitung personenbezogener Daten gemäß Art. 32 DS-GVO zu gewährleisten. Dazu gehört insbesondere auch das zeitnahe Einspielen von sicherheitsrelevanten Software-Updates. Da mit der Veröffentlichung von Software-Updates auch mögliche Angreifer von Schwachstellen erfahren, ist besonders bei kritischen Schwachstellen Eile geboten. Grundsätzlich ist es für den sicheren Betrieb von IT-Systemen oder -Diensten erforderlich, dass die Versorgung mit Sicherheits-Updates für eingesetzte Software durch den Hersteller sichergestellt ist. Auch ist die Beobachtung vertrauenswürdiger Informationsquellen hinsichtlich des Be-

kanntwerdens von Schwachstellen erforderlich. Sollte eine Schwachstelle bekannt werden und ein verfügbares Sicherheits-Update noch nicht eingespielt werden können oder ist noch kein Update des Herstellers verfügbar, so ist das durch die Schwachstelle verursachte Risiko zu bewerten. Abhängig vom Ergebnis sind gegebenenfalls weitere Maßnahmen zu ergreifen, die die Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO wieder gewährleisten und bis zu einer Deaktivierung betroffener Systeme reichen können. Das Vorgehen sollte in jedem Fall vom Verantwortlichen dokumentiert werden, um seinen Nachweispflichten gemäß Art. 24 Abs. 1 DS-GVO nachzukommen.

„ProxyLogon“-Schwachstellen in Microsoft Exchange Server

Dass diese Art von „Zero-Day“-Angriffen für im Internet erreichbare IT-Dienste katastrophale Auswirkungen für Unternehmen und die öffentlichen Verwaltungen sowie Bürgerinnen und Bürger in Hessen haben können, hat sich mit den am Mittwoch, den 3. März 2021, allgemein bekannt gewordenen schwerwiegenden Schwachstellen in der E-Mail-Server-Software Exchange der Firma Microsoft (Microsoft Exchange) gezeigt. Die Schwachstellen mit den CVE-IDs CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 und CVE-2021-27065, die auch unter dem Namen „ProxyLogon“ bekannt wurden, existierten in einer Vielzahl von Microsoft Exchange-Versionen und ermöglichten es Angreifern, über das Internet betroffene IT-Systeme (Exchange-Server) zu kompromittieren (BSI, „Cyber-Sicherheitswarnung: Mehrere Schwachstellen in MS Exchange, CSW-Nr. 2021-197772-11032“, https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-197772-1132.pdf). Damit war es Angreifern möglich, Zugriff auf die betroffenen IT-Systeme und damit grundsätzlich auch auf die dort gespeicherten oder verarbeiteten personenbezogenen Daten zu erlangen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ging allein in Deutschland von 57.000 betroffenen Exchange-Servern aus und stufte die Schwachstellen mit der höchst möglichen Kritikalität als „IT-Bedrohungslage rot“ ein. Betroffene Verantwortliche mussten daher von einer realen und unmittelbaren Gefährdung für die von ihnen betriebenen Exchange-Server ausgehen. Als Folge der Schwachstellen wurde eine Vielzahl der verwundbaren Exchange-Server aktiv angegriffen und sehr häufig auch kompromittiert. Dementsprechend haben viele Verantwortliche in Hessen mögliche oder auch bereits konkret erkannte Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO bei mir gemeldet.

Zum technischen Hintergrund gehört, dass sich die ProxyLogon-Schwachstellen in den Komponenten oder der Funktionalität der Exchange-Server befanden, die eine Verbindung über das Hypertext Transfer Protocol Secure (HTTPS) ermöglichten. Dies wird beispielsweise für die häufig genutzte

Web-Mail-Schnittstelle Outlook Web Access (OWA), dem Modul Unified Messaging (UM) oder für die Synchronisation von mobilen Endgeräten mit „ActiveSync“ benötigt. Dementsprechend waren Exchange-Server, die diese Funktionaltäten nicht verwendeten oder für die wirksame zusätzliche technische Maßnahmen ergriffen worden waren, vor erfolgreichen Angriffen geschützt.

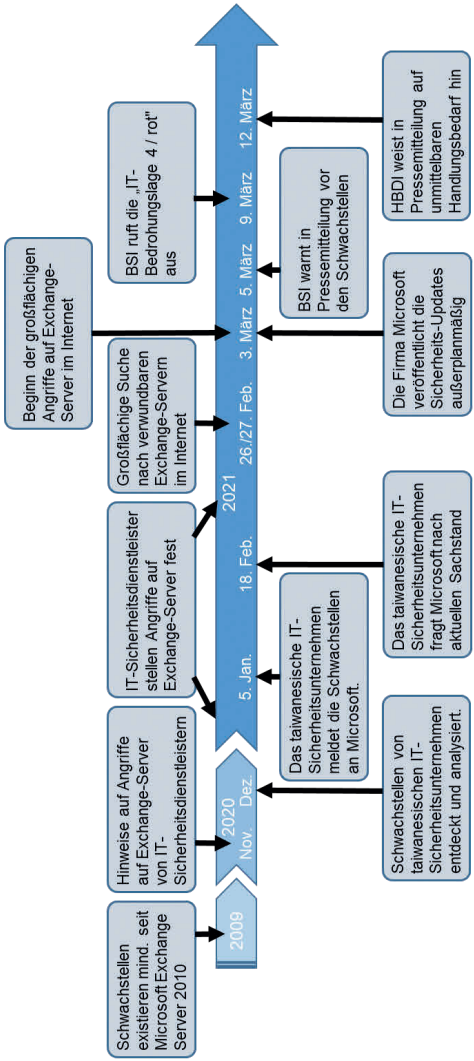


Abb. 4 Zeitstrahl ProxyLogon-Schwachstellen

Der zeitliche Ablauf des Geschehens rund um die ProxyLogon-Schwachstellen ist in Abbildung 4 als Zeitstrahl dargestellt. Dieser macht die Gefährdung durch diese Art von Zero-Day-Schwachstellen deutlich. So waren die unter dem Begriff ProxyLogon zusammengefassten Schwachstellen mindestens seit der Microsoft Exchange-Version 2010, also seit über zehn Jahren in allen Versionen vorhanden.

Das BSI zitiert in seiner Cyber-Sicherheitswarnung IT-Sicherheitsdienstleister, die seit November 2020 bei Kunden Hinweise auf ausgenutzte und bisher unbekannte Schwachstellen gefunden haben. Die ProxyLogon-Schwachstellen wurden dann im Dezember 2020 durch ein taiwanesisches IT-Sicherheitsunternehmen entdeckt, analysiert und der Firma Microsoft am Dienstag, den 5. Januar 2021, gemeldet. Auf Nachfrage wurde dem IT-Sicherheitsunternehmen von Microsoft am Donnerstag, den 18. Februar 2021, mitgeteilt, dass die entsprechenden Sicherheits-Updates am Dienstag, den 9. März, im Rahmen des üblichen „Patchday“ bereitgestellt werden sollten.

Gleichzeitig wurden im Januar und Februar von verschiedenen IT-Sicherheitsdienstleistern Angriffe auf Exchange-Server von einzelnen Unternehmen und Organisationen unter Ausnutzung der Schwachstellen festgestellt. Dies wurde der Firma Microsoft ebenfalls gemeldet. Ab dem 26. oder 27. Februar 2021 haben dann unterschiedliche Angreifer damit begonnen, aktiv und großflächig im Internet nach von den Schwachstellen betroffenen Exchange-Servern zu suchen. Als Reaktion darauf stellte die Firma Microsoft am Mittwoch, den 3. März 2021, die Sicherheits-Updates noch vor dem üblichen Patchday bereit und veröffentlichte eine Sicherheitswarnung mit dem Aufruf, betroffene Exchange-Server umgehend zu aktualisieren. Nach dieser Veröffentlichung begannen Angreifergruppen, die verwundbaren Exchange-Server automatisiert und auf breiter Front anzugreifen und zu kompromittieren. Am Freitag, den 5. März, warnte das BSI in einer Pressemitteilung vor den Schachstellen und kündigte an, Betreiber von betroffenen Exchange-Servern direkt zu kontaktieren und auf die Gefahrenlage hinzuweisen (BSI, Pressemitteilung „BSI warnt: Kritische Schwachstellen in Exchange-Servern – Sofortiges Handeln notwendig!“ vom 5. Mai 2021 https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/210305_Exchange-Schwachstelle.html).

In der darauffolgenden Woche rief das BSI dann die „IT-Bedrohungslage 4/rot“ aus, da immer noch zehntausende Exchange-Server in Deutschland gefährdet waren und ein umgehendes Handeln der Betreiber notwendig war.

Am Freitag, den 12. März 2021, habe ich in einer Pressemitteilung auf den unmittelbaren Handlungsbedarf durch Verantwortliche und Betreiber von betroffenen Exchange-Servern hingewiesen und für diese Art von Vorfällen

konkretisiert, wann eine Meldung des Vorfalls gemäß Art. 33 DS-GVO an mich notwendig ist (HBDI, Pressemitteilung „Unmittelbarer Handlungsbedarf wegen Schwachstellen in Microsoft Exchange-Server“ vom 12. März 2021).

Die Auswirkungen dieser kritischen Schwachstellen für Verantwortliche und Betreiber von betroffenen Exchange-Servern waren weitreichend. Zum einem ist festzustellen, dass die Sicherheits-Updates durch die Firma Microsoft zu einem Zeitpunkt zur Verfügung gestellt wurden, zu dem eine Vielzahl erfolgreicher Angriffe bereits durchgeführt worden waren. Zum anderen mussten zum Teil aufwendige und zeitintensive Vorbereitungen getroffen werden, damit die Sicherheits-Updates für die ProxyLogon-Schwachstellen eingespielt werden konnten.

Da bereits vor der Bereitstellung der Sicherheits-Updates erfolgreiche Angriffe auf betroffene Exchange-Server durchgeführt worden waren, war es nicht ausreichend, ausschließlich die bereitgestellten Updates einzuspielen. Zunächst mussten für betroffene Exchange-Server erfolgreiche Angriffe ausgeschlossen werden, wobei im Zweifelsfall von einer Kompromittierung der IT-Systeme auszugehen war. Daher war es zunächst erforderlich, betroffene Exchange-Server gemäß den verfügbaren Empfehlungen, Anleitungen und Hilfestellungen umfassend zu überprüfen. Stellte der Verantwortliche einen erfolgreichen Angriff auf einen Exchange-Server fest, musste er diesen Angriff wirksam eindämmen und den Angreifern den Zugriff entziehen. Hierzu war es zusätzlich erforderlich, weitere IT-Systeme und -Dienste im Umfeld des betroffenen Exchange-Servers umfassend zu analysieren, um eine laterale Ausbreitung der Angreifer auszuschließen oder dieser zu begegnen.

Datenschutzrechtliche Bewertung und Reaktion

Aus Sicht des Datenschutzes muss festgestellt werden, dass ein erfolgreicher Angriff auf einen Echange-Server im obigen Szenario zu einer Verletzung der in Art. 32 Abs. 1 lit. b DS-GVO definierten Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit führen konnte. Hiervon sind nicht nur die E-Mail-Inhalte einschließlich ihrer Anhänge, sondern auch die zugehörigen Metadaten der E-Mails, mit denen das Kommunikationsverhalten der Nutzer analysiert werden kann, betroffen. Hinzu kommen gegebenenfalls weitere personenbezogene Daten, z. B. Account-Daten, Einträge in Kalendern oder Adressbucheinträge. Von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO war insbesondere dann auszugehen, wenn Hinweise für den Zugriff durch unberechtigte Dritte vorlagen. Unabhängig, ob es zu einer Kompromittierung gekommen ist, verpflichtet Art. 32 Abs. 1 DS-GVO Verantwortliche und Auftragsverarbeiter zu Folgendem:

Art. 32. DS-GVO

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Durch das Vorliegen der ProxyLogon-Schwachstellen war die Sicherheit der Verarbeitung von personenbezogenen Daten gemäß Art. 32 Abs. 1 DS-GVO auf den betroffenen Exchange-Servern gefährdet. Nach Bekanntwerden der Schwachstellen war es daher notwendig, neu zu bewerten, ob ein angemessenes Schutzniveau mit den bis dahin getroffenen technischen und organisatorischen Maßnahmen noch zu gewährleisten war. In der Regel war die Gewährleistung des Schutzniveaus gefährdet und daher eine umgehende Reaktion unerlässlich. Um das erforderliche Schutzniveau wiederherzustellen, war als Maßnahme das unverzügliche Einspielen der Sicherheits-Updates notwendig, aber nicht hinreichend. Da von einer bereits erfolgten Kompromittierung der betroffenen Exchange-Server ausgegangen werden musste, waren mindestens die vom Hersteller Microsoft bzw. dem BSI empfohlen weiteren Maßnahmen umzusetzen.

Die konkrete Bewältigung der durch die ProxyLogon-Schwachstellen ausgelösten Vorfälle war nicht nur für die Verantwortlichen und Betreiber von betroffenen Exchange-Servern eine Ausnahmesituation, sondern hat auch meine Behörde vor Herausforderungen gestellt. Insgesamt kam es in diesem Zusammenhang zu über 250 Meldungen von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO bis Ende Mai 2021. Damit machten diese etwa ein Drittel aller Meldungen gemäß Art. 33 DS-GVO in

diesem Zeitraum aus. Die meisten Meldungen trafen innerhalb der ersten drei Wochen nach dem Bekanntwerden der Schwachstellen ein.

Bei dieser Art von Vorfällen, bei denen IT-Systeme und -Dienste möglicherweise erfolgreich angegriffen und kompromittiert wurden, erfolgt in der Regel eine individuelle technische Sachverhaltsklärung durch meine Mitarbeiterinnen und Mitarbeiter. Hierdurch vergewissere ich mich davon, dass die Verantwortlichen und Auftragsverarbeiter ihren Verpflichtungen nach Art. 33 DS-GVO nachkommen und die als Reaktion auf den Vorfall umgesetzten technischen und organisatorischen Maßnahmen angemessen und wirksam sind, um diesen zu beenden und eine Wiederholung zu verhindern. Weiterhin muss sichergestellt sein, dass bei einem hohen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen die Betroffenen durch den Verantwortlichen gemäß Art. 34 DS-GVO angemessen benachrichtigt werden.

Die große Zahl weitgehend gleichartiger Vorfälle versetzte mich in die Lage, die Bearbeitung der überwiegenden Mehrheit der Fälle durch ein standardisiertes Vorgehen zu vereinheitlichen und effizient zu bearbeiten. Zu diesem Zweck wurde in meiner Behörde zunächst ein optimierter Prozess für diese Art der Vorfälle entworfen, abgestimmt und umgesetzt. Durch meine Mitarbeiterinnen und Mitarbeiter wurde ein Fragebogen entwickelt, der den Verantwortlichen zusammen mit der Eingangsbestätigung zugesandt wurde. Mit diesem Fragebogen wurden die relevanten Aspekte der Vorfälle erfasst und auf Basis der Antworten standardisiert bewertet. Hierauf aufbauend wurde entschieden, in welchen Fällen von einer Erfüllung der datenschutzrechtlichen Verpflichtungen durch die Verantwortlichen ausgegangen werden konnte. Vorfälle bei denen auch nach der Beantwortung des Fragebogens noch datenschutzrechtliche Fragen offen waren, wurden einer individuellen Prüfung unterzogen. Mit diesem Vorgehen war es möglich, neben der Bearbeitung des normalen Aufkommens an Meldungen gemäß Art. 33 DS-GVO die Vorgänge zu den ProxyLogon-Schwachstellen bis Ende des Jahres 2021 weitestgehend abzuschließen.

Zusammenfassend für alle gemeldeten Vorfälle hat die technische Prüfung Folgendes ergeben: Auf Basis des beschriebenen Prozesses haben meine Mitarbeiterinnen und Mitarbeiter über 250 Meldungen gemäß Art. 33 DS-GVO bearbeitet und dabei die Vorfälle geprüft, bewertet und den Verantwortlichen Rückmeldungen gegeben. Bei knapp 30% der gemeldeten Vorfälle kam es nach Angaben der Verantwortlichen zu keiner Kompromittierung der Exchange-Server. Bei etwas über der Hälfte der Verantwortlichen wurde ein erfolgreicher Angriff und eine Kompromittierung des betroffenen Servers festgestellt oder konnte nicht ausgeschlossen werden. Hierbei blieb der jeweilige Vorfall allerdings nach Angaben der Verantwortlichen auf die

jeweils betroffenen Server beschränkt. Eine laterale Ausbreitung auf weitere IT-Systeme wurde für etwas über 15% der Vorfälle gemeldet. Bei 10% der Meldungen konnten die Verantwortlichen ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen nicht ausschließen und haben diese entsprechend Art. 34 DS-GVO benachrichtigt. Nach Auswertung der zurückgesendeten Fragebögen ergaben sich bei etwa einem Drittel der Vorfälle zusätzliche Rückfragen, die im Rahmen einer individuellen Prüfung geklärt wurden. Bis Ende Dezember waren die gemeldeten Vorfälle bis auf weniger als 2% der Vorgänge abgeschlossen.

Im Folgenden werden exemplarisch drei Fälle – in einem Unternehmen, einer öffentlichen Stelle und einer Rechtsanwaltskanzlei – beschrieben, in denen die Schwachstellen von Exchange-Servern von Angreifern ausgenutzt werden könnten.

I. Späte Reaktion auf Exchange-Schwachstellen

Die ProxyLogon-Schwachstellen in der E-Mail-Server-Software der Firma Microsoft haben bewirkt, dass weltweit zehntausende Exchange-Server kompromittiert werden konnten. Eine unverzügliche und angemessene Reaktion der Verantwortlichen hätte in vielen Fällen größeren Schaden verhindern können.

Am 3. März 2021 hatte die Firma Microsoft außerplanmäßige Software-Updates für die Exchange-Server-Software veröffentlicht, die kritische Schwachstellen der Software für Exchange-Server schlossen. Erst am 17. März 2021 meldeten mir 20 Verantwortliche aus Hessen gemäß Art. 33 DS-GVO mögliche Verletzungen des Schutzes personenbezogener Daten, die durch diese Schwachstellen ermöglicht wurden. Unter diesen befand sich ein IT-Systemhaus, dessen Vorfall hier exemplarisch beschrieben wird.

In der Meldung wurde bereits darauf verwiesen, dass neben dem Exchange-Server auch mehrere Domänen-Controller, also IT-Systeme zur Authentifizierung von anderen IT-Systemen und Benutzern, kompromittiert worden waren. Für die Bearbeitung von Meldungen gemäß Art. 33 DS-GVO entwickelte mein Haus in Zusammenhang mit den ProxyLogon-Schwachstellen einen Arbeitsprozess mit einem Fragebogen und übermittelte diesen an alle Verantwortlichen, die Art. 33-Meldungen eingereicht hatten, zur Beantwortung. Auf Basis der Auswertung des beantworteten Fragebogens und der ursprünglichen Meldung habe ich bei dem verantwortlichen IT-Systemhaus weitere Informationen angefordert. Relevant für die technische Prüfung waren dabei die laterale Ausbreitung der Angreifer im IT-Netzwerk des Verantwortlichen, die betroffenen IT-Dienste und die vom Verantwortlichen als Reaktion auf

den Vorfall ergriffenen technischen und organisatorischen Maßnahmen. Der Verantwortliche hat mir hierauf unter anderem den Abschlussbericht des von ihm beauftragten IT-Sicherheitsdienstleisters zur Verfügung gestellt. Diese Art Berichte sind generell für eine technische Prüfung von Datenschutzvorfällen hilfreich und ermöglichen in der Regel, Ausmaß und Kritikalität der Vorfälle besser einzuschätzen.

Für den konkreten Vorfall ergab sich aus dem Bericht, dass die initiale Kompromittierung des Exchange-Servers des Verantwortlichen bereits am 4. März 2021 erfolgte, also einen Tag nach der Veröffentlichung der Sicherheits-Updates durch die Firma Microsoft. Hierbei wurde durch die Angreifer eine sogenannte Web-Shell eingerichtet, die ihnen einen späteren Zugriff auf das IT-System ermöglichte. Vier Tage später, also am 8. März, wurde diese Web-Shell dann von den Angreifern als Ausgangspunkt genutzt, um sich lateral im IT-Netzwerk des Verantwortlichen auszubreiten. Hierbei konnten die Angreifer auch Domänen-Controller vollständig kompromittieren und damit theoretisch vollen Zugriff auf alle daran angebunden IT-Systeme und -Dienste erlangen.

Diese Informationen führten zu weiteren Rückfragen meinerseits, um die Angemessenheit und Wirksamkeit der Maßnahmen des Verantwortlichen als Reaktion auf die schwerwiegende Kompromittierung seiner IT-Infrastruktur und die darin verarbeiteten personenbezogenen Daten zu überprüfen. Der Verantwortliche gab mir gegenüber an, dass die Angreifer zwar weitgehenden Zugang auf seine IT-Systeme hatten. Im Rahmen der IT-forensischen Untersuchung konnten jedoch keine Anzeichen für eine Exfiltration oder anderweitige Verletzung des Schutzes personenbezogener Daten gefunden werden.

Als Reaktion auf den erfolgreichen Angriff hat sich der Verantwortliche entschlossen, die kompromittierten IT-Systeme nicht wiederherzustellen, sondern hat auf zu diesem Zweck beschafften Geräten eine vollständig neue IT-Umgebung aufgesetzt. Weiterhin wurden alle vorgeschlagenen und empfohlenen Maßnahmen des IT-Sicherheitsdienstleisters im vollen Umfang umgesetzt.

Auf Basis der Angaben des Verantwortlichen kam ich zu dem Schluss, dass der Angriff nach der Phase der lateralen Ausbreitung durch den Verantwortlichen entdeckt wurde, aber noch bevor der Schutz personenbezogener Daten durch die Angreifer verletzt wurde.

Als angemessene Reaktion auf Bekanntwerden der kritischen ProxyLogon-Schwachstellen hätten zum einem die am 3. März 2021 von der Firma Microsoft für die Exchange Server veröffentlichten Sicherheits-Updates unverzüglich eingespielt werden müssen. Auf Grund der von Microsoft und dem

BSI herausgegebenen Hinweise war weiterhin bekannt, dass das Einspielen der Sicherheits-Updates nicht ausreichend war, sondern von erfolgreichen Angriffen auf die Exchange Server ausgegangen werden musste. Daher war es notwendig, die betriebenen Exchange-Server auf eine mögliche Kompromittierung zu untersuchen. Der mir vom Verantwortlichen berichtete zeitliche Ablauf legt den Schluss nahe, dass die Einspielung der Sicherheits-Updates nicht unverzüglich erfolgte und auch die notwendige umgehende Untersuchung der Exchange-Server auf eine mögliche Kompromittierung unterblieb. Der Vorfall wurde erst über eine Woche später entdeckt, als die Angreifer bereits Zugriff auf die IT-Infrastruktur des Verantwortlichen hatten und diesen nutzten. Es stellt sich daher die Frage, inwieweit der Verantwortliche seinen Verpflichtungen gemäß Art. 32 DS-GVO zur Gewährleistung der Sicherheit der Verarbeitung nachgekommen ist.

Diese Vorschrift fordert von Verantwortlichen und Auftragsverarbeitern, dass sie ein dem Risiko angemessenes Schutzniveau und ihre Fähigkeit zur dauerhaften Sicherstellung der Schutzziele gewährleisten. Es stellt sich daher die Frage, auf welche Weise und wie schnell auf kritische Schwachstellen in IT-Systemen oder -Diensten zu reagieren ist. Das ungeprüfte und ungeplante Einspielen von Updates kann bei komplexen IT-Systemen zu Störungen im Betriebsablauf oder im ungünstigsten Fall zu einem Ausfall führen. Daher kann es aus betrieblichen Gründen zu Verzögerungen beim Einspielen kommen. Zur Minimierung des Risikos wären dann gegebenenfalls unterstützende Maßnahmen notwendig, um das Ausnutzen der Schwachstellen zu verhindern, mindestens aber zu erkennen. Abhängig vom Risiko spezifischer Schwachstellen, insbesondere wenn diese einfach über das Internet ausnutzbar sind und massenhaft ausgenutzt werden, kann eventuell auch die Deaktivierung von betroffenen IT-Diensten und -Systemen eine angemessene Maßnahme sein. Insbesondere bei dem hier betrachteten Vorfall gab es im Vorfeld nicht nur spezifische Warnungen des BSI mit entsprechenden Handlungsempfehlungen, sondern auch eine breite mediale Berichterstattung über die ProxyLogon-Schwachstellen.

Der Verpflichtung nach Art. 33 DS-GVO, mir innerhalb von 72 Stunden nach Bekanntwerden Verletzungen des Schutzes personenbezogener Daten zu melden, sofern mindestens von einem Risiko für Rechte und Freiheiten der betroffenen Personen auszugehen ist, ist der Verantwortliche nachgekommen.

