35. Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz

gemäß Art. 59 Datenschutz-Grundverordnung

für den Berichtszeitraum
vom 1. Januar bis zum 31. Dezember 2025

Impressum

Herausgeber:
Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18
poststelle@datenschutz-bayern.de

Druck:
Druck + Verlag Ernst Vögel GmbH
93491 Stamsried | Kalvarienbergstraße 22
voegel@voegel.com

Inhaltsverzeichnis

1 Überblick ... 11

1.1 Über diesen Tätigkeitsbericht ... 11

1.2 Neue Beiträge im digitalen Informationsangebot des Landesbeauftragten ... 14

2 Allgemeines Datenschutzrecht ... 15

2.1 Spielbanken Bayern: Datenschutzrechtliche Auskunftsansprüche im Spannungsverhältnis zur Geldwäscheprävention ... 15

2.1.1 Geldwäscherechtliche Sorgfaltspflichten ... 15
2.1.2 Mögliche Konflikte mit dem datenschutzrechtlichen Auskunftsanspruch ... 16
2.1.3 Kein vollständiger Ausschluss des Auskunftsanspruchs ... 17
2.1.4 Fazit ... 19

2.2 Meldung nach Art. 33 DSGVO bei Hackerangriff ... 19

2.2.1 Ausgangssituation ... 19
2.2.2 Insbesondere: Angriff bei IT-Dienstleister ... 20
2.2.3 Empfehlungen für die Erfüllung der Meldepflicht nach Art. 33 DSGVO im Fall eines Hackerangriffs ... 21
2.2.3.1 Erstmeldung innerhalb von 72 Stunden ... 21
2.2.3.2 Zwischenberichte alle zwei Wochen ... 21
2.2.3.3 Abschlussbericht nach Aufklärung des Hackerangriffs oder sonstigen Sicherheitsvorfalls ... 22
2.2.4 Folgen von Defiziten bei der Erfüllung der Meldepflicht nach Art. 33 DSGVO ... 22

2.3 Strafanzeige als technisch-organisatorische Maßnahme nach Hackerangriff? ... 22

2.3.1 Gesetzliche Mitteilungspflichten ... 23
2.3.2 Rolle der Datenschutzaufsichtsbehörden ... 24
2.3.3 Strafanzeige als technisch-organisatorische Maßnahme ... 25
2.3.4 Fazit ... 26

3 Künstliche Intelligenz ... 27

3.1 Allgemeines ... 27

3.1.1 KI-Verordnung ... 27
3.1.2 Tätigkeit der Stabsstelle Digitales & KI ... 28

3.2 Beratungsanfragen in Zusammenhang mit Künstlicher Intelligenz ... 29

3.2.1 Ausgangspunkt: Einordnung der Beteiligten in das datenschutzrechtliche Rollenmodell ... 30
3.2.2 Rechenschaftspflicht nach Art. 5 Abs. 2 DSVGO ... 32
3.2.3 Rechenschaftspflicht im Lichte der EDSA-Stellungnahme 28/2024 ... 32
3.2.4 Rechtmäßigkeitsgrundsatz des Art. 5 Abs. 1 Buchst. a in Verbindung mit Art. 6 Abs. 1 UAbs. 1 DSGVO ... 33
3.2.4.1 Nutzung eines KI-Systems oder KI-Modells als Betriebsmittel ... 33
3.2.4.2 KI-Nutzung und datenschutzrechtliche Generalklausel ... 35
3.2.4.3 Eigenes Initialtraining und Weiter-/Nachtraining von KI-Systemen oder KI-Modellen ... 35
3.2.4.4 Initialtraining und Weiter-/Nachtraining von KI-Systemen oder KI-Modellen durch Dritte zu eigenen Zwecken ... 36
3.2.4.5 Grenzen des Rückgriffs auf die Einwilligung ... 36
3.2.4.6 Art. 9 DSGVO-Daten ... 37

3.2.5 Transparenz und Betroffenenrechte ... 39
3.2.6 Künstliche Intelligenz und Art. 22 DSGVO ... 39
3.2.7 Weitere Entwicklungen ... 40

3.3 KI ohne Grenzen? Einsatz von Drittlandsprodukten in der bayerischen Verwaltung ... 40

3.3.1 Datenschutzrechtliche Anforderungen ... 41
3.3.1.1 Speziell: datenschutzrechtliche Anforderungen an Drittlandanbieter ... 42
3.3.1.2 Speziell: datenschutzrechtliche Anforderungen an bayerische öffentliche Stellen als Betreiber ... 43
3.3.2 KI-Verordnung und Cybersicherheit ... 46

4 Polizei, Justiz, Verfassungsschutz ... 47

4.1 Einsatz von Vertrauenspersonen und Verdeckten Ermittlern ... 47

4.2 Verwarnung eines Polizeipräsidiums wegen rechtswidriger Ausschreibung zur „Kontrolle, soweit nach Polizeirecht zulässig“ ... 48

4.3 Bodycam-Einsatz in Bezirkskrankenhäusern ... 50

4.4 Unzulässige Datenübermittlung an die Mutter einer Beschuldigten ... 52

4.5 Freiwillige Angaben im Ordnungswidrigkeitenverfahren ... 52

4.6 Offenlegung des Tatvorwurfs einer Ordnungswidrigkeit gegenüber dem Arbeitgeber des Betroffenen ... 53

4.7 Unzulässige Datenübermittlung an die Presse im Zusammenhang mit einer Versammlung ... 54

4.8 Prüfung eines abgelehnten Auskunftsantrags beim Bayerischen Landesamt für Verfassungsschutz ... 54

4.9 Prüfung der Umsetzung einer in Aussicht gestellten Löschung von Speicherungen des Bayerischen Landesamtes für Verfassungsschutz ... 55

4.10 Verwarnung einer Staatsanwaltschaft wegen fälschlicher Nennung des Namens einer nicht mehr beschuldigten Person in staatsanwaltschaftlichen Schreiben ... 56

4.11 Zu lange Aufbewahrung einer Strafakte ... 57

5 Allgemeine Innere Verwaltung ... 58

5.1 Wärmeplanungsgesetz: Umsetzung in Bayern ... 58

5.1.1 Datenverarbeitungsbefugnisse der planungsverantwortlichen Stelle ... 58
5.1.2 Planungsverantwortliche Stellen als Schaltstellen bei der Umsetzung der Wärmeplanung ... 59
5.1.3 Datenschutzrechtliche Generalklausel oder Einwilligungen taugen nicht als zusätzliche Datenverarbeitungsbefugnis ... 60
5.1.4 Unterstützung der bayerischen Gemeinden durch staatliche Zurverfügungstellung von Bedarfsdaten ... 61

5.2 Bürgerversammlung, Bürgerbegehren, Bürgerantrag: datenschutzkonformer Umgang mit den Unterschriftenlisten ... 61

5.2.1 Unterschriftenliste nicht pauschal Element der Sitzungsvorbereitung ... 62
5.2.2 Anforderungen an eine Einsichtnahme in die Unterschriftenliste durch den Gemeinderat gemäß Art. 30 Abs. 3 GO ... 62
5.2.3 Kein schutzwürdiges Interesse Dritter am Inhalt einer Unterschriftenliste ... 63

5.3 Datenschutz bei der Ortschronik ... 64

5.4 Drohneneinsatz zur Luftbilderstellung für kommunale Aufgaben ... 66

5.4.1 Ausgangspunkt: Personenbezug von Luftbildaufnahmen ... 66
5.4.2 Erfordernis einer Rechtsgrundlage ... 67
5.4.2.1 Spezialregelung vs. Generalklausel ... 68
5.4.2.2 Besondere Eingriffsintensität der Luftbildaufnahmen ... 68
5.4.2.3 Eingriffsmildernde Maßnahmen ... 69
5.4.2.4 Alternative: Einwilligung ... 69

5.5 Erneut Kameraparken: öffentlich-rechtliche Ausgestaltung der Benutzung sowie Einschaltung privater Dienstleister ... 70

5.5.1 Öffentlich-rechtliche Ausgestaltung der Benutzung ... 70
5.5.2 Einschaltung privater Dienstleister ... 71

5.6 Auch eine Aktiengesellschaft kann eine öffentliche Stelle sein ... 72

5.6.1 Warum ist die Unterscheidung zwischen öffentlicher und nichtöffentlicher Stelle wichtig? ... 72
5.6.2 Was eine bayerische öffentliche Stelle ist, definiert Art. 1 BayDSG ... 72
5.6.3 Aktiengesellschaft als öffentliche Stelle gemäß Art. 1 Abs. 2 Satz 1 BayDSG ... 73
5.6.3.1 Beteiligung einer juristischen Person des öffentlichen Rechts ... 74
5.6.3.2 Aufgabe der öffentlichen Verwaltung ... 74
5.6.3.3 Beherrschung durch eine juristische Person des öffentlichen Rechts ... 74
5.6.4 Fazit ... 75

6 E-Government, öffentliche Register ... 76

6.1 Gesetzgeberischer Handlungsbedarf für „Geoportale“ (Kartenviewer) ... 76

6.1.1 Solarpotenzialkataster ... 76
6.1.2 Datenschutzrechtliche Relevanz ... 76
6.1.3 Geeignete Rechtsgrundlage für die Veröffentlichung ... 77
6.1.3.1 Anhörungserfordernis des Bayerischen Umweltinformationsgesetzes ... 77
6.1.3.2 Geltung des Bayerischen Geodateninfrastrukturgesetzes für Veröffentlichungen (nur) im Geoportal des Landes ... 78
6.1.4 Keine neuen Veröffentlichungsbefugnisse aufgrund der Durchführungsverordnung (EU) 2023/138 zur sogenannten PSI-Richtlinie ... 78
6.1.5 Ausblick ... 79

6.2 Digitalisierung des Wasserbuchs ... 79

6.3 Transparenz bei der Digitalisierung von Planverfahren: Einführung der digitalen Plattform „DiPlanung“ ... 81

6.3.1 Zweck und Hintergrund der digitalen Plattform „DiPlanung“ ... 81
6.3.2 Einwilligung keine Rechtsgrundlage bei der Datenverarbeitung ... 82
6.3.3 Verarbeitungen in gemeinsamer Verantwortlichkeit ... 82
6.3.4 Datenschutzfreundliche Voreinstellungen bei der Ausgestaltung im Detail ... 83

6.4 Meldedatenübermittlung zur Rundfunkfinanzierung ... 83

6.4.1 Beteiligte an den Datenübermittlungen ... 83
6.4.1.1 Meldebehörden ... 83
6.4.1.2 Landesrundfunkanstalt/Beitragsservice ... 84
6.4.2 Meldedatenübermittlungen an die Landesrundfunkanstalt ... 84
6.4.2.1 Meldedatenerhebung durch die Landesrundfunkanstalt, korrespondierende Datenübermittlung durch die Meldebehörde ... 85
6.4.2.2 Regelmäßige Datenübermittlungen durch die Meldebehörde ... 85
6.4.2.3 Periodischer Datenabgleich mit den Melderegistern ... 87
6.4.3 Grundsätzlich kein Widerspruch möglich ... 88

6.4.4 Keine Einwilligung erforderlich ... 88
6.4.5 Zweckbindungen ... 88
6.4.6 Schadensersatz ... 89

7 Gesundheitsverwaltung ... 90

7.1 Datenschutz im Zusammenhang mit freiwilligen Beratungsangeboten der Gesundheitsämter ... 90

7.2 Datenübermittlung an einen externen Gutachter bei Beurteilung der Dienstfähigkeit ... 92

7.2.1 Verpflichtung zur Dienstfähigkeits(zusatz)begutachtung ... 92
7.2.2 Zulässigkeit der Datenübermittlung an externe Zusatzgutachter: Ausgangslage ... 93
7.2.3 Einschränkung durch Art. 27 GDG ... 93
7.2.4 Ergebnis im Beschwerdefall ... 94

8 Öffentliche Krankenhäuser ... 95

8.1 Zuordnung einer wissenschaftlichen Einrichtung einer Universität zu einem Universitätsklinikum und Übertragung der Institutsdaten ... 95

8.1.1 Zuordnung von Einrichtungen zu einem Universitätsklinikum ... 95
8.1.2 Übertragung der Institutsdaten als rechtfertigungsbedürftige Übermittlung von personenbezogenen Daten? ... 96
8.1.2.1 Verarbeitungsbegriff der Datenschutz-Grundverordnung ... 96
8.1.2.2 Besondere Fallkonstellationen, in denen das Vorliegen einer „Verarbeitung“ verneint werden kann ... 97
8.1.3 Sonstige datenschutzrechtliche Anforderungen an die Übernahme von Datenbeständen ... 98

8.2 Aufbewahrung und Löschung von Patientenunterlagen in Krankenhäusern ... 99

8.2.1 Aufbewahrungsfristen für Patientenunterlagen ... 99
8.2.2 Vernichtung beziehungsweise Löschung von Patientenunterlagen ... 100
8.2.3 Keine pauschale 30-jährige Aufbewahrung von Patientenunterlagen für Rechtsverfolgungszwecke ... 101
8.2.4 Löschung im konkreten Fall, aber weiterhin uneinheitliche Praxis ... 101

8.3 „Korrektur“ von Arztbriefen ... 102

8.3.1 Antrag auf „Korrektur“ als Antrag auf Löschung zu verstehen ... 102
8.3.2 Ein Anspruch auf Löschung ist grundsätzlich denkbar ... 103
8.3.3 Ausnahmen vom Recht auf Löschung sind zu beachten ... 104

8.4 CD-ROM als Kopie personenbezogener Daten im Krankenhausbereich? ... 104

8.4.1 Vorab: Verhältnis von Art. 15 DSGVO und § 630g BGB ... 105
8.4.2 Datenschutzrechtlicher Ausgangspunkt: Anforderungen an die Form einer Datenkopie nach Art. 15 Abs. 1, Abs. 3 DSGVO ... 105
8.4.2.1 Keine Anwendung der Vorgaben zur Darstellungsweise von Informationen ... 105
8.4.2.2 Formvorgabe des Art. 12 Abs. 1 Satz 2 DSGVO und Sonderregelung ... 106
8.4.2.3 Gestaltungsspielraum des Verantwortlichen ... 106
8.4.3 Besonderheiten des medizinischen Bereichs ... 107
8.4.4 Ergebnis ... 107

8.5 Videoüberwachung in psychiatrischen Krankenhäusern ... 108

8.5.1 Landeskrankenhausrecht enthält keine hinreichende Rechtsgrundlage ... 108
8.5.2 Spezialgesetzliche Vorschriften im Fall öffentlich-rechtlicher Unterbringungen ... 109
8.5.3 Vorzugswürdig: Videoüberwachung aufgrund einer Einwilligung der betroffenen Person ... 109
8.5.4 Anwendung der allgemeinen gesetzlichen Vorschrift über Videoüberwachungen? ... 110
8.5.5 Nur in Ausnahmefällen: Schutz lebenswichtiger Interessen als Rechtsgrundlage ... 111

9 Gesetzliche Krankenversicherung ... 112

9.1 Auskunft von Diagnosen in der Patientenquittung gesetzlicher Krankenkassen ... 112

9.1.1 Ausgangspunkt: Was ist eine „Patientenquittung“? ... 112
9.1.2 Umfang der Auskunft nach § 305 Abs. 1 Satz 1 SGB V ... 113
9.1.3 Technische Schwierigkeiten bei der Umsetzung ... 113
9.1.4 Exkurs: Zugangsbeschränkung zu Diagnosedaten in der ePA ... 114

9.2 Berichtigung von Diagnosedaten bei gesetzlichen Krankenkassen ... 114

9.2.1 Erhebung von Diagnosedaten durch gesetzliche Krankenkassen ... 115
9.2.2 Grundsätzlich keine Berichtigung der ursprünglich übermittelten Diagnosedaten und keine erneute Übermittlung an die Krankenkassen ... 115
9.2.3 Ausnahme: Verwendung berichtigter Diagnosedaten durch die Krankenkassen bei Unterrichtung der versicherten Person oder Übermittlung an Dritte ... 116
9.2.4 Ergebnis der Beschwerdeverfahren: Anpassung der Berichtigungsverfahren der betroffenen Krankenkasse ... 117

9.3 Neues zum Mammographie-Screening-Programm ... 117

9.3.1 Aktuelle Kurz-Information „Einladungen zum Mammographie-Screening“ ... 117
9.3.2 Online-Kontaktformular ... 118

10 Soziales ... 119

10.1 Schwärzung auch durch Weißung bei der Auskunftserteilung? ... 119

10.1.1 Unkenntlich gemachte Inhalte ... 120
10.1.1.1 Bemerkungen ohne Personenbezug ... 120
10.1.1.2 Bemerkungen mit Personenbezug ... 120
10.1.2 Transparenzprobleme bei Unkenntlichmachungen mittels Weißungen ... 121
10.1.2.1 Bezug des Transparenzgrundsatzes zu personenbezogenen Daten ... 121
10.1.2.2 Kein Transparenzproblem bei Informationen ohne Personenbezug ... 122
10.1.2.3 Auswirkungen des Transparenzproblems ... 123
10.1.2.4 Transparenzverstoß ... 123
10.1.3 Abschließende Bemerkungen ... 124

10.2 Offenlegung von Angaben über die Höhe des Einkommens von Kindern bei Verfahren zur Gewährung von Grundsicherung an die Eltern ... 124

10.2.1 Übergang von Unterhaltsansprüchen auf den Träger der Sozialhilfe ... 125
10.2.2 Befugnis des Sozialleistungsträgers zur Offenlegung von allgemein gehaltenen Angaben über das Einkommen ... 125

10.3 Eignungsfeststellung im Fall der Kindertagespflege ... 126

10.3.1 Voraussetzungen einer Erlaubnis zur Kindertagespflege ... 127
10.3.2 Abschließende Regelung über die Erhebung von Daten im Hinblick auf strafrechtliche Verurteilungen ... 127
10.3.3 Keine abschließende Regelung im Hinblick auf andere Aspekte der Eignung ... 128
10.3.4 Datenerhebung aufgrund Einwilligung zweifelhaft ... 128
10.3.5 Empfehlung: Datenerhebung aufgrund und im Rahmen der bestehenden gesetzlichen Befugnisse ... 129

10.4 Datenanforderungen von Ausländerbehörden bei anderen öffentlichen Stellen ... 130

10.4.1 Übermittlung von Sozialdaten eines Jobcenters an eine kommunale Ausländerbehörde ... 130
10.4.2 Weiterer Fall zur Datenerhebung durch eine bayerische Ausländerbehörde ... 131
10.4.2.1 Verletzung der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO ... 131
10.4.2.2 Meldepflicht gemäß Art. 33 DSGVO ... 132

10.5 Datenschutz bei der Bearbeitung von Unfallanzeigen ... 133

10.5.1 „In Kenntnis setzen“ über Unfallanzeigen: § 193 Abs. 5 Satz 2 SGB VII ... 133
10.5.2 Bereichsspezifische Verarbeitungsbefugnisse ... 134
10.5.3 Art. 4 Abs. 1 BayDSG ... 135
10.5.3.1 Verarbeitung von Gesundheitsdaten ... 135
10.5.3.2 Nur geringfügige Eingriffe ... 135
10.5.3.3 Aufgabenerfüllung ... 136
10.5.3.4 Erforderlichkeit ... 137
10.5.4 Ergebnis ... 138

11 Personalverwaltung ... 139

11.1 Novellierung des Bayerischen Gleichstellungsgesetzes ... 139

11.1.1 Gleichstellungskonzepte ... 139
11.1.2 Informationsrechte der Gleichstellungsbeauftragten ... 141
11.1.3 Weitere Änderungen mit Datenschutzbezug ... 143
11.1.4 Fazit ... 144

11.2 Feststellung der Verfassungstreue bei Bewerberinnen und Bewerbern für den bayerischen öffentlichen Dienst ... 144

11.2.1 Hintergrund und bisherige Rechtslage ... 144
11.2.2 Neuregelung in Art. 19 Abs. 2 BayBG ... 145
11.2.3 Datenschutzrechtliche Bewertung ... 146
11.2.4 Fazit ... 148

11.3 Beschäftigtennamen in dienstlichen Schreiben ... 149

11.3.1 Grundlegendes zur Verarbeitung von Beschäftigtendaten in dienstlichen Schreiben ... 149
11.3.2 Vor- und Nachnamen in dienstlichen Schreiben ... 150
11.3.3 Eigenhändige Unterschriften in dienstlichen Schreiben ... 150
11.3.4 Vor- und Nachnamen in dienstlichen E-Mail-Adressen ... 151
11.3.5 Abschließende Bemerkungen ... 152

11.4 „Sammelermächtigungen“ für Bedienstete der Jugendämter ... 152

12 Schulen ... 155

12.1 Beratung zur Änderung schulrechtlicher Vorschriften ... 155

12.1.1 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen ... 155
12.1.2 Bayerische Schulordnung ... 156
12.1.3 Kultusministerielle Bekanntmachungen ... 156

12.2 Weiterleitung trotz Vertraulichkeitsbitte ... 156

12.3 Hausbesuch vom Hausmeister ... 157

12.4 Heimliches Mithören eines Telefonats ... 158

12.5 Werbung für das Landheim ... 159

13 Informationsfreiheit ... 161

13.1 Einsicht in die nicht vorhandene Konzeptplanung ... 161

13.2 Überprüfung von Schwärzungen ... 161

13.3 Auskunftsantrag und Datenschutz ... 162

14 Technik und Organisation ... 165

14.1 Webarchive datenschutzgerecht füttern ... 165

14.1.1 Warum interessiert sich der Datenschutz für Webarchive? ... 165
14.1.2 Wie schaut die aktuelle Entwicklung aus? ... 166
14.1.3 Gibt es nun etwas zu tun? ... 167

14.2 Datenschutz beim Versand von Brief und Paket ... 169

14.2.1 Verarbeitung personenbezogener Daten beim klassischen (analogen) Versand von Briefen und Paketen ... 169
14.2.2 Häufig auftretende Datenschutzvorfälle ... 170
14.2.3 Prüfschritte zur Gewährleistung eines angemessenen Schutzniveaus vor Postversand ... 171

14.3 Datenschutzkonzepte für Digitalisierungsvorhaben ... 174

14.4 Synergien Datenschutz und Informationssicherheit ... 175

14.5 Prüfung der Verarbeitung von Kernbereichsdaten nach Art. 48 Abs. 5 Bayerisches Digitalgesetz ... 176

14.6 Unzureichende Schwärzung: QR-Code enthielt personenbezogene Daten ... 177

14.7 Verwarnungen nach Art. 58 Abs. 2 Buchst. b DSGVO ... 178

14.7.1 Verwarnung aufgrund unzureichender technisch-organisatorischer Schutzmaßnahmen einer Klinik bei einem Cybervorfall ... 178
14.7.2 Verwarnung wegen unzureichender Nutzertrennung bei Nutzung eines Gastzuganges in einem Online-Antragsverfahren ... 179
14.7.3 Zwei Landratsämter wurden wegen wiederholter Missachtung datenschutzrechtlicher Vorgaben bei der E-Mail-Kommunikation verwarnt ... 180

14.8 Beanstandung auf Grund mehrfacher Datenschutzverstöße im Rahmen des Streamings einer Stadtratssitzung ... 182

14.9 Meldungen von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DSGVO ... 183

14.9.1 Patientin irrtümlich von der Krankenkasse als verstorben gemeldet ... 183
14.9.2 Automatisierter Abruf von Grundbuchdaten ohne erforderliche Zustimmung ... 184

14.10 Zuletzt: Aufregung wegen öffentlich zugänglicher Briefe vom Christkind ... 185

15 Datenschutzkommission ... 186

16 Ländervertreter im EDSA ... 188

Abkürzungsverzeichnis ... 190

Stichwortverzeichnis ... 191

Hinweis zu Abkürzungen

Abkürzungen von Rechtstexten sind im jeweiligen Beitrag bei der erstmaligen Nennung aufgelöst. Andere Abkürzungen enthält das Abkürzungsverzeichnis am Ende des Tätigkeitsberichts. Die folgenden Abkürzungen werden durchgehend verwendet:

BayDSG	Bayerisches Datenschutzgesetz vom 15. Mai 2018 (GVBl. S. 230), zuletzt geändert durch § 2 Gesetz vom 25. Juli 2025 (GVBl. S. 254)
DSGVO	Datenschutz-Grundverordnung; die vollständige Bezeichnung lautet: 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 (ABl. L 119 vom 4. Mai 2016, S. 1, berichtigt ABl. L 314 vom 22. November 2016, S. 72, ABl. L 127 vom 23. Mai 2018, S. 2, und ABl. L 74 vom 4. März 2021, S. 35)
RLDSJ	Datenschutz-Richtlinie für Polizei und Strafjustiz; die vollständige Bezeichnung lautet: Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4. Mai 2016, S. 89, berichtigt ABl. L 127 vom 23. Mai 2018, S. 9, und ABl. L 74 vom 4. März 2021, S. 36)

1 Überblick

1.1 Über diesen Tätigkeitsbericht

Als Datenschutzaufsichtsbehörde des bayerischen öffentlichen Sektors nimmt der Bayerische Landesbeauftragte für den Datenschutz seit 1978 die Datenschutzaufsicht bei einigen tausend bayerischen öffentlichen Stellen wahr. Das Spektrum reicht von den Staatsministerien über die Landesämter und die Behörden der Mittelstufe bis zu den unteren Verwaltungsbehörden, etwa Landratsämtern oder staatlichen Schulen. Die Zuständigkeit des Landesbeauftragten erfasst weiterhin die bayerischen Kommunen, also Bezirke, Kreise, Städte und Gemeinden, Verwaltungsgemeinschaften oder Zweckverbände, ferner Universitäten und andere Hochschulen, zahlreiche Krankenhäuser aller Versorgungsstufen und die Sozialleistungsträger der Landesebene. Auch bei der Bayerischen Polizei, dem Landesamt für Verfassungsschutz, den Staatsanwaltschaften, bei Justizverwaltungen und Justizvollzugsanstalten führt der Landesbeauftragte die Datenschutzaufsicht. Mit Beteiligungsunternehmen der öffentlichen Hand und ganz kleinen öffentlichen Stellen wie Jagdgenossenschaften oder bevollmächtigten Bezirksschornsteinfegern schließt sich der Kreis noch lange nicht.[1]

Datenschutzprobleme können bei allen diesen öffentlichen Stellen auftreten. Und weil das Datenschutzrecht des öffentlichen Sektors trotz aller unionsrechtlichen Harmonisierung weiterhin in vielerlei Hinsicht national geprägt ist, werde ich als Landesbeauftragter in Beschwerden, Beratungsanfragen oder anderen Prüfvorgängen immer wieder mit bereichsspezifischen Regelungen konfrontiert, deren Anwendung nicht nur Vertrautheit mit der jeweiligen Verwaltungsmaterie, sondern auch eine diesem Rahmen angepasste Herangehensweise erfordert. Die Datenschutzaufsicht im öffentlichen Sektor kennt zwar einige Standardkonstellationen; überwiegend ist sie aber kein „Massengeschäft", sondern „Maßarbeit".

Im öffentlichen Sektor genügt es für eine Datenschutzaufsichtsbehörde also nicht, kompetent mit der Datenschutz-Grundverordnung und dem allgemeinen nationalen Datenschutzrecht umzugehen. Polizeirecht, Schulrecht, Sozialrecht, Recht des öffentlichen Dienstes, der Krankenhäuser oder der Gesundheitsverwaltungen, Registerrecht oder Kommunalrecht – alle diese Materien enthalten wie noch viele weitere eigene Vorschriften mit datenschutzrechtlichem Gehalt, als einzelne Normen, als Gruppen, hin und wieder sogar als ein ganzes „Sonderrecht". Ihre Wirkungen entfalten solche Vorschriften stets im Verbund mit der Datenschutz-Grundverordnung und dem allgemeinen nationalen Datenschutzrecht.

Ich kann in meiner Behörde auf einen Wissens- und Erfahrungsschatz zurückgreifen, der erhalten, gepflegt, kontinuierlich aus- und weitergebaut werden muss. Das kommt dann nicht nur dem Datenschutzniveau im bayerischen öffentlichen Sektor

[1] Ein gängiger Gesetzeskommentar entfaltet das Spektrum der bayerischen öffentlichen Stellen in einem 97 Randnummern langen Glossar, bemerkt dazu aber: „Das Glossar gibt einen Überblick [...]. Es kann weder die Staatsbehörden vollständig erfassen noch auch nur annähernd die Vielfalt im staatsmittelbaren Bereich abbilden, insbesondere was die Beteiligungsunternehmen der bayerischen Kommunen betrifft" (Engelbrecht, in Schröder, Bayerisches Datenschutzgesetz, 2021, Art. 1 Rn. 60 ff.).

zugute, sondern trägt auch wesentlich – insbesondere durch die Tätigkeitsberichte und andere Publikationen vermittelt – zum föderalen Wettbewerb um gute Lösungen bei.

Eine wichtige Voraussetzung dafür bildet der bewährte Personalaustausch mit den Ressorts der Bayerischen Staatsregierung. Erfahrene Referentinnen und Referenten insbesondere aus den Staatsministerien nahmen auch im aktuellen Berichtszeitraum wieder ihren Dienst in meiner Geschäftsstelle auf oder kehrten – nach meist drei bis fünf Jahren – mit gefestigter Datenschutzkompetenz wieder zurück. Ich hoffe, dass auch weiterhin viele Ressorts am Personalaustausch teilnehmen und so die in Bayern seit Jahren bewährte praxisnahe, nicht „entrückte" Datenschutzarbeit mit ermöglichen.

Der vorliegende Tätigkeitsbericht ist umfangreicher ausgefallen als in den Vorjahren. Gleichwohl habe ich aus der Gesamtheit der Prüfvorgänge wieder nur einen kleinen Teil ausgewählt. Viele der Fälle machen deutlich: Die zu bewältigen Probleme „stecken" oftmals in den Details des Fachrechts.

Ein Beispiel bildet gleich der Eingangsbeitrag zum **allgemeinen Datenschutzrecht**, der die Spielbanken der Staatlichen Lotterie- und Spielbankverwaltung betrifft (Nr. 2.1). Hier stellte sich die grundsätzliche Frage, wie der datenschutzrechtrechtliche Auskunftsanspruch (Art. 15 DSGVO) zu erfüllen ist, wenn zu einer Kundin oder einem Kunden eine Dokumentation nach dem Geldwäschegesetz vorliegt. Zwei weitere Beiträge haben Reaktionen bayerischer öffentlicher Stellen auf Cyberangriffe zum Gegenstand; eine Meldung nach Art. 33 DSGVO ist hier oftmals geboten (Nr. 2.2), eine Strafanzeige bei einer zuständigen Strafverfolgungsbehörde kann eine sinnvoll ergänzende Option sein (Nr. 2.3).

An Bedeutung für die Aufsichtspraxis hat im Berichtsjahr das Thema **„Künstliche Intelligenz"** gewonnen. Mein Tätigkeitsbericht skizziert die Entwicklungen des Regulierungsrechts im Jahr 2025 (Nr. 3.1), gibt einen Überblick zu Beratungsanfragen von allgemeinem Interesse (Nr. 3.2) und geht insbesondere auf die datenschutzrechtlichen Implikationen beim Einsatz von KI-Produkten aus Drittländern ein (Nr. 3.3).

Im Bereich von **Polizei und Justiz** kann ich etwa über eine Prüfung zum Einsatz von Vertrauenspersonen und Verdeckten Ermittlern berichten (Nr. 4.1). In mehreren Fällen des unrechtmäßigen Einsatzes polizeilicher Bodycams in psychiatrischen Kliniken der Bezirke habe ich Beanstandungen aussprechen müssen (Nr. 4.3). Eine Verwarnung erging gegenüber einer Staatsanwaltschaft, die einem Dritten in einem Ermittlungsverfahren den Namen einer nicht mehr beschuldigten Person offengelegt hatte (Nr. 4.10).

Die **Allgemeine Innere Verwaltung** begegnet Bürgerinnen und Bürgern insbesondere in den Rathäusern. Hier war ich mehrmals mit der Gewinnung der Datenbasis für kommunale Wärmeplanungen befasst. Gezielte Datenerhebungen einiger Gemeinden stießen auf datenschutzrechtliche Grenzen. Dennoch konnte ich gemeinsam mit dem Wirtschaftsministerium eine Lösung entwickeln, bei der eine qualitativ hochwertige Planungsgrundlage mit abstrakt errechneten Bedarfsdaten erreicht, eine individuelle „Ausforschung" aber vermieden wird (Nr. 5.1). Beschäftigt haben mich weiterhin Datenschutzfragen beim Umgang mit Unterschriftenlisten im Zusammenhang mit Bürgerbegehren, Bürgeranträgen und Bürgerversammlungen (Nr. 5.2) sowie die Erstellung von Ortschroniken (Nr. 5.3).

Infolge der fortschreitenden Digitalisierung von Verwaltungsdienstleistungen stellen sich regelmäßig neue Datenschutzfragen zum **E-Government**. Das gilt in besonderem Maße für Geodatendienste. Im Berichtsjahr standen hier die Solarpotenzialkataster im Fokus (Nr. 6.1). Bei der Einführung der digitalen Plattform „DiPlanung“ für die Digitalisierung von Planungs- und Beteiligungsverfahren konnte ich im Austausch mit dem Bauministerium Verbesserungen erwirken, die den Datenschutzrechten der Bürgerinnen und Bürger zugutekommen (Nr. 6.3).

Der Bereich **„Soziales und Gesundheit“** bildet in diesem Jahr einen Schwerpunkt meines Tätigkeitsberichts.

So war habe ich etwa die **Gesundheitsverwaltung** beraten, wie mit personenbezogenen Hinweisen aus der Bevölkerung umzugehen ist, die Anlass zur Unterbreitung freiwilliger Beratungsangebote geben (Nr. 7.1). Bei den **öffentlichen Krankenhäusern** war das rechtliche „Schicksal“ eines Bestands von Gesundheitsdaten zu klären, wenn ein Institut von einer bayerischen Universität an ihr Klinikum umgegliedert wird (Nr. 8.1). Fälle zur Aufbewahrung und Löschung von Patientendaten (Nr. 8.2), zur „Korrektur“ von Arztbriefen (Nr. 8.3) sowie zum Auskunftsmittel „CD-ROM“ (Nr. 8.4) betrafen den Krankenhausalltag. Bei den bayerischen **gesetzlichen Krankenkassen** war ich zum Beispiel mit Diagnosen in der sog. „Patientenquittung“ (Nr. 9.1) oder mit der Berichtigung von Diagnosedaten befasst (Nr. 9.2).

Im **Sozialdatenschutz** stellte sich die auch darüber hinaus bedeutsame Frage, ob eine Schwärzung auch eine Weißung sein darf (Nr. 10.1). In mehreren Fällen habe ich Datenerhebungen von Sozialleistungsträgern bei „vorgeschossenem“ Elternunterhalt geprüft (Nr. 10.2). Weitere Beiträge betreffen die Sachverhaltsermittlung vor Erteilung einer Erlaubnis zur Kindertagespflege (Nr. 10.3) sowie Datenflüsse zwischen Ausländerbehörden und Sozialleistungsträgern (Nr. 10.4). Schließlich konnte ich eine Position zu der Frage formulieren, inwieweit Fachkräfte für Arbeitssicherheit bei bayerischen öffentlichen Stellen an personenbezogene Informationen zu Arbeitsunfällen gelangen können (Nr. 10.5).

Was den **Personaldatenschutz** betrifft, ist von zwei Gesetzgebungsverfahren zu berichten: Bei der Novellierung des Bayerischen Gleichstellungsgesetzes konnte ich mich frühzeitig einbringen; die darin zum Schutz von Datenschutzrechten enthaltenen Vorschriften erfuhren eine behutsame Fortentwicklung (Nr. 11.1). Eine Neuregelung im Bayerischen Beamtengesetz zur Prüfung der Verfassungstreue in Einstellungsverfahren habe ich aus Datenschutzsicht intensiv kritisch begleitet (Nr. 11.2). Umfassend dargestellt habe ich meine Prüfungs- und Beratungspraxis zum Thema „Beschäftigtennamen in dienstlichen Schreiben“ (Nr. 11.3).

Datenschutzfragen stellten sich auch bei den bayerischen **öffentlichen Schulen**. Prüfvorgänge betrafen etwa Umfeldermittlungen durch einen Schulhausmeister nach Zweifeln an der Krankmeldung eines Schulkindes (Nr. 12.3) oder die Wahrung von Vertraulichkeit, wenn sich Eltern zur Überprüfung einer schulischen Maßnahme an die Schulaufsichtsbehörde wenden (Nr. 12.2). Zudem konnte ich in Rechtsetzungsverfahren aus dem Schulrecht datenschutzrechtliche Verbesserungen erreichen (Nr. 12.1).

Das **Informationsfreiheit** gewährende allgemeine Recht auf Auskunft ist in Art. 39 BayDSG geregelt und daher ebenfalls von meiner Kontrollzuständigkeit erfasst. Insofern waren etwa die Fragen zu klären, in welchen Grenzen Zugang auch

zu personenbezogenen Daten Dritter erlangt werden kann (Nr. 13.3), und in welchem Umfang eine öffentliche Stelle Informationen schwärzen darf (Nr. 13.2).

Im Bereich des **technisch-organisatorischen Datenschutzes** habe ich schließlich Hinweise zur Gestaltung von Webseiten mit Blick auf eine Archivierung in Webarchiven (Nr. 14.2) und zum Versand von Briefen und Paketen geben können (Nr. 14.2). Ein weiterer Beitrag macht auf mögliche Synergien von Datenschutz und Informationssicherheit aufmerksam (Nr. 14.4). Zwei Verwarnungen zeigen abermals, wie wichtig es für Verantwortliche ist, erforderliche technisch-organisatorische Schutzmaßnahmen konsequent umzusetzen. Das gilt nicht nur, wenn es um die Abwehr von Cyberangriffen geht (Nr. 14.7.1), sondern auch beim ganz alltäglichen E-Mail-Versand (Nr. 14.7.3).

1.2 Neue Beiträge im digitalen Informationsangebot des Landesbeauftragten

Die Erläuterung des datenschutzrechtlichen Handlungsrahmens in einem breit gefächerten Informationsangebot für Verantwortliche des bayerischen öffentlichen Sektors ist mir seit jeher ein besonderes Anliegen.

Im Berichtsjahr entstanden große Teile zweier **Orientierungshilfen**, die den Einsatz Künstlicher Intelligenz bei bayerischen öffentlichen Stellen sowie die Anwendung des Gesundheitsdatennutzungsgesetzes betreffen. Da ich diese Orientierungshilfen erst 2026 veröffentlicht habe, werde ich sie im nächsten Tätigkeitsbericht vorstellen.

In der Reihe der **„Aktuellen Kurz-Informationen“** habe ich im Berichtsjahr die Nummern 57 bis 64 bereitgestellt.

Von meinem zweisprachigen (deutsch/englisch) Newsletter **„Privacy in Bavaria“** konnte ich 2025 erfreulicherweise elf Ausgaben veröffentlichen.

Verantwortliche des bayerischen öffentlichen Sektors, ihre behördlichen Datenschutzbeauftragten und alle anderen am Datenschutz Interessierten erfahren auf meinem **Mastodon-Kanal** https://social.bund.de/@BayLfD tagesaktuell, was es an Neuem gibt.

2 Allgemeines Datenschutzrecht

2.1 Spielbanken Bayern: Datenschutzrechtliche Auskunftsansprüche im Spannungsverhältnis zur Geldwäscheprävention

Bargeldintensiver Betrieb und hohe Umsätze machen Anbieter von Glücksspiel attraktiv für das Einschleusen und „Reinigen" von illegalen Geldern. Vor diesem Hintergrund übernehmen die staatlichen Spielbanken Bayern wichtige Aufgaben zur Verhinderung von Geldwäsche. Zur wirksamen Prävention und Bekämpfung von Geldwäsche und Terrorismusfinanzierung sind sie nach dem Geldwäschegesetz (GwG) verpflichtet, umfassende interne Sicherungsmaßnahmen zu ergreifen und ein risikoorientiertes Verfahren zur Kundenüberwachung zu etablieren. Diese Pflichten dienen dem Ziel, die Integrität des Finanzsystems zu schützen und das Einschleusen illegaler Gelder zu verhindern.

2.1.1 Geldwäscherechtliche Sorgfaltspflichten

Bei Transaktionen ab 2.000 Euro müssen Spielbanken gemäß § 10 Abs. 1, Abs. 5 GwG in Verbindung mit § 2 Nr. 15 GwG insbesondere die Identität des Vertragspartners überprüfen und weitere Sorgfalts- und Abklärungspflichten erfüllen. Diese allgemeinen Sorgfaltspflichten regelt § 10 Abs. 1 GwG:

> **§ 10 GwG**
> **Allgemeine Sorgfaltspflichten**
> (1) Die allgemeinen Sorgfaltspflichten sind:
> 1. die Identifizierung des Vertragspartners und gegebenenfalls der für ihn auftretenden Person nach Maßgabe des § 11 Absatz 4 und des § 12 Absatz 1 und 2 sowie die Prüfung, ob die für den Vertragspartner auftretende Person hierzu berechtigt ist,
> 2. die Abklärung, ob der Vertragspartner für einen wirtschaftlich Berechtigten handelt, und, soweit dies der Fall ist, die Identifizierung des wirtschaftlich Berechtigten nach Maßgabe des § 11 Absatz 5 und des § 12 Absatz 3 und 4; dies umfasst in Fällen, in denen der Vertragspartner keine natürliche Person ist, die Pflicht, die Eigentums- und Kontrollstruktur des Vertragspartners mit angemessenen Mitteln in Erfahrung zu bringen,
> 3. die Einholung und Bewertung von Informationen über den Zweck und über die angestrebte Art der Geschäftsbeziehung, soweit sich diese Informationen im Einzelfall nicht bereits zweifelsfrei aus der Geschäftsbeziehung ergeben,
> 4. die Feststellung mit angemessenen, risikoorientierten Verfahren, ob es sich bei dem Vertragspartner oder dem wirtschaftlich Berechtigten um eine politisch exponierte Person, um ein Familienmitglied oder um eine bekanntermaßen nahestehende Person handelt, und
> 5. die kontinuierliche Überwachung der Geschäftsbeziehung einschließlich der Transaktionen, die in ihrem Verlauf durchgeführt werden, zur Sicherstellung, dass diese Transaktionen übereinstimmen
>   a) mit den beim Verpflichteten vorhandenen Dokumenten und Informationen über den Vertragspartner und gegebenenfalls über den wirtschaftlich Berechtigten, über deren Geschäftstätigkeit und Kundenprofil und,
>   b) soweit erforderlich, mit den beim Verpflichteten vorhandenen Informationen über die Herkunft der Vermögenswerte;
>
>   im Rahmen der kontinuierlichen Überwachung haben die Verpflichteten sicherzustellen, dass die jeweiligen Dokumente, Daten oder Informationen unter Berücksichtigung des jeweiligen Risikos im angemessenen zeitlichen Abstand aktualisiert werden.
> [...]

Die konkreten Maßnahmen zur Erfüllung der allgemeinen Sorgfaltspflichten hat der Verpflichtete entsprechend dem Risiko des jeweiligen Vertragspartners, der jeweiligen Geschäftsbeziehung oder der jeweiligen Transaktion zu bestimmen. § 10 Abs. 2 GwG bestimmt insofern:

> **§ 10 GwG**
> **Allgemeine Sorgfaltspflichten**
> […]
> (2) Der konkrete Umfang der Maßnahmen nach Absatz 1 Nummer 2 bis 5 muss dem jeweiligen Risiko der Geldwäsche oder Terrorismusfinanzierung, insbesondere in Bezug auf den Vertragspartner, die Geschäftsbeziehung oder Transaktion, entsprechen. Die Verpflichteten berücksichtigen dabei insbesondere die in den Anlagen 1 und 2 genannten Risikofaktoren. Darüber hinaus zu berücksichtigen haben sie bei der Bewertung der Risiken zumindest
> 1. den Zweck des Kontos oder der Geschäftsbeziehung,
> 2. die Höhe der von Kunden eingezahlten Vermögenswerte oder den Umfang der ausgeführten Transaktionen sowie
> 3. die Regelmäßigkeit oder die Dauer der Geschäftsbeziehung.
>
> Verpflichtete müssen gegenüber den Aufsichtsbehörden auf deren Verlangen darlegen, dass der Umfang der von ihnen getroffenen Maßnahmen im Hinblick auf die Risiken der Geldwäsche und der Terrorismusfinanzierung angemessen ist.
> […]

Mit der Erfüllung der Sorgfaltspflichten kann die Einstufung von Kundinnen und Kunden in interne Risiko- oder Beobachtungslisten verbunden sein, die Prüfung der Herkunft der Mittel sowie die unverzügliche Meldung verdächtiger Transaktionen an die Zentralstelle für Finanztransaktionsuntersuchungen (die beim Zoll eingerichtete „Financial Intelligence Unit“) und gegebenenfalls an Ermittlungs- und Aufsichtsbehörden (vgl. § 43 Abs. 1 GwG).

Die bei Erfüllung der Sorgfaltspflichten entstehenden Aufzeichnungen (vgl. § 8 Abs. 1 GwG) können hinsichtlich der einzelnen Spielbankbesucherinnen und -besucher Identifikationsdaten, Hinweise auf auffällige Vorgänge, Beobachtungen, Risiko- und Verdachtsbewertungen, methodische Details (zum Beispiel Indikatoren für Auffälligkeiten, Schwellenwerte) und anderes mehr enthalten. Ebenso wird aufgezeichnet, wer Zugriff auf diese Daten hatte und an wen sie weitergegeben wurden. Datenschutzrechtlich gesehen, werden dergestalt eine Vielzahl persönlicher Daten aufgezeichnet und gegebenenfalls weitergegeben.

2.1.2 Mögliche Konflikte mit dem datenschutzrechtlichen Auskunftsanspruch

Art. 15 Abs. 1 DSGVO gewährt betroffenen Personen einen Anspruch auf Auskunft über die personenbezogenen Daten, die der Verantwortliche – vorliegend die staatlichen Spielbanken in Bayern – von ihnen verarbeitet. Die im Rahmen der Erfüllung der geldwäscherechtlichen Sorgfaltspflichten anfallenden Aufzeichnungen enthalten regelmäßig personenbezogene Daten gemäß Art. 4 Nr. 1 DSGVO, nämlich „Informationen, die sich auf eine identifizierte oder identifizierbare Person […] beziehen“. Diese werden im Sinne von Art. 4 Nr. 2 DSGVO verarbeitet, da unter diesem weiten Begriff jeder Umgang mit personenbezogenen Daten durch den Verantwortlichen zu verstehen ist, einschließlich des Erfassens, Speicherns oder der Offenlegung dieser Daten gegenüber anderen Stellen. Die Voraussetzungen des Auskunftsanspruchs nach Art. 15 Abs. 1 DSGVO sind somit grundsätzlich erfüllt.

Durch die Erfüllung von Auskunftsansprüchen könnten allerdings auch sensible interne Informationen über Maßnahmen zur Geldwäschebekämpfung bekanntwerden. Auch wenn sich der datenschutzrechtliche Auskunftsanspruch nur auf die Daten der betroffenen Person bezieht, kann schon die Information, welche konkreten Verhaltensweisen der Spielbankbesucherinnen und -besucher als verdächtig aufgezeichnet werden, Schlüsse auf die Ausgestaltung der risikoorientierten Sorgfaltsmaßnahmen der Spielbank zulassen. Das könnte jedoch die Wirksamkeit der Maßnahmen zur Geldwäscheprävention erheblich gefährden. Kriminelle könnten sich darauf einstellen und ihr Verhalten dementsprechend anpassen. Der Erfolg der Geldwäschepräventionsmaßnahmen hängt aber nicht zuletzt entscheidend davon ab, dass die Strategie der Bayerischen Spielbanken und die Kriterien für die Annahme eines Verdachts nicht öffentlich bekannt werden.

2.1.3 Kein vollständiger Ausschluss des Auskunftsanspruchs

Vor diesem Hintergrund wollte die Staatliche Lotterie- und Spielbankverwaltung von mir wissen, ob die staatlichen Spielbanken Bayern datenschutzrechtliche Auskunftsersuchen nach Art. 15 Abs. 1 DSGVO gänzlich und pauschal zurückweisen können. Sie befürchtete insbesondere, dass Auskünfte die geldwäscherechtlichen Präventionsmaßnahmen entwerten könnten. Dieser Meinung konnte ich mich jedoch nicht vollumfänglich anschließen.

— Zunächst ist festzuhalten, dass Art. 15 DSGVO auf Spielbanken auch dann anwendbar ist, wenn es um die Auskunft über personenbezogene Daten geht, die im Zusammenhang mit der Geldwäschebekämpfung verarbeitet werden. Spielbanken können sich insofern nicht auf Art. 2 Abs. 2 Buchst. d DSGVO berufen. Nach dieser Vorschrift gilt die Datenschutz-Grundverordnung nicht für die Verarbeitung von Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung oder Verfolgung von Straftaten. Diese Vorschrift richtet sich an Behörden, die spezifisch für die genannten Zwecke zuständig sind. Die Bayerischen Spielbanken übernehmen bei der Geldwäschebekämpfung jedoch nur eine Hilfsfunktion zugunsten anderer Stellen. Ihre Hauptaufgabe bleibt das Anbieten von Glücksspiel.

— Obwohl die Datenschutz-Grundverordnung somit anwendbar ist und der Auskunftsanspruch nach Art. 15 Abs. 1 DSGVO grundsätzlich greift, wird die Auskunft in vorliegendem Zusammenhang jedoch nicht in jedem Fall uneingeschränkt erteilt. Der Bundesgesetzgeber hat nämlich von der in Art. 23 DSGVO vorgesehenen Möglichkeit zur verhältnismäßigen Beschränkung des Auskunftsrechts Gebrauch gemacht und in § 11a Abs. 2 GwG Meldungen an die Zentralstelle für Finanztransaktionsuntersuchungen auf der Grundlage des Geldwäschegesetzes von der Auskunft nach Art. 15 DSGVO ausdrücklich ausgenommen (vgl. auch § 47 Abs. 1 GwG).

> **§ 11a GwG**
> **Verarbeitung personenbezogener Daten durch Verpflichtete**
> (1) Verpflichtete nach § 2 dürfen personenbezogene Daten nur verarbeiten, soweit dies auf Grundlage dieses Gesetzes für Zwecke der Verhinderung von Geldwäsche und Terrorismusfinanzierung erforderlich ist.
> (2) Soweit ein den Vorschriften dieses Gesetzes unterliegender Verpflichteter nach § 2 personenbezogene Daten für Zwecke gemäß Absatz 1 an die zuständigen Aufsichtsbehörden oder die Personen und Einrichtungen, deren sich die zuständigen Aufsichtsbe-

hörden bei der Durchführung ihrer Aufgaben bedienen, oder an die Zentralstelle für Finanztransaktionsuntersuchungen übermittelt, bestehen die Pflicht zur Information der betroffenen Person nach Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 und das Recht auf Auskunft der betroffenen Person nach Artikel 15 der Verordnung (EU) 2016/679 nicht.
(3) Die Absätze 1 und 2 finden entsprechende Anwendung auf Dritte im Sinne von § 17, auf die ein Verpflichteter zur Erfüllung der allgemeinen Sorgfaltspflichten nach § 10 Absatz 1 Nummer 1 bis 4 zurückgreift.

Angesichts dieses klaren Wortlauts kann § 11a Abs. 2 GwG allerdings nicht zu weiteren Verkürzungen der Auskunft dienen. Das muss auch für Maßnahmen im Vorfeld einer Meldung an die Zentralstelle gelten. Eine solche pauschale Vorwirkung der Meldung kann schon deshalb nicht angenommen werden, weil nicht in jedem Fall der verdachtsunabhängig zu erfüllenden Sorgfaltspflichten später noch eine Meldung an die Zentralstelle für Finanztransaktionsuntersuchungen erfolgt.

– Das bedeutet im Ergebnis trotzdem nicht, dass die Spielbanken Bayern durch die Erfüllung von Auskunftsansprüchen praktisch Gefahr liefen, ihre Kontrollmechanismen zur Geldwäscheprävention auszuhöhlen. Auch wenn, wie gezeigt, ein gänzlicher, pauschaler Ausschluss des Auskunftsrechts nicht in Betracht kommt, ist insbesondere zu berücksichtigen, dass die allgemeinen Datenschutzgesetze auf der Basis von Art. 23 DSGVO den Auskunftsanspruch für bestimmte Konstellationen einschränken. Beispiele für derartige Regelungen sind Art. 10 Abs. 2 Nr. 1 BayDSG und § 29 Abs. 1 Satz 2 Bundesdatenschutzgesetz. Demnach unterbleibt die Auskunft, soweit sie die ordnungsgemäße Erfüllung von Aufgaben der Gefahrenabwehr oder die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten gefährden würde beziehungsweise die Informationen ihrem Wesen nach geheim gehalten werden müssen.

– Auch wenn diese Vorschriften eine Einzelfallprüfung vorsehen, wobei jeweils die Interessen der betroffenen Person an der Auskunft mit den gegenläufigen Interessen der Spielbanken an der Wirksamkeit ihrer geldwäscherechtlichen Präventionsmaßnahmen abgewogen werden müssen, dürften schutzwürdige Interessen der Spielbanken aus Datenschutzsicht regelmäßig keinen vollständigen Ausschluss einer Auskunftserteilung rechtfertigen. Im Rahmen der Abwägung im Einzelfall kommt es vielmehr darauf an, inwieweit konkret zu befürchten ist, dass die Auskunft über personenbezogene Daten tatsächlich den Zielen des Geldwäschegesetzes oder anderen Schutzgütern widerspricht, und über welche Daten daher keine Auskunft zu erteilen ist.

– Manche Informationen werden vor diesem Hintergrund regelmäßig nicht herausgegeben werden können, etwa Beschreibungen von Verdacht auslösendem Verhalten einschließlich der maßgeblichen Beurteilungskriterien. Andererseits ist kein Grund ersichtlich, generell eine Auskunft hinsichtlich der gespeicherten Adressdaten oder Besuchstermine zu verweigern. Auch das spricht gegen einen pauschalen Ausschluss der Auskunft.

– Schließlich ist zu bedenken, dass sich die Beurteilung der Relevanz einzelner Informationen ändern kann. Da das datenschutzrechtliche Auskunftsrecht zeitlich nicht beschränkt ist, können im Rahmen der Einzelfallprüfung Gesichtspunkte wie Zeitablauf eine Rolle spielen, etwa ob eine Meldung an die Zentralstelle für Finanztransaktionsuntersuchungen überhaupt noch im Raum steht, ob sich ein Verdacht bestätigt hat oder nicht, ob zwischenzeitlich die interne

Methodik der Risikoermittlung geändert wurde, so dass Rückschlüsse auf eine alte Methodik nicht mehr relevant wären, und anderes mehr. Je nachdem, zu welchem Ergebnis die Abwägung der widerstreitenden Interessen gelangt, sind also mal mehr, mal weniger Daten zu beauskunften.

2.1.4 Fazit

Zusammenfassend können die von der Staatlichen Lotterie- und Spielbankverwaltung vorgetragenen Aspekte für eine Beschränkung des Auskunftsrechts durchaus durchschlagen, aber eben nur, soweit sie im Einzelfall auch tatsächlich zutreffen.

Ich gehe davon aus, dass die Staatliche Lotterie- und Spielbankverwaltung mit meiner Antwort zufrieden war, da das Kernanliegen der Anfrage, die Wirksamkeit der Maßnahmen zur Geldwäscheprävention nicht zu gefährden, gewahrt bleibt.

2.2 Meldung nach Art. 33 DSGVO bei Hackerangriff

Kein Verantwortlicher wünscht sich einen Hackerangriff. Dennoch kommen solche Angriffe nach meinen Erfahrungen immer öfter auch bei bayerischen öffentlichen Stellen und ihren IT-Dienstleistern vor. Hackerangriffe kosten Geld und Nerven, wenn personenbezogene Daten betroffen sind, auch schnell Vertrauen. Besonders wichtig ist daher gute Prävention und Absicherung der IT-Systeme. Am besten „fährt" der Verantwortliche, der die Routinen für den Fall eines Hackerangriffs stets aktuell verfügbar hat – und dann nie benötigt.

Der vorliegende Beitrag befasst sich mit einem Aspekt dieser Routinen, nämlich der Meldepflicht für Datensicherheitsverletzungen nach Art. 33 DSGVO.

Wozu dient die Meldung? Die Meldung dient dazu, Transparenz über den Vorfall zu schaffen und sicherzustellen, dass geeignete Maßnahmen ergriffen werden, um die betroffenen Personen zu schützen und den Schaden zu begrenzen. Dabei sind unter anderem die Art des Angriffs, der Umfang der betroffenen Daten und die möglichen Folgen darzulegen.

Herausgegriffen sind einige Punkte, die in meiner Prüfungs- und Beratungspraxis immer wieder Anlass zu (Nach-)Fragen gegeben haben.

2.2.1 Ausgangssituation

In letzter Zeit nehmen Angriffe auf die IT-Infrastruktur bayerischer öffentlicher Stellen und ihrer IT-Dienstleister stark zu. Betroffen sind insbesondere Krankenhäuser, Gemeinden, Landratsämter und Hochschulen. Die möglichen Folgen solcher Angriffe sind vielfältig; sie reichen von Datenabfluss und Datenverschlüsselung über andere Störungen der Verfügbarkeit bis hin zu mehrwöchigen Systemabschaltungen. Derartige Hackerangriffe bedrohen potenziell alle bayerischen öffentlichen Stellen. Viele Stellen haben zwar offenbar immer noch die Hoffnung, sie wären zu klein oder für Angreifer gänzlich uninteressant. Gerade umfassende Angriffe auf bekannte Sicherheitslücken zeigen jedoch, dass diese Hoffnung trügerisch ist.

Obwohl die meisten Angriffsversuche von der Sicherheitsinfrastruktur der öffentlichen Stellen – etwa von Firewalls oder Systemen zur Angriffserkennung – abgewehrt werden können, kommt es auch immer wieder zu erfolgreichen Angriffen, in deren Verlauf ein Hacker die Kontrolle über IT-Komponenten, im schlimmsten Fall gar einen Zugriff auf personenbezogene Daten erlangt. In diesem Sinn erfolgreich ist ein Angriff insbesondere dann, wenn der Hacker

— personenbezogene Datenbestände verschlüsseln, verändern, löschen oder abziehen konnte und/oder

— Zugriff auf eine Administrator-Kennung oder Zugang zu einer IT-Komponente im internen Netz (zum Beispiel Storage-Systeme, Backup-Systeme, virtuelle Server/Hypervisor) erlangen konnte und ein Zugriff auf Bestände personenbezogener Daten nicht zweifelsfrei ausgeschlossen werden kann.

In diesen Fällen ist stets zu prüfen, ob eine Meldung nach Art. 33 DSGVO erforderlich ist; in aller Regel werden die Voraussetzungen erfüllt sein. Die Vorgehensweise bei einer solchen Prüfung sowie bei der Erfüllung der Meldepflicht erläutert eine Orientierungshilfe, die auf meiner Homepage bereitgestellt ist.[2] Sie geht auch auf andere Fälle ein, etwa wenn personenbezogene Daten aufgrund von Sicherheitslücken über das Internet für Unbefugte zugänglich sind und deshalb mit unbefugten Zugriffen gerechnet werden muss.

2.2.2 Insbesondere: Angriff bei IT-Dienstleister

Bayerische öffentliche Stellen lagern den IT-Betrieb oftmals ganz oder in Teilen an IT-Dienstleister aus. Leider hat sich in der Vergangenheit gezeigt, dass auch solche IT-Dienstleister von erfolgreichen Hackerangriffen betroffen sein können. Vielerorts besteht die Auffassung, die Bearbeitung eines derartigen Sicherheitsvorfalls und damit auch die Erfüllung der Meldepflicht nach Art. 33 DSGVO sei allein Aufgabe des IT-Dienstleisters. Dies trifft jedoch nur für dessen eigene (!) Daten zu, nicht für die Daten des Auftraggebers, für den der IT-Dienstleister – meist im Rahmen eines Auftragsverarbeitungsverhältnisses – tätig wird.[3]

Folglich bleibt bei Hackerangriffen oder sonstigen Sicherheitsvorfällen die bayerische öffentliche Stelle als Auftraggeber Verantwortlicher im Sinne der Datenschutz-Grundverordnung, auch wenn sich der Vorfall – rein praktisch betrachtet – in der Sphäre des IT-Dienstleisters abspielt. Daran ändert sich selbst dann nichts, wenn der Auftragsverarbeiter den Hackerangriff erleichtert hat, weil er beispielsweise Sicherheitsupdates nicht rechtzeitig eingespielt hat. Hier zeigt sich wieder einmal, wie wichtig eine sorgfältige Auswahl und auch eine regelmäßige Kontrolle von IT-Dienstleistern ist; Einzelheiten habe ich in einem Leitfaden erläutert, der auf meiner Homepage abrufbar ist.[4]

[2] Bayerischer Landesbeauftragter für den Datenschutz, Meldepflicht und Benachrichtigungspflicht des Verantwortlichen, Stand 6/2019, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

[3] Allerdings hat der Auftragsverarbeiter den verantwortlichen Auftraggeber dabei zu unterstützen, siehe Art. 28 Abs. 3 Satz 2 Buchst. f, Art. 33 Abs. 2 DSGVO.

[4] Bayerischer Landesbeauftragter für den Datenschutz, Leitfaden zum Outsourcing kommunaler IT, Stand 3/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

Der Auftragsverarbeiter muss im Fall eines Hackerangriffs grundsätzlich seinen Auftraggeber verständigen. Der Auftraggeber muss dann die Meldepflicht nach Art. 33 DSGVO erfüllen. Hierbei genügt es nicht, allgemeine Informationsschreiben des Dienstleisters an die Datenschutzaufsichtsbehörde „durchzureichen". Der Auftraggeber muss den Vorfall vielmehr eigenständig bewerten und insbesondere für die eigenen betroffenen Daten eine Risikoanalyse durchführen.

Ein „vorsorgender" Auftraggeber wird diese Aspekte bereits bei der Beschaffung einer IT-Dienstleistung berücksichtigen: Es spricht nichts dagegen, mit dem Auftragsverarbeiter ausdrücklich eine Verpflichtung zu vereinbaren, im Fall eines Hackerangriffs die für eine Meldung nach Art. 33 DSGVO nötigen Informationen bereitzustellen – soweit erforderlich unter Einschluss einer den einschlägigen Standards entsprechenden Risikoanalyse.

2.2.3 Empfehlungen für die Erfüllung der Meldepflicht nach Art. 33 DSGVO im Fall eines Hackerangriffs

Auf einen Hackerangriff folgt – wie auch auf manch anderen Sicherheitsvorfall – oftmals eine längere Phase der „Sachverhaltserhärtung", die in der Regel forensische Analysen und polizeiliche Ermittlungen einschließt. Auch das Wiederaufsetzen der betroffenen IT-Systeme und die Implementierung geeigneter technisch-organisatorischer Maßnahmen kosten Zeit.

Vor diesem Hintergrund ist auch für die Erfüllung der Meldepflicht nach Art. 33 DSGVO ein „abschichtendes" Vorgehen sinnvoll:

2.2.3.1 Erstmeldung innerhalb von 72 Stunden

Wenn nach einer komplexen Datensicherheitsverletzung Risiken für die Rechte und Freiheiten der betroffenen Personen nicht zweifelsfrei ausgeschlossen werden können, ist eine Meldung nach Art. 33 DSGVO angezeigt. In der Meldung sind alle bisher bekannten Tatsachen zum Angriff oder Sicherheitsvorfall aufzuführen. Insbesondere sollte eine erste Einschätzung zur Sensibilität der Daten und zur Anzahl der betroffenen Personen abgegeben werden. Zudem sollten bereits Angaben gemacht werden, ob eine Information der betroffenen Personen gemäß Art. 34 DSGVO vorgesehen oder schon erfolgt ist.

2.2.3.2 Zwischenberichte alle zwei Wochen

Die Meldepflicht nach Art. 33 DSGVO ist erst erfüllt, wenn der Datenschutz-Aufsichtsbehörde alle gesetzlich geforderten, im Online-Meldeformular[5] strukturierten Angaben übermittelt sind. Bei längerem Klärungsbedarf und anzunehmender Betroffenheit von besonders sensiblen personenbezogenen Daten – insbesondere nach Art. 9 Abs. 1 DSGVO – ist es zweckmäßig, unaufgefordert alle zwei Wochen einen kurzen schriftlichen Zwischenbericht zu den wichtigsten Punkten zu erstatten. Dies betrifft insbesondere Krankenhäuser und andere medizinische Einrichtungen.

[5] Internet: https://www.datenschutz-bayern.de/service/data_breach.html.

2.2.3.3 Abschlussbericht nach Aufklärung des Hackerangriffs oder sonstigen Sicherheitsvorfalls

Spätestens nach der internen Aufklärung des Vorfalls ist ein Abschlussbericht erforderlich – sei es mit dem Ergebnis, dass kein Zugriff auf personenbezogene Daten erfolgte und somit keine Risiken bestanden, sei es mit folgenden Informationen und Unterlagen:

- endgültige Anzahl der betroffenen Personen und Kategorien von personenbezogenen Daten;
- konkrete Risikoanalyse hinsichtlich der betroffenen Daten;
- forensischer Abschlussbericht, insbesondere zur Ursache des Vorfalls und zur Möglichkeit eines Datenabflusses;
- Ermittlungsergebnisse der zuständigen Polizeidienststelle (soweit vorhanden);
- Ergebnisse einer Darknet-Recherche, wenn ein Datenabfluss festgestellt wurde, oder Begründung, warum keine Darknet-Recherche durchgeführt wurde;
- Erläuterung der ergriffenen und geplanten Maßnahmen beim Verantwortlichen und einem gegebenenfalls beauftragten IT-Dienstleister;
- Angaben zur Erfüllung einer Benachrichtigungspflicht nach Art. 34 DSGVO mit Kopie eines entsprechenden Informationsschreibens (soweit erforderlich).

2.2.4 Folgen von Defiziten bei der Erfüllung der Meldepflicht nach Art. 33 DSGVO

Defizite bei der Erfüllung der Meldepflicht nach Art. 33 DSGVO können Anlass für eine Beanstandung (Art. 16 Abs. 4 Satz 1 BayDSG) oder eine Verwarnung (Art. 58 Abs. 2 Buchst. b DSGVO) sein; im Einzelfall kann auch die Anordnung einer Verarbeitungsbeschränkung oder eines Verarbeitungsverbots (Art. 58 Abs. 2 Buchst. f DSGVO) in Betracht kommen – etwa dann, wenn wiederholte Datenschutzverletzungen belegen, dass der Verantwortliche nicht in der Lage ist, eine sichere Verarbeitung der betroffenen personenbezogenen Daten zu gewährleisten. Bezieht sich die Pflichtverletzung auf eine Tätigkeit, mit der die öffentliche Stelle am Wettbewerb teilnimmt, kann auch eine Geldbuße (Art. 83 Abs. 4 Buchst. a DSGVO) verhängt werden. Die Meldepflicht nach Art. 33 DSGVO ist also ernst zu nehmen.

2.3 Strafanzeige als technisch-organisatorische Maßnahme nach Hackerangriff?

Öffentliche Stellen sind nach Art. 33 DSGVO verpflichtet, Datensicherheitsverletzungen zu melden, wenn diese ein Risiko für die Rechte und Freiheiten natürlicher Personen darstellen. Dies gilt insbesondere in Fällen von Hackerangriffen, bei de-

nen personenbezogene Daten betroffen sein können. Die Meldung an die zuständige Datenschutzaufsichtsbehörde muss unverzüglich und, sofern möglich, innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls erfolgen.

Die Meldepflicht dient dazu, Transparenz über den Vorfall zu schaffen und sicherzustellen, dass geeignete Maßnahmen ergriffen werden, um die betroffenen Personen zu schützen und den Schaden zu begrenzen. Dabei sind unter anderem die Art des Angriffs, der Umfang der betroffenen Daten und die möglichen Folgen darzulegen.

Es besteht allerdings grundsätzlich keine gesetzliche Verpflichtung, nach Art. 33 DSGVO meldepflichtige Vorfälle auch den Strafverfolgungsbehörden mitzuteilen. Dies führt in der Praxis nicht selten dazu, dass eine Strafanzeige unterbleibt.

2.3.1 Gesetzliche Mitteilungspflichten

Neben der Meldepflicht nach Art. 33 DSGVO können weitere Mitteilungspflichten eingreifen. Betreiber kritischer Infrastrukturen sowie von Energieversorgungsnetzen und von bestimmten Energieanlagen trifft eine Pflicht zur Meldung an das Bundesamt für Sicherheit in der Informationstechnik, wenn bestimmte Störungen auftreten (§ 8b Abs. 4 BSI-Gesetz – BSIG – und § 11 Abs. 1c Energiewirtschaftsgesetz – EnWG).[6] Staatliche und sonstige an das bayerische Behördennetz angeschlossene Stellen müssen nach Art. 43 Abs. 3 Satz 1 Bayerisches Digitalgesetz (BayDiG) das Landesamt für Sicherheit in der Informationstechnik und ihre jeweilige oberste Dienstbehörde unterrichten, wenn Informationen bekannt werden, die zur Abwehr von Gefahren für die Sicherheit in der Informationstechnik von Bedeutung sind.

> **Hinweis:**
> Die „jeweilige oberste Dienstbehörde" ist bei nachgeordneten staatlichen Stellen das im Behördenaufbau übergeordnete Staatsministerium. Erfüllen Stellen – wie etwa die Regierungen – Aufgaben aus mehreren Geschäftsbereichen, dürfte es darauf ankommen, mit welcher dieser Aufgaben der meldepflichtige Vorfall in Zusammenhang steht. Bei nicht staatlichen Stellen dürfte als oberste Dienstbehörde im vorliegenden Sinne das Staatsministerium anzusehen sein, das die Aufgabe der obersten Aufsichtsbehörde wahrnimmt; jedenfalls legt der systematische Zusammenhang mit Art. 43 Abs. 2 BayDiG nahe, die oberste Dienstbehörde hier nicht entsprechend Art. 2 Satz 1, Art. 136 Bayerisches Beamtengesetz zu bestimmen.

Die Strafprozeßordnung sieht ein Recht zur Strafanzeige vor;[7] eine allgemeine, jeden treffende „Anzeigepflicht" für strafrechtlich relevante Vorgänge besteht demgegenüber grundsätzlich nicht. Zu beachten sind in diesem Zusammenhang aber insbesondere zwei Punkte:

— Bestimmte **Amtsträger** sind zu einer Strafanzeige verpflichtet, wenn ihnen (jedenfalls) in dienstlicher Eigenschaft der Anfangsverdacht einer Straftat bekannt wird. Dies gilt etwa für Polizeibeamte oder Staatsanwälte.[8] Meldepflichtige Datensicherheitsverletzungen im Bereich der Bayerischen Polizei sowie

[6] Näher Hessel/Potel, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit, 2023, § 8b BSIG Rn 13 ff. und Voigt/Böhme, a. a. O., § 11 EnWG Rn. 130 ff.

[7] § 158 Abs. 1 StPO, dazu Kölbel/Ibold, in: Münchener Kommentar zur Strafprozessordnung, 2. Aufl. 2024, § 158 StPO Rn. 11 f.

[8] Näher Weingarten, in: Karlsruher Kommentar zur Strafprozessordnung, 9. Aufl. 2023, § 158 StPO Rn. 25 ff.

der Staatsanwaltschaften dürften daher regelmäßig eine Strafanzeige oder die Einleitung eines Ermittlungsverfahrens veranlassen.

— § 138 Abs. 1 Strafgesetzbuch (StGB) stellt ausnahmsweise die „Nichtanzeige" ausgewählter, besonders schwerwiegender Straftaten unter eine Strafdrohung. Die Vorschrift zielt auf eine Abwendung der Bezugstat oder ihrer Folgen.[9] Sie begründet indirekt eine Pflicht zur Strafanzeige für **jedermann**, also auch für Beschäftigte bayerischer öffentlicher Stellen, die von einer Bezugstat gegen ihren Dienstherrn oder Arbeitgeber erfahren. Richtet sich ein Hackerangriff darauf, Staatsgeheimnisse zu erlangen oder auf IT-Infrastruktur einzuwirken, die für einen sicheren Bahn-, Straßen-, Schiffs- oder Luftverkehr erforderlich ist, sollte eine Pflicht zur Strafanzeige nach § 138 Abs. 1 StGB bedacht werden.

Beispiel:
Der Beschäftigte einer IT-Stelle, welche die Verkehrszentrale einer bayerischen Großstadt betreut, stellt fest, dass externe Nichtberechtigte versuchen, Kontrolle über die zentral gesteuerten Lichtzeichenanlagen zu erlangen. – Soweit eine Bezugstat nach § 315 Abs. 3 StGB im Raum steht, sollte der Beschäftigte einen Vorgesetzten informieren, der für den Verantwortlichen als „Bedrohten" (§ 138 Abs. 1 StGB) handeln darf.

Die angesprochenen Mitteilungspflichten unterscheiden sich hinsichtlich ihrer Zielrichtung, der zuständigen Stellen und der konkreten Anforderungen. Während datenschutzrechtliche Meldepflichten den Schutz personenbezogener Daten in den Vordergrund stellen, zielen die Meldepflichten nach dem BSI-Gesetz zunächst einmal auf den Schutz der Infrastruktur ab. Alle Pflichten dienen jedoch dem Schutz bestimmter Rechtsgüter, sollen Transparenz schaffen und effektive Gegenmaßnahmen ermöglichen.

Rechtsgrundlage	Zuständige Stelle	Mitteilungspflichtiger Vorfall
Art. 33 DSGVO	Datenschutzaufsichtsbehörde	Verletzungen des Schutzes personenbezogener Daten
§ 8b Abs. 4 BSIG	Bundesamt für Sicherheit in der Informationstechnik	Störungen bei Betreibern kritischer Infrastruktur
§ 11 Abs. 1c EnWG	Bundesamt für Sicherheit in der Informationstechnik	Störungen bei Betreibern von Energieversorgungsnetzen und von bestimmten Energieanlagen
Art. 43 Abs. 3 Satz 1 BayDiG	Landesamt für Sicherheit in der Informationstechnik und oberste Dienstbehörde	Bekanntwerden von Informationen, die zur Abwehr von Gefahren für die Sicherheit in der Informationstechnik von Bedeutung sind
§ 138 StGB	Strafverfolgungsbehörde, Bedrohter	Vorhaben oder Ausführung bestimmter schwerer Straftaten

2.3.2 Rolle der Datenschutzaufsichtsbehörden

Die Datenschutzaufsichtsbehörden spielen eine zentrale Rolle bei der Kontrolle der Einhaltung der datenschutzrechtlichen Vorgaben, insbesondere im Zusammenhang mit der Datenschutz-Grundverordnung. Sie sind nach Art. 57 Abs. 1

[9] Sternberg-Lieben, in: Schönke/Schröder, Strafgesetzbuch, 30. Aufl. 2019, § 138 StGB Rn. 1 f.

Buchst. a DSGVO verpflichtet, die Anwendung der Datenschutz-Grundverordnung zu überwachen und durchzusetzen. Dabei prüfen und untersuchen sie Datenschutzverstöße, beraten die Verantwortlichen und verhängen geeignete Maßnahmen.

Im Falle von Hackerangriffen sind die Datenschutzaufsichtsbehörden die ersten Anlaufstellen, um die gesetzlich vorgeschriebenen Meldungen im Hinblick auf den Schutz personenbezogener Daten zu prüfen und sicherzustellen, dass die Verantwortlichen angemessen reagieren.

Die Datenschutzaufsichtsbehörden können etwa Empfehlungen geben oder Anordnungen treffen, um den Schaden zu begrenzen oder Wiederholungen zu verhindern, wie zum Beispiel die Implementierung technisch-organisatorischer Maßnahmen zur Verbesserung der Datensicherheit. Die Aufgaben der Datenschutzaufsichtsbehörden beschränken sich allerdings auf die Anwendung der datenschutzrechtlichen Vorgaben; dementsprechend sind die Befugnisse in Art. 58 Abs. 1 DSGVO auf das Handlungsfeld „Datenschutz“ fokussiert. Zudem stehen hier der Verantwortliche und dessen Handlungsmöglichkeiten im Mittelpunkt. Die Entscheidung, ob eine Strafanzeige erstattet wird, obliegt grundsätzlich erst einmal der betroffenen öffentlichen Stelle. Die Datenschutzaufsichtsbehörde kann dem Verantwortlichen diese Entscheidung nicht abnehmen; sie wird oftmals eine Strafanzeige empfehlen und auf die Vorteile eines solchen Vorgehens hinweisen.