Ein weiterer zu prüfender Aspekt ist es, ob eine Benachrichtigung der Betroffenen über die Verletzung des Schutzes ihrer personenbezogenen Daten nach Art. 34 Abs. 1 DS-GVO notwendig ist. Relevant für die Frage, ob eine Benachrichtigung der betroffenen Personen nach Art. 34 Abs. 1 DS-GVO zu erfolgen hat, ist der Umstand, ob durch den Vorfall voraussichtlich ein

hohes Risiko für Rechte und Freiheiten der betroffenen Personen vorliegt. Der Verantwortliche kam in seiner Risikobewertung zu dem Schluss, dass es zu keiner Verletzung des Schutzes personenbezogener Daten gekommen ist, da keine Anzeichen für einen Datenabfluss oder Zugriff der Angreifer auf personenbezogene Daten vorlagen und auch sonst keine Verletzungen von Schutzzielen identifiziert werden konnten.

Bei der abschließenden Bewertung des Vorfalls und der Reaktion des Verantwortlichen kam ich zu dem Schluss, dass dessen eingeleitete Maßnahmen zwar verspätet, dann aber angemessenen und hinreichend waren, um den Vorfall zu beenden und eine Wiederholung des Sachverhaltes zu verhindern. Nach der Entdeckung hat der Verantwortliche umgehend reagiert und einen externen IT-Sicherheitsdienstleister mit der umfassenden Analyse des Vorfalls beauftragt. Wichtig war auch, dass die kompromittierten IT-Systeme nicht nur bereinigt oder wiederhergestellt, sondern auf neuer Hardware eine neue IT-Umgebung aufgebaut und dabei die vorgeschlagenen und empfohlenen Maßnahmen des IT-Sicherheitsdienstleisters umgesetzt wurden.

Die Angabe des Verantwortlichen, dass es bei dem Vorfall zu keinem hohen Risiko und zu keiner konkreten Verletzung des Schutzes personenbezogener Daten gekommen ist, weil kein Datenabfluss festgestellt werden konnte und damit keine Benachrichtigung der Betroffenen gemäß Art. 34 DS-GVO notwendig war, habe ich akzeptiert, wobei ich ihn darauf hingewiesen habe, dass er nach Art. 33 Abs. 4 DS-GVO verpflichtet ist, mir eine veränderte Informationslage oder neue Erkenntnisse mitzuteilen.

II. Auswirkungen der Exchange-Schwachstellen bei einem hessischen Landkreis

Auch im Bereich der öffentlichen Verwaltung wirkten sich die Schwachstellen der Software für Exchange-Server als Einfallstor für Angriffe und für die Möglichkeit von Datenschutzverletzungen aus und erforderten umfassende Schutz- und Vorsorgemaßnahmen.

Am 10. März 2021 meldete mir ein hessischer Landkreis fristgerecht gemäß Art. 33 Abs. 1 DS-GVO, dass ein Microsoft Exchange-Server von den kurz vorher bekanntgewordenen Sicherheitslücken betroffen war und die Möglichkeit einer Verletzung des Schutzes personenbezogener Daten bestand. Der betroffene Microsoft Exchange-Server sei möglicherweise Ziel eines Angriffs geworden, in dessen Rahmen die Sicherheitslücken mit den Bezeichnungen CVE-2021-26855, CVE-2021-26857, CVE-2021-27065 und CVE-2021-26858 ausgenutzt worden waren. Diese Sicherheitslücken

sind auch als „Hafnium“-Sicherheitslücken bekannt, weil Microsoft vermutet, dass hinter den Angriffen eine Hackergruppe mit demselben Namen steht.

In der Meldung legte der Verantwortliche dar, dass bis zu 450 Beschäftigte von einer möglichen Verletzung des Schutzes ihrer personenbezogenen Daten betroffen sein könnten. Die Meldung sei jedoch nur vorsorglich abgegeben worden, weil eine tatsächliche Schutzverletzung noch nicht nachgewiesen werden konnte. Der Landkreis kam in der von ihm durchgeführten Risikoabschätzung zu dem Ergebnis, dass voraussichtlich kein hohes Risiko für Rechte und Freiheiten der betroffenen Personen vorläge. Dementsprechend müsse auch keine Benachrichtigung der betroffenen Personen gemäß Art. 34 Abs. 1 DS-GVO erfolgen. Gleichwohl habe er die möglicherweise betroffenen Beschäftigten am Tag nach Bekanntwerden der potenziellen Schutzverletzung freiwillig informiert.

In seiner Meldung stellte er mir auch die von ihm ergriffenen und geplanten technischen und organisatorischen Maßnahmen (TOM) dar, mit denen er sicherstellen wollte, dass eine konkrete weitere Schutzverletzung nicht eintreten könne. Als Sofortmaßnahme habe er die vom Hersteller Microsoft bereitgestellten Sicherheitsupdates eingespielt, nachdem die möglicherweise betroffenen Server offline genommen worden waren. Geplant sei zudem, eine Web-Application-Firewall in Betrieb zu nehmen, die geeignet sei, vergleichbaren Angriffen zu begegnen, da bei den vorliegenden Sicherheitslücken ein Angriff über die Web-Anwendung „Microsoft Outlook Web App“ erfolgen kann.

Auch dem Landkreis wurde der für die Bearbeitung der Art. 33-Meldungen zu den Exchange-Schwachstellen erstellte Fragebogen zugesandt. Dessen Fragen richteten sich insbesondere auf die Bewertung des Risikos für Rechte und Freiheiten der betroffenen Personen durch den Verantwortlichen sowie die von ihm im Rahmen des Vorfalls ergriffenen TOMs. Ich musste jedoch den Landkreis an die Beantwortung meines Fragebogens erinnern, da er die gesetzte Frist fruchtlos verstreichen ließ. Der Vorschrift des § 43 Abs. 3 BDSG folgend, stehen mir gegenüber öffentlichen Stellen wie der hier verantwortlichen Gebietskörperschaft zwar keine bußgeldbewehrten Abhilfemaßnahmen zur Verfügung, falls sie ihrer Pflicht gemäß Art. 31 DS-GVO zur Zusammenarbeit mit meiner Behörde nicht nachkommen. Jedoch verfüge ich auch in diesen Fällen über die Möglichkeit, sie gemäß Art. 58 Abs. 1 lit. a DS-GVO anzuweisen, die erforderlichen Informationen bereitzustellen. Von diesen Befugnissen musste ich jedoch keinen Gebrauch machen, da der Landkreis noch rechtzeitig auf meine Erinnerung reagierte und den ausgefüllten Fragebogen übermittelte.

Aus den Antworten ging beispielsweise hervor, dass er mindestens die vom Hersteller Microsoft sowie vom BSI bereitgestellten Informationen ausge-

wertet und die entsprechenden Maßnahmen umgesetzt hatte. Vertiefende Rückfragen wurden lediglich deshalb notwendig, weil sich der Verantwortliche nicht unmittelbar in der Lage sah festzustellen, dass seine Analysen des Vorfalls ausreichend waren. Gleichzeitig konnte er jedoch einen Datenabfluss ausschließen. Im Rahmen der Rücksprache mit ihm konnte er diesbezügliche Rückfragen meinerseits zufriedenstellend beantworten. Abschließend konnte ich daher davon ausgehen, dass der Verantwortliche angemessene und hinreichende Maßnahmen umgesetzt hatte, um den Vorfall zu beenden und eine Wiederholung zu verhindern. Mit einer entsprechenden Mitteilung schloss ich die Bearbeitung des Vorgangs ab.

III. Angriffe auf Exchange-Schwachstellen in Rechtsanwaltskanzleien

Auch hessische Rechtsanwaltskanzleien waren Ziele von Angriffen, die Schwachstellen der Exchange-Server-Software ausnutzten. Rechtsanwaltskanzleien müssen als datenschutzrechtlich Verantwortliche gemäß Art. 24 DS-GVO i. V. m. Art. 32 DS-GVO die Sicherheit der Verarbeitung der ihnen anvertrauten Daten gewährleisten und müssen sich daher proaktiv und ernsthaft mit dem Thema der Informationssicherheit auseinandersetzen.

Rechtsanwaltskanzleien in Hessen waren ebenfalls von der Ausnutzung der Sicherheitslücken in Microsofts Exchange-Server-Software betroffen. Meine Behörde hat sich hierzu frühzeitig an die hessischen Rechtsanwaltskammern gewendet und über die Problematik informiert. Die Rechtsanwaltskammer Frankfurt am Main hat daraufhin eine Warnung und Hinweise zu Abhilfemaßnahmen des BSI auf ihrer Internetseite veröffentlicht. In der Folge wurden mir zahlreiche Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DS-GVO gemeldet.

Rechtsanwaltskanzleien müssen als datenschutzrechtlich Verantwortliche gemäß Art. 32 DS-GVO für die Sicherheit der Verarbeitung personenbezogener Daten Sorge tragen. Hierzu gehören „geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“. Nach dem Bekanntwerden von Sicherheitslücken in der elektronischen Datenverarbeitung muss eine unverzügliche Untersuchung und Absicherung potenziell betroffener Systeme erfolgen. Dies setzt voraus, dass der Verantwortliche sich entweder selbst oder durch beauftragte Dienstleister bereits im Vorfeld aktiv über Entwicklungen im Bereich der IT-Sicherheit informiert. Der unbestimmte Rechtsbegriff des „Stands der Technik“ unterliegt einem stetigen Wandel, den der Verantwortliche verfolgen muss.

Nachdem die Bedrohung durch die Installation der vom Hersteller bereitgestellten Sicherheitsupdates und durch ergänzende Maßnahmen zunächst abgewendet zu sein schien, erreichten mich Ende des Jahres 2021 immer noch Meldungen über das Ausnutzen vorhandener oder neu aufgetretener Sicherheitslücken in der Exchange-Server-Software. Häufig wurden die kompromittierten Server zum Versand von E-Mails mit Hyperlinks verwendet, die Schadsoftware nachladen und dadurch weitere Systeme der Nachrichtenempfänger infizieren können. Hierbei sind praktisch in allen Fällen personenbezogene Daten betroffen, da die versandten E-Mails regelmäßig Metadaten und Nachrichteninhalte der gespeicherten Korrespondenz enthalten, um beim Empfänger den Anschein der Echtheit zu erwecken. Die nachgeladene Schadsoftware kann wiederum eine Verschlüsselung der Zielsysteme vornehmen, um im Anschluss Lösegeld für die verschlüsselten Daten zu erpressen. Ein solcher Vorfall beeinträchtigt die Verfügbarkeit personenbezogener Daten und kann gravierende Folgen für den laufenden Geschäftsbetrieb von Rechtsanwaltskanzleien haben.

Zu beachten ist außerdem, dass gemäß Art. 34 Abs. 1 DS-GVO eine Benachrichtigung betroffener Personen über die Verletzung des Schutzes personenbezogener Daten erforderlich ist, wenn hohe Risiken für deren Rechte und Freiheiten nicht ausgeschlossen werden können. Dies liegt bei einem Abfluss von personenbezogenen Daten, die einem Berufsgeheimnisträger anvertraut sind, besonders nahe. Benachrichtigungen wurden von den Verantwortlichen zumeist proaktiv vorgenommen. In einzelnen Fällen erfolgte dies erst nach einem Hinweis meiner Behörde. Gemäß Art. 34 Abs. 3 lit. c DS-GVO kann die Benachrichtigung auch durch öffentliche Bekanntmachung, wie einem Hinweis auf der Internetseite des Verantwortlichen, erfolgen, wenn sie ansonsten mit unverhältnismäßigem Aufwand verbunden wäre.

Die beschriebenen Vorfälle zeigen eindrucksvoll, dass Rechtsanwälte und Notare, die Informationstechnologie zur beruflichen Kommunikation nutzen, sich ernsthaft und kontinuierlich mit der Absicherung und Instandhaltung ihrer Systeme auseinandersetzen müssen. In der vernetzten Welt ist jedes über das Internet erreichbare System ein potenzielles Ziel für Cyberattacken. Dies gilt ohne Rücksicht auf Standort, Größe, Rechtsform oder etwaige Eigenschaft des Verantwortlichen als Berufsgeheimnisträger.

18.4
Verlust von Datenträgern

Der Verlust von Geräten und Datenträgern wie Speicherkarten, USB-Sticks, CDs/DVDs und Festplatten ist von besonderer Bedeutung, wenn auf diesen

Geräten Gesundheitsdaten, die ein höheres Missbrauchsrisiko haben, gespeichert sind.

Tagtäglich kommt es vor, dass Patienten beispielsweise von einer Arztpraxis die Zusendung von Unterlagen aus ihrer Patientenakte wünschen. Schnell sind die anforderten Befunde von der Arztpraxis auf einen einfachen USB-Stick kopiert, in einem Briefumschlag kuvertiert und per Post verschickt. Einige Tage später kommt der Anruf des Patienten, der Briefumschlag sei zwar angekommen, der USB-Stick sei aber nicht enthalten gewesen.

Wenn die auf dem USB-Stick enthaltenen Daten nicht gesichert waren, besteht theoretisch sowohl die Möglichkeit, dass es zu einer Offenlegung der personenbezogenen Daten kommen könnte, als auch, dass Unbefugte Zugang zu den Daten erhalten haben. Da man in diesen Fällen meist nichts Genaues zum Verbleib des USB-Sticks ermitteln kann, wird man diese Gefahr zumindest nicht ausschließen können. Es ist also von einer „Verletzung des Schutzes personenbezogener Daten“ gemäß Art. 4 Nr. 12 DS-GVO auszugehen.

Gemäß Art. 33 Abs. 1 DS-GVO ist der Verantwortliche – hier die Arztpraxis – verpflichtet, unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt geworden ist, diese der zuständigen Aufsichtsbehörde zu melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht, wenn ihnen Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile drohen (vgl. Erwägungsgrund 85 DS-GVO).

Zusätzlich sieht Art. 34 DS-GVO vor, dass die betroffenen Personen über die Datenpanne zu informieren sind, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat. Dabei wird bei Schutzverletzungen, die besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO (z. B. Gesundheitsdaten) betreffen, in den meisten Fällen von einem voraussichtlich hohen Risiko auszugehen sein, das eine Benachrichtigungspflicht begründet. Kein hohes Risiko bestünde dann, wenn die Daten sicher verschlüsselt worden wären, so dass Unberechtigte auch bei hohem Aufwand die Daten nicht nutzen könnten.

Die Benachrichtigung muss gemäß Art. 34 DS-GVO i. V. m. Art. 33 Abs. 3 lit. b, c und d DS-GVO die folgenden Informationen erhalten: Art der Schutzverletzung, den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen, eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten, eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen sowie Empfehlungen an die betroffenen Personen, wie die nachteiligen Auswirkungen der Schutzverletzung gemindert werden können.

Für den beschriebenen Fall stellt sich außerdem die Frage, ob Daten per USB-Stick und Briefpost überhaupt unverschlüsselt versendet werden dürfen. Die DS-GVO verlangt nach Art. 24, 25 Abs. 1 und 32, dass der Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen und umzusetzen hat. Dass immer wieder einmal Postsendungen verloren gehen, wird auch in Zukunft nicht auszuschließen sein. Im Unterschied zu einem normalen Brief besteht bei elektronischen Datenträgern, wie z. B. USB-Sticks, jedoch die Möglichkeit, den Inhalt sicher zu verschlüsseln. Mit einer solchen Maßnahme lässt sich auch der Postversand sicherer gestalten. Die Gefahr, dass bei einem Verlust des Datenträgers die enthaltenen Daten Unbefugten zur Kenntnis gelangen können, kann mit dem Einsatz von verschlüsselten Datenträgern deutlich minimiert werden. Ein solcher Schutz ist damit grundsätzlich geboten.

Die gewählte Form der Verschlüsselung muss dabei geeignet sein, die gespeicherten personenbezogenen Daten tatsächlich wirksam vor einem unbefugten Zugriff zu schützen. Sie muss mit einer Verschlüsselungssoftware durchgeführt werden, die einen entsprechend starken Verschlüsselungsalgorithmus, wie z. B. AES-256, unterstützt. Verantwortliche können ihre Suche nach geeigneter Software mit diesem Schlüsselwort zielführend gestalten, wobei verschiedene kommerzielle und frei verfügbare Produkte zur Auswahl stehen, die einzelne Dateien oder ganze Datenträger verschlüsseln können. Die Übermittlung des Passworts zur Entschlüsselung an den Empfänger muss ebenfalls auf sichere Weise erfolgen. Das Passwort darf also nicht etwa im gleichen Umschlag wie das Speichermedium übermittelt werden. Eine Übermittlung auf separatem Weg (z. B. Telefon, verschlüsselte E-Mail, gesonderter Brief mit zeitversetztem Versand) ist zu empfehlen.

Wären auf dem Datenträger die Daten in einer ausreichend, nach Stand der Technik verschlüsselten Form enthalten, könnte sowohl eine Meldung der Datenpanne als auch das Risiko, dass Daten Unbefugten zur Kenntnis gelangen könnten, in vielen Fällen vermieden werden.

18.5 Phase-Out nicht datenschutzrechtskonformer Technologien am Beispiel Fax

Die datenschutzrechtlichen Vorgaben zur Technikgestaltung und Sicherheit der Verarbeitung personenbezogener Daten verpflichten Verantwortliche, ihren Technologieeinsatz kritisch zu evaluieren und an sich verändernde Rahmenbedingungen anzupassen. Am Beispiel des Fax zeigt sich, dass bestimmte Technologien nicht länger datenschutzrechtskonform eingesetzt werden können. Bei der schrittweisen Ablösung des Fax stehen Verantwortlichen in vielen Anwendungsgebieten durch die Digitalisierung bereits konkrete datenschutzrechtskonforme Alternativen zur Verfügung.

I. Ausgangslage

Nicht zuletzt der technologische Wandel führt häufig zu veränderten Rahmenbedingungen bei der Verarbeitung personenbezogener Daten. Diese können die bisherige Datenschutzrechtskonformität eingesetzter Technologien in Frage stellen. Die datenschutzrechtlichen Vorgaben machen es erforderlich, dass Verantwortliche verändernde technologische Rahmenbedingungen beobachten und auf sie reagieren, wenn sich durch die veränderten Gegebenheiten auch das Risiko für die verarbeiteten personenbezogenen Daten verändert. Unter Umständen müssen Technologien, die nicht länger datenschutzrechtskonform eingesetzt werden können, durch solche ersetzt werden, bei denen dies möglich ist. Dabei kann in vielen Bereichen Digitalisierung helfen, Datenschutz zu verbessern.

Verantwortliche befinden sich in der Pflicht, diese Vorgabe umzusetzen, haben bei der Frage der genauen Art der Umsetzung jedoch einen Spielraum, der insbesondere die Auswahl konkreter datenschutzrechtskonformer Alternativen betrifft. Sofern hier eine Auswahl zwischen mehreren Alternativen besteht und die Verantwortlichen die vollständige Kontrolle über solche Mittel und Verfahren ausüben können – gegebenenfalls unter Zuhilfenahme von Auftragsverarbeitern –, ist dies nicht lediglich dem Erreichen der Datenschutzrechtskonformität zuträglich, sondern stärkt auch die digitale Souveränität der Verantwortlichen, also die Möglichkeit, ihre Rollen in der

digitalen Welt selbstständig, selbstbestimmt und sicher ausüben und ihre datenschutzrechtlichen Pflichten erfüllen zu können (s. Ziff. 3)

Als anschauliches Beispiel dafür, wie diese Anforderungen aussehen und wie Verantwortliche ihnen gerecht werden können, wird hier das Kommunikationsmedium „Fax“ betrachtet. Zu dessen Einsatz bei der Verarbeitung personenbezogener Daten habe ich im Berichtszeitraum Stellung genommen (Pressemitteilung „Zur Übermittlung personenbezogener Daten per Fax“ vom 14. September 2021, https://datenschutz.hessen.de/datenschutz/it-und-datenschutz/zur-%C3%BCbermittlung-personenbezogener-daten-per-fax).

II. Bedarf nach Ersatz nicht mehr datenschutzrechtskonformer Technologie

Verantwortliche müssen gemäß Art. 5 Abs. 2 DS-GVO bei der Verarbeitung personenbezogener Daten die Grundsätze der Datenverarbeitung aus Art. 5 Abs. 1 DS-GVO (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit) gewährleisten und deren Einhaltung nachweisen können. Gemäß Art. 25 DS-GVO (Datenschutz durch Systemgestaltung und durch datenschutzfreundliche Voreinstellungen) sind sie verpflichtet, diese Grundsätze zum Zeitpunkt der Festlegung der Mittel sowie zum Zeitpunkt der eigentlichen Verarbeitung durch geeignete technische und organisatorische Maßnahmen wirksam umzusetzen. Daraus ergibt sich eine Pflicht, Entwicklungen zum Beispiel im technologischen Umfeld zu beobachten, um auf relevante Veränderungen unverzüglich reagieren zu können.

Auch bei sich verändernden technologischen Rahmenbedingungen sind die Gewährleistung der Grundsätze der Integrität und der Vertraulichkeit gemäß Art. 5 Abs. 1 lit. f DS-GVO weiterhin sicherzustellen. Technologische Veränderungen betreffen häufig die Art und Weise, wie personenbezogene Daten verarbeitet werden, was dazu führen kann, dass eine angemessene Sicherheit der Verarbeitung personenbezogener Daten nicht mehr gewährleistet ist. Um die Vorgabe aus Art. 32 Abs. 1 DS-GVO, ein angemessenes Schutzniveau zu gewährleisten, erfüllen zu können, müssen Verantwortliche daher insbesondere gemäß Art. 32 Abs. 1 lit. d DS-GVO regelmäßig bewerten, überprüfen und evaluieren, ob die von ihnen umgesetzten Maßnahmen hierfür geeignet sind. Dies betrifft vor allem Risiken durch eine unbefugte oder unrechtmäßige Verarbeitung und durch unbeabsichtigten Verlust, unbeabsichtigte Zerstörung oder unbeabsichtigte Schädigung der personenbezogenen Daten infolge der technologischen Veränderung.

Um die Einhaltung dieses und anderer Grundsätze der Verarbeitung gemäß Art. 25 DS-GVO dauerhaft zu gewährleisten, müssen Verantwortliche gemäß Art. 25 Abs. 1 DS-GVO den Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des mit der Verarbeitung verbundenen Risikos für die Rechte und Freiheiten natürlicher Personen berücksichtigen. Davon ausgehend müssen sie im Sinne eines Datenschutzes durch Systemgestaltung und durch datenschutzfreundliche Voreinstellungen angemessene und geeignete Mittel zur Datenverarbeitung sowie technische und organisatorische Maßnahmen festlegen, um ein dem Risiko angemessenes Schutzniveau sicherzustellen.

Durch die vorherrschende Rolle, die das Internet zur Vernetzung unterschiedlichster Lebensbereiche in unser aller Alltag heute spielt, kommt der Übermittlung im Rahmen der Verarbeitung personenbezogener Daten eine besondere Rolle zu. Häufig finden Verarbeitungsvorgänge nicht mehr nur innerhalb einer isolierten und vom Verantwortlichen vollständig kontrollierten technischen Umgebung statt. Stattdessen beinhalten sie auch eine Übermittlung an eine oder mehrere weitere IT-Systeme, seien es Server, mobile Endgeräte oder netzwerktechnisch angebundene Alltagsgegenstände („Internet of Things“). Im Rahmen der zunehmenden Vernetzung unter Zuhilfenahme von Internet-Protokollen oder auch der Digitalisierung vormals analoger Technologien werden die übermittelten Datenpakete über eine Vielzahl von Verbindungen zwischen mehreren vermittelnden Punkten zwischen den beteiligten Endstellen übertragen. Die genutzten Verbindungen und Punkte sind dabei – im Gegensatz zur früheren Leitungsvermittlung – nicht für die beiden Endstellen reserviert. Daher ist es denkbar, dass die beteiligten IT-Systeme weltweit verteilt sind und von verschiedenen staatlichen oder privaten Akteuren betrieben werden. Diese Akteure haben hierbei grundsätzlich die Möglichkeit, auf die von ihnen vermittelten Pakete Zugriff zu nehmen. Dies wird insbesondere dann problematisch, wenn die beiden Endstellen die von ihnen versandten Pakete nicht verschlüsseln.

Ein Verantwortlicher muss seine oben dargestellten Pflichten jederzeit bei der Verarbeitung personenbezogener Daten erfüllen können. Mit Blick auf seine Pflichten zur Gewährleistung der Sicherheit der Verarbeitung muss gemäß Art. 32 Abs. 1 DS-GVO unter anderem der Stand der Technik Berücksichtigung finden. Hierbei muss stets auch berücksichtigt werden, welche datenschutzrechtskonformen Alternativen zur Ablösung einer veralteten und nicht mehr datenschutzrechtskonformen Technologie zur Verfügung stehen. Die Vergleichbarkeit alternativer Technologien orientiert sich dabei ganz wesentlich an den Anwendungsszenarien der jeweiligen Verarbeitungstätigkeit, für welche die Technologien potenziell zum Einsatz kommen sollen. Beispielsweise

wäre ein asynchrones Kommunikationsmedium (wie z. B. E-Mail) nicht ohne weiteres als Ersatz für ein Medium zur synchronen Kommunikation (wie z. B. das Telefon) geeignet, da es nicht in den gleichen Anwendungskontexten zum Einsatz kommt. Ebenso kann die Eignung verschiedener Technologien je nach betrachtetem Lebensbereich abweichen und etwa eine rechtssichere Kommunikation mit Behörden andere Eigenschaften erfordern als die alltägliche Kommunikation zwischen Bürgerinnen und Bürgern. Der Faktor der Nutzerfreundlichkeit einer Technologie darf allerdings nicht gegenüber der Möglichkeit zur Gewährleistung des erforderlichen Schutzniveaus der jeweils verarbeiteten personenbezogenen Daten in den Vordergrund treten.

Im Ergebnis erfordert dies ein stufenweises Vorgehen bei der Ablösung nicht mehr datenschutzrechtskonformer Technologien. Verantwortliche sollten also

1. identifizieren, welche von ihnen eingesetzten Technologien dazu führen, dass bestimmte Verarbeitungstätigkeiten nicht länger datenschutzrechtskonform umgesetzt werden können,
2. ermitteln, welche datenschutzrechtskonformen Alternativen für diese existieren –gegebenenfalls unter Berücksichtigung mehrerer verschiedener Alternativen für unterschiedliche Teilbereiche – und schließlich
3. die entsprechenden Technologien ersetzen.

Die Ablösung nicht länger datenschutzrechtskonformer Technologien soll dabei in letzter Konsequenz stets vollständig umgesetzt werden, muss jedoch nicht zwingend in einem einzigen Schritt erfolgen. Eine Teilablösung ist unter Berücksichtigung der einzelnen Umstände möglich, wenn Alternativen unter der Berücksichtigung der relevanten funktionalen Eigenschaften ermittelt wurden.

III. Beispiel Fax

Das Fax stellt ein konkretes Beispiel für eine Technologie dar, die vormals auf einer analogen leitungsbasierten Datenübermittlung basierte. Dabei waren Absender und Empfänger – identifiziert durch ihre jeweiligen Faxnummern – die beiden Endstellen, zwischen denen eine analoge Verbindung aufgebaut wurde. Diese Verbindung wurde dann vom einen zum anderen Ende zur Übermittlung der Datenströme genutzt, die das Fax repräsentierten. Die Verbindung war für die beiden Endstellen reserviert und wurde für die Dauer der Kommunikation exklusiv von diesen Endstellen genutzt. Diese Art der Vermittlung und Übertragung war bis einschließlich der Nutzung der ISDN-Technologie üblich.

Heutzutage findet jedoch auch beim Fax die paketvermittelte Datenübermittlung mit den zuvor genannten Risiken ihren Einsatz. Bis 2022 soll darüber

hinaus deutschlandweit die analoge Telefonie und die Nutzungsmöglichkeit von ISDN-Anschlüssen vollständig abgeschaltet werden. Bei der heutzutage überwiegend genutzten paketvermittelten Übertragungsmethode als Fax over IP (FoIP) auf Basis von Standards zur Datenübermittlung über das Internet oder bei der Nutzung von Diensten, die Faxe automatisiert in E-Mails umwandeln, werden die Daten ohne zusätzliche Maßnahmen nicht verschlüsselt und damit ungeschützt übertragen. Durch die Übertragung über mehrere verteilte Zwischenstellen besteht dabei grundsätzlich eine Zugriffsmöglichkeit für unbefugte Dritte. Hinzu kommen prinzipbedingte weitere Risiken bei der Nutzung des Faxes, z. B. eine unbefugte Offenlegung personenbezogener Daten bei einer Fehleingabe der Zielnummer oder beim Ausdruck über öffentliche zugängliche Zielgeräte.

Daher habe ich Verantwortliche darauf hingewiesen, dass die datenschutzrechtlichen Vorgaben es erfordern, die Nutzung des Fax insbesondere vor dem Hintergrund des Schutzbedarfs der personenbezogenen Daten kritisch zu reflektieren. Da das Fax auch von solchen Verantwortlichen genutzt wird, die besondere Kategorien personenbezogener Daten gemäß Art. 9 oder 10 DS-GVO verarbeiten, habe ich klargestellt, dass personenbezogene Daten, die einen besonderen Schutzbedarf aufweisen, grundsätzlich nicht per Fax übertragen werden sollten, wenn keine wirksamen zusätzlichen Schutzmaßnahmen bei den Absendern und Empfängern umgesetzt sind.

Auch alle übrigen Stellen sollten prüfen, ob datenschutzrechtskonforme Alternativen zur Verfügung stehen. Die Digitalisierung, die die Sicherheit des Fax schwächt, ermöglicht aber auch sichere Lösungen der elektronischen Kommunikation. Schon jetzt kommen konkrete digitale Technologien in Frage, wie etwa

- der Versand inhaltsverschlüsselter E-Mail-Nachrichten (PGP oder S/MIME),
- Portallösungen, bei denen die Kommunikationspartner Nachrichten und Inhalte verschlüsselt bereitstellen und abrufen können,
- DE-Mail oder
- bereichsspezifische digitale Kommunikationsdienste, wie etwa die Kommunikation über die Infrastruktur des elektronischen Rechtsverkehrs (EGVP/beA/beN/beBPo) oder die Kommunikation im Medizinwesen (KIM).

Da meine Behörde für Bürgerinnen und Bürger sowie private und öffentliche Stellen über alternative datenschutzrechtskonforme Kommunikationswege erreichbar ist, habe ich meine eigenen Fax-Nummern von allen Web-Seiten und Formatvorlagen in meiner Verantwortlichkeit entfernt.

19. Arbeitsstatistik Datenschutz

19.1
Zahlen und Fakten

Die statistische Auswertung der Arbeitsmengen unter dieser Ziffer entspricht den formalen Anforderungen, die die Datenschutzkonferenz vorgibt, um eine bundeseinheitliche Aussage treffen zu können. Diese Werte werden u. a. der Europäischen Kommission und dem Europäischen Datenschutzausschuss gemäß Art. 59 DS-GVO vorgelegt.

Zahlen und Fakten	Fallzahlen 01.01.2020 bis 31.12.2020	Fallzahlen 01.01.2021 bis 31.12.2021
a. „Beschwerden“ Anzahl von Beschwerden, die im Berichtszeitraum nach DS-GVO eingegangen sind. Als Beschwerden werden bei Eingang solche Vorgänge gezählt, die schriftlich eingehen und bei der eine natürliche Person eine persönliche Betroffenheit darlegt, auf die Art. 77 DS-GVO anwendbar ist. Dies schließt Abgaben ein. Telefonische Beschwerden werden nur dann gezählt, wenn sie verschriftlicht werden (z. B. durch Vermerk).	5.414 (davon 855 Abgaben)	**5.179** (davon 953 Abgaben)
b. „Beratungen“ Anzahl von schriftlichen Beratungen. Dies umfasst summarisch Beratungen von Verantwortlichen, betroffenen Personen und der eigenen Regierung. **Nicht:** (Fern-)mündliche Beratungen, Schulungen, Vorträge etc.	1.983	**2.123**
c. „Meldungen von Datenschutzverletzungen“ Anzahl schriftlicher Meldungen	1.433	**2.016**
d. „Abhilfemaßnahmen“ Anzahl der getroffenen Maßnahmen, die im Berichtszeitraum getroffen wurden.		
(1) nach Art. 58 Abs. 2 a (Warnungen)	(1) 1	(1) **1**
(2) nach Art. 58 Abs. 2 b (Verwarnungen)	(2) 31	(2) **28**
(3) nach Art. 58 Abs. 2 c-g und j (Anweisungen und Anordnungen)	(3) 13	(3) **3**
(4) nach Art. 58 Abs. 2 i (Geldbußen)	(4) 2	(4) **29**
(5) nach Art. 58 Abs. 2 h (Widerruf von Zertifizierungen)	(5) 0	(5) **0**

e. „Europäische Verfahren“		
(1) Anzahl der Verfahren mit Betroffenheit (Art.56)	(1) 198	(1) **47**
(2) Anzahl der Verfahren mit Federführung (Art. 56)	(2) 5	(2) **16**
(3) Anzahl der Verfahren gemäß Kap. VII DS-GVO (Art. 60 ff.)	(3) 724	(3) **1011**
f. „Förmliche Begleitung bei Rechtsetzungsvorhaben“		
Hier werden pauschaliert als Gesamtzahl die von Parlament/ Regierung angeforderten und durchgeführten Beratungen genannt. Dies umfasst auch die Teilnahme in öffentlichen Ausschüssen und Stellungnahmen ggü. Gerichten	54	**34**

19.2
Ergänzende Erläuterungen zu Zahlen und Fakten

Die nachstehenden Darstellungen erläutern und ergänzen die Auswertungen zu Ziff. 19.1 auch im Vergleich mit dem Vorjahr und den weiteren Arbeitsgebieten im Berichtsjahr. Insgesamt stabilisiert sich die Zahl der Fälle in meiner Behörde sechs Jahre nach dem Inkrafttreten und vier Jahre nach dem Wirksamwerden der DS-GVO auf einem sehr hohen Niveau. Dabei lässt sich beobachten, dass sich in vielen Bereichen die Qualität der Beschwerden und des Beratungsbedarfes verändert. Während zu Beginn Fragen nach eher formalen Anforderungen der DS-GVO im Vordergrund standen (etwa nach der Pflicht zur Bestellung eines Datenschutzbeauftragten, zu Informations- und Auskunftsrechten des Betroffenen), gehen viele Fragen, mit denen ich mich im Berichtsjahr zu befassen hatte, mehr in die Tiefe und werfen grundsätzliche Fragen auf.

Beschwerden und Beratungen

Auch in diesem Jahr war die datenschutzrechtliche Umsetzung der sich immer wieder ändernden Vorgaben der Corona-Verordnungen durch die Verantwortlichen über das gesamte Jahr hinweg präsent. Allerdings brachte der durch die Pandemie ausgelöste Digitalisierungsschub auch über die Pandemie hinaus ganz grundsätzlichen Beratungsbedarf mit sich. So zeichnete sich im Berichtsjahr ab, dass technische Lösungen wie etwa Videokonferenztechnik, die in der Pandemie schnell zum Einsatz gebracht wurde, um Schulen, Hochschulen, Betriebe und die Verwaltung am Laufen zu halten, auch über die Pandemie hinaus zum Einsatz kommen soll. Da bei der Einführung Eile geboten war, müssen nun im Nachhinein die Anforderungen des Datenschutzes zur Geltung gebracht werden. Auch andere große Digitalisierungsprojekte, wie zum Beispiel die Umsetzung des Onlinezugangsgesetzes, das Bund, Länder und Kommunen verpflichtet, bis 2022 ihre Verwaltungsleistungen

über Verwaltungsportale auch online anzubieten, schlagen in der Statistik nicht in dem Ausmaß zu Buche, wie sie den HBDI tatsächlich beschäftigen.

Die mittlerweile fast allen Webseiten vorgeschalteten Cookie-Banner werfen viele Fragen auf und sorgen für einen deutlichen Anstieg der Fallzahlen im Bereich Internet.

In fast allen Bereichen, in denen ich tätig bin, spielt auch weiterhin die Frage nach den Anforderungen an DS-GVO-konforme internationale Datentransfers eine große Rolle.

Deutlich zurückgegangen sind die Zahlen im Bereich Auskunfteien und Inkasso. Bei näherer Betrachtung ist allerdings zu beobachten, dass hier vor allem die Zahl der Beschwerden zurückgeht, die sich auf die Auskunftserteilung beziehen und in der Bearbeitung im Gegensatz zu Fällen, bei denen es um die Speicherung von Negativmerkmalen oder Inkasso geht, meist einfacher zu bearbeiten sind.

Schließlich ist im Vergleich zum außergewöhnlich hohen Aufkommen an telefonischen Anfragen die Zahl im Berichtsjahr wieder auf das normale Maß zurückgegangen.

Die nachfolgende Übersicht stellt die Mengen der Eingabe (Beschwerden und Beratungen) des Berichtsjahres im Vergleich zum Vorjahr dar:

Fachgebiete	Anzahl 2020			Anzahl 2021		
	Beschwerden	Beratungen	Eingaben insgesamt	Beschwerden	Beratungen	Eingaben insgesamt
Auskunfteien, Inkasso	1.201	19	1.220	634	11	**645**
Schule, Hochschule, Archive	191	545	736	132	811	**943**
e-Kommunikation, Internet	565	53	618	772	56	**828**
Beschäftigtendatenschutz	263	170	433	255	208	**463**
Videobeobachtung	317	90	407	413	74	**487**
Kreditwirtschaft	323	15	338	314	9	**323**
Handel, Handwerk, Gewerbe	264	74	338	212	53	**265**
Verkehr, Geodaten, Landwirtschaft	238	47	285	220	49	**269**

Gesundheit, Pflege	201	86	287	286	160	**446**
Betriebliche/ Behördliche DSB	17	258	275	7	180	**187**
Kommunen, Wahlen	137	115	252	142	146	**288**
Polizei, Justiz, Verfassungsschutz	201	73	274	141	90	**231**
Vereine, Verbände	80	119	199	72	73	**145**
Adresshandel, Werbung	169	4	173	197	5	**202**
Wohnen, Miete	65	59	124	77	48	**125**
Soziales	63	56	119	85	52	**137**
Versorgungs unternehmen	91	17	108	79	10	**89**
IT-Sicherheit, DV-Technik**	3	91	94	11	32	**43**
Versicherungen	52	29	81	94	12	**106**
Rundfunk, Fernsehen, Presse	57	0	57	25	2	**27**
Religionsgemeinschaften	20	3	23	2	3	**5**
Datenschutz außerhalb der EU	11	29	40	8	19	**27**
Forschung, Statistik	10	1	11	17	5	**21**
Ausländerrecht	s. Sonstiges	s. Sonstiges	s. Sonstiges	3	7	**10**
Steuerwesen	s. Sonstiges	s. Sonstiges	s. Sonstiges	14	3	**17**
Zertifizierung					1	**1**
Sonstige Themen < 10 (z. B. Kammern, Ausländerwesen, Finanzwesen)	20	6	26	14	4	**18**
Zwischensumme Beschwerden und Beratungen	**4.559**	**1.959**	**6.518**	**4.226**	**2.123**	**6.348**

BCR-Verfahren mit deutscher oder europaweiter Federführung des HBDI	**40**	**40**
Meldungen von Datenpannen*	**1.433**	**2.016**

Gesamtsumme dokumentierter Eingaben	**7.991**	**8.404**
Zzgl. Summe telefonischer Beratungen und Auskünfte von mehr als 10 Min.**	**9.444**	**6.384**
Gesamtsumme dokumentierter + telefonischer Eingaben	**17.435**	**14.789**

*Telefonischen Nachfragen, die keinen schriftlichen Niederschlag finden, werden pauschaliert erfasst. Sie erfolgten als Beratungen, Auskünfte, Erläuterungen und Verständnisfragen zur DS-GVO u. Ä. sowohl zu allgemeinen Themen als auch zu spezifischen Fragestellungen, wie z. B. zur konkreten datenschutzrechtlichen Umsetzung der Corona-Verordnungen. Exemplarisch werden derartige Telefonate im November, als Monat ohne besondere Vorkommnisse, gezählt und als Durchschnittswert hochgerechnet.

**Weitere IT-Themen waren begleitend zu einer rechtlichen Anfrage oder einer Datenpannenmeldung zu prüfen und wurden deshalb nicht eigenständig gezählt.

Unberücksichtigt in den obigen Tabellen, aber nicht weniger erwähnenswerte Aufgaben und Themen, die im Berichtsjahr bearbeitet wurden, sind beispielsweise:

– **Tätigkeiten der internen Datenschutzbeauftragten beim HBDI**

  Es wurden **38** Auskunftsersuchen von Bürgerinnen und Bürgern zur Verarbeitung ihrer Daten beim HBDI bearbeitet sowie **11** entsprechende Beratungen durchgeführt.

– **Regelmäßige Beratungen**

  Mit den intern bestellten Datenschutzbeauftragten aus verschiedenen öffentlichen Bereichen (z. B. von Ministerien, Städten und Kommunen und den europäischen Datenschutz-Aufsichtsbehörden) wurden Austausche gepflegt und z. T. regelmäßige Beratungsleistungen erbracht.

– **Presse und Öffentlichkeitsarbeit**

  Im Jahr 2021 erhielt ich **95** Presseanfragen. Zahlreiche Veröffentlichungen und Hilfestellungen wurden Verantwortlichen, Bürgerinnen und Bürgern auf meiner Homepage (z. B. zum Thema Videokonferenztechnik) zur Verfügung gestellt.

– **Ausbildungsleistungen**

  Es wurden Referendare und Referendarinnen in ihren Wahl- bzw. Verwaltungsstationen ausgebildet.

– **Fortbildung und Vorträge**

  Es wurden **29**, zum Teil mehrtägige datenschutzrechtliche Schulungen, Seminare und Fortbildungen im öffentlichen und nichtöffentlichen Bereich durchgeführt.

– **Teilnahme an Konferenzen, Arbeitskreisen und Arbeitsgruppen**

  Beratungen und Abstimmungen der Aufsichtsbehörden untereinander und in ihren Gremien auf Landes-, Bundes- und EU-Ebene, aber auch übergreifend mit Ansprechpartnern aus außereuropäischen Drittstaaten, sind mittlerweile essenziell für einen erfolgreichen Datenschutz in Hessen. Die Gremienarbeit ist mitunter sehr zeitintensiv, aber nicht mehr verzichtbar. Aufgrund der pandemischen Entwicklungen wurden persönliche Treffen oft durch Videokonferenzen ersetzt. Die Konferenzen der Datenschutzbeauftragten (DSK) und der Informationsfreiheitsbeauftragten (IFK) tagten ca. alle zwei Monate zu aktuellen Themen. Die Ergebnisse des Jahres 2021 sind im Anhang zu I und Anhang zu II auszugsweise abgedruckt, im Einzelnen aber auch auf der Homepage der Datenschutzkonferenz www.datenschutzkonferenz.de nachzulesen.

  In den Arbeitskreisen der DSK bin ich in allen Bereichen beteiligt. Auch in den Unterarbeitsgruppen, die zu Spezialthemen eingesetzt werden, engagieren sich Mitarbeiterinnen und Mitarbeiter. In zahlreiche EU-

Gremien (z. B. International Transfers Expert Subgroup, Border, Travel, Law Enforcement Expert Subgroup, Financial Matters Expert Subgroup, CSC, SCG SIS II, SCG Eurodac, SCG VIS) konnten sie ihre Mitarbeit einbringen. Daneben erfolgten auch Unterstützungsleistungen an die EU-Kommission, wie z. B. durch die Teilnahme und Beiträge im Rahmen der Schengen-Evaluierung.

Abhilfemaßnahmen und Gerichtsverfahren

Abhilfemaßnahmen	**Anzahl 2020**	**Anzahl 2021**
(1) Warnungen (Art. 58 Abs. 2 a DS-GVO)	1	1
(2) Verwarnungen (Art. 58 Abs. 2 b DS-GVO)	31	28
(3) Anweisungen und Anordnungen (Art. 58 Abs. 2 c-g, j DS-GVO)	13	3
(4) Geldbußen (Art. 58 Abs. 2 i DS-GVO)	2	29
(5) Widerruf von Zertifizierungen (Art. 58 Abs. 2 h DS-GVO)	0	0
Gesamt	**47**	**61**

Gerichtsverfahren	**Anzahl 2020**	**Anzahl 2021**
Klagen gemäß Art. 78 Abs. 1 DS-GVO	19	24
Klagen gemäß Art. 78 Abs. 2 DS-GVO	2	2
Sonstige	4	8*
Gesamt	**25**	**34**

* Davon zwei Vorlageverfahren vor dem EuGH und 2 Verfahren vor dem VGH in 2. Instanz.

Meldungen von Datenschutzverletzungen

Meldungen nach Art. 33 DS-GVO und § 60 HDSIG

Gesamtübersicht		
Grund	**Anzahl 2020**	**Anzahl 2021**
Fehlversand	494	628
Hackerangriffe, Phishing, Schadsoftware	184	579
Verlust/ Diebstahl von Unterlagen, Datenträgern etc.	142	144
Unrechtmäßige Offenlegung/Weitergabe von Daten	107	121
Unzulässige Einsichtnahme (fehlerhafte Einrichtung von Zugriffsrechten u. a.)	85	98
Offener E-Mail-Verteiler	76	73
Missbrauch von Zugriffsrechten	43	44
Unzulässige Veröffentlichung	25	38
Fehlerhafte Zuordnung von Daten	21	19
Nicht datenschutzkonforme Entsorgung	9	12
Unverschlüsselter E-Mail-Versand	7	7
Sonstige	240	253
Gesamt	**1.433**	**2.016**

am stärksten betroffene Bereiche	**Fälle 2020**	**Fälle 2021**
Kreditwirtschaft, Auskunfteien, Handel und Gewerbe	491	640
Beschäftigtendatenschutz	254	399
Gesundheitsbereich	230	288

Anhang zu I

1. Ausgewählte Entschließungen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

„Chancen der Corona-Warn-App 2.0 nutzen“ vom 29. April 2021

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) erinnert angesichts der bereits seit mehr als einem Jahr andauernden Pandemie und der damit auch im Bereich des Datenschutzes einhergehenden Grundrechtseingriffe an das grundlegende rechtsstaatliche Erfordernis, diese Eingriffe fortlaufend kritisch zu bewerten und zu evaluieren. Die DSK bittet im Zuge einer solchen Evaluation und Anpassung infektionsschutzrechtlicher Instrumente durch Bund und Länder, die mit der Version 2.0 der Corona-Warn-App (CWA) eröffneten datensparsameren Möglichkeiten der pseudonymisierten Clustererkennung und Kontaktbenachrichtigung eingehend und zeitnah zu prüfen.

Die DSK empfiehlt den Ländern, die Nutzung der CWA jedenfalls als ergänzende Möglichkeit zur Benachrichtigung potenziell infizierter Personen und zur Clustererkennung in ihren Konzepten zur Pandemiebekämpfung zu berücksichtigen.

Seit dem Update auf die Version 2.0 verfügt die CWA über eine entsprechende Funktion, die genutzt werden kann, um sich an Orten oder Veranstaltungen, wo viele Menschen zusammenkommen, zu registrieren. Auch wenn hierbei – anders als bei anderen Apps – keine personenbezogenen Daten erhoben und später an ein Gesundheitsamt übermittelt werden können, kann die pseudonymisierte Clustererkennung der CWA einen erheblichen Beitrag zur Unterbrechung von Infektionsketten leisten.

Durch die unmittelbare Vernetzung der CWA-Nutzenden werden Personen, die einem potenziellen Infektionsrisiko ausgesetzt waren, unmittelbar und somit schneller als über die Gesundheitsämter informiert. Zudem ist aufgrund der hohen Akzeptanz der CWA mit mittlerweile über 27 Millionen Downloads die Wahrscheinlichkeit hoch, dass Personen auf diese Möglichkeit der aus datenschutzrechtlicher Sicht zu bevorzugenden pseudonymen digitalen Registrierung zurückgreifen.

Die Förderung der Nutzung der CWA zur Clustererkennung könnte dazu führen, dass die App von noch mehr Personen genutzt werden würde. Dies wiederum würde auch die Chance der Erkennung und Warnung vor Risikobegegnungen außerhalb der Nutzung der Clustererkennung weiter erhöhen und damit aktiv zur Pandemiebekämpfung beitragen.

2. Ausgewählte Beschlüsse der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

2.1
„Energieversorgerpool“ darf nicht zu gläsernen Verbraucher*innen führen“ vom 15. März 2021

Bei Auskunfteien und Energieversorgern gibt es Überlegungen, einen sog. Energieversorgerpool zu schaffen. In diesem zentralen Datenpool sollen auch Positivdaten der Kund*innen gespeichert und an andere Energieversorger übermittelt werden. Positivdaten sind Daten über Verträge, bei denen die Belieferten keinen Anlass zu Beanstandungen geben, sich also vertragskonform verhalten.

Informationen über die Anzahl abgeschlossener Verträge und die jeweilige Vertragsdauer können Hinweise darauf geben, ob Verbraucher*innen eine längere Vertragsbeziehung zu einem Stromversorger beabsichtigen oder etwa regelmäßig Angebote für Neukund*innen nutzen. Verbraucher*innen, die regelmäßig das für Sie kostengünstigste Angebot am Markt wählen und dazu den Anbieter wechseln möchten, könnten dann von Versorgungsunternehmen bei preislich attraktiven Angeboten ausgeschlossen werden.

Jede Bürgerin und jeder Bürger hat jedoch das Recht, den Wettbewerb zwischen den Energieversorgern zu nutzen und am Markt nach günstigen Angeboten zu suchen. Der Wunsch, vermeintliche „Schnäppchenjäger“ in einem zentralen Datenpool zu erfassen, um sie bei Vertragsanbahnung als solche identifizieren und ggf. von Angeboten ausschließen zu können, stellt kein berechtigtes Interesse i. S. d. Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO dar. Es war gerade das Ziel des Gesetzgebers, durch die Liberalisierung des Energiemarktes einen wirksamen und unverfälschten Wettbewerb bei der Versorgung mit Elektrizität und Gas zu ermöglichen. Der Versuch, preisbewusste und wechselfreudige Verbraucher*innen zu identifizieren und sie ggf. von bestimmten Angeboten auszuschließen, liefe dieser Zielsetzung zuwider.