2.3.3 Strafanzeige als technisch-organisatorische Maßnahme

Im Zusammenhang mit Hackerangriffen kann eine Strafanzeige nämlich eine technisch-organisatorische Maßnahme im Sinn von Art. 32 Abs. 1, Art. 33 Abs. 3 Buchst. d DSGVO darstellen, auch wenn sie nicht durch besondere gesetzliche Regelungen vorgeschrieben ist.

Art. 33 Abs. 3 Buchst. d DSGVO verpflichtet Verantwortliche, im Rahmen der Meldung eines Datenschutzvorfalls an die zuständige Datenschutzaufsichtsbehörde auch Informationen über ergriffene Maßnahmen zur Minderung der nachteiligen Auswirkungen bereitzustellen. Diese Regelung lässt erkennen, dass Art. 32 Abs. 1 DSGVO im Fall einer Datensicherheitsverletzung konkrete Gegenmaßnahmen des Verantwortlichen fordert. Eine Strafanzeige bei den zuständigen Strafverfolgungsbehörden kann in diesem Kontext eine wirksame Maßnahme sein, die zur Aufklärung und zur Verhinderung weiterer Schäden beiträgt. Möchte eine öffentliche Stelle von einer Strafanzeige absehen, sollte dokumentiert werden, warum diese nicht als mindernde Maßnahme bewertet wurde.

Eine Strafanzeige eröffnet die Möglichkeit, über die datenschutzrechtlichen Aspekte hinaus die strafrechtliche Dimension eines Vorfalls zu beleuchten. Dies ist insbesondere dann zweckmäßig, wenn die Angriffsmethoden oder der verursachte Schaden weitreichende Konsequenzen haben. Die Strafanzeige initiiert nämlich Ermittlungen, die darauf abzielen, die Hintergründe und Ursachen des Angriffs zu analysieren. Durch die Zusammenarbeit mit den Ermittlungsbehörden können wichtige Informationen über den Angriff erlangt werden, etwa über die Angreifer und mögliche Schwachstellen in den eigenen Systemen. Dieses Wissen hilft der betroffenen Stelle dabei, die unmittelbaren Auswirkungen zu begrenzen und zukünftige Angriffe besser zu verhindern.

Auch liegen bei den Strafverfolgungsbehörden möglicherweise Kenntnisse über die üblichen Vorgehensweisen von Angreifergruppen vor, so dass beispielsweise die Wahrscheinlichkeit eines Datenabflusses oder einer möglicherweise noch folgenden Veröffentlichung von erbeuteten Daten vom Verantwortlichen besser eingeschätzt werden kann. Dies kann auch für die Entscheidung über die Benachrichtigung der von der Verletzung des Schutzes personenbezogener Daten betroffenen Personen nach Art. 34 DSGVO von wesentlicher Bedeutung sein.

Darüber hinaus verfügen die Strafverfolgungsbehörden über Werkzeuge und Kompetenzen, um Beweismaterial zu sichern, das für die Analyse und Behebung eines Angriffs entscheidend sein kann. Dies schließt etwa die Identifikation von Schadsoftware, die Rückverfolgung digitaler Spuren und die Analyse der verwendeten Infrastruktur ein. Diese Ergebnisse können dazu beitragen, die Kontrolle über die betroffenen Systeme wiederherzustellen und weiteren Schaden zu verhindern.

Weiterhin kann eine Strafanzeige rechtzeitig zu einem Ermittlungserfolg führen, sodass entwendete personenbezogene Daten sichergestellt oder deren weitere Verbreitung verhindert werden können.

Auf der organisatorischen Ebene kann eine Strafanzeige zu einer intensiveren Auseinandersetzung mit Sicherheitsprozessen führen und das Bewusstsein der Mitarbeitenden für Cybersicherheitsrisiken verbessern.

2.3.4 Fazit

Eine Strafanzeige und die Meldung nach Art. 33 DSGVO erfüllen unterschiedliche, aber sich ergänzende Zwecke. Während die Datenschutzaufsichtsbehörde die Einhaltung der Datenschutz-Grundverordnung sicherstellt und die Rechte der betroffenen Personen schützt, fokussieren sich die Strafverfolgungsbehörden auf die rechtliche Verfolgung der Täter und die Prävention weiterer Vorfälle. In Ergänzung können beide Maßnahmen dazu beitragen, die möglichen nachteiligen Auswirkungen eines Vorfalls abzumildern.

Auch wenn zumeist keine Pflicht zur Anzeige bei den Strafverfolgungsbehörden besteht, empfehle ich, die Prüfung eines solchen Vorgehens standardmäßig in die internen Prozesse zum „Handling“ von Hackerangriffen aufzunehmen. Dadurch kann nicht nur das behördeninterne Niveau von Datenschutz und IT-Sicherheit gehoben, sondern auch behördenübergreifend ein Beitrag zur Bekämpfung von Cyberkriminalität geleistet werden.

3 Künstliche Intelligenz

3.1 Allgemeines

3.1.1 KI-Verordnung

Während ich bereits in meinem 32. Tätigkeitsbericht 2022 über die Diskussion zu einem europäischen Gesetz über Künstliche Intelligenz informiert (Nr. 1.1.1.4) und in meinem 33. Tätigkeitsbericht 2023 die wesentlichen Inhalte der KI-Verordnung[10] knapp zusammengefasst habe, mache ich daran anknüpfend darauf aufmerksam, dass die ersten Teile der am 1. August 2024 in Kraft getretenen KI-Verordnung nunmehr seit dem 2. Februar 2025 beziehungsweise dem 2. August 2025 gelten. Dies betrifft gemäß Art. 113 KI-Verordnung insbesondere die allgemeinen Bestimmungen der KI-Verordnung einschließlich KI-Kompetenz (vgl. Kapitel I KI-Verordnung), die Vorschriften zu verbotenen Praktiken (vgl. Kapitel II KI-Verordnung) und zu KI-Modellen mit allgemeinem Verwendungszweck (vgl. Kapitel V KI-Verordnung) sowie die Regelungen zu benannten Stellen (Kapitel III Abschnitt 4 KI-Verordnung) und zu Governance und Sanktionen (vgl. Kapitel VII und Kapitel XII mit Ausnahme von Art. 101 KI-Verordnung). Gleichzeitig sind im Rahmen des Vorschlags der Europäischen Kommission für eine Digital-Omnibus-Verordnung zur KI[11] bereits erste Änderungen der KI-Verordnung geplant.

Die KI-Verordnung, deren Anwendungsbereich in Art. 2 KI-Verordnung und die wichtigsten Begriffsbestimmungen in Art. 3 KI-Verordnung geregelt sind, unterscheidet grundsätzlich vier verschiedene Risikostufen für Künstliche Intelligenz: verbotene KI-Praktiken, Hochrisiko-KI-Systeme, KI-Systeme mit begrenztem Risiko sowie KI-Systeme mit keinem oder geringem Risiko. Die Einordnung hängt dabei insbesondere von der Zweckbestimmung und den konkreten Anwendungsbereichen des jeweiligen KI-Systems oder KI-Modells,[12] das heißt dem ermittelten Risiko, ab und resultiert in jeweils unterschiedlichen Vorgaben und Verpflichtungen je Risikostufe; deren Anforderungen sind umso strenger, je risikoreicher das konkrete Einsatzfeld ist. Diese Vorgaben richten sich insbesondere an die Betreiber, das heißt Verwender (Art. 3 Nr. 4 KI-Verordnung), und Anbieter (Art. 3 Nr. 3 KI-Verordnung, einschließlich der sogenannten Quasi-Anbieter nach Art. 25 KI-Verordnung) von KI-Systemen oder KI-Modellen.

Zu deren Einhaltung, aber auch zur Überwachung und Durchsetzung der Verpflichtungen, werden durch die KI-Verordnung sowohl auf Unionsebene Governance-Strukturen etabliert als auch die Mitgliedstaaten verpflichtet, auf nationaler Ebene zuständige Behörden zu benennen.

[10] Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L 2024/1689 vom 12. Juli 2024).

[11] Internet: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0836.

[12] Der hier verwendete Begriff „KI-Modell“ erfasst sämtliche KI-Modelle, insbesondere auch solche mit allgemeinem Verwendungszweck im Sinne von Art. 3 Nr. 63 KI-Verordnung.

Trotz Ablauf der von der KI-Verordnung für den 2. August 2025 vorgesehenen Frist zur Benennung einer Marktüberwachungsbehörde im Sinne von Art. 70 Abs. 1 Satz 1 in Verbindung mit Art. 74 KI-Verordnung ist in Deutschland eine Benennung dieser im Berichtszeitraum nicht erfolgt. Es liegt lediglich ein nach Kritik von unter anderem der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder wegen insbesondere Verstoßes gegen die föderale Zuständigkeitsordnung des Grundgesetzes[13] geänderter Gesetzentwurf der Bundesregierung vom 10. Februar 2026 vor, welcher in § 2 Abs. 1 grundsätzlich eine zentrale Zuständigkeit der Bundesnetzagentur als KI-Marktüberwachungsbehörde vorsieht und für die Fälle des Art. 74 Abs. 8 Satz 1 KI-Verordnung ausweislich § 2 Abs. 5 in Verbindung mit § 4 Entwurf bei der Bundesnetzagentur eine unabhängige KI-Marktüberwachungskammer etabliert. Ausnahmen von dieser zentralen Zuständigkeitsfestlegung gelten ausweislich § 2 Abs. 2 bis 4 und 8 Entwurf für bestimmte Produktüberwachungsbehörden sowie gemäß § 2 Abs. 6 Satz 1 Entwurf für die Fälle, in denen öffentliche Stellen der Länder im Sinne des § 2 Abs. 2 und 3 Bundesdatenschutzgesetz KI-Systeme in Verkehr bringen, in Betrieb nehmen oder verwenden. In Bezug auf Letztere soll die Marktüberwachung den nach Landesrecht zuständigen Behörden obliegen. Eine entsprechende landesrechtliche Regelung ist nach Abschluss des Gesetzgebungsverfahrens auf Bundesebene zu erwarten.

Zweck der KI-Verordnung ist es, das Funktionieren des Binnenmarkts zu verbessern und die Einführung einer auf den Menschen ausgerichteten und vertrauenswürdigen Künstlichen Intelligenz zu fördern – unter gleichzeitiger Gewährleistung eines hohen Schutzniveaus in Bezug auf Gesundheit, Sicherheit und die in der Charta verankerten Grundrechte, einschließlich Demokratie, Rechtsstaatlichkeit und Umweltschutz, vor schädlichen Auswirkungen von KI-Systemen in der Union und Unterstützung der Innovation (Art. 1 Abs. 1 KI-Verordnung).

Das Verhältnis der KI-Verordnung zum Datenschutzrecht ist dabei klar geregelt: Art. 2 Abs. 7 KI-Verordnung besagt nicht nur, dass die Rechtsvorschriften der Union zum Schutz personenbezogener Daten, der Privatsphäre und der Vertraulichkeit der Kommunikation für die Verarbeitung personenbezogener Daten im Zusammenhang mit den in der KI-Verordnung festgelegten Rechten und Pflichten gelten, sondern regelt auch ausdrücklich, dass die KI-Verordnung, unbeschadet Art. 10 Abs. 5 und Art. 59 KI-Verordnung, die Datenschutz-Grundverordnung nicht berührt. Sobald also KI-Systeme oder KI-Modelle personenbezogene Daten im Anwendungsbereich des Datenschutzrechts verarbeiten, ist dieses vollumfänglich auf die Datenverarbeitungen anwendbar.

3.1.2 Tätigkeit der Stabsstelle Digitales & KI

Zur Bündelung der datenschutzrechtlichen (Grundsatz-)Fragen, die sich im Zusammenhang mit Künstlicher Intelligenz stellen, und in Wahrnehmung meiner Aufgabe nach Art. 57 Abs. 1 Buchst. i DSGVO, maßgebliche Entwicklungen zu verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie

[13] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Stellungnahme der vom 10. Oktober 2025 zum Entwurf eines Gesetzes zur Durchführung der Verordnung über künstliche Intelligenz (KI-VO), Internet: https://www.datenschutzkonferenz-online.de, Rubrik „Stellungnahmen".

und der Geschäftspraktiken, habe ich daher bereits im März 2024 in meiner Geschäftsstelle die „Stabsstelle Digitales & KI“ eingerichtet. Ziel der neuen Organisationseinheit ist es, die zunehmende Verbreitung und Nutzung von Künstlicher Intelligenz datenschutzrechtlich zu begleiten und sicherzustellen, dass der Einsatz von Künstlicher Intelligenz im Einklang mit dem geltenden Datenschutzrecht erfolgt und die Grundrechte der betroffenen Personen gewahrt bleiben. Die Stabsstelle ist bei der Wahrnehmung der aufsichtlichen Aufgaben insbesondere in die Beratung bayerischer öffentlicher Stellen und in die Tätigkeit verschiedener Gremien involviert.

In diesem Kontext ist insbesondere der Arbeitskreis „Künstliche Intelligenz“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu nennen, welchen diese auf ihrer 108. Konferenz am 14. November 2024 in Wiesbaden mit einstimmigem Beschluss eingerichtet hat. Dieser Arbeitskreis hat im Berichtszeitraum insbesondere an einer „Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen“ mitgewirkt, eine „Orientierungshilfe zu datenschutzrechtlichen Besonderheiten generativer KI-Systeme mit RAG-Methode“ veröffentlicht[14] sowie Beiträge zur gemeinsamen Stellungnahme des Europäischen Datenschutzausschusses und des Europäischen Datenschutzbeauftragten zum Vorschlag der Europäischen Kommission für eine Digital-Omnibus-Verordnung zur KI[15] geleistet.

Bereits im Jahr 2024 hat sich der Arbeitskreis zudem mit Anmerkungen im Verfahren des Europäischen Datenschutzausschusses zur Erarbeitung und Veröffentlichung einer „Stellungnahme zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen“[16] beteiligt. Dieser Stellungnahme sind entscheidende Aspekte betreffend die Auswirkungen der (auch rechtswidrigen) Verarbeitung personenbezogener Daten auf KI-Modelle zu entnehmen, welche auch von bayerischen öffentlichen Stellen im Zusammenhang mit dem Einsatz von Künstlicher Intelligenz zu berücksichtigen sind. In der Stellungnahme werden beispielsweise die Fragen behandelt, unter welchen Umständen ein mit personenbezogenen Daten trainiertes KI-Modell als „anonym“ angesehen werden kann, und ob eine rechtswidrige Datenverarbeitung im Zusammenhang mit dem Training eines KI-Modells Folgen für die Rechtmäßigkeit der späteren Verarbeitungstätigkeit oder des späteren Betriebs des KI-Modells hat.

3.2 Beratungsanfragen in Zusammenhang mit Künstlicher Intelligenz

Gerade auch vor dem Hintergrund der demografischen Entwicklung birgt Künstliche Intelligenz enormes Potential für die öffentliche Verwaltung. Bayerische öffentliche Stellen haben dieses Potential erkannt und die verschiedenen Einsatzszenarien und Systeme, mit denen ich im Berichtszeitraum befasst war, spiegeln

[14] Beide abrufbar unter https://www.datenschutz-bayern.de, Rubrik „Infothek“.

[15] Internet: https://www.edpb.europa.eu/system/files/2026-01/edpb_edps_jointopinion_202601_proposal_ai-omnibus_en.pdf.

[16] Europäischer Datenschutzausschuss, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen, Stand 12/2024, Internet: https://www.edpb.europa.eu/system/files/2025-05/edpb_opinion_202428_ai-models_de.pdf.

die Einsatzvielfalt Künstlicher Intelligenz in der Verwaltung wider. So war ich sowohl auf Ministerialebene als auch für kleine(re) öffentliche Stellen beratend tätig. Dabei haben mich insbesondere Praxisfragen konkret geplanter Nutzungen verschiedenster Ausgestaltung (Einsatz „fertiger" KI-Systeme, „Eigenentwicklungen" und „Nachtraining" eines bestimmten KI-Systems) sowie die Beratung des Gesetzgebers zu Regelungen betreffend Künstliche Intelligenz beschäftigt.

Ausgangspunkt meiner Tätigkeit ist dabei der Grundsatz, dass – unabhängig von dem konkreten zur Anwendung kommenden Produkt und dem jeweiligen Einsatzszenario – die Vorgaben des Datenschutzrechts und insbesondere der Datenschutz-Grundverordnung einzuhalten sind, sobald und soweit bayerische öffentliche Stellen personenbezogene Daten mittels Künstlicher Intelligenz verarbeiten.

Dem vorgelagert stellt sich die vom Verantwortlichen zu prüfende Frage, ob zur Erfüllung des konkreten Verarbeitungszwecks tatsächlich Daten mit Personenbezug erforderlich sind, oder ob der Verarbeitungszweck nicht auch mit nicht personenbezogenen, anonymisierten oder synthetischen Daten oder nachrangig zumindest mit pseudonymisierten Daten erreicht werden kann.

Erfolgt eine Verarbeitung personenbezogener Daten, ergeben sich auch bei Verarbeitung mittels Künstlicher Intelligenz grundsätzlich die „üblichen" datenschutzrechtlichen Problemkreise: Insbesondere sind Fragen der Verantwortlichkeit, das zwingende Erfordernis einer Rechtsgrundlage für die Datenverarbeitung (Art. 5 Abs. 1 Buchst. a, Art. 6 Abs. 1 DSGVO), die Verarbeitungsgrundsätze des Art. 5 Abs. 1 DSGVO, die Transparenzpflichten und die Betroffenenrechte zu beachten. Deren Ausgestaltung und Umsetzung kann beim Einsatz von Künstlicher Intelligenz allerdings zusätzlichen Herausforderungen unterliegen. Zur umfassenden Erschließung der insoweit relevanten Fragestellungen für bayerische öffentliche Stellen habe ich daher wesentlich im Berichtszeitraum die Orientierungshilfe „Datenschutz bei KI-Projekten in der bayerischen Verwaltung" sowie die einzelne KI-Nutzungsszenarien kompakt darstellenden Veröffentlichungen „AI in a nutshell" erarbeitet.[17] Im Folgenden möchte ich ausgewählte Problempunkte hervorheben:

3.2.1 Ausgangspunkt: Einordnung der Beteiligten in das datenschutzrechtliche Rollenmodell

Ausgangspunkt für die Beurteilung der Datenschutzkonformität von Verarbeitungen personenbezogener Daten ist die Einordnung aller beteiligten Akteure in das datenschutzrechtliche Rollenmodell, auf deren Grundlage sich die entsprechenden Rechte und Pflichten ergeben. Angesichts der Komplexität und der unterschiedlichen Komponenten eines KI-Systems oder KI-Modells sind hier oftmals verschiedene Akteure in verschiedenen Phasen (insbesondere Training – Nutzung – Nachtraining) und verschiedenen Rollen (Verantwortlicher – gemeinsame Verantwortliche – Auftragsverarbeiter - Dritter) beteiligt.[18]

[17] Internet: https://www.datenschutz-bayern.de, Rubrik „KI".

[18] Zum Ganzen Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz bei KI-Projekten in der bayerischen Verwaltung, Orientierungshilfe, Stand 3/2026, Rn. 274 ff., Internet: https://www.datenschutz-bayern.de, Rubrik „KI".

Mehrere auf meiner Website veröffentlichte Hilfestellungen können bayerische öffentliche Stellen bei der Einordnung verschiedener Beteiligter in das datenschutzrechtliche Rollenmodell und bei Abschluss entsprechender Vereinbarungen unterstützen.[19]

Folgendes Beispiel soll die Vielzahl der möglichen Beteiligten im KI-Kontext verdeutlichen:

Eine bayerische öffentliche Stelle nutzt zur Erstellung von Gratulationsschreiben und damit zur Verarbeitung personenbezogener Bürgerdaten ein generatives Großes Sprachmodell (LLM) des Anbieters A, das dieser in der Cloud des Anbieters B betreibt. Mittels eines Retrieval Augmented Generation (RAG)-Subsystems des Anbieters C werden zusätzlich verwaltungsinterne Dokumente für das Große Sprachmodell zugänglich gemacht.

Hinweis:
KI-Sprachmodelle nutzen beim Beantworten von Prompts grundsätzlich nur die Daten und Dokumente, mit denen sie trainiert wurden. Mit RAG werden KI-Sprachmodelle in die Lage versetzt, weitere (außerhalb des Sprachmodells liegende) Datenquellen wie Dokumentensammlungen, Datenbanken oder einen Knowledge Graph heranzuziehen (sogenanntes RAG-Subsystem). Hierfür werden diese Datenquellen zunächst aufbereitet, beispielsweise durch Aufteilung in kürzere Absätze (Chunks), Überführung dieser Chunks in Vektoren mittels eines KI-Embedding-Modells und Speicherung der Vektoren in einer Vektordatenbank. Wann immer Nutzer dann Prompts eingeben, wird die Anfrage im RAG-Subsystem mittels des Embedding-Modells ihrerseits in einen Anfragevektor überführt und an den sogenannten Retriever übergeben, der die Vektorbank nach denjenigen Vektoren durchsucht, welche eine möglichst geringe Distanz (das heißt große semantische Nähe) zum Anfragevektor haben. Anschließend wird die Eingabe des Nutzers um das Suchergebnis des Retrievers, das heißt die Informationen aus den angebundenen Datenquellen, ergänzt, bevor sie vom RAG-Subsystem an ein KI-System mit Sprachmodell weitergegeben. Dieses soll ausschließlich (technisch derzeit noch nicht erreichbarer Idealfall) beziehungsweise jedenfalls vorrangig nur diese relevanten Inhalte als Kontext für die Beantwortung des Prompts nutzen und das KI-Sprachmodell zur reinen Textgenerierung verwenden (sogenanntes RAG-System).[20]

In dieser Konstellation ist die bayerische öffentliche Stelle datenschutzrechtlich Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO und der Anbieter A des Großen Sprachmodells deren Auftragsverarbeiter im Sinne von Art. 28 Abs. 1 DSGVO, vorausgesetzt, dass er die personenbezogenen Daten ausschließlich auf Weisung der öffentlichen Stelle verarbeitet (Art. 29, Art. 28 Abs. 10 DSGVO). Der Anbieter B der Cloud wird unter denselben Voraussetzungen wiederum als Unterauftragsverarbeiter des Anbieters A des Großen Sprachmodells tätig (zu möglichen Drittlandübermittlungen im Zusammenhang mit Cloud-Nutzung vgl. Nr. 3.3.1.2). Auch der Anbieter C der im RAG-Subsystem zum Einsatz kommenden KI-Systeme beziehungsweise KI-Modelle ist regelmäßig als Auftragsverarbeiter einzuordnen. Eine Nutzung der von der öffentlichen Stelle eingegebenen personenbe-

[19] Bayerischer Landesbeauftragter für den Datenschutz, Auftragsverarbeitung, Orientierungshilfe, Stand 4/2019; Gemeinsame Verantwortlichkeit, Orientierungshilfe, Stand 6/2024; Datenschutz als Kriterium im Vergabeverfahren, Orientierungshilfe, Stand 2/2024; KI ohne Grenzen? Einsatz von Drittlandsprodukten in der bayerischen Verwaltung, Aktuelle Kurz-Information 60, Stand 3/2025, jeweils Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

[20] Zum Ganzen Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz bei KI-Projekten in der bayerischen Verwaltung (Fn. 18), Rn. 177 ff.; Anbindung eines RAG-Subsystems an ein KI-System mit Sprachmodell, AI in a nutshell 1, Internet: https://www.datenschutz-bayern.de, Rubrik „KI".

zogenen Daten zu eigenen Zwecken der (Unter-)Auftragsverarbeiter – beispielsweise dem allgemeinen Nachtraining des Großen Sprachmodells – ist nicht zulässig und sollte nicht nur vertraglich, sondern auch, soweit möglich, durch entsprechende Konfiguration ausgeschlossen werde. Findet dennoch eine Datenverarbeitung zu eigenen Zwecken des (Unter-)Auftragsverarbeiters statt, ist dieser insoweit Verantwortlicher, Art. 28 Abs. 10 DSGVO.

3.2.2 Rechenschaftspflicht nach Art. 5 Abs. 2 DSVGO

Setzt eine bayerische öffentliche Stelle Künstliche Intelligenz für die Verarbeitung personenbezogener Daten ein beziehungsweise geht mit dem Einsatz Künstlicher Intelligenz durch eine bayerische öffentliche Stelle die Verarbeitung personenbezogener Daten einher, so muss diese öffentliche Stelle als datenschutzrechtlich Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO in Verbindung mit Art. 1 Abs. 1 BayDSG ihrer Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO nachkommen. Konkret umfasst die Rechenschaftspflicht die jederzeitige Gewährleistung einer rechtskonformen Verarbeitung personenbezogener Daten sowie den Nachweis, dass der Einsatz Künstlicher Intelligenz im konkreten Anwendungsszenario den datenschutzrechtlichen Vorgaben entspricht. Dies bedarf stets einer Einzelfallbetrachtung unter Berücksichtigung des gegebenenfalls vereinbarten Vertragswerks, der einzelnen verwendeten Produkte, ihrer konkreten Funktionen sowie der Zwecke des Einsatzes in der konkreten technisch-organisatorischen Umgebung.

Insoweit ist zu beachten, dass KI-Systeme und KI-Modelle, unabhängig von der Art ihres Einsatzes (das heißt, „fertiges“ KI-System oder KI-Modell, „Eigenentwicklung“ oder „Nachtraining“), oftmals komplex sind. Daher kann es im Einzelfall eine Herausforderung darstellen, die mit deren Nutzung einhergehenden Datenflüsse nachzuvollziehen und für jede Verarbeitung personenbezogener Daten die Vorgaben aus der Datenschutz-Grundverordnung, dem Bayerischen Datenschutzgesetz und/oder dem möglicherweise einschlägigen Fachrecht einzuhalten. So musste ich in meiner Beratungspraxis wiederholt feststellen, dass Verantwortliche keinen der datenschutzrechtlichen Rechenschaftspflicht genügenden Überblick über die verschiedenen, im Zusammenhang mit dem jeweiligen KI-System oder KI-Modell stehenden Verarbeitungsvorgänge hatten. Genau dieses Wissen ist jedoch essenziell, um datenschutzrechtliche Vorgaben umfassend berücksichtigen und damit den Schutz personenbezogener Daten von sowohl Bürgerinnen und Bürgern als auch von Beschäftigten vollumfänglich gewährleisten zu können.

Diesbezüglich habe ich mich im Rahmen meiner Beratungstätigkeit bei verschiedenen Stellen der Bayerischen Staatsregierung dafür eingesetzt, durch die Schaffung geeigneter rechtlicher Rahmenbedingungen sowie entsprechender Hilfestellungen die Grundlage für einen datenschutzkonformen Einsatz von Künstlicher Intelligenz zu legen.

3.2.3 Rechenschaftspflicht im Lichte der EDSA-Stellungnahme 28/2024

Speziell bezogen auf die Rechenschaftspflicht des datenschutzrechtlich Verantwortlichen im Zusammenhang mit dem Einsatz von KI-Modellen stellt die bereits genannte EDSA-Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der

Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen[21] Folgendes heraus: KI-Modelle, die mit personenbezogenen Daten trainiert wurden, können regelmäßig nicht für anonym befunden werden. Sind zum Zeitpunkt der Nutzung (weiterhin) personenbezogene Daten in dem jeweils – gegebenenfalls als Teil eines KI-Systems – eingesetzten KI-Modell vorhanden, umfasst die Rechenschaftspflicht des Verantwortlichen auch die „angemessene Bewertung" der Datenschutzkonformität des KI-Modells und deren Auswirkungen auf die Rechtmäßigkeit der mit dessen Nutzung oder einem (Nach-)Training verbundenen Datenverarbeitungen, einschließlich – soweit erforderlich – die Prüfung der Umsetzung einzelfallspezifischer sogenannter „risikomindernder Maßnahmen".[22] Diese Bewertung und Prüfung sollten dokumentiert werden, um der datenschutzrechtlichen Rechenschaftspflicht jederzeit nachkommen zu können.[23]

Dies macht einmal mehr deutlich, dass datenschutzrechtliche Anforderungen von Beginn an mitgedacht und bereits in den Konzeptions- und Entwicklungs- beziehungsweise Beschaffungsprozess für das jeweilige KI-System oder KI-Modell integriert werden müssen.

3.2.4 Rechtmäßigkeitsgrundsatz des Art. 5 Abs. 1 Buchst. a in Verbindung mit Art. 6 Abs. 1 UAbs. 1 DSGVO

Der Verantwortliche benötigt für jede Verarbeitung personenbezogener Daten eine Rechtsgrundlage, Art. 5 Abs. 1 Buchst. a in Verbindung mit Art. 6 Abs. 1 UAbs. 1 DSGVO. Dabei muss jeder Einzelfall individuell betrachtet und nach einzelnen Verarbeitungsschritten differenziert werden.

Im Berichtszeitraum gab es weder in der Datenschutz-Grundverordnung noch im Bayerischen Datenschutzgesetz oder im Fachrecht gesetzliche Grundlagen, die speziell den Einsatz oder das Training von Künstlicher Intelligenz regeln. Allerdings kann zumindest die Nutzung von Künstlicher Intelligenz in vielen Fällen auf bestehende Rechtsgrundlagen gestützt werden:

3.2.4.1 Nutzung eines KI-Systems oder KI-Modells als Betriebsmittel

So kann oftmals die Nutzung eines KI-Systems oder KI-Modells als Betriebsmittel für eine Datenverarbeitung aufgrund einer bestehenden Verarbeitungsbefugnis in Betracht gezogen werden. Öffentliche Stellen können sich dabei regelmäßig auf Art. 6 Abs. 1 UAbs. 1 Buchst. e (Erforderlichkeit zur Aufgabenwahrnehmung), Abs. 2, Abs. 3 Satz 1 Buchst. b DSGVO – gegebenenfalls in Verbindung mit Art. 4 Abs. 1 BayDSG – in Verbindung mit der jeweils einschlägigen Aufgabenzuweisungsnorm, stützen.[24] Auch Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO (Vertragserfüllung oder Durchführung vorvertraglicher Maßnahmen) oder Einwilligungen gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO können in Einzelfällen als Verarbeitungsgrundlage herangezogen werden.[25] Der Rechtsgrundlage des Art. 6 Abs. 1

[21] Europäischer Datenschutzausschuss, Stellungnahme 28/2024 (Fn. 16).
[22] Europäischer Datenschutzausschuss, Stellungnahme 28/2024 (Fn. 16), Rn. 122, 132, 134.
[23] Zum Ganzen Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz bei KI-Projekten in der bayerischen Verwaltung (Fn. 18), Rn. 166 ff.
[24] Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz bei KI-Projekten in der bayerischen Verwaltung (Fn. 18), Rn. 221 ff.
[25] Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz bei KI-Projekten in der bayerischen Verwaltung (Fn. 18), Rn. 229 ff.

UAbs. 1 Buchst. c DSGVO (Erforderlichkeit für die Erfüllung einer rechtlichen Verpflichtung) kommt dagegen in Bezug auf die Verarbeitung personenbezogener Daten durch KI-Systeme oder KI-Modelle mit Blick auf deren regelmäßig Vielzahl an Rechenleistungen bisher allenfalls untergeordnete Bedeutung zu.[26] Insbesondere ist derzeit keine gesetzlich normierte Verpflichtung für (Weiter-)Training oder Nutzung von KI-Systemen oder KI-Modellen bekannt.

Voraussetzung für die Einordnung von Künstlicher Intelligenz als Betriebsmittel für eine Datenverarbeitung aufgrund einer bestehenden Verarbeitungsbefugnis ist, wie vor jeder Nutzung eines Betriebsmittels, insbesondere eine Prüfung, ob dessen Einsatz zur Erreichung des jeweiligen Verarbeitungszwecks erforderlich ist.[27]

Zu beachten ist dabei, dass personenbezogene Daten in unterschiedlichen Phasen des Lebenszyklus' eines KI-Systems oder KI-Modells verarbeitet werden können, beispielsweise in Form der Erhebung und Verarbeitung von Trainings-, Test- und Validierungsdaten, der Erhebung, Aufzeichnung und Speicherung von Anmeldedaten und Eingabeaufforderungen der Nutzenden, der Verarbeitung innerhalb eines KI-Systems oder KI-Modells, der Ergebnisausgabe sowie gegebenenfalls der Weiternutzung der Anmelde- und Eingabedaten, etwa zum Weitertraining eines KI-Systems oder KI-Modells (zu eigenen Zwecken des Anbieters).[28] Ein KI-System oder KI-Modell kann dabei nicht nur Inhaltsdaten – also etwa Daten zur Aufgabenerfüllung, die mit dem Betriebsmittel Künstliche Intelligenz unterstützt wird –, sondern auch Nutzerdaten (beispielsweise in Form von Beschäftigtendaten) und spezifische Betriebsmitteldaten wie etwa die IP-Adressen der Nutzer verarbeiten. Bei Nutzung eines (von einem Dritten) vortrainierten KI-Modells, zu dessen Training (auch) personenbezogene Daten verwendet wurden, die weiterhin in dem – gegebenenfalls als Teil eines KI-Systems – eingesetzten KI-Modell vorhanden sind, umfasst die Prüfpflicht des Verantwortlichen auch die „angemessene Bewertung" der mit dem Training des KI-Modells einhergehenden Datenverarbeitungen und deren Auswirkungen auf die Rechtmäßigkeit späterer Verarbeitungen mittels dieses KI-Modells.[29]

Sollte es durch das jeweilige KI-System oder KI-Modell zu einem bedeutenden „Mehr" an Datenverarbeitung kommen als durch andere zur Verfügung stehende Betriebsmittel, so ist zu prüfen, ob die Rechtsgrundlage, im Rahmen derer das KI-System oder KI-Modell als Betriebsmittel herangezogen wird, dessen Einsatz noch abbilden kann.

Soll ein KI-System oder KI-Modell unter den oben genannten Voraussetzungen als Betriebsmittel für eine Verarbeitung personenbezogener Daten genutzt werden, ist der einsetzenden öffentlichen Stelle als datenschutzrechtlich Verantwortlichem zu empfehlen, das betreffende KI-System oder KI-Modell nach Prüfung der Einhaltung der datenschutzrechtlichen Vorgaben (Art. 24 Abs. 1 Satz 1 und

[26] Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz bei KI-Projekten in der bayerischen Verwaltung (Fn. 18), Rn. 219 f.

[27] Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz bei KI-Projekten in der bayerischen Verwaltung (Fn. 18), Rn. 142.

[28] Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz bei KI-Projekten in der bayerischen Verwaltung (Fn. 18), Rn. 137 ff.

[29] Europäischer Datenschutzausschuss, Stellungnahme 28/2024 (Fn. 16), Rn. 122, 132, 134; Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz bei KI-Projekten in der bayerischen Verwaltung (Fn. 18), Rn. 168.

Art. 5 Abs. 2 DSGVO) für ihre Mitarbeitenden zur Nutzung freizugeben, gegebenenfalls unter Festlegung bestimmter Rahmenbedingungen.[30] Insoweit dürfte es sich oftmals anbieten, beispielsweise in einer Dienstanweisung oder Dienstvereinbarung festzulegen, ob und welche personenbezogenen Daten mit Hilfe des jeweiligen KI-Systems oder KI-Modells verarbeitet werden dürfen. Entsprechend habe ich auch schon bayerische öffentliche Stellen bei der Erstellung interner datenschutzrechtlicher Vorgaben beraten.

Insoweit liegt es nahe, – ressortübergreifend oder auch ressortspezifisch – kleineren öffentlichen Stellen Muster oder andere Unterstützung zur Verfügung zu stellen, um ein kohärentes Vorgehen innerhalb der Bayerischen Verwaltung über die verschiedenen Verwaltungsebenen hinweg zu ermöglichen. Den behördlichen Datenschutzbeauftragten vor Ort kommt dabei die wichtige Aufgabe zu, konkrete Bedarfe vor Ort zu eruieren und Unterstützungsbedarf weiterzugeben.

3.2.4.2 KI-Nutzung und datenschutzrechtliche Generalklausel

Soweit es sich um Datenverarbeitungen mit eher geringer Eingriffsintensität handelt, ist es im Einzelfall auch denkbar, die Nutzung von Künstlicher Intelligenz als Betriebsmittel auf die datenschutzrechtliche Generalklausel des Art. 4 Abs. 1 BayDSG zu stützen; eingriffsintensivere – wie auch massenhafte – Datenverarbeitungen können dagegen nicht auf Grundlage der allgemeinen Datenverarbeitungsbefugnis des Art. 4 Abs. 1 BayDSG erfolgen.[31] Die Frage insbesondere der Eingriffsintensität ist jeweils mit Blick auf die Art der zu erfüllenden konkreten Aufgabe als auch auf die konkrete „Wirkweise“ sowie das konkrete Einsatzszenario des Betriebsmittels zu bewerten. Diese Prüfung obliegt zunächst der einsetzenden Stelle als datenschutzrechtlich Verantwortlichem.

3.2.4.3 Eigenes Initialtraining und Weiter-/Nachtraining von KI-Systemen oder KI-Modellen

Die angeführten Aspekte sind auch für die Frage relevant, ob das Initialtraining oder Weiter-/Nachtraining eines KI-Systems oder KI-Modells mit personenbezogenen Daten auf die genannten Rechtsgrundlagen gestützt werden kann.

Aufgrund des Bestimmtheitsgrundsatzes und der Wesentlichkeitstheorie dürften (fach-)gesetzliche Regelungen für Datenverarbeitungen, die den Kontext „Training von Künstlicher Intelligenz“ nicht spezifisch erfassen, dabei oftmals keine Rechtsgrundlage für das Training – gleich welcher Form – von KI-Systemen oder KI-Modellen mit personenbezogenen Daten bilden können.

In Bezug auf die Generalklausel des Art. 4 BayDSG sind darüber hinaus dessen oben beschriebene Grenzen zu berücksichtigen und kann die Norm im Ergebnis allenfalls in engen Ausnahmefällen als Rechtsgrundlage für Training herangezogen werden. In den meisten Fällen wird durch das Training – gleich welcher Form – eine Eingriffstiefe erreicht werden, die den Rückgriff auf die datenschutz-

[30] Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz bei KI-Projekten in der bayerischen Verwaltung (Fn. 18), Rn. 373 ff.

[31] Vgl. hierzu Bayerischer Verwaltungsgerichtshof, Beschluss vom 15. Februar 2024, 4 CE 23.2267, BeckRS 2024, 29658, Rn. 20 ff.; Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz bei KI-Projekten in der bayerischen Verwaltung (Fn. 18), Rn. 223 ff.

rechtliche Generalklausel versperrt. Zudem dürfte zumindest das Initialtraining eines KI-Systems oder KI-Modells für die konkrete Aufgabenerfüllung oftmals nicht erforderlich sein.

Um hier Rechtssicherheit zu schaffen, wäre eine Regelung des bayerischen Gesetzgebers wünschenswert. Entsprechend habe ich im Berichtszeitraum verschiedene Stellen der Bayerischen Staatsregierung beraten.

Im Übrigen zeigt die Praxis, dass ein Training von KI-Systemen oder KI-Modellen auch mit Daten ohne Personenbezug möglich ist: So war ich im Berichtszeitraum mit verschiedenen Projekten befasst, in denen sowohl im Rahmen des Initialtrainings als auch des Nachtrainings ausschließlich synthetische Daten (beispielsweise eigens hierfür erstellte fiktive Urkunden über Berufsabschlüsse) oder anonymisierte Daten verarbeitet wurden.

3.2.4.4 Initialtraining und Weiter-/Nachtraining von KI-Systemen oder KI-Modellen durch Dritte zu eigenen Zwecken

Derzeit existiert weder in der Datenschutz-Grundverordnung noch im Fachrecht oder im Bayerischen Datenschutzgesetz eine Regelung, die eine Übermittlung von personenbezogenen Daten an Dritte, wie etwa Hersteller, Anbieter oder Betreiber eines KI-Systems oder KI-Modells zu deren eigenen Zwecken in Form von Training ausdrücklich vorsieht. Dies gilt auch im Zusammenhang mit einer Tätigkeit als Auftragsverarbeiter für eine öffentliche Stelle.

Daher müssen bayerische öffentliche Stellen sicherstellen, dass die von ihnen eingesetzten Auftragsverarbeiter die im Rahmen der Auftragsausführung zu verarbeitenden personenbezogenen Daten nur weisungsgemäß für Zwecke des Verantwortlichen verarbeiten und nicht in datenschutzwidriger Weise „für sich selbst" verwenden (Art. 28 Abs. 1, Abs. 10, Art. 29 DSGVO, mit Ausnahme in Art. 29 Halbsatz 2 DSGVO für Verarbeitungen aufgrund einer Rechtspflicht). Aus diesem Grund sollte beispielsweise das zu nutzende KI-System oder KI-Modell vom Verantwortlichen so konfiguriert werden, dass das Weiter-/Nachtraining des Produkts durch den jeweiligen Hersteller, Anbieter oder Betreiber mit den Anmelde- und Eingabedaten ausgeschlossen ist. Verstößt ein Auftragsverarbeiter durch Verarbeitung von personenbezogenen Daten zu eigenen Zwecken gegen die rechtlichen Vorgaben zum und Weisungen im Auftragsverarbeitungsverhältnis, gilt er ausweislich Art. 28 Abs. 10 DSGVO in Bezug auf diese Verarbeitung als Verantwortlicher und muss insbesondere sämtliche entsprechenden Pflichten aus der Datenschutz-Grundverordnung erfüllen.

Ist ein Auftragsverarbeiter in Bezug auf bestimmte Verarbeitungsschritte oder im Hinblick auf bestimmte Daten eigenständiger datenschutzrechtlicher Verantwortlicher, bedarf die Übermittlung von personenbezogenen Daten an ihn in dieser Rolle im Übrigen wiederum einer Rechtsgrundlage, Art. 5 Abs. 1 Buchst. a, Art. 6 Abs. 1 DSGVO.

3.2.4.5 Grenzen des Rückgriffs auf die Einwilligung

Grundsätzlich kann auch die Einwilligung der betroffenen Person nach Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO als Rechtsgrundlage für Verarbeitungen personenbezogener Daten im Zusammenhang mit Künstlicher Intelligenz herangezogen werden, vorausgesetzt, diese genügt den Anforderungen der Art. 4 Nr. 11,

Art. 6 Abs. 1 UAbs. 1 Buchst. a (bei besonderen Kategorien personenbezogener Daten zusätzlich Art. 9 Abs. 2 Buchst. a), Art. 7 DSGVO.[32] Danach muss eine rechtmäßige Einwilligung insbesondere für einen bestimmten Zweck, freiwillig, in informierter Weise und unmissverständlich erteilt werden.

Im Verhältnis zwischen Bürger und Staat kommt der Einwilligung als Rechtsgrundlage allerdings nur eingeschränkte Relevanz zu, da das Kriterium der Freiwilligkeit in dieser Konstellation kritisch zu sehen ist: Notwendig für die Freiwilligkeit ist ein freier Willensentschluss, das heißt eine echte und freie Wahl (EG 42 DSGVO). Nach EG 43 Satz 1 DSGVO soll eine Einwilligung keine taugliche Rechtsgrundlage darstellen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt und deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde.[33]

Für den Fall, dass eine bayerische öffentliche Stelle beispielsweise in Erwägung zieht, auf Einwilligungsbasis personenbezogene Daten aus einem KI-gestützten Antragsverfahren für ein Nachtraining des zugrundeliegenden KI-Systems nutzbar zu machen, muss die Einwilligung von dem betreffenden Verwaltungsverfahren dergestalt „entkoppelt" werden, dass für die betroffene Person ohne weiteres transparent erkennbar ist, dass ihre Entscheidung im Hinblick auf die Erteilung einer Einwilligung keinen Einfluss auf die Bearbeitung ihres Antrages haben kann. Insoweit empfiehlt es sich, die Einwilligung von der Antragseinreichung zu trennen und dieser nachzulagern (etwa: Hinweistext „Ihr Antrag wurde erfolgreich eingereicht", anschließend „weiter" und dann Text zur Einwilligung betreffend die Nutzung der personenbezogenen Antragsdaten zum Nachtraining des KI-Systems und Einwilligungsmöglichkeit).

Des Weiteren muss die Einwilligung so gestaltet sein, dass sie einen bestimmten Zweck im Sinne von Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO in Verbindung mit Art.°7 DSGVO hinreichend konkret erkennen lässt. In diesem Zusammenhang sollten der betroffenen Person im geschilderten Fall auch Informationen zu der verwendeten Künstlichen Intelligenz sowie zu deren Training, für das die einwilligungsgegenständlichen Daten verwendet werden sollen, zur Verfügung gestellt werden. Für die betroffene Person muss klar, transparent und nachvollziehbar dargestellt werden, wie „ihre" personenbezogenen Daten in das jeweilige KI-System oder KI-Modell einfließen, und insbesondere ob eine Umsetzung ihrer Betroffenenrechte, beispielsweise in Form von Löschung ihrer personenbezogenen Daten, möglich ist. Dies setzt eine umfassende Kenntnis der Architektur und der Funktionalitäten des betreffenden KI-Systems oder KI-Modells durch den Verantwortlichen voraus.

3.2.4.6 Art. 9 DSGVO-Daten

Vor dem Einsatz beziehungsweise Training oder Weiter-/Nachtraining von KI-Systemen oder KI-Modellen ist sorgfältig zu prüfen, ob die Verarbeitung von besonderen Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1

[32] Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz bei KI-Projekten in der bayerischen Verwaltung (Fn. 18), Rn. 229 ff.

[33] Ausführlich Bayerischer Landesbeauftragter für den Datenschutz, Die Einwilligung nach der Datenschutz-Grundverordnung, Orientierungshilfe, Stand 9/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

DSGVO im Raum steht. Insoweit ist zu berücksichtigen, dass solche besonders geschützten Daten auch durch eine Verschneidung „innerhalb des Systems" entstehen können. In diesem Fall wären dann zusätzlich zu Art. 6 Abs. 1 DSGVO die insofern gesteigerten Rechtmäßigkeitsanforderungen des Art. 9 Abs. 2 DSGVO zu beachten.[34]

Ob besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO verarbeitet werden, hängt maßgeblich vom Einsatzbereich eines KI-Systems oder KI-Modells ab. So wäre beispielsweise bei Nutzung von Sprachübersetzungstools, wozu mich im Berichtszeitraum mehrere Beratungsanfragen erreicht haben, diesbezüglich Folgendes zu beachten: Beim Einsatz von Tools zur Kommunikation fremdsprachiger Bürgerinnen und Bürger mit dem Gesundheits- oder Sozialamt ist regelmäßig davon auszugehen, dass deren Eingaben (sowohl in Form des gesprochenen als auch des geschriebenen Wortes) Gesundheitsdaten im Sinne von Art. 9 Abs. 1 in Verbindung mit Art. 4 Nr. 15 DSGVO enthalten. Dabei sind auch solche Daten erfasst, aus denen mittelbar Rückschlüsse auf den Gesundheitszustand möglich sind, sofern ein derartiger Auswertungskontext besteht. Bei einer größeren Menge an eingegebenen Informationen und unter Berücksichtigung der mit Künstlicher Intelligenz verbundenen Verschneidungsmöglichkeiten wird dies (im bestimmten Anwendungskontext, insbesondere im Gesundheitsamt) häufig anzunehmen sein. Daneben kann auch die Erfassung des gesprochenen Wortes, also der Sprache selbst, eine Verarbeitung von besonders sensiblen Daten (üblicherweise der Nutzerinnen und Nutzer, unter Umständen aber auch von Beschäftigten) im Sinne von Art. 9 Abs. 1 DSGVO begründen. Dies wäre beispielsweise dann der Fall, wenn bestimmte Sprachfehler ersichtlich wären oder aus der Sprache die ethnische Herkunft der nutzenden Person hervorginge, vgl. Art. 9 Abs. 1 DSGVO.

Neben Sicherstellung einer Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 DSGVO (gegebenenfalls in Verbindung mit Art. 4 Abs. 1 BayDSG, siehe oben unter 1.2.4.1) wäre die Verarbeitung besonders sensibler personenbezogener Daten im Zusammenhang mit der Nutzung eines KI-Systems oder KI-Modells wie eines Sprachübersetzungstools dann zusätzlich auch nach Art. 9 Abs. 2 DSGVO sowie gegebenenfalls Art. 8 BayDSG zu prüfen.

Die datenschutzrechtliche Generalklausel kommt dabei, wie bereits erläutert, nur dann als Rechtsgrundlage in Betracht, soweit es sich um Datenverarbeitungen mit eher geringer Eingriffsintensität handelt. Speziell mit Blick auf den Einsatz von Sprachübersetzungstools ist die hierfür erforderliche Bewertung anhand der Art der zu erfüllenden konkreten Aufgabe als auch der konkreten „Wirkweise" (etwa reine Texteingaben oder auch unmittelbare Spracheingaben) sowie des konkreten Einsatzszenarios des Betriebsmittels „Künstliche Intelligenz" zu bewerten: So wäre der Einsatz eines KI-Sprachübersetzungstools bei einer Kfz-Anmeldung als Übersetzungsunterstützung im Bedarfsfall anders zu bewerten als ein standardisierter Einsatz eines KI-Übersetzungstools zur Übersetzung aller fremdsprachigen Dokumente, die bei Antragstellung auf Sozialhilfeleistungen eingereicht werden. Sollte die Schwelle der geringen Eingriffsintensität (wie dies etwa im Fall der Verarbeitung besonders sensibler Daten regelmäßig anzunehmen ist) überschritten werden, wäre die jeweilige Datenverarbeitung an einer spezialgesetzlichen

[34] Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz bei KI-Projekten in der bayerischen Verwaltung (Fn. 18), Rn. 252 ff.

– insbesondere fachrechtlichen – (nationalen) Regelung im Sinne von Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 DSGVO zu messen.

3.2.5 Transparenz und Betroffenenrechte

Die sowohl für die Einordnung in das datenschutzrechtliche Rollenmodell als auch für die Identifikation von tragfähigen Rechtsgrundlagen erforderliche umfassende Kenntnis der Architektur und der Funktionalitäten des betreffenden KI-Systems oder KI-Modells durch den Verantwortlichen ist schließlich auch von wesentlicher Bedeutung für die Erfüllung der Transparenzanforderungen sowie die Gewährleistung und Umsetzung der Betroffenenrechte aus der Datenschutz-Grundverordnung gegenüber den betroffenen Personen.[35]

So müssen die nach Art. 13, Art. 14 DSGVO notwendigen Informationen eine transparente Darstellung zumindest der abstrakten Funktions- und Verfahrensweise des betreffenden KI-Systems oder KI-Modells umfassen, beispielsweise indem die einzelnen Verarbeitungsschritte eines KI-Systems oder KI-Modells von Anfang an soweit wie möglich nachvollzogen und für die Nutzer ebenso schrittweise beschrieben werden.

Auch in Bezug auf die Betroffenenrechte muss eine sorgfältig nach Verarbeitungsvorgängen getrennte Betrachtung erfolgen, die zudem den Stand der Technik und Wissenschaft berücksichtigt.

Eine vollumfängliche Umsetzung der datenschutzrechtlichen Anforderungen erfordert dabei regelmäßig, dass diese von Beginn an mitgedacht und bereits in den Konzeptions- und Entwicklungs- beziehungsweise Beschaffungsprozess für das jeweilige KI-System oder KI-Modell integriert werden.

3.2.6 Künstliche Intelligenz und Art. 22 DSGVO

Bereits bei der Konzeption von KI-basierten Systemen ist zudem zu bedenken, dass diese grundsätzlich keine menschliche Entscheidung mit Rechtswirkung ersetzen dürfen: Gemäß Art. 22 Abs. 1 DSGVO haben betroffene Personen das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung, einschließlich Profiling (Art. 4 Nr. 4 DSGVO), unterworfen zu werden, die ihnen gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.[36]

Gerade wenn ein KI-System oder KI-Modell durch bayerische öffentliche Stellen im Bürgerkontakt, mit Bürgerbezug oder im Verhältnis zu Beschäftigten eingesetzt wird, kann möglicherweise eine solche automatisierte Entscheidung im Sinne von Art. 22 Abs. 1 DSGVO vorliegen.[37] Soll beispielsweise ein KI-System durch Plausibilitätskontrollen oder „Vollständigkeitschecks“ die Beantragung einer Leistung durch Bürger unterstützen und gleichzeitig die Verwaltung durch Steigerung der „Antrags-Qualität“ entlasten, kann – abhängig von der konkreten

[35] Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz bei KI-Projekten in der bayerischen Verwaltung (Fn. 18), Rn. 295 ff.

[36] Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz bei KI-Projekten in der bayerischen Verwaltung (Fn. 18), Rn. 328 ff.

[37] Vgl. Europäischer Gerichtshof, Urteil vom 7. Dezember 2023, C-634/21.

Prozessausgestaltung – das in Art. 22 Abs. 1 DSGVO enthaltene Verbot automatisierter Entscheidungen eine Rolle spielen: Sollte eine automatisierte Entscheidung nicht aufgrund der Erfüllung eines der in Art. 22 Abs. 2 DSGVO (bei besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO zusätzlich Art. 22 Abs. 4 DSGVO) genannten Ausnahmetatbestände ausnahmsweise erlaubt sein, so muss der Prozess so gestaltet werden, dass keine automatisierte Entscheidung im Einzelfall vorliegt. Dies bedeutet, dass das zum Einsatz kommende System die Antragstellung nicht „unüberwindbar" verhindern darf, beispielsweise durch automatische Ablehnung nicht plausibler oder unvollständiger Anträge.

Anhaltspunkte für insoweit in Betracht kommende angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Personen lassen sich dabei dem eigentlich in Zusammenhang mit Art. 22 Abs. 2 bis 4 DSGVO anwendbaren EG 71 Satz 4 ff. DSGVO entnehmen. Angemessene Maßnahmen stellen danach insbesondere dar: das Recht der betroffenen Person, das direkte Eingreifen einer Person (das heißt insbesondere eines Amtsträgers der verantwortlichen Stelle) zu erwirken, das Recht auf Darlegung des eigenen Standpunkts, das Recht auf Anfechtung der Entscheidung, das Recht der betroffenen Person auf spezifische Unterrichtung, das Recht auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung, die Sicherstellung, dass im Regelfall keine Kinder betroffen sind, sowie technische und organisatorische Maßnahmen zur Gewährleistung einer fairen und transparenten Verarbeitung, insbesondere um das Risiko von Fehlern zu minimieren und diskriminierende Wirkungen zu vermeiden. Die ersten drei der genannten Kriterien, die auch in Art. 22 Abs. 3 DSGVO Ausdruck finden, sowie die technischen und organisatorischen Maßnahmen zur Gewährleistung einer fairen und transparenten Verarbeitung stellen dabei auch nach der Rechtsprechung des Europäischen Gerichtshofs diejenigen Maßnahmen dar, die mindestens zu ergreifen sind.[38] Im konkreten Beispielsfall könnte der KI-unterstützte Antragsprozess daher etwa so gestaltet werden, dass für den Antragstellenden die Möglichkeit besteht, ein von dem KI-gestützten System identifiziertes Problem bei der Antragstellung während des Antragsprozesses zu adressieren, beispielsweise durch eine erneute Dateneingabe beziehungsweise einen erneuten Dokumentenupload sowie die Eröffnung einer unmittelbaren Kontaktmöglichkeit zu der für das Verfahren verantwortlichen öffentlichen Stelle direkt an der kritischen Stelle des Verfahrens.

3.2.7 Weitere Entwicklungen

Zur Gewährleistung einer vertrauenswürdigen Künstlichen Intelligenz der Zukunft werde ich auch weiterhin die Entwicklungen der KI-spezifischen datenschutzrechtlichen Fragestellungen fortlaufend begleiten.

3.3 KI ohne Grenzen? Einsatz von Drittlandsprodukten in der bayerischen Verwaltung

Künstliche Intelligenz (KI) ist eine Schlüsseltechnologie der Digitalisierung. Ihr Potenzial lässt sich auch für eine Steigerung der Verwaltungseffizienz erschließen. Zunehmend leistungsfähige KI-Angebote unterschiedlicher Herkunft drängen auf

[38] Europäischer Gerichtshof, Urteil vom 7. Dezember 2023, C-634/21, Rn. 65 f.

den Markt. Bei bayerischen öffentlichen Stellen besteht mitunter eine gewisse Unsicherheit, inwiefern sie von diesem „Boom“ profitieren können – gerade, wenn attraktive Tools von Anbietern stammen, die außerhalb des Geltungsbereichs der Datenschutz-Grundverordnung beheimatet sind. Der vorliegende Beitrag befasst sich daher mit den Anforderungen aus den Bereichen Datenschutz (Nr. 3.3.1) und IT-Sicherheit (Nr. 3.3.2), denen bei Drittland-KI Rechnung getragen werden sollte.

3.3.1 Datenschutzrechtliche Anforderungen

Für Verarbeitungen personenbezogener Daten im Zusammenhang mit KI-Tools ist die Datenschutz-Grundverordnung zu beachten, wenn nach den allgemeinen Regeln ihr Anwendungsbereich eröffnet ist.

Verarbeitungen personenbezogener Daten kommen im Zusammenhang mit KI-Anwendungen vielfältig in Betracht, so beispielsweise

— im Rahmen des Trainings durch Erhebung und Nutzung von personenbezogenen Daten als Trainingsdaten,[39]

— bei der Nutzung in Form der Erhebung, Aufzeichnung und Speicherung von Anmeldedaten und Eingabeaufforderungen der Nutzenden (bei Großen Sprachmodellen [LLM] „Prompts“) oder

— durch Weiternutzung der Anmelde- und Eingabedaten zu eigenen Zwecken des Anbieters, etwa zum Weitertraining der KI-Anwendung, zur Erstellung und Erkennung von Nutzerprofilen – nicht nur aufgrund der Nutzung der betreffenden KI-Anwendung an sich, sondern zum Beispiel auch aufgrund von Tastatureingabemustern – sowie zu Analyse- oder Werbezwecken.

Zur umfassenden Gewährleistung des in Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz, Art. 8 Charta der Grundrechte der Europäischen Union verankerten Schutzes personenbezogener Daten findet die Datenschutz-Grundverordnung gemäß ihrem Art. 3 auf sämtliche Verarbeitungen personenbezogener Daten Anwendung, die in einem Zusammenhang mit der Europäischen Union stehen – unabhängig von der Niederlassung des Verantwortlichen und dem Ort der Verarbeitung.

Dabei gilt: Verarbeitet eine KI-Anwendung personenbezogene Daten in der Europäischen Union (sogenanntes Niederlassungsprinzip) oder befinden sich die betroffenen Personen in der Europäischen Union (sogenanntes Marktortprinzip), ist der Anwendungsbereich der Datenschutz-Grundverordnung eröffnet. Dann muss der datenschutzrechtlich Verantwortliche deren Anforderungen, insbesondere in Gestalt der Verarbeitungsgrundsätze des Art. 5 Abs. 1 DSGVO einhalten, unter anderem

[39] Bayerischer Landesbeauftragter für den Datenschutz, Fotos veröffentlichen = KI trainieren?, Aktuelle Kurz-Information 55, Stand 4/2024, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek“.

- das zwingende Erfordernis einer Rechtsgrundlage für die Datenverarbeitung (Art. 5 Abs. 1 Buchst. a, Art. 6 Abs. 1 DSGVO, bei Verarbeitungen besonderer Kategorien personenbezogener Daten in Verbindung mit Art. 9 DSGVO),

- den Grundsatz der Zweckbindung (Art. 5 Abs. 1 Buchst. b DSGVO, bei zweckändernden Weiterverarbeitungen Art. 6 Abs. 4 DSGVO und Art. 6 BayDSG),

- die Informationspflichten (Art. 5 Abs. 1 Buchst. a, Art. 12 ff. DSGVO)[40] und

- die Betroffenenrechte (Art. 15 ff. DSGVO).[41]

Hinzu treten bei Nutzung von Produkten von Drittlandanbietern regelmäßig die Vorgaben der Art. 44 ff. DSGVO betreffend Datenverarbeitungen mit Drittlandbezug.

Konkretisiert werden diese Vorgaben durch Art. 24 Abs. 1 Satz 1, Art. 25, Art. 32 Abs. 1 DSGVO, wonach unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen durch geeignete technische und organisatorische Maßnahmen sicherzustellen und nachzuweisen ist, dass die Verarbeitung im Einklang mit der Datenschutz-Grundverordnung erfolgt und ein dem Risiko angemessenes Schutzniveau gewährleistet wird.

Der datenschutzrechtlich Verantwortliche muss die Einhaltung der Anforderungen jederzeit nachweisen können (Art. 5 Abs. 2 DSGVO „Rechenschaftspflicht").

Datenschutzrechtlich Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist dabei die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Dies ist je nach Verarbeitungsvorgang der Anbieter oder der Betreiber[42] einer KI-Anwendung: Geht es um Verarbeitungen personenbezogener Daten im Zusammenhang mit der Entwicklung und dem Training einer KI-Anwendung, ist in der Regel der Anbieter für deren Datenschutzkonformität verantwortlich. Für Datenverarbeitungen, die mit der Nutzung einer KI-Anwendung einhergehen, trifft die datenschutzrechtliche Verantwortlichkeit dagegen den Betreiber der jeweiligen KI-Anwendung, das heißt beispielsweise die jeweilige die KI-Anwendung als Betriebsmittel einsetzende bayerische öffentliche Stelle, gegebenenfalls in Zusammenarbeit mit dem Anbieter als Auftragsverarbeiter im Sinne des Art. 28 DSGVO.

3.3.1.1 Speziell: datenschutzrechtliche Anforderungen an Drittlandanbieter

Verarbeitet eine KI-Anwendung eines nicht in der Europäischen Union niedergelassenen Verantwortlichen personenbezogene Daten von betroffenen Personen,

[40] Bayerischer Landesbeauftragter für den Datenschutz, Informationspflichten des Verantwortlichen, Orientierungshilfe, Stand 11/2018, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

[41] Bayerischer Landesbeauftragter für den Datenschutz, Das Recht auf Auskunft nach der Datenschutz-Grundverordnung, Orientierungshilfe, Stand 12/2019; Das Recht auf Löschung nach der Datenschutz-Grundverordnung, Orientierungshilfe, Stand 6/2022, jeweils Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

[42] Begrifflichkeiten in Anlehnung an Art. 3 Nr. 3 und 4 Verordnung (EU) 2024/1689 (Fn. 10).

die sich in der Europäischen Union befinden (Art. 3 Abs. 2 Buchst. a DSGVO), ist der Anwendungsbereich der Datenschutz-Grundverordnung eröffnet und muss der Verantwortliche die oben genannten Anforderungen einhalten.

Der (Drittland-)Anbieter einer KI-Anwendung ist dabei regelmäßig für Entwicklung und Training datenschutzrechtlich verantwortlich im Sinne des Art. 4 Nr. 7 DSGVO. Nicht in der Union niedergelassene Verantwortliche, die im Zusammenhang mit dem Angebot von Waren oder Dienstleistungen in der Union personenbezogene Daten von betroffenen Personen verarbeiten, die sich in der Union befinden (vgl. Art. 3 Abs. 2 Buchst. a DSGVO), müssen dabei nach Art. 27 Abs. 1 DSGVO schriftlich einen Vertreter in der Union benennen. Dies soll insbesondere die effektive Wahrnehmung und Durchsetzung der Betroffenenrechte ermöglichen und die Zusammenarbeit mit den europäischen Datenschutzaufsichtsbehörden erleichtern.

Stellt ein Anbieter eine KI-Anwendung zur Nutzung durch einen Dritten als Verantwortlichen (Betreiber) bereit, wird er je nach Einzelfallgestaltung gegebenenfalls als Auftragsverarbeiter im Sinne der Art. 28, Art. 29, Art. 4 Nr. 8 DSGVO tätig. Vorausgesetzt ist dabei, dass der Anbieter personenbezogene Daten (nur) im Auftrag und auf Weisung des Verantwortlichen verarbeitet.[43] In der Rolle des Auftragsverarbeiters muss der Anbieter hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen eine Verarbeitung im Einklang mit den Anforderungen der Datenschutz-Grundverordnung sicherstellen und so der Schutz der Rechte der betroffenen Personen gewährleistet ist (vgl. Art. 28 Abs. 1 DSGVO). Der Inhalt des Auftragsverarbeitungsverhältnisses ist in einem Vertrag oder anderen Rechtsinstrument entsprechend den Vorgaben des Art. 28 Abs. 3 DSGVO zu regeln. Bestimmt ein Auftragsverarbeiter allerdings entgegen Art. 29, Art. 4 Nr. 8 DSGVO die Zwecke und Mittel einer Verarbeitung personenbezogener Daten, ist er in Bezug auf diese Verarbeitung Verantwortlicher (Art. 28 Abs. 10 DSGVO). Dann treffen ihn auch die entsprechenden Pflichten. Das ist beispielsweise dann der Fall, wenn der Anbieter einer KI-Anwendung die Anmeldedaten und Eingabeaufforderungen des Betreibers als Verantwortlichen ohne dessen entsprechende Weisung erhebt, aufzeichnet und speichert oder wenn er diese Daten zu eigenen Zwecken wie dem Weitertraining der KI-Anwendung nutzt.

3.3.1.2 Speziell: datenschutzrechtliche Anforderungen an bayerische öffentliche Stellen als Betreiber

Nutzt eine bayerische öffentliche Stelle als Betreiber eine KI-Anwendung als Betriebsmittel zur Aufgabenerfüllung, ist die öffentliche Stelle insoweit datenschutzrechtlich Verantwortlicher, Art. 4 Nr. 7 Halbsatz 2 DSGVO in Verbindung mit Art. 3 Abs. 2, Art. 1 BayDSG. Sie muss die datenschutzkonforme Nutzung sicherstellen und nachweisen (Art. 5 Abs. 2 DSGVO). Der Verantwortliche muss dabei in Hinblick auf Art. 24 Abs. 1 und 2 DSGVO auch nachweisen können, dass er einer Pflicht zur „angemessenen Bewertung“[44] der Datenschutzkonformität der als Betriebsmittel eingesetzten KI-Anwendung nachgekommen ist, und dass er – soweit

[43] Bayerischer Landesbeauftragter für den Datenschutz, Auftragsverarbeitung, Orientierungshilfe, Stand 4/2019, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek“.

[44] Europäischer Datenschutzausschuss, Opinion 28/2024 (Fn. 16), Rn. 122. Die Aufsichtsbehörden sollten dabei unter anderem berücksichtigen, ob der Verantwortliche beispielsweise die für das der Anwendung zugrundeliegende KI-Modell verwendete Datenquelle und einen mögli-

erforderlich – eine Umsetzung sogenannter „mitigierender Maßnahmen“ geprüft hat.[45]

Wird die KI-Anwendung dabei ausschließlich in eigener Verantwortlichkeit (On-Premises, On-Prem) und in einem abgeschotteten System betrieben, besteht eine Alleinverantwortlichkeit der öffentlichen Stelle bezüglich sämtlicher Datenschutzaspekte.

Greift eine öffentliche Stelle für eine Verarbeitung personenbezogener Daten auf eine externe KI-Anwendung zurück, wird deren (Drittland-)Anbieter je nach Einzelfallgestaltung gegebenenfalls als Auftragsverarbeiter im Sinne der Art. 28, Art. 29, Art. 4 Nr. 8 DSGVO im Auftrag und auf Weisung für die öffentliche Stelle als Verantwortlichen tätig. Die öffentliche Stelle darf dabei ausweislich Art. 28 Abs. 1 DSGVO nur mit solchen Auftragsverarbeitern arbeiten, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der Datenschutz-Grundverordnung erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet. Dazu gehören auch die Einhaltung der gesetzlichen Vorgaben zu Drittstaatentransfers (Art. 44 ff. DSGVO, vgl. Nr. 3.3) sowie der Ausschluss von Verarbeitungen zu eigenen Zwecken des Anbieters. Den Verantwortlichen trifft insoweit eine fortlaufende Prüf- und Überwachungspflicht. Das Auftragsverarbeitungsverhältnis ist durch einen Vertrag oder ein anderes Rechtsinstrument entsprechend den Vorgaben des Art. 28 Abs. 3 DSGVO zu regeln.

Nutzt eine bayerische öffentliche Stelle eine KI-Anwendung eines Drittlandanbieters, ist ein besonderer Fokus auf die Voraussetzungen der Art. 44 ff. DSGVO zu legen, da es im Zusammenhang mit der Nutzung der KI-Anwendung regelmäßig zu Datenübermittlungen der nutzenden öffentlichen Stelle als Datenexporteur an den Anbieter als Datenimporteur in Länder außerhalb des Geltungsbereichs der Datenschutz-Grundverordnung, das heißt der Europäischen Union beziehungsweise des Europäischen Wirtschaftsraums (sogenannte Drittländer), kommt. Typischerweise finden Drittlandübermittlungen bei der Nutzung einer (fremdentwickelten) KI-Anwendung eines Drittlandanbieters als Cloud-Lösung statt, wenn der Server der Cloud sich ebenfalls in einem Drittland befindet oder unabhängig vom Serverstandort zumindest Meta- und Telemetriedaten in ein Drittland übermittelt werden; in diesem Fall stellt sich zudem die Frage der Datensouveränität.[46] Denkbar ist auch eine Drittlandübermittlung aufgrund der (gesetzlich angeordneten) Einräumung von Zugriffsrechten auf eine KI-Anwendung (und die darin enthaltenen personenbezogenen Daten) für drittstaatliche (Sicherheits-)Behörden oder verbundene Unternehmen.[47]

chen (gegebenenfalls aufsichtsbehördlich oder gerichtlich festgestellten) Verstoß des KI-Modells gegen die Datenschutz-Grundverordnung bewertet hat. Der Grad der Bewertung des Verantwortlichen und der von den Aufsichtsbehörden erwartete Detaillierungsgrad können dabei in Abhängigkeit von verschiedenen Faktoren variieren, einschließlich der Art und des Ausmaßes der Risiken, die durch die Verarbeitung im KI-Modell während seines Einsatzes in Bezug auf die betroffenen Personen, deren Daten zur Entwicklung des Modells verwendet wurden, entstehen, Rn. 130.

45 Hierzu Europäischer Datenschutzausschuss, Opinion 28/2024 (Fn. 16), Rn. 132, 134.

46 Zu den mit Cloud-Services verbundenen Problemstellungen vgl. Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz als Kriterium im Vergabeverfahren, Orientierungshilfe, Stand 2/2024, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek“.

47 Juarez, in: Wolff/Brink/v. Ungern-Sternberg, Beck’scher Online-Kommentar Datenschutzrecht,

Liegt ein solcher Drittstaatentransfer vor, spezifizieren Art. 44 ff. DSGVO die zusätzlichen Anforderungen an die Rechtmäßigkeit der Übermittlung personenbezogener Daten an Drittländer.[48]

— Hierbei ist zunächst zu prüfen, ob ein gültiger Angemessenheitsbeschluss der Europäischen Kommission für das Drittland im Sinne von Art. 45 Abs. 1 und 3 DSGVO vorliegt.

— Ist dies nicht der Fall beziehungsweise ist ein Angemessenheitsbeschluss auf den betreffenden Sachverhalt nicht anwendbar, kommt eine Datenübermittlung vorbehaltlich geeigneter Garantien (vgl. EG 108 DSGVO) sowie durchsetzbarer Rechte und wirksamer Rechtsbehelfe für die betroffenen Personen gemäß Art. 46 Abs. 1 DSGVO in Betracht, vorausgesetzt diese Garantien gewährleisten ein Schutzniveau für die übermittelten personenbezogenen Daten, das dem in der Union garantierten Schutzniveau der Sache nach gleichwertig ist. Ist dem Anbieter als Datenimporteur nach der Rechtslage im Drittland die Einhaltung seiner vertraglichen Verpflichtungen nicht möglich, beispielsweise aufgrund gesetzlicher Zugriffsbefugnisse für drittstaatliche (Sicherheits-)Behörden auf die verarbeiteten personenbezogenen Daten, muss der Verantwortliche als Datenexporteur auf der Grundlage einer umfassenden Prüfung der Datenschutzsituation im Drittland zusätzliche Maßnahmen ergreifen, die geeignet sind, die Einhaltung des Schutzniveaus zu gewährleisten.

— Kann die Übermittlung weder auf einen Angemessenheitsbeschluss nach Art. 45 Abs. 1 DSGVO noch auf geeignete Garantien nach Art. 46 Abs. 1 DSGVO gestützt werden, sieht Art. 49 DSGVO als Auffangtatbestand Ausnahmen für bestimmte Fälle von Drittlandübermittlungen vor.

Mit Blick auf die Rechenschaftspflicht des Art. 5 Abs. 2 DSGVO ist es bayerischen öffentlichen Stellen daher zu empfehlen, grundsätzlich nicht mit Drittlandanbietern von KI-Anwendungen zusammenzuarbeiten, die intransparent im Hinblick auf die von ihnen (im Auftrag) vorgenommene Verarbeitung personenbezogener Daten agieren.

Unter Beachtung der Art. 24 Abs. 1 Satz 1, Art. 25, Art. 32 Abs. 1 DSGVO[49] kann der On-Prem-Betrieb von KI-Systemen eine Maßnahme zur Risikominimierung und Gewährleistung des Datenschutzes darstellen. Durch die Kontrolle über die physische und logische Infrastruktur, auf der die KI-Anwendung betrieben wird, können bayerische öffentliche Stellen sicherstellen, dass die Datenverarbeitung im Einklang mit den datenschutzrechtlichen Anforderungen der Datenschutz-Grundverordnung steht. So kann die in Art. 25 DSGVO geforderte Datensicherheit durch Technikgestaltung und datenschutzfreundliche Voreinstellungen leichter

51. Edition 5/2023, Art. 44 DSGVO Rn. 15; Schröder, in: Kühling/Buchner, DSGVO/BDSG, 4. Aufl. 2024, Art. 44 DSGVO Rn. 16; Bayerischer Landesbeauftragter für den Datenschutz, Internationale Datentransfers, Orientierungshilfe, Stand 5/2023, Rn. 28 ff., Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

48 Zum Ganzen ausführlich Bayerischer Landesbeauftragter für den Datenschutz, Internationale Datentransfers (Fn. 47); Erste Hilfe zum Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework, Aktuelle Kurz-Information 51, Stand 12/2023, beide Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

49 Bayerischer Landesbeauftragter für den Datenschutz, Die Datenschutz-Grundverordnung – Anforderungen an Technik und Sicherheit der Verarbeitung, Stand 11/2017, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

umgesetzt werden. Eine aktive Steuerung der Sicherheitsmaßnahmen kommt der Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Daten zugute; die Abhängigkeit von externen Drittanbietern wird reduziert. Der On-Prem-Betrieb entbindet bayerische öffentliche Stellen jedoch nicht von ihrer Verantwortung, erforderliche Maßnahmen nach Art. 32 Abs. 1 DSGVO zu treffen. Um ein angemessenes Schutzniveau zu erreichen, muss stets in einer umfassenden Risikoanalyse geklärt werden, welche Risiken bestehen und wie ihnen zu begegnen ist.

Sind die datenschutzrechtlichen Vorgaben nicht vollumfänglich erfüllt, verstößt die betreffende Verarbeitung personenbezogener Daten mittels einer KI-Anwendung gegen die Datenschutz-Grundverordnung. Dies sollten öffentliche Stellen bei der Auswahl, der Beschaffung[50] und dem Einsatz entsprechender KI-Anwendungen, einschließlich der Etablierung technisch-organisatorischer Sicherungsmaßnahmen, beachten. Beschäftigte der öffentlichen Stellen sollten hierfür sensibilisiert werden.

3.3.2 KI-Verordnung und Cybersicherheit

Über diese datenschutzrechtlichen Problemstellungen hinaus sind unter anderem Anforderungen aus der KI-Verordnung[51] (speziell hinsichtlich Transparenz) sowie betreffend die Cybersicherheit zu beachten. Letztere steht insbesondere bei potenziellen Zugriffsmöglichkeiten drittstaatlicher (Sicherheits-)Behörden, bei schwachen Sicherheitsvorkehrungen und bei einer möglichen Manipulierbarkeit von KI-Anwendungen (für kriminelle Zwecke) in Frage.