Selbst wenn die Interessen der Unternehmen als berechtigt angesehen würden, überwiegen in derartigen Fällen die schutzwürdigen Interessen und Grundrechte der Kund*innen. Vertragstreue Verbraucher*innen dürfen zu Recht erwarten, dass keine über den Vertragszweck hinausgehende Verarbeitung ihrer Daten erfolgt, die ggf. ihre Möglichkeiten einschränkt, frei am Markt agieren zu können.

Die Speicherung und Übermittlung von Positivdaten durch einen Energieversorgerpool würde erheblich zu gläsernen Verbraucher*innen beitragen und wäre nach Art. 6 Absatz 1 Satz 1 lit. f) DS-GVO rechtswidrig.

2.2
„Verarbeitung von Positivdaten von Privatpersonen aus Verträgen über Mobilfunkdienste und Dauerhandelskonten durch Auskunfteien“ vom 22. September 2021

Die DSK beschließt Folgendes:

Nach erneuter Prüfung der Rechtslage wird der Beschluss der DSK vom 11.06.2018 aufrechterhalten, so dass weiterhin

1. die Übermittlung und Verarbeitung von sog. Positivdaten an bzw. durch Handels- und Wirtschaftsauskunfteien grundsätzlich nicht auf Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO gestützt werden kann und
2. es für eine Übermittlung und Verarbeitung von sog. Positivdaten regelmäßig einer wirksamen Einwilligung der betroffenen Person unter Beachtung der hohen Anforderungen an die Freiwilligkeit bedarf.

Begründung:

Die DSK hat mit Beschluss vom 11. Juni 2018 festgestellt, dass Handels- und Wirtschaftsauskunfteien sog. Positivdaten zu Privatpersonen grundsätzlich nicht auf Grundlage des Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO erheben können. Dabei sind Positivdaten 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. Bei solchen Positivdaten überwiegt regelmäßig das schutzwürdige Interesse der betroffenen Personen, selbst über die Verwendung ihrer Daten zu bestimmen. Werden die Daten von einem Verantwortlichen an eine Auskunftei übermittelt, ist insoweit bereits die Übermittlung dieser Daten nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO regelmäßig unzulässig. Ebenso unzulässig ist die Verarbeitung dieser Daten durch die Auskunftei.

Die DSK hatte nun zu überprüfen, ob für die verbreitete Praxis der Übermittlung und Verarbeitung von Positivdaten zu Verträgen über Mobilfunkdienste und Dauerhandelskonten von Privatpersonen eine andere Bewertung erforderlich ist. Diese Praxis betrifft längerfristige Verträge, die durch Vorausleistungsverpflichtungen oder Finanzierungs- bzw. Stundungselemente als kreditorische Risiken betrachtet werden, aber keine Vertragsstörungen aufweisen. Sie werden bei der Bildung von Scorewerten der betroffenen Personen, die Handel oder Kreditwirtschaft zur Bonitätsprüfung heranziehen, regelmäßig neben einer Vielzahl weiterer Sachverhalte einbezogen.

Im Rahmen dieser Überprüfung hatten Unternehmen und Verbände bis zum 31. August 2021 Gelegenheit, Stellungnahmen zu den aufgeworfenen Rechtsfragen abzugeben. Nach sorgfältiger Auswertung der eingegan-

genen Stellungnahmen kommt die DSK zu dem Ergebnis, dass für die Übermittlung der Positivdaten durch die Mobilfunkdiensteanbieter und die Handelsunternehmen zwar berechtigte Interessen bestehen, die Qualität der Bonitätsbewertungen zu verbessern und die beteiligten Wirtschaftsakteure vor kreditorischen Risiken zu schützen. Besondere Umstände, die – wie bei Kreditinstituten insbesondere auf Grund ihrer spezifischen Verpflichtungen nach dem Kreditwesengesetz – entsprechend dem Beschluss der DSK vom 11.06.2018 regelmäßig ein die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person überwiegendes Interesse der Verantwortlichen oder Dritter an der Verarbeitung bestimmter Positivdaten vermitteln würden, konnte die DSK im Rahmen ihrer Überprüfung jedoch nicht feststellen. Eine von der oben genannten Grundregel abweichende Bewertung ist daher nicht begründbar: Auch bei Positivdaten zu Verträgen über Mobilfunkdienste und Dauerhandelskonten kommt den Interessen, Grundrechten und Grundfreiheiten der betroffenen Person, selbst darüber zu bestimmen, ob sie die sie betreffenden Positivdaten für eine Übermittlung durch Mobilfunkdienstleister und Handelsunternehmen und eine Verarbeitung durch Auskunfteien zur Bonitätsbewertung preisgeben will, entscheidende Bedeutung zu. Hierbei fällt besonders ins Gewicht, dass ansonsten unterschiedslos große Datenmengen über übliche Alltagsvorgänge im Wirtschaftsleben erhoben und verarbeitet würden, ohne dass die betroffenen Personen hierzu Anlass gegeben haben. Deshalb können weder Verantwortliche noch Dritte ein überwiegendes Interesse an diesen Verarbeitungen geltend machen.

Eine gegen den Willen der betroffenen Person stattfindende Datenverarbeitung von Positivdaten über Mobilfunkdienstverträge und Dauerhandelskonten durch Vertragspartner und Auskunfteien ist daher unbeschadet anderweitiger Anforderungen nicht nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO gerechtfertigt. Ihre datenschutzkonforme Übermittlung und Verarbeitung ist nur auf der Grundlage einer Einwilligung der betroffenen Person zulässig, für die die allgemeinen Anforderungen gewahrt werden müssen. Insbesondere darf die Erteilung der Einwilligung in die Speicherung des Positivdatums nicht zur Bedingung des betroffenen Vertragsabschlusses gemacht werden.

2.3
„Verarbeitungen des Datums ‚Impfstatus' von Beschäftigten durch die Arbeitgeberin oder den Arbeitgeber" vom 19. Oktober 2021

Arbeitgeberinnen und Arbeitgeber dürfen das Datum „Impfstatus" ihrer Beschäftigten ohne eine ausdrückliche gesetzliche Ermächtigung grundsätzlich nicht verarbeiten – auch nicht im Rahmen der COVID-19-Pandemie.

Als Rechtsgrundlage kommt für die Verarbeitung des Datums „Impfstatus“ von Beschäftigten § 26 Absatz 3 Satz 1 des Bundesdatenschutzgesetzes (BDSG) nicht zum Tragen.

Bei dem Datum „Impfstatus“ handelt es sich um ein Gesundheitsdatum gemäß Artikel 4 Nummer 15 Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DS-GVO) und damit um eine besondere Kategorie personenbezogener Daten, Artikel 9 Absatz 1 DS-GVO. Deren Verarbeitung ist grundsätzlich verboten und nur ausnahmsweise erlaubt.

In Einzelfällen ist eine Verarbeitung des Datums „Impfstatus“ auf Grundlage gesetzlicher Regelungen möglich:

– Bestimmte – im Gesetz genannte – Arbeitgeberinnen und Arbeitgeber aus dem Gesundheitsbereich (Krankenhäuser, Arztpraxen usw.) dürfen unter den in §§ 23a, 23 Absatz 3 des Infektionsschutzgesetzes (IfSG) genannten gesetzlichen Voraussetzungen den Impfstatus ihrer Beschäftigten verarbeiten;
– Bestimmte – im Gesetz genannte – Arbeitgeberinnen und Arbeitgeber, zum Beispiel Trägerinnen und Träger von Kindertageseinrichtungen, ambulante Pflegedienste usw., dürfen unter den in § 36 Absatz 3 IfSG genannten Voraussetzungen den Impfstatus ihrer Beschäftigten im Zusammenhang mit COVID-19 verarbeiten;
– Arbeitgeberinnen und Arbeitgeber dürfen den Impfstatus derjenigen Beschäftigten verarbeiten, die ihnen gegenüber einen Anspruch auf Geldentschädigung (Lohnersatz) nach § 56 Absatz 1 IfSG geltend machen. Dessen Voraussetzungen können im Einzelfall auch im Fall einer möglichen Infektion mit COVID-19 sowie einer sich anschließenden Quarantäne vorliegen. Anspruchsvoraussetzung ist unter anderem, ob die Möglichkeit einer Schutzimpfung bestand.
– Arbeitgeberinnen und Arbeitgeber dürfen den Impfstatus von Beschäftigten auch verarbeiten, soweit dies durch Rechtsverordnungen zur Pandemiebekämpfung auf Basis des IfSG vorgegeben ist.

Die Verarbeitung des Datums „Impfstatus“ von Beschäftigten auf der Grundlage von Einwilligungen ist nur dann möglich, wenn die Einwilligung freiwillig und damit rechtswirksam erteilt worden ist, § 26 Absatz 3 Satz 2 und Absatz 2 BDSG. Aufgrund des zwischen Arbeitgeberinnen und Arbeitgebern sowie ihren Beschäftigten bestehenden Über- und Unterordnungsverhältnisses bestehen regelmäßig Zweifel an der Freiwilligkeit und damit Rechtswirksamkeit der Einwilligung von Beschäftigten.

Im Zusammenhang mit der Abfrage des Datums „Impfstatus“ sind weiter zu beachten:

– Grundsatz der „Datenminimierung“, Artikel 5 Absatz 1 Buchstabe c DS-GVO:
  Zunächst muss geprüft werden, ob die reine Abfrage des Impfstatus zur Zweckerreichung bereits ausreichend ist. Dann ist keine Speicherung erforderlich. Soll der Impfstatus gespeichert werden, dürfen keine Kopien von Impfausweisen oder vergleichbaren Bescheinigungen (im Original oder als Kopie) in die Personalakte aufgenommen werden. Es ist ausreichend, wenn vermerkt wird, dass diese jeweils vorgelegt worden sind.
– Grundsatz der „Speicherbegrenzung“, Artikel 5 Absatz 1 Buchstabe e DS-GVO, Recht auf Löschung, Artikel 17 DS-GVO:
  Sobald der Zweck für die Speicherung des Impfstatus entfallen ist, muss dieses personenbezogene Datum gelöscht werden.
– Grundsatz der „Rechenschaftspflicht“, Artikel 5 Absatz 2 DS-GVO:
  Arbeitgeberinnen und Arbeitgeber müssen – sofern einschlägig – auch die Freiwilligkeit einer Einwilligung nachweisen können, Artikel 7 Absatz 1 DS-GVO.

2.4
Zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO auf ausdrücklichen Wunsch betroffener Personen“[1] vom 24. November 2021

1. Die vom Verantwortlichen nach Art. 32 DSGVO vorzuhaltenden technischen und organisatorischen Maßnahmen beruhen auf objektiven Rechtspflichten, die nicht zur Disposition der Beteiligten stehen.
2. Ein Verzicht auf die vom Verantwortlichen vorzuhaltenden technischen und organisatorischen Maßnahmen oder die Absenkung des gesetzlich vorgeschriebenen Standards auf der Basis einer Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO ist nicht zulässig.
3. Unter Beachtung des Selbstbestimmungsrechts der betroffenen Person und der Rechte weiterer betroffener Personen kann es in zu dokumentierenden Einzelfällen möglich sein, dass der Verantwortliche auf ausdrücklichen, eigeninitiativen Wunsch der informierten betroffenen Person bestimmte vorzuhaltende technische und organisatorische Maßnahmen ihr gegenüber in vertretbarem Umfang nicht anwendet.
4. Kapitel V der DSGVO (Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen) bleibt hiervon unberührt.

1 Der Beschluss wurde durch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder gegen die Stimme Sachsens beschlossen.

3. Ausgewählte Orientierungshilfen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail[1] (Stand 16. Juni 2021)

1. Zielstellung

Die vorliegende Orientierungshilfe zeigt auf, welche Anforderungen an die Verfahren zum Versand und zur Entgegennahme von E-Mail-Nachrichten durch Verantwortliche, ihre Auftragsverarbeiter und öffentliche E-Mail-Diensteanbieter[2] auf dem Transportweg zu erfüllen sind. Diese Anforderungen richten sich nach den Vorgaben der Art. 5 Abs. 1 lit. f, 25 und 32 Abs. 1 DS-GVO. Die Orientierungshilfe nimmt den Stand der Technik zum Veröffentlichungszeitpunkt als Ausgangspunkt für die Konkretisierung der Anforderungen.

Verantwortliche und Auftragsverarbeiter[3] sind gesetzlich gehalten, die Risiken, die sich aus ihren Verarbeitungen personenbezogener Daten ergeben, hinreichend zu mindern. Sie müssen hierbei Art, Umfang, Umstände und Zwecke ihrer Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen berücksichtigen. Diese Orientierungshilfe behandelt ausschließlich die Risiken, die mit einer Verletzung von Vertraulichkeit und Integrität personenbezogener Daten verbunden sind. Sie setzt voraus, dass die Verantwortlichen bzw. ihre Auftragsverarbeiter einschätzen, welche Schäden aus einem Bruch von Vertraulichkeit und Integrität resultieren können.

Die Orientierungshilfe geht von typischen Verarbeitungssituationen aus. Sie bestimmt hierbei ausgehend vom Stand der Technik, den typischen Implementierungskosten und deren Verhältnis zu den Risiken einer Übermittlung personenbezogener Daten per E-Mail Anforderungen an die Maßnahmen, die Verantwortliche und Auftragsverarbeiter zur ausreichenden Minderung der Risiken zu treffen haben. Die Verantwortlichen und Auftragsverarbeiter sind verpflichtet, die Besonderheiten ihrer Verarbeitungen, darunter insbesondere den Umfang, die Umstände und die Zwecke der vorgesehenen

---

1 Die Orientierungshilfe wurde durch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder gegen die Stimme Bayerns beschlossen.

2 Diensteanbieter, die eigene oder fremde E-Mail-Dienste zur öffentlichen Nutzung bereithalten.

3 Auftragsverarbeiter ausschließlich im Hinblick auf ihre Pflichten nach Art. 32 DS-GVO.

Übermittlungsvorgänge, zu berücksichtigen, die ggf. in abweichenden Anforderungen resultieren können. Dabei müssen sie berücksichtigen, dass die vorliegende Orientierungshilfe ausschließlich Risiken betrachtet, die sich auf dem Transportweg ergeben. Risiken, denen ruhende Daten wie bereits empfangene E-Mails ausgesetzt sind oder die durch eine Weiterverarbeitung wie z. B. automatische Weiterleitungen entstehen, werden in dieser Orientierungshilfe nicht betrachtet und können weitere Maßnahmen oder eine andere Gewichtung der im Folgenden aufgeführten Maßnahmen notwendig machen. Können die Anforderungen an eine sichere Übermittlung per E-Mail nicht erfüllt werden, so muss ein anderer Kommunikationskanal gewählt werden.[4]

2. Anwendungsbereich und Grundsätze

Der gesetzlich gebotene Schutz personenbezogener Daten im Zuge der Übermittlung von E-Mail-Nachrichten erstreckt sich sowohl auf die personenbezogenen Inhalte als auch auf die Umstände der Kommunikation, soweit sich aus letzteren Informationen über natürliche Personen ableiten lassen.[5] Dieser Schutz muss abseits des Blickwinkels dieser Orientierungshilfe ergänzt werden durch Maßnahmen zum Schutz der beteiligten Systeme und zur Minimierung, Speicherbegrenzung und Zweckbindung der auf diesen Servern verarbeiteten Verkehrsdaten.

Bestimmte Personen, wie Rechtsanwältinnen und Rechtsanwälte sowie Ärztinnen und Ärzte haben als Berufsgeheimnisträger besondere Pflichten zur Geheimhaltung ihnen anvertrauter Daten. Sie müssen neben dem Datenschutzrecht zusätzliche Strafvorschriften, z. B. § 203 StGB, und Berufsrecht beachten. Für den Vollzug dieser Vorschriften sind nicht die Datenschutzaufsichtsbehörden, sondern Strafverfolgungsbehörden, andere Behörden oder Kammern für bestimmte Berufsgruppen zuständig.

Dennoch haben Datenschutzaufsichtsbehörden bei der Beurteilung des Risikos einer Verarbeitung personenbezogener Daten zu berücksichtigen, ob die Daten einem Berufsgeheimnis unterliegen. In Erwägungsgrund 75 der DS-GVO heißt es hierzu: „Die Risiken für die Rechte und Freiheiten natürlicher Personen … können aus einer Verarbeitung personenbezogener

4 Für die Kommunikation mit betroffenen natürlichen Personen (z. B. mit Kunden) kann ein Kommunikationsweg in der Bereitstellung eines Webportals bestehen.

5 Informationen über die Umstände der Kommunikation lassen sich verschiedenen Verarbeitungsprozessen entnehmen, die mit Versand und Empfang von E-Mail-Nachrichten in Verbindung stehen (vom Abruf von Angaben aus dem DNS bis zur Protokollierung der Kommunikation auf verschiedenen Geräten). Diese Orientierungshilfe thematisiert lediglich den Schutz der in den Kopfzeilen einer E-Mail-Nachricht enthaltenen Angaben während des Transports der Nachricht.

Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu … einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten … führen kann …“

Wenn Daten einem Berufsgeheimnis unterliegen, ist daher aus datenschutzrechtlicher Sicht stets zu prüfen, ob deren Verarbeitung zu einem hohen Risiko im Sinne der DS-GVO führt. Dies ist insbesondere bei der Auswahl von technischen und organisatorischen Maßnahmen im Sinne des Art. 32 DS-GVO zu berücksichtigen, vgl. Abschnitt 4.2.3.

Datenschutzrechtlich sind die Verantwortlichen verpflichtet, die dort aufgeführten Maßnahmen in dem beschriebenen Umfang und Maß zu treffen.

Die Anforderung, derartige Maßnahmen zu treffen, kann sich ebenso aus Berufsrecht und berufsspezifischem Strafrecht ergeben. Darüber hinaus kann dieses Recht weitergehende Verpflichtungen begründen, die unabhängig vom Datenschutzrecht zu erfüllen wären.

Diese Orientierungshilfe thematisiert den Vertraulichkeitsschutz der personenbezogenen Inhalte der E-Mail-Nachrichten lediglich insoweit, wie diese nicht bereits vorab (z. B. anwendungsspezifisch) gemäß dem Stand der Technik so verschlüsselt wurden, dass nur der Empfänger sie entschlüsseln kann.

Sowohl Ende-zu-Ende-Verschlüsselung als auch Transportverschlüsselung mindern für ihren jeweiligen Anwendungszweck Risiken für die Vertraulichkeit der übertragenen Nachrichten. Daher müssen Verantwortliche beide Verfahren in der Abwägung der notwendigen Maßnahmen berücksichtigen.

Der durchgreifendste Schutz der Vertraulichkeit der Inhaltsdaten wird durch Ende-zu-Ende-Verschlüsselung erreicht, wofür derzeit die Internet-Standards SI/MIME (RFC 5751) und OpenPGP (RFC 4880) i. d. R. in Verbindung mit PO/MIME (RFC 3156) zur Verfügung stehen. Ende-zu-Ende-Verschlüsselung schützt nicht nur den Transportweg, sondern auch ruhende Daten. Bei Ende-zu-Ende-Verschlüsselung kann die Verarbeitung unverschlüsselter Inhaltsdaten auf besonders geschützte Netzsegmente bzw. auf solche Teile des Netzes beschränkt werden, die ausschließlich zur Nutzung durch Befugte (wie eine Personalabteilung oder einen Amtsarzt) vorgesehen sind.

Der Einsatz von Transportverschlüsselung bietet einen Basisschutz und stellt eine Mindestmaßnahme zur Erfüllung der gesetzlichen Anforderungen dar. In Verarbeitungssituationen mit normalen Risiken wird dabei bereits durch die Transportverschlüsselung eine ausreichende Risikominderung erreicht.

Die Transportverschlüsselung reduziert die Erfolgswahrscheinlichkeit passiver Abhörmaßnahmen Dritter auf dem Transportweg auf ein geringfügiges Maß. Um auch gegen Dritte zu bestehen, die aktiv in den Netzverkehr eingreifen,

muss sie in qualifizierter Weise durchgeführt und durch Maßnahmen zur kryptografischen Absicherung der Angaben der Empfänger über die zur Entgegennahme der Nachrichten berechtigten Geräte flankiert werden.

Eine Darstellung der Anforderungen an die einfache und an die qualifizierte obligatorische Transportverschlüsselung sowie an die Ende-zu-Ende-Verschlüsselung und die Signatur von E-Mail-Nachrichten ist in Abschnitt 5 niedergelegt.

3. Die Inanspruchnahme von E-Mail-Diensteanbietern

3.1. Grundlegende technische Anforderungen an die Erbringung von E-Mail-Diensten

Zum Schutz der Vertraulichkeit und Integrität der verarbeiteten personenbezogenen Daten müssen öffentliche E-Mail-Diensteanbieter die Anforderungen der TR 03108-1 des Bundesamts für Sicherheit in der Informationstechnik (BSI) einhalten.

Dies bedeutet, dass sie verpflichtend die in dieser Technischen Richtlinie niedergelegten Voraussetzungen für einen geschützten Empfang von Nachrichten schaffen und bei dem Versand von Nachrichten in Bezug auf die Anwendung von kryptografischen Algorithmen und die Überprüfung der Authentizität und Autorisierung der Gegenstelle den unter den gegebenen Bedingungen auf Empfängerseite bestmöglichen, mit verhältnismäßigen Mitteln erreichbaren Schutz erzielen müssen.

3.2. Sorgfaltspflicht bei der Inanspruchnahme von E-Mail-Diensteanbietern

Verantwortliche, die öffentliche E-Mail-Diensteanbieter in Anspruch nehmen, müssen sich davon überzeugen, dass die Anbieter hinreichende Garantien für die Einhaltung der Anforderungen der DS-GVO und insbesondere der genannten Technischen Richtlinie bieten. Dies schließt auch die sichere Anbindung eigener Systeme und Endgeräte an die Diensteanbieter ein.

Darüber hinaus müssen die Verantwortlichen die Risiken sorgfältig einschätzen, die mit dem Bruch der Vertraulichkeit und Integrität von E-Mail-Nachrichten verbunden sind, die sie versenden oder gezielt empfangen. In Abhängigkeit von diesen Risiken können sich die im Folgenden dargestellten zusätzlichen Anforderungen ergeben, deren Erfüllung sie durch Weisung an den Diensteanbieter (z. B. durch Vornahme geeigneter Konfigurationseinstellungen, soweit solche von dem Diensteanbieter angeboten werden) durchsetzen müssen.

4. Fallgruppen

4.1. Gezielte Entgegennahme von personenbezogenen Daten in den Inhalten von E-Mail-Nachrichten

Verantwortliche, die gezielt personenbezogene Daten per E-Mail entgegennehmen, z. B. durch explizite Vereinbarung des Austauschs personenbezogener Daten per E-Mail oder die Aufforderung auf der Homepage, personenbezogene Daten per E-Mail zu übermitteln, haben die im Folgenden beschriebenen Verpflichtungen zu erfüllen.

4.1.1. Verpflichtungen bei normalen Risiken[6]

Der Schutz von Vertraulichkeit und Integrität von personenbezogenen Daten bei der Übermittlung von E-Mail-Nachrichten setzt voraus, dass Sender und Empfänger zusammenarbeiten. Die Verantwortung für den einzelnen Übermittlungsvorgang liegt bei dem Sender. Wer jedoch gezielt personenbezogene Daten per E-Mail entgegennimmt, ist verpflichtet, die Voraussetzungen für den sicheren Empfang von E-Mail-Nachrichten über einen verschlüsselten Kanal zu schaffen. Das bedeutet, dass der Empfangsserver mindestens den Aufbau von TLS-Verbindungen (direkt per SMTPS oder nach Erhalt eines STARTTLS-Befehls über SMTP) ermöglichen muss und hierbei ausschließlich die in der BSI TR 02102-2 aufgeführten Algorithmen verwenden darf. Um den Aufbau verschlüsselter Verbindungen zu erleichtern, sollte der Verantwortliche für Verschlüsselung und Authentifizierung ein möglichst breites Spektrum an qualifizierten Algorithmen anbieten.

Um die Authentizität und Integrität der empfangenen E-Mail-Nachrichten zu überprüfen, sollten Verantwortliche DKIM-Signaturen prüfen und signierte Nachrichten, bei denen die Prüfung fehlschlägt, markieren oder, bei entsprechender Festlegung des Absenders über einen DMARC-Eintrag im DNS, zurückweisen.

4.1.2. Verpflichtungen bei hohen Risiken

Nimmt ein Verantwortlicher Daten gezielt per E-Mail entgegen, bei denen der Bruch der Vertraulichkeit ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen darstellt, dann muss er sowohl qualifizierte

6 Zur Einstufung von Risiken s. das Kurzpapier Nr. 18 der unabhängigen Datenschutzbehörden des Bundes und der Länder „Risiko für die Rechte und Freiheiten natürlicher Personen“, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/kurzpapiere/DSK_KPNr 18_Risiko.pdf.

Transportverschlüsselung (s. u. Nr. 5.2) als auch den Empfang von Ende zu Ende verschlüsselter Nachrichten ermöglichen.

Nimmt ein Verantwortlicher Daten gezielt per E-Mail entgegen, bei den der Bruch der Integrität ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen darstellt, dann muss er bestehende (PGP- oder S/MIME-) Signaturen qualifiziert prüfen (s. u. Nr. 5.4).

4.2. Versand von E-Mail-Nachrichten

4.2.1. Verpflichtungen bei normalen Risiken

Alle Verantwortlichen, die E-Mail-Nachrichten mit personenbezogenen Daten versenden, bei denen ein Bruch der Vertraulichkeit (des Inhalts oder Umstände der Kommunikation, soweit sie sich auf natürliche Personen beziehen) ein Risiko für die Rechte und Freiheiten von natürlichen Personen darstellt, sollten sich an der TR 03108-1 orientieren und müssen eine obligatorische Transportverschlüsselung sicherstellen.

4.2.2. Versand von E-Mail-Nachrichten bei hohem Risiko

Verantwortliche, die E-Mail-Nachrichten versenden, bei denen ein Bruch der Vertraulichkeit von personenbezogenen Daten im Inhalt der Nachricht ein hohes Risiko für die Rechte und Freiheiten von natürlichen Personen darstellt, müssen regelmäßig eine Ende-zu-Ende-Verschlüsselung und eine qualifizierte Transportverschlüsselung vornehmen. Inwieweit entweder auf die Ende-zu-Ende-Verschlüsselung oder die Erfüllung einzelner Anforderungen an diese (s. Kap. Ende-zu-Ende-Verschlüsselung) oder an die qualifizierte Transportverschlüsselung (z. B. DANE oder DNSSEC) verzichtet werden kann, hängt von den bestehenden Risiken, der konkreten Ausgestaltung des Übertragungsweges und ggf. getroffenen kompensierenden Maßnahmen ab.

4.2.3. Versand von E-Mail-Nachrichten durch gesetzlich zur Verschwiegenheit Verpflichtete

Gemäß Erwägungsgrund 75 der DS-GVO können bei der Verarbeitung von personenbezogenen Daten, die einem Berufsgeheimnis unterliegen, durch einen Verlust der Vertraulichkeit Risiken für die Rechte und Freiheiten der betroffenen Person auftreten. Erhalten so Personen unbefugt Zugang zu den in einer E-Mail-Nachricht enthaltenen personenbezogenen Daten, stellt dies eine Verletzung des Schutzes personenbezogener Daten dar, die durch technische und organisatorische Maßnahmen (wie individuelle Adressierung und gegebenenfalls Verschlüsselung) zu verhindern ist.

Weil das Vorliegen eines Berufsgeheimnisses ein Indiz für ein hohes Risiko darstellen kann, haben Berufsgeheimnisträger die Höhe des jeweiligen Risikos besonders zu prüfen. Umgekehrt bedeutet die Tatsache, dass eine Datenverarbeitung, hier die Offenbarung bzw. Offenlegung der Daten, straf- oder berufsrechtlich nicht verboten ist, nicht automatisch, dass sie auch datenschutzrechtlich zulässig ist oder dass aus datenschutzrechtlicher Sicht kein hohes Risiko besteht.

Sind Verantwortliche zur Geheimhaltung besonders verpflichtet, z. B. Berufsgeheimnisträger i. S. d. § 203 StGB[7], und bestehen bei der Übermittlung von Nachrichten hohe Risiken für Betroffene, so sind die in Abschnitt 4.2.2 aufgeführten Anforderungen umzusetzen. Soweit angesichts der konkreten Umstände nur normale Risiken bestehen, gelten die Anforderungen des Abschnitts 4.2.1.

4.2.4. Zulässige Empfänger einer E-Mail

Bei dem Versand einer E-Mail-Nachricht muss – durch technische und organisatorische Maßnahmen – zusätzlich sichergestellt werden, dass bei dem Empfänger nur Personen die zu versendende Nachricht bei ihrer Entgegennahme zur Kenntnis nehmen, denen gegenüber eine Offenlegung der Nachricht gestattet ist. Eine geeignete Maßnahme insbesondere bei hohem Risiko besteht in einer Ende-zu-Ende-Verschlüsselung mit individueller Adressierung an eine Person, für die die Inhalte zulässigerweise bestimmt sind.

5. Anforderungen an die Verschlüsselungs- und Signaturverfahren

5.1. Obligatorische Transportverschlüsselung

Durch eine obligatorische Transportverschlüsselung soll eine unverschlüsselte Übermittlung der Nachrichten ausgeschlossen werden. Sie kann über das Protokoll SMTPS oder durch Aufruf des SMTP-Befehls STARTTLS und den nachfolgenden Aufbau eines mit dem Protokoll TLS verschlüsselten Kommunikationskanals realisiert werden, wobei die Anforderungen der TR 02102-2 des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu erfüllen sind.

Bei dem letztgenannten Verfahren (STARTTLS) kann die obligatorische Transportverschlüsselung durch entsprechende Konfiguration des sendenden MTA (Mail Transfer Agent) durch folgende Maßnahmen erreicht werden – die entsprechenden Konfigurationseinstellungen werden (En)Forced TLS, Mandatory TLS o. ä. genannt. Unterstützt die Gegenstelle kein TLS, dann

7 Zum Verhältnis von Datenschutzrecht zum Berufsrecht siehe Abschnitt 2.

wird der Verbindungsaufbau abgebrochen. Einige MTA ermöglichen eine domänenspezifische oder regelbasierte Spezifizierung dieses Verhaltens.

5.2. Qualifizierte Transportverschlüsselung

Transportverschlüsselung erreicht unter folgenden Voraussetzungen einen ausreichenden Schutz gegen aktive Angriffe von Dritten, die in der Lage sind, den Netzwerkverkehr auf der Übermittlungsstrecke zu manipulieren:

1. Die eingesetzten kryptografischen Algorithmen und Protokolle entsprechen dem Stand der Technik: Sie erfüllen die Anforderungen der Technischen Richtlinie BSI TR-02102-2 und garantieren Perfect Forward Secrecy.
2. Die Bezeichnung der zum Empfang autorisierten Mailserver und ihre IP-Adressen wurden auf Empfängerseite per DNSSEC signiert. Die Signaturen der DNS-Einträge werden auf Senderseite überprüft. Alternativ kann die Bezeichnung der zum Empfang autorisierten Mailserver auch durch Kommunikation mit dem Empfänger verifiziert werden.
3. Der empfangende Server wird im Zuge des Aufbaus der verschlüsselten Verbindung entweder zertifikatsbasiert authentifiziert oder anhand eines öffentlichen oder geheimen Schlüssels, der über einen anderen Kanal zwischen Sender und Empfänger abgestimmt wurde.
4. Erfolgt die Authentifizierung zertifikatsbasiert, so führt der Empfänger die Authentizität des Zertifikats auf ein vertrauenswürdiges Wurzelzertifikat bzw. einen via DANE publizierten Vertrauensanker zurück.

Die Einhaltung dieser Anforderungen muss nachgewiesen werden.

5.3. Ende-zu-Ende-Verschlüsselung

Durch eine Ende-zu-Ende-Verschlüsselung mit den Verfahren S/MIME und OpenPGP ist es möglich, die Inhalte einer E-Mail-Nachricht durchgreifend gegen unbefugte Kenntnisnahme zu schützen. Dieser Schutz erstreckt sich dabei nicht nur auf den eigentlichen Transportweg, sondern auch auf die Zwischenspeicherung und -verarbeitung auf den an der Übermittlung beteiligten Servern. Um diese Wirksamkeit zu erreichen, sind folgende Voraussetzungen einzuhalten:

1. Der Verantwortliche muss die öffentlichen Schlüssel der Empfänger auf die Einhaltung hinreichender Sicherheitsparameter (insbesondere einer hinreichenden Schlüssellänge) überprüfen, sie durch Verifikation der Zertifikate bzw. Beglaubigungen authentisieren, vor jedem Versand bzw. Signaturprüfung auf Gültigkeit überprüfen und zuverlässig verwalten.

2. Die Überprüfung der Authentizität eines Schlüssels kann regelmäßig durch Verifikation eines Zertifikats eines vertrauenswürdigen Zertifikatsdiensteanbieters (S/MIME) oder Beglaubigung anderer vertrauenswürdiger und nachweislich zuverlässiger Dritter (OpenPGP) erfolgen. Es sei ausdrücklich darauf hingewiesen, dass die Veröffentlichung eines Schlüssels auf einem OpenPGP-Schlüsselserver kein Indiz für die Authentizität dieses Schlüssels ist. Die Überprüfung des Fingerprints eines OpenPGP-Keys ist für die Überprüfung der Authentizität eines Schlüssels ausreichend, sofern der Fingerprint mit einer sicheren kryptografischen Hashfunktion (s. BSI TR-02102) ermittelt und die Authentizität des Vergleichswerts z. B. durch direkte Kommunikation mit dem Empfänger über einen anderen Kanal überprüft wurde.
3. Die Authentizität eines über Web Key Directory (WKD) bereitgestellten öffentlichen Schlüssels ist äquivalent zu der Authentizität des bereitstellenden Webservers. Für die Überprüfung gelten die Anforderungen an die Überprüfung der Authentizität des empfangenden Mailservers entsprechend.
4. Diese Anforderung kann auch nachträglich in Bezug auf Schlüssel erfüllt werden, die zunächst opportunistisch ausgetauscht wurden (z. B. per Autocrypt). Hierzu ist eine Verifikation der Authentizität über einen anderen Kanal erforderlich.
5. Die Überprüfung der Gültigkeit eines S/MIME-Schlüssels vor seinem Einsatz soll durch Abruf von Gültigkeitsinformationen bei dem Zertifikatsdiensteanbieter (Abruf von CRI via http, OCSP) erfolgen. Die Überprüfung der Gültigkeit eines Open-PGP-Schlüssels ist nur möglich, wenn der Eigner bekannt gegeben hat, wo er ggf. Revokationszertifikate zu veröffentlichen beabsichtigt. Dies kann z. B. ein Open-PGP-Schlüsselserver oder die Webseite des Schlüsseleigners sein. Sofern es an einer solchen Abrufmöglichkeit fehlt, müssen Garantien dafür bestehen, dass alle Nutzer eines Schlüssels unverzüglich informiert werden, wenn dieser seine Gültigkeit – insbesondere aufgrund einer Kompromittierung des zugehörigen privaten Schlüssels – verliert.

Wer Nachrichten Ende zu Ende verschlüsselt, sollte beachten, dass Perfect Forward Secrecy durch Ende-zu-Ende-Verschlüsselung allein nicht gegeben ist, so dass eine Kompromittierung des privaten Schlüssels eines Empfängers alle Nachrichten gefährdet, die mit dem zugehörigen öffentlichen Schlüssel verschlüsselt wurden. E-Mail-Nachrichten, die von Dritten abgefangen werden, können von diesen aufbewahrt und bei Offenlegung des privaten Schlüssels eines der Empfänger zu einem späteren Zeitpunkt entschlüsselt werden.

5.4. Signatur

Durch eine Signatur mit den Verfahren SI/MIME und OpenPGP ist es möglich, die Integrität der Inhalte einer E-Mail-Nachricht nachhaltig gegen unbefugte Beeinträchtigung zu schützen. Dieser Schutz erstreckt sich dabei nicht nur auf den eigentlichen Transportweg, sondern auch auf die Zwischenspeicherung und -verarbeitung auf den an der Übermittlung beteiligten Servern. Um diese Wirksamkeit zu erreichen, sind folgende Voraussetzungen einzuhalten:

Sender müssen die eigenen Signaturschlüssel mit hinreichenden Sicherheitsparametern erzeugen, die privaten Schlüssel sicher speichern und nutzen; soweit kein direkter Abgleich der Schlüssel zwischen Sender und Empfänger stattfindet, die korrespondierenden öffentlichen Schlüssel von zuverlässigen und vertrauenswürdigen Dritten zertifizieren lassen und sie ihren Kommunikationspartnern zur Verfügung stellen.

Empfänger sollen in Abhängigkeit von den Authentizitäts- und Integritätsrisiken die in Kap. Ende-zu-Ende-Verschlüsselung aufgeführten Maßnahmen auf die Überprüfung und das Management der Schlüssel der Sender in entsprechender Weise anwenden.

II

Zweiter Teil

4. Tätigkeitsbericht zur Informationsfreiheit

1. Einführung Informationsfreiheit

Der vorliegende vierte Tätigkeitsbericht zur Informationsfreiheit beschreibt und analysiert die Informationsfreiheit in Hessen im Jahr 4 seit der Regelung des Rechts eines allgemeinen und voraussetzungslosen Zugangs zu Akten der öffentlichen Verwaltung im Hessischen Datenschutz- und Informationsfreiheitsgesetz (HDSIG). Seit dem 25. Mai 2018 sind dieser Anspruch, seine Einschränkungen und seine Durchsetzung im Vierten Teil des Gesetzes geregelt. Danach hat jede Person freien, voraussetzungslosen und kostenfreien Zugang zu Informationen, die in öffentlichen Stellen vorhanden sind. Dabei sind die Grundrechte Dritter zu achten und zu wahren. Diese betreffen die freie Selbstbestimmung über die eigenen personenbezogenen Daten und den Schutz schützenswerter Geheimnisse. Die betroffenen Dritten sind an dem Verfahren zur Freigabe der Informationen zu beteiligen. Ebenso können überwiegende öffentliche Belange wie etwa die öffentliche Sicherheit dem Zugang zu Informationen entgegenstehen. Um die Entscheidungsfindung der öffentlichen Stellen nicht zu beeinträchtigen, besteht der Informationszugang nur zu Akten aus abgeschlossenen Verfahren. Der Informationszugang ist bei öffentlichen Stellen ausgeschlossen, soweit er die Aufgabenerfüllung dieser Stellen behindern würde. Dieses Regelungskonzept begründete der Gesetzgeber wie folgt:

> „Das Verwaltungshandeln soll zukünftig offener und transparenter gestaltet werden. Im Vierten Teil … werden deshalb erstmals Regelungen für ein Recht auf Informationszugang gegenüber den öffentlichen Stellen in Hessen geschaffen. Bürgerinnen und Bürger erhalten damit die Möglichkeit, unmittelbar Einblick in Vorgänge der öffentlichen Verwaltung zu nehmen. Entscheidungen der Verwaltung werden damit nachvollziehbar, deren Akzeptanz wird erhöht. Die Schaffung eines Anspruchs auf Informationszugang hat so eine wichtige demokratische und rechtstaatliche Funktion, denn der freie Zugang zu bei öffentlichen Stellen vorhandenen Informationen ist wesentlicher Bestandteil öffentlicher Partizipation und der Kontrolle staatlichen Handelns. Er fördert die demokratische Meinungs- und Willensbildung. Der effektive Schutz personenbezogener Daten bleibt dabei gewährleistet, entgegenstehende berechtigte öffentliche und private Interessen werden angemessen berücksichtigt“ (Landtags-Drucksache 19/5728, S. 97).

Der Bund und zwölf Länder hatten bereits seit Jahren Regelungen zur Informationsfreiheit oder sogar zur Transparenz der Verwaltung getroffen, die den Informationszugang zu allen öffentlichen Stellen eröffneten. Hessen wählte jedoch ein eigenes Regelungskonzept. Das Recht des allgemeinen Informationszugangs gilt nur gegenüber der Landesverwaltung. Die Gemeinden und Landkreise sollen jedoch jeweils für sich selbst durch Satzung entscheiden, ob sie einen Informationszugang zu ihren Akten eröffnen. Solche Informationsfreiheitssatzungen haben bisher jedoch nur vier Landkreise, eine Großstadt und wenige kleine Städte verabschiedet. Für die meisten Verwaltungen in

Hessen gilt daher noch keine Informationsfreiheit. Dementsprechend ist die Informationsfreiheit in der Praxis der Verwaltung in Hessen auch noch in geringem Maße ausgeprägt und muss sich künftig noch entwickeln (s. Ziff. 2).

Als Informationsfreiheitsbeauftragter hatte ich dennoch im Berichtsjahr viele interessante Fragen zur Informationsfreiheit zu beantworten, unterstützte Bürgerinnen und Bürger bei der Durchsetzung ihrer Ansprüche, beteiligte mich an der Diskussion zur rechtspolitischen Fortentwicklung der Informationsfreiheit und arbeitete mit anderen Informationsfreiheitsbeauftragten in Deutschland in der Konferenz der Informationsfreiheitsbeauftragten (IFK) zusammen. Zu diesen Tätigkeitsfeldern bietet der vierte Tätigkeitsbericht eine kleine Auswahl. Er untersucht die Frage, welche Daten der antragstellenden Person an welche Stellen weitergegeben werden dürfen (s. Ziff. 3), erläutert, warum der Informationsfreiheitsbeauftragte nicht stellvertretend für eine antragstellende Person Informationen beschaffen kann (s. Ziff. 4), und beschreibt die politische Diskussion über ein Open Data-Gesetz in Hessen (s. Ziff. 5).

2. „Voraussetzungsloser“ Informationszugang und kommunaler Satzungsvorbehalt

Der Anspruch auf Informationen gegenüber öffentlichen Stellen knüpft im Informationsfreiheitsrecht nicht an die Betroffenheit der antragstellenden Person in einer bestimmten Angelegenheit an. Der Antrag auf Informationszugang darf nur dann abgelehnt werden, wenn sich das aus dem Informationsfreiheitsrecht normativ herleiten lässt. Erlässt eine Kommune eine Informationsfreiheitssatzung im Sinne des HDSIG nur bezogen auf ihren Selbstverwaltungsbereich, ist das zwar nicht rechtswidrig, aber es harmoniert nicht mit der Gesamtkonzeption des hessischen Informationsfreiheitrechts.

1. Die Informationsfreiheitsbeschwerde

Ein Rechtsanwalt (Beschwerdeführer) wandte sich in einer Straßenverkehrsangelegenheit (Geschwindigkeitsverstoß seines Mandanten) an mich und rügte, dass ihm die Einsicht in Unterlagen zu Probemessungen (Radaranlagen) in der Stadt Kassel nicht gewährt worden sei. Das hessische Innenministerium sei in diesem Kontext involviert und habe einen Informationszugangsanspruch abgelehnt. Der Petent bat mich deshalb, die Frage des Informationszugangsanspruchs in der Angelegenheit zu überprüfen.

2. „Voraussetzungsloser“ Informationszugang

Das Hessische Ministerium des Innern und für Sport (HMdIS) hatte in einem Schreiben an den Beschwerdeführer seine Verneinung des Informationsfreiheitsanspruchs unter anderem mit folgender Ausführung gerechtfertigt:

> „Die Transparenz des Bußgeldverfahrens und der Rechtsschutz Ihres Mandanten wurden folglich durch die Verweigerung in die Unterlagen zu den Probemessungen nicht verletzt. Vor diesem Hintergrund hatten wir bereits ausgeführt, dass auch eine vom Klageverfahren losgelöste Einsichtnahme in die Unterlagen der Probemessungen nach den §§ 80 ff. Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG) ausscheidet.“

Diese Darlegung war für mich Anlass, das HMdIS um eine ergänzende Stellungnahme mir gegenüber zu bitten. Denn die zitierte Passage suggeriert, der Informationsfreiheitsanspruch sei nur dann gegeben, wenn der Antragsteller geltend machen könne, in der konkreten Angelegenheit belastet zu sein, etwa durch fehlende „Transparenz des Bußgeldverfahrens“.

Genau das ist aber nicht der Fall: Insoweit ist die Informationsfreiheit „voraussetzungslos“, ja das ist geradezu ihr Spezifikum gegenüber anderen Auskunftsansprüchen (etwa Art. 15 DS-GVO oder § 29 HVwVfG), also sozusagen ihre Essenz.

Informationszugangsanträge dürfen nur dann abgelehnt werden, wenn die Regelungen der Informationsfreiheit das rechtfertigen (§ 80 HDSIG).

§ 80 HDSIG

(1) Jeder hat nach Maßgabe des Vierten Teils (=Informationsfreiheit) gegenüber öffentlichen Stellen Anspruch auf Zugang zu amtlichen Informationen (Informationszugang) …

(2) Soweit besondere Rechtsvorschriften die Auskunftserteilung regeln, gehen sie den Vorschriften des Vierten Teils vor.

Vor diesem Hintergrund bat ich das Ministerium um Erläuterung, weshalb genau die §§ 80 ff. HDSIG dem Informationsbegehren in der Angelegenheit entgegenstehen, und informierte den Beschwerdeführer über diesen Sachstand.

Daraufhin teilte mir der Beschwerdeführer mit, dass die Stadt Kassel, und mitgetragen vom Innenministerium, ihm gegenüber mit Blick auf das Informationsfreiheitsrecht den Informationszugang mit der Begründung abgelehnt habe, die Informationsfreiheitssatzung der Stadt Kassel betreffe nur den Selbstverwaltungsbereich, aber nicht den Bereich der übertragenen Verwaltungsaufgaben, um den es hier gehe.

Daraufhin habe ich mir von der Stadt Kassel ihre Informationsfreiheitssatzung vorlegen lassen, die explizit den Informationszugang nur für den Selbstverwaltungsbereich, den eigenen Wirkungskreis der Stadt (§ 2 HGO), eröffnet.

3. Kommunaler Satzungsvorbehalt im hessischen Informationsfreiheitsrecht

Rechtliche Grundlage für Informationszugangsatzungen im kommunalen Bereich ist § 81 Abs. Nr. 7 HDSIG.

§ 81 HDSIG

(1) Nach Maßgabe des § 2 Abs. 1 bis 3 gelten die Vorschriften über den Informationszugang auch für

(…)

7. die Behörden und sonstigen öffentlichen Stellen der Gemeinden und Landkreise sowie deren Vereinigungen ungeachtet ihrer Rechtsform, soweit die Anwendung des Vierten Teils durch Satzung ausdrücklich bestimmt wird.

Diese Vorschrift stellt die Geltung des hessischen Informationsfreiheitsrechts im kommunalen Bereich also unter Satzungsvorbehalt.

Im Gesetzgebungsverfahren gab es keine Zweifel, dass der Satzungsvorbehalt sich sowohl auf den Informationszugang im kommunalen Selbstverwaltungsbereich als auch auf die den Kommunen vom Land übertragenen Aufgaben bezieht (vgl. hierzu § 4 HGO: Weisungsaufgaben, Auftragsangelegenheiten). Es war auch nicht angedacht worden, dass eine Kommune auf die „Idee“ kommen könnte, den Informationszugang mit Blick auf den Aufgabentyp zu splitten. Eine solche Splittung für rechtswidrig zu halten, wäre der Informationsfreiheit freilich nicht förderlich, denn dann könnte sich die Kommune auch ebenso dafür entscheiden, den Informationszugang (wiederum) ganz zu versagen: Also besser Teilzugang als überhaupt keiner.

Gleichwohl ist die Situation in Kassel für das Hessische Informationsfreiheitsrecht skurril: Der Landesgesetzgeber hat sich für den Landesbereich durch Normierung der §§ 80 ff. HDSIG zur Informationsfreiheit bekannt. Kassel versagt nun den Informationszugang zu den dem Land ja gerade rechtlich nahestehenden Weisungsaufgaben und Auftragsangelegenheiten im Sinne des § 4 HGO, indem es explizit in seiner Satzung den Informationszugang gerade nur für den Selbstverwaltungsbereich (den eigenen Wirkungskreis im Sinne des § 2 HGO) eröffnet.

Insgesamt ist die Rechtslage in Kassel trotz alledem relativ positiv, denn die anderen größeren Städte in Hessen haben bislang überhaupt keine Informationszugangssatzung erlassen und verwehren dadurch Informationszugangsansprüche komplett. Und von den Landkreisen haben sich bislang auch nur Marburg-Biedenkopf, Groß-Gerau, Darmstadt-Dieburg und der Main-Taunus-Kreis für eine Informationsfreiheitssatzung entschieden, also gerade einmal vier von 21 Landkreisen in Hessen.

Den Beschwerdeführer habe ich den Vorgang abschließend über die oben beschriebene Sach- und Rechtslage informiert.

3. Weitergabe von Daten der antragstellenden Person

Falls eine antragstellende Person der Stelle, die um Auskunft ersucht wird, die Weitergabe ihrer Daten an Dritte untersagt, ist das von der Stelle zu beachten. Dies kann aber dazu führen, dass in diesem Fall keine Auskunft in der Sache gegeben werden kann.

1. Der Anlass

Ein Bürger beschwerte sich bei mir darüber, dass er bei einer Hochschule bislang erfolglos den Informationszugang zu Vertragsvereinbarungen mit einem Institut begehrt hatte. Ich forderte daraufhin die Hochschule auf, den Informationszugangsantrag nach Maßgabe des hessischen Informationsfreiheitsrechts (§§ 80 ff. HDSIG) zu bescheiden. Vor diesem Hintergrund entschied sich die Hochschule, den Informationszugangsantrag nicht nur inhaltlich, sondern mitsamt den Personalia des Antragstellers dem Institut für dessen Stellungnahme bekannt zu geben. Dies geschah, obwohl in dem Antrag ausdrücklich die Weitergabe von personenbezogenen Daten an Dritte untersagt worden war.

Die Hochschule war der Ansicht, hierzu befugt zu sein, damit das Institut für seine Positionierung zu dem Informationszugangsantrag umfassend informiert ist.