Eine kürzlich bekannt gewordene Datenpanne bei einer Drittland-KI verdeutlicht die Risiken, die mit unzureichenden Sicherheitsmaßnahmen bei KI-Anwendungen verbunden sind: Aufgrund einer Fehlkonfiguration war eine Datenbank mit über einer Million sensibler Datensätze, darunter Chatverläufe und Systemprotokolle, ungeschützt und öffentlich im Internet erreichbar. Die Sicherheitslücke erlaubte nicht nur den Zugriff auf vertrauliche Informationen, sondern eröffnete auch die Möglichkeit zur Manipulation der Datenbank. Obwohl das Unternehmen nach der Entdeckung schnell reagierte und die Datenbank sicherte, bleibt nicht nur unklar, wie lange die Daten vorher exponiert waren, sondern auch, ob unbefugte Dritte darauf zugegriffen haben. Dieser Vorfall unterstreicht die Notwendigkeit wirksamer Sicherheitsanforderungen für KI-Anwendungen, insbesondere wenn diese aus Ländern stammen, in denen Datenschutz- und Sicherheitsstandards möglicherweise nicht den europäischen Anforderungen entsprechen.

[50] Zur Berücksichtigung von Datenschutz als Kriterium im Vergabeverfahren Fn. 46.
[51] Fn. 42.

4 Polizei, Justiz, Verfassungsschutz

4.1 Einsatz von Vertrauenspersonen und Verdeckten Ermittlern

Gemäß dem Bericht des Parlamentarischen Kontrollgremiums vom 8. Februar 2023 (Landtags-Drucksache 18/26890) meldete die Bayerische Polizei für das Jahr 2021 zwei Einsätze von Verdeckten Ermittlern gegen eine bestimmte Person mit Wohnungsbetretung nach Art. 37 Abs. 2, Abs. 1 Polizeiaufgabengesetz (PAG) und einen Einsatz einer Vertrauensperson gegen eine bestimmte Person mit Wohnungsbetretung nach Art. 38 Abs. 2, Abs. 1 PAG.

Im Rahmen meiner gesetzlichen Verpflichtung nach Art. 51 Abs. 2 Satz 1 PAG habe ich im Berichtszeitraum im Zusammenhang mit diesen Einsätzen eine Prüfung durchgeführt. Hierfür habe ich bei einem Vor-Ort-Termin Einsicht die betreffenden Unterlagen eingesehen und zu den berichteten Fällen Nachfragen gestellt, welche mir die Polizei bereitwillig beantwortet hat.

Im Ergebnis habe ich im Rahmen der Prüfung insbesondere folgende Punkte bezüglich der Zurückstellung der Benachrichtigung sowie der Protokollierung der Maßnahmen festgestellt:

– Dokumentation

  Im Falle eines Einsatzes eines Verdeckten Ermittlers oder einer Vertrauensperson sind die betroffenen Personen gemäß Art. 50 Abs. 1 Satz 1 Nr. 3 PAG unverzüglich zu benachrichtigen, sobald dies ohne Gefährdung des Zwecks der Maßnahme, der eingesetzten Polizeibeamten, der Vertrauenspersonen oder der in der jeweiligen Befugnisnorm genannten Rechtsgüter möglich ist. Wird die Benachrichtigung zurückgestellt, so sind die Gründe hierfür gemäß Art. 50 Abs. 5 PAG zu dokumentieren, um eine effektive Kontrolle zu ermöglichen. Laut der polizeilichen Dokumentation im geprüften Fall erfolgte die Zurückstellung zwar wegen Gefährdung der Weiterverwendung des Verdeckten Ermittlers beziehungsweise der Vertrauensperson. Inwiefern die Zurückstellung wirklich geboten war, konnte ich anhand der erfolgten Dokumentation jedoch kaum nachvollziehen. Die Zurückstellungsgründe konnte ich letztlich nur aus den folgenden richterlichen Beschlüssen entnehmen. Es mangelte damit an einer ordnungsgemäßen Dokumentation der polizeilichen Zurückstellung im Sinne des Art. 50 Abs. 5 PAG.

  Ich wies die Polizei zudem darauf hin, dass allein die bloße Gefährdung des künftigen Einsatzes des Verdeckten Ermittlers oder der Vertrauensperson nach Abschluss des Verfahrens für eine Zurückstellung der Benachrichtigung grundsätzlich noch nicht ausreicht. Andernfalls würde die Benachrichtigungspflicht für unabsehbare Zeit ausgeschlossen und letztlich von zukünftigen ermittlungstaktischen Erwägungen der Sicherheitsbehörden abhängig gemacht. Dies widerspricht dem verfassungsrechtlichen Anliegen der Gewährung effektiven Rechtsschutzes. Aus Art. 50 Abs. 1 Satz 2 PAG ergibt sich allerdings, dass eine Gefährdung der weiteren Verwendung von Verdeckten Ermittlern beziehungsweise von Vertrauenspersonen als ein bedeutender Belang jedoch im Rahmen der vorzunehmenden Abwägung berücksichtigt werden kann.

— Zurückstellungsfrist

  Gemäß Art. 50 Abs. 4 Nr. 2 PAG bedarf die weitere Zurückstellung einer Benachrichtigung der richterlichen Zustimmung, wenn sie nicht ein Jahr nach Beendigung der Maßnahme erfolgt. Zwar konnte die Polizei im Rahmen der Prüfung einen gerichtlichen Beschluss zur weiteren Zurückstellung nachweisen, jedoch wurde hierbei die genannte Jahresfrist aufgrund einer verspäteten Antragsstellung nicht gewahrt.

— Protokollierung

  Gemäß Art. 51 Abs. 1 Satz 1 PAG müssen die Einsätze auch entsprechend protokolliert werden. Die Polizei verwendete hierfür das mir bereits bekannte Tool „ProMa“ (Protokollierung polizeilicher Maßnahmen), welches die vom Bundesverfassungsgericht in seinem BKAG-Urteil aufgestellten Anforderungen grundsätzlich gut erfüllt (siehe hierzu bereits mein 34. Tätigkeitsbericht 2024 unter Nr. 2.8). Die konkrete Befüllung des Tools offenbarte allerdings zum Teil Schwierigkeiten bei der Auslegung datenschutzrechtlicher Begrifflichkeiten. Im Rahmen der Prüfung konnte ich bei der Klärung der fraglichen Begriffsbestimmungen behilflich sein.

Abschließend habe die Polizei über die festgestellten Mängel schriftlich informiert und um zukünftige Beachtung der gesetzlichen Vorgaben gebeten.

4.2 Verwarnung eines Polizeipräsidiums wegen rechtswidriger Ausschreibung zur „Kontrolle, soweit nach Polizeirecht zulässig“

Im Berichtszeitraum wurde ich auf einen Fall aufmerksam, bei dem eine Person durch das Vorgehen eines Polizeipräsidiums erheblich in ihren Datenschutzrechten verletzt wurde. Ich habe den Vorgang mit einer Verwarnung des Polizeipräsidiums gemäß Art. 58 Abs. 2 Buchst. b DSGVO in Verbindung mit Art. 28 Abs. 1 Satz 1 Nr. 1, Abs. 2 Satz 2, Art. 34 Abs. 1 Satz 1 BayDSG und Art. 66 Satz 1 Polizeiaufgabengesetz (PAG) abgeschlossen.

Vorausgegangen war das an mich gerichtete Ersuchen der Person, insbesondere die Umstände einer für sie selbst unerklärlichen Ausschreibung „Kontrolle, soweit nach Polizeirecht zulässig“, aufzuklären, die ihr von einer außerbayerischen Polizeibehörde im Rahmen eines Auskunftsantrags mitgeteilt worden war.

Diesen Fahndungshinweis hatte ein bayerisches Polizeipräsidium im Informationssystem der Polizei „INPOL“ veranlasst, und er war dort bundesweit für die daran angeschlossen Polizeibehörden in direkter Verknüpfung mit den personenbezogenen Daten der betreffenden Person abrufbar. Hinzu kam, dass diese Ausschreibung im Rahmen eines weiteren Auskunftsantrags von der Bayerischen Polizei gegenüber der betroffenen Person, anders als von der Polizei des anderen Bundeslandes, nicht offengelegt wurde.

Die Befugnis zur Ausschreibung von personenbezogenen Daten zur gezielten Kontrolle stützt sich auf Art. 40 PAG:

Art. 40 PAG
Ausschreibung zur polizeilichen Beobachtung

(1) Unbeschadet der Möglichkeiten zur Ausschreibung nach dem Recht der Europäischen Union kann die Polizei personenbezogene Daten, insbesondere die Personalien einer Person sowie Kennzeichen eines von ihr benutzten Fahrzeugs, zur polizeilichen Beobachtung oder gezielten Kontrolle ausschreiben, wenn

1. die Gesamtwürdigung der Person einschließlich ihrer bisher begangenen Straftaten erwarten lässt, dass von ihr auch künftig eine Gefahr für bedeutende Rechtsgüter ausgeht,
2. sie für eine drohende Gefahr für bedeutende Rechtsgüter verantwortlich ist oder
3. tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass es sich um eine mutmaßlich mit der Gefahrenlage im Zusammenhang stehende Kontaktperson einer Person nach Nr. 1 oder Nr. 2 handelt.

[...]

Das Polizeiaufgabengesetz ordnet eine Ausschreibung „zur gezielten Kontrolle" gemäß Art. 40 PAG als Maßnahme der Datenerhebung ein und verlangt aufgrund des hohen Eingriffsgewichts dementsprechend hohe Voraussetzungen für eine entsprechende Veranlassung. So setzt etwa Art. 40 Abs. 1 Satz 2 Nr. 1 PAG voraus, dass die Gesamtwürdigung der Person einschließlich ihrer bisher begangenen Straftaten erwarten lässt, dass von ihr auch künftig eine Gefahr für bedeutende Rechtsgüter ausgeht.

Im Zuge meiner datenschutzrechtlichen Prüfung wurde allerdings sehr frühzeitig klar, dass diese materiellen Voraussetzungen in Bezug auf die betroffene Person nicht gegeben waren.

Auf meine Anfrage hin konnte das veranlassende Polizeipräsidium jedoch keine zutreffende Rechtsgrundlage angeben. Auch sollte mit der Fahndungsnotierung „Kontrolle, soweit nach Polizeirecht zulässig" zulasten der betroffenen Person gar keine Ausschreibung zur gezielten Kontrolle nach Art. 40 PAG beabsichtigt gewesen sein, sondern ein anderer Zweck verfolgt werden – so zumindest die Einlassung der Polizei. Diese „andere Zielsetzung" der Ausschreibung konnte mir trotz umfangreichen Schriftverkehrs nicht schlüssig dargelegt werden. Zudem würde ein anderer nicht erkennbarer subjektiver Wille des Polizeipräsidiums nichts daran ändern, dass Polizeibeamte im gesamten Bundesgebiet die veranlasste Ausschreibung im INPOL nur im Sinne einer „gezielten Kontrolle" verstehen konnten.

Da die Polizei nicht von einer Maßnahme nach Art. 40 PAG ausging, war in der Folge die Anordnung der Ausschreibung zur gezielten Kontrolle zusätzlich entgegen der gesetzlichen Regelungen weder durch einen hochrangigen Polizeibeamten oder eine hochrangige Polizeibeamtin erfolgt (sog. Behördenleitervorbehalt; Art. 40 Abs. 3 Satz 1 PAG), noch war die Befristung der Maßnahme auf die Dauer eines Jahres (Art. 40 Abs. 3 Satz 3 PAG) beachtet worden.

Des Weiteren sind die von einer Maßnahme betroffenen Personen gemäß Art. 50 Abs. 1 Nr. 4 PAG unverzüglich zu benachrichtigen, sobald dies ohne Gefährdung des Zwecks der Maßnahme, der eingesetzten Polizeibeamten oder Vertrauenspersonen oder der in der jeweiligen Befugnisnorm genannten Rechtsgüter geschehen kann. Nachdem das Polizeipräsidium den zutreffenden Art. 40 PAG als nicht einschlägig erachtete, wäre demzufolge auch keine Benachrichtigung nach Art. 50 PAG vorgesehen gewesen. Der betroffenen Person wären dadurch nachträgliche Rechtsschutzmöglichkeiten verwehrt geblieben, zumal die Maßnahme erst auf meine Nachfrage hin überhaupt (nachträglich) beauskunftet worden ist.

Darüber hinaus legt Art. 51 Abs. 2 Satz 1 und 2 PAG fest, dass ich im Bereich der Maßnahmen nach den Art. 34 bis 46 PAG im Abstand von längstens zwei Jahren eine Kontrolle durchführe und mir zu diesem Zweck die Protokolle sowie die Dokumentationen von Datenlöschungen und Vernichtungen von Unterlagen in auswertbarer Weise zur Verfügung zu stellen sind. Schließlich werden auch darüber die Datenschutzrechte von Betroffenen „besonderer Maßnahmen der Datenerhebung“ gewahrt und die Rechtsschutzmöglichkeiten im Bereich dieser in aller Regel verdeckten polizeilichen Maßnahmen gestärkt.

Daher kam für mich als Datenschutzaufsichtsbehörde erschwerend hinzu, dass durch die vom Polizeipräsidium praktizierte Vorgehensweise meine gesetzlichen Kontrollmöglichkeiten und Kontrollpflichten nach Art. 51 Abs. 2 Satz 1 PAG untergraben wurden. Denn wenn wie im vorliegenden Fall eine Ausschreibung zur gezielten Kontrolle aus für mich nicht nachvollziehbaren Gründen nicht nach dem zutreffenden Art. 40 PAG veranlasst wird, würde ich demzufolge von dem Polizeipräsidium auf eine entsprechende Anfrage hin weder diesen noch vergleichbare Fälle vorgelegt bekommen.

Auch wenn die Ausschreibung „Kontrolle, soweit nach Polizeirecht zulässig“ bezüglich der betroffenen Person schließlich gelöscht wurde, war angesichts der Erheblichkeit des Datenschutzverstoßes eine Verwarnung des Polizeipräsidiums erforderlich.

4.3 Bodycam-Einsatz in Bezirkskrankenhäusern

Regelmäßig finden polizeiliche Einsätze auch in Bezirkskrankenhäusern statt. Die Polizei wird in diesen Fällen meistens kontaktiert, um das Pflegepersonal in konkreten Situationen zu unterstützen. Oft geht es um die Fixierung der zu behandelnden Person durch die Anwendung von unmittelbarem Zwang. Immer wieder werden die polizeilichen Einsätze dabei mittels „körpernah getragenen Aufnahmegeräten“, den sogenannten „Bodycams“ aufgezeichnet.

Nach einem solchen Ereignis wandte sich die Datenschutzbeauftragte eines Bezirks an mich und trug vor, dass die an der Fixierung beteiligten Beschäftigten des Bezirkskrankenhauses anlässlich der Videoaufzeichnung stark verunsichert gewesen seien. Dies nahm ich zum Anlass, den Einsatz von Bodycams im Zusammenhang mit Bezirkskrankenhäusern datenschutzrechtlich zu prüfen. Stichprobenartig habe ich hierfür insgesamt drei entsprechende Einsätze bei zwei unterschiedlichen Polizeipräsidien überprüft. Durch die angeforderten Videoaufzeichnungen, welche etwa drei bis sieben Minuten lang waren, konnte ich mir ein gutes Bild über die jeweiligen Situationen verschaffen.

So stellte ich fest, dass die Bodycam-Aufzeichnungen teilweise auf dem Flur und im Aufenthaltsraum der geschlossenen Abteilung erfolgten. Für diese Aufzeichnungen konnten mir die Polizeipräsidien im Rahmen ihrer Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO in Verbindung mit Art. 28 Abs. 1 Satz 1 Nr. 1, Abs. 2 Satz 1 Nr. 2 BayDSG und Art. 66 Satz 1 Polizeiaufgabengesetz (PAG) jedoch nicht die erforderliche Befugnis gemäß Art. 6 Abs. 1 UAbs. 1 DSGVO in Verbindung mit Art. 28 Abs 1 Satz 1 Nr. 1, Abs. 2 Satz 1 Nr. 2 BayDSG nachweisen. Die Aufzeichnungen konnten insbesondere nicht auf den speziell dafür vorgesehenen Art. 33 Abs. 4 PAG gestützt werden. Dieser lautet wie folgt:

„[1]Die Polizei kann bei Maßnahmen der Gefahrenabwehr an öffentlich zugänglichen Orten Personen offen mittels automatisierter Bild- und Tonaufzeichnung, insbesondere auch mit körpernah getragenen Aufnahmegeräten, kurzfristig technisch erfassen, wenn dies zum Schutz von Polizeibeamten oder Dritten erforderlich ist. [2]Verarbeitungsfähige Aufzeichnungen dürfen gefertigt werden, wenn dies nach den Umständen zum Schutz von Polizeibeamten oder eines Dritten vor Gefahren für ein bedeutendes Rechtsgut erforderlich ist. [3]In Wohnungen dürfen Maßnahmen nach diesem Absatz nur zur Abwehr einer dringenden Gefahr für Leben, Gesundheit oder Freiheit einer Person erfolgen, sofern damit nicht die Überwachung der Wohnung verbunden ist. [4]Der Einsatz von körpernah getragenen Aufzeichnungsgeräten in Wohnungen soll gegenüber den Betroffenen in geeigneter Weise dokumentiert werden. [5]Eine Verwertung der nach Satz 3 erlangten Erkenntnisse ist zum Zweck der Gefahrenabwehr nur zulässig, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt wurde. [6]In Wohnungen darf zudem keine kurzfristige technische Erfassung ohne unverzügliche Fertigung verarbeitungsfähiger Aufzeichnungen erfolgen. [7]Es ist sicherzustellen, dass im Falle einer kurzfristigen technischen Erfassung im Sinn von Satz 1, an die sich keine unverzügliche Fertigung verarbeitungsfähiger Aufzeichnungen anschließt, die betroffenen personenbezogenen Daten unverzüglich gelöscht werden."

Art. 33 Abs. 4 PAG stellt die Befugnis für einen Einsatz von Bodycams an „öffentlich zugänglichen Orten" und in „Wohnungen" dar. Unter „öffentlich zugänglichen Orten" versteht man im Allgemeinen alle Orte, die von jedermann (jedenfalls zeitweise) ohne Beschränkung betreten werden können. Eine geschlossene Abteilung eines Bezirkskrankenhauses kann mit ihren strikten Zugangsregeln damit keinesfalls als „öffentlich zugänglicher Ort" gewertet werden. Das Merkmal „an öffentlich zugänglichen Orten" wurde auch auf mein Betreiben ins Gesetz aufgenommen, um einen ausufernden Einsatz zu verhindern und um gerade zu vermeiden, dass sich Einsätze von Bodycams der Kontrolle durch die Öffentlichkeit entziehen.

Im Wesentlichen wurde von der Polizei sodann vertreten, dass, wenn schon ein Einsatz in Wohnungen stattfinden dürfe, dann erst recht ein Einsatz auf dem Flur oder im Aufenthaltsraum eines Bezirkskrankenhauses möglich sein müsse. Dieser Argumentation konnte ich mich jedoch nicht anschließen, da diese Örtlichkeiten nicht „weniger" als eine Wohnung, sondern etwas völlig anderes sind.

Ich habe die festgestellten Verstöße gegenüber den Polizeipräsidien gemäß Art. 16 Abs. 4 BayDSG beanstandet. Das Bayerisches Staatsministerium des Innern, für Sport und Integration habe ich hierüber in Kenntnis gesetzt. Zusätzlich habe ich darauf hingewiesen, dass ich auch Zweifel an der grundsätzlichen Geeignetheit des Einsatzes von Bodycams in Bezirkskrankenhäusern habe. Zwar ist ein disziplinierender Effekt einer offenen Videoaufzeichnung grundsätzlich nicht von der Hand zu weisen. Dennoch werden bei Personen, die sich in Bezirkskrankenhäusern befinden (ähnlich wie im Falle stark alkoholisierter Personen), die verhaltenslenkenden Wirkungen erheblich eingeschränkt sein. Dies war auch auf den der Prüfung zugrundeliegenden Aufzeichnungen eindeutig zu erkennen.

Ich habe außerdem darauf hingewiesen, dass ich die Erfassung Dritter in diesem Zusammenhang als problematisch ansehe, da Art. 33 Abs. 7 PAG die Verarbeitung sensibler Gesundheitsdaten nicht ausdrücklich erlaubt. Die Tatsache, dass sich jemand in einer geschlossenen Abteilung eines Bezirkskrankenhauses befindet, wird jedoch in den meisten Fällen als Gesundheitsdatum einzustufen sein. Der Argumentation der Polizei, dass es für die kameraführenden Polizeibeschäftigten jedoch schwierig sei, in einer Fixierungssituation zusätzlich das Hintergrundgeschehen im Blick zu behalten und gegebenenfalls eine Erfassung Dritter zu verhindern,

zeigt nur umso mehr, dass Bodycams in einer solchen Situation nicht eingesetzt werden sollten.

4.4 Unzulässige Datenübermittlung an die Mutter einer Beschuldigten

Im Rahmen eines Ermittlungsverfahrens gegen eine junge Frau hat die ermittelnde Polizeibeamtin darauf bestanden, dass die Mutter der Beschuldigten bei der Aussage anwesend sein soll. Trotz der wiederholten Ablehnung dieser Forderung durch die – zu diesem Zeitpunkt bereits volljährige – Frau hat die Polizeibeamtin die Mutter kontaktiert, diese über den Vorfall aufgeklärt und einen gemeinsamen Termin vereinbart.

Die junge Frau legte daraufhin Beschwerde bei mir ein. Im Rahmen der eingeholten Stellungnahme beim betroffenen Polizeipräsidium hat dieses den Fehler sofort eingeräumt. Der Fehler sei aufgrund eines Rechtsirrtums der Beamtin erfolgt, die davon ausgegangen sei, dass auch bei Heranwachsenden die Eltern eingebunden werden müssten. Eine derartige gesetzliche Befugnis existiert jedoch nicht. Auch konnte die Datenübermittlung nicht auf Art. 59 Abs. 1 Polizeiaufgabengesetz gestützt werden, da sie insbesondere nicht zur Aufgabenerfüllung erforderlich war.

Ich habe gegenüber dem Polizeipräsidium einen Datenschutzverstoß festgestellt, da die Polizei personenbezogene Daten ohne erforderliche Befugnis gemäß Art. 6 Abs. 1 UAbs. 1 DSGVO in Verbindung mit Art. 28 Abs 1 Satz 1 Nr. 1, Abs. 2 Satz 1 Nr. 2 BayDSG an Dritte übermittelt hat. Von aufsichtlichen Maßnahmen habe ich im Rahmen des mir eingeräumten Ermessens gleichwohl abgesehen. Das Polizeipräsidium hatte die Angelegenheit bereits umfangreich aufgearbeitet, so dass aufsichtliche Maßnahmen keinen Mehrwert gehabt hätten. Die Dienststellenleitung und die handelnde Beamtin haben sich inzwischen bei der jungen Frau entschuldigt.

4.5 Freiwillige Angaben im Ordnungswidrigkeitenverfahren

Ein wiederkehrendes Thema in meiner Prüfungspraxis stellt die datenschutzrechtliche Zulässigkeit von Maßnahmen im Rahmen der Verfolgung und Ahndung von Ordnungswidrigkeiten im Straßenverkehr dar. Hierzu hatte ich in vergangenen Tätigkeitsberichten wiederholt ausgeführt, so unter anderem im 30. Tätigkeitsbericht 2020 unter Nr. 2, im 29. Tätigkeitsbericht 2019 unter Nr. 4.5, im 27. Tätigkeitsbericht 2016 unter Nr. 5.6 und im 26. Tätigkeitsbericht 2014 unter Nr. 5.5.1, Nr. 5.5.2 und Nr. 5.5.3.

In aller Regel werden auf Grundlage der Ermittlungsgeneralklausel nach § 46 Abs. 1 Ordnungswidrigkeitengesetz (OWiG) in Verbindung mit §161 Abs. 1 Strafprozeßordnung (StPO) an Zeugen und Betroffene einer Ordnungswidrigkeit von der Verfolgungsbehörde Anhörungsbögen zur Aufklärung des Sachverhalts versandt. Im Hinblick auf die Vorschrift des § 111 OWiG haben die genannten Personen sodann wenigstens Angaben zu Vor-, Familien- oder Geburtsnamen, dem Ort und Tag ihrer Geburt, ihrem Familienstand, ihrem Beruf, ihrem Wohnort, ihrer Wohnung und ihrer Staatsangehörigkeit zu machen. Weitere Angaben zur Person sind freiwillig.

§ 111 OWiG
Falsche Namensangabe
(1) Ordnungswidrig handelt, wer einer zuständigen Behörde, einem zuständigen Amtsträger oder einem zuständigen Soldaten der Bundeswehr über seinen Vor-, Familien- oder Geburtsnamen, den Ort oder Tag seiner Geburt, seinen Familienstand, seinen Beruf, seinen Wohnort, seine Wohnung oder seine Staatsangehörigkeit eine unrichtige Angabe macht oder die Angabe verweigert.
[…]

In einem von mir geprüften Fall verwendete die Verfolgungsbehörde einen Anhörungsbogen für Betroffene nach § 55 OWiG, der zwar zwischen den genannten Pflichtangaben und freiwilligen Angaben unterschied. Allerdings ordnete der Anhörungsbogen auch Angaben zur Telefonnummer und zum Arbeitgeber den Pflichtangaben zu. Ich konnte erreichen, dass der Anhörungsbogen entsprechend abgeändert wurde, so dass Angaben zur Telefonnummer künftig zwar weiterhin möglich, jedoch ausdrücklich als freiwillige Angaben gekennzeichnet sind. Die Frage nach dem Arbeitgeber wurde komplett aus dem Abhörungsbogen entfernt.

4.6 Offenlegung des Tatvorwurfs einer Ordnungswidrigkeit gegenüber dem Arbeitgeber des Betroffenen

Ein Bürger wandte sich mit einer Beschwerde an mich und rügte, dass im Rahmen der Verfolgung einer von ihm begangenen Ordnungswidrigkeit zunächst sein Arbeitgeber unter Offenlegung des gesamten Tatvorwurfs von der betreffenden Stadt als für die Verfolgung der Ordnungswidrigkeit zuständigen Behörde angeschrieben worden war.

Der Betroffene war dabei beobachtet worden, wie er unzulässigerweise Abfall in einer Wertstoffinsel entsorgte. Da er hierbei mit einem Auto unterwegs war, konnte ein Zeuge das Kennzeichen notieren und die Stadt in der Folge eine Halterabfrage durchführen.

Im Rahmen der von mir durchgeführten Prüfung unter Beiziehung der entsprechenden Bußgeldakte stellte sich heraus, dass der Stadt der Name des Betroffenen bereits frühzeitig vom Leasinggeber als Halter des Fahrzeugs mitgeteilt worden war. Als Adresse des Fahrzeughalters hatte der Leasinggeber eine Firmenanschrift mitgeteilt. Gleichzeitig hatte der Leasinggeber den Namen des unter der Firmenanschrift ansässigen Unternehmens angegeben. Dadurch war objektiv erkennbar, dass es sich bei dem betreffenden Fahrzeug um den Firmenwagen des Betroffenen handelte. Dennoch wurde zunächst nicht der Betroffene selbst unter der Firmenanschrift angeschrieben, sondern das ebenfalls genannte Unternehmen. Das Schreiben diente dazu, die Privatadresse des Betroffenen bei dem Unternehmen als seinem Arbeitgeber zu erfragen. Im Rahmen dieses Schreibens wurde – ohne dass dies für die Ermittlungen erforderlich gewesen wäre – der gesamte Tatvorwurf gegenüber dem Arbeitgeber des Betroffenen offengelegt. In dem betreffenden Fall wäre es der Stadt ohne weiteres möglich gewesen, den Beschwerdeführer zunächst selbst unter der Firmenanschrift anzuschreiben und seine Privatadresse auf diesem Weg zu erfragen. Denkbar wäre es auch gewesen, den Arbeitgeber ohne Offenlegung der Einzelheiten des Tatvorwurfs im Wege einer Zeugenbefragung um Mitteilung der Privatadresse des Betroffenen zu ersuchen.

Das Vorgehen der Stadt begründete somit einen Verstoß gegen Art. 5 Abs. 1 Buchst. a DSGVO in Verbindung mit Art. 28 Abs. 1 Satz 2, Abs. 2 Nr. 2 BayDSG (Grundsatz der Rechtmäßigkeit der Datenverarbeitung), da die erfolgte Datenübermittlung für den Ermittlungszweck nicht erforderlich war und daher auch nicht von der Ermittlungsgeneralklausel gemäß § 46 Abs. 2 Gesetz über Ordnungswidrigkeiten in Verbindung mit § 161 Abs. 1 Strafprozeßordnung gedeckt war.

Ich sprach daher eine Verwarnung gegenüber der Stadt aus. Die Stadt hat den Verstoß eingeräumt und angekündigt, die in diesem Bereich tätigen Mitarbeiter entsprechend zu sensibilisieren, um vergleichbare Verstöße künftig zu vermeiden.

4.7 Unzulässige Datenübermittlung an die Presse im Zusammenhang mit einer Versammlung

Aufgrund der Bearbeitung einer Beschwerde war ich mit einer unzulässigen Datenübermittlung im Zuge einer Versammlung befasst. Im Rahmen einer groß angelegten landkreisübergreifenden Versammlung übermittelten die Anmelder der Versammlung Unterlagen zu deren Standort und Verlauf an die zuständigen Sicherheitsbehörden. Des Weiteren enthielten diese Unterlagen unter anderem Namen und Telefonnummern der jeweiligen organisatorischen Ansprechpartner vor Ort. Diese personenbezogenen Daten eines der Betroffenen wiederum wurden von einer der Sicherheitsbehörden an die Presse übermittelt, da man die genannten Unterlagen als Anhang zu einer Pressemitteilung hinzugefügt hatte.

Dieses Vorgehen verletzte den Betroffenen in seinem Recht aus Art. 5 Abs. 1 Buchst. a, Art. 6 Abs. 1 DSGVO (Grundsatz der Rechtmäßigkeit der Datenverarbeitung), da diese Datenübermittlung weder von einer Einwilligung des Betroffenen gedeckt noch eine sonstige Rechtsgrundlage für diese Datenübermittlung ersichtlich war.

Eine weitere Veröffentlichung dieser Daten durch die Presse unterblieb indes, da die Sicherheitsbehörde den Fehler alsbald bemerkte und entsprechend mittels Versands einer bereinigten Anlage zur Pressemitteilung korrigierte.

Aufgrund dieser Umstände habe ich gegen die Sicherheitsbehörde eine Verwarnung gemäß Art. 58 Abs. 2 Buchst. b DSGVO ausgesprochen.

4.8 Prüfung eines abgelehnten Auskunftsantrags beim Bayerischen Landesamt für Verfassungsschutz

Das Bayerische Landesamt für Verfassungsschutz (BayLfV) hat den gesetzlichen Auftrag, Informationen unter anderem über Bestrebungen zu sammeln und auszuwerten, die gegen die freiheitliche demokratische Grundordnung gerichtet sind. Im Rahmen dieser Aufgabe werden zwangsläufig zahlreiche Daten verarbeitet.

Der Gesetzgeber hat grundsätzlich auch im Bereich nachrichtendienstlicher Aufgabenwahrnehmung für Bürgerinnen und Bürger ein Mindestmaß an Transparenz vorgesehen. Zu diesem Zweck beinhaltet Art. 23 Abs. 1 Bayerisches Verfassungsschutzgesetz (BayVSG) ein Recht auf Auskunft (siehe bereits meine Ausführungen im 28. Tätigkeitsbericht 2018 unter Nr. 5.4 und Nr. 5.5, im 29. Tätigkeitsbericht 2019 unter Nr. 3.6 und zuletzt im 33. Tätigkeitsbericht 2023 unter Nr. 3.11).

Nicht selten wird einer Person, die eine solche Beauskunftung beantragt, zwar mitgeteilt, dass sie in Dateien und Akten der Verfassungsschutzbehörde gespeichert sei, weitergehende Auskünfte allerdings unterbleiben müssten. Angesichts dieser Sachlage wenden sich die betroffenen Personen an mich und bitten insbesondere um eine datenschutzrechtliche Überprüfung, ob dieses Vorgehen (sog. „Teilauskunft") zulässig sei.

Tatsächlich ist das Auskunftsrecht nach Art. 23 Abs. 1 BayVSG nicht mit dem weitreichenden Auskunftsrecht nach Art. 15 DSGVO vergleichbar, da den Verfassungsschutzbehörden generell ein höheres Geheimhaltungsinteresse zugestanden wird als anderen Stellen. Daher beinhaltet Art. 23 Abs. 2 BayVSG bezüglich einer Auskunft sog. Versagungsgründe, also solche Gründe, bei deren Vorliegen das BayLfV eine Auskunft im Einzelfall einschränken oder sogar gänzlich unterlassen darf.

In diesen Fällen steht mir allerdings die Möglichkeit einer datenschutzrechtlichen Überprüfung der konkreten Umstände zu, die zur Einschränkung des Auskunftsrechts der betroffenen Person geführt haben. Üblicherweise lasse ich mir im Rahmen eines Vor-Ort-Termins beim BayLfV zunächst den Aktenrückhalt und die fachlichen Gründe darlegen, die aus Sicht des Verfassungsschutzes zur Einschränkung der Auskunft geführt hatten. Falls notwendig fordere ich eine schriftliche Stellungnahme des BayLfV an, in der die rechtlichen Bewertungsmaßstäbe des Art. 23 Abs. 2 BayVSG am konkreten Vorgehen beleuchtet werden. Auf Grundlage dieser Informationen kann ich schließlich meine datenschutzrechtliche Prüfung vornehmen. Erfreulicherweise komme ich zumeist zu dem Ergebnis, dass das Vorgehen des BayLfV den gesetzlichen Vorgaben entsprochen hatte und nicht zu beanstanden war.

Weitere Informationen zum Thema „Auskunftsrecht gegenüber dem Bayerischen Landesamt für Verfassungsschutz" finden sich auf meiner Homepage.[52]

4.9 Prüfung der Umsetzung einer in Aussicht gestellten Löschung von Speicherungen des Bayerischen Landesamtes für Verfassungsschutz

In meinem 33. Tätigkeitsbericht 2023 habe ich unter Nr. 3.11 darüber informiert, dass ich regelmäßig aus eigener Initiative heraus die gesetzlichen Speicherungsvoraussetzungen von Fällen überprüfe, bei denen das Bayerische Landesamt für Verfassungsschutz (BayLfV) dem ursprünglichen Löschungsantrag der Betroffenen nicht entsprochen hat.

Im Rahmen einer solchen Prüfung stellte ich nach der Begutachtung des Aktenrückhalts fest, dass die Speicherungen zu einer Person zulässig sind.

Weil die zugrunde liegenden Erkenntnisse jedoch bereits längere Zeit zurücklagen und die Person seitdem nicht mehr in einem extremistischen Umfeld aufgetreten war, hatte mir das BayLfV auf meine entsprechenden diesbezüglichen Anmerkungen hin allerdings zugesagt, die Speicherungsvoraussetzungen nach weiteren zwei Jahren nochmals zu überprüfen.

[52] Internet: https://www.datenschutz-bayern.de, Rubrik „Themengebiete – Verfassungsschutz – Häufige Fragen".

Da zum Zeitpunkt dieser erneuten Überprüfung bezüglich der betroffenen Person keine neuen Anhaltspunkte hinzugekommen waren, die einen zwischenzeitlichen Bezug zum früheren extremistischen Umfeld erkennen ließen, teilte mir das BayLfV mit, dass man sich nun dazu entschieden habe, eine Aussonderung bereits vor der generellen Speicherdauer von 15 Jahren vorzunehmen.

Im Rahmen eines späteren Vor-Ort-Termins konnte ich mich schließlich von der tatsächlichen Löschung der Speicherungen zu der betreffenden Person überzeugen.

4.10 Verwarnung einer Staatsanwaltschaft wegen fälschlicher Nennung des Namens einer nicht mehr beschuldigten Person in staatsanwaltschaftlichen Schreiben

Im Berichtszeitraum verwarnte ich eine Staatsanwaltschaft. Diese hatte im Laufe des weiteren Ermittlungsverfahrens unbefugt personenbezogene Daten eines vormals beschuldigten Beschwerdeführers in zwei nach außen gerichteten Schreiben offenbart.

Der Beschwerdeführer war kurzzeitig Beschuldigter in einem Ermittlungsverfahren wegen Anlagebetrugs, da er die betreffende Geldanlage Bekannten weiterempfohlen hatte. Zu einem frühen Zeitpunkt im Ermittlungsverfahren konnte geklärt werden, dass er selbst Geschädigter und nicht Mittäter des Anlagebetrugs war. Das Ermittlungsverfahren gegen ihn wurde daraufhin eingestellt. Im weiteren Verlauf des Verfahrens gegen die mutmaßlichen Täter wurden dennoch in zwei Fällen Schreiben an Privatpersonen versandt, welche im Rubrum neben den Namen der weiteren Beschuldigten auch den vollen Namen des Beschwerdeführers auswiesen. Darüber hinaus enthielt eines der Schreiben zusätzlich das Geburtsdatum des Beschwerdeführers.

Die subjektiven Datenschutzrechte des Beschwerdeführers wurden vorliegend mehrfach verletzt: Zum einen waren die den Beschwerdeführer betreffenden übermittelten Daten sachlich unrichtig. da er in den betreffenden Schreiben als Beschuldigter genannt wurde, obwohl das Ermittlungsverfahren gegen ihn zu diesem Zeitpunkt bereits eingestellt war. Mit der Einstellung des Verfahrens war die Beschuldigteneigenschaft des Beschwerdeführers jedoch entfallen.[53] Zum anderen wurden personenbezogene Daten des Beschwerdeführers gegenüber Dritten offengelegt und damit verarbeitet, ohne dass es hierfür eine entsprechende Rechtsgrundlage gegeben hätte. Mangels Erforderlichkeit war diese Datenübermittlung insbesondere nicht von der Ermittlungsgeneralklausel des § 161 Abs. 1 Strafprozeßordnung gedeckt.

Trotz einer Entschuldigung der Staatsanwaltschaft und weiterer Sensibilisierungsmaßnahmen innerhalb der Behörde sah ich mich aufgrund der Schwere der Datenschutzverstöße gezwungen, eine Verwarnung der Staatsanwaltschaft gemäß Art. 58 Abs. 2 Buchst. b DSGVO in Verbindung mit Art. 28 Abs. 1 Satz 1 Nr. 2, Abs. 2 Satz 2, Art. 34 Abs. 1 Satz1 BayDSG auszusprechen.

[53] Vgl. Kölbel/Ibold, in: Münchener Kommentar zur StPO, 2. Aufl. 2024, § 163a StPO Rn. 6.

Zudem nahm ich den Vorfall zum Anlass, die dahinterstehende IT-Problematik gegenüber dem Bayerischen Staatsministerium der Justiz zu thematisieren. Das Justizministerium teilte mir daraufhin mit, dass im Rahmen mehrerer Dienstbesprechungen unter anderem mit den Leiterinnen und Leitern der bayerischen Staatsanwaltschaften – in anonymisierter Weise – auf den entsprechenden Vorfall eingegangen worden sei, um derartige Datenschutzverstöße in Zukunft zu vermeiden.

4.11 Zu lange Aufbewahrung einer Strafakte

Im Rahmen der Beschwerdesachbearbeitung wurde ich damit befasst, dass eine Staatsanwaltschaft die Akte eines abgeschlossenen Verfahrens zu lange aufbewahrt hatte.

Die Staatsanwaltschaften speichern personenbezogene Daten zum großen Teil in den jeweiligen Verfahrensakten. Diese werden auch nach Abschluss des Ermittlungs- sowie des sich gegebenenfalls anschließenden Strafvollstreckungsverfahrens aufbewahrt. Die hierfür einschlägige Rechtsgrundlage findet sich für den Bereich der Gerichte, Staatsanwaltschaften und Justizvollzugsbehörden in der Verordnung über die Aufbewahrung von Schriftgut der Gerichte, Staatsanwaltschaften und Justizvollzugsbehörden (Aufbewahrungsverordnung –AufbewV).

In der zur Aufbewahrungsverordnung dazugehörigen Anlage ist ausdrücklich geregelt, wie lange entsprechende Akten aufzubewahren sind, wobei beispielsweise für unterschiedlich schwerwiegende Straftaten jeweils gesonderte Fristen gelten.

Im konkreten Fall war die für die gegenständliche Akte geltende Aufbewahrungsfrist bereits um mehrere Jahre überschritten. Der Mitteilung der Staatsanwaltschaft war zu entnehmen, dass sich dieser individuelle Fehler durch eine Änderung der Aufbewahrungsverordnung sowie die manuelle Übertragung bei der Umstellung auf ein EDV-System ergeben hatte.

Auf mein Hinwirken hin sicherte die betroffene Staatsanwaltschaft die unverzügliche Vernichtung der fraglichen Akte sowie die Entfernung der dazugehörigen Daten aus dem IT-System zu.

Aufgrund des langen Zeitraums der unzulässigen Aufbewahrung der Akte habe ich gegen die betroffene Staatsanwaltschaft eine Verwarnung gemäß Art. 58 Abs. 2 Buchst. b DSGVO ausgesprochen.

5 Allgemeine Innere Verwaltung

5.1 Wärmeplanungsgesetz: Umsetzung in Bayern

Am 1. Januar 2024 ist das Gesetz für die Wärmeplanung und zur Dekarbonisierung der Wärmenetze (Wärmeplanungsgesetz – WPG) in Kraft getreten. Bekanntlich war der Gesetzgebungsprozess auf Bundesebene Gegenstand intensiver Diskussionen in der Öffentlichkeit (ich erinnere hier nur an das Schlagwort „Heizungshammer"). Dass im Rahmen der Umsetzung der Wärmeplanung vor Ort gerade auch datenschutzrechtliche Aspekte eine große Rolle spielen, ist dabei in der Diskussion nach meinem Eindruck manchmal zu Unrecht etwas in den Hintergrund getreten. Gerade insoweit bin ich im Berichtszeitraum mehrfach zum Schutz des Grundrechts auf informationelle Selbstbestimmung der Bürgerinnen und Bürger in datenschutzrechtlicher Hinsicht aktiv geworden.

5.1.1 Datenverarbeitungsbefugnisse der planungsverantwortlichen Stelle

Das Wärmeplanungsgesetz enthält detaillierte und ausdifferenzierte Regelungen zu Datenverarbeitungsbefugnissen der planungsverantwortlichen Stelle gemäß § 3 Abs. 1 Nr. 9 WPG. So ist diese etwa gemäß § 10 Abs. 1 WPG befugt, zur Erfüllung der ihr nach den Abschnitt 4 (Durchführung der Wärmeplanung) und Abschnitt 6 (Entscheidung über die Ausweisung von Gebieten im Sinne des Gebäudeenergiegesetzes; Transformation von Gasnetzen) von Teil 2 des WPG obliegenden Aufgaben Daten für die Bestandsanalyse nach § 15 WPG oder für die Potentialanalyse nach § 16 WPG schriftlich und in elektronischer oder maschinenlesbarer Form zu verarbeiten, wenn und soweit dies für die Aufgabenerfüllung erforderlich ist. Gemäß § 10 Abs. 1 Satz 3 WPG ist im Rahmen der Potenzialanalyse nach § 16 WPG die Verarbeitung personenbezogener Daten explizit nicht umfasst. Anders ist dies bei der Bestandsanalyse nach § 15 WPG. Die hierfür zulässigerweise zu erhebenden Daten sind abschließend und detailliert in Anlage 1 zu § 15 WPG geregelt, wobei im Hinblick auf den Datenschutz für die Bürgerinnen und Bürger vor allem deren Nummern 1 bis 3 von Belang sind. Im Wesentlichen versucht das Wärmeplanungsgesetz insoweit, die Eingriffe in das Recht auf informationelle Selbstbestimmung durch Aggregierung, also Zusammenfassung mehrerer Datensätze betroffener natürlicher Personen, möglichst abzumildern.

> **§ 10 WPG**
> **Datenverarbeitung zur Aufgabenerfüllung**
> (1) Die planungsverantwortliche Stelle ist befugt, zur Erfüllung der ihr nach den Abschnitten 4 bis 6 obliegenden Aufgaben für die Bestandsanalyse nach § 15 oder für die Potenzialanalyse nach § 16 Daten schriftlich und in elektronischer und maschinenlesbarer Form zu verarbeiten, wenn und soweit dies für die Aufgabenerfüllung erforderlich ist. Dies umfasst insbesondere die Erhebung, Speicherung und Verwendung der Daten. Die Datenverarbeitung im Rahmen der Potenzialanalyse nach § 16 schließt die Verarbeitung personenbezogener Daten nicht ein.
> (2) Endenergieverbräuche von Gas oder Wärme dürfen durch die planungsverantwortliche Stelle nur erhoben werden, soweit sie keine personenbezogenen Daten beinhalten. Hierzu kann die Datenerhebung insbesondere aggregiert für mindestens fünf benachbarte Hausnummern oder Anschlussnutzer, Messeinrichtungen oder Übergabepunkte erfolgen.
> […]

§ 15 WPG
Bestandsanalyse

(1) Im Rahmen der Bestandsanalyse ermittelt die planungsverantwortliche Stelle als Grundlage für das Zielszenario nach § 17, für die Einteilung des beplanten Gebiets in voraussichtliche Wärmeversorgungsgebiete nach § 18 Absatz 1, für die Darstellung von Gebieten nach § 18 Absatz 5 und für die Darstellung der Wärmeversorgungsarten für das Zieljahr nach § 19

1. den derzeitigen Wärmebedarf oder Wärmeverbrauch innerhalb des beplanten Gebiets einschließlich der hierfür eingesetzten Energieträger,
2. die vorhandenen Wärmeerzeugungsanlagen und
3. die für die Wärmeversorgung relevanten Energieinfrastrukturanlagen.

(2) Im Rahmen der Bestandsanalyse sind von der planungsverantwortlichen Stelle die für die Wärmeplanung relevanten Informationen und erforderlichen Daten zur aktuellen Versorgung des beplanten Gebiets mit Wärme systematisch und qualifiziert zu erheben. Hierzu ist die planungsverantwortliche Stelle nach Maßgabe von Abschnitt 3 berechtigt, die in Anlage 1 genannten Daten zu erheben.

§ 16 WPG
Potenzialanalyse

(1) Im Rahmen der Potenzialanalyse ermittelt die planungsverantwortliche Stelle quantitativ und räumlich differenziert die im beplanten Gebiet vorhandenen Potenziale zur Erzeugung von Wärme aus erneuerbaren Energien, zur Nutzung von unvermeidbarer Abwärme und zur zentralen Wärmespeicherung. Bekannte räumliche, technische, rechtliche oder wirtschaftliche Restriktionen für die Nutzung von Wärmeerzeugungspotenzialen sind zu berücksichtigen.

[…]

Anlage 1 zu § 15 WPG

Die planungsverantwortliche Stelle ist berechtigt, unter Beachtung der Bestimmungen von Teil 2 Abschnitt 3 für die Bestandsanalyse nach § 15 die folgenden Daten zu erheben:

1. nach Maßgabe von § 10 Absatz 2 bei bestehender leitungsgebundener Gasversorgung die bei Mehrfamilienhäusern adressbezogenen, bei Einfamilienhäusern nur aggregiert für mindestens fünf Hausnummern und bei bestehender leitungsgebundener Wärmeversorgung die auf die Übergabestation bezogenen gemittelten jährlichen Gas- oder Wärmeverbräuche der letzten drei Jahre in Kilowattstunden pro Jahr,
2. bei Mehrfamilienhäusern adressbezogene, bei Einfamilienhäusern nur aggregiert für mindestens drei Hausnummern Informationen und Daten zu dezentralen Wärmeerzeugungsanlagen mit Verbrennungstechnik
   a) zur Art des Wärmeerzeugers, zum Beispiel zentraler Brennwertkessel, Etagenheizung, Therme,
   b) zum eingesetzten Energieträger,
   c) zur thermischen Leistung des Wärmeerzeugers in Kilowatt,
3. Informationen und Daten zum Gebäude, bei Mehrfamilienhäusern adressbezogenen, bei Einfamilienhäusern nur aggregiert,
   a) zur Lage,
   b) zur Nutzung,
   c) zur Nutzfläche sowie
   d) zum Baujahr,
   […]

5.1.2 Planungsverantwortliche Stellen als Schaltstellen bei der Umsetzung der Wärmeplanung

Zentrale Bedeutung bei der konkreten Umsetzung der Wärmeplanung vor Ort kommt damit, gerade auch im Hinblick auf die Datenverarbeitungsbefugnisse, den planungsverantwortlichen Stellen zu. Wer diese wichtige Aufgabe übernehmen sollte, bedurfte zunächst gemäß § 3 Abs. 1 Nr. 9 WPG noch der landessrechtlichen Umsetzung. In Bayern wurde diese Rolle durch § 8 Abs. 1 Satz 1 Verordnung zur

Ausführung energiewirtschaftlicher Vorschriften (AVEn) mit Wirkung zum 2. Januar 2025 den Gemeinden übertragen.

> **§ 8 AVEn**
> **Zuständigkeiten**
> (1) [1]Planungsverantwortliche Stellen im Sinne des Wärmeplanungsgesetzes (WPG) sind die Gemeinden. [2]Sie sind verpflichtet, für ihr jeweiliges Gemeindegebiet allein oder gemeinsam mit anderen Gemeinden Wärmepläne nach Maßgabe des Wärmeplanungsgesetzes unter Einhaltung der in § 4 Abs. 2 WPG genannten Zeitpunkte zu erstellen, soweit die Pflicht zur Wärmeplanung nicht gemäß § 5 Abs. 2 WPG entfällt. [3]Die Gemeinden nehmen die Pflichten und Aufgaben in eigener Verantwortung wahr, soweit Bundes- oder Landesrecht nicht entgegensteht.

Manche Gemeinden fühlten jedoch bereits vor ihrer „offiziellen Benennung" einen subjektiven Handlungsdruck, die Wärmeplanung vor Ort inhaltlich voranzubringen, manchmal wohl auch, um sich bestimmte Förderprogramme des Bundes zu „sichern". Hier musste ich manchmal bremsend auf die Gemeinden einwirken. Zum einen, weil sich die Gemeinden (noch) nicht auf die Datenverarbeitungsbefugnisse aus dem Wärmeplanungsgesetz berufen konnten, zum anderen, weil für die von diesen Gemeinde verarbeiten Daten auch nach der erfolgten Aufgabenzuweisung als planungsverantwortliche Stelle nach dem Wärmeplanungsgesetz keine Verarbeitungsbefugnis existierte.

5.1.3 Datenschutzrechtliche Generalklausel oder Einwilligungen taugen nicht als zusätzliche Datenverarbeitungsbefugnis

Konkret bin ich etwa auf die Konstellation getroffen, dass manche Gemeinden flächendeckend mittels entsprechender Fragebögen und personenscharf bei den Bürgerinnen und Bürgern individuelle konkrete und zukünftige Energiebedarfsdaten erheben wollten. Dem bin ich aus datenschutzrechtlicher Sicht entgegengetreten und habe die Gemeinden auf Folgendes hingewiesen:

Zunächst einmal findet sich hierfür auch nach der Benennung als planungsverantwortliche Stelle nach dem Wärmeplanungsgesetz vom Grundsatz her gerade keine entsprechende personenscharfe Verarbeitungsbefugnis im Wärmeplanungsgesetz. Auch kann eine flächendeckende Erhebung personenbezogener Daten aufgrund des damit einhergehenden intensiven Eingriffs in das Recht auf informationelle Selbstbestimmung anerkanntermaßen nicht auf die allgemeine Befugnisnorm des Art. 4 Abs. 1 BayDSG gestützt werden.[54] Im Übrigen ist der Rückgriff auf die allgemeine Befugnisnorm auch schon aufgrund des lex-specialis-Grundsatzes (hier: Vorrang des Wärmeplanungsgesetz) versperrt. Wie bereits dargestellt, hat nämlich der Bundesgesetzgeber im Wärmeplanungsgesetz eine ausdifferenzierte Regelung zu den Datenverarbeitungsbefugnissen getroffen. Diese sind grundsätzlich als abschließend anzusehen. Auch die Einholung von Einwilligungen als Rechtsgrundlage gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO ist für das großflächige Anschreiben von Haushalten hinsichtlich konkreter Verbrauchsdaten nicht zulässig. Wie von mir seit jeher betont, haben sich öffentliche Stellen bei der Verarbeitung personenbezogener Daten grundsätzlich auf den durch den Gesetzgeber vorgegebenen Rahmen zu beschränken und können ihre

[54] Bayerischer Verwaltungsgerichtshof, Beschluss vom 15. Februar 2024, 4 CE 23.2267, BeckRS 2024, 2968.

gesetzlichen Befugnisse nicht beliebig mit Hilfe von Einwilligungen erweitern. Daher kommen für bayerische öffentliche Stellen Einwilligungen als Rechtsgrundlage primär nur zur Abrundung gesetzlich ungeregelter Randbereiche in Frage. Auch in diesem Zusammenhang gilt aber: Der Bundesgesetzgeber hat im Wärmeplanungsgesetz detaillierte Regelungen zu den Datenverarbeitungsbefugnissen getroffen. Eine flächenhafte Erweiterung dieser Befugnisse durch Einholung von Einwilligungen würde die klare Absicht des Gesetzgebers unterlaufen, im Wärmeplanungsgesetz abschließende Regelungen im Hinblick auf Datenverarbeitungsbefugnisse zu schaffen.

5.1.4 Unterstützung der bayerischen Gemeinden durch staatliche Zurverfügungstellung von Bedarfsdaten

Den gerade dargestellten Wunsch von bayerischen Gemeinden nach einer möglichst breiten und tragfähigen Datenbasis kann ich im Grundsatz nachvollziehen. Schließlich ist es für eine effiziente und für die Bürgerinnen und Bürger gewinnbringende Wärmeplanung essentiell, dass diese auf einer soliden und durchdachten Datengrundlage fußt. Daher habe ich mich bereits frühzeitig mit dem zuständigen Bayerischen Staatsministerium für Wirtschaft, Landesentwicklung und Energie in Sachen (datenschutzkonforme) Umsetzung des Wärmeplanungsgesetzes in Bayern ausgetauscht. Erfreulicherweise konnten an dieser Stelle die entsprechenden Weichen gestellt werden, die Wärmeplanung in Bayern mit einer guten und zugleich datensparsamen Datengrundlage zu unterstützen. So bilden in Bayern primär modellhafte, also abstrakt errechnete Bedarfsdaten und gerade eben nicht reale (aggregierte) Verbrauchsdaten die Basis von gemeindlichen Wärmeplänen. Dabei werden die entsprechenden Daten den Gemeinden vom Freistaat Bayern für ihr jeweiliges Gemeindegebiet in Gestalt eines Kurzgutachtens mitsamt Wärmebedarfskarte zur Verfügung gestellt.

5.2 Bürgerversammlung, Bürgerbegehren, Bürgerantrag: datenschutzkonformer Umgang mit den Unterschriftenlisten

Die Gemeindeordnung (GO) enthält in Gestalt des Antrags auf Durchführung einer Bürgerversammlung gemäß Art. 18 Abs. 2 Satz 1 GO, des Bürgerbegehrens gemäß Art.18 a Abs. 6 GO sowie des Bürgerantrags gemäß Art. 18b Abs. 1 GO an das Erreichen bestimmter Quoren gebundene Elemente direkter Beteiligung. Wollen die Bürgerinnen und Bürger von diesen gemeinderechtlichen Partizipationsrechten Gebrauch machen, so müssen sie insbesondere eine Unterschriftenliste mit einer bestimmten Anzahl an Unterstützerinnen und Unterstützern „vor Ort“ bei der Kommune vorlegen. Wie ich bereits in meinem 17. Tätigkeitsbericht 1996 unter Nr. 8.4.2[55] herausgestellt und in der Folge immer wieder, beispielsweise in meinem 21. Tätigkeitsbericht 2004 unter der Nr. 11.11, betont habe, dienen die Unterschriftenlisten ausschließlich zur Prüfung, ob das jeweils in der Gemeindeordnung vorgeschriebene Quorum erreicht ist, kurz gesagt, „ob genug Gemeindebürgerinnen und Gemeindebürger unterschrieben haben“. Dagegen soll die jeweilige Unterschriftenliste es gerade nicht der Kommune ermöglichen, zu erfassen oder zu dokumentieren, wer das jeweilige Anliegen unterstützt hat. Insoweit

[55] Dort ausschließlich in Bezug auf Bürgerbegehren, diese Vorgaben sind jedoch auch auf den Bürgerantrag, vgl. dazu Bayerischer Landesbeauftragter für den Datenschutz, 23. Tätigkeitsbericht 2008, Nr. 9.6, und auf den Antrag zur Durchführung einer Bürgerversammlung anzuwenden.

musste ich in der Vergangenheit bereits das Anrufen und Befragen von Unterzeichnern eines Bürgerbegehrens durch kommunale Vertreter[56] oder das Verlesen einer Unterschriftenliste der Unterzeichner eines Bürgerbegehrens in öffentlicher Gemeinderatssitzung datenschutzrechtlich beanstanden.[57] Auch in diesem Berichtszeitraum war der Umgang mit solchen Unterschriftenlisten mehrfach Gegenstand von Datenschutzbeschwerden bei mir. Hierbei hatte ich Gelegenheit, die Bürgerinnen und Bürger bei der Ausübung ihrer gemeinderechtlichen Partizipationsrechte aus datenschutzrechtlicher Sicht zu unterstützen. Folgende Konstellationen möchte ich insoweit herausgreifen:

5.2.1 Unterschriftenliste nicht pauschal Element der Sitzungsvorbereitung

Wenn die Unterschriftenliste bei der Kommune abgegeben wurde, ist diese für den datenschutzkonformen Umgang mit der Liste verantwortlich. Verwaltungsintern ist dann gerade auch der Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 Buchst. c DSGVO zu beachten. Er besagt, dass nur solche personenbezogenen Daten verarbeitet werden dürfen, welche für die konkrete Aufgabenerfüllung benötigt werden. Im Berichtszeitraum war ich mit einem Fall befasst, an dem sich gut verdeutlichen lässt, was dieser doch recht abstrakte Grundsatz in der Praxis etwa für die Vorbereitung der Gemeinderatssitzung durch die Bürgermeisterin oder den Bürgermeister konkret bedeutet.

Hat der oder die nach der internen Geschäftsverteilung zuständige Beschäftigte die Unterschriftenliste ausgewertet und final geprüft, dass „genug" Gemeindebürgerinnen und Gemeindebürger unterschrieben haben, dann ist die Vorprüfung durch die Gemeindeverwaltung abgeschlossen. Dies bedeutet, dass selbst die Bürgermeisterin oder der Bürgermeister nach der abgeschlossenen Vorprüfung nicht mehr ohne konkreten Anlass in die Unterschriftenliste Einsicht nehmen kann. Für die anstehende Sitzungsvorbereitung muss sie oder er lediglich wissen, dass „genug Personen gültig unterschrieben haben", nicht jedoch, wer unterschrieben hat. Kurz gesagt: Ist die verwaltungsinterne Vorprüfung einmal abgeschlossen, so hat die Unterschriftenliste ihren Zweck (vorerst) erfüllt und ist nicht mehr pauschales Element der Sitzungsvorbereitung.

5.2.2 Anforderungen an eine Einsichtnahme in die Unterschriftenliste durch den Gemeinderat gemäß Art. 30 Abs. 3 GO

Grundsätzlich kann der Gemeinderat gemäß Art. 30 Abs. 3 GO unter Beachtung des Grundsatzes der Zweckbindung Einsicht in eine durch die Kommunalverwaltung bereits ausgewertete Unterschriftenliste nehmen. Hierfür muss in formeller Hinsicht zunächst ein Beschluss des Gemeinderats über die Geltendmachung des Rechts aus Art. 30 Abs. 3 GO gefasst werden.[58] In welcher konkreten Form die Einsichtnahme in die Unterschriftenliste eines Bürgerbegehrens in Ausübung des Rechts aus Art. 30 Abs. 3 GO durch den Gemeinderat in datenschutzkonformer

[56] Vgl. beispielsweise Bayerischer Landesbeauftragter für den Datenschutz, 27. Tätigkeitsbericht 2016, Nr. 6.6.

[57] Vgl. beispielsweise Bayerischer Landesbeauftragter für den Datenschutz, 19. Tätigkeitsbericht 2000, Nr. 8.6.1.

[58] Vgl. im Einzelnen Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz und Akteneinsichtsrechte im Gemeinderat, Arbeitspapier, Stand 9/2020, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

Weise erfolgen kann, habe ich bereits in meinem 19. Tätigkeitsbericht 2000 unter der Nr. 8.6.1 dargestellt und in meinem 23. Tätigkeitsbericht 2007 unter Nr. 9.5 bekräftigt: Die Einsichtnahme hat unter Beachtung des Grundsatzes der Zweckbindung entweder in nichtöffentlicher Sitzung oder durch ein vom Gemeinderat durch Beschluss mit dieser Aufgabe beauftragtes Gemeinderatsmitglied in den Amtsräumen der Verwaltung zu erfolgen.

Hieran halte ich unverändert (für alle drei Partizipationsformen) fest. Im Berichtszeitraum musste ich einer Kommune erläutern, warum eine Einsichtnahme in öffentlicher Sitzung hinter Trennwänden keine datenschutzkonforme Alternative darstellt. Eine Einsichtnahme in die Unterschriftenliste in öffentlicher Sitzung kann nämlich, auch wenn dies von der Gemeinde (hoffentlich) nicht gewollt ist, dennoch einen Einschüchterungscharakter haben. Bei den Bürgerinnen und Bürgern vor Ort kann so der Eindruck entstehen, dass sie, wenn sie von ihrem Partizipationsrechten Gebrauch machen, Gefahr laufen, dass ihre Unterschrift für ein bestimmtes Anliegen und die darin zum Ausdruck kommende persönliche Meinung und möglicherweise auch politische Gesinnung, zwangsläufig sämtlichen Gemeinderatsmitgliedern offenbart wird. Außerdem kann – selbst bei entsprechenden Handlungsanweisungen und Belehrungen – nicht völlig ausgeschlossen werden, dass es, aus der Spontansituation heraus, bei einer Einsichtnahme in öffentlicher Sitzung zu Äußerungen der Gemeinderatsmitglieder im Hinblick auf die Unterzeichnereigenschaft bestimmter Personen oder zu anderen einschüchternd wirkenden Reaktionen kommen kann. Dies kann durchaus Bürgerinnen und Bürger davon abhalten, zukünftig von ihren in der Gemeindeordnung vorgesehenen Partizipationsrechten Gebrauch zu machen.

5.2.3 Kein schutzwürdiges Interesse Dritter am Inhalt einer Unterschriftenliste

Die Zweckbindung der Unterschriftenliste bedeutet auch, dass die Liste nicht an Dritte übermittelt werden darf beziehungsweise Dritte nicht Einsicht in die jeweilige Liste nehmen dürfen.[59] Im Berichtszeitraum war ich mit einem Fall befasst, an dem sich das gut verdeutlichen lässt: Gegenstand einer beantragten Bürgerversammlung nach Art. 18 Abs. 2 Satz 1 GO war konkret, dass betroffene Anwohner eine bereits beschlossene Straßenumbenennung wieder rückgängig machen wollten. Die Gemeinde leitete diesen Antrag samt Unterschriftenliste an einen Dritten weiter. Grund hierfür war, dass der Dritte ein Interesse an dem Inhalt des Antrags geltend gemacht hatte. Konkret bestand dieses Interesse in der Beibehaltung des „neuen“ Straßennamens. Für eine solche Übermittlung konnte nicht Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2, Abs. 3 DSGVO in Verbindung mit Art. 5 Abs. 1 Nr. 2 BayDSG als Rechtsgrundlage herangezogen werden. Auch wenn das jeweilige Anliegen, auf das sich das gemeinderechtliche Partizipationsrecht bezieht, einen Dritten mittelbar oder unmittelbar betreffen mag, ist schon kein berechtigtes Interesse eines Dritten daran erkennbar, welche konkreten Personen hierfür unterschrieben haben. Selbst wenn man dies anders sehen wollte, wäre das schutzwürdige Interessen der Personen bedeutend höher zu gewichten, die

[59] Vgl. beispielsweise Bayerischer Landesbeauftragter für den Datenschutz, 23. Tätigkeitsbericht 2018, Nr. 9.5 zu der Konstellation, dass eine Unterschriftenliste an Medienvertreter übergeben, die Liste (teilweise) gefilmt und anschließend ausgestrahlt wurde, und Bayerischer Landesbeauftragter für den Datenschutz, 18. Tätigkeitsbericht 1998, Nr. 8.4.2 für die Konstellation, dass ein Bauantragsteller und Grundstückseigentümer, gegen dessen Vorhaben die Unterschriftenlisten eingereicht worden waren, in die Liste Einsicht nehmen möchte.

eine Unterschrift geleistet haben. Sie berührt nämlich das in einer freiheitlich-demokratischen Grundordnung essentielle Interesse, Partizipationsrechte ausüben zu können, und die darin zum Ausdruck kommende Meinung äußern zu können, ohne persönliche Konsequenzen fürchten zu müssen,. Dies schließt eine (zweckändernde) Übermittlung der Unterschriftliste, die einzig dem Nachweis eines ausreichenden Quorums von Fürsprechern vor Ort dient, an Dritte aus.

5.3 Datenschutz bei der Ortschronik

Viele bayerische Gemeinden können auf eine jahrhundertelange Geschichte voller historisch gewachsener Traditionen zurückblicken. Daher ist es nicht unüblich, dass sich auch die Wurzeln so mancher im Gemeindegebiet ansässigen Familie, insbesondere im ländlichen Raum, über mehrere Generationen hinweg zurückverfolgen lassen. Im Laufe der Zeit entwickelten sich manchmal auch „Spitz- oder Hausnamen", die nicht den jeweiligen „amtlichen" Nachnamen entsprachen. Diese dienten der örtlichen Gemeinschaft jedenfalls in früheren Zeiten aber gleichwohl zur unzweideutigen Identifikation eines Hauses oder Hofes und der dortigen Bewohnerinnen und Bewohner im „nicht-amtlichen" Austausch untereinander und wurden manchmal auch gleichsam von Generation zu Generation „vererbt".

Im Berichtszeitraum gab nun eine Gemeinde anlässlich eines „runden" Gründungsjubiläums eine Ortschronik heraus, welche unter anderem eine Sammlung dieser historisch gewachsenen „Spitz- oder Hausnamen" ihrer – früheren, aber auch jetzigen – Gemeindebürger enthielt.[60] Konkret handelte es sich dabei um eine Auflistung von mehreren Hundert Namen von Familien, die bereits seit mehreren Generationen im Gemeindegebiet ansässig waren und dort seit jeher nicht nur unter ihren amtlichen Familiennamen, sondern auch unter einem speziellen „Spitz- oder Hausnamen" bekannt waren, beziehungsweise auch heute noch sind. Die veröffentlichten Namen waren vorher über einen längeren Zeitraum von einer durch die Gemeinde beauftragten Privatperson zusammengetragen worden. Die Gemeinde handelte hierbei augenscheinlich mit den besten Absichten, wollte sie doch traditionelle Namen und die dahinterstehenden Geschichten entsprechend würdigen und für die Nachwelt erhalten. Leider wurde dabei jedoch versäumt, vor Veröffentlichung der Ortschronik Einwilligungen von den im Buch genannten noch lebenden Betroffenen einzuholen und bei Verweigerung gegebenenfalls von einer Namensnennung abzusehen. Hierüber hat sich ein Betroffener, der sich durch die Veröffentlichung seines historisch tradierten „Spitz- oder Hausnamens" herabgesetzt fühlte, zu Recht bei mir beschwert. Denn auch wenn die Herausgabe einer Ortschronik in aller Regel mit den besten Absichten erfolgt, ist bei der hiermit verbundenen Verarbeitung von personenbezogenen Daten gleichwohl Vorsicht geboten. Im Wesentlichen musste ich die Gemeinde aus datenschutzrechtlicher Sicht auf Folgendes hinweisen:

Zunächst einmal ist die Gemeinde als Herausgeberin der Ortschronik auch dann datenschutzrechtlich Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO, wenn die veröffentlichten Haus- und Spitznamen von einer dritten, damit von der Gemeinde

[60] Zur datenschutzrechtlichen Problematik der Behandlung eines Bürgerantrags auf Änderung des historischen Gemeindewappens in öffentlicher Gemeinderatssitzung vgl. Bayerischer Landesbeauftragter für den Datenschutz, 33. Tätigkeitsbericht 2023, Nr. 4.3.

beauftragten, Privatperson zusammengetragen wurden. Als Verantwortlicher benötigt die Gemeinde für die Veröffentlichung von personenbezogenen Daten eine Rechtsgrundlage (vgl. Art. 6 Abs. 1 DSGVO).

Nun kann die Erstellung einer Ortschronik zwar grundsätzlich (abstrakt) der gemeindlichen Öffentlichkeitsarbeit zugerechnet werden, wobei es sich hierbei um eine freiwillige Aufgabe im eigenen Wirkungskreis handelt, welche gesetzlich nicht näher ausgestaltet ist.[61] Die Kommunen können ganz allgemein ihre Öffentlichkeitsarbeit etwa dazu nutzen, die örtliche Identität zu pflegen, ihre Einwohnerschaft zur Mitwirkung an gemeindlichen Projekten zu bewegen oder aber auch über die Gemeinde und ihre Historie zu informieren. Idealerweise sollte bei der Erstellung einer Ortschronik zunächst die Aufgabe durch einen Beschluss des Gemeinderats festgelegt und auf diese Weise nach Art und Umfang näher konkretisiert werden.[62]

Unabhängig hiervon müssen aber bei der Veröffentlichung personenbezogener Daten wie „Spitz- oder Hausnamen" in einer Ortschronik die Grundsätze der Erforderlichkeit (zur Aufgabenerfüllung, also hier: Öffentlichkeitsarbeit) und der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) eingehalten werden. Die Gemeinde hat anhand dieser Maßstäbe zu prüfen, ob die Veröffentlichung der „Spitz- oder Hausnamen" in einer Ortschronik tatsächlich für die Öffentlichkeitsarbeit im Sinne von Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG erforderlich ist. Dabei ist das Recht auf informationelle Selbstbestimmung des Betroffenen (Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 GG) mit hinreichendem Gewicht zu beachten. Insoweit wird man aber zu dem Ergebnis kommen müssen, dass auch ein etwaig vorliegender Gemeinderatsbeschluss nur die Ortschronikerstellung als solche als Teil der gemeindlichen Öffentlichkeitsarbeit konkretisiert, aber für eine Veröffentlichung sensibler Daten, wie etwa tradierter „Spitz- und Hausnamen", nicht hinreicht, um im Zusammenwirken mit Art. 5 Abs. 1 Nr. 1 BayDSG eine gesetzliche Befugnis gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO hierfür zu eröffnen.[63]

Sofern also im Rahmen der Herausgabe einer Ortschronik personenbezogene Daten der Bürgerinnen und Bürger veröffentlicht werden sollen, empfehle ich daher dringend, wirksame Einwilligungen gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO der Betroffenen einzuholen.[64] Im vorliegenden Fall konnte mir die Gemeinde keine Einwilligungserklärungen der in der Ortschronik genannten noch lebenden Personen vorlegen. Da die Gemeinde jedoch sehr um Schadensbegrenzung bemüht war und die besagte Ortschronik nur in sehr geringer Auflage in den Umlauf gebracht wurde, konnte ich vorliegend ausnahmsweise von förmlichen

[61] Zur parallelen Problematik bei der Veröffentlichung gemeindlicher Mitteilungsblätter vgl. die Hinweise in Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz bei kommunalen Mitteilungsblättern, Stand 7/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

[62] Zur parallelen Problematik bei der Erstellung von Fotografien im Rahmen der Öffentlichkeitsarbeit vgl. die Hinweise in Bayerischer Landesbeauftragter für den Datenschutz, Fotografien in der Öffentlichkeitsarbeit bayerischer Kommunen, Aktuellen Kurz-Information 16, Stand 12/2018, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

[63] Zu einer möglichen anderen Beurteilung beim Vorliegen einer kommunalen Satzung vgl. die Hinweise in Bayerischer Landesbeauftragter für den Datenschutz, Datennutzungssatzungen bei bayerischen Kommunen?, Aktuelle Kurz-Information 41, Stand 1/2022, Internet: https://www.datenschutz-bayern.de , Rubrik „Infothek".

[64] Zu den Anforderungen an die Einholung wirksamer Einwilligungen vgl. die Hinweise in Bayerischer Landesbeauftragter für den Datenschutz, Die Einwilligung nach der Datenschutz-Grundverordnung, Stand 9/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

Aufsichtsmaßnahmen absehen. Die Gemeinde versicherte mir insoweit glaubhaft, die Vorgaben des Datenschutzrechts zukünftig strikt einzuhalten.

5.4 Drohneneinsatz zur Luftbilderstellung für kommunale Aufgaben

Der Einsatz von Drohnen ist mittlerweile allgegenwärtig und findet auch im öffentlichen Bereich immer stärkere Verbreitung. Daher verwundert es nicht, dass zunehmend mehr bayerische Kommunen (oftmals mit Hilfe von Ingenieurbüros als Auftragsverarbeitern) auf diese Möglichkeit zurückgreifen, um zwecks Erfüllung eigener Aufgaben besonders präzise Bilddaten zu gewinnen – effizient und regelmäßig kostensparend. Die Einsatzzwecke sind dabei sehr vielfältig: von der Kontrolle des baulichen Zustandes der Infrastruktur, über Notfalleinsätze in schwer zugänglichen Gebieten bis hin zu Datenerhebungen mittels Luftbildaufnahmen für die Erstellung von Starkregenkonzepten. Zunehmend erreichen mich insoweit Beratungsbitten von Kommunen, die sich bei mir nach der datenschutzrechtlichen Zulässigkeit eines derartigen Drohneneinsatzes erkundigen. Insoweit mache ich regelmäßig zunächst darauf aufmerksam, dass, soweit auch Privatgrundstücke überflogen und erfasst werden, der Drohneneinsatz bereits dadurch datenschutzrechtlich relevant wird. Mit Blick auf diese Entwicklungen und die aktuelle Rechtsprechung des Bayerischen Verwaltungsgerichtshofs betreffend Drohnenbefliegung zur Ermittlung der Geschossflächenzahl[65] gebe ich im Wesentlichen folgende weitere Hinweise:

5.4.1 Ausgangspunkt: Personenbezug von Luftbildaufnahmen

Der Anwendungsbereich des Datenschutzrechts und die damit verbundenen datenschutzrechtlichen Anforderungen an Datenverarbeitungen ist dann eröffnet, wenn personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO verarbeitet werden, vgl. Art. 2 Abs. 1 DSGVO. Danach sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Der Personenbezug kann hierbei auch mittelbar aus Sachdaten, wie Luftbildaufnahmen eines Grundstücks oder Gebäudes, hergestellt werden, wenn sie zugleich eine Information enthalten, die sich auf eine (identifizierbare) natürliche Person bezieht – etwa aufgrund individualisierender Identifikationsmerkmale, des Detaillierungsgrads oder der Einzigartigkeit der Sache. Zum Personenbezug von Geodaten, vereinfacht gesagt Daten mit Grundstücksbezug, habe ich mich bereits im Beitrag Nr. 6.2 meines 31. Tätigkeitsberichts 2021 (dort: zum gesetzgeberischen Handlungsbedarf für die Veröffentlichung der Geodaten im BayernAtlas) geäußert.[66]

Im Kontext von Luftbildaufnahmen kann ein solcher Personenbezug etwa für den Fall der Georeferenziertheit von Daten, also der Verknüpfung von Informationen mit Geodaten zur Lage eines Grundstücks, angenommen werden, genauso wie bei einem hinreichenden Detaillierungsgrad von Luftbildaufnahmen. Auch können die mithilfe von Drohnen gefertigten Luftbildaufnahmen beispielsweise Terrassen, Balkone, Schwimmbecken, persönliche Einrichtungsgegenstände und

[65] Bayerischer Verwaltungsgerichtshof, Beschluss vom15. Februar 2024, 4 CE 23.2267.

[66] Zum Personenbezug im Allgemeinen vgl. Bayerischer Landesbeauftragter für den Datenschutz, Wann ist eine natürliche Person identifizierbar?, Aktuelle Kurz-Information 53, Stand 1/2024, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek“.