2. Rechtliche Bewertung

Diese Weitergabe von Personalien des Antragstellers durch die Hochschule an ein Institut war jedoch rechtswidrig. Eine Rechtsgrundlage für eine solche Datenübermittlung gegen den Willen des Antragstellers, also evident ohne seine Einwilligung (Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO), ist in einer derartigen Konstellation nach Maßgabe des Datenschutz- und Informationsfreiheitsrechts nicht vorhanden (mit Blick auf Art. 6 Abs. 1 UAbs. 1 lit. e, Abs. 2 und 3 DS-GVO, §§ 22, 83 HDSIG).

Selbst aus der speziellen Verfahrensvorschrift bei Beteiligung Dritter, § 86 HDSIG, lässt sich eine Befugnis der informationspflichtigen Stelle zur Weitergabe der Personalia des Antragstellers gegen seinen Willen nicht ableiten, sondern die informationspflichtige Stelle muss dem Dritten nur Gelegenheit zur Stellungnahme bezüglich des Antrags auf Informationszugang geben.

§ 86 HDSIG

Die informationspflichtige Stelle gibt einem Dritten, dessen Belange durch den Antrag auf Informationszugang berührt sind, schriftlich Gelegenheit zur Stellungnahme innerhalb eines Monats, sofern Anhaltspunkte dafür vorliegen, dass er ein schutzwürdiges Interesse am Ausschluss des Informationszugangs haben kann.

Allerdings kann die Verweigerung eines Antragstellers, dass etwa sein Name dem Dritten, der durch den Informationszugang mitbetroffen ist, bekannt gegeben wird, dazu führen, dass der Dritte sich gegen die begehrte Auskunftserteilung ausspricht. Das kann dann die Rechtsfolge haben, etwa wenn ein Geschäftsgeheimnis des Dritten betroffen ist, dass keine Auskunft gegeben wird, § 82 Nr. 4 HDSIG.

Über diese Rechtslage habe ich den Antragsteller und die Hochschule unterrichtet. Die Hochschule habe ich zusätzlich aufgefordert, bei dem Institut die Löschung der übermittelten Daten des Antragstellers zu veranlassen, was dann auch geschah.

Im vorliegenden Fall hatte das Institut auch keine Einwände gegen die Auskunftserteilung und die Hochschule bot daraufhin dem Antragsteller die Unterlagen zur Einsicht an.

4. (Keine) Informationsbeschaffung für den Antragsteller seitens des Informationsfreiheitsbeauftragten

Weigert sich eine Stelle, einem Antragsteller Informationen zugänglich zu machen, kann die Hessische Informationsfreiheitsbehörde weder diese Stelle zur Informationsbereitstellung rechtsverbindlich verpflichten, noch darf der Hessische Informationsfreiheitsbeauftragte sich selbst die Informationen zu dem Zweck besorgen, sie anschließend dem Betroffenen zur Verfügung zu stellen.

1. Der Anlass

Ein Bürger wandte sich mit dem Anliegen an mich, ich solle eine Stelle, von der er selbst ohne Erfolg Informationen verlangt hatte, dazu verpflichten, diese Informationen an mich herauszugeben, und im Anschluss solle ich die Informationen dann ihm übermitteln.

2. Rechtliche Bewertung

2.1 (Keine) Verpflichtende Anordnung

Das hessische Informationsfreiheitsrecht (§§ 80 ff. = Vierter Teil des HDSIG) regelt in § 89 HDSIG den Rechtsstatus des Hessischen Informationsfreiheitsbeauftragten (Informationsfreiheitsbehörde). Diese Norm gibt nach ihrem Abs. 1 jeder Person, die sich in ihrem Informationsfreiheitsrecht verletzt sieht, das Recht, sich bei der Hessischen Informationsfreiheitsbehörde zu beschweren.

> *§ 89 HDSIG*
>
> *(1) Jeder, der sich in seinem Recht nach dem Vierten Teil verletzt sieht, kann unbeschadet anderweitiger Rechtsbehelfe die Hessische Informationsfreiheitsbeauftragte oder den Hessischen Informationsfreiheitsbeauftragten anrufen.*

Im Falle einer solchen Informationsfreiheitsbeschwerde wird diese von der Hessischen Informationsfreiheitsbehörde überprüft. Ist die Beschwerde begründet, kann die Informationsfreiheitsbehörde die informationspflichtige Stelle (also die Stelle, die über die begehrten Informationen verfügt, § 85 Abs. 1 S. 1 HDSIG) auffordern, den Verstoß gegen das hessische Informationsfreiheitsrecht zu beheben, also der Beschwerde abzuhelfen (§ 89 Abs. 3 S. 3 HDSIG).

§ 89 HDSIG

(3) (…) Stellt die oder der Hessische Informationsfreiheitsbeauftragte Verstöße gegen die Vorschriften des Vierten Teils fest, kann sie oder er ihre Behebung in angemessener Frist fordern. Darüber ist die zuständige Aufsichtsbehörde zu unterrichten.

Eine solche Aufforderung ist jedoch kein (rechtsverbindlicher) Bescheid der Hessischen Informationsfreiheitsbehörde gegenüber der informationspflichtigen Stelle, sondern (nur) ein rechtlicher Appell. Die Handlungsform Verwaltungsakt im Sinne des Hessischen Verwaltungsverfahrensrechts (§ 35 HVwVfG), also eine verbindliche Anordnung zu handeln, steht nämlich der Hessischen Informationsfreiheitsbehörde gegenüber öffentlichen Stellen nicht zur Verfügung.

Insofern besteht also ein erheblicher Unterschied zum Datenschutzrecht. Der Hessische Datenschutzbeauftragte ist in diesem Rechtsbereich nämlich durchaus befugt, gegenüber öffentlichen Stellen Verwaltungsakte zu erlassen (vgl. Art. 58 Abs. 2 DS-GVO), aber auch hier nur unter bestimmten Bedingungen (vgl. § 14 Abs. 1 Satz 2 HDSIG). Im Informationsfreiheitsrecht hingegen ist eine „Aufforderung“ wie bereits angesprochen (nur) ein Appell an die informationspflichtige Stelle. Ein zusätzlicher Nachdruck entsteht durch die Unterrichtung der Aufsichtsbehörde der informationspflichtigen Stelle (§ 89 Abs. 3 Satz 4 HDSIG).

Insoweit konnte dem Begehren des Beschwerdeführers, die Hessische Informationsfreiheitsbehörde möge die informationspflichtige Stelle „verpflichten“, die begehrten Informationen zu Verfügung zu stellen, nicht entsprochen werden.

2.2 Keine Informationsverschaffung seitens der Hessischen Informationsfreiheitsbehörde zugunsten des Beschwerdeführers

Allerdings gibt es noch eine weitere Vorschrift, deren Bedeutung von der Hessischen Informationsfreiheitsbehörde gegenüber dem Beschwerdeführer mit Blick auf sein Anliegen, mit ihrer Hilfe an die begehrten Unterlagen zu gelangen, klarzustellen war. Immerhin gibt das Hessische Informationsfreiheitsrecht der Informationsfreiheitsbehörde das Recht, hinsichtlich des Beschwerdegegenstandes bei der informationspflichtigen Stelle Auskunft zu erhalten und Einsicht in die betreffenden Dateien und Akten zu nehmen (§ 89 Abs. 3 Satz 2 Nr. 1 HDSIG).

§ 89 HDSIG

(3) (…) Der oder dem Hessischen Informationsfreiheitsbeauftragten ist dabei insbesondere

1. hinsichtlich des Anliegens, dessentwegen sie oder er angerufen wurde, Auskunft zu erteilen und Einsicht in betreffende Dateien und Akten zu verschaffen (…).

Diese Regelung erlaubt der Hessischen Informationsfreiheitsbehörde jedoch nicht, sich die vom Beschwerdeführer begehrten Informationen selbst zu verschaffen, um sie im Anschluss daran dem Beschwerdeführer zu Verfügung zu stellen.

Denn das würde im Ergebnis die gesetzgeberische Entscheidung, dass die Informationsfreiheitsbehörde gegenüber der informationspflichtigen Stelle nur appellieren kann, konterkarieren.

Eine solche Vorgehensweise würde nämlich eine unzulässige „Vollstreckung“ seitens der Informationsfreiheitsbehörde im Wege einer der Informationsfreiheitsbehörde nicht zustehenden „Ersatzvornahme“ zu Lasten der informationspflichtigen Stelle bedeuten. Ein derartiges Vorgehen steht jedoch der Hessischen Informationsfreiheitsbehörde nicht zu.

Dem Betroffenen bleibt daher im Fall der (endgültigen) Weigerung der informationspflichtigen Stelle nur die Möglichkeit, diese vor dem Verwaltungsgericht auf Informationsgewährung zu verklagen (vgl. auch § 87 Abs. 5 HDSIG).

Ich habe den Beschwerdeführer über diese Rechtslage unterrichtet.

5. Kommt Open Data nach Hessen?

Im Berichtszeitraum erreichte mich die Bitte des Hessischen Landtags, zu einem Gesetzentwurf der FDP-Fraktion zur Eröffnung eines Zugangs zu sog. Open Data Stellung zu nehmen.
Grundsätzlich befürworte ich den Zugang zu Open Data im Sinne der größtmöglichen Transparenz der öffentlichen Hand. Die aktuellen Entwicklungen in der Europäischen Union zeigen, dass ein Ausbau des Zugangs zu Daten öffentlicher Stellen wünschenswert ist und die EU einen rechtlichen Rahmen für einen unkomplizierten Zugang zu Daten öffentlicher Stellen und die Einrichtung von „Datenräumen“ etablieren will.

1. Vorteile der Bereitstellung und Verwendung von Open Data

Bei der Bereitstellung von Open Data ist im Gegensatz zur bisherigen Rechtslage, wonach bei Behörden ein Antrag auf Zugang zu amtlichen Informationen gestellt werden muss, kein Antrag mehr notwendig. Die amtlichen Informationen werden bereits von Amts wegen vorgehalten und zugänglich gemacht. Dies erhöht die begrüßenswerte Transparenz der öffentlichen Hand.

Aber auch wirtschaftliche Gesichtspunkte lassen die Bereitstellung von Open Data wünschenswert erscheinen. Zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben erheben öffentliche Stellen zahlreiche Daten. Die Bereitstellung dieser enormen Datenpools über die Grenzen der jeweiligen Behörde hinaus hat eine große wirtschaftliche Bedeutung. So verspricht die Nutzung von Open Data Wertschöpfungsgewinne für weite Teile der Wirtschaft – gerade auch für kleine und mittelständische Unternehmen (Open-Data-Strategie der Bundesregierung, 2021, S. 10). Nachfolgend werde ich daher die aktuell geltende Rechtslage in der EU, in der Bundesrepublik Deutschland und in Hessen, die Open-Data-Strategie der EU und der Bundesregierung sowie das Daten-Governance-Gesetz kurz darstellen, um aufzuzeigen, wie künftig eine Nutzung von Open Data gestaltet werden könnte.

2. Begriff „Open Data“ und Ziel der Bereitstellung offener Daten

Der Begriff „Open Data“ und der Zweck der Bereitstellung von Open Data sind in Erwägungsgrund (EG) 16 zur Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (Open Data-Richtlinie) definiert (Amtsblatt 172 vom 26. Juni 2019, S. 56).

EG 16 Open Data-Richtlinie

Das Konzept „offene Daten“ (Open Data) bezeichnet nach dem allgemeinen Verständnis Daten in einem offenen Format, die von allen zu jedem Zweck frei verwendet, weiterverwendet und weitergegeben werden können. Eine Politik der Förderung offener Daten, die eine breite Verfügbarkeit und Weiterverwendung von Informationen des öffentlichen Sektors zu privaten oder kommerziellen Zwecken mit minimalen oder keinen rechtlichen, technischen oder finanziellen Beschränkungen unterstützt und die die Verbreitung von Informationen nicht nur für Wirtschaftsakteure, sondern vor allem für die Öffentlichkeit fördert, kann eine wichtige Rolle spielen, wenn es darum geht, soziales Engagement zu fördern und die Entwicklung neuer Dienstleistungen, die solche Informationen auf neuartige Weise kombinieren und nutzen, anzustoßen und zu fördern. Die Mitgliedstaaten werden daher ermutigt, die Erzeugung von Daten nach dem Grundsatz „konzeptionell und standardmäßig offen“ (open by design and by default) für alle Dokumente, die in den Anwendungsbereich dieser Richtlinie fallen, zu fördern. Dadurch sollten sie ein kohärentes Maß des Schutzes der im Allgemeininteresse liegenden Ziele, etwa der öffentlichen Sicherheit, gewährleisten, auch in den Fällen, in denen es sich um sensible vertrauliche Informationen über den Schutz kritischer Infrastrukturen handelt. Sie sollten ebenfalls gewährleisten, dass der Schutz personenbezogener Daten sichergestellt ist, auch in den Fällen, in denen die Informationen in einem einzelnen Datensatz zwar nicht die Gefahr einer Identifizierung oder des Herausgreifens einer natürlichen Person bergen, aber in Kombination mit anderen verfügbaren Informationen eine derartige Gefahr hervorrufen könnten.

Die Möglichkeit des Zugangs zu Open Data soll keinen Zugang zu personenbezogenen Daten eröffnen. Soweit personenbezogene Daten in den bereitzustellenden Daten enthalten sind, ist sicherzustellen, dass diese vor der Bereitstellung anonymisiert werden und dass auch unter Zuhilfenahme von Zusatzwissen keine Re-Identifikation betroffener Personen erfolgen kann.

3. Rechtliche Grundlagen auf EU-Ebene und Bundesebene

Aus dem Erwägungsgrund 16 zur Open Data-Richtlinie wird bereits ersichtlich, dass die Bereitstellung von Open Data durch öffentliche Stellen innerhalb der EU ein erklärtes Ziel ist. Auch auf Bundesebene gibt es rechtliche Grundlagen für die Bereitstellung von Open Data. Erstmals wurden durch das sog. Open-Data-Gesetz (BGBl. I, 2206) mit dem am 13. Juli 2018 in Kraft getretenen § 12a E-Government-Gesetz (EGovG) Behörden der unmittelbaren Bundesverwaltung zur Bereitstellung von Open Data verpflichtet. Mit dem sog. zweiten Open-Data-Gesetz vom 16. Juli 2021 (BGBl I, 2941) wurde diese Pflicht auf grundsätzlich alle Behörden der mittelbaren Bundesverwaltung ausgeweitet. Zur Umsetzung der Open Data-Richtlinie regelt das Datennutzungsgesetz (DNG) vom 16. Juli 2021 (BGBl. I S. 2941, 2942, 4114) schließlich Details zur Bereitstellung und Weiterverwendung von offenen Daten. Die Bundesregierung hat eine Open Data-Strategie erarbeitet, die die Umsetzung der rechtlichen Grundlagen konkretisiert.

4. Rechtslage in Hessen

Die gesetzliche Verpflichtung öffentlicher Stellen zur Bereitstellung von Open Data geht noch einen Schritt weiter als die bislang in Hessen geltenden Regelungen zur Informationsfreiheit. Das Prinzip der Informationsfreiheit besagt, dass öffentliche Stellen auf Antrag Zugang zu amtlichen Informationen gewähren müssen. In Hessen ist dies im Vierten Teil des HDSIG geregelt. Bislang gibt es in Hessen keine Verpflichtung zur Bereitstellung von Open Data, auch wenn das DNG von der Bereitstellung von Open Data durch die Länder ausgeht (Open Data-Strategie der Bundesregierung, 2021, S. 16).

5. Open-Data-Richtlinie der EU

Durch die Open Data-Richtlinie werden die Mitgliedsstaaten verpflichtet sicherzustellen, dass öffentliche Daten von öffentlichen Stellen weiterverwendet werden können, und zwar sowohl für nichtkommerzielle als auch für kommerzielle Zwecke. Der erweiterte Zugang zu Daten sollte stets kostenlos sein, wobei Ausnahmen nach Art. 6 Abs. 2 der Richtlinie z. B. für Bibliotheken und Museen möglich sind. Ausnahmen von der Verpflichtung zur Bereitstellung offener Daten sind in Art. 1 Abs. 2 der Richtlinie geregelt und betreffen z. B. Dokumente, die Geschäftsgeheimnisse oder vertrauliche Informationen enthalten, oder solche, die aus Gründen des Schutzes der nationalen Sicherheit nicht öffentlich zugänglich sind.

Die Open Data-Richtlinie hat in Kapitel V Sonderregelungen für thematische Kategorien hochwertiger Datensätze geschaffen. Welche das sind, definiert sie in Art. 2 Nr. 10 und in Art. 14 Abs. 2 Satz 1.

Art. 2 Nr. 10 Open-Data-Richtlinie

Im Sinne dieser Richtlinie bezeichnet der Ausdruck

10. „hochwertige Datensätze“ Dokumente, deren Weiterverwendung mit wichtigen Vorteilen für die Gesellschaft, die Umwelt und die Wirtschaft verbunden ist, insbesondere aufgrund ihrer Eignung für die Schaffung von Mehrwertdiensten, Anwendungen und neuer, hochwertiger und menschenwürdiger Arbeitsplätze sowie aufgrund der Zahl der potenziellen Nutznießer der Mehrwertdienste und -anwendungen auf der Grundlage dieser Datensätze;

Art. 14 Abs. 2 Satz 1 Open-Data-Richtlinie

(2) Die Ermittlung bestimmter hochwertiger Datensätze gemäß Absatz 1 beruht auf der Bewertung ihres Potenzials

a) für die Erzielung bedeutender sozioökonomischer oder ökologischer Vorteile und innovativer Dienstleistungen,

b) für eine große Zahl von Nutzern, insbesondere KMU, von Nutzen zu sein,
c) der Erzielung von Einnahmen zu dienen und
d) mit anderen Datensätzen kombiniert zu werden.

Die Kommission erlässt nach Art. 14 Abs. 1 Satz 1 der Open Data-Richtlinie Durchführungsrechtsakte, mit denen die Liste dieser hochwertigen Datensätze festgelegt wird. In Anhang 6 zur Richtlinie sind derzeit sechs Kategorien hochwertiger Datensätze genannt, und zwar Geodaten, Erdbeobachtung und Umwelt, Meteorologie, Statistik, Unternehmen und Unternehmenseigentum sowie Mobilität. Diese speziellen hochwertigen Datensätze müssen nach Art. 14 Abs. 1 Satz 2 der Open Data-Richtlinie maschinenlesbar, grundsätzlich kostenlos, über API und gegebenenfalls als Massen-Download verfügbar sein.

6. Open-Data-Strategie der Bundesregierung

Die Open Data-Strategie der Bundesregierung nennt drei Handlungsfelder, um Open Data künftig effizienter und sinnvoller nutzen zu können (Open-Data-Strategie der Bundesregierung, 2021, S. 19 ff.):

– Verbesserung der Datenbereitstellung sowie leistungsfähige und nachhaltige Ausgestaltung der Dateninfrastruktur;
– Steigerung einer innovativen, gemeinwohlorientierten und verantwortungsvollen Datennutzung;
– Steigerung der Datenkompetenz und Etablieren einer neuen Kultur im Umgang mit Daten, um die Qualität und Nutzbarkeit bereitgestellter Daten zu erhöhen.

7. Ausblick: Das Daten-Governance-Gesetz der EU

Da die bislang geltenden Regelungen zum Zugang zu offenen Daten die Weiterverwendung von Daten, durch die die Rechte Dritter berührt werden, nicht gestattet, hat die EU-Kommission einen Vorstoß geplant, um auch die Weiterverwendung solcher Daten zu ermöglichen. Mit dem Vorschlag vom 25. November 2020 für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz; nachfolgend DGG) (COM(2020) 767 final) bereitete die Europäische Kommission einen europäischen Datenraum vor, der Grundlage für eine zukünftige Datenwirtschaft sein soll. Nach Stellungnahme des Parlaments und dem gemeinsamen Standpunkt des Rates einigten sich Rat und Parlament am 20. November 2021 im Trilog auf eine gemeinsame Fassung der

Verordnung (Rats-Dokument 14606/21), die noch von Rat und Parlament förmlich beschlossen werden muss.

Die Verordnung dient zum einen der Vermeidung von Wettbewerbsverzerrungen im Binnenmarkt durch die öffentliche Hand in Bezug auf Mehrwertdienste, die auf der Grundlage von Daten des öffentlichen Sektors entwickelt und angeboten werden (Nichtdiskriminierung, Verbot von Ausschließlichkeitsvereinbarungen). Zum anderen harmonisiert die Richtlinie Bedingungen der Weiterverwendung von zugänglichen Daten (Formate, Entgelte) (Hartl/Ludin, Recht der Datenzugänge, MMR 2021, 534 (535)). Hierfür sollen öffentliche Stellen, private Unternehmen und betroffene Personen Daten, über die sie verfügen, anderen zur Verwendung preisgeben. Dies soll im Unterschied zu den bisherigen Regelungen zur Bereitstellung von offenen Daten auch für personenbezogene Daten gelten. Hierbei ist zu beachten, dass in dem künftigen Datenraum die Grundrechte betroffener Personen gewahrt werden sollen. Dafür soll das EU-Recht im europäischen Datenraum wirksam durchgesetzt und der Schutz der personenbezogenen Daten uneingeschränkt geachtet werden (Roßnagel, Grundrechtsschutz in der Datenwirtschaft, ZRP 2021, 173 (174)).

Das DGG ist der erste Versuch, Datennutzung und Datenschutz normativ in Einklang zu bringen. Dies erfolgt vor allem dadurch, dass die DS-GVO auch im Bereich der Datenwirtschaft ihre volle Geltung behält und durch das DGG nur punktuell in Bezug auf drei Typen von Verantwortlichen ergänzt wird: öffentliche Stellen, Datenmittler und datenaltruistische Organisationen. Bezogen auf den Datenschutz ist es sinnvoll, zwischen personenbezogenen und nicht personenbezogenen Daten zu differenzieren (Roßnagel, ZRP 2021, 173 (175f.)). Für den Schutz personenbezogener Daten sind spezifische Schutzvorkehrungen notwendig, die nur in den Erwägungsgründen zum DGG, nicht aber im Gesetzestext selbst enthalten sind. Maßgeblich ist, dass eine Re-Identifizierung der betroffenen Personen verhindert wird. Ist ein solch ausreichender Grundrechtsschutz gewährleistet, ist die Schaffung eines europäischen Datenraums durch ein Daten-Governance-Gesetz durchaus wünschenswert.

Eine Stärkung der europäischen Wirtschaft durch freieren Zugang zu Daten ist darüber hinaus auch durch einen Zugang zu Daten möglich, die von privaten Stellen erhoben worden sind (sog. „Business-to-Business data sharing“ oder „B2B data sharing“). Das DGG fordert allerdings keinen gesetzlichen Zugang zu den Daten Privater, sondern stärkt das freiwillige Datenteilen.

Noch weiter als die vorstehend skizzierten Regelungen geht der Vorschlag der Europäischen Kommission für ein Gesetz über digitale Märkte (Digital Markets Act – DMA) (COM(2020) 842 final). Es bleibt abzuwarten, wie die

weiteren Regelungen über den Zugang zu Daten die wirtschaftlichen Interessen einerseits und den erforderlichen Grundrechtsschutz andererseits miteinander in Einklang bringen.

In Hessen wird zu diskutieren sein, wie diese Entwicklung unterstützt und wie dafür die Hessische Rechtsordnung den entstehenden Regelungen des Unionsrecht angepasst werden muss und diese konkretisieren und ergänzen kann.

6. Arbeitsstatistik Informationsfreiheit

Im Vergleich zum Vorjahr ergab sich ein geringer Anstieg an Beschwerden und Beratungen.

IFG	2020	2021
Beschwerden	64	71
Beratungen	47	52

ANHANG zu II

1. Ausgewählte Entschließungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland

1.1 „Mehr Transparenz beim Verfassungsschutz – Vertrauen und Legitimation stärken!“ vom 2. Juni 2021

Die Verfassungsschutzbehörden in Bund und Ländern haben die Aufgabe, die freiheitlich demokratische Grundordnung der Bundesrepublik Deutschland vor Bedrohungen zu schützen. Die im Vorfeld konkreter Gefahren zur Erfüllung ihrer Aufgaben vorgenommenen Maßnahmen der Informationsgewinnung unterliegen dabei zumeist der Geheimhaltung. Dies bedeutet aber nicht, dass ihre gesamte Tätigkeit zwangsläufig intransparent sein muss.

Transparenzpflichten, wie die Pflicht zur Erstellung von Verfassungsschutzberichten, finden sich nicht nur in den Verfassungsschutzgesetzen des Bundes und der Länder (vgl. § 16 BVerfSchG). Auch die Presse hat grundsätzlich einen presserechtlichen Auskunftsanspruch, sofern nicht das operative Geschäft der Behörden betroffen ist. So sind z. B. Themen und Teilnehmende von Hintergrundgesprächen auch gegen den Willen der Behörden transparent zu machen. Bürgerinnen und Bürger haben darüber hinaus nach den Umweltinformationsgesetzen des Bundes und der Länder prinzipiell einen Anspruch auf Zugang zu Umweltinformationen gegenüber den Verfassungsschutzbehörden.

Wenn die Behörden nach dem Presse- oder dem Umweltinformationsrecht Auskunft geben müssen, sofern nicht ihre geheime Tätigkeit betroffen ist, erschließt es sich nicht, warum sie auf entsprechende allgemeine Fragen nach dem Informationsfreiheitsrecht schweigen dürfen.

Mehr Transparenz stärkt das Vertrauen in die Verfassungsschutzbehörden und erhöht ihre Legitimation.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert daher die Gesetzgeber in Bund und den betroffenen Ländern auf, die Bereichsausnahmen für den Verfassungsschutz abzuschaffen und die entsprechende Ausnahmeregelung auf den Schutz konkreter Sicherheitsbelange im Einzelfall zu beschränken.

1.2
„Forderungen für die neue Legislaturperiode des Bundes: Ein Transparenzgesetz mit Vorbildfunktion schaffen!“ vom 2. Juni 2021

Informationen sind die Basis einer Demokratie. Ein demokratischer Staat kann nicht ohne freie und möglichst gut informierte öffentliche Meinung bestehen. Das Recht auf Zugang zu Informationen ist ein zentrales Element zur Regelung des Informationsflusses von staatlichen Stellen zu Bürgerinnen und Bürgern in Deutschland. Moderne Transparenzgesetze stellen die Informationen über ein Register im Internet voraussetzungs- und kostenlos zur Verfügung.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) fordert den Gesetzgeber daher auf, das Informationsfreiheitsrecht des Bundes in der nächsten Legislaturperiode zu modernisieren und das Informationsfreiheitsgesetz des Bundes zu einem modernen Transparenzgesetz mit einem Transparenzregister weiterzuentwickeln. Die IFK fordert insbesondere:

A Weiterentwicklung des Informationsfreiheitsgesetzes in ein Transparenzgesetz mit einem Transparenzregister

– Das Informationsfreiheitsgesetz (IFG) des Bundes muss zu einem echten Transparenzgesetz mit einem gesetzlich geregelten Transparenzregister weiterentwickelt werden.
– In dem Transparenzgesetz des Bundes müssen das IFG und das Umweltinformationsgesetz (UIG) zusammengelegt werden. Unterschiedliche Regelungen im IFG und UIG verkomplizieren den Zugang zu Informationen unnötig. Die Zusammenfassung der Informationsansprüche in einem Gesetz ist übersichtlicher und bürgerfreundlicher. „Ein einheitliches, übergreifendes Transparenzgesetz würde die Bekanntheit, die Anwenderfreundlichkeit und die Durchsetzungskraft aller Informationszugangsgesetze erhöhen.“ (vgl Umweltbundesamt (Dezz. 2020): Evaluation des UIG; S. 163)
– Das Transparenzregister sollte wie in mehreren Ländern einen Katalog veröffentlichungspflichtiger Informationen enthalten. Die Veröffentlichung weiterer geeigneter Informationen sollte ausdrücklich zugelassen werden.
– Zu den Informationen, die im Transparenzregister veröffentlicht werden, sollten insbesondere Kabinettbeschlüsse und deren dazugehörige Kabinettvorlagen, Verträge von öffentlichem Interesse, Gutachten, Studien und wesentliche Unternehmensdaten staatlicher Beteiligungen gehören.
– In das Gesetz sollte eine Regelung aufgenommen werden, nach der Informationen, die auf individuellen Antrag hin zugänglich gemacht wurden,

auch im Informationsregister veröffentlicht werden können (Access for one = access for all), wenn ein öffentliches Interesse an der Veröffentlichung besteht.

B Bereichsausnahmen und Ausschlussgründe

– Die Ausschlussgründe des IFG bedürfen einer grundlegenden Überarbeitung, da einige Ausschlussgründe überflüssig sind oder sich überschneiden. Sie sollten reduziert und harmonisiert werden.
– Eine allgemeine Güterabwägung zwischen Informations- und Geheimhaltungsinteresse (sog. public interest test) sollte als zusätzliches Korrektiv eingeführt werden.
– Die Bereichsausnahme für den Verfassungsschutz geht zu weit und sollte in einem neuen Transparenzgesetz nicht mehr enthalten sein.

C Regelungen zur Förderung der Informationsfreiheit

– Die Anforderungen an die Informationsfreiheit sind i. S. v. „Informationsfreiheit by Design“ bereits von Anfang an in die Gestaltung der IT-Systeme und organisatorischen Prozesse einzubeziehen.
– In dem neuen Transparenzgesetz sollte die Benennung eines behördlichen Informationsfreiheitsbeauftragten verbindlich vorgesehen werden.

D Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

– Der bzw. die Bundesbeauftragte sollte eine Anordnungsbefugnis bekommen, um Rechtsverstöße gegen das Informationsfreiheitsrecht beseitigen zu können.

E Rechtspolitik

– Die Bundesrepublik Deutschland sollte in der neuen Legislaturperiode die Tromsø-Konvention ratifizieren. Die Tromsø-Konvention ist ein im Jahr 2020 in Kraft getretener völkerrechtlicher Vertrag, der Mindeststandards setzt für das Recht auf Zugang zu amtlichen Dokumenten.

1.3
„Mehr Transparenz durch behördliche Informationsfreiheitsbeauftragte!“ vom 02. Juni 2021

Alle öffentlichen Stellen sollten Beauftragte für Informationsfreiheit benennen, so wie es bereits für den Datenschutz verpflichtend ist. In zwei Ländern ist dies schon im Gesetz vorgesehen: Sowohl in Rheinland-Pfalz als auch in Thüringen soll durch Bestellung von behördlichen Beauftragten das Recht auf Informationszugang gefördert werden.

Die Vorteile einer solchen Bestellung liegen auf der Hand:

– Informationsfreiheitsbeauftragte können die öffentlichen Stellen in ähnlicher Weise unterstützen und die Informationsfreiheit fördern, wie es im Bereich des Datenschutzes schon seit Langem vorgesehen ist.
– Informationsfreiheitsbeauftragte können ihren öffentlichen Stellen behilflich sein, wenn diese Fragen zur Auslegung des Informationsfreiheitsgesetzes haben, beispielsweise wenn es um die Berechtigung und den Umfang erhobener Informationszugangsansprüche geht. Dies garantiert zugleich die einheitliche Rechtsanwendung innerhalb der öffentlichen Stelle.
– Sie können zudem sicherstellen, dass eine auf einen Informationszugang gerichtete Anfrage als Antrag zur Verwirklichung eines subjektiven Rechts und nicht lediglich als „einfache Bitte“ qualifiziert, sondern fristgerecht bearbeitet wird.
– Zielführend wäre auch, dass sie die Bearbeitung der entsprechenden Anträge koordinieren. Hierbei können die Informationsfreiheitsbeauftragten unterstützend zur Verfügung stehen. Dies führt letztlich zu einer Arbeitserleichterung, da die Beschäftigten von deren Kenntnis im Informationsfreiheitsrecht profitieren.
– Die Informationsfreiheitsbeauftragten unterrichten und beraten die öffentlichen Stellen auch zu der proaktiven Veröffentlichung von Informationen.
– Gleichzeitig stehen sie Antragstellenden für Fragen im Zusammenhang mit dem Informationsfreiheitsgesetz als Ansprechstellen zur Verfügung.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) fordert daher den Bundes- und die Landesgesetzgeber auf, die Bestellung von behördlichen Informationsfreiheitsbeauftragten in allen deutschen Informationsfreiheitsgesetzen verbindlich vorzusehen. Die IFK empfiehlt informationspflichtigen Stellen, im Rahmen ihrer Organisationshoheit auch ohne Verpflichtung behördliche Informationsfreiheitsbeauftragte zu benennen.

1.4
„EU-Richtlinie zum Whistleblowerschutz zeitnah umsetzen! Hinweisgeberinnen und Hinweisgeber umfassend und effektiv schützen!“ vom 03. November 2021

Whistleblowerinnen und Whistleblower sind Menschen, die Hinweise auf erhebliche Missstände in Unternehmen oder Behörden geben. Sie helfen, dadurch gravierende Rechtsverstöße aufzudecken, deren Beseitigung im öffentlichen Interesse liegt. Zumeist geschieht dies dadurch, dass sie Informationen „befreien“, Rechtsverstöße den Behörden melden oder bei deren Untätigkeit die Medien informieren. Whistleblowerinnen und Whistleblower sorgen so für Transparenz und Aufklärung. Die Information der Öffentlichkeit steht jedoch regelmäßig in einem Spannungsverhältnis zu ihren arbeitsrechtlichen Loyalitäts- und Verschwiegenheitspflichten. Wenn Beschäftigte Rechtsverstöße transparent machen, laufen sie nicht selten Gefahr, insbesondere gegen arbeitsvertragliche Pflichten zu verstoßen. Hinweisgebende riskieren durch die Offenlegung von Informationen oftmals nicht nur ihren Arbeitsplatz, sondern auch ihre Karriere und ihr Ansehen.

Vor diesem Hintergrund hat die EU im Oktober 2019 eine Richtlinie erlassen, die nicht nur die Voraussetzungen für den Schutz von Whistleblowerinnen und Whistleblowern, sondern auch einen Mindestschutzstandard festlegt (Richtlinie (EU) 2019/1937). Die Richtlinie gilt für die Meldung von Verstößen gegen europäisches Recht. Sie erlaubt es den Mitgliedstaaten aber ausdrücklich, den Schutz auch auf Hinweisgebende zu erstrecken, die Verstöße gegen nationales Recht melden. Whistleblowerinnen und Whistleblower, die sich an das in ihr vorgegebene Meldeverfahren halten, sollen vor jeglichen Repressalien geschützt werden. Stichtag für eine fristgemäße Umsetzung ist der 17. Dezember 2021. Die Bundesrepublik Deutschland hat die Richtlinie bisher jedoch nicht umgesetzt, da sich die letzte Bundesregierung nicht über die Reichweite eines Whistleblower-Schutzgesetzes einigen konnte.

Eine Ungleichbehandlung der Whistleblowerinnen und Whistleblower ist nicht nachvollziehbar. Warum sollte jemand, der Verstöße gegen europäisches Recht meldet, besser geschützt werden als jemand, der Verstöße gegen deutsches Recht offenbart? Schließlich liegt es im öffentlichen Interesse, Kenntnis von jedem relevanten Rechtsverstoß zu erhalten und diesen abzustellen. Auch können Whistleblowerinnen und Whistleblower wegen der Verzahnung von europäischem und nationalem Recht vorab oftmals nur sehr schwer einschätzen, welche Rechtsmaterie konkret betroffen ist. Es ist deshalb wichtig, dass der Gesetzgeber alle Hinweisgebenden gleichermaßen gut schützt und Rechtssicherheit schafft.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) fordert den Bundesgesetzgeber auf, die EU-Richtlinie zum Schutz von Whistleblowerinnen und Whistleblowern so schnell wie möglich umzusetzen und den Schutz auch auf Hinweisgebende zu erstrecken, die Verstöße gegen nationales Recht melden.

1.5
„Umweltinformationen: Beratungs- und Kontrollkompetenz auch auf Landesbeauftragte für Informationsfreiheit übertragen!“ vom 03. November 2021

Das Gutachten zur Evaluierung des Umweltinformationsgesetzes des Bundes (UIG) hat im Oktober 2020 vorgeschlagen, eine Bundesbeauftragte oder einen Bundesbeauftragten für Umweltinformationsfreiheit zu schaffen, die oder der für die Einhaltung und Kontrolle der Vorschriften des Umweltinformationsrechts zuständig ist. In dem Gutachten wird empfohlen, diese Aufgabe der bzw. dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zu übertragen. Der Bundesgesetzgeber ist dieser Empfehlung im März 2021 gefolgt und hat der bzw. dem BfDI in § 7a UIG ausdrücklich die Befugnis gegeben, die Einhaltung des Umweltinformationsrechts zu kontrollieren.

Während im Bund nun explizit eine einheitliche Beratungs- und Kontrollkompetenz für beide Rechtsmaterien besteht, ist dies in den meisten Ländern bisher nicht der Fall. Die Landesbeauftragten für Informationsfreiheit kontrollieren oftmals nur die Einhaltung des allgemeinen Informationsfreiheitsrechts, nicht jedoch des Umweltinformationsrechts. Da sich die Rechtsmaterien nicht wesentlich unterscheiden, bleibt ihre vorhandene Fachkompetenz ungenutzt. Bei den Menschen, die sich an sie wenden, stößt dies auf Unverständnis. Sie wollen dahingehend unterstützt werden, dass ihrem Anliegen umfassend Rechnung getragen wird. Gleiches gilt für die Behörden, die die Informationsfreiheitsbeauftragten schon jetzt im Umweltinformationsrecht um Unterstützung bitten.

Eine antragstellende Person kann derzeit in Streitfällen mit Bundesbehörden zwar auf die Unterstützung des Bundesbeauftragten zählen. Die Schlichtung im Streit mit Landesbehörden oder Gemeinden bleibt ihr hingegen weitestgehend versagt, nur weil sich der Antrag auf Informationen über die Umwelt an eine Landesbehörde richtet. Diese Ungleichbehandlung lässt sich nicht nachvollziehbar begründen.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert daher die Landesgesetzgeber auf, dem Vorbild des Bundes zu folgen und den Landesbeauftragten für Informationsfreiheit, soweit noch nicht gesche-

hen, ausdrücklich auch die Beratungs- und Kontrollkompetenz für das Umweltinformationsrecht zu übertragen. Zur Erfüllung dieser neuen Aufgabe sind die Beauftragten mit ausreichenden personellen und sachlichen Mitteln auszustatten.

1.6
„Tromsø-Konvention ratifizieren und einheitlichen Mindeststandard für den Zugang zu Informationen in ganz Deutschland schaffen!“ vom 03. November 2021

Die Konferenz der Informationsbeauftragten (IFK) fordert die neue Bundesregierung auf, die Tromsø-Konvention in der neuen Legislaturperiode zu unterzeichnen und das Ratifizierungsverfahren einzuleiten.

Am 1. Dezember 2020 ist die Konvention Nr. 205 des Europarats über den Zugang zu amtlichen Dokumenten (Tromsø-Konvention) vom 18. Juni 2009 ohne deutsche Beteiligung in Kraft getreten.

Bei der Konvention handelt es sich um einen völkerrechtlichen Vertrag, der seine Mitgliedstaaten verpflichtet, im Wege der nationalen Gesetzgebung ein allgemeines Recht auf Zugang zu amtlichen Dokumenten der öffentlichen Verwaltung zu schaffen und dabei Mindeststandards bei der Bearbeitung von Informationszugangsanträgen festzulegen. Die Konvention gilt damit als weltweit erstes internationales Abkommen, das ein generelles Recht auf Informationszugang zu amtlichen Dokumenten konstituiert. Im Falle des Verstoßes eines Vertragsstaates kann der Europäische Gerichtshof für Menschenrechte angerufen werden.

Die Bundesrepublik Deutschland hat auf eine Unterzeichnung und Ratifikation des Vertrags bisher verzichtet. Die letzte Bundesregierung argumentierte, dass mit dem Informationsfreiheitsgesetz des Bundes (IFG) ein solcher Mindeststandard für ganz Deutschland bereits geschaffen und das Ziel der Konvention erreicht sei. Eine Ratifikation sei daher nicht notwendig.

Diese Auffassung ist unzutreffend, denn das IFG gilt nur für den Bund, nicht jedoch für die Länder. Nicht alle Länder haben ein Informationsfreiheitsgesetz mit Landesbeauftragten für die Informationsfreiheit geschaffen. Bayern, Niedersachsen und Sachsen haben derzeit weder Informationsfreiheitsgesetze noch entsprechende Landesbeauftragte. Ein einheitlicher Mindeststandard für den Zugang zu Informationen, den die Konvention vorsieht, existiert in Deutschland daher nicht.

Hinzu kommt, dass sich die Regelungen der Konvention nicht vollkommen mit den Vorschriften der bereits vorhandenen Informationsfreiheitsgesetze des Bundes und der Länder decken. Die Konvention ist insbesondere bei

der Erhebung von Gebühren wesentlich bürgerfreundlicher als das deutsche Recht.

Wer Transparenz und Informationsfreiheit dauerhaft verwirklichen will, muss den Zugang zu amtlichen Informationen auch völkerrechtlich garantieren. Mehr als zwölf Jahre nach Entstehung des Abkommens wird es höchste Zeit, dass Deutschland sich zu einem europaweiten Mindeststandard für den Informationszugang bekennt.

Verzeichnis der Abkürzungen

ABl. EU	Amtsblatt der Europäischen Union
Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
AES	Advanced Encryption Standard
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
API	Application Programming Interface (Anwendungsschnittstelle oder Programmierschnittstelle)
ArbZG	Arbeitszeitgesetz
Art.	Artikel
BAG	Bundesarbeitsgericht
BBB	BigBlueButton
BCR	Binding Corporate Rules (verbindliche interne Datenschutzvorschriften)
BDSG	Bundesdatenschutzgesetz
beA	Besonderes elektronisches Anwaltspostfach
beBPo	Besonderes Behördenpostfach
beN	Besonderes Notarpostfach
Beschl.	Beschluss
BetrVG	Betriebsverfassungsgesetz
BfDI	Bundesbeauftragter für Datenschutz und Informationsfreiheit
BFH	Bundesfinanzhof
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BMG	Bundesmeldegesetz
BTDrucks. und BT-Drs.	Bundestagsdrucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BTLE	Borders, Travel & Law Enforcement (Subgroup)
Buchst.	Buchstabe
BVerfG	Bundesverfassungsgericht
BYOD	Bring Your Own Device (mobiles Arbeiten mit einem privaten Endgerät der oder des Beschäftigten)
bzw.	beziehungsweise
ca.	Circa

CoKoBeV	Corona-Kontakt- und Betriebsbeschränkungsverordnung
CoSchuV	Coronavirus-Schutzverordnung
COVID-19	Coronavirus-Krankheit-2019
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
dass.	dasselbe
d. h.	das heißt
DNG	Datennutzungsgesetz
DS-GVO, DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder; kurz: Datenschutzkonferenz
EDSA	Europäischer Datenschutzausschuss
EDSB	Europäischer Datenschutzbeauftragter
efA	Einer für Alle
E-Government	Electronic Government
EGovG	E-Government-Gesetz
EGVP	Elektronisches Gerichts- und Verwaltungspostfach
ErwGr	Erwägungsgrund
etc.	et cetera
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
EWR	Europäische Wirtschaftsraum
EWO	Einwohnermeldeamt
f.	folgende
FAER	Fahreignungsregister
ff.	folgende (Seiten) / fortfolgende
FIU	Zentralstelle für Finanztransaktionsuntersuchungen
FristenVO	Verordnung zur Festlegung der Regeln für die Fristen, Daten und Termine
GG	Grundgesetz
ggf.	gegebenenfalls
GPS	Global Positioning System (Globales Positionsbestimmungssystem)
GVBl.	Gesetz- und Verordnungsblatt (Hessen)

GWG	Geldwäschegesetz
HBDI	Hessischer Beauftragter für Datenschutz und Informationsfreiheit
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz
HGO	Hessische Gemeindeordnung
HHG	Hessisches Hochschulgesetz
HMdJ	Hessisches Ministerium der Justiz
HKM	Hessisches Kultusministerium
HSchG	Hessisches Schulgesetz
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HLKA	Hessisches Landeskriminalamt
HMdIS	Hessisches Ministerium des Innern und für Sport
HTTPS	Hypertext Transfer Protocol Secure
IBAN	Internationale Bankkontonummer
ID	Identifikationsnummer
i. d. R.	in der Regel
IfSG	Infektionsschutzgesetz
IKU	Inkassounternehmen
i. R. d.	im Rahmen der/des
i. S. d.	im Sinne der/des
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
IfSG	Infektionsschutzgesetz
IMI	Internal Market Information System (Binnenmarkt-Informationssystem)
ISDN	Integrated Services Digital Network
IT	Informationstechnik
Kfz	Kraftfahrzeug
KI	Künstliche Intelligenz
KOM	Europäische Kommission
Landes-VKS	Videokonferenzsystem des Landes für Schulen
lit.	Litera, Buchstabe
LfV	Landesamt für Verfassungsschutz
LT-Drs.	Landtagsdrucksache (Hessen)

MMR	Multimedia und Recht (Zeitschrift)
NZA	Neue Zeitschrift für Arbeitsrecht
Nr.	Nummer
o. Ä.	oder Ähnliches
o. g.	oben genannt/genannte/genannter/genanntes
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
OWA	Outlook Web Access
OWiG	Gesetz über Ordnungswidrigkeiten
OZG	Onlinezugangsgesetz
PGP	Pretty Good Privacy
PIMS	Personal Information Management Service
POLAS	Polizeiauskunftssystem
PSD2	Payment Services Directive 2
QR-Code	Quick Response Code
RED	Rechtsextremismus Datei
Rdnr./Rn.	Randnummer
RegMoG	Registermodernisierungsgesetz
Rs.	Rechtssache
S.	Seite *oder* Satz
s.	siehe
s. a.	siehe auch
SDG-VO	Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates vom 2. Oktober 2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012
SIS II SCG	Schengen Information System II
S/MIME	Secure / Multipurpose Internet Mail Extensions
sog.	sogenannte/sogenannter/sogenanntes
SPH	Schulportal Hessen
Steuer-ID	Steuerliche Identifikationsnummer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung

StrlSchG	Strahlenschutzgesetz
StVG	Straßenverkehrsgesetz
s. u.	siehe unten
TB	Tätigkeitsbericht
TKG	Telekommunikationsgesetz
TOM	Technisch-organisatorische Maßnahmen
TTDSG	Telekommunikation-Telemedien-Daten-schutz-Gesetz
u.	und
u. a.	unter anderem
UAbs.	Unterabsatz
UM	Unified Messaging
US(A)	Vereinigte Staaten von Amerika
usw.	und so weiter
VersammlG	Versammlungsgesetz
VG	Verwaltungsgericht
vgl.	vergleiche
VKS	Video-Konferenzsystem
VPN	Virtual Private Network
z. B.	zum Beispiel
Ziff.	Ziffer
ZRP	Zeitschrift für Rechtspolitik

Register der Rechtsvorschriften

Zitiert werden die jeweils zum Bearbeitungszeitpunkt geltenden Fassungen.