Ähnliches erfassen, und damit Details über die Wohnverhältnisse Einzelner dokumentieren.[67] Dies wiederum lässt Rückschlüsse auf deren Vermögensverhältnisse zu. Die übliche Auflösung von Luftbildaufnahmen durch Drohnen (wie bei einer 2 cm-Pixelgröße) würde dies abbilden können. Dies allein begründet bereits einen Personenbezug im Sinne von Art. 4 Nr. 1 DSGVO. Insoweit übersteigt die datenschutzrechtliche Sensibilität der Drohnenaufnahmen in erheblichem Maße die Qualität „normaler" Luftaufnahmen, die mittels Kameras im Rahmen von Luftbefliegungen angefertigt werden.[68] Die Erstgenannten können von viel höherer Auflösung sein und nicht nur senkrecht von oben, sondern in allen denkbaren Winkeln und damit auch in Räume hinein beziehungsweise in nicht für jedermann von der Straße aus einsehbaren Bereichen erstellt werden.

Der Personenbezug wird hierbei nicht bereits dadurch ausgeschlossen, dass es nicht (mehr) möglich ist, Gesichter von Personen zu identifizieren oder Nummernschilder von Autos zu lesen, wenn der Personenbezug sich (auch) aus anderen Umständen ergibt – etwa, weil der hohe Detaillierungsgrad der erhobenen (Grundstücks-)Daten mittelbar eine Information über einzelne Personen zulässt. Insoweit wirkt sich auch ein etwaiger Ausschluss von Bildaufnahmen „in die Wohnungen hinein" nicht unbedingt auf den Personenbezug der Luftbildaufnahmen von Grundstücken und Gebäuden aus.

Die Grundstückseigentümer und/oder Bewohner der einzelnen Wohngebäude sind auch identifizierbar im Sinne von Art. 4 Nr. 1 DSGVO. Hierfür ist es nach EG 26 DSGVO zwar nicht notwendig, dass der Verantwortliche selbst die Identifizierung durchführen kann. Mit den Kommunen vorliegenden Informationen und der Kenntnis der geographischen Gegebenheiten vor Ort ist es jedoch bereits den verantwortlichen Stellen ohne weiteres möglich, die einzelnen von der Drohnenbefliegung betroffenen Grundstückseigentümer zu identifizieren.

5.4.2 Erfordernis einer Rechtsgrundlage

Für jede Verarbeitung personenbezogener Daten nach Art. 4 Nr. 2 DSGVO (hier: in Form der Datenerhebung bei Anfertigung von Luftbildaufnahmen mittels Drohnen) benötigen öffentliche Stellen eine Rechtsgrundlage, vgl. Art. 6 Abs. 1 DSGVO. Bei der Erfüllung ihrer öffentlichen Aufgaben finden insoweit primär spezielle fachgesetzliche Befugnisse zur Verarbeitung personenbezogener Daten Anwendung, vgl. Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 DSGVO. Unter Umständen kommt auch ein Rückgriff auf die allgemeine Verarbeitungsbefugnis des Art. 4 Abs. 1 BayDSG in Betracht. Dies gilt auch für Datenverarbeitungen des für eine öffentliche Stelle tätigen Auftragsverarbeiters: Liegt ein Auftragsverarbeitungsverhältnis vor, leitet sich die Rechtmäßigkeit der in diesem Rahmen vorgenommenen Verarbeitung personenbezogener Daten aus der Rechtsgrundlage ab, auf die der Verantwortliche selbst die betreffende Verarbeitung personenbezogener Daten stützt.

[67] Bayerischer Verwaltungsgerichtshof, Beschluss vom 15. Februar 2024, 4 CE 23.2267, Rn. 14.

[68] Vgl. zur Verwendung von Luftbildaufnahmen zur Ermittlung der Veranlagungsgrundlagen für Abwassergebühren Bayerischer Landesbeauftragter für den Datenschutz, 25.Tätigkeitsbericht 2012, Nr. 6.7 und zur Beweissicherung bei gemeindlichen Straßenbaumaßnahmen per Foto Bayerischer Landesbeauftragter für den Datenschutz, 30. Tätigkeitsbericht 2020, Nr. 6.6.

5.4.2.1 Spezialregelung vs. Generalklausel

An einer fachgesetzlichen Regelung für die Erstellung von Luftbildaufnahmen unter Zuhilfenahme von Drohnen durch Kommunen dürfte es regelmäßig fehlen.[69] Insoweit kommt es für die Beurteilung der Rechtmäßigkeit der Datenverarbeitung (Art. 5 Abs. 1 Buchst. a, Art. 6 DSGVO) entscheidend auf die Frage an, ob eine solche Datenverarbeitung noch durch die allgemeine Verarbeitungsbefugnis des Art. 4 Abs. 1 BayDSG (gegebenenfalls in Verbindung mit einer die Aufgabe konkretisierenden Regelung in einer kommunalen Satzung[70]) gedeckt ist. Dies hängt wiederum davon ab, ob es sich bei der Erstellung von Luftbildaufnahmen mittels Drohnen um Datenverarbeitungen mit hoher Eingriffsintensität handelt. Diese sind durch den Gesetzgeber spezialgesetzlich zu normieren. Die den Eingriff legitimierende gesetzliche Grundlage muss klare und präzise Regelungen für die Tragweite und die Anwendung der fraglichen Maßnahme vorsehen, damit die Adressaten ihr Verhalten darauf einstellen können.

Da grundsätzlich davon auszugehen ist, dass den durch Drohnen angefertigten Luftbildaufnahmen eine besondere Eingriffsintensität zukommt (siehe Nr. 5.4.2.2), sollten Kommunen, die über den Einsatz von Drohnen zur Erstellung von Luftbildaufnahmen nachdenken, bis zum Inkrafttreten einer derartigen Regelung daher dringend Maßnahmen zur Absenkung der Eingriffsintensivität ergreifen (siehe Nr. 5.4.2.3). Im Einzelnen:

5.4.2.2 Besondere Eingriffsintensität der Luftbildaufnahmen

Ob von einer besonderen Eingriffsintensität auszugehen ist, bemisst sich nach dem Umfang der Datenerhebungen sowohl hinsichtlich der Zahl der betroffenen Grundstücke als auch der Menge und Qualität der einzelnen Daten, der Zielrichtung der Datenerhebung und in geringerem Maße auch nach den wirksamen Schutzmaßnahmen, die der Verantwortliche ergreift, um die Eingriffe in Persönlichkeitsrechte Einzelner zu minimieren.

So geht der Bayerische Verwaltungsgerichtshof in der vorgenannten Entscheidung davon aus, dass flächendeckende Drohnenbefliegungen zur Ermittlung von Geschossflächenzahlen einen erheblichen Grundrechtseingriff darstellen. Nach Auffassung des Gerichts greift ein Drohneneinsatz zum Zwecke der fotografischen Dokumentation eines Wohngrundstücks und des dortigen Wohngebäudes von außen in den Kernbereich der persönlichen Lebensgestaltung und -führung ein und zwar bereits dann, wenn Aufnahmen der zur Wohnung zählenden Terrassen, Balkone sowie Gartenflächen mit deren Ausstattung und Gestaltung hergestellt werden. Schon ein umfriedetes Grundstück (und nicht erst das Gebäudeinnere) ist der Privatsphäre zuzurechnen – jedenfalls dann, wenn es dem Nutzer die Möglichkeit gibt, frei von öffentlicher Beobachtung zu sein.[71] Insoweit wirkt sich die zusätzliche Gefahr, mittels Drohnen Einblicke in die Wohnung zu nehmen, erschwerend mit Blick auf die Eingriffsintensität aus. Der Ausschluss dieser Gefahr

[69] Für den Feuerwehrbereich gilt die fachgesetzliche Verarbeitungsbefugnis des Art. 30 Bayerisches Feuerwehrgesetz.

[70] Bayerischer Landesbeauftragter für den Datenschutz, Datennutzungssatzungen bei bayerischen Kommunen?, Aktuelle Kurz-Information 41, Stand 1/2022, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

[71] Bayerischer Verwaltungsgerichtshof, Beschluss vom 15. Februar 2024, 4 CE 23.2267, Rn. 27 m. w. N.

würde jedoch nicht umgekehrt automatisch die bereits erhebliche Eingriffsintensität von Luftbildaufnahmen von umfriedeten Grundstücken verringern.

„Einfache“ Luftbildaufnahmen (sog. Orthofotos) eines bebauten Grundstücks, die durch eine Befliegung mittels eines mit einer stereophotogrammetrischen Kamera ausgestatteten Flugzeugs gewonnen werden, dürften dagegen nicht mit hoher Eingriffsintensität verbunden sein. Denn sie weisen nicht nur eine grobe Auflösung auf, die keine fotografische Wiedergabe von Einzelheiten des Grundstücks oder Gebäudes oder sich dort aufhaltenden Personen erlaubt. Auch die Einsehbarkeit von Innenräumen, etwa durch vorhandene Glasflächen, ist aufgrund des fehlenden Detailgrades der Aufnahmen ausgeschlossen.[72]

5.4.2.3 Eingriffsmildernde Maßnahmen

Soweit die Zwecke der Datenerhebung bereits nicht die Eingriffsintensität nahezu „vorgeben“, da sie bestimmte Datenverarbeitungen voraussetzen (etwa bei der Ermittlung der Geschossflächenzahl), kann der Verantwortliche gegebenenfalls die Eingriffsintensität, welche durch Nutzung von Drohnen entsteht, durch technische und organisatorische Schutzmaßnahmen abmildern. Bei deren Auswahl ist darauf zu achten, dass sich diese Maßnahmen auf der Ebene der Datenerhebung an sich auswirken müssen. Die Zusicherung, dass die hergestellten Luftbildaufnahmen weder veröffentlicht noch weitergegeben würden, erfüllt daher die Anforderung einer wirksamen Maßnahme mit Blick auf die Datenerhebung nicht. Eine eingeschränkte oder unterlassene Weitergabe der Daten würde einen (neuen) selbständigen Verarbeitungsvorgang darstellen, der datenschutzrechtlich separat zu betrachten wäre.

Eine Ankündigung der Drohnenbefliegung im Gemeindeblatt könnte zwar vereinzelt dazu führen, dass die betroffenen Personen gewisse Vorkehrungen zum Schutz der Privatsphäre treffen (etwa durch Parken in der Garage und nicht im freien Bereich des Grundstücks, Abdeckung von Gartenmöbeln, Aufenthalt im Inneren). Alleine hierdurch bietet der Verantwortliche jedoch keinen ausreichenden Schutz für alle Betroffenen. Auch sind gewisse Vorkehrungen durch die Eigentümer generell kaum umsetzbar (beispielsweise mit Blick auf Gestaltung der Gartenanlagen bei großen Anwesen). Schließlich sind die Drohnen an sich nur schwer wahrnehmbar, so dass das Verbleiben der betroffenen Personen im Innenbereich bereits aus diesem Grund nicht erwartet werden kann; daher stellt eine entsprechende Ankündigung keine wirksame Schutzmaßnahme des Verantwortlichen dar.

Insgesamt erscheint ein Bündel an Maßnahmen des Verantwortlichen empfehlenswert, das insbesondere auf grobe Auflösung der Aufnahmen, Verzicht auf horizontale Aufnahmen sowie zeitlich stark eingeschränkten Einsatz in wenig frequentierten Stunden beziehungsweise Jahreszeiten abzielt und die Information der betroffenen Personen in eindeutiger und transparenter Weise vorsieht.

5.4.2.4 Alternative: Einwilligung

Im Übrigen wäre eine datenschutzrechtskonforme Datenerhebung betreffend einzelne private Grundstücke mittels Drohnenbefliegung aufgrund der Einwilligungen betroffener Personen (Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO), meist

[72] Verwaltungsgericht Düsseldorf, Beschluss vom 17. Februar2025, 29 L 3128/24, Rn. 50.

Grundstückseigentümer, denkbar. Sie wäre allerdings mit einigen Unzulänglichkeiten verbunden. So besteht beispielsweise nach Art. 7 Abs. 3 Satz 1 DSGVO das Recht, die Einwilligung jederzeit widerrufen zu können, welches – sollte es ausgeübt werden – eine Weiterverwendung von gewonnenen Daten verbieten würde.

5.5 Erneut Kameraparken: öffentlich-rechtliche Ausgestaltung der Benutzung sowie Einschaltung privater Dienstleister

In meinem 33. Tätigkeitsbericht 2023 unter Nr. 4.7 habe ich erläutert, was öffentliche Stellen datenschutzrechtlich bei einer automatisierten Kennzeichenerfassung im Rahmen eines zivilrechtlich ausgestalteten Kameraparkens beachten müssen.

Zur Erinnerung: Beim Kameraparken wird mittels automatisierter Kennzeichenerfassung auf das Passieren von Schranken, sowie das Ziehen von Parktickets bei der Einfahrt und deren anschließende Entwertung vor der Ausfahrt verzichtet. Vielmehr erfasst eine Kamera bei allen einfahrenden Kraftfahrzeugen die Kennzeichen als (Einzel-)Bild und speichert sie zusammen mit der Uhrzeit. Bei der Ausfahrt werden die Kennzeichen nochmals als (Einzel-)Bild erfasst, und es wird überprüft, ob das nach der jeweiligen Parkdauer geschuldete Entgelt am Kassenautomaten – regelhaft ist hierfür die Eingabe des Kennzeichens erforderlich – entrichtet wurde. Zusammengefasst habe ich beim zivilrechtlichen, also bilateral auf Ebene der Gleichordnung durch Vertrag ausgestalteten Kameraparken, die hiermit verbundenen Datenverarbeitungen auf Basis wirksamer Einwilligungen der Parkenden gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO bei Erfüllung folgender Kriterien als möglich angesehen: Nachweis der Notwendigkeit einer Kennzeichenerfassung, Sicherstellung der Wahlmöglichkeit durch Information, Karenzzeit und Zweckbindung. Da ich im aktuellen Berichtszeitraum wiederholt mit der Thematik befasst war, möchte ich folgende ergänzende Erläuterungen geben:

5.5.1 Öffentlich-rechtliche Ausgestaltung der Benutzung

Falls öffentliche Stellen im Rahmen ihrer Wahlfreiheit bei der leistungsverwaltungsrechtlichen Aufgabenerfüllung das Kameraparken nicht zivilrechtlich durch Vertrag, sondern öffentlich-rechtlich durch Erlass entsprechender kommunaler Satzungen ausgestalten möchten, mache ich darauf aufmerksam, dass der Erlass entsprechender Satzungen per se grundsätzlich keine Befugnis im Sinne von Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO zur Verarbeitung personenbezogener Daten vermittelt, was ich umfassend in einer Aktuellen Kurz-Information[73] erläutert habe.

Auch bei einer öffentlich-rechtlichen Ausgestaltung des Benutzungsverhältnisses beim Kameraparken kommt die öffentliche Stelle daher regelmäßig nicht umhin, entsprechende Datenverarbeitungen auf das Rechtsinstitut der Einwilligung gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO zu stützen. Auch wenn die Einholung von Einwilligungen zur Erweiterung öffentlich-rechtlicher (hier: satzungsrechtli-

[73] Bayerischer Landesbeauftragter für den Datenschutz, Datennutzungssatzungen bei bayerischen Kommunen?, Aktuelle Kurz-Information 41, Stand 1/2022, Internet: https://datenschutz-bayern.de, Rubrik „Infothek".

cher) Befugnisse, schon angesichts der in Erwägungsgrund 34 zur DSGVO angemahnten kritischen Beurteilung hinsichtlich deren Freiwilligkeit, abstrakt betrachtet nicht bedenkenfrei ist, war für mich konkret ausschlaggebend, eine faktische Gleichbehandlung mit der zivilrechtlichen Ausgestaltungsmöglichkeit zu erreichen. Dies erschien mir aufgrund der bereits angesprochenen Wahlfreiheit bei der leistungsverwaltungsrechtlichen Aufgabenerfüllung (liegt beim Kameraparken vor), sowie der geringeren Grundrechtssensibilität der Leistungsverwaltung, als bei der insoweit deutlich kritischeren Eingriffsverwaltung[74] sachlich veranlasst. Bei strikter Erfüllung der in Nr. 4.7 meines 33. Tätigkeitsberichts 2023 entwickelten Kriterien, insbesondere Sicherstellung der Wahlmöglichkeiten der Parkenden durch hinreichende Information und Gewährung einer „datenverarbeitungsfreien" Karenzzeit, erscheint daher auch eine öffentlich-rechtliche Ausgestaltung der Benutzung grundsätzlich möglich.

5.5.2 Einschaltung privater Dienstleister

Öffentliche Stellen, die private Dienstleister in das von ihnen angebotene Kameraparken einbinden möchten, sollten bedenken, dass etwaige von ihnen veranlasste/zu verantwortende Datenübermittlungen von Nutzerdaten (insbesondere KfZ-Kennzeichen) an den Privaten grundsätzlich einer Rechtsgrundlage im Sinne von Art. 6 Abs. 1 DSGVO bedürfen. Anders kann man dies nur sehen, wenn sich öffentliche Stelle und privater Dienstleister hinsichtlich des Datenaustausches auf die sog. Privilegierungswirkung der Auftragsverarbeitung berufen können. Gemeint damit ist Folgendes: Wie ich in einer Orientierungshilfe[75] dargelegt habe, ist die Weitergabe von Daten durch einen Verantwortlichen an einen Dienstleister im Fall der Auftragsverarbeitung gegenüber anderen Konstellationen der Datenweitergabe privilegiert. Bei Vorliegen der rechtlichen Voraussetzungen für eine Auftragsverarbeitung (insbesondere Art. 28 DSGVO) ist grundsätzlich für die Weitergabe personenbezogener Daten an den Auftragsverarbeiter sowie für die Verarbeitung durch diesen regelmäßig keine weitere Rechtsgrundlage im Sinne von Art. 6 bis 10 DSGVO erforderlich als diejenige, auf die der Verantwortliche selbst die Verarbeitung stützt.

Ich rate daher, bei der Einbindung Privater sicherzustellen, dass die Voraussetzungen einer Auftragsverarbeitung gemäß Art. 28 DSGVO vorliegen, was in der Regel voraussetzt, dass die öffentliche Stelle „Herrin des Verfahrens" bleibt. Daran wird es aber regelmäßig fehlen, wenn die öffentliche Stelle dem privaten Dienstleister die inhaltliche Ausgestaltung des Nutzungsverhältnisses dergestalt überträgt, dass dieser auch eigene Zwecksetzungen verfolgt, also selbst zum Verantwortlichen im Sinne von Art. 4 Nr. 7 DSGVO wird. Wenn der private Dienstleister bei der Durchführung des Kameraparkens (zumindest teilweise) eigenverantwortlich personenbezogene Daten verarbeitet, bedarf dies einer eigenständigen Rechtsgrundlage. Vereinbarungen nach Art. 26 DSGVO stellen dabei keine solche Rechtsgrundlage[76] dar. Daher wird die Datenverarbeitung regelmäßig nur auf der Basis wirksamer Einwilligungen der Parkenden – und zwar gegenüber beiden

[74] Siehe die Ausführungen hinsichtlich der Unzulässigkeit einer regelhaften Einholung von Einwilligungen zur Ausweitung gesetzlich beschränkter Eingriffsbefugnisse in Bayerischer Landesbeauftragter für den Datenschutz, 30. Tätigkeitsbericht 2020, Nr. 7.3.

[75] Bayerischer Landesbeauftragter für den Datenschutz, Auftragsverarbeitung, Stand 4/2019, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

[76] Bayerischer Landesbeauftragter für den Datenschutz, Gemeinsame Verantwortlichkeit, Orientierungshilfe, Stand 6/2024, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

Verantwortlichen – erfolgen können. Schon aus Gründen der Transparenz gemäß Art. 5 Abs. 1 Buchst. a DSGVO kommt es hier besonders auf klare und verständliche Hinweise gegenüber den Parkkunden an, dass in eine Datenverarbeitung durch zwei Verantwortliche eingewilligt werden soll. Natürlich müssen daneben auch die in Nr. 4.7 meines 33. Tätigkeitsberichts 2023 erläuterten sonstigen Voraussetzungen und zusätzlich auch die Anforderungen des Art. 26 BayDSG erfüllt sein.

5.6 Auch eine Aktiengesellschaft kann eine öffentliche Stelle sein

Immer öfter kommt es vor, dass Gebietskörperschaften wie Gemeinden die Erfüllung ihrer öffentlichen Aufgaben der Leistungsverwaltung teilweise an eigens dafür gegründete privatrechtlich organisierte Unternehmen „outsourcen". Solche Unternehmen sind sehr häufig als Gesellschaften mit beschränkter Haftung organisiert, aber auch andere Rechtsformen, wie die einer Aktiengesellschaft kommen mittlerweile vor. Auch letztere Rechtsform kann eine „öffentliche Stelle" im datenschutzrechtlichen Sinne sein, was im Berichtszeitraum verwaltungsgerichtlich bestätigt wurde.[77]

5.6.1 Warum ist die Unterscheidung zwischen öffentlicher und nichtöffentlicher Stelle wichtig?

Die Unterscheidung zwischen öffentlichen und nicht-öffentlichen Stellen ist zunächst wesentlich für die Auswahl der richtigen Aufsichtsbehörde, da in Bayern zwei unterschiedliche Datenschutzaufsichtsbehörden jeweils den privatwirtschaftlichen Sektor (Bayerisches Landesamt für Datenschutzaufsicht) und den öffentlichen Bereich (Bayerischer Landesbeauftragter für den Datenschutz) überwachen. Auch das Rechtsregime, an dem Datenverarbeitungen zu messen sind, unterscheidet sich: Während für den Privatsektor neben der Datenschutz-Grundverordnung vordergründig das Bundesdatenschutzgesetz (BDSG) gilt, sind für bayerische öffentliche Stellen das Bayerische Datenschutzgesetz sowie gegebenenfalls vorrangige fachspezifische Regelungen einschlägig. Das Bayerische Datenschutzgesetz enthält beispielsweise eine Spezialnorm für die Videoüberwachung durch bayerische öffentliche Stellen.

5.6.2 Was eine bayerische öffentliche Stelle ist, definiert Art. 1 BayDSG

Die Datenschutz-Grundverordnung unterscheidet selbst zwar nicht zwischen „öffentlichen" und „nichtöffentlichen" Stellen, verbietet den Mitgliedsstaaten aber auch nicht, eine solche Unterscheidung vorzunehmen.[78] In Deutschland werden diese Begriffe sowohl im Bundesdatenschutzgesetz als auch in den landesrechtlichen Regelungen wie dem Bayerischen Datenschutzgesetz beschrieben. Um die Zuständigkeitsfrage und die Frage nach dem einschlägigen Rechtsregime beantworten zu können, ist also zunächst zu klären, was sich hinter dem Begriff der „öffentlichen Stelle" konkret verbirgt. Geht es um Behörden wie Ministerien oder Bezirksregierungen oder etwa um Gebietskörperschaften wie Gemeinden oder Landkreise, fällt die Einordnung nicht schwer; auf eine tiefergehende Prüfung

[77] Verwaltungsgericht München, Urteil vom 12. Februar 2025, M 7 K 22.4558.
[78] Klar/Kühling, in: Kühling/Buchner, DSGVO/BDSG, 4. Aufl. 2024, § 2 BDSG Rn. 2.

kann hier weitgehend verzichtet werden. Bei privatrechtlich organisierten Stellen ist hingegen ein genauerer Blick ins Gesetz veranlasst, wobei sich zunächst die Frage stellt, welches Gesetz eigentlich die maßgebliche Definition enthält.

Geht man entsprechend der bundesstaatlichen Normenhierarchie „von oben nach unten" vor, fällt der Blick konsequenterweise zunächst auf § 2 Abs. 2 bis 4 Bundesdatenschutzgesetz.

> **§ 2 BDSG**
> **Begriffsbestimmungen**
> […]
> (2) Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes oder sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.
> (3) Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nichtöffentlicher Stellen als öffentliche Stellen des Bundes, wenn
> 1. sie über den Bereich eines Landes hinaus tätig werden oder
> 2. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.
>
> Andernfalls gelten sie als öffentliche Stellen der Länder.
> […]
> (4) Nichtöffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. Nimmt eine nichtöffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.
> […]

Weil aber das BDSG insgesamt nach dessen § 1 Abs. 1 Satz 1 Nr. 2 gegenüber dem Datenschutzrecht der Länder keinen Vorrang beansprucht, haben § 2 Abs. 2 bis 4 BDSG in der Praxis keine große Bedeutung.[79] Die Grundregel des Art. 31 Grundgesetz „Bundesrecht bricht Landesrecht" gilt bei der Einordnung als öffentliche Stelle also gerade nicht: Das Bundesdatenschutzgesetz gilt für öffentliche Stellen der Länder nämlich nur dann, wenn der Datenschutz nicht durch Landesgesetz geregelt ist. Das Bundesdatenschutzgesetz hat insoweit lediglich den Charakter eines „Auffanggesetzes".[80] Da auch Bayern seine Kompetenz zur Normierung des Datenschutzes genutzt und das Bayerische Datenschutzgesetz erlassen hat, ist für die Frage, was eine bayerische öffentliche Stelle ist, nicht das Bundesdatenschutzgesetz, sondern das Bayerische Datenschutzgesetz maßgeblich.

5.6.3 Aktiengesellschaft als öffentliche Stelle gemäß Art. 1 Abs. 2 Satz 1 BayDSG

Auch Aktiengesellschaften in öffentlicher Hand können nach Art. 1 Abs. 2 BayDSG öffentliche Stellen sein, wenn die im Folgenden erläuterten Voraussetzungen zutreffen.

[79] Engelbrecht, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, § 2 BDSG Rn. 26 f.

[80] Bundestags-Drucksache 18/11325, S. 79.

Art. 1 BayDSG
Anwendungsbereich des Gesetzes
[...]
(2) [1]Öffentliche Stellen sind auch Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen – ungeachtet der Beteiligung nicht öffentlicher Stellen – eine oder mehrere der in Abs. 1 Satz 1 genannten juristischen Personen des öffentlichen Rechts unmittelbar oder durch eine solche Vereinigung beteiligt sind. [2]Öffentlich rechtliche Finanzdienstleistungsunternehmen sowie ihre Zusammenschlüsse und Verbände gelten als nicht öffentliche Stellen.
[...]

5.6.3.1 Beteiligung einer juristischen Person des öffentlichen Rechts

Insoweit sind auch die gerade bei Holdingstrukturen anzutreffenden Schachtelbeteiligungen nicht ausgeschlossen. Insoweit ist irrelevant, ob das zwischengeschaltete Unternehmen auch selbst eine Aufgabe der öffentlichen Verwaltung wahrnimmt oder das operative Geschäft mit dem „Enkelunternehmen" teilt.[81]

5.6.3.2 Aufgabe der öffentlichen Verwaltung

Dies ist eine Aufgabe, die zwar auch durch einen Hoheitsträger hoheitlich oder schlicht-hoheitlich erfüllt werden kann, jedoch von ihm deswegen nicht erfüllt wird, weil sich der Hoheitsträger hierfür einer privatrechtlichen Vereinigung bedient, die diese Aufgabe in Privatrechtsform wahrnimmt.[82] Beispielsweise ist die Gewährleistung des öffentlichen Personennahverkehrs eine solche Aufgabe der öffentlichen Verwaltung. Diese umfasst nicht nur die unmittelbare Erbringung der Verkehrsdienstleistungen (vgl. Art. 57 Abs. 1 Gemeindeordnung und Art. 83 Abs. 1 Verfassung des Freistaates Bayern), sondern auch die diese bedingenden und begleitenden Bau-, Beschaffungs- und Bereitstellungs-dienstleistungen, was sich aus Art. 4 Abs. 3 Gesetz über den öffentlichen Personennahverkehr in Bayern (BayÖPNVG) ableiten lässt. Insoweit ist gerade keine hoheitliche Aufgabe erforderlich. Das Bayerische Datenschutzgesetz kennt zwar auch den Begriff der hoheitlichen Aufgabe, aber in anderem Zusammenhang, nämlich im Fall der Beleihung privater Stellen (vgl. Art. 1 Abs. 4 BayDSG). Dagegen umfasst Art. 1 Abs. 2 BayDSG gerade die sog. Leistungsverwaltung, also die Erbringung der klassischen Daseinsvorsorgeleistungen, wie etwa die Versorgung mit Wasser – oder eben die Erbringung von Verkehrsdienstleistungen des öffentlichen Personennahverkehrs auf der Ebene der Gleichordnung, regelmäßig zivilrechtlich eingehegt durch Verträge mit den Kundinnen und Kunden.

5.6.3.3 Beherrschung durch eine juristische Person des öffentlichen Rechts

Art. 1 Abs. 2 BayDSG enthält als ungeschriebenes Tatbestandsmerkmal zudem noch die Vorgabe, dass eine juristische Person des öffentlichen Rechts im Sinne von Art. 1 Abs. 1 Satz 1 BayDSG bei einer Beteiligung, eine beherrschende Stellung innehaben muss.[83] Ein Beherrschungsverhältnis kann etwa angenommen werden, wenn eine juristische Person die Mehrheit der Anteile hält. Eine Beherrschung durch die öffentliche Hand liegt aber auch vor, wenn sämtliche Anteilseig-

[81] Engelbrecht, in: Schröder, Bayerisches Datenschutzgesetz, 2021, Art. 1 BayDSG Rn. 31.
[82] Niese, in: Wilde/Ehmann/Niese/Knoblauch, Datenschutz in Bayern, 38. Erg.-Lief. 2025, Art. 1 BayDSG Rn. 13, 45.
[83] Engelbrecht, in: Schröder, Bayerisches Datenschutzgesetz, 2021, Art. 1 BayDSG Rn. 26.

ner oder Mitglieder zu den in Art. 1 Abs. 1 Satz 1 BayDSG genannten (bayerischen) juristischen Personen des öffentlichen Rechts zählen.[84] Auch im kürzlich gerichtlich überprüften Fall hielt die Kommune mittelbar einhundert Prozent der Aktien des Unternehmens.

5.6.4 Fazit

Auch Aktiengesellschaften sind bayerische öffentliche Stellen, wenn die gerade eben erläuterten Voraussetzungen des Art. 1 Abs. 2 BayDSG vorliegen. Eine gegenüber gemeindlichen Gesellschaften mit beschränkter Haftung abweichende Bewertung würde letztlich auch dazu führen, dass durch entsprechende Rechtsformwahl eine wenig überzeugende „Fluchtmöglichkeit ins private Datenschutzregime“ eröffnet würde.

[84] Engelbrecht, in: Schröder, Bayerisches Datenschutzgesetz, 2021, Art. 1 BayDSG Rn. 28.

6 E-Government, öffentliche Register

6.1 Gesetzgeberischer Handlungsbedarf für „Geoportale“ (Kartenviewer)

Auch in diesem Berichtszeitraum war ich intensiv mit datenschutzrechtlichen Fragestellungen im Zusammenhang mit der Veröffentlichung von grundstücks- oder gebäudebezogenen Daten auf unterschiedlichen Online-Portalen (Kartenviewern) befasst. So habe ich nicht nur staatliche Kartenviewer, etwa bei der Veröffentlichung von Windkraftstandorten oder bei der Darstellung von Hochwassergefahren, datenschutzrechtlich betrachtet, sondern mich auch verstärkt den gemeindlichen Angeboten gewidmet. Insoweit möchte ich wegen der Vielzahl von Beratungsanfragen und der grundsätzlichen Praxisrelevanz für die bayerischen öffentlichen Stellen in Ergänzung meines Beitrags „BayernAtlas: gesetzgeberischer Handlungsbedarf“ in meinem 31. Tätigkeitsbericht 2021 unter Nr. 6.2 einige ausgewählte Aspekte näher erläutern.

6.1.1 Solarpotenzialkataster

Das Augenmerk vieler Beratungsanfragen der bayerischen Kommunen lag auf datenschutzrechtlichen Möglichkeiten für kartenbasierte Veröffentlichungen von Solarpotenzialdaten gemeindlicher Dachflächen, insbesondere der Informationen über deren Eignung für Photovoltaik-Anlagen.

6.1.2 Datenschutzrechtliche Relevanz

Dass auch Geodaten personenbezogene Daten sein können, habe ich bereits ausführlich in meinem 31. Tätigkeitsbericht 2021 unter Nr. 6.2.1 behandelt. So stellen auch (veröffentlichte) Photovoltaik-Solarpotenzialdaten von Hausdächern privater Eigentümer, welche mit einzelnen Grundstücken – etwa durch eine flurstücksbezogene Darstellung – verknüpft sind, regelmäßig personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO dar.

Zum einen sind die Eigentümer der betreffenden Grundstücke über das Liegenschaftskataster und das Grundbuch beziehungsweise durch eigene Verzeichnisse des für die Veröffentlichung Verantwortlichen zumindest für diesen bestimmbar. Zudem sind die jeweiligen Grundstückseigentümer regelmäßig bereits aufgrund besonderer Ortskenntnisse für Nutzer eines kartenbasierten Solarpotenzialkatasters unschwer zu ermitteln. Dies gilt grundsätzlich auch bei Gebäude- und Dachflächendarstellungen, die „nur“ mittels Adresse mit den Grundstücken verknüpft sind.

Zum anderen vermitteln die Solarpotenzialdaten Informationen über den mit dem Hausdach zu erzielenden Ertrag, mithin Informationen über sachliche und mittelbar auch über wirtschaftliche Verhältnisse von bestimmbaren natürlichen Personen. Einen solchen Rückschluss erlaubt bereits die Angabe über die grundsätzliche Eignung der einzelnen Dachflächen für die Gewinnung von Solarenergie – etwa im Sinne einer (farblich dargestellten) Einstufung (geeignet, ungeeignet, be-

dingt geeignet). Auch wenn hierdurch nicht der tatsächliche Wert des zu erzielenden Ertrags abgebildet wird, enthält die Information durchaus eine Aussage über die grundsätzliche Ertragsfähigkeit einer bestimmten Dachfläche. Üblicherweise basiert diese Einstufung der Dachfläche auf einer Berechnung anhand der portalseitig errechneten Größe der Dachfläche, die hierdurch eine andere Qualität als eine Einschätzung eines Passanten erfährt. Auch hier gilt: je genauer und umfassender die im Internet veröffentlichten kartenbasierten Angaben zur Ertragsfähigkeit und die Darstellung der Karte sind und je mehr Funktionalitäten das Solarpotenzialkataster bietet, desto eingriffsintensiver ist es.

6.1.3 Geeignete Rechtsgrundlage für die Veröffentlichung

Mit der Veröffentlichung von Solarpotenzialdaten auf einer Karte werden personenbezogene Daten verarbeitet, Art. 4 Nr. 2 DSGVO, wofür die Verantwortlichen eine Rechtsgrundlage benötigen. Die Tatsache, dass die Informationen alle schon vorhanden und öffentlich einsehbar sind, vermag nicht per se die Rechtmäßigkeit der Verarbeitung der hiervon umfassten personenbezogenen Daten zu begründen. Vielmehr ist gemäß Art. 6 Abs. 1, Abs. 3 DSGVO eine Rechtsgrundlage für die Datenverarbeitung – hier die Veröffentlichung in einem weltweit zugänglichen Internetportal – erforderlich. Wie mehrfach ausgeführt, kommen für öffentliche Stellen insbesondere Art. 6 Abs. 1 UAbs. 1 Buchst. c oder Buchst. e DSGVO in Betracht – in Verbindung mit der zugrundeliegenden rechtlichen Verpflichtung oder Aufgabe mit Verarbeitungsbefugnis aus dem Unionsrecht oder einer hinreichend konkreten nationalrechtlichen Regelung, die insbesondere den Zweck der Verarbeitung festlegt (Art. 6 Abs. 3 DSGVO). Dieser muss sich auf eine proaktive, anlasslose und generelle Veröffentlichung in einem frei zugänglichen Portal erstrecken (vgl. meinen 31. Tätigkeitsbericht 2021 unter Nr. 6.2.2.1). Insoweit sind etwaige allgemeine Verarbeitungsbefugnisse, wie etwa Art. 4 Abs. 1 BayDSG in Verbindung mit Art. 57 Gemeindeordnung grundsätzlich ungeeignet, solche Datenverarbeitungen zu rechtfertigen.

6.1.3.1 Anhörungserfordernis des Bayerischen Umweltinformationsgesetzes

Als eine solche fachgesetzliche Rechtsgrundlage für die Veröffentlichung kommt grundsätzlich Art. 10 in Verbindung mit Art. 8 Abs. 1 Bayerisches Umweltinformationsgesetz (BayUIG) in Betracht, der die Unterrichtung der Öffentlichkeit über Umweltinformationen regelt. Für die Veröffentlichung eines Solarpotenzialkatasters greifen die öffentlichen Stellen allerdings bereits deshalb nicht auf Art. 8 Abs. 1 BayUIG zurück, weil die Betroffenen vor der Entscheidung über die Offenbarung der Informationen anzuhören sind, vgl. Art. 10 Abs. 6 in Verbindung mit Art. 8 Abs. 1 Satz 3 BayUIG. Auch bei einer kleinen Gemeinde könnte eine solche Anhörung die Veröffentlichung der Daten für das gesamte Gemeindegebiet verhindern.

Nicht zu vernachlässigen ist darüber hinaus, dass regelmäßig vorab eine Abwägung der schutzwürdigen Interessen der betroffenen Grundstückseigentümer und des öffentlichen Interesses an der Bekanntgabe durchgeführt werden und zugunsten des Letzteren ausfallen muss. Dies wird häufig aus Gründen, die ich bereits in meinem 24. Tätigkeitsbericht 2010 unter Nr. 6.5 angeführt habe, zu verneinen sein.

6.1.3.2 Geltung des Bayerischen Geodateninfrastrukturgesetzes für Veröffentlichungen (nur) im Geoportal des Landes

Das Bayerische Geodateninfrastrukturgesetz (BayGDIG) sieht für sogenannte betroffene Geodaten im Sinne des Art. 2 Abs. 1 BayGDIG sogar eine Verpflichtung von Behörden vor, Geodatendienste bereitzustellen. Es vermittelt jedoch keine Veröffentlichungspflicht oder -befugnis für die Veröffentlichung von Solarpotenzialkatastern durch bayerische öffentliche Stellen, namentlich die Kommunen oder Landkreise. Denn der Zugang zu den betroffenen Geodaten erfolgt nach Art. 6 Abs. 2 BayGDIG in Verbindung mit Art. 1 Abs. 2 BayGDIG durch ein Geoportal des Landes. Dies ist das Geoportal Bayern mit dem dazugehörigen BayernAtlas als Kartenviewer. Insbesondere Veröffentlichungen in Internetportalen der Kommunen sind von dieser Rechtsfolge daher nicht gedeckt.

Zudem ist bei personenbezogenen Daten nach Art. 8 Abs. 3 Satz 2 Nr. 1 BayGDIG – ähnlich wie im Rahmen des Art. 8 Abs. 1 BayUIG – der Zugang der Öffentlichkeit zu den Daten eingeschränkt, soweit hierdurch schutzwürdige Interessen der Betroffenen beeinträchtigt würden, es sei denn, die Betroffenen haben zugestimmt, das öffentliche Interesse an dem Zugang überwiegt, oder die Geodaten sind nach anderen Rechtsvorschriften für die Öffentlichkeit zugänglich.[85]

6.1.4 Keine neuen Veröffentlichungsbefugnisse aufgrund der Durchführungsverordnung (EU) 2023/138 zur sogenannten PSI-Richtlinie[86]

Die Vorschriften der unmittelbar in den Mitgliedstaaten geltenden Durchführungsverordnung (EU) 2023/138 der Kommission vom 21. Dezember 2022 zur Festlegung bestimmter hochwertiger Datensätze und der Modalitäten ihrer Veröffentlichung und Weiterverwendung (DVO-HVD) regeln keine neuen Bereitstellungspflichten für öffentliche Stellen, sondern setzen diese voraus:

Die DVO-HVD geht zurück auf die sogenannte PSI-Richtlinie, die in Deutschland unter anderem durch das Datennutzungsgesetz umgesetzt wurde. Mit ihr hat die Europäische Kommission thematische Kategorien hochwertiger Datensätze und besondere (technische) Anforderungen an deren Weiterverwendungsmodalitäten festgelegt. Die DVO-HVD soll dafür sorgen, dass Nutzerinnen und Nutzer öffentliche Daten mit hohem sozioökonomischem Wert einfach und kostenlos weiterverwenden können (vgl. EG 2 DVO-HVD). Die DVO-HVD enthält aber selbst keine eigenen Zugangsansprüche zu solchen Daten – und kann in dieser Hinsicht auch nicht über die PSI-Richtlinie hinausgehen –, sondern regelt nur die (Modalitäten der) Weiterverwendung von bereits auf anderer Rechtsgrundlage zur Verfügung gestellter Daten, vgl. § 1 Abs. 2 Datennutzungsgesetz (DNG): „Eine Bereitstellungspflicht oder ein Anspruch auf Zugang zu Daten wird mit diesem Gesetz nicht begründet."

Mit Blick auf die Bereitstellung von personenbezogenen Daten stellt die DVO-HVD zudem ausdrücklich klar, dass diese Verarbeitung im Einklang mit dem Uni-

[85] Vgl. Bayerischer Landesbeauftragter für den Datenschutz, 31. Tätigkeitsbericht 2021, Nr. 6.2.2.2.

[86] 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 (ABl. L 172 vom 26. Juni 2019, S. 56).

onsrecht zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, insbesondere der Datenschutz-Grundverordnung, und mit allen Bestimmungen des nationalen Rechts zur Präzisierung der Anwendung der Datenschutz-Grundverordnung erfolgen soll (EG 8 Satz 1 DVO-HVD). Die PSI-Richtlinie und das sie umsetzende Datennutzungsgesetz nehmen explizit Daten aus dem Anwendungsbereich heraus, die unter anderem deshalb nicht oder nur eingeschränkt zugänglich sind, weil der Schutz personenbezogener Daten entgegensteht (Art. 1 Abs. 2 Buchst. h PSI-Richtlinie, § 2 Abs. 3 Nr. 1 Buchst. a Doppelbuchst. aa DNG).

Damit korrespondierend begründet die DVO-HVD auch keinen Anspruch Einzelner auf Zugang zu den dort festgelegten hochwertigen Datensätzen in einer dort festgelegten Form.

6.1.5 Ausblick

Bereits seit 2021 setze ich mich für eine übergreifende und zukunftsoffene gesetzliche Lösung ein, die alle „Geoportale“ (Kartenviewer) des Landes und der Kommunen, wie die vorgenannten Solarpotenzialkataster, adressieren könnte. Dies wäre unter Berücksichtigung der Interessen Einzelner im Wege einer Überarbeitung und Ergänzung des Bayerischen Geodateninfrastrukturgesetzes meines Erachtens gut erzielbar. Insoweit stehe ich mit dem zuständigen Bayerischen Staatsministerium der Finanzen und für Heimat im Austausch.

6.2 Digitalisierung des Wasserbuchs

Der Zugang zu sauberem Wasser ist ein Menschenrecht, wie die Vereinten Nationen per Resolution im Jahr 2010 ausdrücklich anerkennen.[87] Nutzungsansprüche und Vorgaben zum Umgang mit Wasser waren aber schon deutlich früher Gegenstand des Rechts, insbesondere auch von gesetzlichen Regelungen. So entstammen etwa die ersten Wassergesetze im Freistaat Bayern bereits dem Jahr 1852. Wasserrechtliche Erlaubnisse und Gestattungen sind heute nicht nur für die Industrie mit ihrem hohen Bedarf an Nutzwasser von Relevanz, sondern gerade auch für natürliche Personen, beispielsweise bei der Grundwasserentnahme für Brunnenanlagen, bei der Installation von Wärmepumpen oder für Erlaubnisse in Bezug auf Kleinkläranlagen. Damit kann auch das Wasserrecht datenschutzrelevante Fragestellungen beinhalten.

Wasserrechtliche Erlaubnisse haben eine oftmals eine lange Lebensdauer und können über Generationen hinweg quasi „vererbt“ werden. Auch heute noch können daher sogenannte historische „Altrechte“ eine Rolle spielen. All diese neuen und alten Erlaubnisse und Gestattungen werden bei den zuständigen Behörden (zumeist den Kreisverwaltungsbehörden) im sogenannten Wasserbuch aufgeführt. Diese Wasserbücher wurden bisher oftmals noch in analoger Form, als papierbasierte Register, geführt. Dies hat einen schnellen und effizienten Informationsaustausch im Rahmen des Erforderlichen über Zuständigkeits-(Landkreis)-grenzen hinaus, an die sich insbesondere Fließgewässer auch nicht halten, oftmals

[87] Vereinte Nationen, Generalversammlung, Resolution 64/292 vom 28. Juli 2010, A/RES/64/292.

deutlich erschwert. Auch angesichts neuer Herausforderungen wie Extremwetterereignissen und der dadurch verstärkten Notwendigkeit einer engen Zusammenarbeit von Behörden über Zuständigkeitsgrenzen hinaus hat der bayerische Gesetzgeber insoweit einen Modernisierungsbedarf gesehen. Mit der Novelle des Bayerischen Wassergesetzes (BayWG)[88] wurde daher neben einigen Neuerungen bei der öffentlichen Trinkwasserversorgung, im Hochwasserschutz und der Einführung des sog. „Wassercents" gerade auch die Digitalisierung des Wasserbuchs beschlossen. Dieses nachvollziehbare Vorhaben habe ich aus datenschutzrechtlicher Sicht begleitet.

Nach der bisher gültigen Regelung überführten die Kreisverwaltungsbehörden ihre getroffenen wasserrechtlichen Erlaubnisse (mit einigen Einschränkungen, beispielsweise bei „untergeordneter wasserwirtschaftlicher Bedeutung" – § 87 Abs. 2 Wasserhaushaltsgesetz) in das Wasserbuch. Dieses stellte sich damit primär als Sammlung von Bescheiden und anderen Regelungen dar. Das Wasserbuch hatte also bislang eher einen „nachweisenden oder archivierenden" Charakter. Sein Sinn war es letztlich vorrangig, behördenintern einen Überblick über die in speziellen wasserrechtlichen Verfahren bereits getroffenen Entscheidungen zu ermöglichen. Einheitliche Vorgaben zu dessen Ausgestaltung und insbesondere zu Digitalisierungsmaßnahmen gab es bisher nicht.

Das hat sich durch die Digitalisierung des Wasserbuchs im Rahmen der Novelle des Bayerischen Wassergesetzes in mehrfacher Hinsicht geändert. Zunächst hat das bayernweite digitale Wasserbuch nun nicht mehr nur einen behördeninternen „nachweisenden oder archivierenden" Charakter. Vielmehr soll es als gemeinsame digitale „lebende" Arbeitsplattform für mehrere zuständige Behörden in laufenden wasserrechtlichen Verfahren dienen. Auch sieht es – unter der Prämisse der ausdrücklich bereits im Normtext adressierten Erforderlichkeit – Einsichtsrechte für solche Stellen vor, die selbst keine Erlaubnisse erteilen, dennoch einen (aufsichtlichen) Einblick in wasserrechtliche Verfahren benötigen. Bei der Begleitung dieser Neuregelung war mir aus datenschutzrechtlicher Sicht insbesondere wichtig, dass klare Regelungen zu den Zwecken dieses digitalen Wasserbuchs getroffen werden, und dass die meines Erachtens vorliegende gemeinsame Verantwortlichkeit gemäß Art. 26 DSGVO klar als solche benannt wird. Auch konnte ich erreichen, dass ein Berechtigungs- und Zugriffskonzept sowie Löschvorgaben im Rahmen einer konkretisierenden Verordnung bestimmt werden sollen. Aus datenschutzrechtlicher Sicht ist außerdem begrüßenswert, dass auf eine Verpflichtung zur Veröffentlichung des Wasserbuchs verzichtet wurde, denn dieses stellt gerade kein öffentliches Register dar. Am 1. Januar 2026 trat die Neuregelung im Wortlaut wie folgt in Kraft:

> **Art. 53 BayWG**
> **Digitales bayernweites Wasserbuch (Zu § 87 WHG)**
> (1) [1]Die nach Art. 63 zuständigen Behörden führen jeweils für ihren Zuständigkeitsbereich von Amts wegen das bayernweite digitale Wasserbuch in gemeinsamer Verantwortlichkeit im Sinne des Art. 26 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO). [2]In das digitale Wasserbuch sind alle wasserrechtlichen Rechtsakte und Anzeigen mit den jeweiligen Anlagen und zugehörigen Planbeilagen einzutragen. [3]Bei rechtzeitig angemeldeten behaupteten alten Rechten und Befugnissen tritt an die Stelle des Bescheids die Anmeldung.
> (2) [1]Die im Sinne von Art. 63 zuständigen Behörden können die Daten des Wasserbuchs im Rahmen ihrer örtlichen Zuständigkeit soweit erforderlich für die in Abs. 3 genannten Zwecke

[88] GVBl. 2025 S. 667.

verarbeiten. [2]Die im Sinne von Art. 58 zuständigen Behörden können diese Daten im Rahmen ihrer örtlichen Zuständigkeit soweit erforderlich auslesen und verwenden.

(3) Die Verarbeitung der Daten der Wasserbücher erfolgt zu folgenden Zwecken:

1. Grundlage für wasserwirtschaftliche Planungen und Gewässerausbauvorhaben nach diesem Gesetz, dem Wasserhaushaltsgesetz und sonstigen wasserrechtlichen Vorschriften,
2. Grundlage für einzelne Bewirtschaftungsmaßnahmen nach diesem Gesetz, dem Wasserhaushaltsgesetz und sonstigen wasserrechtlichen Vorschriften,
3. Kenntnis über die Rechtsverhältnisse an Gewässern, insbesondere in Bezug auf die Feststellung Beteiligter in einem wasserrechtlichen Verfahren und die Ermittlung wasserrechtlicher Belange in sonstigen Verfahren,
4. Vollzug des Teils 5 und des Kapitels 5 WHG,
5. Vollzug des Teils 7 und des Abwasserabgabengesetzes (AbwAG),
6. wissenschaftliche Forschung sowie
7. Erfüllung von Informations- und Berichtspflichten.

(4) [1]Das Staatsministerium regelt in der Rechtsverordnung nach Art. 69 Abs. 6, wie das Wasserbuch einzurichten und zu führen ist. [2]Es kann insbesondere die Pflichten der Verantwortlichen für die Datenverarbeitung im Sinne des Art. 26 DSGVO festlegen und bestimmen, welche in analoger Form vorhandenen Inhalte zur Begrenzung des Aufwands von einer Überführung in die digitale Form ausgenommen werden. [3]Ein Berechtigungs- und Zugriffskonzept sowie Vorgaben zum Löschen sind vorzusehen.

(5) Entstehung, Abänderung und Untergang eintragungsfähiger Rechtsverhältnisse bleiben durch die Eintragung in das Wasserbuch unberührt.

6.3 Transparenz bei der Digitalisierung von Planverfahren: Einführung der digitalen Plattform „DiPlanung“

Im Berichtszeitraum wurde ich vom zuständigen Bayerischen Staatsministerium für Wohnen, Bau und Verkehr bei der Einführung der digitalen Plattform „DiPlanung“ beteiligt. Hierbei konnte ich für die betroffenen Bürgerinnen und Bürger ein deutliches „Mehr“ an Transparenz erreichen.

6.3.1 Zweck und Hintergrund der digitalen Plattform „DiPlanung“

Die Plattform „DiPlanung“ dient der Digitalisierung von Planungs- und Beteiligungsverfahren, insbesondere im Bereich der Bauleitplanung nach dem Baugesetzbuch. Dazu werden den jeweils zuständigen Stellen folgende drei Komponenten zur Nachnutzung angeboten:

— „DiPlan Portal“: Zugang zu rechtswirksamen/rechtskräftigen Planwerken,

— „DiPlan Beteiligung“: digitale Durchführung von Beteiligungsprozessen über eine Portallösung,

— „DiPlan Cockpit“: digitale Verfahrenssteuerung und Verknüpfung von „DiPlan Portal“ und „DiPlan Beteiligung“.

Die Plattform wurde ursprünglich von der Freien und Hansestadt Hamburg entwickelt und wird nun im Rahmen des „EfA“-Prinzips („Einer für Alle“) nach dem Onlinezugangsgesetz anderen Ländern zur Verfügung gestellt. Dazu haben Hamburg und der Freistaat Bayern ein entsprechendes Verwaltungsabkommen sowie in datenschutzrechtlicher Hinsicht eine Vereinbarung über eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO geschlossen. Die in der Plattform verarbeite-

ten Daten werden auf der Cloud eines Drittanbieters in Schleswig-Holstein gespeichert. Insoweit besteht zwischen Hamburg und dem Drittanbieter eine Auftragsverarbeitungsvereinbarung nach Art. 28 Abs. 3 DSGVO. Genutzt werden soll die Plattform zunächst einmal vor allem von den die Bauleitplanung betreibenden Kommunen (vgl. § 1 Abs. 3 Baugesetzbuch – BauGB) als sog. Nachnutzung. Bei der (Nach)Nutzung der Plattform werden personenbezogene Daten der Mitarbeitenden der jeweiligen Stelle und der von der Bauleitplanung betroffenen Bürgerinnen und Bürger – insbesondere bei der Erhebung von etwaigen Einwendungen im Rahmen der Öffentlichkeitsbeteiligung – verarbeitet.

6.3.2 Einwilligung keine Rechtsgrundlage bei der Datenverarbeitung

Die ursprüngliche Konzeption der Plattform sah insoweit vor, dass Bürgerinnen und Bürger, die im Rahmen der Öffentlichkeitsbeteiligung bei der Bauleitplanung personenbezogene Einwendungen erheben wollen („DiPlan Beteiligung", vgl. oben), eine Einwilligung zur Verarbeitung ihrer personenbezogenen Daten abgeben müssen. Diesbezüglich habe ich das Bauministerium darauf aufmerksam gemacht, dass sich öffentliche Stellen grundsätzlich nur zur Aufgabenabrundung (arrondierend), nicht aber für zentrale, beziehungsweise gewichtige, weil eingriffsintensive Verarbeitungsschritte, auf Einwilligungen berufen können. Grundsätzlich werden personenbezogene Daten nämlich von öffentlichen Stellen auf Grundlage gesetzlicher Verarbeitungsbefugnisse – hier solchen des Planungsrechts – verarbeitet (siehe meine Ausführungen im 29. Tätigkeitsbericht 2019 unter Nr. 5.6.2 und im 30. Tätigkeitsbericht 2020 unter Nr. 7.3.2). Bei der Erhebung von personenbezogenen Daten sind jedoch die Informationspflichten nach Art. 13 DSGVO zu erfüllen. In diesem Kontext konnte ich erreichen, dass die ursprünglich für die Einholung entsprechender Einwilligungen vorgesehene Konzeption gleichsam umgewidmet wurde und nun für die Erfüllung dieser Informationspflichten genutzt wird.

6.3.3 Verarbeitungen in gemeinsamer Verantwortlichkeit

Im Rahmen meiner Beteiligung hat sich ergeben, dass eine dem datenschutzrechtlichen Transparenzgebot des Art. 5 Abs. 1 Buchst. a DSGVO gerecht werdende Digitalisierung am ehesten erreicht werden kann, wenn die Datenverarbeitungen beim Betrieb des Portals in einer gemeinsamen Verantwortlichkeit aller beteiligten Stellen gleichsam eingehegt werden. Die beteiligten Stellen sind im Einzelnen Hamburg, das Bauministerium und die jeweilige nachnutzende Stelle, also zunächst einmal primär die jeweilige das Portal zur Bauleitplanung nutzende Kommune. Insoweit handelt es sich um ein komplexes System, in welchem verschiedene Stellen unterschiedliche Einflussmöglichkeiten im Hinblick auf die erfolgenden Verarbeitungstätigkeiten haben. In einer solchen Konstellation besteht meine Intention regelmäßig darin, für die betroffenen Bürgerinnen und Bürger ein Höchstmaß an Transparenz im Sinne von Art. 5 Abs. 1 Buchst. a DSGVO zu schaffen. Um dies zu gewährleisten, wird daher die zwischen Hamburg und dem Bauministerium bereits in der Vergangenheit geschlossene (bilaterale) Vereinbarung nach Art. 26 DSGVO jeweils mittels einer entsprechenden Vereinbarung auf die konkreten nachnutzenden Stellen (multilateral) erweitert. Dies erfolgt auf unbürokratischem Wege, indem im Rahmen der administrativen Anbindung der nachnutzenden Stellen durch Setzen eines „Häkchens" eine verlinkte – passgenau – vorformulierte Vereinbarung abgeschlossen wird (vgl. dazu meine Ausführungen im

32. Tätigkeitsbericht 2022 unter Nr. 6.1.1). Bei der Formulierung dieser Vereinbarung habe ich das Bauministerium intensiv beraten und konnte dabei vor allem Verbesserungen im Hinblick auf die Transparenz erreichen. Wichtig war mir insbesondere, dass für alle Bereiche der gemeinsamen Verantwortlichkeit klar geregelt ist, welche der beteiligten Stellen welche Pflichten nach der Datenschutz-Grundverordnung gegenüber den Bürgerinnen und Bürgern wahrnimmt.

6.3.4 Datenschutzfreundliche Voreinstellungen bei der Ausgestaltung im Detail

Ich habe das zuständige Staatsministerium auch gebeten, bei der weiteren Ausgestaltung der Plattform im Detail insbesondere Einstellungen vorzusehen, welche (versehentliche) datenschutzwidrige Weiterverarbeitungen durch nachnutzende Stellen möglichst vermeiden. Ich denke in diesem Zusammenhang beispielsweise daran, dass eine Gemeinde personenbezogene Inhalte der Plattform im Rahmen einer öffentlichen Gemeinderatssitzung per „Beamer" datenschutzwidrig der Gemeindeöffentlichkeit präsentiert. Insoweit habe ich daran erinnert, dass personenbezogene Einwendungen in öffentlicher Gemeinderatssitzung in der Regel in anonymisierter Form zu behandeln sind (siehe meine Ausführungen im 29. Tätigkeitsbericht 2019 unter Nr. 5.1.2.3).

6.4 Meldedatenübermittlung zur Rundfunkfinanzierung

Der Rundfunkbeitrag ist ein tendenziell eher kontroverses Instrument der Rundfunkfinanzierung. Nicht wenige Beitragspflichtige wehren sich gegen diese Last, zumal wenn sie am Angebot des öffentlich-rechtlichen Rundfunks keinerlei Interesse haben. In den letzten Monaten haben mich vermehrt Beratungsanfragen bayerischer Kommunen erreicht, die in Zusammenhang mit Datenübermittlungen an die Landesrundfunkanstalt/den Beitragsservice zur Zahlung von Schadensersatz aufgefordert wurden. Die entsprechenden Schreiben stellen auch datenschutzbezogene Überlegungen an.

Der vorliegende Beitrag erläutert den Datenfluss von den bayerischen Meldebehörden an die Landesrundfunkanstalt/den Beitragsservice. Sie zeigt, dass der Gesetzgeber zwar etwas verschachtelte, jedoch ausreichende Rechtsgrundlagen vorgesehen hat.

6.4.1 Beteiligte an den Datenübermittlungen

6.4.1.1 Meldebehörden

Meldedaten werden von den Meldebehörden bereitgestellt. Das sind in Bayern grundsätzlich die Gemeinden (Art. 1 Abs. 1 Satz 1 Bayerisches Gesetz zum Melde-, Pass- und Personalausweiswesen – BayGMPP). Gehört eine Gemeinde einer Verwaltungsgemeinschaft an, nimmt diese die Aufgabe der Meldebehörde wahr, weil es sich dabei um eine Aufgabe des übertragenen Wirkungskreises handelt (Art. 4 Abs. 1 Satz 1 Verwaltungsgemeinschaftsordnung, Art. 1 Abs. 1 Satz 2 BayGMPP).

6.4.1.2 Landesrundfunkanstalt/Beitragsservice

Empfänger der Meldedaten ist die Landesrundfunkanstalt/der Beitragsservice. Landesrundfunkanstalt ist in Bayern der Bayerische Rundfunk. Für den Einzug des Rundfunkbeitrags nutzt der Sender – wie die übrigen Landesrundfunkanstalten – die Dienste des Beitragsservice.[89]

Diese Konstruktion ist in § 10 Abs. 7 Satz 1 Rundfunkbeitragsstaatsvertrag (im Folgenden: RBeitrStV) vorgesehen. Dort heißt es:

> „Jede Landesrundfunkanstalt nimmt die ihr nach diesem Staatsvertrag zugewiesenen Aufgaben und die damit verbundenen Rechte und Pflichten ganz oder teilweise durch die im Rahmen einer nichtrechtsfähigen öffentlich-rechtlichen Verwaltungsgemeinschaft betriebene Stelle der öffentlich-rechtlichen Landesrundfunkanstalten selbst wahr."

Der Beitragsservice „verbirgt" sich hier hinter der sperrigen Formulierung „im Rahmen einer nichtrechtsfähigen öffentlich-rechtlichen Verwaltungsgemeinschaft betriebene Stelle der öffentlich-rechtlichen Landesrundfunkanstalten". Die Vertragsparteien verfolgen ein Konzept, demzufolge die einzelnen Landesrundfunkanstalten jeweils „das Heft in der Hand" behalten – der Beitragsservice soll also grundsätzlich wie eine auf den Beitragseinzug spezialisierte eigene Organisationseinheit der einzelnen Landesrundfunkanstalt agieren –, sich aber gleichzeitig alle Anstalten gemeinsam den Beitragsservice teilen. Die einzelne Landesrundfunkanstalt erhebt den Rundfunkbeitrag also im eigenen Namen und auf eigene Rechnung durch den Beitragsservice; in einschlägigen Verwaltungsstreitsachen ist sie selbst, nicht der Beitragsservice Verfahrensbeteiligte.[90]

Datenschutzrechtlich lässt sich die skizzierte Konstruktion in einer Rollenverteilung abbilden, die den Beitragsservice als einen Teil der öffentlichen Stelle „Landesrundfunkanstalt" ansieht – der nur eben die Besonderheit aufweist, in einem anderen Bundesland ansässig und gemeinsam mit anderen Landesrundfunkanstalten getragen zu sein.[91]

6.4.2 Meldedatenübermittlungen an die Landesrundfunkanstalt

Datenübermittlungen von den Meldebehörden an die Landesrundfunkanstalt/den Beitragsservice sind gesetzlich geregelt. Die einschlägigen Vorschriften sehen sowohl Datenerhebungsbefugnisse für die Landesrundfunkanstalten/den Beitragsservice (a) als auch Datenübermittlungsbefugnisse für die Meldebehörden (b) vor.

[89] Siehe § 2 Rundfunkbeitragssatzung (des Bayerischen Rundfunks), Internet: https://www.br.de/unternehmen/inhalt/organisation/rechtsgrundlagen/rechtsgrundlagen-gesetzestext-gesetze-100.html.

[90] Näher Wissenschaftliche Dienste des Deutschen Bundestages, Beitragseinzugsverfahren des öffentlich-rechtlichen Rundfunks in Deutschland, WD 10 - 3000 - 041/21, S. 11 f.; Vollstreckung von Rundfunkbeitragsforderungen, WD 7 - 3000 - 001/24, S. 7.

[91] Dies entspräche auch dem „Selbstbild" des Beitragsservice, vgl. https://www.rundfunkbeitrag.de/datenschutz/datenschutz_beim_beitragseinzug/index_ger.html#wer_ist_fuer_die_datenverarbeitung_verantwortlich.

6.4.2.1 Meldedatenerhebung durch die Landesrundfunkanstalt, korrespondierende Datenübermittlung durch die Meldebehörde

Zum Zweck der Beitragserhebung sowie zur Feststellung, ob überhaupt eine Beitragspflicht besteht, darf die Landesrundfunkanstalt/der Beitragsservice personenbezogene Daten bei öffentlichen und nichtöffentlichen Stellen ohne Kenntnis der betroffenen Person verarbeiten, (vgl. § 11 Abs. 4 Satz 1 RBeitrStV). Öffentliche Stellen sind in diesem Zusammenhang solche Stellen, die zur Übermittlung der Daten einzelner Inhaber von Wohnungen oder Betriebsstätten befugt sind, darunter die Meldebehörden.

Eine solche Datenerhebung ist allerdings nicht voraussetzungslos möglich; sie muss vielmehr folgende Anforderungen erfüllen (§ 11 Abs. 4 Satz 5 RBeitrStV):

— Eine vorherige Datenerhebung unmittelbar bei der betroffenen Person war erfolglos oder nicht möglich;

— die Datenbestände sind dazu geeignet, Rückschlüsse auf die Beitragspflicht zuzulassen, insbesondere durch Abgleich mit dem Bestand der bei den Landesrundfunkanstalten gemeldeten Beitragsschuldner und

— die Daten beschränken sich auf Angaben, die der Anzeigepflicht nach § 8 RBeitrStV unterliegen, und es besteht kein erkennbarer Grund zu der Annahme, dass die betroffene Person ein schutzwürdiges Interesse an dem Ausschluss der Verarbeitung hat.

Fordert die Landesrundfunkanstalt/der Beitragsservice unter diesen Voraussetzungen bei einer Meldebehörde Daten an, darf die Meldebehörde nach Maßgabe von § 34 Abs. 1 Bundesmeldegesetz (BMG) personenbezogene Daten in dem Umfang übermitteln, der auch im Rahmen des periodischen Datenabgleichs zu liefern ist. Die Meldebehörde prüft, ob die Voraussetzungen von § 34 Abs. 1 BMG erfüllt sind; sie muss sich von der Landesrundfunkanstalt/dem Beitragsservice insbesondere die Erforderlichkeit zur dortigen Aufgabenerfüllung darlegen lassen. Die Voraussetzungen von § 11 Abs. 4 Satz 5 RBeitrStV hat die Meldebehörde dagegen nicht zu würdigen; insofern liegt die Verantwortung bei der Landesrundfunkanstalt/dem Beitragsservice. Die Übermittlung nach § 34 Abs. 1 BMG steht im Ermessen der Meldebehörde; die Meldebehörde muss dieses Ermessen auch ausüben (darf also nicht „blind“ der Anforderung folgen).

6.4.2.2 Regelmäßige Datenübermittlungen durch die Meldebehörde

Von den soeben dargestellten Fällen abgesehen, kann die Meldebehörde zugunsten des öffentlich-rechtlichen Rundfunks auch von Amts wegen tätig werden. Eine sog. regelmäßige Datenübermittlung ist an bestimmte Anlässe gebunden. Rechtsgrundlage ist § 36 Abs. 1 BMG; Einzelheiten sind – auf Grund der Ermächtigungen in § 55 Abs. 5 BMG und Art. 11 Nr. 4 BayGMPP – in der (bayerischen) Meldedatenverordnung (MeldDV) festgelegt.

§ 23 Abs. 1 Satz 1 MeldDV bestimmt insofern konkretisierend, dass der Landesrundfunkanstalt/dem Beitragsservice bei der Anmeldung, der Abmeldung oder einem Todesfall folgende Daten volljähriger Einwohner übermittelt werden können:

- der Familienname,
- Vornamen,
- ein Doktorgrad,
- das Geburtsdatum,
- die derzeitige und die letzte frühere Anschrift,
- Einzugsdatum und Auszugsdatum beziehungsweise
- das Datum der Anmeldung oder Abmeldung von Amts wegen, ferner
- das Sterbedatum.

Die Übermittlung unterbleibt nach § 23 Abs. 1 Satz 2 MeldDV, wenn eine Auskunftssperre nach § 51 BMG eingetragen ist (etwa zum Schutz vor einem gewalttätigen früheren Partner oder aus beruflichen Gründen).

Die Formulierung von § 23 Abs. 1 Satz 1 MeldDV deutet darauf hin, dass die regelmäßigen Datenübermittlungen an die Landesrundfunkanstalt/den Beitragsservice im Ermessen der Meldebehörden stehen („kann"). Dies dürfte auch nicht als ein „Versehen" des Verordnungsgebers zu werten sein.[92] Das frühere bayerische Melderecht kannte grundsätzlich einen Unterschied zwischen pflichtigen und nicht pflichtigen regelmäßigen Datenübermittlungen.[93] Die Übermittlungen an den Rundfunk waren bereits vor Inkrafttreten des Bundesmeldegesetzes als nicht pflichtig ausgestaltet.[94] Dass der Verordnungsgeber mit § 23 Abs. 1 Satz 1 MeldDV diese „Traditionslinie" fortgeführt hat, ist nicht fernliegend – zumal die bundesrechtliche Ermächtigung hinsichtlich einer Verpflichtung der Meldebehörden zu regelmäßigen Datenübermittlungen indifferent formuliert ist (§ 36 Abs. 1 BMG: „Datenübermittlungen […] sind zulässig"), landesrechtliche Regelungen ohne Verpflichtungswirkung also nicht ausschließt.

Daraus sollte allerdings nicht gefolgert werden, dass die Meldebehörde der Landesrundfunkanstalt/dem Beitragsservice nach Belieben „den Datenhahn zudrehen" kann. Die im Rahmen des Ermessens anzustellende Abwägung von Zugangs- und Vertraulichkeitsinteresse dürfte grundsätzlich zugunsten des Zugangsinteresses ausfallen. Der öffentlich-rechtliche Rundfunk stellt Leistungen bereit, die von jedermann jederzeit in Anspruch genommen werden können, ohne dass dies im Einzelfall mit einem realistischen Aufwand nachzuweisen ist. Daher wird das Interesse, sich (dennoch) vor einer Erfassung als Beitragspflichtiger zu „verstecken", regelmäßig als kaum schutzwürdig erscheinen.[95]

Nicht geklärt ist, ob eine Meldebehörde das Ermessen dafür nutzen kann, über den Fall von § 23 Abs. 1 Satz 2 MeldDV weitere Konstellationen von einer Übermittlung auszunehmen. In Betracht kämen insofern etwa Fälle einer beantragten, aber

92 In diese Richtung aber Ehmann, Blockade von Datenübermittlungen an den „Beitragsservice"?, Stand 2/2025, unter Nr. 6.

93 Siehe Art. 28 Abs. 5 Satz 4 Meldegesetz in der bis zum 31. Oktober 2015 geltenden Fassung: „Das Staatsministerium wird ermächtigt, durch Verordnung die regelmäßige Datenübermittlung der in […] genannten Daten zuzulassen und vorzuschreiben". Die Vorschrift entspricht der Vorgängerregelung des Art. 31 Abs. 5 Satz 1 Meldegesetz in der bis zum 14. Dezember 2006 geltenden Fassung. Die Gesetzesbegründung hierzu stellt die Verpflichtung der Meldebehörden als Option dar, Landtags-Drucksache 10/164, S. 26 (linke Spalte unten).

94 § 31 Abs. 1 Meldedatenverordnung in der bis zum 31. Oktober 2015 geltenden Fassung; zuvor § 12a Abs. 1 Bayerische Meldedaten-Übermittlungsverordnung in der bis zum 30. Juni 2007 geltenden Fassung.

95 So auch Ehmann (Fn. 92).

noch nicht eingerichteten oder einer ausgelaufenen und voraussichtlich zu erneuernden Auskunftssperre.

Das eingeräumte Ermessen dürfte der Meldebehörde im Übrigen eine „Schrumpfung" des übermittelten Datensatzes gestatten, etwa die Übermittlung nur der Rufnamen anstatt aller Vornamen.

6.4.2.3 Periodischer Datenabgleich mit den Melderegistern

Über diese regelmäßigen Datenübermittlungen hinaus ist zusätzlich noch ein periodischer Datenabgleich mit den Melderegistern vorgesehen. Dabei handelt es sich ebenfalls um eine regelmäßige Datenübermittlung nach § 36 Abs. 1, § 55 Abs. 5 BMG.[96] Die Einzelheiten sind hier in § 11 Abs. 5 Satz 1 RBeitrStV geregelt, der im Rang eines bayerischen Parlamentsgesetzes steht.[97] Mit dem periodischen Datenabgleich soll die Aktualität des Datenbestands bei der Landesrundfunkanstalt zusätzlich abgesichert werden – gerade auch, was beitragspflichtig gewordene Personen betrifft. Der periodische Datenabgleich wird alle vier Jahre durchgeführt, beginnend im Jahr 2022. Ob die aktuelle Regelung mit dem Grundgesetz vereinbar ist, hat das Bundesverfassungsgericht noch nicht entschieden;[98] der Bayerische Verfassungsgerichtshof hat jedenfalls eine vergleichbare Vorgängerregelung als vereinbar mit dem Grundrecht auf informationelle Selbstbestimmung (der Verfassung des Freistaates Bayern) angesehen.[99]

In Rahmen des periodischen Datenabgleichs übermittelt jede Meldebehörde obligatorisch an einem bundesweit einheitlichen Stichtag gegen Kostenerstattung von allen volljährigen Personen an die zuständige Landesrundfunkanstalt:

- den Familiennamen,
- Vornamen unter Bezeichnung des Rufnamens,
- frühere Namen,
- einen Doktorgrad,
- den Familienstand,
- den Tag der Geburt,
- die gegenwärtige und die letzte Anschrift von Haupt- und Nebenwohnungen, einschließlich aller vorhandenen Angaben zur Lage der Wohnung, und
- den Tag des Einzugs in die Wohnung.

96 Ehmann (Fn. 92), unter Nr. 5.

97 Zur Transformation von Staatsverträgen in das Landesrecht näher Möstl, in: Lindner/Möstl/Wolff, Verfassung des Freistaates Bayern, 2. Aufl. 2017, Art. 72 Rn. 5, 13.

98 Vgl. dazu Bundesverfassungsgericht, Beschluss vom 21. Januar 2022, 1 BvR 1296/21, BeckRS 2022, 6838, Rn. 15 f.

99 Bayerischer Verfassungsgerichtshof, Entscheidung vom 20. November 2018, Vf. 1-VII-18, BeckRS 2018, 29768, Rn. 18 ff.; siehe auch Verfassungsgerichtshof des Landes Berlin, Beschluss vom 19. Juni 2020, VerfGH 185/17, BeckRS 2020, 47443, Rn. 28 ff. für das Datenschutzgrundrecht der Verfassung von Berlin.

6.4.3 Grundsätzlich kein Widerspruch möglich

Das Melderecht sieht für Datenübermittlungen aus den Melderegistern an die Landesrundfunkanstalt/den Beitragsservice kein eigenständiges Widerspruchsrecht vor; das Widerspruchsrecht für Übermittlungen etwa an Parteien zur Wahlwerbung oder an Adressbuchverlage hilft hier nicht weiter.

Demgegenüber ist das allgemeine Widerspruchsrecht aus Art. 21 Abs. 1 DSGVO für die Meldedatenübermittlung im Einzelfall (§ 34 Abs. 1 BMG) sowie anlässlich der Anmeldung (§ 36 Abs. 1 BMG, § 23 Abs. 1 Satz 1 MeldDV) nicht von vornherein ausgeschlossen. Dafür wäre nämlich eine strikte Verpflichtung der Meldebehörden erforderlich, an der es gerade fehlt. Das Widerspruchsrecht nach Art. 21 Abs. 1 DSGVO ist allerdings nicht voraussetzungslos. Für einen auf diese Vorschrift gestützten Widerspruch bei der Meldebehörde müsste die betroffene Person konkrete Gründe vortragen, die sich aus ihrer besonderen Situation ergeben (Art. 21 Abs. 1 Satz 1 Halbsatz 1 DSGVO), sie also aus dem Kreis der übrigen Rundfunkbetragspflichtigen herausheben. Eine solche besondere Situation dürfte in Bezug auf die in Rede stehende Datenübermittlung aber regelmäßig nicht zu begründen sein. In Betracht kämen dafür wohl am ehesten Situationen, in denen eine Auskunftssperre nach § 51 BMG zu erwarten ist, insbesondere, wenn diese ihren Grund im außerdienstlichen Verhalten eines Beschäftigten der Landesrundfunkanstalt oder des Beitragsservice haben.

Auf den periodischen Datenabgleich nach § 36 Abs. 1 BMG, § 11 Abs. 5 Satz 1 RBeitrStV ist das Widerspruchsrecht aus Art. 21 Abs. 1 DSGVO nicht anwendbar, weil hier eine Verpflichtung der Meldebehörde im Sinn von Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO vorliegt.

6.4.4 Keine Einwilligung erforderlich

In den erläuterten Fällen des Datentransfers von der Meldebehörde zur Landesrundfunkanstalt/zum Beitragsservice vermitteln die Verarbeitungsbefugnisse jeweils eine Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO, im Fall des periodischen Datenabgleichs eine Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO. Sind die Voraussetzungen der jeweiligen Rechtsgrundlage erfüllt und ist ein eingeräumtes Ermessen ordnungsgemäß ausgeübt, hat eine darauf gestützte Datenverarbeitung eine ausreichende Rechtsgrundlage. Eine Einwilligung der betroffenen Person als (weitere) Rechtsgrundlage wird dann nicht benötigt.

6.4.5 Zweckbindungen

Für die Meldedaten, welche die Landesrundfunkanstalt/den Beitragsservice erreichen, ist in § 11 Abs. 7 Satz 1 RBeitrStV eine erfreulich klare Zweckbindung vorgesehen. Diese Zweckbindung schließt insbesondere Zweckänderungen nach Art. 6 Abs. 2 BayDSG aus. Nicht zulässig sind vor allem eine Weiterübermittlung an andere öffentliche Stellen, ebenso eine Nutzung zu eigenen journalistischen oder kommerziellen Zwecken, namentlich in Form des Adressverkaufs.[100]

[100] Vgl. Herb, in: Binder/Vesting, Beck'scher Kommentar zum Rundfunkrecht, 5. Aufl. 2024,

6.4.6 Schadensersatz

Nach Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen die Datenschutz-Grundverordnung ein materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Halten sich die Meldebehörden sowie die Landesrundfunkanstalt/der Beitragsservice an die dargestellten Vorgaben, bestehen für Schadensersatzansprüche betroffener Personen insofern schon in Ermangelung eines Datenschutzverstoßes grundsätzlich keine Anknüpfungspunkte.

§ 11 RBeitrStV Rn. 66 ff.

7 Gesundheitsverwaltung

Meine Datenschutzaufsicht erfasst im Gesundheitsbereich zunächst die Gesundheitsbehörden, vom Bayerischen Staatsministerium für Gesundheit, Pflege und Prävention bis zu den hergebracht als Gesundheitsämtern bezeichneten Organisationseinheiten der Landratsämter sowie einiger kreisfreier Städte.

Einen Schwerpunkt von Beschwerden und Beratungsanfragen bildeten hier Verarbeitungen im Kontext „Masernimpfschutz". Über das Berichtsjahr habe ich hier viele neue Prüfungserkenntnisse gewonnen. Diese Erkenntnisse konnte ich sukzessive in eine Publikation einfließen lassen, die ich voraussichtlich 2026 bereitstellen werde. Das Thema bleibt in diesem Tätigkeitsbericht daher ausgespart.

Ich möchte stattdessen zwei Fragen ansprechen, die in der Arbeit der Gesundheitsämter immer wieder auftauchen: Wie nämlich mit personenbezogenen Hinweisen aus der Bevölkerung umzugehen ist, die Anlass zur Unterbreitung freiwilliger Beratungsangebote geben, etwa bei Anhaltspunkten für ein Suchtmittelproblem (Nr. 7.1), und welche datenschutzrechtlichen Anforderungen zu beachten sind, wenn in Dienstfähigkeitsbeurteilungen von Beamtinnen und Beamten Zusatzgutachter eingebunden werden soll (Nr. 7.2).

7.1 Datenschutz im Zusammenhang mit freiwilligen Beratungsangeboten der Gesundheitsämter

Eine Beratungsanfrage aus einem bayerischen Landratsamt nahm Datenverarbeitungen zur Unterbreitung von freiwilligen Beratungsangeboten nach Art. 7 Abs. 2 Gesundheitsdienstgesetz in den Blick. In dieser Vorschrift heißt es auszugsweise:

> „[1]Die Gesundheitsämter klären die Bevölkerung in Fragen der Gesundheit in körperlicher, psychischer und sozialer Hinsicht auf und beraten über Gesunderhaltung und Krankheitsverhütung. [2][…] [3]Auf den Gebieten der Gesundheitsvorsorge und der Gesundheitshilfe bieten sie insbesondere folgende Dienste an:
> 1. […]
> 2. gesundheitliche Beratung für Menschen, die an einer Sucht, an einer psychischen Krankheit, einer chronischen Krankheit oder an einer Behinderung leiden, von ihr bedroht oder dadurch gefährdet sind, über Personen, Einrichtungen und Stellen, die vorsorgende, begleitende und nachsorgende Hilfen gewähren können."

In der Praxis erhielten die Gesundheitsämter oftmals von Angehörigen oder Vermietern Hinweise, dass eine betroffene Person abhängig machende Substanzen in einem problematischen Umfang konsumiere. Für den öffentlichen Gesundheitsdienst stelle sich dann die Frage, ob und wie die so erlangten Kontaktdaten genutzt werden dürfen, an die betroffene Person heranzutreten, um konkrete Hilfsangebote zu unterbreiten. Beschwerden bei mir zeigen, dass ein solches Herantreten mitunter als übergriffig wahrgenommen wird.

Ich habe dem Landratsamt zum datenschutzrechtlichen Handlungsrahmen im Wesentlichen unter anderem folgende Hinweise gegeben:

Wenn aufgrund eines Hinweises ein freiwilliges Beratungsangebot unterbreitet werden soll, werden personenbezogene Daten der betroffenen Person verarbeitet. Dafür ist eine Rechtsgrundlage erforderlich (Art. 6 Abs. 1 UAbs. 1 DSGVO). Die Verarbeitung hat Kontaktdaten (Name, Adresse) zum Gegenstand, wird sich meist aber auch auf spezifische Gesundheitsinformationen beziehen. Dies gilt insbesondere dann, wenn Informationen zu einem möglichen Missbrauch von Suchtmitteln gespeichert und für die Auswahl des Beratungsangebots genutzt werden. Insofern ist der Anwendungsbereich von Art. 9 DSGVO eröffnet.

Da das Gesundheitsdienstgesetz selbst keine passenden spezialgesetzlichen Verarbeitungsbefugnisse bereithält und auch keine sonstigen bereichsspezifischen Datenschutzvorschriften ersichtlich sind, können als Verarbeitungsbefugnisse nur die allgemeinen Vorschriften des Bayerischen Datenschutzgesetzes herangezogen werden.

Betrifft die Speicherung beziehungsweise Verwendung der personenbezogenen Daten Gesundheitsdaten im Sinne des Art. 9 Abs. 1 DSGVO, ist zuvorderst Art. 8 Abs. 1 Satz 1 Nr. 3 BayDSG zu berücksichtigen. Danach ist eine Verarbeitung von Daten im Sinne des Art. 9 Abs. 1 DSGVO unter anderem zulässig, soweit sie zum Zweck der Gesundheitsvorsorge, der Versorgung oder Behandlung im Gesundheits- oder Sozialbereich erforderlich ist, wenn diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden.

Nachdem Art. 8 Abs. 1 Satz 1 Nr. 3 BayDSG nur die gesteigerten Anforderungen des Art. 9 Abs. 2 DSGVO abbildet, muss die Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 DSGVO der „Generalklausel" des Art. 4 Abs. 1 BayDSG entnommen werden. Diese Bestimmung sieht vor, dass eine Verarbeitung personenbezogener Daten durch eine öffentliche Stelle unbeschadet sonstiger Bestimmungen zulässig ist, „wenn sie zur Erfüllung einer ihr obliegenden Aufgabe erforderlich ist." Eine entsprechende Aufgabenzuweisung für die Gesundheitsämter ergibt sich dabei aus meiner Sicht aus Art. 7 Abs. 2 Satz 3 Nr. 2 GDG. Ob eine Speicherung beziehungsweise Verwendung der Daten auch jeweils „erforderlich" (Art. 8 Abs. 1 Satz 1 Nr. 3 und Art. 4 Abs. 1 BayDSG) ist, müssen die Gesundheitsämter im Einzelfall sorgfältig prüfen. Im Streitfall müssen sie (auch) hierüber Rechenschaft ablegen können.

Sofern keine Gesundheitsdaten verarbeitet werden, stellt Art. 4 Abs. 1 BayDSG die Rechtsgrundlage für eine Datenverarbeitung allein.

Hinzuweisen ist in diesem Zusammenhang auch auf die besonderen Vorgaben aus Art. 27 GDG. Insbesondere sieht Art. 27 Abs. 1 GDG vor, dass die Gesundheitsämter Geheimnisse, die Amtsangehörigen in der Eigenschaft als Arzt oder als andere gemäß § 203 Abs. 1 oder 3 Strafgesetzbuch zur Wahrung des Berufsgeheimnisses verpflichtete Person in Wahrnehmung der unter anderem in Art. 7 GDG genannten Aufgaben anvertraut oder sonst bekannt geworden sind, bei der Erfüllung einer anderen Aufgabe als der, bei deren Wahrnehmung die Erkenntnisse gewonnen wurden, nicht verarbeiten dürfen (Art. 27 Abs. 1 Satz 1 Nr. 1 GDG). Mit Art. 27 Abs. 1 Satz 1 GDG wird ein strenger Zweckbindungsgrundsatz für die erfassten Geheimnisse etabliert. Damit soll ausgeschlossen werden, dass

Daten, die dem besonderen Geheimnisschutz unterliegen, für „materiell andersartige Aufgaben“ verarbeitet werden.[101] Sofern also aufgrund eines Hinweises Daten bekannt werden, die dem besonderen Geheimnisschutz nach Art. 27 Abs. 1 GDG unterliegen, dürfen diese nur für die Erfüllung eben derjenigen Aufgabe verarbeitet werden, bei deren Wahrnehmung die Erkenntnisse gewonnen wurden. Das Angebot freiwilliger Beratungen nach Art. 7 Abs. 2 Satz 3 Nr. 2 GDG stellt eine solche Aufgabe der Gesundheitsämter dar. Sofern sich die Verarbeitung beziehungsweise Verwendung der Daten daher im Rahmen dieser Aufgabe bewegt, steht Art. 27 Abs. 1 GDG einer solchen Verarbeitung nicht entgegen.

Im Ergebnis hindert das Datenschutzrecht nicht, dass bayerische Gesundheitsämter Hinweise aus der Bevölkerung nutzen, um betroffenen Personen freiwillige Beratungsangebote zu unterbreiten. Zur Erfüllung der Rechenschaftspflicht des Verantwortlichen sollte aber darauf geachtet werden, dass eine an den gesetzlichen Vorgaben für einschlägige Datenverarbeitungen ausgerichtete Prüfroutine eingehalten wird.

7.2 Datenübermittlung an einen externen Gutachter bei Beurteilung der Dienstfähigkeit

Im Rahmen eines Beschwerdeverfahrens hatte ich die datenschutzrechtliche Zulässigkeit der Einbindung eines externen Gutachters bei Beurteilung der Dienstfähigkeit eines bayerischen Beamten zu überprüfen. Der Fall ist schnell zusammengefasst: Der Beamter sollte von der Medizinischen Untersuchungsstelle (MUS) einer Regierung im Hinblick auf seine Dienstfähigkeit amtsärztlich begutachtet werden. Die MUS stieß fachlich an Grenzen und sah sich veranlasst, einen externen Sachverständigen mit einer ergänzenden Begutachtung zu beauftragen. In der Folge übermittelte sie einschlägige Unterlagen an diesen Sachverständigen; dabei lag keine Einwilligung des Beamten vor. Der Beamte hielt dies für rechtswidrig und wandte sich mit einer Beschwerde an mich.

7.2.1 Verpflichtung zur Dienstfähigkeits(zusatz)begutachtung

Bei Zweifeln über die Dienstunfähigkeit sind Beamtinnen und Beamte verpflichtet, sich nach Weisung ihrer Dienstvorgesetzten ärztlich untersuchen zu lassen (Art. 65 Abs. 2 Satz 1 Bayerisches Beamtengesetz – BayBG). Zuständig für Dienstfähigkeitsbegutachtungen sind gemäß Art. 5 Satz 1 in Verbindung mit Art. 8 Gesundheitsdienstgesetz (GDG) grundsätzlich die Regierungen in ihrer Funktion als höhere Gesundheitsbehörden. Betroffene Beamtinnen und Beamte haben sich auf Verlangen des Amtsarztes oder der Amtsärztin der jeweiligen MUS gegebenenfalls ergänzend einer fachärztlichen Zusatzbegutachtung zu unterziehen (vgl. Art. 65 Abs. 2 Satz 2 BayBG). Das erstellte Zusatzgutachten soll die fachliche Expertise von Amtsärztinnen und Amtsärzten im erforderlichen Umfang ergänzen; es ist damit vom Gutachtensauftrag durch die Dienstvorgesetzten der betroffenen Personen umfasst und dient zur Erfüllung dieses Auftrags (vgl. Abschnitt 8 Nr. 1.5. Verwaltungsvorschriften zum Beamtenrecht – VV-BeamtR).

[101] Gesetzentwurf der Staatsregierung, Landtags-Drucksache 10/8972, S. 14.

7.2.2 Zulässigkeit der Datenübermittlung an externe Zusatzgutachter: Ausgangslage

Um ein Zusatzgutachten einholen zu können, muss die zuständige MUS die dafür nötigen personenbezogene Daten des oder der betroffenen Bediensteten an den externen Zusatzgutachter übermitteln können. Eine entsprechende Übermittlungsbefugnis ergibt sich regelmäßig aus Art. 5 Abs. 1 Satz 1 Nr. 1 Var. 1 in Verbindung mit Art. 8 Abs. 1 Satz 1 Nr. 2 und 3 BayDSG. Hiernach darf eine bayerische öffentliche Stelle personenbezogene Daten an andere – auch nicht öffentliche – Stellen übermitteln, soweit dies für die Aufgabenerfüllung der übermittelnden Stelle – vorliegend zur Durchführung einer Begutachtung nach Art. 65 Abs. 2 BayBG in Verbindung mit Art. 5 und 8 GDG – erforderlich ist. In diesem Rahmen ist auch eine Übermittlung von Gesundheitsdaten – und damit von besonderen Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO – zulässig, soweit die Übermittlung zur Wahrnehmung von Rechten und Pflichten der öffentlichen Stellen auf dem Gebiet des Dienst- und Arbeitsrechts sowie zur Beurteilung der Dienst- und Arbeitsfähigkeit erforderlich ist (Art. 8 Abs. 1 Satz 1 Nr. 2 und 3 BayDSG). Dabei ist der eingriffsmildernde Umstand zu berücksichtigen, dass der Datenempfänger ebenfalls der ärztlichen Schweigepflicht unterliegt, die übermittelten Daten daher in der „Sphäre“ von Berufsgeheimnisträgern verbleiben.

7.2.3 Einschränkung durch Art. 27 GDG

Auch wenn eine Rechtsgrundlage für die fragliche Datenübermittlung vorhanden ist, müsste diese gleichwohl unterbleiben, wenn die Daten nach Art. 27 Gesundheitsdienstgesetz (GDG) geheim zu halten sind. Die Erkenntnisse aus Begutachtungen der Dienstfähigkeit unterliegen grundsätzlich dem Anwendungsbereich von Art. 27 Abs. 1 Satz 1 Nr. 2, Satz 3 GDG und sind insoweit auch von der besonderen Geheimhaltungspflicht der Gesundheitsbehörden erfasst.

Die Weitergabe der fraglichen Daten zum Zwecke der Einholung eines Zusatzgutachtens ist nach meinem Verständnis jedoch regelmäßig nach Art. 27 Abs. 2 GDG von dem Weiterverarbeitungs- und Übermittlungsverbot des Art. 27 Abs. 1 GDG ausgenommen. Denn die gegenständliche Datenübermittlung erfolgt aufgrund einer gesetzlichen Verarbeitungsbefugnis zur Erfüllung der im Art. 65 Abs. 2 BayBG gesetzlich speziell normierten Aufgabe der Gesundheitsbehörde, in bestimmten Fällen, nämlich bei der Bewertung der Dienstfähigkeit, Zusatzbegutachtungen durchzuführen (Art. 27 Abs. 2 Satz 1 Nr. 1 GDG). Daneben ist auch Art. 27 Abs. 2 Satz 4 GDG zu beachten, der eine Offenbarung an die in § 203 Abs. 3 Strafgesetzbuch (StGB) genannten Personen unter bestimmten Voraussetzungen für zulässig erklärt, soweit insbesondere die Wahrung des Berufsgeheimnisses gewährleistet ist. Da der externe Gutachter als „sonstige mitwirkende Person“ im Sinne des § 203 Abs. 3 Satz 2 StGB bewertet werden kann und die übermittelten Daten vorliegend die „Sphäre“ von Berufsgeheimnisträgern nicht verlassen, dürfte auch die Ausnahme des Art. 27 Abs. 2 Satz 4 GDG eingreifen.

7.2.4 Ergebnis im Beschwerdefall

Im vorliegenden Fall kam ich daher zu dem Ergebnis, dass die MUS die erforderlichen Daten auch ohne Einwilligung des Beamten an den Zusatzgutachter übermitteln durfte. Die Datenübermittlung konnte auf eine gesetzliche Verarbeitungsbefugnis gestützt werden.

8 Öffentliche Krankenhäuser

Meine Zuständigkeit als Datenschutzaufsichtsbehörde erstreckt sich unter anderem auf sechs Universitätskliniken sowie gut 200 Krankenhäusern kommunaler Träger, die gemeinsam gut 70 Prozent der aufgestellten Klinikbetten vorhalten. Vor diesem Hintergrund wird es nicht überraschen, dass täglich Beschwerden, Beratungsanfragen oder Datenpannen-Meldungen aus diesem Bereich bei mir eingehen. Was Beschwerden und Beratungsanfragen betrifft, bildet der Zugang zur Patientenakte einen Schwerpunkt. Thematisiert werden jedoch auch vielfältige Verarbeitungen von Patientendaten. Bei den Datenpannen-Meldungen mögen Cyberangriffe in der öffentlichen Wahrnehmung einen prominenten Rang einnehmen (siehe dazu Nr. 14.7.1), weit höhere Fallzahlen erreichen gleichwohl Alltagspannen wie etwa der Fehlversand von Arztbriefen (dazu etwa mein 28. Tätigkeitsbericht 2018 unter Nr. 3.2.2).

Im Folgenden möchte ich auf einige aus meiner Sicht durchaus spannende Vorgänge eingehen. Eine ganz grundsätzliche Frage betraf das rechtliche „Schicksal" eines Bestands von Gesundheitsdaten bei der Umgliederung eines Instituts von einer bayerischen Universität an ihr Klinikum (Nr. 8.1). Im Krankenhausalltag spielen Fälle zu Aufbewahrung und Löschung von Patientendaten (Nr. 8.2), zur „Korrektur" von Arztbriefen (Nr. 8.3) sowie zum Auskunftsmittel „CD-ROM" (Nr. 8.4). Umfassend betrachtet habe ich den Einsatz von Videoüberwachungsanlagen in psychiatrischen Kliniken der öffentlichen Hand (Nr. 8.5).

8.1 Zuordnung einer wissenschaftlichen Einrichtung einer Universität zu einem Universitätsklinikum und Übertragung der Institutsdaten

Ein grundsätzliches Problem, für das auch keine Präzendenzfälle zur Verfügung standen, ergab sich, als sich ein Universitätsklinikum wegen datenschutzrechtlicher Fragen im Zusammenhang mit einer Umorganisation an mich wandte. Dabei ging es um die Zuordnung eines Instituts von einer bayerischen Universität zum anfragenden Klinikum. Das Klinikum vertrat dabei den Standpunkt, dass eine solche Zuordnung von Einrichtungen sowie die damit notwendig werdende Übertragung der Institutsdaten, die im konkreten Fall Gesundheitsdaten und genetische Daten umfassten, datenschutzrechtlich „neutral" sei und daher keiner besonderen Rechtsgrundlage bedürfe.

8.1.1 Zuordnung von Einrichtungen zu einem Universitätsklinikum

Die bayerischen Universitätsklinika wurden zum 1. Juni 2006 als Anstalten des öffentlichen Rechts neu errichtet. Die originäre Zuordnung von Einrichtungen zu den Universitätsklinika vollzog sich gemäß Art. 1 Abs. 2 Bayerisches Universitätsklinikagesetz (BayUniKlinG) in der Fassung vom 23. Mai 2006[102] im Wege einer Gesamtrechtsnachfolge. Konkret sah die gesetzliche Regelung vor, dass die neu errichteten Universitätsklinika in die Rechte und Pflichten der bisherigen Staatsbetriebe eintreten, und dass die Rechte und Pflichten des Freistaates Bayern und

[102] GVBl. S. 285.

der jeweiligen Universität sowie die Zuständigkeiten auf das Klinikum übergehen sollten (Art. 1 Abs. 2 Satz 1 und 2 BayUniKlinG a. F.).

Art. 1 Abs. 2 BayUniKlinG in seiner aktuell geltenden Fassung sieht demgegenüber vor, dass das Bayerische Staatsministerium für Wissenschaft und Kunst über die Zuordnung von Einrichtungen zu einem Universitätsklinikum durch Verwaltungsakt entscheidet. Die ausdrückliche gesetzliche Anordnung einer Gesamtrechtsnachfolge bei der Zuordnung von Einrichtungen war durch das Änderungsgesetz vom 9. Juli 2012[103] entfallen. Auch in Anbetracht dieser Änderung der Rechtslage war das Universitätsklinikum weiterhin der Auffassung, dass in der Sache noch immer eine Gesamtrechtsnachfolge anzunehmen sei. Das zuständige Staatsministerium hatte gegen diese Haltung des Universitätsklinikums keine Einwände und war dazu bereit, einen entsprechenden Verwaltungsakt zu erlassen.

8.1.2 Übertragung der Institutsdaten als rechtfertigungsbedürftige Übermittlung von personenbezogenen Daten?

Ich bin unabhängig von der Antwort auf die Frage des Vorliegens einer Gesamtrechtsnachfolge zu der Einschätzung gelangt, dass in der vom Universitätsklinikum geschilderten Fallkonstellation kein Verarbeitungsvorgang im Sinne des Art. 4 Nr. 2 DSGVO vorliegt, der einer Rechtsgrundlage im Sinne des Art. 6 Abs. 1 DSGVO bedarf. Dafür waren folgende Überlegungen maßgeblich:

8.1.2.1 Verarbeitungsbegriff der Datenschutz-Grundverordnung

Der datenschutzrechtliche Begriff der Verarbeitung umfasst nach seiner abstrakten Definition „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten“ (Art. 4 Nr. 2 DSGVO). Die Vorschrift erwähnt hierzu beispielhaft eine Reihe von typischerweise anzutreffenden Verarbeitungsvorgängen. Insbesondere fällt unter den Begriff der Verarbeitung auch die „Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung“. Werden personenbezogene Daten verarbeitet (also zum Beispiel offengelegt), muss dies nach Art. 6 Abs. 1 DSGVO auf eine taugliche Rechtsgrundlage gestützt werden können. Sind davon auch besonders sensible Daten wie etwa Gesundheitsdaten oder genetische Daten umfasst, sind zusätzlich auch die Anforderungen des Art. 9 Abs. 2 DSGVO zu beachten.

Eine Offenlegung in diesem Sinne erfasst grundsätzlich alle Fälle, in denen personenbezogene Daten anderen Stellen derart zugänglich gemacht werden, dass diese Kenntnis vom Informationsgehalt der Daten nehmen können. Dabei ist es – anders als beim Übermittlungsbegriff des früheren Bundesdatenschutzgesetzes – nicht erforderlich, dass die andere Stelle ein „Dritter“ im Sinne von Art. 4 Nr. 10 DSGVO ist.[104] Es reicht aus, wenn die Daten an einen „Empfänger“ nach Art. 4 Nr. 9 DSGVO offengelegt werden. Eine Übermittlung lässt sich dementspre-

[103] GVBl. S. 339; siehe dazu auch Landtags-Drucksache 16/11984.

[104] Vgl. etwa Bundesarbeitsgericht, Beschluss vom 9. April 2019, 1 ABR 51/17, BeckRS 2019, 14744, Rn. 32.

chend – einen Unterfall der Offenlegung bildend – als gezielte Weitergabe von Daten an einen Empfänger verstehen.[105] Das spezifische Datenschutzrisiko einer Offenlegung beziehungsweise einer Übermittlung liegt darin, dass sich die Zahl der Stellen, die Kenntnis von den Daten haben, verdoppelt oder gar vervielfacht.

Nach dem sogenannten Doppeltürmodell[106] stellt eine Übermittlung von Daten auf Seiten des Empfängers in der Regel eine (weitere) Datenverarbeitung in Gestalt einer Erhebung dar, die grundsätzlich ebenfalls auf eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO und gegebenenfalls nach Art. 9 Abs. 2 DSGVO gestützt werden muss.

Auf den ersten Blick erschien es daher durchaus naheliegend, auch in der vom Universitätsklinikum geschilderten Fallkonstellation der Zuordnung eines Instituts, welche mit der Übertragung des entsprechenden Datenbestands einhergeht, von einer rechtfertigungsbedürftigen Datenverarbeitung in Gestalt einer Übermittlung (sowie und einer korrespondierenden Datenerhebung) auszugehen.

8.1.2.2 Besondere Fallkonstellationen, in denen das Vorliegen einer „Verarbeitung“ verneint werden kann

Allerdings gibt es einige Fallkonstellationen, in denen das Vorliegen einer Verarbeitung aufgrund der besonderen Umstände zu verneinen ist.

Dies gilt etwa nach ganz überwiegender Meinung im Hinblick auf Unternehmenstransaktionen im Fall eines sogenannten **Share Deals**, bei dem die Anteile an einer Gesellschaft auf den Erwerber übergehen. Dabei findet keine Übermittlung und auch keine anderweitige Datenverarbeitung im Sinne des Art. 4 Nr. 2 DSGVO statt, da nur die Anteile an einer Gesellschaft übertragen werden, diese ansonsten jedoch unverändert fortgeführt wird und keine Änderung in der Person des Verantwortlichen erreicht wird.[107]

Ebenso wird in den Fällen einer **Gesamtrechtsnachfolge** (beispielsweise im Fall einer Erbfolge oder einer Verschmelzung, Auf-/Abspaltung beziehungsweise einer Ausgliederung im Sinne des Umwandlungsrechts) ganz überwiegend angenommen, dass keine Übermittlung und auch keine andere Form der Datenverarbeitung im Sinne des Art. 4 Nr. 2 DSGVO vorliegt. Die gespeicherten personenbezogenen Daten gehen in diesem Fall auf den Gesamtrechtsnachfolger über, der vollkommen in die Stellung seines Rechtsvorgängers eintritt.[108]

[105] Vgl. etwa Bundesarbeitsgericht, Beschluss vom 9. April 2019, 1 ABR 51/17, BeckRS 2019, 14744, Rn. 32.

[106] Siehe Bundesverfassungsgericht, Beschluss vom 24. Januar 2012, 1 BvR 1299/05, BeckRS 2012, 47556, Rn. 123, und Beschluss vom 27. Mai 2020, 1 BvR 1873/13, 1 BvR 2618/13, BeckRS 2020, 16236, Rn. 93, 201; Bayerisches Oberstes Landesgericht, Beschluss vom 6. Dezember 2024, 101 VA 129/24, BeckRS 2024, 34857, Rn. 23.

[107] Vgl. etwa Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Übermittlungen personenbezogener Daten an die Erwerberin oder den Erwerber eines Unternehmens im Rahmen eines Asset-Deals, Beschluss vom 11. September 2024, S. 1, Internet: https://www.datenschutzkonferenz-online.de, Rubrik „Beschlüsse“.

[108] Vgl. etwa Bundesverwaltungsgericht (Österreich), Erkenntnis vom 22. August 2023, W137 2251172-1/16E, BeckRS 2023, 25880, Rn. 70.

Diesen Ausnahmefällen ist aus meiner Sicht gemeinsam, dass personenbezogene Daten, die sich im Gewahrsam einer Organisationseinheit befinden, mit dieser Organisationseinheit auf einen neuen „Eigentümer“ übergehen, der die Organisationseinheit ansonsten unverändert übernimmt (sei es dadurch, dass die Anteile übertragen werden, im Übrigen aber die Organisationseinheit als eigene verantwortliche Stelle unverändert bestehen bleibt – wie im Fall eines „Share Deals“ –, sei es, dass das Vermögen als Gesamtheit auf einen übernehmenden Rechtsträger übergeht, so im Fall der Gesamtrechtsnachfolge). Sofern im Gegenzug der vormalige „Eigentümer“ jegliche Einwirkungsmöglichkeit auf die Daten verliert, entsteht für die betroffenen Personen auch nicht die Gefahr, fortan einer Datenverarbeitung durch mehrere Stellen ausgesetzt zu sein. Im Ergebnis ändern sich damit nur die zugrundeliegenden „Eigentumsverhältnisse“ an der Organisationseinheit. Unter diesen Voraussetzungen kann aus meiner Sicht das Vorliegen einer Übermittlung oder einer anderen Datenverarbeitung im Sinne des Art. 4 Nr. 2 DSGVO verneint werden.

So liegt der Fall auch bei der Zuordnung eines Instituts von einer Universität zum Universitätsklinikum. Durch die Zuordnungsentscheidung gehen das Institut und der entsprechende Datenbestand unverändert auf den neuen „Eigentümer“ in Gestalt des Universitätsklinikums über. Die neue Zuordnung bewirkt, dass der vormalige „Eigentümer“, die Universität, den Zugriff auf die Daten verliert. Im Hinblick das spezifische Datenschutzrisiko einer Offenlegung von personenbezogenen Daten ist diese besondere Konstellation daher mit den anerkannten Fallgruppen, in denen das Vorliegen einer Verarbeitung zu verneinen ist („Share Deals“ und Fälle der Gesamtrechtsnachfolge), vergleichbar.

Vor diesem Hintergrund habe ich gegen die Haltung des Universitätsklinikums jedenfalls im Ergebnis keine Einwände erhoben.

8.1.3 Sonstige datenschutzrechtliche Anforderungen an die Übernahme von Datenbeständen

Gleichwohl habe ich das Universitätsklinikum noch auf einige weitere Maßgaben hinweisen können, die bei der Zuordnung einer Einrichtung zum Universitätsklinikum und der Übertragung der Institutsdaten aus Datenschutzsicht zu beachten sind.

Das Universitätsklinikum übernimmt ab dem Zeitpunkt des Übergangs des vormaligen Instituts der Universität die datenschutzrechtlichen Rechte und Pflichten im Hinblick auf den Datenbestand des Instituts. Ich habe darauf aufmerksam gemacht, dass alle sonstigen datenschutzrechtlichen Vorgaben, die für das Universitätsklinikum gelten (zum Beispiel zur Sicherheit der Verarbeitung nach Art. 32 DSGVO), ab diesem Zeitpunkt dann in gleicher Form auch für den Datenbestand des Instituts gelten.

Dies umfasst insbesondere auch die Frage, ob mit der Neuzuordnung des Instituts eine Ausgliederung der dort genutzten IT-Systeme aus dem Netzwerk der Universität und eine Eingliederung in das medizinische Netz des Universitätsklinikums verbunden sein wird, oder ob die IT-Systeme in Eigenregie vom Institut betrieben werden sollen. Da es sich bei Universität und Universitätsklinikum um unterschiedliche Verantwortliche handelt, müssten bei einem Verbleib in der IT-Infrastruktur der Universität – gegebenenfalls neben rechtlichen Vereinbarungen – zusätzliche

technisch-organisatorische Schutzmaßnahmen ergriffen werden, um zum Beispiel sicherzustellen, dass die Administratoren oder anderes Personal der Universität keinen Zugriff mehr auf die Daten des Instituts nehmen können.

Zudem habe ich darauf hingewiesen, dass insgesamt eine Überprüfung der technischen und organisatorischen Maßnahmen erforderlich erscheint. Zum einen haben Daten des Universitätsklinikums im Anwendungsbereich von Art. 9 DSGVO einen erhöhten Schutzbedarf. Zum anderen unterfällt das Universitätsklinikum als kritische Infrastruktur auch der BSI-Kritis-Verordnung: Die erforderlichen Maßnahmen und Auditierungen müssen zukünftig daher auch auf die Datenbestände und IT-Systeme des Instituts angewandt werden.

8.2 Aufbewahrung und Löschung von Patientenunterlagen in Krankenhäusern

Eine betroffene Person wandte sich mit dem Anliegen an mich, die Löschung ihrer Patientenunterlagen bei einem städtischen Klinikum zu erreichen. Dort war sie vor über zehn Jahren einmal behandelt worden. Die betroffene Person hatte bei dem Klinikum nun einen Antrag auf Löschung (Art. 17 DSGVO) ihrer alten Patientenakte gestellt. Das Klinikum hatte diesen Antrag abgelehnt, allerdings die Verarbeitung eingeschränkt (Art. 18 DSGVO).

Das Klinikum war der Auffassung, dass die unter anderem in § 630f Abs. 3 Bürgerliches Gesetzbuch (BGB) für die Aufbewahrung von Patientenakten vorgesehene Zehnjahresfrist eine reine Mindestaufbewahrungsfrist darstelle. Eine individuelle Festlegung der Aufbewahrungsdauer nach Abschluss der Behandlung oder in festen Zeitabständen komme aus praktischen Gründen nicht in Betracht. Stattdessen würden ambulante Behandlungsakten generell nach zehn Jahren gelöscht, Patientenakten über stationäre Aufenthalte hingegen generell 30 Jahre aufbewahrt. Das Klinikum verwies dazu unter anderem auf den Leitfaden „Aufbewahrungspflichten und -fristen von Dokumenten im Krankenhaus“ der Deutschen Krankenhausgesellschaft (Stand Dezember 2024).[109] In dem konkreten Fall habe die betroffene Person den Auskunftsanspruch erst mit einem größeren zeitlichen Abstand zur Behandlung geltend gemacht, wobei nicht ersichtlich sei, zu welchem Zweck sie diese Auskunft zu verwenden gedenke. Es entstehe ein Ungleichgewicht, wenn die betroffene Person 30 Jahre lang Ansprüche geltend machen könne, das Klinikum aber aufgrund einer Löschung gegebenenfalls einen Beweismittelverlust erleide.

8.2.1 Aufbewahrungsfristen für Patientenunterlagen

Für Patientenunterlagen gilt nach dem ärztlichen Berufsrecht eine Aufbewahrungsfrist von zehn Jahren. § 10 Abs. 3 Berufsordnung für die Ärzte Bayerns sieht dazu vor:

> „Ärztliche Aufzeichnungen sind für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach gesetzlichen Vorschriften eine längere Aufbewahrungspflicht besteht.“

[109] Internet: https://www.dkgev.de/fileadmin/default/Mediapool/Bilder_fuer_Newsletter/Dokumente/DKG-Leitfaden_Aufbewahrungspflichten_-fristen_von_Dokumenten_im_KH_Reinfassung_Anlage1.pdf.

Ebenso besagt § 630f Abs. 3 BGB:

> „Der Behandelnde hat die Patientenakte für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach anderen Vorschriften andere Aufbewahrungsfristen bestehen."

Neben diesen allgemeinen Vorschriften besteht eine Reihe von spezialgesetzlichen Regelungen, wie etwa im Transfusionsrecht (zum Beispiel 15- oder 30-jährige Mindestaufbewahrung nach § 14 Abs. 3 Transfusionsgesetz) oder im Strahlenschutzrecht (zum Beispiel 30-jährige Aufbewahrung nach § 85 Abs. 2 Nr. 1 Strahlenschutzgesetz), welche die Pflicht zur Aufbewahrung gegebenenfalls verlängern können.

Was allen diesen Aufbewahrungsfristen gemeinsam ist: Sie machen keinen Unterschied zwischen Patientenunterlagen, die in Papierform vorliegen, und Patientenunterlagen, die elektronisch geführt werden. Die Fristen gelten daher sowohl für die Aufbewahrung der Papierunterlagen als auch die Speicherung von digitalen Unterlagen.

Im Gegensatz hierzu sieht die Vorschrift des § 199 Abs. 2 BGB, auf welche das Klinikum im Ausgangsfall insbesondere Bezug genommen hat, selbst keine Aufbewahrungsfrist vor. Stattdessen legt sie für bestimmte Konstellationen von Schadensersatzansprüchen (nämlich solche, die auf der Verletzung des Lebens, des Körpers, der Gesundheit oder der Freiheit beruhen) eine Verjährungshöchstfrist fest. Dies bedeutet, dass solche Ansprüche ohne Rücksicht auf ihre Entstehung und die Kenntnis oder grob fahrlässige Unkenntnis nach 30 Jahren verjähren.

8.2.2 Vernichtung beziehungsweise Löschung von Patientenunterlagen

Für die Frage der Vernichtung von Papierunterlagen wie auch der Löschung von elektronischen Patientendaten ist Art. 17 DSGVO maßgeblich (im Folgenden ist einheitlich von „Löschung" die Rede). Wie Art. 17 Abs. 1 DSGVO klarstellt, ist eine Löschung nicht nur im Fall eines entsprechenden Antrags der Patientin oder des Patienten erforderlich. Die verantwortlichen Stellen sind auch selbst verpflichtet, zu prüfen, ob eine Löschung von Patientendaten vorzunehmen ist.

Patientendaten sind zu löschen, wenn eine der in Art. 17 Abs. 1 Buchst. a bis f DSGVO aufgezählten Gründe zutrifft und kein Ausnahmegrund nach Art. 17 Abs. 3 DSGVO eingreift. Insbesondere sind sie zu löschen, wenn die Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden (insbesondere zur Durchführung des Behandlungsvertrags) nicht mehr notwendig sind (Art. 17 Abs. 1 Buchst. a DSGVO).

Die unter Nr. 8.2.1 genannten Aufbewahrungsfristen können jedoch als „rechtliche Verpflichtung" (Art. 17 Abs. 3 Buchst. b Alt. 1 DSGVO) einer Löschung entgegenstehen. Solange Aufbewahrungsfristen in diesem Sinne noch laufen, sind die Patientendaten weiter zu speichern. Ein Anspruch auf Löschung von Patientendaten kommt in dem zehnjährigen Zeitraum nach Abschluss der Behandlung grundsätzlich nicht in Betracht.

8.2.3 Keine pauschale 30-jährige Aufbewahrung von Patientenunterlagen für Rechtsverfolgungszwecke

Unter gewissen Umständen kann eine längere Speicherung, gestützt auf Art. 17 Abs. 3 Buchst. e DSGVO, zulässig oder geboten sein. Diese Vorschrift sieht vor, dass die Pflicht zur Löschung nicht gilt, soweit die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

Wie bei allen Ausnahmetatbeständen des Art. 17 Abs. 3 DSGVO muss jedoch auch in solchen Fällen die Verarbeitung für die Rechtsverfolgungszwecke „erforderlich" sein und daher insbesondere in zeitlicher Hinsicht auf das notwenige Maß beschränkt werden. Die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen muss daher bereits stattfinden oder mit einer hinreichend hohen Wahrscheinlichkeit bevorstehen. Im Rahmen der bei Art. 17 Abs. 3 Buchst. e DSGVO erforderlichen Prognose können neben der konkreten Wahrscheinlichkeit eines Rechtsstreits auch die – insbesondere wirtschaftliche – Bedeutung der fraglichen Ansprüche und die Belange der betroffenen Person Berücksichtigung finden.[110]

Dem Argument des Klinikums, im Hinblick auf die Verjährungshöchstfrist nach § 199 Abs. 2 BGB bei Patientenunterlagen über stationäre Aufenthalte generell einer Beweisnot zu unterliegen, konnte ich mich nicht anschließen. Nach der Rechtsprechung der Zivilgerichte sind Krankenunterlagen – vorbehaltlich besonderer Gründe, die ausnahmsweise eine längere Aufbewahrungsfrist fordern können – grundsätzlich nicht länger als zehn Jahre aufzubewahren. Eine längere Aufbewahrung kann dadurch gerechtfertigt sein, dass ein Arzt oder Krankenhausträger nach Ablauf von zehn Jahren seit Durchführung der relevanten Behandlung mit einer Inanspruchnahme rechnen muss. Muss der Arzt oder Krankenhausträger die Krankenunterlagen nicht länger als zehn Jahre aufbewahren, darf ihm wegen der Vernichtung, wegen des Verlusts oder ihrer Unvollständigkeit nach diesem Zeitpunkt auch kein Nachteil entstehen.[111] Die Beweislastumkehr nach § 630h Abs. 3 BGB greift diese Rechtsprechung auf und erstreckt sich ausdrücklich nur auf den Zeitraum der Zehnjahresfrist des § 630f Abs. 3 BGB.[112]

Ich habe dem Klinikum daher mitgeteilt, dass es sich aus meiner Sicht nur auf den Ausnahmetatbestand des Art. 17 Abs. 3 Buchst. e DSGVO berufen kann, wenn Rechtsverfolgungszwecke im Einzelfall ausnahmsweise eine Aufbewahrung über die Regel-Aufbewahrungsfrist von zehn Jahren hinaus erfordern.

8.2.4 Löschung im konkreten Fall, aber weiterhin uneinheitliche Praxis

In dem konkreten Fall konnte das Klinikum solche auf den Einzelfall bezogenen Gründe nicht nachvollziehbar darlegen. Die angeführten Tatsachen reichten aus meiner Sicht nicht aus, um zu begründen, dass die Geltendmachung, Ausübung

[110] Vgl. dazu auch Bayerischer Landesbeauftragter für den Datenschutz, Das Recht auf Löschung nach der Datenschutz-Grundverordnung, Orientierungshilfe, Stand 6/2022, Rn. 90 f., Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

[111] Siehe Oberlandesgericht Düsseldorf, Urteil vom 1. Juli 2021, 8 U 165/20, BeckRS 2021, 16801, Rn. 16 f.; vgl. auch Oberlandesgericht Hamm, Urteil vom 9. Mai 2017, 26 U 91/16, BeckRS 2017, 111857, Rn. 35; Oberlandesgericht Karlsruhe, Urteil vom 11. Februar 2004, 7 U 174/02, BeckRS 2004, 18606, Rn. 7.

[112] Vgl. auch Bundestags-Drucksache 17/10488, S. 30.

oder Verteidigung von Rechtsansprüchen bereits stattfinden oder mit einer hinreichend hohen Wahrscheinlichkeit bevorstehen würde. Insbesondere konnte ein Auskunftsantrag nach Art. 15 DSGVO ohne weitere Anhaltspunkte für eine eventuelle Geltendmachung von (Schadensersatz-)Ansprüchen durch die betroffene Person eine „aufbewahrungsgünstige" Prognose nicht tragen. Das Klinikum erklärte sich schließlich dazu bereit, die Patientenunterlagen der betroffenen Person zu löschen. Das Beschwerdeverfahren konnte damit im Sinne der betroffenen Person abgeschlossen werden.

In meiner aufsichtlichen Praxis begegnet mir dieses Problem einer pauschal zu langen Aufbewahrung von Patientenunterlagen in den Krankenhäusern immer wieder. Nach meiner Erfahrung ist dies im Hinblick auf elektronisch geführte Patientenakten teilweise dadurch bedingt, dass manche Krankenhausinformationssysteme keine hinreichende Funktionalität für die technische Umsetzung von Löschungen vorsehen. Solche Schwierigkeiten liefern jedoch schon mit Blick auf Art. 25 DSGVO keine hinreichende Begründung dafür, datenschutzrechtlich gebotene Löschungen von Patientenunterlagen einfach zu unterlassen.

8.3 „Korrektur" von Arztbriefen

Mit der Bitte um Beratung zur Frage der Möglichkeit einer „Korrektur" von Arztbriefen wandte sich ein städtisches Klinikum an mich. Eine Patientin hatte bei dem Klinikum einen Antrag gestellt, dass bestimmte Ausführungen in einem Arztbrief zu Vordiagnosen entfernt werden sollen, der Arztbrief also nachträglich geändert werden soll. Konkret ging es dabei um Ausführungen im Arztbrief, dass die Patientin im Vorjahr mehrfach wegen Alkoholvergiftungen behandelt wurde. Bei der aktuellen Behandlung, die Gegenstand des Arztbriefs war, hatte dies aber offenkundig keine Bedeutung.

Bei der IT-gestützten Generierung eines Arztbriefes wurden im eingesetzten Krankenhausinformationssystem aufgrund der Softwarekonfiguration alle Vordiagnosen automatisch übernommen, auch wenn es – wie in dem konkreten Fall – an einer gegebenenfalls erforderlichen ausdrücklichen Einwilligung im Sinne des Art. 9 Abs. 2 Buchst. a DSGVO fehlte. Das Personal des Klinikums hatte nur die Möglichkeit, einzelne oder alle Diagnosen „abzuwählen" und so die Übernahme der Vordiagnosen in einem neuen Behandlungsfall zu verhindern.

8.3.1 Antrag auf „Korrektur" als Antrag auf Löschung zu verstehen

Ein generelles Recht auf „Korrektur" von Arztbriefen ergibt sich weder aus der Datenschutz-Grundverordnung noch aus sonstigen datenschutzrechtlichen Vorschriften.

Bei dem Antrag der Patientin handelte es sich aus meiner Sicht um einen Antrag auf Löschung nach Art. 17 DSGVO. Ein grundsätzlich ebenfalls denkbarer Antrag auf Berichtigung nach Art. 16 DSGVO käme nur in Betracht, wenn die Patientin die Unrichtigkeit der fraglichen Informationen rügen würde. Dem war offenbar nicht so; die Patientin wollte nur im „Neufall" von der damit nicht zusammenhängenden „Altdiagnose" verschont bleiben.

Eine wichtige Einschränkung für die Durchsetzung des Rechts auf Löschung ergibt sich jedoch daraus, dass sich diese nur auf personenbezogene Daten beziehen kann, welche das Klinikum verarbeitet. Für einen Arztbrief bedeutet dies konkret, dass sich ein Löschungsantrag nur auf Daten erstrecken kann, die beispielsweise in der digitalen oder analogen Patientenakte des Klinikums enthalten sind. Arztbriefe, die an die Patientin oder an Dritte versandt wurden und vom Klinikum nicht weiter verarbeitet werden, können daher nicht mehr Gegenstand eines Löschungsanspruchs sein. Unter Umständen ist jedoch nach Art. 19 Satz 1 DSGVO eine Mitteilung der Löschung gegenüber den Empfängern erforderlich, denen die Daten offengelegt wurden (also an die zum Beispiel der Arztbrief übersandt wurde).

8.3.2 Ein Anspruch auf Löschung ist grundsätzlich denkbar

Die grundsätzlichen Voraussetzungen für einen Anspruch auf Löschung ergeben sich aus Art. 17 Abs. 1 DSGVO. Als Löschungsgrund kam aus meiner Sicht in der geschilderten Konstellation insbesondere Art. 17 Abs. 1 Buchst. d DSGVO in Betracht. Dieser Tatbestand sieht vor, dass Daten zu löschen sind, wenn die personenbezogenen Daten unrechtmäßig verarbeitet werden. Die „Rechtmäßigkeit" einer Verarbeitung im Sinne des Art. 17 Abs. 1 Buchst. d DSGVO bemisst sich danach, ob der jeweilige Verarbeitungsvorgang auf eine Rechtsgrundlage nach Art. 6 DSGVO gestützt werden kann.[113]

Die hier relevante Verarbeitung von Daten war aus meiner Sicht nicht die Speicherung der Vordiagnosen, da sich die Patientin nicht gegen diese Speicherung an sich wandte. Der Patientin ging es vielmehr um die Tatsache der Verknüpfung dieser Daten mit dem neuen Behandlungsvorgang. Eine solche Verknüpfung stellt eine gesonderte Verarbeitung von Daten der Patientin dar. Um rechtmäßig zu sein, muss die Verknüpfung auf eine taugliche Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 DSGVO gestützt werden können. Da es sich bei den Daten aus der Vordiagnose in aller Regel um Gesundheitsdaten im Sinne des Art. 9 Abs. 1 DSGVO handeln wird, sind dabei zusätzlich die Voraussetzungen von Art. 9 Abs. 2 und gegebenenfalls Abs. 3 DSGVO zu beachten.

Eine (ausdrückliche) Einwilligung nach Art. 6 Abs. 1 UAbs. 1 Buchst. a in Verbindung mit Art. 9 Abs. 2 Buchst. a DSGVO lag in dem konkreten Fall nicht vor und kam daher auch nicht als Rechtsgrundlage für die Verknüpfung in Frage. Außer auf eine Einwilligung kann eine Datenverarbeitung unter Umständen auch auf gesetzliche Befugnisse gestützt werden (Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2 und 3 in Verbindung mit Art. 9 Abs. 2 Buchst. h, Abs. 3 DSGVO). Als eine solche Befugnis kam hier insbesondere Art. 27 Abs. 4 Satz 1 Bayerisches Krankenhausgesetz (BayKrG) in Betracht.

Diese Vorschrift sieht vor, dass die Krankenhausärzte Patientendaten nutzen dürfen, „soweit dies im Rahmen des krankenhausärztlichen Behandlungsverhältnisses […] erforderlich ist". Ich habe dem Klinikum daher anheimgestellt, zu prüfen, ob in der geschilderten Konstellation

[113] Vgl. Europäischer Gerichtshof, Urteil vom 4. Mai 2023, C-60/22, Rn. 51 ff.

— gegenüber der Patientin ein krankenhausärztliches Behandlungsverhältnis zustandegekommen war und

— aus fachlicher Sicht die Verknüpfung der Daten der Vordiagnose mit dem neuen Behandlungsvorgang „erforderlich“ war.

Sofern alle Voraussetzungen nach Art. 27 Abs. 4 Satz 1 BayKrG sowie ergänzend Art. 9 Abs. 2 Buchst. h und Abs. 3 DSGVO erfüllt sind, ist die Datenverarbeitung rechtmäßig. Ein Anspruch beziehungsweise eine Pflicht zur Löschung aufgrund „unrechtmäßiger Verarbeitung“ (Art. 17 Abs. 1 Buchst. d DSGVO) besteht in diesem Fall nicht.

Erweist sich die Verknüpfung jedoch als rechtswidrig, besteht grundsätzlich ein Anspruch auf Löschung. Diesem steht meines Erachtens auch nicht entgegen, dass sich die Antragstellerin nicht gegen die Speicherung der Vordiagnosen an sich wendet, sondern nur gegen die Verknüpfung mit dem neuen Behandlungsvorgang. Art. 17 Abs. 1 Buchst. d DSGVO setzt durch seine allgemeine Bezugnahme auf die Unrechtmäßigkeit der Verarbeitung voraus, dass sich der Anspruch auf Löschung auch auf andere Verarbeitungsvorgänge wie etwa eine Datenverknüpfung beziehen kann. Ein Anspruch auf Löschung kann sich daher auch allein auf die Löschung der Verknüpfung der Vordiagnosen mit einem neuen Behandlungsvorgang beziehen.

8.3.3 Ausnahmen vom Recht auf Löschung sind zu beachten

Auch wenn grundsätzlich ein Anspruch auf Löschung nach Art. 17 Abs. 1 DSGVO besteht, sind jedoch die Ausnahmen nach Art. 17 Abs. 3 DSGVO zu beachten.

In Betracht kommt dabei insbesondere der Ausnahmegrund der „Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert“ (Art. 17 Abs. 3 Buchst. b Alt. 1 DSGVO). Hiernach können unter Umständen die besonderen Vorgaben der arztrechtlichen Dokumentationspflichten (siehe etwa § 630f Bürgerliches Gesetzbuch) berücksichtigt werden.

Sofern grundsätzlich von einem Anspruch auf Löschung ausgegangen wird, habe ich dem Klinikum daher anheimgestellt, zu prüfen, ob die Verarbeitung der Daten aus einem dieser Gründe erforderlich und daher ein Löschungsanspruch abzulehnen ist.

8.4 CD-ROM als Kopie personenbezogener Daten im Krankenhausbereich?

Wer in einem Krankenhaus ärztlich behandelt wurde, möchte sich manchmal anschließend einen Überblick verschaffen, welche Daten von ihm dort verarbeitet wurden und weiter gespeichert sind. Diesem Zweck dient ein Antrag auf eine Kopie der verarbeiteten personenbezogenen Daten (Art. 15 Abs. 1, Abs. 3 DSGVO).. Betroffene Personen äußern in diesem Zusammenhang mitunter den Wunsch, die Kopie in einer bestimmten Form (zum Beispiel auf Papier oder einem Datenträger) zu erhalten. Das ist ein legitimes Anliegen.

In einem Beschwerdefall bat eine betroffene Person ein bayerisches öffentliches Krankenhaus, ihr eine Kopie der personenbezogenen Daten vorzugsweise elektronisch (zum Beispiel per E-Mail oder mittels Downloads aus einem Cloudspeicher), alternativ in Papierform, zugänglich zu machen. Das Krankenhaus übersandte ihr per Post eine CD-ROM, auf welcher die entsprechenden Informationen gespeichert waren. Ich hatte zu klären, ob diese Vorgehensweise der Datenschutz-Grundverordnung entsprach.

8.4.1 Vorab: Verhältnis von Art. 15 DSGVO und § 630g BGB

Im medizinischen Bereich können betroffene Personen neben dem datenschutzrechtlichen Auskunftsrecht nach Art. 15 Abs. 1, Abs. 3 DSGVO grundsätzlich auch auf das Einsichtsrecht in die Behandlungsakte nach § 630g Bürgerliches Gesetzbuch (BGB) zurückgreifen, soweit sie Auskunft über Informationen betreffend eine ärztliche Behandlung wünschen. Das datenschutzrechtliche Auskunftsrecht umfasst dabei grundsätzlich einen unentgeltlichen Anspruch auf eine originalgetreue Reproduktion der eigenen personenbezogenen Daten, welche der Verantwortliche der betroffenen Person auch zusenden muss. § 630g Abs. 1 Satz 1 BGB verschafft einem Patienten demgegenüber einen Anspruch auf Einsicht in die vollständige ihn betreffende Behandlungsakte. Nach § 630g Abs. 1 Satz 3, Satz 4 BGB kann der Patient auch Abschriften von der Behandlungsakte verlangen, wobei jedoch nur die erste Abschrift unentgeltlich zur Verfügung gestellt werden muss. Das Einsichtsrecht in die Behandlungsakte ist grundsätzlich eine Holschuld, der Patient muss also den Ort aufsuchen, an dem sich die Behandlungsakte befindet (§ 630g Abs. 1 Satz 2, § 811 Abs. 1 Satz 1 BGB). Eine Behandlungsakte kann auch Informationen enthalten, welche über die nach Art. 15 Abs. 1, Abs. 3 DSGVO zu beauskunftenden personenbezogenen Daten hinausgehen. Dagegen bezieht sich das datenschutzrechtliche Auskunftsrecht grundsätzlich auf alle personenbezogenen Daten im Verantwortungsbereich des Verantwortlichen, auch auf solche, die sich nicht in einer Behandlungsakte befinden. Während das Einsichtsrecht in die Behandlungsakte im Falle des Todes des Patienten zur Wahrnehmung der vermögensrechtlichen Interessen dessen Erben oder nächsten Angehörigen zustehen kann (§ 630g Abs. 3 BGB), kann das datenschutzrechtliche Auskunftsrecht postmortal nicht ausgeübt werden (Erwägungsgrund 27 DSGVO). Beschränkungen des datenschutzrechtlichen Auskunftsrechts ergeben sich aus Art. 15 Abs. 4 DSGVO, § 83 Zehntes Buch Sozialgesetzbuch, Art. 10 BayDSG. Das Einsichtsrecht in die Behandlungsakte besteht nicht, soweit erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen (§ 630g Abs. 2 Satz 1 BGB). Diese Ausnahme steht unter den Voraussetzungen des § 630g Abs. 4 Satz 3 BGB auch dem datenschutzrechtlichen Auskunftsrecht entgegen. Im Übrigen wird das datenschutzrechtliche Auskunftsrecht durch das Einsichtsrecht in die Behandlungsakte nicht berührt (§ 630g Abs. 4 Satz 1 BGB).

8.4.2 Datenschutzrechtlicher Ausgangspunkt: Anforderungen an die Form einer Datenkopie nach Art. 15 Abs. 1, Abs. 3 DSGVO

8.4.2.1 Keine Anwendung der Vorgaben zur Darstellungsweise von Informationen

Die Datenschutz-Grundverordnung sieht in Art. 12 Abs. 1 Satz 1 Halbsatz 1 Var. 2 DSGVO vor, dass der Verantwortliche geeignete Maßnahmen trifft, um der betroffenen Person alle Mitteilungen gemäß den Artikeln 15 bis 22, die sich auf die

Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Art. 12 Abs. 1 Satz 1 DSGVO enthält insoweit Vorgaben für die Darstellungsweise von Informationen, die der Verantwortliche der betroffenen Person zukommen lassen muss.[114] Nicht anwendbar sind diese Vorgaben aber auf das Recht auf eine Datenkopie, weil dieses Recht der betroffenen Person einen Anspruch darauf vermittelt, bestimmte Daten gerade in der Form zu erhalten, in welcher der Verantwortliche selbst über diese verfügt.[115] Anforderungen an die Darstellungsweise passen hierzu nicht[116] und sind insoweit nicht auf die Form der Kopie personenbezogener Daten übertragbar.

8.4.2.2 Formvorgabe des Art. 12 Abs. 1 Satz 2 DSGVO und Sonderregelung

Anders verhält es sich mit Art. 12 Abs. 1 Satz 2 DSGVO, wonach die Übermittlung der Informationen schriftlich oder in anderer Form, gegebenenfalls auch elektronisch erfolgt. Diese Vorschrift betrifft die Form von Informationen und ist deshalb grundsätzlich auch auf das Recht auf eine Datenkopie anzuwenden. Dabei ist allerdings zu beachten, dass Art. 15 Abs. 3 Satz 3 DSGVO insoweit eine Sonderregelung bereithält.[117] Bei einer antragsgebundenen Informationspflicht wie dem Recht auf eine Datenkopie steht die Form der Information ein Stück weit zur Disposition der betroffenen Person.[118] Nach Art. 15 Abs. 3 Satz 3 DSGVO sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, wenn die betroffene Person den Antrag elektronisch gestellt stellt und nichts anderes angibt. . Andere Informationsformen kann die betroffene Person hingegen nicht verbindlich vorgeben, sondern lediglich Entscheidungsspielräume des Verantwortlichen eröffnen oder erweitern.[119] Insbesondere vermittelt die Datenschutz-Grundverordnung keinen (ausdrücklich geregelten) Anspruch der betroffenen Person auf eine schriftliche Information.[120]

8.4.2.3 Gestaltungsspielraum des Verantwortlichen

Nach Art. 12 Abs. 2 Satz 1 DSGVO erleichtert der Verantwortliche der betroffenen Person die Ausübung ihrer Rechte gemäß den Artikeln 15 bis 22. Dieses Erleichterungsgebot verpflichtet den Verantwortlichen, seine Kommunikation mit der betroffenen Person so einzurichten, dass deren Betroffenenrechte ohne übermäßigen Aufwand erfüllt werden können.[121] Allerdings belässt diese Vorschrift dem Verantwortlichen einen Gestaltungsspielraum, sodass sich eine Verletzung erst feststellen lässt, wenn der Verantwortliche es der betroffenen Person ohne erkennbaren sachlichen Grund erheblich erschwert, ihre Rechte auszuüben oder gebotene Informationen entgegenzunehmen.[122] Stellt die betroffene Person den Auskunftsantrag elektronisch, so sind die Informationen nach Art. 15 Abs. 3 Satz 3 DSGVO in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt. In diesem Fall kann der Verantwortliche ein gängiges Format wählen, das die betroffene Person mit allgemein verfügbarer (nicht

[114] Bäcker in: Kühling/Buchner, DSGVO/BDSG, 4. Aufl. 2024, Art. 12 DSGVO Rn. 9.
[115] Bäcker in: Kühling/Buchner, DSGVO/BDSG, 4. Aufl. 2024, Art. 12 DSGVO Rn. 10.
[116] Bäcker a. a. O.
[117] Bäcker in: Kühling/Buchner, DSGVO/BDSG, 4. Aufl. 2024, Art. 12 DSGVO Rn. 14.
[118] Bäcker in: Kühling/Buchner, DSGVO/BDSG, 4. Aufl. 2024, Art. 12 DSGVO Rn. 17.
[119] Bäcker a. a. O.
[120] Bäcker a. a. O.
[121] Bäcker in: Kühling/Buchner, DSGVO/BDSG, 4. Aufl. 2024, Art. 12 DSGVO Rn. 25.
[122] Bäcker a. a. O. mit weiteren Nachweisen.

notwendigerweise kostenloser) Software verarbeiten kann.[123] Erwägungsgrund 63 Satz 4 DSGVO erwähnt in diesem Kontext, dass der Verantwortliche nach Möglichkeit den Fernzugang zu einem sicheren System bereitstellen kann, welcher der betroffenen Person einen direkten Zugang zu ihrem personenbezogenen Daten ermöglicht. Hierzu ist der Verantwortliche jedoch nicht verpflichtet.[124] Auch eine Übersendung der Daten per Post auf einem physischen Datenträger etwa ist zulässig, sofern Anforderungen an die Datensicherheit aus Art. 32 DSGVO nicht entgegenstehen.[125]

8.4.3 Besonderheiten des medizinischen Bereichs

Der Beschwerdefall zeigt beispielhaft, dass insbesondere im medizinischen Bereich regelmäßig umfangreiche und detaillierte Bilddateien (Röntgenaufnahmen, MRT-Aufnahmen, CT-Aufnahmen) zu beauskunften sind. Insoweit erleichtert eine elektronische Datenübermittlung die Erfüllung der Auskunftspflicht des Verantwortlichen. Dies gilt auch für die postalische Übersendung einer CD-ROM, auf der die Daten in elektronischer Formgespeichert sind.

Jedenfalls im medizinischen Bereich sehe ich eine CD-ROM weiterhin als ein gängiges Medium im Sinne von Art. 15 Abs. 3 Satz 3 DSGVO an, gerade wenn es um die Bereitstellung von Bilddateien geht. Nach den Erfahrungen meiner Prüfpraxis halten Krankenhäuser regelmäßig zentrale Einrichtungen vor, in welchen Daten auf CD-ROMs gebrannt werden und die CD-ROMs zum Zwecke der Zuordnung mit entsprechenden Aufklebern versehen werden können. Diese Infrastruktur dient der Datenweitergabe an andere Krankenhäuser oder Nachbehandelnde wie auch der Erfüllung von Auskunftsansprüchen der Patientinnen und Patienten. Es mögen zwar modernere Formen der Datenbereitstellung verfügbar sein, dies ändert aber nichts daran, dass der Begriff des „gängigen elektronischen Formats“ auf die tatsächlichen Gegebenheiten, nicht auf einen technischen Idealzustand verweist.

Allenfalls wenn eine betroffene Person zu verstehen gibt, mit einer CD-ROM überhaupt nichts anfangen zu können und deshalb auf eine schriftliche Auskunft angewiesen zu sein, dürfte das Krankenhaus auf eine analoge Auskunft zu verwiesen sein. Ein solcher Fall kann etwa vorliegen, wenn sich die betroffene Person jeder Digitalisierung verschlossen hat und auch nicht die Hilfe Dritter – etwa von Verwandten – in Anspruch nehmen kann.

8.4.4 Ergebnis

Ein Krankenhaus darf einen Antrag auf Kopie der personenbezogenen Daten regelmäßig auch mittels einer CD-ROM erfüllen. Die betroffene Person kann dann nicht verlangen, dass für ihre spezifischen Bedürfnisse ein neuer Workflow aufgebaut wird. Eine rein analoge Beauskunftung muss das Krankenhaus nur in Aus-

[123] Bäcker in: Kühling/Buchner, DSGVO/BDSG, 4. Aufl. 2024, Art. 15 DSGVO Rn. 44d.
[124] Vgl. Bäcker a. a. O.
[125] Bäcker a. a. O.

nahmefällen anbieten. Auch im Beschwerdefall war der Anspruch aus eine Datenkopie nach Art. 15 Abs. 1, Abs. 3 DSGVO durch Bereitstellung einer CD-ROM mit den Behandlungsdaten erfüllt.

8.5 Videoüberwachung in psychiatrischen Krankenhäusern

Berichten möchte ich weiterhin über eine Beschwerde betreffend die Videoüberwachung in einem psychiatrischen Krankenhaus, konkret in einem Patientenzimmer einer offen geführten Station. Zwar hat die betroffene Person die Beschwerde später zurückgenommen, sodass ich das Beschwerdeverfahren eingestellt habe. Aufgrund der besonderen Situation in einem psychiatrischen Krankenhaus habe ich jedoch von der Möglichkeit Gebrauch gemacht, die Videoüberwachung von Amts wegen zu überprüfen.

Auf der betreffenden Station waren sechs von elf Patientenzimmern sowie Teile des Flurs mit Kameras ausgestattet. In den Patientenzimmern war die Videoüberwachung nicht durchgehend aktiviert, sondern wurde nur genutzt, wenn dafür aus Sicht des Personals eine akute medizinische Notwendigkeit bestand. Die Videoüberwachung des Flurs diente der Unterstützung des Personals im Nachtdienst. Es handelte sich um eine Videoüberwachung in Form der Videobeobachtung (auch als „verlängertes Auge“ bezeichnet); eine Aufzeichnung fand nicht statt. Die Videoaufnahmen waren im Stationszimmer auf einem Monitor zu sehen und zumindest zeitweise nicht nur für das Stationspersonal, sondern potentiell auch für andere Personen auf der Station wahrnehmbar. Dies resultierte daraus, dass Sichtschutzfolien nach Mitteilung des Krankenhauses zunächst nicht lieferbar waren. Zum Zeitpunkt meiner Kontrolle war die Videoüberwachung in den Patientenzimmern erst einmal zum Einsatz gekommen, nämlich in dem Fall der ursprünglich erhobenen Beschwerde.

Im Austausch mit dem Krankenhaus ging es mir insbesondere darum zu klären, unter welchen rechtlichen Voraussetzungen die aus therapeutischer Sicht in bestimmten Fällen veranlasste Videoüberwachung auch tatsächlich eingesetzt werden durfte. Dabei zeigte sich, dass die Praxis der öffentlichen Krankenhäuser in Bayern uneinheitlich ist und beträchtliche Unsicherheiten hinsichtlich der Bestimmung der möglichen Rechtsgrundlagen und deren jeweiliger Reichweite bestehen.

8.5.1 Landeskrankenhausrecht enthält keine hinreichende Rechtsgrundlage

Grundsätzlich denkbar wäre es, die Videoüberwachung auf die allgemeine Datenerhebungsbefugnis nach Art. 27 Abs. 2 Satz 1 Bayerisches Krankenhausgesetz (BayKrG) zu stützen. Danach dürfen Patientendaten nur erhoben und aufbewahrt werden, soweit dies zur Erfüllung der Aufgaben des Krankenhauses oder im Rahmen des krankenhausärztlichen Behandlungsverhältnisses erforderlich ist oder die betroffene Person eingewilligt hat.

Insofern ist aus meiner Sicht jedoch zu beachten, dass diese allgemein gehaltene Vorschrift des Landeskrankenhausrechts nicht auf die besondere Eingriffsintensität einer Videoüberwachung angepasst ist. Aufgrund der verfassungsrechtlichen Anforderungen an eine gesetzliche Verarbeitungsbefugnis wird ganz überwie-

gend angenommen, dass allgemeine Verarbeitungsbefugnisse nur Verarbeitungen tragen können, die mit einem „lediglich geringfügigen Eingriff“ in die Rechte der betroffenen Personen verbunden sind.[126]

Nach meiner Bewertung enthält Art. 27 Abs. 2 Satz 1 BayKrG keine hinreichend spezifischen und klaren Begrenzungen für Eingriffe durch Videoüberwachung, welche die in der erwähnten Rechtsprechung formulierten Anforderungen erfüllen würden. Art. 27 Abs. 2 Satz 1 BayKrG kommt daher als Rechtsgrundlage für Videoüberwachungsmaßnahmen nicht in Betracht.

8.5.2 Spezialgesetzliche Vorschriften im Fall öffentlich-rechtlicher Unterbringungen

Soweit es sich um öffentlich-rechtliche Unterbringungen im Sinne des Art. 5 ff. Bayerisches Psychisch-Kranken-Hilfe-Gesetz (BayPsychKHG) handelt, kann eine Videoüberwachung in Gestalt einer Videobeobachtung aufgrund von Art. 29 Abs. 1, Abs. 2 Nr. 1 BayPsychKHG durchgeführt werden, wenn die dort genannten Voraussetzungen erfüllt sind. Eine dort zulässige besonderen Sicherungsmaßnahmen ist die „ständige Beobachtung, auch mit technischen Mitteln“.

Für den Maßregelvollzug sieht Art. 25 Abs. 1, Abs. 2 Nr. 1 Bayerisches Maßregelvollzugsgesetz eine entsprechende Regelung vor.

8.5.3 Vorzugswürdig: Videoüberwachung aufgrund einer Einwilligung der betroffenen Person

Soweit Patientinnen und Patienten dazu in der Lage sind, über eine Einwilligung nach Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO (gegebenenfalls in Verbindung mit Art. 9 Abs. 2 Buchst. a DSGVO) zu entscheiden, erscheint eine Anwendung dieser Rechtsgrundlage vorzugswürdig; dies gilt jedenfalls für die Videoüberwachung in Patientenzimmern. Das Krankenhaus hat mir mitgeteilt, dass es auch aus therapeutischer Sicht in aller Regel sinnvoller ist, eine Videoüberwachung auf eine Einwilligung der Patientinnen und Patienten zu stützen. Diese Auffassung kann ich aus datenschutzrechtlicher Sicht unterstützen.

Im Hinblick auf die Voraussetzungen einer wirksamen Einwilligung wird aus meiner Sicht insbesondere zu beachten sein, dass die Patientinnen und Patienten auch tatsächlich einwilligungsfähig sind, die Freiwilligkeit der Einwilligung gegeben (vgl. Art. 7 Abs. 4 und 4 Nr. 11 DSGVO) und die Einwilligung – im Sinne von Art. 9 Abs. 2 Buchst. a DSGVO – auch hinreichend spezifisch ist.

Soweit es um eine Videoüberwachung außerhalb von Patientenzimmern geht, wie zum Beispiel auf öffentlich zugänglichen Flächen, kommen Einwilligungen kaum als Rechtsgrundlage in Betracht. Insbesondere kann das bloße Betreten einer

[126] Vgl. entsprechend Bayerischer Verwaltungsgerichtshof, Beschluss vom 15. Februar 2024, 4 CE 23.2267, BeckRS 2024, 2968, Rn. 19 ff.; Bundesverfassungsgericht, Beschluss vom 23. Februar 2007, 1 BvR 2368/06, BeckRS 2007, 22066, unter II. 3. b) bb) (2) (b).

überwachten Fläche üblicherweise nicht als hinreichend eindeutige und informierte Einwilligung verstanden werden.[127]

8.5.4 Anwendung der allgemeinen gesetzlichen Vorschrift über Videoüberwachungen?

Gegebenenfalls könnte die Regelung des Art. 24 BayDSG einschlägig sein, welche ausdrücklich die Frage der Videoüberwachung adressiert und dafür bestimmte Voraussetzungen aufstellt. Art. 24 Abs.1 BayDSG sieht dabei Folgendes vor:

> „Die Verarbeitung personenbezogener Daten mit Hilfe von optisch-elektronischen Einrichtungen (Videoüberwachung) ist zulässig, wenn dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts erforderlich ist,
> 1. um Leben, Gesundheit, Freiheit oder Eigentum von Personen, die sich im Bereich öffentlicher Einrichtungen, öffentlicher Verkehrsmittel, von Dienstgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen oder in deren unmittelbarer Nähe aufhalten, oder
> 2. um Kulturgüter, öffentliche Einrichtungen, öffentliche Verkehrsmittel, Dienstgebäude oder sonstige bauliche Anlagen öffentlicher Stellen sowie die dort oder in deren unmittelbarer Nähe befindlichen Sachen
>
> zu schützen und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der betroffenen Personen beeinträchtigt werden."

Auf Art. 24 BayDSG können sich Behörden und sonstige öffentliche Stellen des Freistaates Bayern, der Gemeinden, Gemeindeverbände und der sonstigen der Aufsicht des Freistaates Bayern unterstehenden juristischen Personen des öffentlichen Rechts berufen (Art. 1 Abs. 1 Satz 1 BayDSG). Grundsätzlich ist die Vorschrift auch auf bayerische öffentliche Krankenhäuser anwendbar.

Eine Einschränkung ergibt sich jedoch aus Art. 1 Abs. 3 BayDSG. Nach dieser Vorschrift gelten für öffentliche Stellen, ihre Zusammenschlüsse und Verbände die Vorschriften für nicht-öffentliche Stellen, soweit sie „als Unternehmen am Wettbewerb teilnehmen". In diesem Fall wäre Art. 24 BayDSG nicht anwendbar.

Nach meiner Einschätzung stehen die bayerischen öffentlichen Krankenhäuser „als Unternehmen im Wettbewerb", soweit sie etwa Aufgaben der Patientenversorgung wahrnehmen, die in vergleichbarer Form auch von Krankenhäusern in privater (oder kirchlicher) Trägerschaft erbracht werden.[128] Videoüberwachungsmaßnahmen, die grundsätzlich im Zusammenhang mit einer wettbewerblichen Tätigkeit stehen, weisen für sich genommen jedoch nicht notwendigerweise immer einen wettbewerblichen Charakter auf.[129]

Mir gegenüber konnte das Krankenhaus in nachvollziehbarer Weise schildern, dass in den hier relevanten Fallkonstellationen keine Teilnahme als Unternehmen

[127] Vgl. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Videoüberwachung nach der Datenschutz-Grundverordnung, Kurzpapier Nr. 15, Stand 12/2018, S. 1, Internet: https://www.datenschutzkonferenz-online.de, Rubrik „Kurzpapiere"; Bundesverwaltungsgericht, Urteil vom 27. März 2019, 6 C 2/18, BeckRS 2019, 9874, Rn. 22 f.

[128] Vgl. Bayerischer Landesbeauftragter für den Datenschutz, 28. Tätigkeitsbericht 2018, Nr. 8.4.1.

[129] Siehe Bayerischer Landesbeauftragter für den Datenschutz, Videoüberwachung durch bayerische öffentliche Stellen, Orientierungshilfe, Stand 2/2020, Rn. 13, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

am Wettbewerb vorliegt. Das Krankenhaus habe insofern – anders als vergleichbare nicht-öffentliche Krankenhäuser – den psychiatrischen Vollversorgungsauftrag vom zuständigen Bezirk übernommen und komme daher einer öffentlichen Aufgabe nach. Die entsprechenden Patientinnen und Patienten würden von nicht-öffentlichen Krankenhäusern in der Regel nicht aufgenommen. Aus Sicht des Krankenhauses kommt Art. 24 BayDSG daher für die Videoüberwachung im Rahmen der Patientenbehandlung im Patientenzimmer von nicht-einwilligungsfähigen Patienten in Betracht. Hiergegen habe ich keine Einwände erhoben.

Gleiches gilt aus meiner Sicht auch für eine Videoüberwachung auf Fluren. Insofern besteht nur ein gelockerter Zusammenhang mit der Aufgabe der Patientenversorgung, sodass unabhängig von der Frage der Wettbewerbstätigkeit in diesem Rahmen eine Videoüberwachung aufgrund von Art. 24 BayDSG in Betracht kommt.

Zu den einzelnen inhaltlichen Voraussetzungen einer Videoüberwachung nach Art. 24 BayDSG verweise ich auf die Ausführungen in meiner einschlägigen Orientierungshilfe.[130]

8.5.5 Nur in Ausnahmefällen: Schutz lebenswichtiger Interessen als Rechtsgrundlage

Für Videoüberwachungsmaßnahmen in Patientenzimmern, die weder auf eine Einwilligung noch auf die oben genannten gesetzlichen Verarbeitungsbefugnisse gestützt werden können, kann schließlich in Ausnahmefällen eine Verarbeitung zum Schutz lebenswichtiger Interessen (Art. 6 Abs. 1 UAbs. 1 Buchst. d in Verbindung mit Art. 9 Abs. 2 Bucht. c DSGVO) in Betracht kommen.

Dabei ist jedoch zu beachten, dass eine solche Verarbeitung nur unter engen Voraussetzungen zulässig ist: Die Verarbeitung muss dem Zweck dienen, „lebenswichtige Interessen“ der betroffenen Person zu schützen. Aufgrund des Ausnahmecharakters der Vorschrift wird dies nur selten angenommen werden können, so etwa, wenn eine lebensbedrohliche Situation konkret zu befürchten ist. Die betroffene Person muss ferner aus körperlichen oder rechtlichen Gründen außerstande sein, ihre Einwilligung zu erteilen. Die Verarbeitung muss schließlich zu dem oben genannten Zweck erforderlich sein. Ich habe das Krankenhaus daher darauf hingewiesen, dass bei einer Videoüberwachung in Patientenzimmern auf dieser Grundlage äußerste Zurückhaltung angebracht ist.