Gesetz/Vorschrift	Fundstelle(n)
AEUV	Vertrag über die Arbeitsweise der Europäischen Union, Fassung aufgrund des am 01.12.2009 in Kraft getretenen Vertrages von Lissabon (Konsolidierte Fassung bekanntgemacht im ABl. EG Nr. C 115 vom 09.05.2008, S. 47) zuletzt geändert durch die Akte über die Bedingungen des Beitritts der Republik Kroatien und die Anpassungen des Vertrags über die Europäische Union, des Vertrags über die Arbeitsweise der Europäischen Union und des Vertrags zur Gründung der Europäischen Atomgemeinschaft (ABl. EU L 112/21 vom 24.04.2012)
ArbZG	Arbeitszeitgesetz 06.06.1994 (BGBl. I S. 1170, 1171); zuletzt geändert durch Gesetz vom 22.12.2020 (BGBl. I S. 3334)
BDSG	Bundesdatenschutzgesetz vom 30.06.2017 (BGBl. I S. 2097), zuletzt geändert durch Art. 12 Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU vom 20.11.2019 (BGBl. I S. 1626)
BDSG	Bundesdatenschutzgesetz vom 30.06.2017 (BGBl. I S. 2097), zuletzt geändert durch Artikel 10 des Gesetzes vom 23.06.2021 (BGBl. I S. 1858)
BDSG	Bundesdatenschutzgesetz vom 30.06.2017 (BGBl. I S. 2097), zuletzt geändert durch Art. 10 G vom 23.06.2021 (BGBl. I S. 1858, 1968)
BGB	Bürgerliches Gesetzbuch i. d. F. vom 02.01.2002 (BGBl. I S. 42)
BGB	Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 02.01.2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Art. 2 des Gesetzes vom 21.12.2021 (BGBl. I. S. 5252)
BetrVG	Betriebsverfassungsgesetz in der Fassung vom 10.12.2021 (BGBl. I, S. 5162)
BMG	Bundesmeldegesetz
CoKoBeV/ Corona-Kontakt- und Betriebs-beschränkungs-verordnung	Verordnung zur Beschränkung von sozialen Kontakten und des Betriebes von Einrichtungen und von Angeboten aufgrund der Corona-Pandemie (Corona-Kontakt- und Betriebsbeschränkungsverordnung) vom 07.05.2020, aufgeh. durch Artikel 4 Nr. 3 der Verordnung vom 26.11.2020 (GVBl. S. 826)

CoKoBeV/ Corona-Kontakt- und Betriebs-beschränkungs-verordnung	Verordnung zur Beschränkung von sozialen Kontakten und des Betriebes von Einrichtungen und von Angeboten aufgrund der Corona-Pandemie in der Fassung der am 15.08.2020 in Kraft tretenden Änderungen durch Art. 3 der Siebzehnten Verordnung zur Anpassung der Verordnungen zur Bekämpfung des Corona-Virus vom 11.08.2020 (GVBl. S. 538)
CoSchuV/ Coronavirus-Schutzverordnung	Verordnung zum Schutz der Bevölkerung vor Infektionen mit dem Coronavirus SARS-CoV 2 vom 22.06.2021, aufgehoben durch Artikel 2 der Verordnung vom 24.11.2021 (GVBl. S. 742)
CoKoBeV/ Corona-Kontakt- und Betriebs-beschränkungs-verordnung	Corona-Kontakt- und Betriebsbeschränkungsverordnung vom 26.11.2020, zuletzt geändert durch Artikel 2 der Verordnung vom 26.05.2021 (GVBl. S. 272)
CoSchuV/ Coronavirus-Schutzverordnung	Verordnung zum Schutz der Bevölkerung vor Infektionen mit dem Coronavirus-SARS-CoV-2 vom 22.06.2021 (GVBl. 2021, 282)
CoSchuV/ Coronavirus-Schutzverordnung	Verordnung zum Schutz der Bevölkerung vor Infektionen mit dem Coronavirus SARS-CoV-2 vom 24.11.2021, zuletzt geändert durch Verordnung vom 15.01.2022 (GVBl. S. 57)
Coronavirus-Einreiseverordnung	Verordnung zum Schutz vor einreisebedingten Infektionsgefahren in Bezug auf das Coronavirus SARS-CoV-2 vom 28.09.2021 (BAnz AT 29.09.2021 V1)
DGG	Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz; nachfolgend DGG) (COM(2020) 767 final)
DNG	Datennutzungsgesetz vom 16.07.2021 (BGBl. I S. 2941, 2942, 4114)
DS-GVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU L 119 S. 1)
EGovG	Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz) (BGBl I, 2749), zuletzt geändert durch Gesetz vom 16.07.2021 (BGBl I, S. 2941)
EU-US-Privacy Shield	EU-US-Privacy Shield (EU-US-Datenschutzschild) Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12.07.2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes (bekannt gegeben unter Aktenzeichen C(2016) 4176)

FristenVO	Verordnung (EWG, Euratom) Nr. 1182/71 des Rates vom 03.06.1971 zur Festlegung der Regeln für die Fristen, Daten und Termine (ABl. Nr. L 124 S. 1)
GG	Grundgesetz
GWG	Geldwäschegesetz vom 23.06.2017 (BGBl. I S. 1822), das zuletzt durch Artikel 269 der Verordnung vom 19.06.2020 (BGBl. I S. 1328) geändert worden ist.
Gesetz über künstliche Intelligenz (Vorschlag der Europäischen Kommission)	Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM/2021/206 final, 21.04.2021
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz vom 03.05.2018 (GVBl. S. 82), in Kraft gesetzt am 25.05.2018, geändert durch Art. 9 des Gesetzes vom 15.11.2021 (GVBl. S. 718, 729)
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz vom 03.05.2018 (GVBl. S. 82), in Kraft gesetzt am 25.05.2018, geändert durch Art. 5 des Gesetzes vom 12.09.2018 (GVBl. S. 570)
HGO	Hessische Gemeindeordnung in der Fassung der Bekanntmachung vom 07.03.2005, geändert durch Art. 3 des Gesetzes vom 11. Dezember 2020 (GVBl. S. 915)
HGO	Hessische Gemeindeordnung (HGO) In der Fassung der Bekanntmachung vom 07.03.2005 (GVBl. I S. 142), zuletzt geändert durch Artikel 1 des Gesetzes vom 07.05.2020 (GVBl. S. 318)
HHG	Gesetz zur Neuregelung und Änderung hochschulrechtlicher Vorschriften und zur Anpassung weiterer Rechtsvorschriften vom 14.12.2021 (GVBl. Nr. 56 S. 931 ff)
HSchG	Hessisches Schulgesetz vom 01.08.2017, zuletzt geändert durch Art. 1 des Gesetzes vom 18.01.2021 (GVBl. S. 166).
HSchG	Hessisches Schulgesetz vom 01.08.2017, zuletzt geändert durch Art. 1 des Gesetzes vom 29.09.2020 (GVBl. S. 706).
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung vom 14.01.2005 (GVBl. I 2005 S. 14), zuletzt geändert durch Artikel 3 des Gesetzes vom 30.09.2021 (GVBl. S. 622)
IfSG	Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen vom 20.07.2000 (BGBl. I S. 1045), zuletzt geändert durch Artikel 2 des Gesetzes vom 10.12.2021 (BGBl. I S. 5162)

IfSG	Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen vom 20.07.2000 (BGBl. I S. 1045), zuletzt geändert durch Artikel 4a des Gesetzes vom 21.12.2020 (BGBl. I S. 3136)
Open-Data-Gesetz	Erstes Gesetz zur Änderung des E-Government-Gesetzes (1. EGovGÄndG) (BGBl. I, 2206)
Open-Data-Richtlinie	Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20.06.2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (Amtsblatt 172 vom 26.06.2019, S. 56).
OWiG	Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19.02.1987 (BGBl. I S. 602), zuletzt geändert durch Artikel 3 des Gesetzes vom 30.11.2020 (BGBl. I S. 2600)
OZG	Onlinezugangsgesetz vom 14.08.2017 (BGBl. I S. 3122, 3138), das zuletzt durch Artikel 16 des Gesetzes vom 28.06.2021 (BGBl. I S. 2250) geändert worden ist.
RED-G	Gesetz zur Errichtung einer standardisierten zentralen Datei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus (Rechtsextremismus-Datei-Gesetz – RED-G) vom 20.08.2012 (BGBl. I S. 1798) FNA 12-13, zuletzt geändert durch Art. 23 Elfte ZuständigkeitsanpassungsVO vom 19.06.2020 (BGBl. I S. 1328)
RegMoG	Registermodernisierungsgesetz vom 28.03.2021 (BGBl. I S. 591), das zuletzt durch Artikel 11 des Gesetzes vom 09.07.2021 (BGBl. I S. 2467) geändert worden ist.
SDG-VO	Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates vom 02.10.2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012
SGB IX	Das Neunte Buch Sozialgesetzbuch – Rehabilitation und Teilhabe von Menschen mit Behinderungen, in der Fassung der Bekanntmachung vom 23.12.2016 (BGBl. I S. 3234), zuletzt geändert durch durch Artikel 7c des Gesetzes vom 27.09.2021 (BGBl. I S. 4530)
SIS II	Beschluss 2007/533/JI des Rates vom 12.06.2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II)
StGB	Strafgesetzbuch in der Fassung der Bekanntmachung vom 13.11.1998 (BGBl. I S. 3322), das zuletzt durch Artikel 47 des Gesetzes vom 21.12.2020 (BGBl. I S. 3096) geändert worden ist.

StPO	Strafprozessordnung, in der Fassung der Bekanntmachung vom 07.04.1987, zuletzt geändert durch Art. 2 G zur Durchführung der VO (EU) 2019/1148 des Europäischen Parlaments und des Rates vom 20.06.2019
StPO	Strafprozessordnung in der Fassung der Bekanntmachung vom 07.04.1987 (BGBl. I S. 1074, 1319, zuletzt geändert durch Art. 1 des Gesetzes vom 21.12.2021 (BGBl. I S. 5252)
StrlSchG	Gesetz zum Schutz vor der schädlichen Wirkung ionisierender Strahlung vom 27.06.2017 (BGBl. I S. 196), zuletzt geändert durch Art. 1, 2 Erstes ÄndG vom 20.05.2021 (BGBl. I S. 1194 i. V. m. Bek. v. 03.01.2022, BGBl. I S. 15)
StVG	Straßenverkehrsgesetz vom 05.03 2003 zuletzt geändert durch Art. 3 des Gesetzes vom 26.11.2020 (BGBl. I S. 2575)
TKG	Telekommunikationsgesetz vom 23.06.2021 (BGBl. I S. 1858), zuletzt geändert durch Artikel 8 des Gesetzes vom 10.09.2021 (BGBl. I S. 4147)
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz vom 23.06.2021 (BGBl. I S. 1982), das zuletzt durch Artikel 4 des Gesetzes vom 12.08.2021 (BGBl. I S. 3544) geändert worden ist.
VersammlG	Versammlungsgesetz in der Fassung der Bekanntmachung vom 15.11.1978 (BGBl. I S. 1789), zuletzt geändert durch Artikel 6 des Gesetzes vom 30.11.2020 (BGBl. I S. 2600)

Sachwortverzeichnis

Sachworte	Fundstellen
A	
Abhilfemaßnahmen	I 18.1, I 18.2, I 18.3, I. 19.1, I 19.2
Account	I 9.4, I 18.3
Aktenvernichter	I 2.2
Amtshilfe	I 5.1
Amtshilfeersuchen	I 5.1
Anonymität	I 17.6
Arbeitnehmer	I 11.1, I 11.3
Arbeitszeiterfassung	I 11.1, I 11.2
Aufbewahrungspflicht	I 17.3
Aufsichtsbehörde	
– Federführende	I 5.5
– Betroffene	I 5.1
Aufsichtstätigkeit	I 1, I 2.3
Auftragsverarbeiter	I 3.1, I 4.1, I 4.2, I 5.1, I 10.3, I 11.4, I 14.2, I 18.1, I 18.2, I 18.3, I 18.5, Anhang I 3.1
Auftragsverarbeitung	I 1, I 4.2, I 8.1
Auskunftserteilung	I 14.1, I 15.1, I 15.2, I 17.1, I 19.2, II 2.2, II 3.2
Auskunfts-	
– -pflicht	I 14.2
– -anspruch	I 1, I 1.6, I 9.6, I 14.2, I 17.1, Anhang II 1.1
– -recht	I 9.6
Auskunfteien	I 1, I 15.1, I 15.2, I 19.2, Anhang I 2.2

Ausweiskopie	I 2.2
B	
Bankkonto	I 14.1
BCR (Binding Corporate Rules)	I 5.1, I 19.2
Benachrichtigungspflicht	I 18.1, I 18.4
Benutzer	I 11.3, I 18.2
Beschäftigte	I 1, I 2.1, I 2.5, I 6.2, I 6.3, I 11.1, I 11.2, I 11.3, I 11.4, I 13.2, I 18.1 Anhang I 2.3, Anhang II 1.4
Beschäftigtendatenschutz	I 2.1, I 2.5,, I 6.3, I 11, I 11.1, I 18.1, I 19.1
Beschäftigungsverhältnis	I 2.5, I 11.1, I 11.2, I 11.3
Beschwerde	I 1, I 2.2, I 2.3, I 2.5, I 3.1, I 5.1, I 6.1, I 6.2, I 6.3, I 7.4, I 8.2, I 9.2, I 9.6, I 10.1, I 11.2, I 11.3, I 11.4, I 12.1, I 12.2, I 13.2, I 14.1, I 14.2, I 15.2, I 16.1, I 18.2, I 19.1, I 19.2, I 2.1, II 2.2, II 2.3, II 4.2, II 6
Betroffenenrechte	I 2.2, I 2.6, I 3.6, I 6.2, I 8.2, I 9.6
Binnenmarkt-Informationssystem	I 5.1
Bonitätsprüfung	Anhang I 2.2
Brexit	I 5.1
Bundesnetzagentur	I 6.1
Bußgeld	
– -zumessung	I 1, I 6.1, I 6.2, I 18.3, II.2.2
– -bescheid	I 6.2, I 12.1
– -verfahren	I 6.1, I 6.2, I 11.2, I 11.3, I 11.4
C	
Clearview AI	I 7.1
Cookies	I 1, I 12.1, I 12.2

Corona	
– -Pandemie	I 1, I 2, I 3, I 4, I 6.2, I I 8.2, I 9.2, I 9.3, I 9.7, I 11, Anhang I 1, Anhang I 2.3
– -Schutzverordnung	I 2.1, I 2.2, I 2.4, I 2.6
– -Warn-App	I 2.1, Anhang I 1
Cyberkriminalität	I 18.1
D	
Darknet	I 18.2
Daten	
– Biometrische	I 7.1
– Offene	II 5
– Sensible	I 2.4, I 17.2, I 17.3
– -minimierung	I 2.3, I 3.2, I 4.1, I 4.2, I 9.2, I 9.3, I 17.4, I 18.5, Anhang I 2.3
Daten-Governance-Gesetz	II 5.1, II 5.7
Datenpanne	I 6.2, I 6.3, I 18.1, I 18.4, I 19.2
Datenschutzinformation/-hinweise	I 7.3, I 12.1
Datenschutzmanagement	I 18.2
Datenschutzverletzungen	I 6.2, 18.1, I 18.2, I 19.1, I 19.2
Datenübermittlung	I 3.1, I 5.1, I 15.1, I 18.5, II 3.2
Datentransfers	I 1, I 4.1, I 19.2
Datenverarbeitung	
– grenzüberschreitend	I 1, I 2.4, I 5.1, I 6.1, I 8.1
– Sicherheit der	I 4.1, I 9.1, I 9.4
– Zweck der	I 2.2, I 2.3, I 2.5, I 3.2, I 4.2, I 6.2, I 7.2, I 7.3, I 9.1, I 9.2, I 9.3, I 10.1, I 10.2, I 10.3, I 11.1, I 11.2, I 11.3, I 11.4, I 12.2, I 13.2, I 14.1, I 17.2, I 17.4, I 17.5, Anhang I 2.1, Anhang I 2.3, Anhang I 3
Diensteanbieter, E-Mail	Anhang I 3.3
Dienstleister, externer	I 4.1, I 4.2, I 11.4, I 18.2,

Digitale Souveränität	I 3, I 4
Digitalisierung	I 1, I 2.1, I 3.2, I 8.1, I 9.1, I 9.4, I 9.5, I 9.7, I 11.1, I 18.5, I 19.2
Drittland/staaten	I 3.1, I 4.2, I 9.7, I 19.2
E	
EDSA	I 1, I 5.1, I 6.1
E-Government-Verfahren	I 8.1
E-Mail	
– -Adressen	I 18.1
– -Diensteanbieter	Anhang I 3
– -Kommunikation	I 18.5, Anhang I 3.1; Anhang I 4, Anhang I 5
– -Nachrichten	I 18.3, I 18.5, Anhang I 3.1, Anhang I 4, Anhang I 5
– -Server	Anhang I 5.2, Anhang I 5.3
– -Verteiler	I 19.2
EfA-Prinzip („Einer-für-Alle“-Prinzip)	I 8.1
Einkaufspassage	I 13.2
Einwilligung	I 1, I 24, I 2.5, I 4.1, I 4.2, I 6.2, I 8.2, I 9.1, I 9.2, I 9.4, I 12.2, I 17.1, I 17.2, I 17.6, I 17.5, Anhang I 2.3, Anhang I 2.4, II 3
Einzelhandel	I 2.2, Anhang I 2.3
Energieversorgerpool	Anhang I 2.1
Elektronischer Rechtsverkehr	I 18.5
Ende-zu-Ende-Verschlüsselung	I 17.2, Anhang I 3.2, Anhang I 4.2, Anhang I 5.3, Anhang I 5.4
Erforderlichkeit	I 2.5, I 7.2, I 7.4, I 13.2
EuGH (Europäischer Gerichtshof)	I 3.1, I 4.1, I 5.1, I 6.3, I 10.1, I 10.2, I 11.1, I 11.3, I 11.4
EU-US-Privacy-Shield	I 3.1, I 5.1

Exchange I 18.2

F

Facebook I 1, I 19.1, I 19.2

Fahreignungsregister I 7.4

Fahrzeughalter I 16

Fanpages I 1

Federführung I 5.1, I 19.1, I 19.2

Fehlversand I 14.3, I 18.1, I 19.2

Fernprüfungen, elektronische I 9.2

Fingerabdruck I 7.1

Forderungsmanagement, -beitreibung I 15.1

Forschungsvorhaben I 17.6

Fotoaufnahmen I 9.5, I 17.3

Fragebogen I 18.3

Friseurbetriebe, -salon I 2.2, I 2.3

G

Gästedaten I 2.2, I 2.3, I 6.2

Gaststätten I 2.2, I 2.3,

Geldbuße I 6.2, I 11.4, I 19.1, I 19.2

Gemeindevertretung I 8.2

Gesichtserkennung I 7.1

Gesundheits-
– -daten I 2.2, I 2.4, I 2.5, I 6.2, I 11.1, I 14.3, I 17.2, I 17.3, I 17.4, I 17.6, I 18.1, I 18.3
– -status I 2.5

GPS-Tracking I 11.3

Google I 9.4

Grundrechtsschutz I 1, I 3.1, I 4.2, II 5.7

H

Hochschulen I 1, I 4.2, I 9.2

Home-Office I 1, I 2.1, I 4.1, I 11.2, I 11.2, I 18.1

Hausrecht I 13.2

Hygienemaßnahmen, -regeln I 2.2

I

Identifikationsdaten I 15.2

Identifizierung I 2.1, II 5.7

IMI-System I 5.1

Impfausweis Anhang I 2.3

Impfdaten I 2.5

Impfstatus Anhang I 2.3

Infektionsschutz Anhang I 1

Infektionsketten I 2.2, I 2.6, Anhang I 1

Informationszugang II 1, II 2, II.3, Anhang II 1.2, Anhang II 1.6

Informationsfreiheit II 1, II 2, II 3, II 4, II 5, Anhang II

Inkassounternehmen II 15.1

Interessen, berechtigte I 9.6, I 11.3, I 15.1, Anhang I 2.2

Internet
– - nutzer I 1, I 12.2
– - seite I 8.2, I 18.2
– - veröffentlichung I 2.5, I 8.2, I 11.2, I 18.2

Informationspflichten I 2.2, I 2.6, I 6.3, I 8.3

Informationssystem, polizeiliches I 6.2, I 7.1, I 7.2

Interessenabwägung I 11.2, I 11.3, I 13.5

International-Transfers-Subgroup I 2.1, I 19.2

J

Justiziariat I 6, I 11.3, I 11.4

K

Kennzeichen I 16.1

Kindertagesstätten I 1, I 2.4

Klage I 1, I 3.1, I 6.3, I 13.2, I 19.2, II 4

Kohärenzverfahren I 5.1, I 6.1

Kommunen I 8

Kooperationsverfahren I 5.1, I 6.1

Konfiguration I 3.1, I 4.2, I 11.2, Anhang I 3.2

Kontaktnachverfolgung I 2.2, I 2.3, I 2.6, I 6.2, I 11.1

Kontaktbeschränkungen I 4.2

Kontoauszüge I 18.2

Krankenhäuser I 17.1, I 17.5, Anhang I 2.3

Kundendaten I 11.4, I 14.3, I 17.2, I 18.2

L

Landeskriminalamt, Hessisches (HLKA) I 7.2

Landtag, Hessischer I 10

Lehrkräfte I 4.2, I 9.1, I 9.4, I 9.7

Lock-In-Effekt I 3.1

Löschung I 1, I 6.3, I 8.2, I 9.3, I 9.6, I 10.3, I 11.3, I 17.4, I 18.2, Anhang I 2.3, II 3

M

Maßnahmen, präventivpolizeiliche I 7.2

Meldepflicht I 14.3, I 18.1

Meldeverfahren	Anhang I 1.4
Mitarbeiter/innen	I 6.2, I 11, I 14.1, I 15.2
– Exzess	I 6.2
– Überwachung von	I 11
Mitglieder	I 11.4, I 13.1, I 17.2
Mobiles Endgerät	I 9.3, I 11.2, I 18.3, I 18.5
N	
Nachrichtendienste	I 3.1
Nachverfolgung	I 1, I 2.1, I 2.2, I 2.3, I 2.6, I 6.2, I 11.1
Nutzerprofile	I 12.2
O	
Offenbarung	I 9.6, Anhang I 4.2
Offenlegung	I 2.3, I 2.4, I 2.5, I 3.1, I 18.1, I 18.4, I 19.2, Anhang I 4.2, Anhang I 5.3, Anhang II 1.4
One-Shop-Stop	I 5.1
Online-Dienste	I 4
Onlinezugangsgesetz	I 3.2, I 8.1, I 19.1
Open Data	I 9.4, II 1, II 5
Open-Source	I 5
Ordnungswidrigkeiten	I 2.2, I 6.2, I 7.4, I 13.2
P	
Padlet	I 9.4
Pandemie	I 2, I 8.2
Parkplätze	I 16.1
Parlament	I 2.6, I 3.1, I 8.1, I 10.1, I 10.2, I 10.3, II 5

Patienten
– - daten I 8.4, I 8.7, I 17.4
– - akte I 17.4

Personalakte I 2.3

Personalausweis I 2.2, I 2.3, I 17.1

Persönlichkeits-
– - recht I 9.5, I 11.1, I 11.2, I 11.3, I 12.1,
– - profil I 12.2, I 13.2
I 8.1, I 12.2

Petitionsgesetz I 10.2

PIMS (Personal Information Management Services) I 12.2

Plausibilitätsprüfung I 14.1, I 16.1

Polizei I 6.2, I 7.1, I 7.2, I 7.3

Polizei 2020 I 7.3

Privacy-Shield I 3.1, I 5.1

Positivdaten Anhang I 2.2

Profilbildung/Profiling I 6.3, I 8.1, I 9.3, I 12.2

Prognose I 3.1

ProxyLogon I 18.2, I 18.3

Pseudonymisierung I 11.3, I 18.4, Anhang I 1

R

Ransomware I 18.2

Rechenschaftspflicht I 11.2, Anhang I 2.3

Rechnungsversand I 17.2

Rechtsbehelf I 3.1, I 6.3, II 4

Rechtsextremismusdatei (RED) I 7.2

Rehabilitation I 13.1

Registermodernisierung	I 8.1
Reiserückkehrer	I 2.4
Restaurant	I 2.1, I 2.3, I 6.2, I 7.3
Risikobewertung	I 18.2, I 18.3
Risikogebiete	I 2.4, I 8.1
S	
Sanktionen	I 6.1, I 18.2, I 11.4, I 18.1
Satzungsvorbehalt, kommunaler	II 2
Scoring	I 18.3
Schengener Informationssystem der zweiten Generation (SIS II)	I 7.2
Schrems II-Urteil	I 1, I 3.1, I 4.1, I 5.1
Schüler/-innen	I 4.2, I 9.1, I 9.3, I 9.5, I 9.7
Schulportal	I 9.1, I 9.7
Schulträger	I 4.2, I 9.3, I 9.7
Schutzniveau	I 1, I 3.1, I 5.1, I 17.2, I 18.3, I 18.5
Schwachstellen	I 18.3
Schwärzungen	I 9.6
Schweigepflicht	I 17.1, I 17.3
Screenshots	I 11.2
Sicherheitsbehörden	I 3.1
Sicherheit der Verarbeitung	I 3.2, I 4.1, I 6.1, I 18.2, I 18.3, I 18.5
Signatur	Anhang I 3.2
Sitzungsprotokolle	I 8.2
Souveränität, digitale	I 3, I 4
Soziale Netzwerke	I 2.5
Staatliches Schulamt	I 9.3

Stadtverordnetenversammlung	I 8.2
Stammdaten	I 9.6
Standarddatenschutzverträge	I 3.1
Steuerbehörden	I 11.3
Steuer-Identifikationsnummer	I 8.1
Straßenverkehrsangelegenheit	II 2
Speicherdauer	I 7.3, I 11.3
T	
TeleCOVID Hessen	I 17.5
Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG)	I 1, I 12.2, Anhang I 2.5 I 13.1
Telemetrie	I 4.2
Tipping-Off-Verbot	I 14.2
Tracking – GPS-	I 12.2 I 11.3
Trainingsbetrieb	I 10.1
Transfer	I 1, I 4.1, I 5.1, I 19.2
Transparenz	I 3.1, I 8.2, I 17.1, I 18.1, II.1, II.2, II.5, Anhang II 1
Transportverschlüsselung	Anhang I 3.1, Anhang I 3.2, Anhang I 4.2, Anhang I 5.1
U	
Untätigkeit	I 6.3, Anhang II 1.4
V	
Verfassungsschutz	I 7.2, Anhang II 1.1, Anhang II 1.2
Verhältnismäßigkeit	I 2.6, I 7.3, I 9.2, I 11.3
Verkehrsteilnehmer	I 7.4

Versammlungen	I 7.3
Versicherungsverein	I 18.2
Verschlüsselung	I 4.1, I 14.1, I 17.2, I 18.2, I 18.3, I 18.4, Anhang I 3.2, Anhang I 4.1, Anhang I 4.2, Anhang I 5
Vertraulichkeit	I 9.6, I 17.1, I 17.2, I 17.3, I 18.2, I 18.3, I 18.4, I 18.5, Anhang I 3, Anhang I 4
Verwarnung	I 11.2, I 19.1, I 19.2
Videoüberwachung	I 6.2, I 7.1, I 7.3, I 13.2
Videokameras	I 13.2
Videokonferenzsysteme	I 3, I 4, I 11.1, I 18
VKS-Systeme	I 3, I 4, I 11.1, I 18
W	
Web	
– -analyse	I 12.2
– -seiten	I 18.2, I 19.2
Werbung	I 6.2, I 12.2, I 19.2
Wohnkomplex, Videoüberwachung im	I 13.2
Z	
Zahlungsdiensterichtlinie der EU, Payment Services Directive 2 (PSD2)	I 14.1
Zugriffe	I 3.1, I 8.2, I 9.3
Zustellung, postlagernde	I 15.2
Zutrittskontrolle	I 11.1
Zweckbindung	I 6.2, I 7.1, I 9.2, I 9.3, I 10.2, I 18.5, Anhang I 3.2