[130] Siehe Fn. 129.

9 Gesetzliche Krankenversicherung

Im Bereich der Gesetzlichen Krankenversicherung nehme ich die Datenschutzaufsicht bei den sog. landesunmittelbaren Krankenkassen wahr. Dazu zählen – als bekanntester Anbieter – die AOK Bayern, jedoch auch einige Betriebskrankenkassen (BKK), nämlich die BKK Akzo Nobel Bayern, die BKK Faber-Castell & Partner, die Koenig & Bauer BKK und die Krones BKK. Zuständig bin ich ferner für die Kassenärztliche Vereinigung Bayerns sowie für den Medizinischen Dienst Bayern, der zuvorderst für die Krankenkassen gutachterliche Aufgaben wahrnimmt.

Wie nicht anders zu erwarten, war das Berichtsjahr von der sukzessiven Einführung der elektronischen Patientenakte und ihren datenschutzrechtlichen Implikationen geprägt. Gleichwohl waren auch viele Vorgänge aus ganz anderen Kontexten zu bearbeiten. So habe ich mich etwa mit Diagnosen in der sog. „Patientenquittung“ (Nr. 9.1) oder der Berichtigung von Diagnosedaten (Nr. 9.2). Der Datenschutz beim Mammografie-Screening-Programm (siehe zuletzt meinen 29. Tätigkeitsbericht 2019 unter Nr. 7.3) konnte weiter optimiert werden (Nr. 9.3).

9.1 Auskunft von Diagnosen in der Patientenquittung gesetzlicher Krankenkassen

Mehrere Beschwerden haben mich zur sog. Patientenquittung einer bayerischen Krankenkasse erreicht. Kritisiert wurden fehlende Angaben zu Diagnosen sowie Diagnose-Kennzeichen.

9.1.1 Ausgangspunkt: Was ist eine „Patientenquittung“?

Bei der sog. Patientenquittung (auch „Versichertenauskunft“) handelt es sich um eine verpflichtende Unterrichtung der Versicherten über die Leistungen, die zu Lasten der gesetzlichen Krankenversicherung in Anspruch genommen wurden. Eine solche Aufstellung können Versicherte zum einen bei ihrer gesetzlichen Krankenversicherung beantragen, wobei typischerweise ein Datenabruf auf elektronischem Wege ermöglicht wird. Maßgeblich ist insofern § 305 Abs. 1 Satz 1 Fünftes Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (SGB V). Zum anderen kann eine Patientenquittung nach § 305 Abs. 2 SGB V im Anschluss an die Behandlung auch von den Leistungserbringern – etwa Ärzten oder Krankenhäusern – verlangt werden; dies sieht § 305 Abs. 2 SGB V vor.

Daneben bleibt es den Versicherten unbenommen, auch zusätzlich den Auskunftsanspruch nach Art. 15 DSGVO geltend zu machen, um beispielsweise von der Kassenärztlichen Vereinigung Bayern die an die jeweilige Krankenkasse übermittelten Abrechnungsdaten zur eigenen Person zu erhalten.

9.1.2 Umfang der Auskunft nach § 305 Abs. 1 Satz 1 SGB V

§ 305 Abs. 1 Satz 1 SGB V vermittelt den Versicherten das Recht auf Auskunft über „die in Anspruch genommenen Leistungen und deren Kosten". Welche Daten im Einzelnen beauskunftet werden müssen, ergibt sich nicht abschließend aus der Norm. Es ist aber die Intention des Gesetzgebers gewesen, eine einfache und transparente Information der Versicherten zu gewährleisten:

Während die Krankenkassen in der Vergangenheit keine Gesamtübersicht der von den Versicherten in Anspruch genommenen Leistungen erstellen durften und daher auch keine Auskunft zu Diagnosen geben konnten (siehe hierzu bereits meinen 19. Tätigkeitsbericht 2000 unter Nr. 4.4.3) kam es durch zwischenzeitliche gesetzliche Anpassungen in § 305 SGB V zu einem Paradigmenwechsel:[131] Die bis dato im Gesetz festgelegte Trennung der Information über die ärztlichen Leistungen von den ärztlich veranlassten und verordneten Leistungen und das Verbot der Erstellung einer Gesamtübersicht der von den Versicherten in Anspruch genommenen Leistungen wurden aufgehoben, da dies nach Auffassung des Gesetzgebers nicht mehr dem Ziel einer einfachen und transparenten Information der Versicherten entsprach.[132]

Die Auskunft der Krankenkassen nach § 305 Abs. 1 Satz 1 SGB V umfasst nun alle von den Kassenärztlichen Vereinigungen übersandten Daten inklusive Diagnosen (ICD-Code) und Diagnose-Kennzeichen (A= ausgeschlossene Diagnose, G= gesicherte Diagnose, V= Verdachtsdiagnose, Z= Zustand nach Diagnose).

9.1.3 Technische Schwierigkeiten bei der Umsetzung

Meine Prüfung ergab, dass bei der Umsetzung der vollständigen Auskunft im Rahmen der elektronischen Patientenquittung sowohl in der App-Version als auch bei der Onlineversion der Krankenkasse die Diagnosekennzeichen aus technischen Gründen zeitweilig nicht mehr übertragen wurden.

Mit Blick auf diese Unzulänglichkeiten habe ich versucht, den Versicherten auf anderem Wege zur umfassenden Erfüllung Ihrer Auskunftsrechte zu verhelfen und die Krankenkasse ersucht, über den (vorübergehenden) Umstand der fehlenden Angaben in der Patientenquittung in transparenter Weise zu informieren. So wurde für den Zeitraum, in dem die Diagnosen nicht im Rahmen der elektronischen Patientenquittung dargestellt werden konnten, auf der Startseite der jeweiligen Benutzeroberfläche ein Hinweis auf das Fehlen der Diagnosen und Diagnosekennzeichen in der Patientenquittung angebracht. Zudem sagte mir die Krankenkasse zu, auf Antrag der Versicherten die vollständige Auskunft (zusätzlich zur elektronischen Patientenquittung) postalisch zu erteilen.

Aufgrund dieser Maßnahmen habe ich von weiteren aufsichtlichen Maßnahmen gegenüber der Krankenkasse abgesehen. Zwischenzeitlich habe ich erfahren, dass die Schwierigkeiten erfolgreich bewältigt werden konnten und die elektronische Patientenquittung wieder ohne Medienbruch vollständig erteilt werden kann.

[131] Durch die Änderung des § 305 Abs. 1 SGB V auf Grund des Terminservice- und Versorgungsgesetzes vom 6. Mai 2019 (BGBl. I S. 646) mit Wirkung zum 11. Mai 2019.

[132] Vgl. Bundestags-Drucksache 19/6337, S. 144.

9.1.4 Exkurs: Zugangsbeschränkung zu Diagnosedaten in der ePA

In diesem Zusammenhang möchte ich anmerken, dass die Abrechnungsdaten samt Diagnosen (ICD-Code) seit 1. Oktober 2025 verpflichtend auch in der elektronischen Patientenakte (ePA) gespeichert werden.

Hiergegen konnten sich die Versicherten zur Wehr setzen, in dem sie Widerspruch gegen die ePA oder – (nur) gegen die Speicherung der Abrechnungsdaten einlegten.[133]

Aus Datenschutzsicht ist die gesetzliche Änderung zum 1. Januar 2026[134] zu begrüßen, wonach der Zugang zu den Abrechnungsdaten auf den Versicherten selbst begrenzt wurde, die Leistungserbringer also keinen Einblick mehr erhalten. Dadurch müssen Versicherte nicht mehr befürchten, dass ihre Abrechnungsdaten in der ePA frei einsehbar sind.

9.2 Berichtigung von Diagnosedaten bei gesetzlichen Krankenkassen

Informationen zur Krankengeschichte eines Menschen sind oft besonders sensibel. Ihr Bekanntwerden kann für die betroffene Person gravierende nachteilige Folgen haben. Versicherte benötigen die (richtigen) Diagnosedaten oftmals für Weiterbehandlungen durch andere Ärzte oder im Vorfeld des Abschlusses privater Lebens- oder Berufsunfähigkeitsversicherungen. Vor diesem Hintergrund ist es wichtig, dass solche Daten mit der Realität übereinstimmen, mithin richtig sind. Im Berichtszeitraum habe ich mich intensiv mit Beschwerden betroffener Personen befasst, die gegenüber ihrer gesetzlichen Krankenversicherung Berichtigung bestimmter zu ihrer Person gespeicherter Diagnosedaten begehrten.

Versicherte haben gegenüber ihrer Krankenversicherung einen Anspruch auf Unterrichtung über die in Anspruch genommenen Leistungen und deren Kosten (§ 305 Abs. 1 Satz 1 Sozialgesetzbuch Fünftes Buch – Gesetzliche Krankenversicherung – SGB V). Darunter fallen auch die konkreten Diagnosedaten.[135] Auch mittels einer persönlichen elektronischen Gesundheitsakte oder der elektronischen Patientenakte können die Versicherten die gestellten Diagnosen in Erfahrung bringen. Die Krankenkassen übermitteln diesbezügliche Daten nämlich nach § 305 Abs. 1 Satz 2 SGB V auf Verlangen der versicherten Person an entsprechende Anbieter persönlicher elektronischer Gesundheitsakten.[136] Nach § 305 Abs. 1 Satz 3 SGB V werden die entsprechenden Daten auch an die Anbieter

[133] Siehe auch Bayerischer Landesbeauftragter für den Datenschutz, Widerspruchsrechte der Versicherten bei der elektronischen Patientenakte, Aktuelle Kurz-Information 56, Stand 3/2025, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

[134] Durch das Gesetz zur Befugniserweiterung und Entbürokratisierung in der Pflege vom 22. Dezember 2025 (BGBl. I Nr. 371) wurde in § 352 Satz 3 SGB V folgender Satz aufgenommen: „Die Zugriffsrechte nach Satz 1 gelten nicht für Daten nach § 341 Absatz 2 Nummer 8." Daten nach § 341 Abs. 2 Nr. 8 SGB V sind die Abrechnungsdaten der Krankenkasse.

[135] Hess, in: Kasseler Kommentar, Stand 8/2024, § 305 SGB V Rn. 4.

[136] Scholz, in: Rolfs/Giesen/Meßling/Udsching, Beck'scher Online-Kommentar Sozialrecht, 79. Edition 12/2025, § 305 SGB V Rn. 10.

elektronischer Patientenakten übermittelt.[137] Auf diesen Grundlagen können versicherte Personen überprüfen, ob gegebenenfalls Berichtigungen von gestellten Diagnosen angezeigt sind.

9.2.1 Erhebung von Diagnosedaten durch gesetzliche Krankenkassen

Zunächst stellt sich in diesem Kontext die Frage, auf welchen Wegen die Diagnosedaten von den Leistungserbringern (das sind die behandelnden Ärzte) zu den gesetzlichen Krankenkassen gelangen. § 295 SGB V sieht entsprechende Übermittlungspflichten vor. So sind die an der vertragsärztlichen Versorgung teilnehmenden Ärzte und Einrichtungen nach § 295 Abs. 1 Satz 1 Nr. 1, Satz 10 SGB V verpflichtet, die von ihnen festgestellten Arbeitsunfähigkeitsdaten unter Angabe der Diagnosen unmittelbar elektronisch an die Krankenkasse zu übermitteln. Zugleich müssen unter anderem die ärztlichen Behandlungen mit den Diagnosen an die Kassenärztlichen Vereinigungen übermittelt werden (§ 295 Abs. 1 Satz 1 Nr. 2 SGB V). Die Kassenärztlichen Vereinigungen haben in diesen Fällen unter anderem die (verschlüsselten) Diagnosen wiederum gesammelt für jedes Quartal und jeden Behandlungsfall an die Krankenkassen zu übermitteln. Dies ergibt sich aus § 295 Abs. 2 Satz 1 Nr. 1, Nr. 2 und Nr. 6 SGB V.[138]

9.2.2 Grundsätzlich keine Berichtigung der ursprünglich übermittelten Diagnosedaten und keine erneute Übermittlung an die Krankenkassen

Soweit die Leistungserbringer oder die Kassenärztlichen Vereinigungen unrichtige Diagnosedaten an die Krankenkasse übermitteln, können diese grundsätzlich nicht berichtigt werden. § 303 Abs. 4 Satz 2 SGB V verbietet regelmäßig eine nachträgliche Änderung oder Ergänzung von an die Krankenkassen übermittelten unrichtigen Diagnosedaten.

Die Leistungserbringer haben zwar in bestimmten Fällen die Möglichkeit, Abrechnungsdaten direkt bei der Kassenärztlichen Vereinigung korrigieren zu lassen. In diesen Fällen erhalten sie nach der positiven Prüfung durch die Kassenärztliche Vereinigung einen geänderten Honorarbescheid. Die jeweilige Krankenkasse erhält sodann die geänderten Abrechnungsdaten von der Kassenärztlichen Vereinigung im Rahmen der nächsten Quartalsabrechnung. Allerdings hat dies keinen Einfluss auf die bei der Krankenkasse vorliegenden (gegebenenfalls unrichtigen) Diagnosedaten. Auch können weder die Krankenkassen noch die versicherten Personen selbst dieses Verfahren eigenständig in Gang setzen.

Hintergrund des Änderungsverbots von § 303 Abs. 4 Satz 2 SGB V ist, dass eine einseitige Nachcodierung bestimmter Versichertenkollektive durch die damit einhergehende Veränderung der Mittelzuweisungen aus dem Gesundheitsfonds den morbiditätsorientierten Risikostrukturausgleich und damit den fairen Wettbewerb zwischen den Krankenkassen gefährden würde.[139] Das Verbot erfasst Datenübermittlungen an die Krankenkassen, unabhängig davon, ob sie unmittelbar von den

[137] Scholz, in: Rolfs/Giesen/Meßling/Udsching, Beck'scher Online-Kommentar Sozialrecht, 79. Edition 12/2025, § 305 SGB V Rn. 10b.

[138] Vgl. Hess, in: Kasseler Kommentar, Stand: 8/2024, § 295 SGB V Rn. 13.

[139] Scholz, in: Rolfs/Giesen/Meßling/Udsching, Beck'scher Online-Kommentar Sozialrecht, 79. Edition 12/2025, § 303 SGB V Rn. 1.

Leistungserbringern oder über die Kassenärztlichen Vereinigungen erwirkt werden.[140] Eine Ausnahme besteht nach § 303 Abs. 4 Satz 1 SGB V, wenn Datenübermittlungen zu Diagnosen nach §§ 295 und 295a SGB V aufgrund technischer Übermittlungs- oder formaler Datenfehler fehlerhaft oder unvollständig sind. Nur in solchen Fällen ist eine erneute Übermittlung durch die Leistungserbringer oder die Kassenärztliche Vereinigung (vgl. die Fallgruppen oben unter Nr. 9.2.1) in korrigierter oder ergänzter Form zulässig.

9.2.3 Ausnahme: Verwendung berichtigter Diagnosedaten durch die Krankenkassen bei Unterrichtung der versicherten Person oder Übermittlung an Dritte

Nach § 305 Abs. 1 Satz 6 SGB V[141] haben die Krankenkassen auf Antrag der Versicherten und abweichend von § 303 Abs. 4 SGB V Diagnosedaten, die ihnen nach den §§ 295 und 295a SGB V übermittelt wurden und deren Unrichtigkeit durch einen ärztlichen Nachweis belegt wird, in berichtigter Form bei der Unterrichtung nach Satz 1 und bei der Übermittlung nach den Sätzen 2 und 3 zu verwenden.

Voraussetzung für eine derartige Berichtung von Diagnosedaten ist zum einen, dass die versicherte Person einen Antrag auf Berichtigung im Sinne von Art. 16 DSGVO an die jeweilige Krankenkasse stellt („auf Antrag"). Zum anderen muss dem Antrag ein ärztlicher Nachweis über die Unrichtigkeit der Diagnose beiliegen. Der ärztliche Nachweis über die Unrichtigkeit der bisherigen Diagnosedaten sollte in der Regel dem Leistungserbringer stammen, der die ursprüngliche Diagnose gestellt und abgerechnet hat.[142]

Liegen diese Voraussetzungen vor, muss die Krankenkasse die versicherte Person unter Verwendung berichtigter Diagnosedaten unterrichten. Soweit die versicherte Person bereits einmal über die (unrichtigen) Diagnosen unterrichtet wurde, muss diese Unterrichtung folglich in berichtigter Form wiederholt werden.[143] Soweit die versicherte Person die Unrichtigkeit aus der elektronischen Patientenakte oder einer persönlichen elektronischen Gesundheitsakte entnommen hat, muss die Krankenversicherung die Diagnosen (nochmals) in berichtigter Form an den jeweiligen Anbieter übermitteln.[144] Die von den Leistungserbringern oder den Kassenärztlichen Vereinigungen übermittelten unrichtigen Daten werden jedoch aufgrund des § 303 Abs. 4 Abs. 2 SGB V weiter in der ursprünglichen und damit unrichtigen Form bei der Krankenkasse vorgehalten. An diesen darf nichts geändert werden.

So wird gewährleistet, dass der Datenbestand bei den Krankenkassen unverändert bleiben kann, die betroffenen Personen aber gleichwohl eine berichtigte Auskunft zur weiteren Verwendung erhalten und vor allem auch in der elektronischen Patientenakte nur korrigierte (zutreffende) Diagnosedaten enthalten sind. Einen (ordnungsgemäßen und vollständigen, vgl. oben) Antrag nach § 305 Abs. 1 Satz 6

[140] Scholz, in: Rolfs/Giesen/Meßling/Udsching, Beck'scher Online-Kommentar Sozialrecht, 79. Edition 12/2025, § 303 SGB V Rn. 5.
[141] Dabei handelt es sich um eine vergleichsweise neue Vorschrift, die am 20. Oktober 2020 in Kraft getreten ist.
[142] Vgl. Bundestags-Drucksache 19/18793, S. 98.
[143] Scholz, in: Rolfs/Giesen/Meßling/Udsching, Beck'scher Online-Kommentar Sozialrecht, 79. Edition 12/2025, § 305 SGB V Rn. 13.
[144] Scholz a. a. O.

SGB V haben die Krankenkassen innerhalb von vier Wochen nach Erhalt des Antrags zu bescheiden (§ 305 Abs. 1 Satz 7 SGB V).

9.2.4 Ergebnis der Beschwerdeverfahren: Anpassung der Berichtigungsverfahren der betroffenen Krankenkasse

Den mir vorliegenden Beschwerden lag im Wesentlichen das Problem zu Grunde, dass die Rechtslage in die internen Verfahrensabläufe noch nicht umfassend implementiert war.

Die beantragte Berichtigung der unzutreffenden Diagnosen wurde zwar nicht pauschal abgelehnt, allerdings wollte die betroffene Krankenkasse die Kassenärztliche Vereinigung in den Prozess (vorab) einbinden und wohl das Änderungsverfahren aufgrund eines Änderungsantrags der Leistungserbringer „in Gang setzen“ (vgl. dazu oben unter Nr. 1.2.2). Dies war –wohl auch mangels rechtlicher Möglichkeiten, die Leistungserbringer zur Antragsstellung zu bewegen – schwierig umzusetzen und nahm entsprechend viel Zeit in Anspruch. Da die betroffenen Personen die berichtigten Auskünfte jedoch zeitnah benötigten und die in § 305 Abs. 1 Satz 7 SGB V gesetzlich vorgeschriebene Frist von vier Wochen nicht einzuhalten war, wandten sich die Versicherten an mich.

Im Rahmen eines intensiven – auch persönlichen – Austausches konnte ich der Krankenkasse die geltende Rechtslage erläutern und auf sie einwirken, ihre Verfahrensabläufe und die Gestaltung der verwendeten Fachanwendung entsprechend anzupassen. Im Ergebnis können die Berichtigungsanträge nach § 305 Abs. 1 Satz 6 SGB V zukünftig innerhalb der vorgesehenen Frist geprüft und die versicherten Personen über gegebenenfalls berichtigte Diagnosen unterrichtet sowie gegebenenfalls berichtigte Diagnosen an die Anbieter persönlicher elektronischer Gesundheitsakten oder Anbieter der elektronischen Patientenakte übermittelt werden.

9.3 Neues zum Mammographie-Screening-Programm

9.3.1 Aktuelle Kurz-Information „Einladungen zum Mammographie-Screening“

Bürgeranfragen zu datenschutzrechtlichen Fragestellungen rund um das Mammographie-Screening-Programm erreichen mich weiterhin.

Das Mammographie-Screening-Programm zielt auf eine Früherkennung von Brustkrebs. Das Angebot richtet sich an für Frauen im Alter zwischen 50 und 75 Jahren als besonders gefährdete Bevölkerungsgruppe. In Bayern erhalten anspruchsberechtigte Frauen die Einladungsschreiben zur Reihenuntersuchung von der „Zentralen Stelle Mammographie-Screening Bayern“, einer gemeinsamen Einrichtung der bayerischen Krankenkassen und der Kassenärztlichen Vereinigung Bayerns. Die Zentrale Stelle erhält die Kontaktdaten einzuladender Frauen durch regelmäßige Übermittlungen aus dem zentralen Meldedatenbestand, der von den örtlichen Melderegistern beschickt wird. Der ersten Einladung kann nicht widersprochen werden. Was die weiteren Einladungen betrifft, ist ein voraussetzungsloses Widerspruchsrecht geregelt (vgl. hierzu auch den 23. Tätigkeitsbericht 2008 unter Nr. 15.2 und den 24. Tätigkeitsbericht 2010 unter Nr. 2.2.7).

Ich nahm die aktuellen Beschwerden zum Anlass, insbesondere die rechtlichen Grundlagen der Datenverarbeitungen im Rahmen des Mammographie-Screening-Programms sowie die vorhandenen Widerspruchsmöglichkeiten in einer Aktuellen Kurz-Information genauer zu erläutern.[145]

9.3.2 Online-Kontaktformular

Weiterhin habe ich das Online-Kontaktformular zum Mammographie-Screening-Programm auf der Homepage der Zentralen Stelle Mammographie-Screening Bayern überprüft. Im Ergebnis habe ich festgestellt, dass nicht alle im Formular geforderten Daten für den festgelegten Verarbeitungszweck erforderlich waren.

Dem Grundsatz der Datenminimierung (vgl. Art. 5 Abs. 1 Buchst. c DSGVO) entsprechend müssen auch die im Kontaktformular vorgesehenen Pflichtangaben „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein". Mir erschien die zwingende Abfrage des Geburtsdatums als nicht notwendig, wenn es bei der Kontaktaufnahme um die Anforderung von allgemeinem Informationsmaterial ging. Auch die Pflichtangabe einer E-Mail-Adresse hielt ich nicht für angezeigt, wenn gleichzeitig die Postadresse abgefragt oder angegeben wird.

Zudem habe ich das Angebot einer verschlüsselten E-Mail-Kommunikation vermisst, um die Vertraulichkeit der Datenübermittlung im Rahmen der Kontaktaufnahme zu ermöglichen (vgl. Art. 5 Abs. 1 Buchst. f DSGVO). Die Kommunikation per unverschlüsselter E-Mail birgt die Gefahr einer unberechtigten Kenntnisnahme, so dass den Nutzerinnen eine sichere Alternative angeboten werden sollte. Damit kommt der Verantwortliche seiner Pflicht nach, die Verarbeitung auch aus technischer Sicht sicher zu gestalten und vor unberechtigten Zugriffen zu schützen (vgl. Art. 32 DSGVO).

Im Ergebnis hat die Zentrale Stelle meinen Hinweisen Rechnung getragen und die Kontaktformulare auf ihrer Internetseite überarbeitet. Sie hält nun je nach Zweck der Datenerhebung unterschiedliche Formulare vor. Dabei konnten die Pflichtfelder entsprechend angepasst werden. Auch eine verschlüsselte E-Mail-Kommunikation wird nun optional angeboten.

[145] Bayerischer Landesbeauftragter für den Datenschutz, Einladungen zum Mammographie-Screening – datenschutzkonform?, Aktuelle Kurz-Information 59, Stand 3/2025, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

10 Soziales

Über den Bereich der landesunmittelbaren Krankenkassen hinaus nehme ich die Datenschutzaufsicht bei zahlreichen bayerischen öffentlichen Stellen wahr, die Aufgaben von Sozialleistungsträgern wahrnehmen oder sonst datenschutzrechtliche Vorgaben aus dem Sozialgesetzbuch anzuwenden haben.

Zahlreiche Beschwerden gingen mir von Bürgerinnen und Bürgern zu, die mit der Arbeit bayerischer Jugendämter nicht zufrieden waren. Oftmals konnte ich hier schon aus dem Grunde nicht weiterhelfen, dass die Gegenstände der Auseinandersetzung außerhalb des Datenschutzrechts lagen. Enthielt eine Beschwerde eine für mich prüfbare datenschutzrechtliche Frage, blieb das Ergebnis des Beschwerdeverfahrens gleichwohl oft hinter dem zurück, was Beschwerdeführer oder Beschwerdeführerinnen erhoffen. In diesem Zusammenhang möchte ich daran zu erinnern, dass das Datenschutzrecht nur den Schutz des Rechts auf informationelle Selbstbestimmung bezweckt und auch nur darauf bezogene Verfahrensergebnisse haben kann. Wird eine Datenschutzbeschwerde mit einer über diesen Zweck hinausreichenden allgemeinen Gerechtigkeitserwartung erhoben, ist eine Enttäuschung meist vorprogrammiert. Gleichwohl binden Beschwerden mit entsprechendem Hintergrund personelle Kapazitäten in meiner Dienststelle in einem ganz erheblichen Umfang.

Berichten möchte ich diesmal über einige ganz andere, rechtlich interessante Vorgänge aus der Welt des Sozialdatenschutzes. So habe ich mich erstmals mit der Frage befasst, ob eine Schwärzung auch eine Weißung sein darf (Nr. 10.1). Die Überlegungen dazu dürften außerhalb des Sozialdatenschutzrechts ebenfalls Bedeutung erlangen können. Werden Kinder mit hohem Einkommen von einem Sozialleistungsträger wegen „vorgeschossenen“ Elternunterhalts in Anspruch genommen, weniger einkommensstarke Geschwister dagegen nicht, kann der einkommensbezogene „Informationsfluss“ Datenschutzbeschwerden veranlassen – Nr. 10.2 erläutert die Problemstellung exemplarisch. Erteilt eine Behörde eine Erlaubnis zur Kindertagespflege, möchte sie wissen, ob die Kinder bei der Tagespflegeperson in guten Händen sind. Nicht jeder schätzt hier einen allzu gründlichen Blick auf die eigene Vergangenheit; wo die Grenzen liegen, habe ich unter Nr. 10.3 herausgearbeitet. Datenflüsse zwischen Ausländerbehörden und Sozialleistungsträgern waren bereits Gegenstand meines 34. Tätigkeitsberichts 2024 (dort unter Nr. 4.2). Das Thema ist aber noch nicht erschöpft, wie Nr. 10.4 zeigt. Nur peripher zum Sozialdatenschutz gehört der letzte Beitrag dieses Abschnitts. Er befasst sich mit der Frage, inwieweit Fachkräfte für Arbeitssicherheit bei bayerischen öffentlichen Stellen an personenbezogene Informationen zu Arbeitsunfällen gelangen können (Nr. 10.5).

10.1 Schwärzung auch durch Weißung bei der Auskunftserteilung?

Mit dem Auskunftsanspruch aus Art. 15 Abs. 1 DSGVO – auch in seiner Ausprägung als Recht auf Kopie (Art. 15 Abs. 3 DSGVO) – sollen betroffene Personen erfahren können, welche sie personenbezogenen Daten von ihnen Verantwortliche verarbeiten. Der Auskunftsanspruch ist aber nicht unbeschränkt gewährt.

Zwar kann die Auskunft über die personenbezogenen Daten auch durch die Aushändigung von kopierten Dokumenten oder Dokumententeilen erteilt werden, wenn diese personenbezogene Daten der betroffenen Person enthalten. Die betroffene Person hat aus Art. 15 DSGVO aber keinen Anspruch auf all jene Informationen, die keine sie betreffenden personenbezogene Daten darstellen, weil es sich etwa um reine Sachdaten handelt. Eine Grenze ziehen zudem Rechte und Freiheiten anderer Personen, wie Art. 15 Abs. 4 DSGVO zeigt. Soll die Auskunft durch die Übermittlung von Dokumentkopien erfüllt werden, kann es für einen Verantwortlichen geboten sein, Informationen unkenntlich zu machen, auf welche die betroffene Person keinen Anspruch hat.

Eine bayerische öffentliche Stelle hatte eine solche Unkenntlichmachung auf einer ausgedruckten E-Mail anstatt durch die übliche Schwärzung einzelner Textstellen mittels einer kaum erkennbaren Weißung bewirkt. Eine Beschwerde griff diesen Umstand auf und kritisierte die fehlende Transparenz bei der Auskunftserteilung. Es ging vorliegend weniger um das „Ob" der Unkenntlichmachung, sondern um das „Wie".

10.1.1 Unkenntlich gemachte Inhalte

Zunächst prüfte ich, welche Informationen aus welchen Gründen in dem betreffenden Dokument unkenntlich gemacht worden waren. Hierzu ließ ich mir von der bayerischen öffentlichen Stelle das originale Dokument ohne Unkenntlichmachungen vorlegen. Es handelte sich um eine ausgedruckte dienstliche E-Mail, die der Verfasser mit persönlichen Bemerkungen versehen hatte. Der Verfasser hatte diese Bemerkungen selbst weiß übermalt, bevor sie Teil eines Datenkonvoluts wurden, das dann zum Zwecke der Auskunftserfüllung an die betroffene Person herausgegeben wurde.

10.1.1.1 Bemerkungen ohne Personenbezug

Bei den übermalten Passagen handelte es sich einerseits um persönliche Bemerkungen des Verfassers der E-Mail ohne Bezug zu der auskunftssuchenden Person. Insoweit kam es nicht auf eine mögliche Einschränkung der Auskunftserteilung gemäß Art. 15 Abs. 4 DSGVO an, weil keine personenbezogenen Daten des Beschwerdeführers vorlagen und insoweit kein Anspruch gemäß Art. 15 Abs. 1 Satz 1, Abs. 3 DSGVO bestand, der einzuschränken gewesen wäre.

10.1.1.2 Bemerkungen mit Personenbezug

Eine andere mittels Weißung unkenntlich gemachte Passage enthielt eine persönliche Bemerkung des E-Mail-Verfassers zur Situation der betroffenen Person. Insoweit war zu prüfen, ob ein ihn betreffendes personenbezogenes Datum vorlag:

Nach Art. 4 Nr. 1 DSGVO sind „personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Der weit zu verstehende Begriff umfasst potenziell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur in Form von Stellungnahmen oder Beurteilungen, unter der Voraussetzung, dass es sich um Informationen über die in

Rede stehende Person handelt.[146] Diese Voraussetzung ist erfüllt, wenn die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft ist.[147] Die fragliche Bemerkung in der E-Mail stellte sowohl inhaltlich als auch durch den Zweck der Verarbeitung einen Bezug zur Person des Beschwerdeführers her. Der inhaltliche Bezug wurde mittelbar durch Bezugnahme auf seine Situation hergestellt. Der Zweck der Verarbeitung lag in der Kommentierung eines den Beschwerdeführer betreffenden Sachverhalts.

Soweit dieses Datum mittels Weißung unkenntlich gemacht und somit dem Beschwerdeführer mit der Auskunft nicht zugänglich gemacht werden sollte, hätte die öffentliche Stelle zunächst prüfen müssen, ob sie den Auskunftsanspruch zulässig einschränken konnte. In Betracht wäre aufgrund einer möglichen Beeinträchtigung der Rechte und Freiheiten des E-Mail-Verfassers etwa eine Einschränkung gemäß Art. 15 Abs. 4 DSGVO gekommen. Anderenfalls hätte dieses personenbezogene Datum der auskunftsuchenden Person fristgemäß zur Verfügung gestellt werden müssen. Ich habe bei meiner Prüfung angenommen, dass an diesem Datum ein nur geringes Informationsinteresse des Beschwerdeführers bestand und sich das entgegenstehende Datenschutzgrundrecht im Rahmen von Art. 15 Abs. 4 DSGVO hätte durchsetzen können. Eine Unkenntlichmachung wäre somit zwar grundsätzlich in Betracht gekommen.

10.1.2 Transparenzprobleme bei Unkenntlichmachungen mittels Weißungen

Die Unkenntlichmachung der Passagen in der E-Mail war aber durch schwer erkennbare Weißung und nicht durch leicht wahrnehmbare Schwärzung bewirkt worden. Der Beschwerdeführer sah darin einen Verstoß gegen den in Art. 12 Abs. 1 Satz 1 DSGVO geregelten Transparenzgedanken und gegen den Transparenzgrundsatz aus Art. 5 Abs. 1 Buchst a DSGVO. Für ihn seien die Unkenntlichmachungen mittels Weißung nur per Zufall erkennbar gewesen; Ziel sei eine Verschleierung der Unvollständigkeit gewesen.

Gemäß Art. 12 Abs. 1 Satz 1 DSGVO trifft der Verantwortliche geeignete Maßnahmen, um der betroffenen Person unter anderem alle Mitteilungen gemäß Art. 15 DSGVO, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Gemäß Art. 5 Abs. 1 Buchst. a DSGVO müssen personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

10.1.2.1 Bezug des Transparenzgrundsatzes zu personenbezogenen Daten

Art. 12 Abs. 1 Satz 1 DSGVO betrifft Maßnahmen des Verantwortlichen, die sich auf eine Verarbeitung beziehen. Gemeint ist dabei die Verarbeitung der personenbezogenen Daten der betroffenen Person. Die Regelung enthält unter anderem Vorgaben zur Bereitstellung von Informationen für die betroffene Person im Zusammenhang mit der Verarbeitung sie betreffender personenbezogener Daten und zur Ausgestaltung der Kommunikation zwischen Verantwortlichem und betroffener Person im Hinblick auf die datenschutzrechtlichen Betroffenenrechte.[148]

[146] Vgl. Bundesgerichtshof, Urteil vom 15. Juni 2021, VI ZR 576/19, BeckRS 2021, 16831, Rn. 22.
[147] Vgl. Europäischer Gerichtshof, Urteil vom 20. Dezember 2017, C-434/16, Rn. 35.
[148] Vgl. Artikel 29-Datenschutzgruppe, Leitlinien für Transparenz gemäß der Verordnung

Die Transparenzanforderung in Art. 12 Abs. 1 Satz 1 DSGVO soll betroffene Personen in die Lage versetzen, den Umfang und die Konsequenzen der Datenverarbeitung beurteilen zu können.[149] Die Umsetzung der Transparenzanforderung in Art. 12 Abs. 1 Satz 1 DSGVO erfordert also einen Bezug zu den personenbezogenen Daten der betroffenen Person.

Der Bezug zu den personenbezogenen Daten der betroffenen Person ergibt sich beim Transparenzgrundsatz gemäß Art. 5 Abs. 1 Buchst. a DSGVO direkt aus dem Gesetzeswortlaut. Soweit personenbezogene Daten der auskunftsuchenden Person in Dokumenten zum Zwecke der Auskunftserteilung unkenntlich gemacht werden, handelt es sich nach meiner Einschätzung um eine Verarbeitung dieser personenbezogenen Daten gemäß Art. 4 Nr. 2 DSGVO, die dem Transparenzgrundsatz genügen muss. Das bedeutet, dass diese Verarbeitung in Form der Unkenntlichmachung der personenbezogenen Daten der betroffenen Person zumindest nachvollziehbar und somit ersichtlich sein muss.

10.1.2.2 Kein Transparenzproblem bei Informationen ohne Personenbezug

Regelmäßig anders stellt sich die Situation bei Informationen dar, die gar keine personenbezogenen Daten der betroffenen Person enthalten. Solche Informationen sind – von den Metainformationen abgesehen – nicht Gegenstand des Auskunftsrechts aus Art. 15 Abs. 1, 3 DSGVO. Auch die Transparenzanforderungen sind insoweit nicht zu beachten. Dass dies konsequent ist, zeigt folgender Wertungsvergleich:

Erfüllt der Verantwortliche gemäß Art. 15 Abs. 1 DSGVO die Auskunft über die konkret verarbeiteten personenbezogenen Daten der betroffenen Person – was grundsätzlich zulässig ist – in Form einer strukturierten Zusammenstellung, ist für die betroffene Person gar nicht ersichtlich, dass Informationen, die keine personenbezogenen Daten darstellen, weggelassen wurden. Denn die der betroffenen Person zur Verfügung gestellten Daten wurden zuvor vom Verantwortlichen ausgewählt, überschießende Informationen, die nicht der Auskunft unterfallen, wurden weggelassen. Handelt es sich dabei nicht um personenbezogene Daten der auskunftsbegehrenden betroffenen Person, muss diese Entfernung auch nicht transparent gemacht werden. Für die betroffene Person ist dann nicht ersichtlich, welche Daten aus Dokumenten, Akten oder anderen Unterlagen in die Auskunft übernommen wurden und welche nicht. Der Auswahlprozess wird ihr nicht offengelegt. In diesem Fall stellt sich kein Transparenzproblem wegen einer etwaigen Unkenntlichmachung von Informationen; dies freilich unter dem Vorbehalt, dass eine solche strukturierte Zusammenstellung personenbezogener Daten im konkreten Fall die Anforderungen des Art. 12 Abs. 1 Satz 1 DSGVO an eine präzise, verständliche und transparente Auskunftserteilung erfüllt.

Anders liegt der Fall einer Auskunftsbeschränkung hinsichtlich personenbezogener Daten der betroffenen Person – selbst bei einer Auskunftserfüllung mittels strukturierter Zusammenstellung. Im Fall einer gesetzlichen Auskunftsbeschränkung ist die betroffene Person stets auf die Einschränkung der Auskunft hinzuweisen; die Beschränkung ist zu begründen (vgl. neben den Vorgaben in Art. 15 Abs. 4

2016/679, WP 260 rev. 01, S. 4, Internet: https://www.datenschutzkonferenz-online.de, Rubrik „Infothek – Leitlinien der Artikel-29-Gruppe".

[149] Vgl. Pohle/Spittka, in: Taeger/Gabel, DSGVO/BDSG/TTDSG, 4. Aufl. 2022, Art. 12 DSGVO Rn. 9.

DSGVO auch Art. 10 Abs. 3 Satz 1 BayDSG, § 83 Abs. 3 Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz –).

10.1.2.3 Auswirkungen des Transparenzproblems

Der Auskunftsanspruch kann sich aber auch auf die Herausgabe von Kopien von Dokumenten im Rahmen von Art. 15 Abs. 1 und Abs. 3 DSGVO verdichten, insbesondere wenn diese eine Vielzahl personenbezogener Daten der betroffenen Person umfassen. Einen Anspruch auf die Kopie eines Dokuments oder auf einen Auszug aus einer Datenbank hat die betroffene Person, wenn sie nur so erkennen kann, in welchem Zusammenhang ihre Daten verwendet werden.[150] Soweit die Auskunft durch die Übermittlung von Kopien von Dokumenten erfüllt werden soll und dabei Unkenntlichmachungen an personenbezogenen Daten der betroffenen Person für diese nicht ersichtlich vorgenommen werden, wirkt sich ein mögliches Transparenzproblem aus.

Unkenntlichmachungen, die für die betroffene Person nicht oder nur sehr schwer ersichtlich sind, können sich für sie rechtsschutzverkürzend auswirken. Zwar sieht die Datenschutz-Grundverordnung insoweit keine konkreten Formvorgaben etwa zur farblichen Gestaltung vor. Vor diesem Hintergrund lassen sich dem Gesetz keine eindeutigen Anforderungen zu der Frage entnehmen, wie Unkenntlichmachungen genau vorzunehmen sind. Gleichwohl ist für eine betroffene Person bei einer Unkenntlichmachung nicht ersichtlich, was sich hinter der unkenntlich gemachten Passage verbirgt. Es kann sich aus ihrer Sicht immer um personenbezogene Daten handeln, die ihr im Rahmen der Auskunftserteilung eigentlich offen zu legen wären.

Erfahrungsgemäß wird sich das Auskunftsinteresse der betroffenen Person auf bestimmte personenbezogene Daten, gegebenenfalls in bestimmten Dokumenten fokussieren. Für sie besteht dann die Möglichkeit – etwa im Rahmen einer Datenschutzbeschwerde – die Rechtmäßigkeit der Unkenntlichmachung und somit die Beschränkung der Auskunft überprüfen zu lassen.

Ist die Unkenntlichmachung am betreffenden Dokument aber nicht erkennbar – wie etwa im Falle einer Weißung auf weißem Untergrund – und wird – wie vorliegend – die betroffene Person nicht anderweitig auf die Unkenntlichmachung hingewiesen, so wird sie das Dokument im Zweifel für vollständig halten und eine Überprüfung durch mich nicht in Betracht ziehen.

10.1.2.4 Transparenzverstoß

Somit war jedenfalls die Weißung derjenigen Passage, die ein personenbezogenes Datum des Beschwerdeführers enthielt, kritisch zu würdigen. Dieses personenbezogene Datum wurde dem Beschwerdeführer nicht offengelegt. Die insoweit erfolgte Beschränkung der Auskunft wurde nicht transparent gemacht. Ich habe dieses Defizit als Verstoß gegen Art. 12 Abs. 1 Satz 1 DSGVO und Art. 5 Abs. 1 Buchst. a DSGVO gewertet.

Gegenüber der bayerischen öffentlichen Stelle habe ich daher eine Verwarnung ausgesprochen (Art. 58 Abs. 2 Buchst. b DSGVO). Die öffentliche Stelle hat mir

[150] Vgl. Europäischer Gerichtshof, Urteil vom 4. Mai 2023, C-487/21, Rn. 41.

versichert, dass sie bei der Erfüllung von Rechten der betroffenen Person zukünftig keine Weißungen mehr vornehmen wird, sondern auf leichter erkennbare Unkenntlichmachungen zurückgreift.

10.1.3 Abschließende Bemerkungen

Allgemein ist zu beachten, dass Weißungen auch in Fällen, die datenschutzrechtlich nicht zu Transparenzproblemen führen (also etwa Informationen betreffen, die keine Daten der betroffenen Person sind) generell ein vermeidbares Eskalationspotential mit sich bringen. Weißungen können bei betroffenen Personen schnell den Verdacht einer Verschleierung wichtiger Informationen durch die öffentliche Stelle aufkommen lassen, der in den Vorwurf der Intransparenz mündet. Zulässige Unkenntlichmachungen sollten daher stets leicht erkennbarsein. Auf weißem Untergrund ist die klassische Schwärzung einer Weißung daher vorzuziehen.

Im Übrigen gibt die Beschwerde Anlass, Folgendes zu verdeutlichen:

Dienstlicher Schrift- oder E-Mail-Verkehr sollte stets den Gepflogenheiten entsprechen, die bei ordnungsgemäßer Akten- und Vorgangsbearbeitung zu erwarten sind. Unbedachte persönliche Kommentare und Bemerkungen haben in dienstlichem Schriftverkehr nichts verloren und wecken leicht den Wunsch nach einer Unkenntlichmachung, wenn etwa Auskunft zu erteilen ist. Der Begriff der personenbezogenen Daten wird von der Rechtsprechung sehr weit gefasst. Auch interner Schriftverkehr, Vermerke und andere Dokumente, die personenbezogene Daten betroffener Personen enthalten, können jederzeit zum Gegenstand eines Auskunftsrechts gemäß Art. 15 DSGVO gemacht werden. Über den Anwendungsbereich von Art. 15 DSGVO hinaus, der sich nur auf die eigenen personenbezogenen Daten der betroffenen Person bezieht, können auch andere Informationszugangsrechte wie etwa Art. 39 Abs. 1 Satz 1 BayDSG zu einer – unter Umständen noch weiter reichenden – Beauskunftung führen. Dies sollte bei der formellen und inhaltlichen Führung von Akten, insbesondere auch bei interner E-Mail-Kommunikation immer bedacht werden.

10.2 Offenlegung von Angaben über die Höhe des Einkommens von Kindern bei Verfahren zur Gewährung von Grundsicherung an die Eltern

Eine betroffene Person wandte sich mit der Rüge an mich, dass eine kreisfreie Stadt als Sozialleistungsträger unbefugt Einkommensdaten an die Geschwister offengelegt habe. Hintergrund war die Gewährung von Leistungen der Grundsicherung im Alter an die gemeinsamen Eltern. In einem Schreiben an die Geschwister hatte die Stadt insbesondere erkennen lassen, dass die betroffene Person über ein „jährliches Gesamteinkommen [...] von mehr als 100.000 EUR“ verfüge.

Die Stadt war der Auffassung, dass aufgrund der gesetzlichen Vorgaben Auskunftsersuchen an die potentiell haftenden Personen gerichtet werden müssten. Sie sei verpflichtet, die wirtschaftlichen Verhältnisse und insbesondere die Haftungsanteile der Kinder zu ermitteln. Aus ihrer Sicht könne die allgemein gehaltene Offenlegung der Höhe des Einkommens gegenüber den Geschwistern auf die Vorschriften des Sozialdatenschutzrechts gestützt werden.

10.2.1 Übergang von Unterhaltsansprüchen auf den Träger der Sozialhilfe

Für die Gewährung von Grundsicherungsleistungen im Alter sehen die Vorschriften des Zwölften Buchs Sozialgesetzbuch vor, dass ein eventueller Unterhaltsanspruch der Eltern bis zur Höhe der geleisteten Aufwendungen auf den Träger der Sozialhilfe (im Fall die Stadt) übergeht, vgl. § 94 Abs. 1 Satz 1 Zwölftes Buch Sozialgesetzbuch – Sozialhilfe – (SGB XII).

Als Ausnahme hiervon sind jedoch Unterhaltsansprüche der Eltern gegenüber ihren Kindern nicht zu berücksichtigen, es sei denn, dass das jährliche Gesamteinkommen der Kinder jeweils mehr als 100.000 EUR beträgt (sogenanntes Jahreseinkommensgrenze). Unterhalb dieser Grenze ist der Übergang von Unterhaltsansprüchen der Eltern auf den Sozialleistungsträger ausgeschlossen (§ 94 Abs. 1a Satz 1 und 2 SGB XII). Mit dieser Regelung beabsichtigte der Gesetzgeber, auf das Einkommen der unterhaltspflichtigen Kinder von Eltern, die Grundsicherung im Alter beziehen, erst ab einer Höhe von mehr als 100.000 EUR im Jahr zurückzugreifen. Damit sollte eine Entlastung unterhaltspflichtiger Kinder im Verhältnis zu den Sozialleistungsträgern bewirkt werden.[151]

Für den Fall mehrerer gleich naher Verwandter (wie etwa mehrerer Kinder) gilt, dass diese anteilig haften, und zwar nach ihren Erwerbs- und Vermögensverhältnissen (§ 1606 Abs. 3 Satz 1 Bürgerliches Gesetzbuch). Dies bedeutet im Hinblick auf den Übergang des Unterhaltsanspruchs auf den Sozialleistungsträger, dass der Anspruch nur insoweit (anteilig) übergeht, als er auch den Eltern zustünde.

10.2.2 Befugnis des Sozialleistungsträgers zur Offenlegung von allgemein gehaltenen Angaben über das Einkommen

Nach den Vorschriften des Sozialdatenschutzrechts ist eine Übermittlung von Sozialdaten unter anderem zulässig, soweit sie erforderlich ist für die Erfüllung der Zwecke, für die sie erhoben worden sind, oder für die Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle nach dem Sozialgesetzbuch, vgl. § 69 Abs. 1 Nr. 1 Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X).

Die Offenlegung von Einkommensdaten der betroffenen Person war in die Einholung einer Auskunft von den Geschwistern der betroffenen Person eingebettet (§ 117 Abs. 1 SGB XII). Macht ein Sozialleistungsträger ein solches Auskunftsbegehren geltend, ist er aus meiner Sicht auch gehalten, gegenüber den Geschwistern den Grund für die Auskunft anzugeben. Dieser Grund lag hier in der Prüfung, in welchem Umfang ein Unterhaltsanspruch der Eltern gegen die betroffene Person auf die Stadt übergeht. Die Prüfung diente daher dem Zweck, den Haftungsanteil der betroffenen Person zutreffend zu bestimmen. Die in dem Schreiben an die Geschwister angesprochene Jahreseinkommensgrenze in Höhe von 100.000 EUR ergibt sich dabei unmittelbar aus den gesetzlichen Vorschriften (§ 94 Abs. 1a Satz 1 SGB XII).

Um der gesetzlichen Aufgabe zur Feststellung des Haftungsanteils nachzukommen, war die Stadt daher befugt, die allgemeine Angabe zur Höhe des Einkom-

[151] Vgl. Bundestags-Drucksache 19/13399, S. 18.

mens („jährliches Gesamteinkommen [...] von mehr als 100.000 EUR") gegenüber den Geschwistern offenzulegen. Auch im Hinblick auf die datenschutzrechtlichen Grundsätze der Erforderlichkeit (Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO) sowie der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) war aus meiner Sicht kein Verstoß zu erkennen, da eine datensparsamere Verarbeitung aufgrund der leistungsrechtlichen Vorgaben, die vorliegend zu beachten waren, nicht in Betracht kam.

Die Offenlegung der allgemein gehaltenen Angabe über das Einkommen der betroffenen Person konnte daher auf die Vorschriften des Sozialdatenschutzrechts gestützt werden (§ 69 Abs. 1 Nr. 1 SGB X). Ich habe gegen das Vorgehen der Stadt in diesem Fall keine Einwände erhoben.

10.3 Eignungsfeststellung im Fall der Kindertagespflege

Eine kreisfreie Stadt wandte sich als Trägerin der öffentlichen Jugendhilfe (vgl. Art. 15 Satz 1 Gesetz zur Ausführung der Sozialgesetze) mit einer Anfrage an mich, welche die Zulässigkeit der Erhebung von Informationen zur Eignungsfeststellung von Kindertagespflegepersonen betraf. Konkret ging es um die Möglichkeit, Informationen über eine Fremdunterbringung oder kindeswohlrelevante Vorfälle hinsichtlich der eigenen Kinder der Bewerberinnen und Bewerber zu gewinnen. Solche Informationen könnten die Eignung der Bewerberin oder des Bewerbers in Frage stellen. Die Stadt hat dazu auf die Rechtsprechung des Bayerischen Verwaltungsgerichtshofs zu behördlichen Aufforderungen hingewiesen, im Rahmen einer Verlängerung der Erlaubnis zur Kindertagespflege eine Auskunft über gespeicherte polizeiliche Daten („Leumundsauskunft") vorzulegen.[152] In diesem Verfahren hatte auch ich eine Stellungnahme abgegeben. Der Bayerische Verwaltungsgerichtshof war seinerzeit zu dem Ergebnis gekommen, dass die Behörde insofern weder um Übermittlung von polizeilichen Daten nachsuchen, noch von der betroffenen Person eine entsprechende Vorlage verlangen könne.[153]

Aus Sicht der Stadt war es fraglich, ob die Erhebung der Informationen bei den zuständigen Jugendämtern gegebenenfalls aufgrund einer Einwilligung der Bewerberinnen und Bewerber möglich sein könnte. Die Stadt hat dabei auch auf eine Stellungnahme des Bayerischen Landesjugendamts Bezug genommen. Danach sollten, wenn sich in einem Gespräch mit der Bewerberin oder dem Bewerber Anhaltspunkte für Ausschlusskriterien ergeben (wie etwa eine Fremdunterbringung oder kindeswohlrelevante Vorfälle in Bezug auf die eigenen Kinder), weitergehende Ermittlungen mit Einwilligung der Bewerberin oder des Bewerbers angestellt werden. Der Träger der öffentlichen Jugendhilfe sei daher befugt, mit einer solchen Einwilligung das zuständige Jugendamt um Übermittlung entsprechender Daten zu ersuchen.

Aufgrund der aus ihrer Sicht divergierenden Verwaltungspraxis in Bayern wandte sich die Stadt mit einer Bitte um Beratung an mich.

[152] Vgl. Bayerischer Verwaltungsgerichtshof, Beschluss vom 5. Dezember 2012, 12 BV 12.526, BeckRS 2013, 47123.

[153] Vgl. Bayerischer Verwaltungsgerichtshof, Beschluss vom 5. Dezember 2012, 12 BV 12.526, BeckRS 2013, 47123, Rn. 35 ff.

10.3.1 Voraussetzungen einer Erlaubnis zur Kindertagespflege

§ 43 Abs. 2 Achtes Buch Sozialgesetzbuch – Kinder- und Jugendhilfe – (SGB VIII) benennt die Voraussetzungen, die eine Bewerberin oder ein Bewerber erfüllen muss, um eine Erlaubnis zur Kindertagespflege zu erhalten. In der Vorschrift heißt es:

> „Die Erlaubnis ist zu erteilen, wenn die Person für die Kindertagespflege geeignet ist. Geeignet im Sinne des Satzes 1 sind Personen, die
> 1. sich durch ihre Persönlichkeit, Sachkompetenz und Kooperationsbereitschaft mit Erziehungsberechtigten und anderen Kindertagespflegepersonen auszeichnen und
> 2. über kindgerechte Räumlichkeiten verfügen.
>
> Sie sollen über vertiefte Kenntnisse hinsichtlich der Anforderungen der Kindertagespflege verfügen, die sie in qualifizierten Lehrgängen erworben oder in anderer Weise nachgewiesen haben. § 72a Absatz 1 und 5 gilt entsprechend."

Bei bestimmten Kategorien von Vorstrafen gilt nach § 72a SGB VIII ein sogenannter Tätigkeitsausschluss für einschlägig vorbestrafte Personen. Zur Prüfung sollen sich die Träger der öffentlichen Jugendhilfe von den Bewerberinnen und Bewerbern (erweiterte) Führungszeugnisse nach § 30 Abs. 5 und § 30a Abs. 1 Bundeszentralregistergesetz vorlegen lassen (§ 43 Abs. 2 Satz 4 in Verbindung mit § 72a Abs. 1 SGB VIII). Die Jugendhilfeträger dürfen aus den Führungszeugnissen nur bestimmte genauer bezeichnete Daten erheben und speichern (Umstand der Einsichtnahme, Datum des Führungszeugnisses und Information, ob die betreffende Person wegen bestimmter Straftaten rechtskräftig verurteilt worden ist, vgl. § 72a Abs. 5 Satz 1 SGB VIII).

10.3.2 Abschließende Regelung über die Erhebung von Daten im Hinblick auf strafrechtliche Verurteilungen

Ich teile die Auffassung des Bayerischen Verwaltungsgerichtshofs, dass der Gesetzgeber durch § 43 Abs. 2 Satz 4 in Verbindung mit § 72a Abs. 1, 5 SGB VIII die Frage der Erhebung von Daten über strafrechtliche Verurteilungen bereichsspezifisch geregelt hat. Eine darüberhinausgehende Befugnis der Jugendämter zur Datenerhebung ist gesetzlich nicht vorgesehen.

Trifft der Gesetzgeber eine solche bereichsspezifische Regelung zur Datenerhebung, sperrt dies in der Regel den Rückgriff auf allgemeine datenschutzrechtliche Befugnisse gleicher Zielrichtung. Im Hinblick auf Daten über strafrechtliche Verurteilungen ist daher ein Rückgriff auf allgemeine Befugnisse zur Erhebung von Sozialdaten im Jugendhilferecht nach §§ 61 ff. SGB VIII ausgeschlossen.[154] In diesem Rahmen sind über das erweiterte Führungszeugnis hinaus keine Nachweise zu erbringen.

[154] Vgl. Bayerischer Verwaltungsgerichtshof, Beschluss vom 5. Dezember 2012, 12 BV 12.526, BeckRS 2013, 47123, Rn. 38.

10.3.3 Keine abschließende Regelung im Hinblick auf andere Aspekte der Eignung

Allerdings ist aus meiner Sicht zu bedenken, dass sich die Ausführungen des Bayerischen Verwaltungsgerichtshofs auf die Erhebung von Daten zu diesem konkreten Aspekt der Eignungsfeststellung – eventuelle strafrechtliche Verurteilungen mit Relevanz für den Auftrag zum Schutz des Kindeswohls – beschränken. Für andere Aspekte der Eignung im Sinne des § 43 Abs. 2 SGB VIII (Persönlichkeit, Sachkompetenz, Kooperationsbereitschaft, kindgerechte Räumlichkeiten, Qualifikation) kann nicht ohne Weiteres eine solche „Sperrwirkung" angenommen werden. Insbesondere die Erhebung von Daten über eventuelle Fremdunterbringungen oder kindeswohlrelevante Vorfälle hinsichtlich der eigenen Kinder der Bewerberinnen und Bewerber kann sich auf andere Aspekte der persönlichen Eignung beziehen, gerade wenn eine strafrechtliche Verurteilung nicht vorliegt und/oder andere Vorwürfe als die in § 72a Abs. 1 SGB VIII genannten inmitten stehen.

In solchen Fällen ist es aus meiner Sicht auch nicht ausgeschlossen, dass Jugendämter die oben beschriebenen Erhebungen auf die allgemeinen gesetzlichen Befugnisse des Sozialdatenschutzrechts stützen (siehe unten, Nr. 10.3.5).

10.3.4 Datenerhebung aufgrund Einwilligung zweifelhaft

Grundsätzlich denkbar wäre es zwar auch, eine Datenerhebung auf Einwilligungen im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO, § 67b Abs. 2 Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X) zu stützen. Dabei sind jedoch die besonderen Anforderungen an das Vorliegen einer wirksamen Einwilligung (vgl. Art. 7 und Art. 4 Nr. 11 DSGVO) zu beachten. Geht es – wie hier – um die Einholung einer Einwilligung durch eine Behörde, ist insbesondere die Freiwilligkeit der Einwilligung genau zu prüfen.

Wie sich Erwägungsgrund 43 DSGVO entnehmen lässt, ist die Freiwilligkeit vor allem dann zweifelhaft, wenn zwischen der betroffenen Person und dem Verantwortlichen ein „klares Ungleichgewicht" besteht, insbesondere wenn es sich bei dem Verantwortlichen – wie hier – um eine Behörde handelt, und es in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass eine Einwilligung freiwillig erteilt würde. Die Beweislast für das Vorliegen einer wirksamen Einwilligung liegt gemäß Art. 5 Abs. 2, 7 Abs. 1 DSGVO bei der Behörde. Mit der Freiwilligkeit der Einwilligung bei bestehendem Machtungleichgewicht habe ich mich auch in meiner Orientierungshilfe zur Einwilligung näher befasst.[155]

Gerade wenn eine Bewerberin oder ein Bewerber einen Antrag auf Erlaubnis zur (entgeltlichen) Kindertagespflege nach § 43 Abs. 1 SGB VIII stellt, liegt es aus meiner Sicht nahe, dass sich die betroffenen Personen faktisch unter Druck gesetzt fühlen, ein Einwilligungsformular oder ähnliches zu unterzeichnen, um die begehrte Erlaubnis zu erhalten. Ohne die Erteilung dieser Erlaubnis bestünde keine Möglichkeit, der Tätigkeit „Kindertagespflege" nachzugehen. Ich habe daher darauf hingewiesen, dass eine Erhebung von Informationen der Jugendämter auf-

[155] Bayerischer Landesbeauftragter für den Datenschutz, Die Einwilligung nach der Datenschutz-Grundverordnung, Orientierungshilfe, Stand 9/2021, Rn. 71 ff., Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

grund einer Einwilligung keinesfalls regelhaft stattfinden und im Einzelfall sorgfältig geprüft werden muss, ob die Freiwilligkeit der Einwilligung tatsächlich gewährleistet werden kann.

Sofern der zuständigen Behörde eine gesetzliche Verarbeitungsbefugnis zur Verfügung steht, wird der Spielraum für eine Verarbeitung aufgrund Einwilligung noch enger ausfallen. In einem solchen Fall darf den Bewerberinnen oder Bewerbern nicht in irreführender Weise eine Entscheidungsmacht über die Verarbeitung suggeriert werden, die tatsächlich nicht besteht. Ein Rückgriff auf eine Einwilligung wird dann allenfalls in Betracht kommen können, wenn die betroffene Person im Vorfeld deutlich darüber informiert wird, dass die Erhebung alternativ auch auf eine gesetzliche Verarbeitungsbefugnis gestützt werden könnte. Ich habe die Stadt darauf hingewiesen, dass ich von einem großzügigen Einholen von Einwilligungen als „Ersatzrechtsgrundlagen" nachdrücklich abrate.[156]

10.3.5 Empfehlung: Datenerhebung aufgrund und im Rahmen der bestehenden gesetzlichen Befugnisse

Stattdessen habe ich der Stadt geraten, die bestehenden gesetzlichen Befugnisse des Sozialdatenschutzrechts für die beabsichtigte Erhebung von Daten über eine eventuelle Fremdunterbringung oder kindeswohlrelevante Vorfälle hinsichtlich der eigenen Kinder der Bewerberinnen und Bewerber heranzuziehen. Insbesondere kommt dafür aus meiner Sicht die Vorschrift des § 62 Abs. 3 Nr. 2 Buchst. c SGB VIII in Betracht. Danach dürfen Sozialdaten ohne Mitwirkung der betroffenen Person unter anderem erhoben werden, wenn die Erhebung bei der betroffenen Person nicht möglich ist oder die jeweilige Aufgabe ihrer Art nach eine Erhebung bei anderen erfordert, die Kenntnis der Daten aber erforderlich ist für die Wahrnehmung einer Aufgabe nach § 43 SGB VIII. Dabei obliegt die Einschätzung, ob die Kenntnis der Daten insbesondere auch für die Wahrnehmung der Aufgaben nach § 43 Abs. 2 SGB VIII „erforderlich" ist, den jeweils zuständigen Behörden.

Entsprechendes gilt für die Prüfung, ob nach dem sogenannten Doppeltürmodell auf Seiten der übermittelnden Stelle auch die Voraussetzungen einer notwendigen Übermittlungsbefugnis, wie etwa nach § 69 Abs. 1 Nr. 1 Var. 3 SGB X, vorliegen. Nach der verfassungsgerichtlichen Rechtsprechung ist bei einem Datenaustausch zur staatlichen Aufgabenwahrnehmung zwischen dem Datenabruf durch die auskunftsersuchende Stelle und der Datenübermittlung durch die auskunftserteilende Stelle zu unterscheiden. Ein Datenaustausch vollzieht sich durch die einander korrespondierenden Eingriffe von Abfrage und Übermittlung, die jeweils einer eigenen Rechtsgrundlage bedürfen.[157]

[156] Vgl. Bayerischer Landesbeauftragter für den Datenschutz, Die Einwilligung nach der Datenschutz-Grundverordnung (Fn. 155), Rn. 25.

[157] Vgl. Bundesverfassungsgericht, Beschluss vom 24. Januar 2012, 1 BvR 1299/05, BeckRS 2012, 47556, Rn. 123 und Beschluss vom 27. Mai 2020, 1 BvR 1873/13 und 1 BvR 2618/13, BeckRS 2020, 16236, Rn. 93, 201; Bayerisches Oberstes Landesgericht, Beschluss vom 6. Dezember 2024, 101 VA 129/24, BeckRS 2024, 34857, Rn. 23.

10.4 Datenanforderungen von Ausländerbehörden bei anderen öffentlichen Stellen

10.4.1 Übermittlung von Sozialdaten eines Jobcenters an eine kommunale Ausländerbehörde

In meinem 34. Tätigkeitsbericht 2024 unter Nr. 4.2 habe ich über eine Beratungsanfrage einer bayerischen Kommune berichtet, deren Ausländerbehörde Daten bei einem Jobcenter erheben wollte und dabei auf Widerstand stieß. Meine Antwort an die Kommune veranlasste mich insbesondere zu Ausführungen zum sogenannten Doppeltürmodell, das zwischen der Datenübermittlung von der auskunftserteilenden Stelle und dem Datenabruf durch die auskunftsersuchende Stelle unterscheidet, sowie zur datenschutzrechtlichen Verantwortlichkeit bei der Übermittlung von Sozialdaten.

Zwischenzeitlich hat sich die bayerische Kommune – wie von mir vorgeschlagen – an das Bayerische Staatsministerium des Innern, für Sport und Integration gewandt, das seinerseits die Bundesagentur für Arbeit in den Fall zum Zwecke der Abstimmung über die sozialrechtliche Rechtslage einbezog. Schließlich war auch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit als Datenschutzaufsichtsbehörde über das Jobcenter als gemeinsame Einrichtung gemäß §§ 50 Abs. 4 Satz 3, Abs. 2 Zweites Buch Sozialgesetzbuch – Bürgergeld, Grundsicherung für Arbeitsuchende – eingebunden.

Konkret ging es um die Auslegung von § 71 Abs. 2 Satz 1 Nr. 1 Buchst. a Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X). Die Vorschrift erlaubt im Einzelfall auf Ersuchen der Ausländerbehörde die Übermittlung von Sozialdaten eines Ausländers über die Gewährung oder Nichtgewährung von Leistungen, wenn diese für die Entscheidung über den Aufenthalt des Ausländers benötigt werden. Das um eine Auskunft ersuchte Jobcenter war der Meinung, dass der Ausländerbehörde lediglich das „Ob“ der Gewährung von Sozialleistungen mitgeteilt werden darf, allerdings keine weiteren Informationen etwa zur Höhe und Dauer der in Anspruch genommen Sozialleistungen. Die Ausländerbehörde argumentierte hingegen, dass sie in bestimmten Fällen auch Informationen zur Höhe und Dauer der in Anspruch genommenen Sozialleistungen benötige, um eine Entscheidung über den Aufenthalt des Ausländers zu treffen. Das Bayerische Staatsministerium des Innern, für Sport und Integration hat sich der Ansicht der Ausländerbehörde angeschlossen.

Nach Abklärung mit den beteiligten Stellen äußerte sich das Jobcenter schließlich dahingehend, dass bei Vorliegen der entsprechenden Voraussetzungen im Einzelfall Sozialdaten an die Ausländerbehörde übermittelt werden könnten. Soweit dies zur Entscheidung der Ausländerbehörde erforderliche Informationen seien, könnten auch weitere Daten zum Leistungsbezug mitgeteilt werden wie etwa zur Leistungshöhe und Leistungsdauer. Das Jobcenter ist ebenfalls zum Ergebnis gelangt, dass die datenschutzrechtliche Verantwortung für die Datenübermittlung bei der übermittelnden Stelle – vorliegend bei dem Jobcenter selbst – liege. Dieser müsse es aufgrund der Angaben der ersuchenden Stelle möglich sein, das Vorliegen der Voraussetzungen und somit die Rechtmäßigkeit der Datenübermittlung zu prüfen.

Trägt – wie vorliegend gemäß § 67d Abs. 1 Satz 1 SGB X bei einer Datenübermittlung die übermittelnde Stelle die datenschutzrechtliche Verantwortlichkeit, so sollte die ersuchende Stelle die Anfrage möglichst präzise unter Erläuterung des

Sachverhalts stellen, so dass es der übermittelnden Stelle möglich ist, die Rechtmäßigkeit der erwogenen Datenübermittlung abschließend zu prüfen.

10.4.2 Weiterer Fall zur Datenerhebung durch eine bayerische Ausländerbehörde

Von einer bayerischen öffentlichen Stelle wurde ich auf eine Anforderung von Sozialdaten durch eine Ausländerbehörde aufmerksam gemacht. Einbezogen wurde ich in diesem Fall also nicht von der ersuchenden, sondern von der ersuchten Stelle.

Konkret forderte die Ausländerbehörde die Kopie eines Bescheids aus dem Bereich des Sozialrechts an und stützte dies auf §§ 86, 87 Aufenthaltsgesetz. Die ersuchte Stelle übermittelte die gewünschte Bescheidkopie an die Ausländerbehörde, ohne den Sachverhalt vorher ausreichend geprüft zu haben. Im Nachgang kamen der ersuchten Stelle Zweifel, ob das gewählte Vorgehen rechtmäßig war; sie informierte mich im Rahmen einer Meldung nach Art. 33 DSGVO über diese Zweifel. Die Stelle räumte dabei ein, dass sie mit den bisherigen Angaben in der Anfrage keine ausreichende Prüfung der Plausibilität des Anliegens durchführen konnte. Vielmehr hätte sie wegen ihrer Verantwortlichkeit gemäß § 67d Abs. 1 Satz 1 SGB X vor einer Übermittlung der Daten bei der anfragenden Stelle nachfragen und sich den Sachverhalt und die Rechtslage genauer erläutern lassen müssen, um selbst eine zutreffende Einschätzung zur Rechtmäßigkeit der Datenübermittlung vornehmen zu können.

10.4.2.1 Verletzung der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO

Prüft ein datenschutzrechtlich Verantwortlicher zum Zeitpunkt der Datenverarbeitung die Rechtmäßigkeit nicht und kann er diese später dann nicht ausreichend darlegen, verletzt er seine Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO, die sich auch auf den Grundsatz der Rechtmäßigkeit gemäß Art. 5 Abs. 1 Buchst. a, Art. 6 DSGVO bezieht. Vorliegend stellte ich eine Verletzung dieser Rechenschaftspflicht in Bezug auf den Grundsatz der Rechtmäßigkeit durch die übermittelnde Stelle fest.

Die übermittelnde Stelle hätte die Zulässigkeit des Übermittlungsersuchens aufgrund der ihr durch § 67d Abs. 1 SGB X zugewiesenen Verantwortlichkeit beurteilen müssen, was unterblieben ist. Soweit die Angaben der Ausländerbehörde nicht ausreichend waren, um die Zulässigkeit der Übermittlung zu klären, hätte zunächst zur Sachverhaltsergänzung eine Rücksprache mit der Ausländerbehörde stattfinden müssen.

Im Rahmen von § 67d Abs. 1 SGB X muss die ersuchende Behörde alle für die Beurteilung der Datenübermittlung notwendigen Informationen mitteilen. Dazu gehören Ausführungen zum Sachverhalt, insbesondere um den in Betracht kommenden Übermittlungstatbestand unter Berücksichtigung des Erforderlichkeitsprinzips prüfen zu können. Auch muss die Prüfung einer zulässigen Abweichung vom Direkterhebungsgrundsatz (§ 67a Abs. 2 Satz 1 SGB X) möglich sein, weil die Ausländerbehörde die Sozialdaten nicht bei der betroffenen Person, sondern bei der anderen öffentlichen Stelle erhebt.

Das Ersuchen muss daher jedenfalls Angaben zu dem ersuchenden Dritten, zur Identifizierung der betroffenen Person, zu Art und Umfang der ersuchten Sozialdaten, zur den Aufgaben, auf welche sich die Erforderlichkeit der Verarbeitung bezieht, sowie die Gründe für eine Dritterhebung enthalten.[158] Ist der vorgelegte Sachverhalt nicht dicht genug, um eine rechtliche Bewertung der Datenübermittlung durch die übermittelnde Stelle vorzunehmen, muss eine Konkretisierung bei der anfordernden Stelle verlangt werden.

10.4.2.2 Meldepflicht gemäß Art. 33 DSGVO

Da mir der Sachverhalt im Rahmen einer Meldung gemäß Art. 33 DSGVO zugetragen wurde und der öffentlichen Stelle unklar war, ob sie außerdem die betroffene Person gemäß Art. 34 DSGVO benachrichtigen muss, war auch zu prüfen, ob vorliegend überhaupt ein meldepflichtiger Sachverhalt gemäß Art. 33 Abs. 1 DSGVO vorlag. Der Sachverhalt bot daher Anlass, die Voraussetzungen der Meldepflicht näher zu erläutern, eine Thematik, die aus meiner Erfahrung bei vielen bayerischen öffentlichen Stellen Unsicherheiten aufwirft.

Ein Sachverhalt, der die Meldepflicht gemäß Art. 33 Abs. 1 DSGVO auslöst, ist mir vorliegend nicht ersichtlich geworden. Die Meldung nach Art. 33 Abs. 1 Satz 1 DSGVO besteht nur im Falle einer Verletzung des Schutzes personenbezogener Daten. Dies setzt nach Art. 4 Nr. 12 DSGVO eine „Verletzung der Sicherheit“ voraus. Längst nicht jeder Verstoß gegen Datenschutzrecht begründet eine Datensicherheitsverletzung.[159]

Die erforderliche Datensicherheitsverletzung setzt bei Art. 32 DSGVO an, der die den Verantwortlichen dazu verpflichtet, geeignete technische und organisatorische zur Datensicherheit zu ergreifen. Eine Verletzung der Datensicherheit liegt bei einem Versagen technischer und/oder organisatorischer Maßnahmen vor, auch dann, wenn die von der datenverarbeitenden Stelle ergriffenen (technischen/organisatorischen) Maßnahmen in Anbetracht der mit den Verarbeitungstätigkeiten verbundenen Risiken kein hinreichendes Schutzniveau etablieren. Mit anderen Worten steht die Unwirksamkeit technischer und/oder organisatorische Maßnahmen, alternativ ihr Fehlen im Mittelpunkt einer Datensicherheitsverletzung.

Ein Versagen technischer (etwa Berechtigungskonzepte) oder organisatorischer Maßnahmen (etwa spezifische – mir nicht bekannte – innerbehördliche Vorgaben zum Umgang mit derartigen Anfragen von Ausländerbehörden) hat die meldende Stelle nicht vorgetragen. Auch wurde mir nicht ersichtlich, dass die Offenlegung erst durch das Fehlen von hinreichenden technischen und/oder organisatorischen Maßnahmen durch den Verantwortlichen ermöglicht wurde. Vor diesem Hintergrund war keine Datensicherheitsverletzung anzunehmen, sodass weder die Meldepflicht nach Art. 33 DSGVO noch die Benachrichtigungspflicht nach Art. 34 DSGO zu erfüllen waren.

Ich habe auch § 67d SGB X selbst nicht als eine organisatorische Maßnahme gewertet. Die Norm regelt die Verantwortungsverteilung zwischen übermittelnder

[158] Vgl. Cormann, in: Kasseler Kommentar, Stand 12/2019, § 67d SGB X Rn. 6.

[159] Vgl. Bayerischer Landesbeauftragter für den Datenschutz, Meldepflicht und Benachrichtigungspflicht des Verantwortlichen, Orientierungshilfe, Stand 6/2019, Rn. 4 ff., Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek“.

und empfangender Stelle und ist bei der Prüfung der Rechtmäßigkeit der Datenübermittlung als zwingendes Recht zu beachten.

Insgesamt verblieb eine potenziell rechtswidrige Datenübermittlung. Aufgrund der unterbliebenen Prüfung der Rechtmäßigkeit der Datenübermittlung stellte ich lediglich ein Versäumnis des Verantwortlichen im Hinblick auf die Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO bei der Beachtung des Grundsatzes der Rechtmäßigkeit gemäß Art. 5 Abs. 1 Buchst. a, Art. 6 DSGVO fest.

10.5 Datenschutz bei der Bearbeitung von Unfallanzeigen

Mit einer Beratungsanfrage hatte sich eine Fachkraft für Arbeitssicherheit einer bayerischen Kommune an mich gewandt und den Datenschutz bei der Bearbeitung von Unfallanzeigen thematisiert.

Konkret ging es um den Erhalt nicht anonymisierter Unfallanzeigen sowie die Offenlegung weiterer personenbezogener Daten zum Zwecke der eigenen Aufgabenerfüllung dieser Fachkraft. Die Praxis der eigenen Kommune sehe vor der Weiterleitung von Unfallanzeigen an den betriebsärztlichen Dienst und den Fachdienst für Arbeitssicherheit eine Schwärzung insbesondere von Namen vor, wenn keine Einwilligungserklärungen der betroffenen Personen vorlägen. Aufgrund langjähriger Praxis werde in § 193 Abs. 5 Siebtes Buch Sozialgesetzbuch – Gesetzliche Unfallversicherung – (SGB VII) keine ausreichende Rechtsgrundlage für die ungeschwärzte Offenlegung der Unfallanzeige gesehen. Die Anfrage würdigte diese Praxis kritisch und trug vor, dass Fachkräfte für Arbeitssicherheit bei einer Verweigerung von Einwilligungen der betroffenen Personen Ihren gesetzlichen Auftrag nicht erfüllen können.

10.5.1 „In Kenntnis setzen“ über Unfallanzeigen: § 193 Abs. 5 Satz 2 SGB VII

Nach § 193 Abs. 5 Satz 2 SGB VII hat der Unternehmer die Sicherheitsfachkraft und den Betriebsarzt über die Unfall- oder Berufskrankheitenanzeige „in Kenntnis zu setzen“. Unter dem Begriff Sicherheitsfachkraft ist die Fachkraft für Arbeitssicherheit zu verstehen. Der Begriff des Unternehmers ist in § 136 Abs. 3 SGB VII definiert. Die Anzeige bezieht sich auf die Anzeigeverpflichtung des Unternehmers gegenüber dem Unfallversicherungsträger gemäß § 193 Abs. 1 SGB VII, die grundsätzlich eingreift, wenn sich Versicherte bei Unfällen mit der Folge einer mehr als dreitägigen Arbeitsunfähigkeit verletzen

Der Gesetzgeber hat nicht zweifelsfrei entschieden, ob im Rahmen des „In-Kenntnis-Setzens“ gemäß § 193 Abs. 5 Satz 2 SGB VII auch personenbezogene Daten verarbeitet werden dürfen. Insoweit könnte § 193 Abs. 5 Satz 2 SGB VII als Verarbeitungsbefugnis gemäß Art. 6 Abs. 3, Abs. 1 UAbs. 1 Buchst. e DSGVO oder – weil das „In-Kenntnis-Setzen“ als gesetzliche Pflicht formuliert wurde – gemäß Art. 6 Abs. 3, Abs. 1 UAbs. 1 Buchst. c DSGVO fungieren. Dagegen könnte sich der Regelungsgehalt von § 193 Abs. 5 Satz 2 SGB VII aber ebenso gut darin erschöpfen, die Fachkraft für Arbeitssicherheit über die bloße Existenz der Unfallanzeige zu informieren, ohne dabei personenbezogene Daten zu verarbeiten.

Der Normtext fordert nicht zwingend, dass die Fachkraft für Arbeitssicherheit über den vollständigen Inhalt der Unfallanzeige in Kenntnis zu setzen ist, zu dem auch

personenbezogene Daten zählen (siehe die Angaben im Musterformular „Unfallanzeige“ der Deutschen Gesetzlichen Unfallversicherung – DGUV).[160] Im Unterschied zu den in § 193 Abs. 7 SGB VII genannten Konstellationen sieht § 193 Abs. 5 Satz 2 SGB VII nämlich nicht vor, dass der Fachkraft für Arbeitssicherheit eine „Durchschrift der Anzeige“ zur Verfügung zu stellen wäre. Dies bedeutet aber nicht, dass eine Offenlegung personenbezogener Daten gegenüber der Fachkraft für Arbeitssicherheit ausgeschlossen oder nur mit Einwilligung der betroffenen Person möglich wäre. Eine entsprechende Einschränkung lässt sich § 193 Abs. 5 Satz 2 SGB VII nicht entnehmen.

10.5.2 Bereichsspezifische Verarbeitungsbefugnisse

Stellt § 193 Abs. 5 Satz 2 SGB VII selbst keine taugliche Verarbeitungsbefugnis dar, kann gegebenenfalls auf andere gesetzliche Verarbeitungsbefugnisse zurückgegriffen werden. Nach meinem Verständnis handelt es sich vorliegend nicht um eine Verarbeitung von Sozialdaten im Sinne von § 67 Abs. 2 Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X), weil bei der (innerbehördlichen) Offenlegung personenbezogener Daten gegenüber der Fachkraft für Arbeitssicherheit nicht ein Sozialleistungsträger zur Erfüllung sozialrechtlicher Aufgaben tätig wird. Folglich sind die sozialrechtlichen Verarbeitungsbefugnisse aus §§ 67 ff. SGB X nicht anwendbar.

In Betracht kommt aber die Anwendung personaldatenschutzrechtlicher Regelungen aus Art. 103 ff. Bayerisches Beamtengesetz (BayBG), § 50 Beamtenstatusgesetz (BeamtStG), gegebenenfalls in Verbindung mit Art. 145 Abs. 2 BayBG – vorausgesetzt, die betreffenden Daten sind zu den Personalaktendaten zu zählen. Zu den Personalakten werden Unterlagen genommen, die Rechte oder Pflichten im Rahmen des Dienstverhältnisses begründen, feststellen, ändern oder beenden, so auch Unterlagen betreffend die Anerkennung eines Dienstunfalls.[161] Unterlagen in Verfahren der beamtenrechtlichen Unfallfürsorge gemäß Art. 45 ff. Bayerisches Beamtenversorgungsgesetz (BayBeamtVG) stellen grundsätzlich Personalaktendaten dar (vgl. etwa meinen 23. Tätigkeitsbericht 2008 unter Nr. 21.2, an dem ich auch nach Geltungsbeginn der Datenschutz-Grundverordnung festhalte).

Gegebenenfalls könnte sich diese Wertung vorliegend auf Unfallanzeigen gemäß § 193 Abs. 5 SGB VII übertragen lassen. Dann wären auch bei der Einbindung der Fachkraft für Arbeitssicherheit im Rahmen von Unfallanzeigen die Art. 103 ff. BayBG, § 50 BeamtStG für die Verarbeitung der betreffenden personenbezogenen Daten anzuwenden.

Ich neige allerdings der Auffassung zu, die Offenlegung personenbezogener Beschäftigtendaten bei der Einbindung der Fachkraft für Arbeitssicherheit im Rahmen von Unfallanzeigen nicht dem Rechtsregime des Personaldatenschutzes zu unterwerfen. Nach dem materiellen Personalaktenbegriff gehören zur Personalakte alle Unterlagen, die die Beamtin oder den Beamten betreffen, soweit sie mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen

[160] DGUV, Unfallanzeige für Arbeitnehmer mit Erläuterungen – ausfüllbar und barrierefrei, Internet: https://www.dguv.de, Rubrik „Versicherung – Arbeitsunfälle“.

[161] Vgl. Uckelmann/Hedemann, in: Brinktrine/Voitl, Beck’scher Online-Kommentar Beamtenrecht Bayern, 35. Edition 2/2025, Art. 104 BayBG Rn. 66.1.

(§ 50 Satz 2 BeamtStG). Zweck der Personalakte ist es, ein möglichst vollständiges Bild von der Persönlichkeit des Beamten zu geben und vor allem ein lückenloses Bild der Entstehung und Entwicklung des Dienstverhältnisses als in einem historischen Geschehensablauf zu vermitteln. Die Pflicht gemäß § 193 Abs. 5 Satz 2 SGB VII, die Fachkraft für Arbeitssicherheit über Unfall- oder Berufskrankheitenanzeigen „in Kenntnis zu setzen", soll dieser hingegen eine hinreichende Informationsgrundlage verschaffen, um ihre eigenen Aufgaben zu erfüllen. In diesem Rahmen handelt es sich nach meinem Verständnis nicht um Daten, die mit dem Dienstverhältnis der von einem Unfall betroffenen Beschäftigten in einem unmittelbaren inneren Zusammenhang stehen und somit nicht um Personalaktendaten im materiellen Sinn gemäß § 50 Satz 2 BeamtStG.

10.5.3 Art. 4 Abs. 1 BayDSG

Soweit keine bereichsspezifischen datenschutzrechtlichen Verarbeitungsbefugnisse eingreifen, kommt zur Verarbeitung personenbezogener Daten ein Rückgriff auf Art. 4 Abs. 1 BayDSG in Betracht. Art. 4 Abs. 1 BayDSG bestimmt, dass die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle zulässig ist, wenn sie zur Erfüllung einer ihr obliegenden Aufgabe erforderlich ist. Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG ist nicht anzuwenden, weil die Fachkraft für Arbeitssicherheit als Beschäftigter der öffentlichen Stelle kein von dieser getrennter Verantwortlicher ist. Etwas anderes würde gegebenenfalls im Bereich von überbetrieblichen Diensten gemäß § 19 Gesetz über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit (ASiG) gelten.

10.5.3.1 Verarbeitung von Gesundheitsdaten

Sollen Gesundheitsdaten im Sinne von Art. 4 Nr. 15 DSGVO verarbeitet werden, handelt es sich um Daten, die zu den besonderen Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO gehören. Dann wäre zusätzlich Art. 9 Abs. 2 DSGVO – gegebenenfalls in Verbindung mit Art. 8 Abs. 1 BayDSG – zu beachten. Soweit sozial- und arbeitssicherheitsrechtliche Vorgaben erfüllt werden, kann die Verarbeitung von Gesundheitsdaten auf Art. 9 Abs. 2 Buchst. b DSGVO in Verbindung mit Art. 8 Abs. 1 Satz 1 Nr. 1 und Nr. 2 BayDSG gestützt werden. Zulässig ist eine Verarbeitung besonderer Kategorien personenbezogener Daten hiernach, soweit sie erforderlich ist, damit eine bayerische öffentliche Stelle die ihr auf dem Gebiet des Dienst- und Arbeitsrechts oder dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und ihren diesbezüglichen Pflichten nachkommen kann. Bei der Verarbeitung dieser Daten haben bayerische öffentliche Stellen angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen (Art. 8 Abs. 2 Satz 1 BayDSG).

10.5.3.2 Nur geringfügige Eingriffe

Die Verarbeitungsbefugnis aus Art. 4 Abs. 1 BayDSG trägt aufgrund ihrer vergleichsweise geringen tatbestandlichen Bestimmtheit lediglich Datenverarbeitungen, die mit einem weniger intensiven Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz) verbunden ist.[162] Allein dadurch sind dem Umfang und der Qualität der Datenverar-

[162] Vgl. Bayerischer Verwaltungsgerichtshof, Beschluss vom 15. Februar 2024, 4 CE 23.2267,

beitung, die auf Art. 4 Abs.1 BayDSG gestützt wird, Grenzen gesetzt. Bei der Anwendung von Art. 4 Abs. 1 BayDSG kommt es maßgeblich darauf an, ob die Verarbeitung der personenbezogenen Daten zur Erfüllung der jeweiligen Aufgaben erforderlich ist. Dies setzt einerseits eine genaue normative Bestimmung der zu erfüllenden Aufgaben voraus und macht eine andererseits eine das Fachrecht berücksichtigende Erforderlichkeitsprüfung notwendig. Diese gesetzliche Konzeption hat stets eine Einzelfallprüfung im Blick. Eine pauschale Antwort in Bezug auf die Zulässigkeit der Offenlegung einer Vielzahl verschiedener personenbezogener Daten verbietet sich daher.

10.5.3.3 Aufgabenerfüllung

Soweit eine Offenlegung personenbezogener Daten gegenüber der Fachkraft für Arbeitssicherheit im Raum steht, ergeben sich die von der öffentlichen Stelle zu erfüllenden Aufgaben aus gesetzlichen Vorgaben:

Das Gesetz über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit (im Folgenden: ASiG) schafft neben dem Arbeitsschutzgesetz einen Rechtsrahmen des betrieblichen Arbeitsschutzes, der den Arbeitgeber zu einer tauglichen Arbeitsschutzorganisation verpflichtet. § 16 ASiG sieht für die öffentliche Verwaltung vor, dass ein den Grundsätzen dieses Gesetzes gleichwertiger arbeitsmedizinischer und sicherheitstechnischer Arbeitsschutz zu gewährleisten ist. Insoweit kommt es auf konkrete Regelungen für Fachkräfte für Arbeitssicherheit an, die gemäß § 1 ASiG vom Arbeitgeber zu bestellen sind und ihn bei dem Arbeitsschutz und bei der Unfallverhütung unterstützen.

§ 6 ASiG legt die Aufgaben der Fachkraft für Arbeitssicherheit fest. Gemäß § 6 Abs. 1 Satz 1 ASiG haben die Fachkräfte für Arbeitssicherheit gegenüber dem Arbeitgeber einen Unterstützungsauftrag, gemäß § 6 Abs. 1 Satz 2 Nr. 1 ASiG einen Beratungsauftrag und gemäß § 6 Abs. 1 Satz 2 Nr. 3 Buchst. c ASiG einen Untersuchungsauftrag in Bezug auf Arbeitsunfälle. § 6 Abs. 1 Satz 2 Nr. 3 Buchst. c ASiG bezieht sich nicht nur darauf, die Ursachen von Arbeitsunfällen zu untersuchen, sondern auch auf die Erfassung und Auswertung der Untersuchungsergebnisse. Dem Arbeitgeber sind Maßnahmen zur Verhütung dieser Arbeitsunfälle vorzuschlagen.

Die in § 6 ASiG genannten Aufgaben werden durch die Unfallverhütungsvorschriften der Unfallversicherungsträger auf der Grundlage von § 15 Abs. 1 Satz 1 Nr. 6 SGB VII konkretisiert. § 5 DGUV Vorschrift 2[163] enthält etwa Berichtspflichten der Betriebsärzte und Fachkräfte für Arbeitssicherheit. In Anlage 2 Abschnitt 2 DGUV Vorschrift 2 werden verschiedene Aufgabenfelder im Bereich der Grundbetreuung festgelegt. Unter Nr. 5.1 werden Untersuchungen von Ereignissen, Ursachenanalysen und deren Auswertungen genannt. Nr. 5.2 führt das Ermitteln von Unfallschwerpunkten sowie Schwerpunkten arbeitsbedingter Erkrankungen und Nr. 5.3 Verbesserungsvorschläge auf.

Anhang 3 DGUV Vorschrift 2 ergänzt dazu unverbindlich mögliche Aufgaben, die im Rahmen der gesetzlich vorgeschriebenen Aufgaben (vorliegend § 6 ASiG) an-

BeckRS 2024, 2968, Rn. 20.

[163] DGUV, Muster DGUV Vorschrift 2, Unfallverhütungsvorschrift, Betriebsärztinnen und Betriebsärzte sowie Fachkräfte für Arbeitssicherheit, Stand 11/2024, Internet: https://www.dguv.de, Rubrik „Prävention – DGUV Vorschriften- und Regelwerk – DGUV Vorschrift 2“.

fallen können. Nr. 5.1 enthält zur Untersuchung nach Ereignissen, Ursachenanalysen und deren Auswertungen folgende Angaben: Meldepflichtige Unfälle, nichtmeldepflichtige Unfälle, Beinaheunfälle, Erste-Hilfe-Fälle, relevante Zwischenfälle ohne Personenschäden, speziell auch tödliche, lebensbedrohliche und Massenunfälle, Berufskrankheiten (Verdachtsfälle, anerkannte Berufskrankheiten), arbeitsbedingte Erkrankungen, Auswertung von Gesundheitsberichten von Krankenkassen und Wegeunfälle. Nr. 5.3 enthält zu den Verbesserungsvorschlägen folgende Angaben: Ableiten von Verbesserungsvorschlägen aus den Analysen und Untersuchungen zur Vermeidung der Wiederholung der eingetretenen Unfälle und Erkrankungen und anderer Ereignisse, zu Vermeidung vergleichbarer Unfälle, Erkrankungen und anderer Ereignisse und zur Bekämpfung von Unfallschwerpunkten und Schwerpunkten arbeitsbedingter Erkrankungen.

10.5.3.4 Erforderlichkeit

Die jeweilige Verarbeitung personenbezogener Daten muss zur Erfüllung der skizzierten Aufgaben gemäß Art. 4 Abs. 1 BayDSG erforderlich sein. Die Erforderlichkeit einer Verarbeitung ist unionsrechtlich vorgegeben, vgl. Art. 6 Abs. 1 UAbs. 1 Buchst. c und e DSGVO; sie steht im engen Zusammenhang mit dem Grundsatz der Datenminimierung nach Art. 5 Abs. 1 Buchst. c DSGVO. Eine bloße Sachdienlichkeit oder Förderlichkeit reicht zur Erreichung des angestrebten Zwecks insoweit nicht aus.[164] Vielmehr müssen sich Verarbeitungen personenbezogener Daten auf das Notwendige beschränken und die öffentliche Stelle müsste ihre jeweilige Aufgabe ohne die Verarbeitung nicht, nicht vollständig oder nicht in rechtmäßiger oder zumutbarer Weise erfüllen können.[165]

Soweit Fachkräfte für Arbeitssicherheit bei Arbeitsunfällen Ursachenforschung betreiben, eigene Schlüsse ziehen, den Arbeitgeber beraten und Verbesserungsvorschläge unterbreiten, muss ihnen zumindest das Unfallgeschehen möglichst umfassend zur Kenntnis gelangen. Dazu ist die genaue Kenntnis des Unfallhergangs unabdingbar, um auf dieser Informationsgrundlage gegebenenfalls weitere Maßnahmen ergreifen zu können.

Mir leuchtet allerdings nicht ein, dass die Fachkraft für Arbeitssicherheit zur eigenen Aufgabenerfüllung alle in Unfallanzeigen enthaltenen personenbezogenen Daten betroffener Beschäftigter erhalten müsste. Eine pauschale Offenlegung sämtlicher Daten würde den verschiedenen Fallgestaltungen und Unfallszenarien nicht gerecht werden. Mir vorliegende Formulare von Unfallanzeigen enthalten eine Vielzahl personenbezogener Daten betroffener Beschäftigter, etwa neben Namen und Angaben zum Unfallhergang auch Angaben über die Staatsangehörigkeit der betroffenen Person, private Adressdaten, Daten über die Leiharbeitnehmerschaft, einen Anspruch auf Entgeltfortzahlung, sogar ein mögliches Verwandtschaftsverhältnis zur Unternehmensleitung. Die Kenntnis solcher Daten wird zur Wahrnehmung der oben beschriebenen Untersuchungs- und Beratungsaufgaben einer Fachkraft für Arbeitssicherheit nicht benötigt; ihre Offenlegung durch den Verantwortlichen könnte nicht auf Art. 4 Abs. 1 BayDSG gestützt werden.

[164] Vgl. Bayerisches Oberstes Landesgericht, Beschluss vom 6. August 2020, 1 VA 33/20, BeckRS 2020, 18859, Rn. 60.

[165] Vgl. Stief, in: Schröder, Bayerisches Datenschutzgesetz, 2021, Art. 4 BayDSG Rn. 42 f.

Soweit sich der Informationsfluss auf eine Vielzahl unterschiedlicher Fallgestaltungen bezieht, halte ich es für ausreichend, den Unfallhergang und den Namen der vom Unfall betroffenen Person gegenüber der Fachkraft für Arbeitssicherheit zu offenbaren. Bei größeren Verantwortlichen mit verschiedenen Dienststellen oder Organisationseinheiten können auch diese angegeben werden. So erfährt die Fachkraft, was passiert ist, und hat Kontaktinformationen, um im Bedarfsfall Nachfragen bei der verunfallten Person stellen zu können, etwa, wenn es um die konkreten Arbeitsbedingungen, den Umgang mit Schutzvorrichtungen oder mit zurückliegenden Hinweisen auf entsprechende Defizite geht.

Eine anonymisierte Unfallanzeige würde demgegenüber die Arbeit der Fachkräfte für Arbeitssicherheit erheblich erschweren. Gerade bei personalstarken Verantwortlichen hätten die Fachkräfte unter Umständen keine Möglichkeiten, eigene Feststellungen zu einem Unfallgeschehen zu treffen. Die Befassung mit den Unfallanzeigen fände dann auf einem eher theoretischen Level statt; konkrete Auswirkungen etwa auf die Gestaltung von Arbeitsplätzen wären unwahrscheinlich. Der gesetzlichen Aufgabenstellung für die Fachkräfte würde so nur unzureichend entsprochen.

10.5.4 Ergebnis

Vor diesem Hintergrund halte ich es im Rahmen von § 193 Abs. 5 Satz 2 SGB VII für zulässig, nicht nur den Unfallhergang, sondern auch die zur Individualisierung erforderlichen Informationen über den Namen der vom Unfall betroffenen Personen und gegebenenfalls der Dienststelle oder Organisationseinheit mit der Fachkraft für Arbeitssicherheit zu teilen. Bayerische öffentliche Stellen können eine entsprechende Verarbeitung grundsätzlich auf Art. 4 Abs. 1 BayDSG stützen.

11 Personalverwaltung

11.1 Novellierung des Bayerischen Gleichstellungsgesetzes

Knapp zwei Jahrzehnte nach seiner letzten Änderung[166] ist das Bayerische Gleichstellungsgesetz (BayGlG) im Jahr 2025 recht umfassend novelliert worden.[167] Dieses Gesetz zielt insbesondere darauf ab, die Chancengleichheit von Frauen und Männern im bayerischen öffentlichen Dienst zu verwirklichen, vgl. Art. 2 Abs. 1 Sätze 1 und 2 BayGlG. Damit liegt der inhaltliche Schwerpunkt des Bayerischen Gleichstellungsgesetzes zwar nicht im Datenschutzrecht – ohne Verarbeitungen von personenbezogenen Beschäftigtendaten können bayerische Dienstherren und öffentliche Arbeitgeber bestimmte, gesetzlich vorgesehene Maßnahmen zur Erreichung dieses Ziels aber nicht umsetzen. Datenschutzrechtlich relevant sind vor diesem Hintergrund insbesondere die Regelungen zu Gleichstellungskonzepten sowie zu den Informationsrechten der Gleichstellungsbeauftragten.

Umso erfreulicher ist es, dass mich das Bayerische Staatsministerium für Familie, Arbeit und Soziales frühzeitig in seine diesbezüglichen Novellierungsüberlegungen eingebunden hat. Obgleich es im weiteren Gesetzgebungsverfahren mitunter auch hektischer zuging, konnte ich meine datenschutzrechtlichen Erwägungen doch stets in einem konstruktiven Dialog mit dem Sozialministerium einbringen. Die Änderungen des Bayerischen Gleichstellungsgesetz sind am 16. Juli 2025 in Kraft getreten.[168] Soweit diese einen Datenschutzbezug aufweisen, möchte ich sie im nachfolgenden kurz vorstellen und aus Datenschutzsicht einordnen.

11.1.1 Gleichstellungskonzepte

Schon bislang mussten bayerische – insbesondere staatliche und kommunale – Dienststellen in regelmäßigen Abständen Gleichstellungskonzepte (Art. 4 Abs. 1 BayGlG) sowie tabellarische Datenübersichten über die Anteile der beschäftigten Frauen und Männer (Art. 4 Abs. 2 BayGlG) erstellen. Der bayerische Gesetzgeber sieht hierin das wesentliche Steuerungs- und Umsetzungselement für eine geschlechtergerechte Personalentwicklung.[169] Gleichstellungskonzepte sollen die Beschäftigungssituation in der jeweiligen Dienststelle unter Gleichstellungsgesichtspunkten darstellen und erläutern; hierzu enthielten sie bislang geschlechtsspezifische Angaben etwa zu Voll- und Teilzeittätigkeiten, Einstellungen und Beförderungen (vgl. Art. 5 Abs. 2 BayGlG a. F.). Dem Sinn und Zweck nach müssen diese Angaben freilich nicht personenbezogen sein; vielmehr genügt eine statistische Aufbereitung,[170] die keine Rückschlüsse auf einzelne Beschäftigte hinter den aggregierten, also zusammengefassten, Daten zulässt.

[166] Gesetz zur Änderung des Bayerischen Gleichstellungsgesetzes vom 23. Mai 2006 (GVBl. S. 292).
[167] Gesetz zur Änderung des Bayerischen Gleichstellungsgesetzes vom 8. Juli 2025 (GVBl. S. 206).
[168] Vgl. § 2 Gesetz zur Änderung des Bayerischen Gleichstellungsgesetzes (Fn. 167).
[169] Landtags-Drucksache 19/4432, S. 15.
[170] Vgl. Landtags-Drucksache 19/4432, S. 15.

Genau hier liegt allerdings ein datenschutzrechtlicher „Fallstrick“: Der Begriff der personenbezogenen Daten nach Art. 4 Nr. 1 DSGVO ist nämlich recht weit gefasst. Ein Personenbezug liegt demnach bereits dann vor, wenn Daten die Identifizierung einer natürlichen Person „direkt oder indirekt“ – insbesondere mittels „Zusatzwissens“ – ermöglichen.[171] Das bedeutet aber auch: Je umfangreicher und feingranularer die in den genannten Dokumenten enthaltenen Daten sind und je kleiner die Beschäftigtengruppe ist, auf welche sich diese Daten beziehen, desto größer ist das (Re-)Identifizierungsrisiko im Hinblick auf einzelne Beschäftigte – und damit das (unbeabsichtigte) „Hineinrutschen“ in das Datenschutzrecht. Dies wäre umso heikler, als die Gleichstellungskonzepte und tabellarischen Datenübersichten nicht innerhalb der Personalabteilung verbleiben, sondern nach Art. 6 Abs. 1 BayGlG dienststellenweit bekanntzugeben sind. Die enthaltenen, aggregierten Daten werden dabei weit überwiegend aus Personalaktendaten im Sinne von § 50 Satz 2 Beamtenstatusgesetz, Art. 103 ff. Bayerisches Beamtengesetz (BayBG) gewonnen. Die Rechtsgrundlage hierfür stellt Art. 103 Satz 1 BayBG bereit. Eine personenbezogene Offenlegung von Personalaktendaten ohne Einwilligung der betroffenen Beschäftigten lässt Art. 108 BayBG jedoch nur in engen Grenzen zu. Im vorliegenden Zusammenhang ist insbesondere zu beachten, dass Auskünfte aus Personalakten an die zuständigen Behörden oder anderen Stellen zwar erteilt werden dürfen, um Auswertungen für Statistik- und Berichtszwecke sowie deren Abruf durchzuführen – dies aber nur unter der Maßgabe, dass es sich um anonymisierte und damit gerade nicht um personenbezogene Statistik- und Berichtszwecke handelt (Art. 108 Abs. 5 Satz 1 Nr. 1 in Verbindung mit Art. 108 Abs. 2 Nr. 4 BayBG). Die Vorschriften des Personalaktenrechts gelten unmittelbar zwar nur für bayerische Beamtinnen und Beamte; auf (tarif-)vertraglich im bayerischen öffentlichen Dienst Beschäftigte sind sie aber grundsätzlich entsprechend anwendbar, Art. 145 Abs. 2 BayBG.

Das Sozialministerium hat mir frühzeitig signalisiert, dass eine unbeabsichtigte Offenlegung personenbezogener Beschäftigtendaten in Gleichstellungskonzepten und tabellarischen Datenübersichten sicherlich nicht „im Sinne des Erfinders“ wäre. Wie schon bislang begegnet das Bayerische Gleichstellungsgesetz diesem Risiko zum einen dadurch, dass insbesondere Dienststellen, die regelmäßig weniger als 100 Personen beschäftigen, grundsätzlich von der Erstellung von Gleichstellungskonzepten absehen können (Art. 4 Abs. 1 Satz 2 BayGlG). Damit in Gleichstellungshinsicht gleichwohl keine „blinden Flecken“ verbleiben, ermöglicht es der nunmehr neu eingefügte Art. 4 Abs. 1 Satz 4 BayGlG, diese Dienststellen im Gleichstellungskonzept der jeweils übergeordneten Behörde zu berücksichtigen. Für die tabellarischen Datenübersichten nach Art. 4 Abs. 2 Satz 1 BayGlG gelten diese Vorgaben entsprechend, vgl. Art. 4 Abs. 2 Satz 3 BayGlG. Durch diesen Ansatz gehen Angaben zu Beschäftigten kleinerer Dienststellen im Personalkörper der übergeordneten Behörde auf. Die Wahrscheinlichkeit einer (Re-)Identifizierung einzelner Personen wird dadurch maßgeblich verringert. Soweit eine Dienststelle in diesem Rahmen personenbezogene Personalaktendaten an ihre übergeordnete Behörde übermitteln muss, kann sie dies unter den Voraussetzungen von Art. 108 Abs. 5 Satz 1 Nr. 1 in Verbindung mit Art. 108 Abs. 2 Nr. 4 BayBG tun (siehe bereits oben).

[171] Vgl. zu Einzelheiten Bayerischer Landesbeauftragter für den Datenschutz, Wann ist eine natürliche Person identifizierbar?, Aktuelle Kurz-Information 53, Stand: 1/2024, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek“.

Ich habe gleichwohl angeregt, nicht nur – wie dies ursprünglich angedacht war – in der Gesetzesbegründung, sondern unmittelbar im Gesetzestext zu verankern, dass Gleichstellungskonzepte und tabellarische Datenübersichten keine personenbezogenen Inhalte aufweisen dürfen. Erfreulicherweise stellt der neu angefügte Art. 4 Abs. 4 BayGlG dies jetzt unmissverständlich klar:

> **Art. 4 BayGlG**
> **Aufstellung von Gleichstellungskonzepten**
> […]
> (4) Daten, die Rückschlüsse auf Einzelpersonen zulassen, insbesondere solche, die auf einer Datenbasis von weniger als fünf Personen beruhen, dürfen in den Gleichstellungskonzepten nach Abs. 1 sowie den tabellarischen Datenübersichten nach Abs. 2 nicht angegeben werden.

Welche Angaben zum Personalkörper in die Gleichstellungskonzepte aufzunehmen sind, ergab sich bislang aus Art. 5 Abs. 2 BayGlG a. F. (siehe bereits oben). Die dortige Aufzählung war allerdings – anders als bei den tabellarischen Datenübersichten, vgl. Art. 4 Nr. 2 Satz 1 BayGlG a. F. – nicht abschließend formuliert („insbesondere"). Damit verblieb bei den einzelnen Dienststellen mitunter eine Restunsicherheit, welche Angaben der Gesetzgeber in den Gleichstellungskonzepten für erforderlich hält. Dies ist auch in datenschutzrechtlicher Hinsicht misslich, da Personalstellen personenbezogene Beschäftigtendaten zur Erstellung von Gleichstellungskonzepten nur im Rahmen des Erforderlichen verarbeiten dürfen, Art. 103 Satz 1 Nr. 1 BayBG, gegebenenfalls in Verbindung mit Art. 145 Abs. 2 BayBG.

Der Gesetzgeber wollte diesem Befund insbesondere aus Gründen der Entbürokratisierung abhelfen: Künftig richten sich die Inhalte der Gleichstellungskonzepte und tabellarischen Datenübersichten nach Mustervorlagen, welche von der beim Sozialministerium bestehenden Leitstelle für die Gleichstellung von Frauen und Männern bereitgestellt werden (Art. 4 Abs. 2 Satz 2, Art. 5 Abs. 2 BayGlG). Aus Datenschutzsicht wäre es zwar vorzugswürdig gewesen, wenn sich die Inhalte der Gleichstellungskonzepte und tabellarischen Datenübersichten bereits unmittelbar und abschließend aus dem Gesetz ergeben hätten. Gleichwohl bin ich zuversichtlich, dass die Mustervorlagen zu einer – auch aus datenschutzrechtlicher Perspektive wünschenswerten – Standardisierung beitragen werden. Meine Anregung klarzustellen, dass diese Mustervorlagen nicht lediglich Mindest-, sondern „feste Inhalte" vorgeben, hat immerhin in der Gesetzesbegründung Niederschlag gefunden.[172] Für eine datenschutzrechtliche Beratung bei der Erstellung der Mustervorlagen stehe ich dem Sozialministerium natürlich gerne zur Verfügung.

11.1.2 Informationsrechte der Gleichstellungsbeauftragten

Eine ganz wesentliche Rolle im Konzept des Bayerischen Gleichstellungsgesetzes kommt schließlich den Gleichstellungsbeauftragten zu.[173] Diese werden nach Maßgabe von Art. 13 BayGlG von der jeweiligen Dienststelle bestellt.

Die Aufgaben der Gleichstellungsbeauftragten ergeben sich aus Art. 15 BayGlG. Hiernach haben sie insbesondere den Vollzug des Bayerischen Gleichstellungsgesetzes und des jeweiligen Gleichstellungskonzepts ihrer Dienststelle zu fördern und zu überwachen (Art. 15 Abs. 1 Satz 1 BayGlG). Zur Erfüllung dieser Aufgaben

[172] Landtags-Drucksache 19/4432, S. 15.
[173] Vgl. bereits Landtags-Drucksache 13/2784, S. 13.

sind Gleichstellungsbeauftrage darauf angewiesen, die hierfür notwendigen Informationen von ihrer Dienstelle zu erhalten. Soweit diese Informationen einen Personenbezug aufweisen, berührt dies jedoch zugleich die Datenschutzrechte der betroffenen Personen. Dies kann zu Konflikten führen. Verdeutlichen lässt sich dies etwa im Hinblick auf Informationsrechte im Einstellungsverfahren: Bewerberinnen und Bewerber haben regelmäßig ein berechtigtes Interesse daran, dass schon der Umstand ihrer Bewerbung vertraulich behandelt wird. Wird ihren derzeitigen Arbeitgebern oder – bei internen Bewerbungen – Dienstvorgesetzten nämlich bekannt, dass die betreffenden Personen einen Stellenwechsel anstreben, kann dies das bestehende Beschäftigungsverhältnis belasten – vor allem, wenn aus dem angedachten Stellenwechsel nichts wird. Je mehr Personen innerhalb einer Dienststelle von der Bewerbung erfahren – etwa durch eine Einsichtnahme in Bewerbungsunterlagen oder durch die Teilnahme an Vorstellungsgesprächen –, desto größer ist das Risiko, dass die berechtigten Vertraulichkeitserwartungen von Bewerberinnen und Bewerbern nicht erfüllt werden. Dementsprechend sieht Art. 103 Satz 2 BayBG, gegebenenfalls in Verbindung mit Art. 145 Abs. 2 BayBG, vor, dass die Verarbeitung von Bewerbungsdaten nur durch Beschäftigte erfolgen darf, die vom Dienstherrn oder Arbeitgeber mit der Bearbeitung von Personalangelegenheiten betraut sind.

Der Gesetzgeber stand und steht damit vor der anspruchsvollen Aufgabe, die Rechte und Interessen von Gleichstellungsbeauftragten einerseits und von betroffenen Personen andererseits bei der Ausgestaltung der Informationsrechte der Gleichstellungsbeauftragten in einen angemessenen Ausgleich zu bringen. Dabei konnte er berücksichtigen, dass den von der Dienststelle bestellten Gleichstellungsbeauftragten nicht dieselbe demokratische Legitimation zukommt wie Personalräten oder Schwerbehindertenvertretungen, die von der Belegschaft gewählt werden (vgl. Art. 12 ff. Bayerisches Personalvertretungsgesetz, § 177 Neuntes Buch Sozialgesetzbuch – Rehabilitation und Teilhabe von Menschen mit Behinderungen).

Das Bayerische Gleichstellungsgesetz hat dabei bislang einen Regelungsansatz verfolgt, der die Informationsrechte der Gleichstellungsbeauftragten im Hinblick auf die Datenschutzrechte der betroffenen Personen nach meinem Dafürhalten grundrechtsschonend ausgestaltet hat. Dieser Ansatz lässt sich verkürzt wie folgt zusammenfassen: Ein Informationsanspruch von Gleichstellungsbeauftragten setzt regelmäßig einen konkreten Aufgabenbezug voraus, der sich insbesondere aus einem einschlägigen Beteiligungstatbestand ergeben kann (Art. 18 Abs. 2 BayGlG a. F.). In Personalangelegenheiten besteht ein Beteiligungsrecht der Gleichstellungsbeauftragten allerdings nur, wenn die betroffene Person eine solche Beteiligung beantragt hat (Art. 18 Abs. 3 Satz 2 Halbsatz 1 BayGlG a. F.) oder wenn der oder die Gleichstellungsbeauftragte hinreichende Anhaltspunkte vortragen kann, dass die Ziele des Bayerischen Gleichstellungsgesetzes nicht beachtet werden (Art. 18 Abs. 3 Satz 2 Halbsatz 2 BayGlG a. F.). Eine Beteiligung von Gleichstellungsbeauftragten an Vorstellungsgesprächen setzt stets einen entsprechenden Antrag der betroffenen Personen voraus (Art. 18 Abs. 3 Satz 3 BayGlG a. F.).[174]

[174] Vgl. zu Einzelheiten Bayerischer Landesbeauftragter für den Datenschutz, Gleichstellungsbeauftragte: Einsicht in Bewerbungsunterlagen und Teilnahme an Vorstellungsgesprächen, Aktuelle Kurz-Information 35, Stand: 3/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

An dieser Rechtslage hat sich für den staatlichen Bereich durch die Novellierung des Bayerischen Gleichstellungsgesetzes nichts geändert. Es haben sich lediglich die „Hausnummern“ verschoben: Die Rechte und Pflichten der Gleichstellungsbeauftragen ergeben sich nunmehr aus Art. 17 BayGlG. Ferner sieht das Gesetz jetzt ausdrücklich vor, betroffene Bewerberinnen und Bewerber spätestens im Rahmen der Einladung zu einem Vorstellungsgespräch darauf hinzuweisen, dass sie eine Beteiligung der oder des Gleichstellungsbeauftragten an diesem Gespräch beantragen können (Art. 17 Abs. 3 Satz 4 BayGlG).

Etwas anders stellt sich das Bild allerdings im kommunalen Bereich dar: Eine kommunale Satzungsregelung kann nach Art. 19 Abs. 1 Satz 4 BayGlG nunmehr auch eine Beteiligung von Gleichstellungsbeauftragten bei Vorstellungsgesprächen ohne Antrag der betroffenen Person vorsehen. In datenschutzrechtlicher Hinsicht kommt es hierdurch zu einer Schlechterstellung von Bewerberinnen und Bewerbern im kommunalen Bereich. Einen sachlichen Grund hierfür konnte und kann ich weiterhin nicht erkennen. Ich sehe diese Regelung daher unverändert kritisch. Unabhängig hiervon müssen natürlich auch kommunale Satzungsregelungen mit den von der Datenschutz-Grundverordnung aufgestellten Anforderungen – etwa im Hinblick auf den Grundsatz der Datenminimierung nach Art. 5 Abs. 1 Buchst. c DSGVO – vereinbar sein.[175]

11.1.3 Weitere Änderungen mit Datenschutzbezug

Nach Art. 13 Abs. 2 Satz 1 BayGlG haben Dienststellen ihren Beschäftigten die Gleichstellungsbeauftragten nach Bestellung in geeigneter Weise bekanntzumachen. Die Gleichstellungsbeauftragten sind ferner im Geschäftsverteilungsplan auszuweisen. Darüber hinaus haben die Dienststellenleitungen der beim Sozialministerium bestehenden Leitstelle für die Gleichstellung von Frauen und Männern die Namen der bestellten Gleichstellungsbeauftragten unverzüglich mitzuteilen (Art. 13 Abs. 2 Satz 2 BayGlG).

Nach der bisherigen Rechtslage konnten sich die Gleichstellungsbeauftragten gemäß Art. 18 Abs. 1 Satz 2 BayGlG a. F. unmittelbar an mich wenden; in meiner Beratungspraxis hat diese Vorschrift allerdings nahezu keine Rolle gespielt. Europarechtlich sind seit Geltungsbeginn der Datenschutz-Grundverordnung allerdings die Datenschutzbeauftragten nach Art. 37 ff. DSGVO als zentrale Ansprechpartnerinnen und Ansprechpartner in Datenschutzfragen „vor Ort“ etabliert – dies gilt auch im Hinblick auf die Beschäftigten des jeweiligen Verantwortlichen, vgl. Art. 39 Abs. 1 Buchst. a DSGVO. Gleichstellungsbeauftragte können und sollen sich somit mit datenschutzrechtlichen Anliegen jederzeit an den behördlichen Datenschutzbeauftragten oder die behördliche Datenschutzbeauftragte ihrer jeweiligen Dienststelle wenden. Hierdurch kann regelmäßig direkt vor Ort eine (teilweise sogar erhebliche) Verbesserung des Datenschutzniveaus bei der jeweiligen öffentlichen Stelle erreicht werden. Vor diesem Hintergrund habe ich dem Sozialministerium empfohlen, Art. 18 Abs. 1 Satz 2 BayGlG a. F. aufzuheben. Der Gesetzgeber hat dies aufgegriffen.

[175] Vgl. Europäischer Gerichthof, Urteil vom 22. Juni 2021, C-439/19, Rn. 102.

11.1.4 Fazit

Bei der Novellierung des Bayerischen Gleichstellungsgesetzes hat der bayerische Gesetzgeber die Datenschutzrechte von Bewerberinnen und Bewerbern sowie von Beschäftigten im bayerischen öffentlichen Dienst im Blick behalten: In datenschutzrechtlicher Hinsicht hat er die bewährte Linie fortgeführt und zugleich die Gelegenheit zu hilfreichen Klarstellungen genutzt. Besonders gefreut hat es mich, dass ich mich schon frühzeitig in das Gesetzgebungsverfahren einbringen konnte.

11.2 Feststellung der Verfassungstreue bei Bewerberinnen und Bewerbern für den bayerischen öffentlichen Dienst

Zum 1. Januar 2026 sind verschiedene Änderungen des Bayerischen Beamtengesetzes (BayBG) in Kraft getreten.[176] Aus Datenschutzsicht besonders bedeutsam ist der in diesem Zug neu angefügte Art. 19 Abs. 2 BayBG. Gegenstand dieser Regelung sind Anfragen von bayerischen öffentlichen – insbesondere staatlichen und kommunalen – Einstellungs- und Ernennungsbehörden an das Landesamt für Verfassungsschutz, ob diesem Erkenntnisse vorliegen, die Zweifel an der Verfassungstreue von Bewerberinnen und Bewerbern für den bayerischen öffentlichen Dienst begründen können. Die Thematik ist nicht neu: Entsprechende Anfragen waren für Einstellungs- und Ernennungsbehörden schon bislang ein Mittel, um die Verfassungstreue von Bewerberinnen und Bewerbern in Einstellungsverfahren zu prüfen. In der Vergangenheit kontrovers diskutiert war dabei vor allem die Frage, ob und inwieweit solche Anfragen erst bei zuvor bestehenden Zweifeln an der Verfassungstreue oder auch „verdachtsunabhängig" als sogenannte „Regelanfragen"[177] erfolgen konnten.

11.2.1 Hintergrund und bisherige Rechtslage

Im öffentlichen Dienst Beschäftigte sind zur Verfassungstreue verpflichtet. Für Beamtinnen und Beamte ergibt sich diese Verfassungstreuepflicht insbesondere aus den hergebrachten Grundsätzen des Berufsbeamtentums (vgl. Art. 33 Abs. 5 Grundgesetz – GG) und aus Art. 33 Abs. 1 Satz 3 Beamtenstatusgesetz (BeamtStG), für Tarifbeschäftigte der Länder aus § 3 Abs. 1 Satz 2 Tarifvertrag für den öffentlichen Dienst der Länder und für Tarifbeschäftigte der Kommunen etwa aus § 3 Abs. 1.1 Satz 2 Tarifvertrag für den öffentlichen Dienst für den Bereich Verwaltung im Bereich der Vereinigung der kommunalen Arbeitgeberverbände. Die Gewähr dafür zu bieten, jederzeit für die freiheitliche demokratische Grundordnung im Sinne des Grundgesetzes einzutreten, ist Voraussetzung, um in ein Beamtenverhältnis berufen werden zu können (§ 7 Abs. 1 Satz 1 Nr. 2 BeamtStG). Die Prüfung dieser Eignungsvoraussetzung obliegt dabei den Einstellungs- und Ernennungsbehörden.[178]

[176] Vgl. § 1 und § 10 Satz 1 Gesetz zur Änderung dienstrechtlicher Vorschriften vom 23. Dezember 2025 (GVBl. S. 643).
[177] Vgl. Landtags-Drucksache 19/7769, S. 10.
[178] Landtags-Drucksache 19/7769, S. 9.

Einzelheiten zur Prüfung der Verfassungstreue von Bewerberinnen und Bewerbern für den bayerischen öffentlichen Dienst fanden sich bislang in der Verfassungstreue-Bekanntmachung (VerftöDBek) vom 3. Dezember 1991.[179] Als ausreichend wurde es insoweit grundsätzlich erachtet, Bewerberinnen und Bewerber über ihre Verfassungstreuepflicht zu belehren und sie daraufhin einen Fragebogen ausfüllen sowie bestimmte Erklärungen unterschreiben zu lassen (vgl. Teil 2 Nr. 1 VerftöDBek). Schon hiernach konnte diese Prüfung gegebenenfalls auch eine Anfrage beim Landesamt für Verfassungsschutz umfassen, ob dort Tatsachen bekannt sind, die Bedenken gegen die Einstellung der betreffenden Bewerberinnen und Bewerber begründen können. Entsprechende Anfragen setzten dabei grundsätzlich Zweifel an der Verfassungstreue von Bewerberinnen oder Bewerbern voraus, etwa wenn diese sich weigerten, die vorgesehenen Erklärungen zu unterschreiben (vgl. Teil 2 Nr. 2 VerftöDBek). Die betroffenen Bewerberinnen und Bewerber mussten der Anfrage beim Landesamt für Verfassungsschutz ferner grundsätzlich zuvor zugestimmt haben; verweigerten sie ihre Zustimmung, schied eine Einstellung in den bayerischen öffentlichen Dienst allerdings aus (vgl. Teil 2 Nr. 1 VerftöDBek). „Verdachtslose" Anfragen erfolgten demgegenüber bislang nur im Hinblick auf bestimmte Personengruppen (vgl. Teil 2 Nrn. 4.2 und 4.3 VerftöDBek) oder im Zusammenhang mit der Berufung in ein Richterverhältnis (Teil 2 Nr. 4.1 und Teil 3 VerftöDBek); zu der letztgenannten Konstellation hatte ich mich bereits in meinem 27. Tätigkeitsbericht 2016 unter Nr. 5.1.6 geäußert.

Zusammenfassend ging die Verfassungstreue-Bekanntmachung damit davon aus, dass Bewerberinnen und Bewerber für den bayerischen öffentlichen Dienst grundsätzlich verfassungstreu sind. Anfragen beim Landesamt für Verfassungsschutz erfolgten – außerhalb der Richterschaft – grundsätzlich nur bei Vorliegen entsprechender Zweifel.

11.2.2 Neuregelung in Art. 19 Abs. 2 BayBG

Art. 19 Abs. 2 Satz 1 BayBG weicht von diesem Verständnis nunmehr ab: Anfragen beim Landesamt für Verfassungsschutz sind im Einstellungsverfahren für den bayerischen öffentlichen Dienst jetzt grundsätzlich verdachtsunabhängig zulässig – jedenfalls für bestimmte Fachlaufbahnen und fachliche Schwerpunkte, die durch Verordnung der Staatsregierung noch näher zu bezeichnen sind. Die Vorschrift legt ferner abschließend fest, welche Bewerbungsdaten an das Landesamt für Verfassungsschutz im Rahmen einer Anfrage zu übermitteln sind (Art. 19 Abs. 2 Satz 2 BayBG) und trifft Vorgaben zur Aufbewahrung der vom Landesamt an die Einstellungs- und Ernennungsbehörden übermittelten Daten (Art. 19 Abs. 2 Satz 3 BayBG).

> **Art. 19 BayBG**
> **Feststellung der Eignung**
> [...]
> (2) [1]Zur Feststellung der Verfassungstreue eines Bewerbers oder einer Bewerberin können die Ernennungsbehörden vor Einstellungen in bestimmte, durch Verordnung der Staatsregierung näher bezeichnete Fachlaufbahnen und fachliche Schwerpunkte das Landesamt für Verfassungsschutz um Auskunft ersuchen, ob und gegebenenfalls welche Erkenntnisse vorliegen, die Zweifel daran begründen können, dass der Bewerber oder die Bewerberin Gewähr dafür bietet, jederzeit für die freiheitliche demokratische Grundordnung im Sinne des Grund-

[179] AIIMBl. S. 895.

gesetzes einzutreten. [2]Hierzu übermittelt die Ernennungsbehörde dem Landesamt für Verfassungsschutz Namen, Vornamen, Geburtsnamen, Geburtsdatum, Geburtsort, Geschlecht und Staatsangehörigkeit des Bewerbers oder der Bewerberin. [3]Die vom Landesamt für Verfassungsschutz übermittelten Daten werden so zu den Bewerbungs- oder Einstellungsunterlagen genommen, dass sie mittels verschlossenen Umschlags oder durch technische und organisatorische Maßnahmen vor dem Zugriff Unbefugter geschützt sind. [4]Die Sätze 1 bis 3 gelten entsprechend für die erstmalige Berufung in ein Richterverhältnis sowie vor der erstmaligen Übertragung eines Amtes in durch die Verordnung nach Satz 1 näher bezeichneten Fachlaufbahnen und fachlichen Schwerpunkten.

Diese Regelungen gelten sowohl für erstmalige Berufungen in das Richterverhältnis (Art. 19 Abs. 2 Satz 4 BayBG) als auch für den gesamten (tarif-)vertraglichen Bereich (Art. 145 Abs. 2 BayBG in Verbindung mit Art. 19 Abs. 2 BayBG) entsprechend. Während die bisherige Verfassungstreue-Bekanntmachung unmittelbar nur im Hinblick auf Beschäftigte des Freistaates Bayern anwendbar ist und für die Kommunen und für die sonstigen der Aufsicht des Freistaates Bayern unterliegenden juristischen Personen des öffentlichen Rechts lediglich Empfehlungscharakter aufweist (Teil 4 VerftöDBek), adressiert Art. 19 Abs. 2 BayBG nunmehr alle in Art. 1 Abs. 1 BayBG genannten Dienstherren und öffentlichen Arbeitgeber – und damit insbesondere auch die bayerischen Kommunen. Insgesamt ist infolge dieser Neuregelung demzufolge mit einer erheblichen Ausweitung und Zunahme von Anfragen beim Landesamt für Verfassungsschutz in Einstellungsverfahren zu rechnen.

11.2.3 Datenschutzrechtliche Bewertung

Aus datenschutzrechtlicher Sicht ist die Verarbeitung personenbezogener Bewerbungsdaten zur Feststellung der Verfassungstreue in dem eingangs aufgezeigten grundrechtlichen Rahmen zulässig, sofern insbesondere die europarechtlich verankerten datenschutzrechtlichen Vorgaben – allen voran die Datenschutz-Grundsätze nach Art. 5 DSGVO – eingehalten werden. So müssen entsprechende Datenverarbeitungen insbesondere auf eine hinreichende Rechtsgrundlage gestützt werden können (Grundsatz der „Rechtmäßigkeit" der Verarbeitung, Art. 5 Abs. 1 Buchst. a Var. 1, Art. 6 Abs. 1 DSGVO) und für die Erreichung des verfolgten Zwecks erforderlich und angemessen sein (Grundsatz der „Datenminimierung", Art. 5 Abs. 1 Buchst. c DSGVO).

Für Auskünfte des Landesamts für Verfassungsschutz stellt in vorliegendem Zusammenhang Art. 25 Abs. 2 Nr. 3 Buchst. b Doppelbuchst. aa Bayerisches Verfassungsschutzgesetz eine Rechtsgrundlage bereit. Anfragen der Einstellungs- und Ernennungsbehörden wurden bislang auf Art. 103 Satz 1 BayBG gestützt.[180] Diese Norm stellt zwar eine spezifische Befugnis zur Verarbeitung von Bewerbungsdaten durch bayerische Dienstherren und – in Verbindung mit Art. 145 Abs. 2 BayBG – öffentliche Arbeitgeber dar, regelt Anfragen zur Verfassungstreue beim Landesamt für Verfassungsschutz jedoch nicht ausdrücklich.

Der bayerische Gesetzgeber hat allerdings zutreffend erkannt, dass die beschriebenen Regelanfragen schon „aufgrund ihrer Verdachtslosigkeit sowie aufgrund ihrer großen Streubreite" einen „besonders intensiven Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Personen" nach Art. 2 Abs. 1 in

[180] Vgl. Landtags-Drucksache 19/7769, S. 9 f.

Verbindung mit Art. 1 Abs. 1 GG darstellen.[181] Es ist daher aus Datenschutzsicht zunächst zu begrüßen, dass der Gesetzgeber, sofern er solche Anfragen im Einstellungsverfahren für erforderlich erachtet, die damit zusammenhängenden Verarbeitungen personenbezogener Daten insbesondere im Hinblick auf deren Voraussetzungen und Umfang in Art. 19 Abs. 2 BayBG nunmehr ausdrücklich gesetzlich regelt.

Leider führt die Gesetzesbegründung nicht näher aus, weshalb der Gesetzgeber eine Ausweitung der Regelanfrage gegenüber der bisherigen Praxis für erforderlich erachtet hat. Dies ist auch deshalb misslich, weil Art. 19 Abs. 2 Satz 1 BayBG die nähere Festlegung des „Ob" einer Regelanfrage zunächst der Staatsregierung als Verordnungsgeber überlässt. Immerhin macht die Gesetzesbegründung deutlich, dass entsprechende Anfragen beim Landesamt „insbesondere bei Bewerbungen für Tätigkeitsbereiche, die im Hinblick auf die Sicherheit der Bevölkerung innerhalb des Staatsgefüges eine besondere Stellung einnehmen", relevant sind.[182] Es bleibt zu hoffen, dass dieser differenzierte Ansatz auch in der späteren Verordnung der Staatsregierung Niederschlag finden wird.

Jedenfalls ist im künftigen Vollzug des Art. 19 Abs. 2 Satz 1 BayBG im Blick zu behalten, dass diese Vorschrift Anfragen beim Landesamt für Verfassungsschutz nicht in jedem Fall verpflichtend vorsieht, sondern den Einstellungs- und Ernennungsbehörden ein Ermessen einräumt („können"). Diese müssen bei der Einstellung vertraglich Beschäftigter ferner berücksichtigen, dass die Treuepflicht von Arbeitnehmerinnen und Arbeitnehmern des öffentlichen Dienstes nach der Rechtsprechung des Bundesarbeitsgerichts nicht in jedem Fall mit derjenigen von Beamtinnen und Beamten vergleichbar ist – maßgebend sind insoweit Stellung und Aufgabenkreis der betreffenden Beschäftigten.[183] Es bleibt daher zu erwarten, dass im Hinblick auf verdachtsunabhängige Anfragen kein „Automatismus" eintritt, sondern deren Erforderlichkeit unter Berücksichtigung insbesondere der künftigen Stellung und des künftigen Aufgabenkreises der betroffenen Bewerberinnen und Bewerber kritisch geprüft wird.

Ferner ist auf ein datenschutzkonformes Verfahren zur Durchführung von Regelanfragen zu achten. Sofern sich entsprechende Vorgaben nicht bereits aus bestehendem, insbesondere europäischem Datenschutzrecht ergeben, bietet sich für die nähere Ausgestaltung dieses Verfahrens aus meiner Sicht entweder die zu Art. 19 Abs. 2 Satz 1 BayBG noch zu erlassende Verordnung der Staatsregierung oder gegebenenfalls auch eine „fortgeführte" Verfassungstreue-Bekanntmachung an.

In diesem Zusammenhang habe ich das innerhalb der Bayerischen Staatsregierung für das Dienstrecht federführend zuständige Bayerische Staatsministerium der Finanzen und für Heimat im Rahmen des Gesetzgebungsverfahrens insbesondere auf die folgenden Punkte hingewiesen:

— Der bisherigen Praxis entsprechend (vgl. Teil 2 Nr. 4.4 VerftöDBek) sollten Regelanfragen beim Landesamt für Verfassungsschutz erst im Falle einer hinrei-

[181] Landtags-Drucksache 19/7769, S. 10.
[182] Landtags-Drucksache 19/7769, S. 9.
[183] Bundesarbeitsgericht, Urteil vom 6. September 2012, 2 AZR 372/11.

chenden „Einstellungsexspektanz“ erfolgen. Vor diesem Zeitpunkt wird es solchen Anfragen regelmäßig an der Erforderlichkeit im Sinne von Art. 5 Abs. 1 Buchst. c, Art. 6 Abs. 1 DSGVO fehlen.

— Die Durchführung von (Regel-)Anfragen beim Landesamt für Verfassungsschutz ist für die betroffenen Bewerberinnen und Bewerber hinreichend transparent auszugestalten (Grundsatz der „Transparenz“ der Verarbeitung, Art. 5 Abs. 1 Buchst. a Var. 3 DSGVO). Einstellungsbehörden haben in jedem Fall ihre Informationspflichten nach Art. 13 f. DSGVO zu erfüllen. Aufgrund der Sensibilität entsprechender Anfragen habe ich ferner angeregt, das zugrunde liegende Verfahren kompakt und verständlich, etwa in einem Informationsblatt für Bewerberinnen und Bewerber, darzustellen. Ziel sollte dabei stets sein, Bewerberinnen und Bewerbern für den bayerischen öffentlichen Dienst den Umstand und das Ausmaß von Anfragen beim Landesamt für Verfassungsschutz im Rahmen von Einstellungsverfahren klar und transparent zu kommunizieren.

— Ferner habe ich empfohlen zu prüfen, ob das Zustimmungserfordernis für Regelanfragen nach Teil 2 Nr. 4.4 Satz 1 VerftöDBek gegebenenfalls fortgeführt werden soll. Zwar stellt eine solche Zustimmung der betroffenen Person im vorliegenden Zusammenhang schon mangels Freiwilligkeit (vgl. Art. 4 Nr. 11 DSGVO) keine wirksame datenschutzrechtliche Einwilligung im Sinne von Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO dar. Gleichwohl kann eine vorherige Zustimmung als tatbestandliche Voraussetzung für Regelanfragen den damit einhergehenden Grundrechtseingriff schonender ausgestalten. Zugleich würde sie sicherstellen, dass betroffene Personen von der Anfrage erfahren.

— Zum Schutz der Persönlichkeitsrechte von Bewerberinnen und Bewerbern ist festzulegen, wie die Einstellungs- und Ernennungsbehörden bei Zweifeln an der Verfassungstreue weiter verfahren. Nicht zuletzt im Hinblick auf mögliche „Fehltreffer“ („false positives“) sollte betroffenen Personen aus meiner Sicht ein Anhörungsrecht eingeräumt werden (vgl. Teil 2 Nrn. 5 und 6 VerftöDBek).

— Schließlich sind angemessene Löschfristen für die übermittelten Daten festzulegen (Grundsatz der „Speicherbegrenzung“, Art. 5 Abs. 1 Buchst. e DSGVO) – sowohl im Hinblick auf die Einstellungs- und Ernennungsbehörden als auch im Hinblick auf das Landesamt für Verfassungsschutz.

11.2.4 Fazit

Mit Art. 19 Abs. 2 BayBG hat der Gesetzgeber Anfragen von bayerischen öffentlichen – insbesondere staatlichen und kommunalen – Einstellungs- und Ernennungsbehörden an das Landesamt für Verfassungsschutz zur Feststellung der Verfassungstreue von Bewerberinnen und Bewerbern für den bayerischen öffentlichen Dienst gesetzlich geregelt. Gegenüber der bisherigen Rechtslage dürften „verdachtsunabhängige“ (Regel-)Anfragen dabei künftig deutlich zunehmen. Umso mehr ist auf eine datenschutzkonforme und möglichst grundrechtsschonende Ausgestaltung dieses Anfrageverfahrens zu achten. Entsprechende Hinweise habe ich bereits in das Gesetzgebungsverfahren eingebracht. Zugleich habe ich das für das Dienstrecht innerhalb der Staatsregierung federführend zuständige Finanzministerium gebeten, mich in die weitere Ausgestaltung dieses Verfahrens frühzeitig einzubinden.

11.3 Beschäftigtennamen in dienstlichen Schreiben

Im Berichtszeitraum schilderte mir ein Beschäftigter einer bayerischen Stadt, dass Vor- und Nachnamen von Sachbearbeiterinnen und Sachbearbeitern auf dem gesamten Schriftverkehr der Stadt – etwa auf Meldebescheinigungen, Melderegisterauskünften, Führungszeugnissen, Aufenthaltsermittlungen, Aufforderungen zur Anmeldung etc. – abgedruckt werden. Zudem werde in dienstlichen E-Mail-Adressen zwingend der Vor- und Nachname der Beschäftigten angegeben. Dienstliche Schreiben müssten außerdem eigenhändig unterschrieben werden. Diese Vorgaben sollten nach Vorstellung der Stadt dazu dienen, den persönlichen Kontakt aus Gründen der Bürgerfreundlichkeit zu erleichtern. Der betroffene Beschäftigte sah jedoch seine Privatsphäre gefährdet, weil auf diese Weise Bürgerinnen und Bürger personenbezogene Daten der Beschäftigten inklusive der Original-Unterschriften erhalten würden.

Zu ähnlichen Fragestellungen bei der Verarbeitung von Beschäftigtendaten im Publikumsverkehr hatte ich mich bereits in früheren Tätigkeitsberichten mehrfach geäußert, etwa in dem Beitrag Nr. 19.1 meines 22. Tätigkeitsberichts 2006, in dem Beitrag Nr. 11.8.7 meines 25. Tätigkeitsberichts 2012 und in dem Beitrag Nr. 7.5 meines 33. Tätigkeitsberichts 2023.

Bei genauer Betrachtung umfasste die eingangs geschilderte Anfrage allerdings verschiedene Einzelaspekte, die aus Datenschutzsicht differenziert zu betrachten waren:

11.3.1 Grundlegendes zur Verarbeitung von Beschäftigtendaten in dienstlichen Schreiben

Mit der Offenlegung von Beschäftigtendaten in amtlichen Schreiben verarbeitet die jeweilige bayerische – insbesondere staatliche oder kommunale – öffentliche Stelle personenbezogene Sachaktendaten ihrer Beschäftigten zu organisatorischen Zwecken. Um rechtmäßig zu sein, muss diese Verarbeitung auf eine Verarbeitungsbefugnis gestützt werden können. Üblicherweise bietet Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 DSGVO in Verbindung mit Art. 4 Abs. 1 BayDSG für dienststelleninterne Offenlegungen oder in Verbindung mit Art. 5 Abs. 1 Satz 1 Nr. 1 Var. 1 BayDSG für Übermittlungen „nach außen“ eine entsprechende Befugnis, wenn und soweit die Verarbeitung zur Erfüllung einer der öffentlichen Stelle obliegenden Aufgabe erforderlich ist. Die Erforderlichkeit einer Verarbeitung ist nach ständiger Rechtsprechung des Europäischen Gerichtshofs gemeinsam mit dem Grundsatz der Datenminimierung nach Art. 5 Abs. 1 Buchst. c DSGVO zu prüfen, in welchem wiederum der Grundsatz der Verhältnismäßigkeit zum Ausdruck kommt.[184]

Im Rahmen der hiernach gebotenen Erforderlichkeitsprüfung ist damit einerseits das Datenschutzinteresse der betroffenen Person zu berücksichtigen. Andererseits kann die eigene Funktionsfähigkeit der öffentlichen Stelle dergestalt zu berücksichtigen sein, dass den Bürgerinnen und Bürgern jeweilige Ansprechpartnerinnen und Ansprechpartner zumindest soweit bekannt sein müssen, dass eine dienstliche Kontaktaufnahme und Kommunikation unschwer möglich ist.

[184] Vgl. nur Europäischer Gerichtshof, Urteil vom 9. Januar 2025, C-394/23, Rn. 24 und 49.

11.3.2 Vor- und Nachnamen in dienstlichen Schreiben

Dabei wird es aber regelmäßig nicht erforderlich sein, Vor- und Nachnamen von Sachbearbeiterinnen und Sachbearbeitern offenzulegen. In amtlichen Schreiben wird grundsätzlich die Offenbarung des Nachnamens genügen, damit Bürgerinnen und Bürger mit der Ansprechperson Kontakt aufnehmen können. Sollte es mehrere Beschäftigte mit demselben Nachnamen geben, kann etwa der Vorname mit einem Initialbuchstaben abgekürzt angegeben werden.

Soweit der Dienstherr oder öffentliche Arbeitgeber in jedem Fall auf eine Angabe von Vor- und Nachnamen von Beschäftigten in amtlichen Schreiben bestehen sollte, halte ich hierfür eine gesonderte Begründung für notwendig. Die öffentliche Stelle ist als datenschutzrechtlich Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO, Art. 3 Abs. 2 BayDSG – auch gegenüber der Datenschutzaufsichtsbehörde – rechenschaftspflichtig gemäß Art. 5 Abs. 2 DSGVO; sie muss damit unter anderem die Rechtmäßigkeit der Verarbeitung gemäß Art. 5 Abs. 1 Buchst. a, Art. 6 Abs. 1 DSGVO und somit – auf den konkreten Fall bezogen – die Erforderlichkeit der Angabe von Vor- und Nachnamen auf dienstlichen Schreiben nachweisen können.

Sollte die öffentliche Stelle es hiernach für erforderlich erachten, neben dem Nachnamen ausnahmsweise auch den Vornamen der Beschäftigten in dienstlichen Schreiben offenzulegen, so halte ich es dennoch zum Schutz der betroffenen Personen für notwendig, diesen die Möglichkeit eines Widerspruchs einzuräumen. Diese Ansicht habe ich bereits vor Geltung der Datenschutz-Grundverordnung vertreten. Einzelheiten können dem Beitrag Nr. 19.1 meines 22. Tätigkeitsberichts 2006 entnommen werden. Im Geltungsbereich der Datenschutz-Grundverordnung halte ich an dieser Ansicht grundsätzlich fest. Das in Betracht kommende Widerspruchsrecht folgt nunmehr ohnehin aus Art. 21 Abs. 1 DSGVO. Dieses Betroffenenrecht ist vorliegend einschlägig, weil die zugrunde liegende Verarbeitung von Beschäftigtendaten, wie aufgezeigt, auf Grundlage von Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO erfolgt. Für die Widerspruchsgründe gemäß Art. 21 Abs. 1 DSGVO – also für die Gründe, die sich aus der besonderen Situation der betroffenen Person ergeben, – müsste dann die jeweilige persönliche Situation der betroffenen Person betrachtet werden. Zu berücksichtigen wäre etwa, ob der betroffenen Person private Belästigungen drohen könnten. Dies wird regelmäßig anzunehmen sein, wenn Beschäftigte mit der Erstellung belastender Verwaltungsakte befasst sind. Bei der vorzunehmenden Abwägung wären zudem auch die konkreten Aufgaben und Funktionen der Beschäftigten zu betrachten.

Zu beachten ist, dass das Widerspruchsrecht ein Recht der betroffenen Person ist, welches sie gegenüber dem datenschutzrechtlich Verantwortlichen geltend machen muss. Sollte der Dienstherr oder öffentliche Arbeitgeber die Angabe von Vor- und Nachnamen mit behördlichen Gründen rechtfertigen, so kann die betroffene Person ihr Widerspruchsrecht ihm gegenüber ausüben.

11.3.3 Eigenhändige Unterschriften in dienstlichen Schreiben

Die Vorgabe, dienstliche Schreiben eigenhändig zu unterschreiben, betrifft ebenfalls die Verarbeitung personenbezogener Daten – denn die Handschrift einer Person stellt ein personenbezogenes Datum im Sinne von Art. 4 Nr. 1 DSGVO

dar.[185] Im Rahmen der Erforderlichkeitsprüfung kann zugunsten der betroffenen Person berücksichtigt werden, dass bei einer Offenlegung der eigenhändigen Unterschrift etwa (insbesondere digitale) Unterschriftsfälschungen erleichtert werden könnten. Andererseits können aber – je nach Fallkonstellation – auch normative Formvorgaben, die Unterschriftserfordernisse vorsehen, zu beachten sein. Unzweifelhaft ist etwa eine eigenhändige Unterschrift anzubringen, wenn zwingende gesetzliche Formerfordernisse dies vorschreiben.

Soweit sich Formvorgaben aus der Allgemeinen Geschäftsordnung für die Behörden des Freistaates Bayern (AGO) ableiten lassen, gilt diese schon für Gemeinden – und vorliegend kam die Anfrage ja aus dem kommunalen Bereich – nicht unmittelbar; § 36 AGO enthält allerdings eine Anwendungsempfehlung. § 24 Abs. 1 Satz 1 AGO sieht zwar vor, dass Reinschriften von der unterschriftsberechtigten Person grundsätzlich eigenhändig unterschrieben werden sollen. Ausgenommen sind gemäß § 24 Abs. 1 Satz 2 AGO aber Dokumente, die in automatisierten Verfahren hergestellt oder elektronisch versendet werden. Die erste Alternative dürfte mittlerweile im Behördenalltag den Regelfall darstellen, weil automatisierte Verfahren jegliche Dokumenterstellung unter dem Einsatz von Datenverarbeitungssystemen meinen. Gemäß § 24 Abs. 1 Satz 3 AGO ist der Name der unterschreibenden Person in Druckschrift anzugeben; die Amtsbezeichnung kann angegeben werden. Reinschriften, die nicht eigenhändig unterschrieben werden, sind gemäß § 24 Abs. 1 Satz 4 AGO mit dem Namen der unterschriftsberechtigten Person zu versehen; diesem wird der Zusatz „gez." vorangestellt. Mit den – als bloße Verwaltungsvorschriften ohnehin untergesetzlichen – Vorgaben der Allgemeinen Geschäftsordnung für die Behörden des Freistaates Bayern, deren Anwendung für Gemeinden zudem nur empfohlen wird, lässt sich eine Pflicht zur eigenhändigen Unterschrift im Regelfall somit nicht begründen.

Außerhalb zwingender gesetzlicher Formerfordernisse sind mir keine normativen Vorgaben bekannt, die Beschäftigte zu eigenhändigen Unterschriften anhalten würden. Vor diesem Hintergrund müsste der datenschutzrechtlich Verantwortliche die Erforderlichkeit der eigenhändigen Unterschrift in Anbetracht seiner Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO nachvollziehbar begründen. Weshalb eine eigenhändige Unterschrift etwa eine größere Bürgernähe vermitteln sollte als eine maschinenschriftliche Namensangabe, ist mir nicht ersichtlich. Auch erscheint mir im Zeitalter elektronischer Kommunikation eine eigenhändige Unterschrift auf regelmäßigen behördlichen Schreiben, die ohnehin Aussteller und öffentliche Stelle erkennen lassen, nicht erforderlich zu sein; eine dadurch vermittelte etwaige erhöhte Legitimität vermag ich jedenfalls nicht zu erkennen.

11.3.4 Vor- und Nachnamen in dienstlichen E-Mail-Adressen

Soweit in dienstlichen E-Mail-Adressen Vor- und Nachnamen angegeben werden, die E-Mail-Adresse etwa nach dem Muster „Vorname.Nachname@Behörde.de" gebildet wird, handelt es sich meines Wissens um ein übliches Vorgehen bei bayerischen öffentlichen Stellen. Datenschutzrechtlich in der Regel unproblematisch ist dies dann, wenn die dienstliche E-Mail-Adresse nicht im Publikumsverkehr verwendet wird und somit Vor- und Nachnamen der Beschäftigten nicht gleichzeitig „nach außen" offengelegt werden. Sollte allerdings eine Verwendung der Vor- und Nachnamen enthaltenden E-Mail-Adressen im Publikumsverkehr erfolgen, so

[185] Vgl. Europäischer Gerichtshof, Urteil vom 20. Dezember 2017, C-434/16, Rn. 36 f.

gelten für die rechtliche Bewertung die obigen Ausführungen unter Nr. 11.3.2 zu Vor- und Nachnamen in dienstlichen Schreiben entsprechend. Aus Datenschutzsicht halte ich die Verwendung von Funktions-E-Mail-Adressen, beispielsweise für behördliche Datenschutzbeauftragte nach dem Muster „Datenschutz@Behörde.de“, in der Kommunikation nach außen grundsätzlich für vorzugswürdig.

11.3.5 Abschließende Bemerkungen

Welche Erwägungen für oder gegen die Verarbeitung von Beschäftigtennamen im dienstlichen Kommunikationsverkehr sprechen, lässt sich oft nur im Einzelfall unter Kenntnis der besonderen Gegebenheiten vor Ort klären. Für betroffene Beschäftigte ist es daher empfehlenswert, sich mit ihrem Anliegen (gegebenenfalls zunächst) an den behördlichen Datenschutzbeauftragten ihrer öffentlichen Stelle zur weiteren Beratung zu wenden: Der behördliche Datenschutzbeauftragte hat unter anderem die Aufgabe, die Einhaltung der datenschutzrechtlichen Vorschriften bei der jeweiligen öffentlichen Stelle zu überwachen (Art. 39 Abs. 1 Buchst. b DSGVO), und ist mit den örtlichen Gegebenheiten vertraut. Betroffenen Personen steht der behördliche Datenschutzbeauftragte insoweit als Ansprechpartner zur Verfügung (Art. 38 Abs. 4 DSGVO). Er handelt bei der Erfüllung seiner Aufgaben weisungsfrei und ist zur Verschwiegenheit verpflichtet (Art. 38 Abs. 3 Satz 1, Abs. 5 DSGVO).

Betroffenen Bediensteten bleibt es aber natürlich unbenommen, sich – gegebenenfalls im Anschluss – im Wege einer förmlichen datenschutzrechtlichen Beschwerde nach Art. 77 DSGVO, Art. 20 Abs. 1 BayDSG an mich zu wenden.

11.4 „Sammelermächtigungen“ für Bedienstete der Jugendämter

In den durch das Bürgerliche Gesetzbuch vorgesehenen Fällen der Beistandschaft, (vorläufigen) Amtspflegschaft und (vorläufigen) Amtsvormundschaft sind die Jugendämter als Beistand, Pfleger oder Vormund tätig (§ 55 Abs. 1 Sozialgesetzbuch Achtes Buch – Kinder- und Jugendhilfe – SGB VIII). Nach § 59 Abs. 1 Satz 1 SGB VIII sind die Jugendämter befugt, bestimmte Beurkundungen vorzunehmen, beispielsweise von Erklärungen über die Anerkennung der Vaterschaft (§ 59 Abs. 1 Satz 1 Nr. 1 SGB VIII). Die Ausübung beziehungsweise die Wahrnehmung dieser Aufgaben übertragen die Jugendämter auf einzelne ihrer Beschäftigten beziehungsweise ermächtigen diese hierzu (§ 55 Abs. 2 Satz 1 und § 59 Abs. 3 Satz 1 SGB VIII). Was „auf dem Papier“ – auch durch die „Datenschutzbrille“ betrachtet – zunächst unverfänglich klingt, birgt in der praktischen Umsetzung gleichwohl Fehlerpotential, wie der folgende Fall anschaulich zeigt:

Ein bayerisches Landratsamt – Kreisjugendamt hatte vor geraumer Zeit entsprechende Ermächtigungen nach § 55 Abs. 2 Satz 1 und § 59 Abs. 3 Satz 1 SGB VIII schriftlich ausgestellt. Diese waren jedoch nicht für jede vom Landratsamt ermächtigte Person einzeln formuliert worden. Vielmehr wurden „aus Gründen der Vereinfachung“ bis zu elf Beschäftigte durch ein einzelnes Dokument ermächtigt. In diesen „Sammelermächtigungen“ waren die betroffenen Beschäftigten jeweils mit Vor- und Nachnamen benannt. Außerdem war unter anderem die jeweilige Amtsbezeichnung aufgeführt. Die dergestalt ermächtigten Beschäftigten enthielten jeweils eine Ausfertigung dieser Sammelermächtigung.

Die Beschwerdeführerin – die nach eigenen Angaben bereits seit mehreren Jahren nicht mehr im Bereich des Kreisjugendamts tätig war – wandte sich nun mit der Annahme an mich, dass alle auf den Ermächtigungen genannten Kolleginnen und Kollegen diese Sammelermächtigungen noch besäßen und diese damit noch im Umlauf seien. Die Beschwerdeführerin war der Ansicht, dass sich ihre Kolleginnen und Kollegen nicht mit einer Ermächtigung legitimieren dürften, die auch ihre persönlichen Daten enthalte. Manche Ermächtigungen würden beispielsweise in notarielle Urkunden bei Adoptionen oder in Ermittlungsakten der Polizei aufgenommen. Damit würden im jeweiligen Zusammenhang personenbezogene Daten der Beschwerdeführerin verarbeitet, auch wenn sie mit dem konkreten Fall gar nichts zu tun habe. Insofern müsse das Landratsamt die Sammelermächtigungen „aus dem Verkehr ziehen“ und durch Einzelermächtigungen ersetzen. Dies habe die Beschwerdeführerin auch bereits gegenüber dem Landratsamt geltend gemacht, von dort allerdings keine abschließende Rückmeldung erhalten. Die Beschwerdeführerin hatte mir „ihre“ jeweiligen Sammelermächtigungen in Kopie vorgelegt. Diese waren im Briefkopf an die Beschwerdeführerin adressiert, enthielten jedoch, wie von ihr vorgetragen, die oben genannten Angaben auch zu den weiteren ermächtigten Bediensteten.

In einer ersten Einschätzung konnte ich die Vorbehalte der Beschwerdeführerin gut nachvollziehen: Mit der Ausfertigung von Sammelermächtigungen hat das Landratsamt personenbezogene Daten der betroffenen Beschäftigten verarbeitet (vgl. Art. 4 Nr. 1 und 2 DSGVO). Nach dem Grundsatz der Rechtmäßigkeit der Verarbeitung (Art. 5 Abs. 1 Buchst. a DSGVO) ist eine Verarbeitung personenbezogener Daten allerdings nur rechtmäßig, wenn diesbezüglich eine hinreichende Rechtsgrundlage im Sinne des Art. 6 Abs. 1 DSGVO vorliegt. Öffentliche Stellen verarbeiten personenbezogene Daten im Rahmen ihrer Aufgabenerfüllung dabei regelmäßig auf Grundlage des Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO, wobei die jeweilige Rechtsgrundlage für diese Verarbeitungen durch Unions- oder mitgliedstaatliches Recht festzulegen ist, Art. 6 Abs. 3 Satz 1 DSGVO. Da es vorliegend nicht um Personalakten-, sondern um Sachaktendaten Beschäftigter ging, stellt grundsätzlich Art. 4 Abs. 1 BayDSG in Verbindung mit § 55 Abs. 2 Satz 1 und § 59 Abs. 3 Satz 1 SGB VIII eine Rechtsgrundlage für die Ausfertigung entsprechender „Ermächtigungsdokumente“ bereit. Sowohl aus Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO als auch aus Art. 4 Abs. 1 BayDSG ergibt sich jedoch, dass die jeweilige Verarbeitung zur Aufgabenerfüllung der öffentlichen Stelle erforderlich sein muss. Der Europäische Gerichtshof hat in diesem Zusammenhang wiederholt betont, dass sich „die Ausnahmen und Einschränkungen hinsichtlich des Grundsatzes des Schutzes [personenbezogener] Daten auf das absolut Notwendige beschränken müssen“.[186]

Maßgebend im konkreten Fall war hiernach, ob und inwieweit die jeweilige Verarbeitung personenbezogener Beschäftigtendaten durch das Landratsamt zur Ausstellung der genannten Ermächtigungen erforderlich war. Dass eine solche Ermächtigung hinreichende Angaben zur Identifizierung der oder des jeweils ermächtigten Beschäftigten enthalten muss, liegt auf der Hand – hiergegen hatte sich die Beschwerdeführerin auch nicht gewandt. Nicht einleuchtend erschien mir aber, weshalb eine solche Ermächtigung auch personenbezogene Daten anderer ermächtigter Beschäftigter umfassen musste. Dies gilt umso mehr, wenn solche Ermächtigungen im Rechtsverkehr „nach außen“ Verwendung finden und zudem Daten von Beschäftigten umfassen, die mit dem konkreten Fall gar nicht befasst

[186] Vgl. nur Europäischer Gerichtshof, Urteil vom 1. August 2022, C-184/20, Rn. 85.

oder vielleicht sogar überhaupt nicht mehr für das Kreisjugendamt tätig sind. Auf Grundlage des geschilderten Sachverhalts konnte ich somit nicht erkennen, weshalb die Verarbeitung der personenbezogenen Daten der Beschwerdeführerin außerhalb der sie selbst betreffenden Ermächtigung – also sowohl für die Erstellung weiterer Ermächtigungen als auch für deren Verwendung – erforderlich gewesen wäre. Dies gilt selbstverständlich nicht nur für die Beschwerdeführerin, sondern gleichermaßen in Hinblick auf alle weiteren in den Sammelermächtigungen „mitgenannten" Beschäftigten.

Ich habe mich daher an das Landratsamt gewandt. Dieses hat den Sachverhalt bestätigt und mir mitgeteilt, dass es nunmehr „in Folge eines längeren Prozesses" schon damit befasst sei, die genannten Sammelermächtigungen vollständig einzuziehen und auf „Einzelermächtigungen" umzustellen, die allein Angaben zu dem oder der jeweils ermächtigten Bediensteten enthalten.

Da ich aus den Ausführungen des Landratsamts erkennen konnte, dass dieses den Beschwerdesachverhalt bereits vor meinem Einschreiten eigenständig analysiert hatte und schon damit befasst war, die datenschutzrechtliche Problematik zu beheben, habe ich für weitere datenschutzaufsichtliche Maßnahmen keinen Anlass mehr gesehen. So blieb mir nur die erfreuliche Pflicht, der Beschwerdeführerin mitzuteilen, dass das Landratsamt ihren berechtigten Bedenken abgeholfen hat. Noch erfreulicher wäre es natürlich gewesen, wenn das Landratsamt von Anfang an durch schriftliche „Einzelermächtigungen" keinen Anlass zur Beschwerde gegeben hätte.

12 Schulen

12.1 Beratung zur Änderung schulrechtlicher Vorschriften

Im Jahr 2025 wurden unter anderem das Bayerische Gesetz über das Erziehungs- und Unterrichtswesen, die Bayerische Schulordnung und die kultusministeriellen Bekanntmachungen betreffend „Offene Ganztagsangebote an Schulen", „Gebundene Ganztagsangebote an Schulen" sowie „Mittagsbetreuung und verlängerte Mittagsbetreuung an Grund- und Förderschulen" geändert. Betroffen waren dabei auch datenschutzrelevante Vorschriften. Ich habe das Bayerische Staatsministerium für Unterricht und Kultus jeweils eingehend beraten. Folgende Änderungen möchte ich hierbei herausgreifen:

12.1.1 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen

Mit der Änderung des Art. 31 Abs. 3 Satz 4 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG) ist das Kultusministerium erfreulicherweise meiner Forderung nach einer spezialgesetzlichen Regelung für die **Vorlage von erweiterten Führungszeugnissen** nachgekommen. Die Vorlagepflicht der Führungszeugnisse war bis dato lediglich in der Bekanntmachung des Bayerischen Staatsministeriums für Unterricht und Kultus über die Mittagsbetreuung und verlängerte Mittagsbetreuung an Grund- und Förderschulen[187] geregelt. Hierauf wurde ich durch eine Anfrage einer Gemeinde, die Träger einer Mittagsbetreuung ist, aufmerksam und habe mich daraufhin mit dem Kultusministerium in Kontakt gesetzt.

In Angleichung zur Regelung für sonstiges schulisches Personal sowie für Verwaltungs- und Hauspersonal wurde mit der Änderung damit auch für das Personal in Mittagsbetreuungen an Schulen in öffentlicher oder freier Trägerschaft eine spezialgesetzliche Grundlage geschaffen. Die Regelung soll klarstellen, dass auch die persönliche Eignung des Personals der Mittagsbetreuung durch ein höchstens drei Monate altes erweitertes Führungszeugnis gegenüber der Schulaufsicht nachzuweisen ist. Dies wurde durch einen Verweis in Art. 31 Abs. 3 Satz 4 BayEUG auf Art. 60a Abs. 2 und 3 BayEUG mit der Maßgabe der Vorlage bei der zuständigen Schulaufsicht explizit normiert. Für Personal von Mittagsbetreuungen in kommunaler Trägerschaft wird die Vorlagepflicht aufgrund des umfassten Art. 60a Abs. 3 Satz 4 Nr. 2 BayEUG in der Regel entfallen. Hierdurch werden unnötige Doppelprüfungen vermieden und dem Erforderlichkeitsgrundsatz Rechnung getragen.

Die Änderungen betrafen auch Art. 85a BayEUG, der bestimmt, welche Daten im Rahmen der Amtliche Schulverwaltungssoftware (ASV) verarbeitet werden dürfen. Hier wurde unter anderem das Merkmal **„Kinder beruflich Reisender und von Personen ohne ständigen festen Aufenthalt"** aufgenommen. Grundsätzlich sollen die Datenverarbeitungen in der ASV nicht zum „gläsernen Schüler" führen, weshalb die Erforderlichkeit stets besonders zu hinterfragen ist. Das Kultus-

[187] Vom 26. April 2021 (BayMBl. Nr. 316).

ministerium konnte mir jedoch überzeugend darlegen, dass die Verarbeitung dieses Merkmals erforderlich ist, um die Schulen bei Anmelde- und Wechselprozessen von Kindern beruflich Reisender zu unterstützen und eine qualitätsvolle Beschulung dieser Kinder sicherzustellen. Dass die Kenntnis für die aufnehmende Schule von Relevanz ist, um eine schulische Begleitung bestmöglich zu gewährleisten und beispielsweise Lehrkräfte einzusetzen, die sich dieser Kinder besonders annehmen, war für mich nachvollziehbar.

12.1.2 Bayerische Schulordnung

In Abschnitt 1 Nr. 3.2.11 von Anlage 2 der Bayerischen Schulordnung wird geregelt, welche Gesundheitsdaten im Schulverwaltungsprogramm gespeichert werden dürfen. Vor dem Hintergrund der besonderen Schutzbedürftigkeit dieser Daten sowie des Erforderlichkeitsgrundsatzes habe ich im Rahmen der Ressortanhörung zur Änderung der Bayerischen Schulordnung Bedenken bezüglich der geplanten Aufnahme der zusätzlichen Merkmale „Impfungen, Allergien und chronische Erkrankungen“ geäußert. So wurde die Aufnahme des Merkmals „Impfungen“ lediglich damit begründet, dass die Schulen bei der Überprüfung der Nachweispflicht im Rahmen des Masernschutzgesetzes unterstützt werden sollen. Insofern war die Erforderlichkeit der Verarbeitung anderer Impfungen für mich nicht erkennbar. Erfreulicherweise hat das Kultusministerium sodann auf die Aufnahme der zusätzlichen Merkmale gänzlich verzichtet.

12.1.3 Kultusministerielle Bekanntmachungen

Aufgrund der Änderung des Art. 31 Abs. 3 BayEUG waren auch die Bekanntmachungen „Offene Ganztagsangebote an Schulen“,[188] „Gebundene Ganztagsangebote an Schulen“[189] sowie „Mittagsbetreuung und verlängerte Mittagsbetreuung an Grund- und Förderschulen“[190] entsprechend anzupassen. Die nun vorgesehene direkte Vorlage der Führungszeugnisse durch das Personal (statt durch den Träger) bei der Schulleitung beziehungsweise Schulaufsichtsbehörde habe ich im Hinblick auf den Grundsatz der Direkterhebung ausdrücklich begrüßt. Ich habe das Kultusministerium sodann bei der konkreten Umsetzung in der Praxis, beispielsweise zur Kommunikation gegenüber Bewerberinnen und Bewerbern und zur Zurverfügungstellung eines Dokumentationsformblattes beraten.

12.2 Weiterleitung trotz Vertraulichkeitsbitte

Um einen Konfliktfall hinsichtlich der Bewertung eines versäumten Leistungsnachweises ihres Sohnes prüfen zu lassen, wandte sich eine Mutter an die zuständige Schulaufsichtsbehörde. Sie betonte hierbei, dass sie sich aktuell selbst noch um eine Klärung mit der Schulleitung bemühe und zunächst von der Schulaufsicht nur wissen möchte, ob das Vorgehen der Schulleitung in dieser Angelegenheit korrekt gewesen sei. Da sie persönliche Nachteile für ihren Sohn vermeiden

[188] Vom 30. März 2020 (BayMBl. Nr. 227).
[189] Vom 10. Februar 2020 (BayMBl. Nr. 86).
[190] Vom 26. April 2021 (BayMBl. Nr. 316).

wollte, bat die Mutter im Rahmen des Schriftverkehrs ausdrücklich um vertrauliche Behandlung ihres Anliegens.

Trotz der eindeutig geäußerten Bitte um Vertraulichkeit hat die Schulaufsicht das Anliegen inhaltlich und mit Angabe der personenbezogenen Daten an die betreffende Schule weitergegeben. Die Mutter hat hiervon erst im Nachgang durch bestimmte Äußerungen der Schulaufsicht Kenntnis erlangt. Sie legte daraufhin Beschwerde bei mir ein.

Im Rahmen der sodann eingeholten Stellungnahme argumentierte die Schulaufsicht, dass das Anliegen als Beschwerde eingeordnet und dementsprechend abgehandelt worden sei. Die Behandlung einer Beschwerde könne nicht anonymisiert erfolgen. Vielmehr sei es zwingend erforderlich mit der Schule in Kontakt zu treten und deren Stellungnahme einzuholen. Die Weiterleitung des Beschwerdeschreibens sei damit im Rahmen der Aufgabenerfüllung zulässig gewesen. Die Schulaufsicht räumte lediglich ein, dass den Transparenz- und Informationspflichten nicht vollständig genüge getan worden sei.

Die Schulaufsicht konnte damit allerdings die Erforderlichkeit zur Aufgabenerfüllung gemäß Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG in Verbindung mit Art. 114 Abs. 1 Nr. 4 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen nicht ausreichend darlegen. So konnten die Schreiben der Mutter bereits nicht als Beschwerde gewertet werden, da diese mehrfach betont hatte, dass sie zunächst nur eine Einschätzung zum Sachverhalt bei der Aufsichtsbehörde einholen möchte. Aber selbst wenn, wäre eine Datenübermittlung aufgrund des ausdrücklichen Wunsches auf vertrauliche Behandlung und der geäußerten Befürchtung von persönlichen Nachteilen im konkreten Fall nicht verhältnismäßig gewesen. Im Rahmen der Abwägung zwischen dem öffentlichen Interesse an der Aufgabenwahrnehmung der Schulaufsicht und dem informationellen Selbstbestimmungsrecht der Betroffenen überwiegt diese Position im konkreten Fall deutlich. Die Datenübermittlung erfolgte somit ohne die erforderliche Befugnis gemäß Art. 6 Abs. 1 UAbs. 1 DSGVO. Ich habe die Schulaufsichtsbehörde daraufhin gemäß Art. 58 Abs. 2 Buchst. b DSGVO verwarnt.

Für die Zukunft habe ich für den Fall, dass eine Bearbeitung jedenfalls einer als vertraulich bezeichneten Anfrage nur möglich ist, wenn eine Stellungnahme bei der Schule eingeholt wird und dafür eine Datenübermittlung erforderlich ist, empfohlen, hierauf vorab hinzuweisen. Wäre ein solcher Hinweis im vorliegenden Fall erfolgt, hätte die Mutter ihre Anfrage gegebenenfalls noch zurückziehen können.

Vor dem Hintergrund der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) möchte ich zusätzlich noch anmerken, dass selbst im Falle einer zulässigen Übermittlung stets zu prüfen ist, ob tatsächlich eine Weiterleitung des vollständigen Beschwerdeschreibens erforderlich oder nicht die Wiedergabe der relevanten Textpassagen ausreichend ist.

12.3 Hausbesuch vom Hausmeister

Manchmal kontaktieren mich mehrere Beteiligte fast zeitgleich in derselben Angelegenheit. So war es auch, als mich die Eltern eines Schulkindes baten, einen Sachverhalt zu bewerten, ohne dabei die betreffende Schule zu nennen. Nur wenige Tage später bat mich auch die betreffende Schule um Einschätzung der

Rechtslage, ohne die personenbezogenen Daten des betroffenen Kindes zu nennen. Angesichts der übereinstimmenden Schilderungen war für mich naheliegend, dass es sich um denselben Vorgang handelte.

Eine Schule hatte ihren Hausmeister an die Wohnadresse des Schulkindes gesandt, um dort die Anwesenheit des von den Eltern krankgemeldeten Kindes zu prüfen. Die Schule begründete dies mit ihrer Aufgabe zur Überwachung der Schulpflicht (vgl. Art. 85 Abs. 1 Satz 1, Art. 57 Abs. 2 Satz 1, Art. 35 Abs. 1 Satz 1 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen). Sie habe anonyme Hinweise erhalten, dass die Eltern das Kind wiederholt unzutreffend krankgemeldet hätten, um verlängerte Wochenendreisen durchzuführen.

Unabhängig von weiteren Gesichtspunkten – wie etwa die Beauftragung des Hausmeisters zu einem „Hausbesuch" und Weitergabe von Daten an ihn – könnte die beabsichtigte Datenverarbeitung (hier: Feststellung, ob das Kind zu Hause ist) nur dann zur Aufgabenerfüllung der Schule erforderlich sein, wenn sie überhaupt geeignet wäre, um die Erfüllung der Schulpflicht zu überwachen.

Die Eltern, die ihr Kind krankgemeldet hatten, trifft weder eine Pflicht, auf Klingeln die Tür zu öffnen, noch dem Hausmeister Auskünfte zu geben oder gar ihr Kind an der Tür vorzuzeigen. Auch wenn die Tür nicht geöffnet wird und/oder das Kind nicht zu Hause ist, könnte hieraus nicht der Schluss auf eine Verletzung der Schulpflicht gezogen werden. Je nach Art (etwa körperliche oder psychische Erkrankung) und Intensität der die Krankmeldung bestimmenden Beschwerden sowie der weiteren Umstände könnte sich das Kind beispielsweise ohne weiteres an einem anderen Ort aufhalten, etwa zur Betreuung, Beaufsichtigung oder Behandlung. Ebenso wenig würde eine festgestellte Anwesenheit des Kindes (etwa bei einem flüchtigen Sichtkontakt durch den Hausmeister) grundsätzlich eine Erkrankung belegen.

Die von der Schule beabsichtigte Datenerhebung ist also bereits in aller Regel kein geeignetes Mittel, um eine (vermeintliche) Verletzung der Schulpflicht aufzuklären.

Im Übrigen können Schulen nach Maßgabe von § 20 Abs. 2 Satz 1 Nr. 2 Bayerische Schulordnung (BaySchO) die Vorlage eines ärztlichen Zeugnisses verlangen, wenn sich krankheitsbedingte Schulversäumnisse einer Schülerin oder eines Schülers häufen oder Zweifel an der Erkrankung bestehen. Gemäß § 20 Abs. 2 Satz 2 BaySchO kann die Schule auch die Vorlage eines schulärztlichen Zeugnisses verlangen.

Die Schule zeigte sich schnell und umfassend einsichtig und versicherte, ein vergleichbares Vorgehen zukünftig zu unterlassen. Die Eltern wollten kein Beschwerdeverfahren betreiben. Weitere aufsichtliche Maßnahmen waren nicht veranlasst.

12.4 Heimliches Mithören eines Telefonats

Im Berichtszeitraum beschwerte sich ein Vater bei mir, weil er während eines Telefonats mit der Schule seines Kindes zu einem Pausenvorfall hörbares Flüstern im Hintergrund vernahm. Er hegte den Verdacht, seitens der Schule hätte mindestens eine weitere Person das Gespräch über Lautsprecher mitgehört.

Ich forderte die Schule auf, eine Stellungnahme abzugeben.

Die Schule räumte ein, dass die Lehrkraft versäumt habe, den Vater über das Aktivieren des Lautsprechers und die Anwesenheit einer Kollegin zu informieren. Auf Nachfrage teilte die Schule mit, dass die mithörende Lehrkraft weder in die Geschehnisse auf dem Pausenhof involviert, noch unterrichtende Lehrkraft des Kindes gewesen sei.

Das Mithörenlassen war weder durch eine gesetzliche Grundlage (etwa Art. 85 Abs. 1 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen) noch durch eine Einwilligung gedeckt. Offensichtlich war die gesprächsführende Lehrkraft aufgrund vorangegangener Vorwürfe des Vaters unsicher und wollte eine Art „Zeugin“ für den Inhalt des Telefonats. Mag dieses Anliegen auch nachvollziehbar sein, so darf dies nicht ohne Einwilligung des Gesprächspartners erfolgen.

Die Datenverarbeitung erfolgte nicht nur ohne Rechtsgrundlage (Art. 6 Abs. 1 UAbs. 1DSGVO), sondern verstieß zudem auch gegen den Grundsatz der Transparenz (Art. 5 Abs. 1 Buchst. a DSGVO) und der Zweckbindung (Art. 5 Abs. 1 Buchst. b DSGVO) und war geeignet das Vertrauen in die Datenverarbeitungen öffentlicher Stellen zu gefährden.

Ich habe die Schule daher gemäß Art. 58 Abs. 2 Buchst. b DSGVO verwarnt.

12.5 Werbung für das Landheim

Vor dem Besuch des Landheims einer Schule erhielten die Eltern der betreffenden Schülerinnen und Schüler ein Infoblatt mit der Bitte um Unterschrift und Rückgabe. Neben praktischen Hinweisen und Belehrungen zum Landheimbesuch war unter „weitere Hinweise" jedoch folgende Klausel versteckt:

> „Mit meiner Unterschrift bestätige ich, dass Bilder, die im Landheim aufgenommen wurden und auf denen mein Kind zu sehen ist, für den Landheimkalender, die Landheim-Homepage oder Postkarten verwendet werden dürfen.“

Ein aufmerksamer Vater übersandte mir das Infoblatt mit der Bitte um datenschutzrechtliche Prüfung. Daher nahm ich Kontakt zur Schule auf und bat um Erklärung. Im Rahmen der Korrespondenz wurde schnell klar, dass der Schule bereits das Verhältnis zum eingetragenen Verein, welcher das Landheim betreibt, nicht klar war. Auch über erforderliche Rechtsgrundlagen für einen etwaigen Datenaustausch zwischen der Schule und dem Verein hatte man sich offensichtlich bis dahin keine weiteren Gedanken gemacht.

Nach meiner Bitte um Darlegung der Verantwortlichkeit für die Datenverarbeitungen im Zusammenhang mit der genannten Klausel kam die Schule nach eigener Prüfung sodann zu dem Ergebnis, dass sie nach Art. 4 Nr. 7 DSGVO verantwortlich, der Landheimverein jedoch mit der Verarbeitung beauftragt sei. Da auf der Homepage nur Gruppenfotos ohne Erkennbarkeit Einzelner abgebildet seien, der Kalender nicht mehr produziert werde und die Postkarten nur Ansichten des Landheims zeigen würden, wäre die Klausel jedoch ohnehin gegenstandslos. Letztlich habe man nur versäumt, diese zu streichen.

Ich machte die Schule gleichwohl darauf aufmerksam, dass eine Auftragsverarbeitung gemäß Art. 28 DSGVO im konkreten Fall bereits deshalb nicht in Betracht kommt, weil ein Auftragsverarbeiter keine Verarbeitung für eigene Zwecke vornehmen darf. Eine Nachschau hatte jedoch ergeben, dass die Homepage des Landheims nicht nur der Schulfamilie zur Information dient, sondern auch der Werbung externer Gäste, denen es ebenfalls möglich ist, das Landheim zu mieten.

Ich habe die Schule sodann auch zur Ausgestaltung einer wirksamen Einwilligung gemäß Art. 4 Nr. 11 DSGVO beraten und insbesondere auch auf die Hervorhebungspflicht nach Art. 7 Abs. 2 Satz 1 DSGVO aufmerksam gemacht.

Im Hinblick auf den Einwand der Schule, dass auf der Homepage einzelne Personen konkret nicht zu erkennen seien, habe ich darauf hingewiesen, dass Fotoaufnahmen nur dann nicht mehr personenbeziehbar sind, wenn eine individuelle Zuordnung nicht mehr möglich ist. In diesem Zusammenhang ist zu beachten, dass insbesondere den Mitgliedern der Schulfamilie auch bei Gruppenfotos oder Fotos aus der Ferne eine Identifizierung regelmäßig möglich ist, da man sich durch das tägliche Lernen und Leben im Klassenverbund und in der Schulgemeinschaft kennt.

Vom Vater erhielt ich nach Abschluss meines Schriftverkehrs mit der Schule die erfreuliche Rückmeldung, dass Verbesserungen des Datenschutzniveaus bereits jetzt deutlich zu erkennen seien.

13 Informationsfreiheit

13.1 Einsicht in die nicht vorhandene Konzeptplanung

Einer Bürgerin war zu Ohren gekommen, dass ihre Gemeinde die Neubebauung eines Grundstückes plant. Wohnhaft in unmittelbarer Nähe zum Grundstück stellte sie deshalb einen Antrag auf Auskunft nach Art. 39 Abs. 1 BayDSG über die Konzeptentwicklung bei der Gemeinde.

Die Gemeinde lehnte den Antrag jedoch ab und berief sich darauf, dass es kein Verfahren und damit auch keine Akte hierzu geben würde, in die Einsicht gewährt werde könne. Daraufhin bat mich die Bürgerin um Unterstützung bei ihrem Auskunftsersuchen.

Im Rahmen der eingeholten Stellungnahme teilte mir die Gemeinde sodann mit, dass lediglich eine Konzeptplanung zur Bebauung des Grundstücks vorliege. Nachdem die Gemeinde keine weiteren Angaben dazu machte, entstand zunächst der Eindruck, dass die Gemeinde der Auffassung wäre, die genannte Konzeptplanung sei einem Auskunftsrecht gemäß Art. 39 BayDSG nicht zugänglich, da es kein „Verfahren" dazu gibt. Ich wies die Gemeinde deshalb auf Folgendes hin:

Nach Art. 39 Abs. 1 Satz 1 BayDSG hat jeder das Recht auf Auskunft über den Inhalt von Dateien und Akten öffentlicher Stellen. „Akten" sind dabei grundsätzlich alle amtlichen oder dienstlichen Zwecken dienenden Unterlagen. Ob die Unterlagen einem wie auch immer gearteten (formellen) „Verfahren" angehören, spielt für die Bestimmung des Anspruchsgegenstandes dabei keine Rolle.

Die Gemeinde antwortete hierauf, dass die Konzeptplanung bei den im Rathaus Beschäftigten zum Zeitpunkt der Ablehnung des Antrages nicht mehr bekannt gewesen sei und die Unterlagen erst im Nachgang durch Nachfragen aufgefunden werden konnten.

Die Gemeinde hielt es scheinbar weder für nötig, intensiv zu suchen, noch die Antragstellerin über die später aufgefundenen Informationen zu verständigen. Letztendlich konnte ich der Bürgerin im konkreten Fall zur beantragten Auskunft verhelfen. Ich möchte den Vorgang zum Anlass nehmen, darauf hinzuweisen, dass öffentliche Stellen eine Sorgfaltspflicht bei der Suche nach den angefragten Inhalten aus Dateien und Akten nach Art. 39 Abs. 1 BayDSG trifft. Eine Behauptung „ins Blaue hinein", dass nichts vorhanden sei, kann einen Verstoß gegen Art. 39 BayDSG darstellen.

13.2 Überprüfung von Schwärzungen

Bereits in meinem 34. Tätigkeitsbericht 2024 hatte ich unter Nr. 7.4 von der Eingabe eines Bürgers berichtet, dem die voraussichtlich anfallenden Kosten für die von ihm beantragte Auskunft nach Art. 39 Abs. 1 BayDSG über einen städtebaulichen Vertrag mit etwa 450,– Euro beziffert worden waren. Nachdem ich den Bürger darüber informiert hatte, dass die konkrete Kostenentscheidung nicht meiner Aufsichtszuständigkeit unterliegt, formulierte er sein Anliegen mir gegenüber um:

Er bat mich nun, auf die Stadt einzuwirken, dass diese den Vertrag allgemein veröffentlicht oder ihm ungeschwärzt zur Verfügung stellt.

Grundsätzlich wäre die Zurverfügungstellung einer bereinigten oder in Teilen geschwärzten Vertragskopie als Teilablehnung des Antrages zu werten. Diese Teilablehnung wäre auch einer Überprüfung durch mich grundsätzlich zugänglich. Im Rahmen dessen müsste die Stadt die vorgenommenen Schwärzungen mir gegenüber im Einzelfall auch begründen.

Im vorliegenden Fall war jedoch bisher noch keine Teilablehnung des Antrages erfolgt. Vielmehr hat die Stadt dem Bürger gegenüber ausgeführt, dass „[...]vor Gewährung der Akteneinsicht der gesamte Vertrag auf personenbezogene Daten und Geschäftsgeheimnisse eines Dritten geprüft werden und die entsprechenden Bereiche geschwärzt werden“ müsse. Im Rahmen der eingeholten Stellungnahme hat die Stadt ergänzend dargelegt, dass zunächst eine Prüfung stattfinde müsse, ob Schwärzungen erforderlich seien. Hierfür sei die Durchsicht des umfangreichen Vertragswerkes erforderlich. Enthalte der Vertrag keine schützenswerten Daten, dann würden selbstverständlich auch keine Schwärzungen vorgenommen. Die Stadt hat außerdem darauf hingewiesen, dass das Verfahren durch die Rücknahme des Antrages beendet worden sei, bevor die Stadt weitere vorbereitende Maßnahmen für die Auskunftserteilung (Konkretisierungsdialog, Anhörung der Betroffenen, Abwägungsentscheidungen, endgültige Entscheidung über einzelne Schwärzungen) und den eigentlichen Verwaltungsakt vornehmen konnte.

Der Stadt war zu diesem Zeitpunkt damit eine Stellungnahme und mir folglich eine Überprüfung (noch) gar nicht möglich. Andernfalls wäre auch die gesetzgeberische Entscheidung umgangen worden, dass für die Auskunft Kosten nach dem Kostengesetz erhoben werden können. Denn der Bürger, der vorliegend nicht bereit war, den Betrag zu bezahlen, könnte sich möglicherweise später darauf berufen, dass die Durchsicht des Vertrages bereits im Beschwerdeverfahren erfolgt sei.

Ich habe dem Bürger jedoch mitgeteilt, dass ich gern bereit bin, die Teilablehnung zu überprüfen, wenn er seinen Antrag wieder aufleben lässt und die Stadt in der Folge tatsächlich nur eine geschwärzte Kopie zur Verfügung stellt.

Soweit mich der Bürger darum bat, alternativ auf die Stadt einzuwirken, dass diese den Vertrag allgemein veröffentlicht und hierbei vermutlich Art. 52 Gemeindeordnung im Sinn hatte, musste ich diesem mitteilen, dass die Überwachung von kommunalrechtlichen Transparenzvorgaben nicht zu meinen gesetzlichen Aufgaben gemäß Art. 15 BayDSG gehört.

13.3 Auskunftsantrag und Datenschutz

Nicht typisch, aber auch nicht ganz außergewöhnlich ist die Konstellation, dass mittels eines Antrags nach Art. 39 BayDSG auch Auskunft über personenbezogene Daten Dritter begehrt wird. Der Gesetzgeber hat das Spannungsverhältnis zwischen dem allgemeinen Zugang zu Behördeninformationen einerseits und dem Schutz personenbezogener Daten andererseits abgewogen und insbesondere in Art. 39 Abs. 1 Satz 1 Nr. 1 BayDSG eine Regelung getroffen.

Der folgende Fall aus dem Jahr 2025, dessen Hintergrund ein vorangegangenes Überflutungsereignis war, greift eine derartige Konstellation auf. Bei den Aufräumarbeiten kam es auch zu Reinigungstätigkeiten an einer im Privateigentum stehenden Mauer. Der Eigentümer dieser Mauer begehrte Auskunft darüber, von wem diese Mauer gereinigt wurde und forderte die Gemeinde unter anderem auf, die Namen der hierbei beteiligten Personen zu nennen. Er begründete dies damit, die Namen für die Geltendmachung von Schadensersatz zu benötigen, da es durch die Reinigungsarbeiten möglicherweise zu Schäden an seiner Mauer gekommen sei. Die Gemeinde lehnte die Herausgabe personenbezogener Daten ab.

Im Rahmen des bei mir durchgeführten Beschwerdeverfahrens habe ich sowohl die Gemeinde als auch den Eigentümer auf folgende Punkte hingewiesen:

Nach Maßgabe von Art. 39 BayDSG hat jeder das Recht auf Auskunft über den Inhalt von Dateien und Akten öffentlicher Stellen, soweit ein berechtigtes, nicht auf eine entgeltliche Weiterverwendung gerichtetes Interesse glaubhaft dargelegt wird, bei personenbezogenen Daten eine Übermittlung an nicht öffentliche Stellen zulässig ist und Belange der öffentlichen Sicherheit und Ordnung nicht beeinträchtigt werden.

Soweit die Auskunft auf die Übermittlung von personenbezogenen Daten an nicht öffentliche Stellen gerichtet ist, muss diese Übermittlung für die öffentliche Stelle zulässig sein (Art. 39 Abs. 1 Satz 1 Nr. 1 BayDSG), mit anderen Worten: Sie benötigt für diese Datenverarbeitung eine Rechtsgrundlage. Diese kann sich aus Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG ergeben.

Nach dieser Vorschrift ist eine Übermittlung personenbezogener Daten zulässig, wenn der Empfänger eine nicht öffentliche Stelle ist, diese Stelle ein berechtigtes Interesse an ihrer Kenntnis glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat; dies gilt auch, soweit die Daten zu anderen Zwecken als denjenigen, zu denen sie erhoben wurden, übermittelt werden.

Ein berechtigtes Interesse ist in diesem Zusammenhang jedes nach vernünftigen Erwägungen unter Berücksichtigung der Besonderheiten des Falles anzuerkennendes, der Rechtsordnung nicht widersprechendes Interesse. Umfasst sind damit nicht nur die im Zusammenhang mit der Verfolgung von Rechten stehenden rechtlichen Interessen, sondern auch ideelle und wirtschaftliche Interessen.[191]

Vorliegend bestand auf Basis des gestellten Antrags schon kein berechtigtes Interesse an der Herausgabe der personenbezogenen Daten der einzelnen Beschäftigten, welche die Reinigung durchgeführt hatten. Die Reinigung wurde durch eine Stelle durchgeführt, die der Gemeinde zurechenbar war. Schadensersatzansprüche richten sich in diesen Fällen grundsätzlich nach § 839 Bürgerliches Gesetzbuch in Verbindung mit Art. 34 Grundgesetz gegen den Staat oder die Körperschaft, in deren Dienst die handelnde Person steht, vorliegend also gegen die Gemeinde.

[191] Vgl. Niese, in: Wilde/Ehmann/Niese/Knoblauch, Datenschutz in Bayern, 38. Erg.-Lief. 2025, Art. 5 BayDSG Rn. 18.

Im vorliegenden Fall wurden dem Eigentümer die beantragten Auskünfte überwiegend erteilt. Die Verweigerung der Auskunft über die personenbezogenen Daten derjenigen Beschäftigten, welche die Reinigung der Mauer vorgenommen hatten, war nicht zu beanstanden.

14 Technik und Organisation

14.1 Webarchive datenschutzgerecht füttern

Webarchive haben es sich zur Aufgabe gemacht, Inhalte des Internets zu bewahren. Eines der bekanntesten Webarchive ist die sogenannte Wayback Machine. Sie ist Teil des „Internet Archive“, eines gemeinnützigen Projekts aus den USA, das sich der langfristigen Erhaltung digitaler Daten widmet.

Die Wayback Machine erstellt in unregelmäßigen Abständen vollständige Kopien von Internetauftritten, indem alle zugehörigen Webseiten in das Webarchiv übernommen werden. Diese „Zeitschnitte“ hält sie dann öffentlich und kostenlos zum Abruf bereit. Nutzende können etwa die Adresse (URL) einer Webseite eingeben und erhalten Informationen darüber, zu welchem Zeitpunkt diese „eingefroren“ wurde. Durch einen Klick auf das Datum kann die Webseite in ihrer jeweiligen historischen Gestalt aufgerufen werden. Dabei sind zwar nicht alle Funktionalitäten, insbesondere Links auf Unterseiten, „eingefangen“; jedoch können zahlreiche an sich längst überholte Inhalte eingesehen werden – auch zum Beispiel personenbezogene Daten von ehemaligen Beschäftigten bayerischer öffentlicher Stellen. Eine Suchfunktion über alle archivierten Webseiten, wie sie Suchmaschinen zur Verfügung stellen, hat zumindest die Wayback Machine nicht zu bieten. Allerdings wurde das Projekt bereits 1996 gegründet und hat seitdem eine beeindruckende Anzahl an Webseiten archiviert.

Der vorliegende Beitrag skizziert, was das Datenschutzrecht an Webarchiven interessant findet (Nr. 14.1.1), wirft einen Blick auf die aktuelle Entwicklung (Nr. 14.1.2) und gibt Handlungsimpulse (Nr. 14.1.3).

14.1.1 Warum interessiert sich der Datenschutz für Webarchive?

Webarchive können ein Problem für den Schutz personenbezogener Daten darstellen. Im Ausgangspunkt sind bayerische öffentliche Stellen für das Wirken unabhängiger Webarchive zwar grundsätzlich nicht datenschutzrechtlich verantwortlich.[192] Gleichwohl gibt es insbesondere zwei Szenarien, in denen die geschilderte Archivierung von Webseiten datenschutzrechtliche Folgefragen für bayerische öffentliche Stellen mit sich bringen kann:

[192] Zu beachten ist allerdings, dass der Europäische Gerichtshof den Begriff des Verantwortlichen weit auslegt und in der Folge die Schwelle für eine gemeinsame Verantwortlichkeit recht niedrig ansetzt (vgl. nur Europäischer Gerichtshof, Urteil vom 5. Juni 2018, C-210/16, Rn. 26 ff.). Vor diesem Hintergrund kommt bei einer Archivierung von Webseiten insbesondere im Falle eines „Zusammenwirkens“ einer öffentlichen Stelle mit einem Webarchiv gegebenenfalls eine (gemeinsame) Verantwortlichkeit auch der öffentlichen Stelle in Betracht. Maßgebend sind insoweit die konkreten Umstände des Einzelfalls. Näher hierzu Bayerischer Landesbeauftragter für den Datenschutz, Gemeinsame Verantwortlichkeit, Orientierungshilfe, Stand 6/2024, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek“.

– **Szenario 1:** Unrechtmäßig veröffentlichte personenbezogene Daten

So kann es vorkommen, dass versehentlich personenbezogene Daten auf einer Webseite veröffentlicht werden, die nicht zur öffentlichen Einsichtnahme bestimmt sind. Ein Beispiel hierfür sind Sitzungsniederschriften aus einer nichtöffentlichen Gemeinderatssitzung, die unbeabsichtigt im Internetauftritt der Gemeinde zugänglich gemacht sind.

In der Folge crawlen Suchmaschinen die Webseiten des Internetauftritts, um Links und Vorschauen zu erstellen. Ich habe dieses Problem bereits vor einigen Jahren in einem Tätigkeitsbericht aufgegriffen.[193] Außerdem erstellen Webarchive vollständige Kopien – einschließlich der versehentlich veröffentlichten personenbezogenen Daten.

Während die Daten von der ursprünglichen Webseite relativ unkompliziert und zeitnah gelöscht werden können und sich die Suchergebnisse entsprechend – wenn auch mit Verzögerung – aktualisieren, verschwinden die Daten aus Webarchiven nicht ohne weiteres Zutun. Ohne Rechtsgrundlage veröffentlichte personenbezogene Daten können so dauerhaft in Webarchiven sichtbar und abrufbar bleiben. Dies erschwert es einer öffentlichen Stelle, die Folgen eines Datenschutzverstoßes – hier einer versehentlichen Veröffentlichung personenbezogener Daten – zu beseitigen beziehungsweise einzudämmen.

– **Szenario 2:** Veraltete personenbezogene Daten

In einem weiteren Szenario werden personenbezogene Daten zunächst mit Rechtsgrundlage auf einer Webseite veröffentlicht – beispielsweise eine Liste mit wichtigen Ansprechpersonen für Bürgerinnen und Bürger bei einer Gemeinde. Das Angebot wird in der Folge aber sukzessive bei personellen Wechseln nachgeführt.

Auch hier werden Suchmaschinen und Webarchive aktiv. Während sich die Suchergebnisse von Suchmaschinen meist ausreichend schnell automatisch aktualisieren, entfernen sich die „eingefrorenen" Kopien in den Webarchiven mit der Zeit immer weiter von der aktuellen Lage. Jedenfalls die Gemeinde dürfte beispielsweise veraltete Ansprechpersonen-Listen nicht mehr öffentlich bereithalten, weil dies zu ihrer Aufgabenerfüllung nicht (mehr) erforderlich ist.

14.1.2 Wie schaut die aktuelle Entwicklung aus?

Aus Datenschutzsicht ist es daher vordergründig erfreulich, dass Google im Februar 2024 mitgeteilt hat, den Google-Cache einzustellen. Die Google-Cache-Funktion diente dazu, Momentaufnahmen von Webseiten zu speichern, wie sie zum Zeitpunkt der letzten Google-Indexierung aussahen. Im Gegensatz zu Webarchiven, die verschiedene Versionen einer Seite speichern, hielt der Google-Cache lediglich eine, oft relativ aktuelle Kopie bereit. Selbst dies ermöglichte aber mitunter den Zugriff auf veraltete Daten.

Mittlerweile verweist Google allerdings stattdessen auf die Wayback Machine. Im September 2024 gab das „Internet Archive" zudem bekannt, dass der Blick in die

[193] Bayerischer Landesbeauftragter für den Datenschutz, 32. Tätigkeitsbericht 2022, Nr. 12.4.1.

Vergangenheit des Internets mit der Wayback Machine nun leichter zugänglich sei als bisher.[194] Über die Google-Suchergebnisse könne nicht nur der Link auf die aktuelle Webseite gefunden werden, sondern – mit nur wenigen Klicks – auch ein Weg zu alten Versionen genau dieser Webseite.

Während bisher die genaue URL einer Webseite bekannt sein musste, um auf alte Versionen zugreifen zu können, ist es nun möglich, über die Eingabe von Suchbegriffen in Google – ausgehend von der aktuellen Version der Webseite – zu diesen alten Versionen zu gelangen. Google verschlagwortet dabei die Wayback Machine selbst aber nicht. Das bedeutet, dass eine aktive Suche nach veralteten Daten nicht möglich ist. Dennoch wird der Zugang zu veralteten personenbezogenen Daten über die Wayback Machine deutlich erleichtert.

14.1.3 Gibt es nun etwas zu tun?

Die Veröffentlichung personenbezogener Daten auf Webseiten stellt eine Verarbeitung dieser Daten nach Art. 4 Nr. 2 DSGVO dar. Bei jeder Verarbeitung personenbezogener Daten haben Verantwortliche die Datenschutzgrundsätze nach Art. 5 Abs. 1 DSGVO zu beachten; Verantwortliche müssen dies auch nachweisen können (Rechenschaftspflicht, Art. 5 Abs. 2 DSGVO).

Will eine öffentliche Stelle personenbezogene Inhalte in ihrem Internetauftritt einstellen, muss sie sich somit – wie stets – zunächst vergewissern, dass diese Verarbeitung von einer hinreichenden Rechtsgrundlage gedeckt ist (Grundsatz der Rechtmäßigkeit, Art. 5 Abs. 1 Buchst. a, Art. 6 Abs. 1 DSGVO). Besondere Bedeutung erlangen dabei die „Erforderlichkeit" der Veröffentlichung sowie der Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO): Eine Veröffentlichung personenbezogener Daten auf einer Webseite ist ohnehin nur in dem Umfang zulässig, wie dies zur Erreichung des jeweiligen Verarbeitungszwecks notwendig und angemessen ist. Als – aus Datenschutzsicht positiver – „Nebeneffekt" kommt im vorliegenden Zusammenhang für die öffentliche Stelle hinzu: Je weniger personenbezogene Daten auf einer Webseite veröffentlicht werden, desto weniger Sorge bereiten auch unerkannte oder gegebenenfalls unerlaubte Kopien.

Verantwortliche haben ferner durch geeignete technische und organisatorische Maßnahmen nachweisbar sicherzustellen, dass eine Verarbeitung personenbezogener Daten im Einklang mit der Datenschutz-Grundverordnung erfolgt (Art. 24 Abs. 1 Satz 1 DSGVO). Insbesondere ist durch technische und organisatorische Maßnahmen zu gewährleisten, dass die Datenschutzgrundsätze – wie etwa der Grundsatz der Datenminimierung – wirksam umgesetzt werden (Art. 25 Abs. 1 DSGVO). Zu bedenken ist auch: Hat ein Verantwortlicher personenbezogene Daten öffentlich gemacht und ist er nach Art. 17 Abs. 1 DSGVO zu deren Löschung verpflichtet, muss er angemessene Maßnahmen treffen, um andere Verantwortliche, welche die betreffenden Daten verarbeiten, über das Löschungsverlangen der betroffenen Person zu informieren (Art. 17 Abs. 2 DSGVO).[195]

[194] Siehe dazu https://blog.archive.org/2024/09/11/new-feature-alert-access-archived-web-pages-directly-through-google-search.

[195] Ausführlich zu diesem „Recht auf Vergessenwerden" Bayerischer Landesbeauftragter für den Datenschutz, Das Recht auf Löschung nach der Datenschutz-Grundverordnung, Orientierungshilfe, Stand 6/2022, Rn. 60 ff., Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

Öffentliche Stellen sollten daher stets kritisch prüfen, ob und in welchem Umfang sie personenbezogene Daten im eigenen Internetauftritt veröffentlichen dürfen. Eine solche Überprüfung ist eine Daueraufgabe: Veröffentlichte Daten können nämlich veralten, und eine einstmals zulässige Veröffentlichung dieser Daten kann mangels Erforderlichkeit durch Zeitablauf unzulässig werden. Eine dergestalt datensparsame Gestaltung des Internetauftritts lohnt sich auch deshalb, weil sie hilft, Ärger zu vermeiden, der sich aus dem Wirken von Webarchiven ergeben kann.

Gegebenenfalls kommen öffentliche Stellen auch zu dem Schluss, dass sie eine Archivierung durch ein Webarchiv generell unterbinden und bereits bestehende Kopien löschen lassen wollen. Soll eine Archivierung nicht gänzlich verhindert werden, ist es ratsam, den Internetauftritt auf möglicherweise problematische Unterseiten mit personenbezogenen Daten zu überprüfen. Werden solche gefunden, sollte versucht werden, den Zugriff durch das Webarchiv für diese Unterseiten zu blockieren, um eine Archivierung zu vermeiden.

Um die Löschung älterer Versionen zu veranlassen und die Erstellung zusätzlicher Kopien zu vermeiden, empfiehlt etwa die Wayback Machine in ihren häufig gestellten Fragen,[196] eine E-Mail an info@archive.org zu senden. Darin sollten folgende Informationen enthalten sein:

— die URL der betreffenden Webseite,

— der Zeitraum, der von der Archivierung ausgeschlossen werden soll,

— der Zeitraum, in dem die öffentliche Stelle die Kontrolle über die Webseite hatte,

— – zusätzliche Informationen, welche die Anfrage besser verstehen helfen.

Im Internet sind zudem Erfahrungsberichte zu alternativen Methoden zu finden, wie eine Archivierung durch Webarchive möglicherweise verhindert werden kann:

— So soll ein Eintrag der Zeilen „User-agent: archive.org_bot“ und „Disallow: /“ in die Datei „robots.txt“ eine Nichtarchivierung bewirken können.

— Wird ein Apache-Webserver verwendet, soll über die Datei „.htaccess“ ein Zugriff für Webarchive blockiert werden können. Dazu müssen entweder die IP-Adressen der Webarchive oder der „User-Agent-String“ bekannt sein. Diese Methode könne auch dazu beitragen, Webarchive daran zu hindern, bestimmte Unterseiten zu archivieren.

Diese Methoden habe ich nicht getestet; sie sind hier lediglich informatorisch aufgeführt und mögen auch in Betracht kommen, wenn der von der Wayback Machine empfohlene Ansatz nicht erfolgreich sein sollte.

Erfahrungsberichte sprechen dafür, dass sich Webarchive nicht immer zuverlässig blockieren lassen. Auch vor diesem Hintergrund kommt einer bewusst datensparsamen Gestaltung von Webangeboten besondere Bedeutung zu.

[196] Siehe dazu https://help.archive.org/help/how-do-i-request-to-remove-something-from-archive-org.

14.2 Datenschutz beim Versand von Brief und Paket

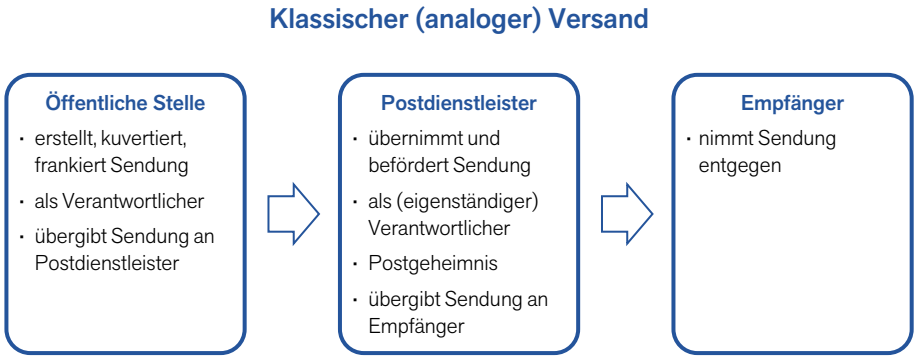
Die Digitalisierung schreitet fort. Gleichwohl versenden bayerische öffentliche Stellen Tag für Tag zahllose Briefe und Pakete. Viele Sendungen enthalten personenbezogene Daten nicht nur auf dem Adressfeld. Dokumente, ganze Akten oder elektronische Speichermedien, die mit der Post transportiert werden, haben mitunter einen ganz erheblichen Schutzbedarf – wie etwa ein Datenträger mit medizinischen Befunden.

Beim Bayerischen Landesbeauftragten für den Datenschutz eingehende Meldungen von Datenpannen, Beschwerden, aber auch Beratungsanfragen bayerischer öffentlicher Stellen zeigen, dass beim Postversand personenbezogener Daten einiges schiefgehen kann. Die möglichen Risiken dabei sind eigentlich überschaubar und gut bewältigbar: Es braucht nur etwas Wissen und sachgerechte Routinen. Der vorliegende Beitrag ruft in Erinnerung, was aus Datenschutzsicht beim Postversand geschieht (Nr. 14.2.1), zeigt häufige Datenschutzvorfälle auf (Nr. 14.2.2) und bietet einen Fragenkatalog zur Fehlervermeidung (Nr. 14.2.3).

14.2.1 Verarbeitung personenbezogener Daten beim klassischen (analogen) Versand von Briefen und Paketen

Briefe und Pakete können neben der Absender- und Empfängeradresse auch inhaltlich – also eingepackt – personenbezogene Daten enthalten. Im Einzelfall können diese sehr sensibel sein. Beim herkömmlichen Postversand erstellt die bayerische öffentliche Stelle den Inhalt, verpackt ihn in einen Brief oder ein Paket und versieht diese „Hülle“ mit einer Adressierung. Dabei verarbeitet sie personenbezogene Daten aufgrund einer Rechtsgrundlage des bereichsspezifischen oder des allgemeinen Datenschutzrechts. Geht die Sendung an eine natürliche Person, ist der konventionelle Transport durch einen Postdienstleister (vgl. § 4 Abs. 1 Postgesetz – PostG) datenschutzrechtlich mit einer Verarbeitung von Adressdaten verknüpft. Dabei gilt der Postdienstleister als eigenständiger Verantwortlicher. Der Postdienstleister verarbeitet die Adressdaten nicht im Auftrag und nach Weisung des Absenders; daher ist er nicht Auftragsverarbeiter, sondern ein eigenständiger Verantwortlicher.

Der Postdienstleister nimmt zum Zweck der Zustellung von den jeweiligen Adressdaten Kenntnis. Die Verarbeitung personenbezogener Daten muss er auf eine Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 DSGVO stützen können. § 68 Abs. 3 Satz 1 PostG enthält eine Rechtsgrundlage, die sich auf die Verarbeitung der Adressdaten zum Zwecke der ordnungsgemäßen Zustellung von Postsendungen bezieht. Der Inhalt der Postsendung geht den Postdienstleister grundsätzlich nichts an; er ist durch das Postgeheimnis nach § 64 PostG sowie die Strafbewehrung des § 206 Strafgesetzbuch geschützt.



Der Versand von Hybridbriefen unterscheidet sich vom klassischen Briefversand durch seine Mehrstufigkeit. Zu diesem Thema liegt bereits eine Aktuelle Kurz-Information vor.[197]

14.2.2 Häufig auftretende Datenschutzvorfälle

Neben Versehen bei der Zuordnung Inhalt – Adressat (etwa Angabe des falschen Adressaten auf dem Umschlag, unbeabsichtigtes Einkuvertieren mehrerer, an unterschiedliche Personen gerichteter Dokumente) stelle ich im Zusammenhang mit dem Postversand immer wieder Datenschutzvorfälle fest, die ihren Grund in der Gestaltung von Geschäftsprozessen oder dafür eingesetzten Ressourcen finden.

Dies betrifft beispielsweise den Entwurf von Vordrucken, wenn der Inhalt eines Schreibens zum Teil – etwa mit einer aussagekräftigen Rechtsnorm oder dem Hinweis auf eine Organisationseinheit der öffentlichen Stelle – bereits im Adressfenster oder auf dem Briefumschlag sichtbar wird und damit auch ohne weitere Kenntnisse Rückschlüsse auf die Umstände der behördlichen Befassung mit dem Adressaten möglich werden. Auch die Wahl des Materials, die Ausführung und Ausgestaltung von Briefumschlägen – insbesondere die Lage der Sichtfenster in Relation zu Briefbogen oder Vordruck sowie eine auffällige Kenntlichmachung, beispielsweise mit eindeutigen Logos –, ferner die Verwendung modifizierter Vordrucke kann die Ursache dafür sein, dass Zusteller, Familienangehörige, Nachbarn oder sonst an eine Postsendung gelangende Personen mehr als für den Versand an den Adressaten nötig erfahren.[198]

Bei einer förmlichen Zustellung durch die Post mit Zustellungsurkunde ist für den notwendigen verschlossenen inneren Umschlag gemäß Art. 3 Abs. 2 Satz 3 Bayerisches Verwaltungszustellungs- und Vollstreckungsgesetz (VwZVG) der Vordruck nach der Zustellungsvordruckverordnung (ZustVV) zu verwenden. Aus Anlage 2 zu § 1 Nr. 2 ZustVV sind die zulässigen (und damit allein datenschutzkonformen) Angaben ersichtlich. Alle eigenmächtigen zusätzlichen Angaben auf dem inneren Umschlag können unerlaubt Rückschlüsse auf den Inhalt zulassen und sind deshalb datenschutzrechtlich unzulässig.[199]

[197] Bayerischer Landesbeauftragter für den Datenschutz, Versand von Hybridbriefen durch bayerische öffentliche Stellen, Aktuelle Kurz-Information 44, Stand 11/2022, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

[198] Beispiel aus der Praxis: Einladung zum Mammografie-Screening, Bayerischer Landesbeauftragter für den Datenschutz, 29. Tätigkeitsbericht 2019, Nr. 7.3.

[199] Näher Bayerischer Landesbeauftragter für den Datenschutz, 33. Tätigkeitsbericht 2023,

Auch das automatische Verschließen und Frankieren ausgehender Post verläuft nicht immer problemlos. Offen versandte Briefumschläge oder nicht zum Inhalt passende Umschläge kommen auch hier vor. Viele Meldungen nach Art. 33 DSGVO zeigen, dass Kuvertiermaschinen nicht immer fehlerfrei arbeiten.

Seit infolge der Marktliberalisierung zahlreiche Unternehmen Postdienstleistungen erbringen, erreichen mich auch immer wieder Hinweise zu Defiziten bei der Zuverlässigkeit einzelner Anbieter: dabei geht es zum Beispiel um Einwürfe in falsche Briefkästen oder die Nichtzustellung eingelieferter Sendungen. Auch ganze Pakete mit Akten gehen teilweise auf dem Transportweg verloren.

Hinweis:
Die Datenschutzaufsicht bei gewerblichen Anbietern von Postdienstleistungen liegt nach § 71 Abs. 1 PostG bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.[200]

14.2.3 Prüfschritte zur Gewährleistung eines angemessenen Schutzniveaus vor Postversand

Jede bayerische öffentliche Stelle ist nach Art. 24 Abs.1, Art. 25 Abs.1 und Art. 32 Abs. 1 DSGVO gehalten, mittels einer wirksamen Umsetzung von Schutzmaßnahmen ein dem Verarbeitungsrisiko beim Versand angemessenes Schutzniveau zu gewährleisten. Vor dem Versand von Schriftstücken oder Speichermedien mit personenbezogenen Daten ist zu prüfen, welche Schutzmaßnahmen erforderlich sind, um Risiken adäquat entgegentreten zu können. Folgende einfache Fragen können dabei helfen:

— **Frage 1:** Wie sensibel sind die Daten, die versandt werden sollen?

  Die erforderlichen technisch-organisatorischen Maßnahmen richten sich nach der Sensibilität und dem Umfang der zu versendenden Daten. Hier kommt es zum einen auf den Umfang des Datenpakets an, zum anderen auf die Frage, ob beispielsweise von Art. 9 Abs. 1 DSGVO erfasste Daten (etwa Gesundheitsdaten) oder sonst besonders schutzbedürftige Daten (etwa Steuerdaten oder Personalaktendaten) verschickt werden sollen.

— **Frage 2:** Welcher Versanddienstleister ist geeignet?

  Bei der Auswahl eines Postdienstleisters sollte dessen Zuverlässigkeit im Blick behalten werden. Neben eigenen Erfahrungen können hier insbesondere anbieter- und ortsbezogen veröffentlichte Prüfungserkenntnisse der Bundesnetzagentur[201] hilfreich sein. Alternativ können auch Kurierdienste oder eigenes Personal genutzt werden. Auch hier müssen allerdings die Eignung geprüft und die Zuverlässigkeit sichergestellt werden.

Nr. 11.6.

200 Vertiefend dazu https://www.bfdi.bund.de/DE/Buerger/Privatwirtschaft/Post/Post_node.html.

201 Abrufbar unter https://www.bundesnetzagentur.de/DE/Vportal/Post/AufgabenMassnahmen/start.html.

— **Frage 3:** Wird eine Nachverfolgbarkeit der Auslieferung benötigt?

Wurde bei Frage 1 festgestellt, dass auf Grund der Sensibilität der Daten besondere Schutzmaßnahmen erforderlich sind, ist insbesondere zu prüfen, ob hier die einfache Versandart als gewöhnlicher Brief ausreicht, oder ob eine Nachverfolgbarkeit der Auslieferung durch Einschreiben (zu unterscheiden sind hier das günstigere Postprodukt „Einschreiben Einwurf“ und das Postprodukt „Einschreiben“ – früher als Übergabe-Einschreiben bezeichnet – , das noch um die Zusatzleistung „Rückschein“ ergänzt werden kann), förmlich mit Zustellungsurkunde oder aber Paketversand vorzuziehen ist.

Einfache Briefe werden in der Regel ohne Sendungsverfolgung transportiert. Daher kann nicht festgestellt werden, ob die Sendung dem Empfänger auch tatsächlich zugestellt wurde und wo es gegebenenfalls verloren gegangen ist. Die Deutsche Post AG bietet mittlerweile Briefmarken mit QR-Code an, die eine Basis-Sendungsverfolgung vom Einlieferungspostzentrum zum Auslieferungspostzentrum ermöglichen, nicht jedoch bis zum eigentlichen Empfänger. Bei der Nachforschung nach einer verloren gegangenen Sendung wäre dann zwar feststellbar, dass diese tatsächlich bei der öffentlichen Stelle ausgelaufen ist und von der Post zum Auslieferungspostzentrum weitertransportiert wurde; daraus könnte jedoch nur geschlossen werden, dass ein Verlust auf dem Weg von diesem Postzentrum zum eigentlichen Empfänger eingetreten sein muss. Ob die Sendung tatsächlich beim Zusteller verloren gegangen ist oder etwa der Empfänger die Sendung versehentlich entsorgt hat, bliebe aber offen. Eine lückenlose Sendungsverfolgung „Ende-zu-Ende“ bietet die Basis-Sendungsverfolgung also nicht.[202]

Bei dem Postprodukt „Einschreiben Einwurf“ ist dagegen das Einlegen in den Briefkasten des Empfängers nachweisbar, bei einem (Übergabe-)Einschreiben die Übergabe an den Empfänger oder einen sonst Empfangsberechtigten; mit der Zusatzleistung „Rückschein“ erhält der Absender zudem eine schriftliche Bestätigung der Zustellung mit Zustelldatum, Auslieferungsbeleg und einem Sendungsbild.[203]

Die Standard-Sendungsverfolgung von Paketen dokumentiert typischerweise die Zustellung an eine Person, an einem vom Empfänger ausgewählten Ablageort oder an eine Packstation. Die Qualität des Nachweises kann je nach Anbieter mit Zusatzleistungen – wie etwa einer Zustellung gegen Unterschrift oder mit Identitätsprüfung – gesteigert werden.[204]

Hinweis:
Für Päckchen bietet die Deutsche Post AG im nationalen Verkehr keine Sendungsverfolgung an; sie kann auch nicht zugebucht werden. Da Päckchen nicht mehr mit Briefmarken freigemacht werden dürfen, steht die Basis-Sendungsverfolgung (Fn. 202) ebenfalls nicht zur Verfügung.

[202] Zur Basis-Sendungsverfolgung der Deutschen Post AG https://www.deutschepost.de/de/b/briefmarke-mit-matrixcode.html.

[203] Zu Einschreiben und zur Zusatzleistung „Rückschein“ am Beispiel der Deutschen Post AG https://www.deutschepost.de/de/e/einschreiben/haeufige-fragen.html.

[204] Siehe für Geschäftskunden etwa Nr. 4 Allgemeine Geschäftsbedingungen DHL Paket/Express (National), Stand 4/2022, Internet: https://www.dhl.de/de/geschaeftskunden/paket/rund-um-den-versand/agb.html.

Die Behörden und Gerichten vorbehaltene förmliche Zustellung mit Zustellungsurkunde bietet einen Nachweis, der vollen Beweis der darin bezeugten Tatsachen begründet (vgl. Art. 3 Abs. 2 Satz 1 VwZVG, § 182 Abs. 1 Satz 2, § 418 Abs. 1 Zivilprozessordnung).

— **Frage 4:** Welche Verpackung ist geeignet? Ist die Sendung verschlossen?

Je nach Umfang und Größe der zu versendenden Schriftstücke (einzelne oder mehrere Blätter, umfangreiche Anlagen, Gehefte, einzelne oder mehrere Aktenordner) ist auf eine ordentliche und stabile Verpackung Wert zu legen.

Bei der Verpackung ist darauf zu achten, dass der Inhalt gegen unbefugten Zugriff gesichert ist (Zukleben des Umschlages, Verwendung eines speziellen Sicherheitsklebebandes zum Verschluss eines Kartons oder Verplombung von Transportkisten) und ein Aufreißen oder Aufplatzen durch Verwendung entsprechend geeigneter Verpackungen sowie fachgerechtes Einpacken verhindert oder wenigstens erschwert wird. Im Zweifelsfall sollte immer eine höherwertige Verpackung gewählt werden.

Gerade bei einer automatischen Kuvertierung sollte auch geprüft werden, ob die Sendungen tatsächlich ordnungsgemäß verschlossen sind. Zudem sollte eine regelmäßige Wartung der entsprechenden Geräte erfolgen.

— **Frage 5:** Ist die Sendung korrekt adressiert und datensparsam beschriftet?

Bei der Beschriftung der gewählten Versandform ist im Sinne der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) auf die für die Postzustellung tatsächlich erforderlichen Daten des Adressaten abzustellen. Darüber hinausgehende Informationen können eine unbefugte Offenlegung von personenbezogenen Daten zur Folge haben (siehe oben Nr. 14.2.2). Insbesondere im Gesundheitsbereich sollte durch eine neutrale Gestaltung von Postsendungen dafür Sorge getragen werden, dass keine Informationen über den Gesundheitszustand oder mögliche Erkrankungen des Empfängers abgeleitet werden können.

— **Frage 6:** Ist bei Verwendung eines elektronischen Speichermediums eine Verschlüsselung erfolgt?

Gerade im Bereich der Krankenhäuser werden häufiger Patientendaten auf elektronischen Speichermedien verschickt (CD, DVD, USB-Stick usw.), wenn zum Beispiel ein Patient Einsicht in seine Patientenakte haben möchte. Dabei ist zum einen auf eine geeignete Verpackung (Umschläge aus reißfestem Material, Luftpolsterumschläge oder fest verschlossene Kartonagen) zu achten. Zum anderen ist beim postalischen Versand eines elektronischen Mediums eine sachgerechte Verschlüsselung der Dateien, die auf dem Medium gespeichert sind, oder die Verschlüsselung des Mediums selbst eine Schutzmaßnahme, die das Risiko einer Vertraulichkeitsverletzung auf dem Versandweg deutlich vermindert. Sind die Kosten für eine Verschlüsselung nach dem Stand der Technik – was regelmäßig der Fall sein dürfte – verhältnismäßig, wird eine solche Verschlüsselung empfohlen. Hierbei ist auch zu berücksichtigen, dass dem Empfänger Passwörter zum Entschlüsseln der Daten nicht in derselben Sendung zur Verfügung gestellt werden wie die Inhalte, die mit ihnen entschlüsselt werden sollen.

— **Frage 7:** Ist die Sendung bis zur Abholung durch den Dienstleister sicher gelagert?

  Insbesondere bei einer größeren Menge personenbezogener Daten (etwa einer Vielzahl sozialrechtlicher Leistungsbescheide) muss auch die sichere Lagerung bis zur Abholung durch den Dienstleister gewährleistet sein. Ein für den Parteiverkehr oder Besucher zugänglicher Bereich ist dafür ungeeignet.

— **Frage 8:** Sind die für den Versand zuständigen Beschäftigten hinsichtlich der möglichen Datenschutzrisiken und Versandarten ausreichend geschult?

  Alle Empfehlungen helfen wenig, wenn keiner an sie denkt. Daher sollte auch darauf geachtet werden, dass die erforderlichen Prozesse und Abläufe entsprechend dokumentiert sind (Prozessbeschreibungen, Dienstanweisungen, Dienstvereinbarungen), dieses Wissen des aktuell mit dem Postversand beauftragten Personals regelmäßig aufgefrischt wird und neues Personal eine Einweisung erhält, was beim Postversand zu beachten ist. Dies betrifft insbesondere auch vorübergehend beschäftigte Personen wie Aushilfskräfte oder Praktikanten.

14.3 Datenschutzkonzepte für Digitalisierungsvorhaben

Im Berichtsjahr habe ich zahlreiche bayerische öffentliche Stellen bei verschiedenen innovativen IT-Projekten und anderen Digitalisierungsvorhaben beraten. Viele dieser Stellen erstellen Datenschutzkonzepte, in welchen die zu Datenschutzfragen erarbeiteten Lösungen laufend nach dem aktuellen Stand des jeweiligen Vorhabens erfasst und dokumentiert werden. Ein solches Konzept hilft der verantwortlichen Stelle bei der Erfüllung ihrer datenschutzrechtlichen Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO).

Bedauerlicherweise erlange ich jedoch auch immer wieder von Vorhaben Kenntnis, bei denen die Beachtung von Standards aus Datenschutz und IT-Sicherheit erkennbar nicht die erforderliche Rolle gespielt hat. Projektverantwortliche erwarten dann von mir nicht selten eine Art „Freigabe“, die von allen einschlägigen Sorgen enthebt. Eine solches Instrument sieht das geltende Recht bewusst nicht vor, und so ist dann die Enttäuschung groß, wenn meine Beratung die Schwächen des Projekts im Bereich des Datenschutzes offenlegt. Solche Enttäuschungen lassen sich leicht vermeiden: Die Erstellung eines Datenschutzkonzepts bereits bei der Konzeption von Projekten unterstützt Verantwortliche für Digitalisierungsvorhaben dabei, die datenschutzrechtlichen Anforderungen systematisch zu erheben und mit allen Akteuren geeignet zu konsolidieren. Ein Datenschutzkonzept begleitet ein Digitalisierungsvorhaben von dessen Beginn bis zum Abschluss. Je nach Komplexität wird das Konzept schrittweise und parallel zum Vorhabensverlauf bedarfsgerecht konkretisiert.

Um bayerischen öffentlichen Stellen konkrete Hilfestellungen für die Verwendung eines derartigen Datenschutzkonzepts zu geben, habe ich eine Aktuelle Kurz-Information[205] veröffentlicht, die ein praxiserprobtes Vorgehen beschreibt. Das Pa-

[205] Bayerischer Landesbeauftragter für den Datenschutz, Datenschutzkonzepte für Digitalisierungsvorhaben, Aktuelle Kurz-Information 64, Stand 9/2025, Internet:

pier gibt Hinweise zur schrittweisen Erstellung der datenschutzrechtlich erforderlichen Nachweise unter Berücksichtigung von Synergiepotenzialen mit der IT-Sicherheit und umfasst auch eine Checkliste für die Strukturierung grundlegender datenschutzrechtlicher Aspekte.

14.4 Synergien Datenschutz und Informationssicherheit

Die Digitalisierung ist ein wesentlicher Faktor für die Optimierung von Geschäftsprozessen und für die Bewältigung großer aktueller Herausforderungen wie zum Beispiel dem Fachkräftemangel. Bei der Konzeption, Planung und dem Betrieb von Verarbeitungen personenbezogener Daten, die in den Prozessen und Fachverfahren bayerischer öffentlichen Stellen integriert sind, und von unterstützenden IT-Systemen treffen regelmäßig Anforderungen des technisch-organisatorischen Datenschutzes und der Informationssicherheit aufeinander. Werden diese – wie in der Praxis häufig zu beobachten – getrennt voneinander und in eigenen „Compliance-Welten" bearbeitet, besteht die Gefahr, dass wichtige Berührungspunkte gar nicht oder erst kurz vor der Inbetriebnahme geklärt werden. Dabei können unterschiedliche Bewertungen und Anforderungen beider Disziplinen eine besonders aufwändige Synchronisation verursachen, was oft zu Unverständnis und einer Forderung nach verbesserter Zusammenarbeit der beiden Disziplinen führt.

Im Berichtsjahr habe ich daher gemeinsam mit drei weiteren fachkundigen bayerischen öffentlichen Stellen die möglichen Synergiepotenziale beim Brückenschlag zwischen den beiden Disziplinen untersucht. Dabei ging es darum, die Anforderungen des technisch-organisatorischen Datenschutz und der Informationssicherheit gemeinsam zu betrachten und bei deren Erhebung sowie Umsetzung von Anfang an systematisch vorhandene Synergien zu nutzen. Die daraus gewonnenen Erkenntnisse wurden in der Praxis schon erprobt und erste Ergebnisse auf den Bayerischen Datenschutz-Tagen 2025 der Bayerischen Akademie für Verwaltungsmanagement sowie auf dem zweiten IT-Grundschutz-Tag 2025 des Bundesamts für Sicherheit in der Informationstechnik (BSI) vorgestellt.

Ein unverzichtbarer Schritt bei dieser Untersuchung war ein methodischer Vergleich, bei dem die Unterschiede und Gemeinsamkeiten zwischen den beiden Disziplinen herausgearbeitet wurden. Für diesen Vergleich standen mit dem IT-Grundschutz des BSI für die Informationssicherheit und mit meinen Arbeitshilfen für den technisch-organisatorischen Datenschutz, die auf Basis schon bestehender Standards (zum Beispiel Standard-Datenschutzmodell[206] der DSK[207]) entwickelt wurden und auf meiner Homepage[208] veröffentlicht sind, zwei geeignete Methoden zur Verfügung.

Der Methodenvergleich hat mehrere Bereiche identifiziert, in denen sich die beiden Disziplinen überschneiden und bedeutende Gemeinsamkeiten aufweisen.

https://www.datenschutz-bayern.de, Rubrik „Infothek".

206 SDM; Internet: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell.

207 Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK); Internet: https://www.datenschutzkonferenz-online.de.

208 Siehe Informationsangebot im Internet: https://www.datenschutz-bayern.de, Rubrik „DSFA".

Durch ein gut aufeinander abgestimmtes Vorgehen beider Disziplinen können daher gewichtige Synergiepotenziale realisiert werden. Insbesondere können unnötige Komplexität sowie Bürokratie systematisch abgebaut werden.

Eine effiziente Zusammenarbeit kann mit der Modellierung der relevanten Sachverhalte beginnen, etwa durch eine gemeinsame Betrachtung und Dokumentation der Verarbeitungs- und Informationsverbunde. Sie kann sich des Weiteren auf die Identifizierung unerwünschter Ereignisse erstrecken, etwa durch die Erstellung eines gemeinsamen Szenarien- oder Gefährdungskatalogs inklusive einer gemeinsamen Einschätzung der Eintrittswahrscheinlichkeiten für diese zu vermeidenden Ereignisse. Schließlich kann die Interaktion beider Disziplinen durch eine gemeinsame Auswahl geeigneter Schutzmaßnahmen den Kernbereich beim risikobasierten Vorgehen besonders effizient ausgestalten und umsetzen.

Aufgrund der großen Bedeutung der bestehenden Synergien werden derzeit die bisher erlangten Erkenntnisse durch weitere umfangreichere Praxisbeispiele und Konkretisierungsschritte konsolidiert und erweitert. Nach Abschluss der praktischen Erprobungsphase sollen alle Ergebnisse umfassend dargestellt und veröffentlicht werden.

14.5 Prüfung der Verarbeitung von Kernbereichsdaten nach Art. 48 Abs. 5 Bayerisches Digitalgesetz

Der Freistaat Bayern stellt das sogenannte Bayerische Behördennetz (BYBN) als digitale Verwaltungsinfrastruktur für die behördenübergreifende Nutzung zur Verfügung. Hierzu habe ich im 19. Tätigkeitsbericht 2000 unter Nr. 17.1.2, im 20. Tätigkeitsbericht 2002 unter Nr. 17.1.1 und im 21. Tätigkeitsbericht 2004 unter Nr. 22.1.1 bereits berichtet. Der zentrale Schutz des Bayerischen Behördennetzes obliegt dem Landesamt für Sicherheit in der Informationstechnik, das im Rahmen seiner gesetzlichen Aufgaben auch personenbezogene Daten verarbeitet, um Gefahren für die Informationstechnik etwa durch Schadprogramme, programmtechnische Sicherheitslücken oder unbefugte Datenverarbeitung zu erkennen und abzuwehren (vgl. Art. 44 Bayerisches Digitalgesetz – BayDiG). Soweit erforderlich, hat diese IT-Sicherheitsbehörde für ihre Verarbeitungen eine Datenschutz-Folgenabschätzung durchgeführt.

Bei diesen Verarbeitungen ist aber nicht ausgeschlossen, dass auch personenbezogene Daten aus dem sogenannte „Kernbereich privater Lebensgestaltung" verarbeitet werden. Der Kernbereich privater Lebensgestaltung bezieht sich auf die grundlegenden Aspekte des persönlichen Lebens eines Individuums, die als besonders schützenswert gelten, und beansprucht gegenüber allen Überwachungsmaßnahmen Beachtung. Können Überwachungsmaßnahmen auch zur Erhebung kernbereichsrelevanter Daten führen, muss der Gesetzgeber Regelungen schaffen, die einen wirksamen Schutz normenklar gewährleisten.[209]

Im Art. 48 Abs. 5 BayDiG ist ausdrücklich geregelt, dass bei dieser Datenverarbeitung der Kernbereich privater Lebensgestaltung zu schützen ist. Konkret wird gefordert, dass Daten, die diesen sensiblen Bereich betreffen, nach Möglichkeit erst gar nicht erfasst werden (Art. 48 Abs. 5 Satz 1 BayDiG). Sollte es dennoch zu einer Erhebung solcher Daten kommen, ist deren Verwendung strikt untersagt und sie

[209] Bundesverfassungsgericht, Beschluss vom 24. Juni 2025, 1 BvR 180/23, Rn. 255.

müssen umgehend gelöscht werden (Art. 48 Abs. 5 Satz 2 BayDiG). Zudem ist erforderlich, dass die Erlangung und die anschließende Löschung dieser Daten dokumentiert werden (Art. 48 Abs. 5 Satz 3 BayDiG).

Im Berichtsjahr habe ich im Hinblick auf die Einhaltung der Vorgaben des Art. 48 Abs. 5 BayDiG eine anlasslose Prüfung durchgeführt.

Damit Daten aus dem Kernbereich privater Lebensgestaltung von Beschäftigen erst gar nicht erhoben werden, werden für die Internetnutzung im Rahmen des Bayerischen Behördennetzes sogenannte Coaching-Seiten genutzt: Wenn ein Beschäftigter einer an das Bayerische Behördennetz angebundenen öffentlichen Stelle eine Webseite, auf der ein Nutzer auch eigene Inhalte, die den Kernbereich privater Lebensgestaltung betreffen könnten, eingeben oder aufrufen kann (zum Beispiel Webseite einer Krankenkasse, bei der online ein Erstattungsantrag gestellt werden kann), wird der Beschäftigte mit Hilfe einer Coaching-Seite, die der eigentlich aufgerufenen Webseite vorgeschaltet ist, auf die aktivierten Schutzmaßnahmen und auf die Optionen für das weitere Vorgehen hingewiesen. Dieser implementierte Schutz vor einer möglichen Erhebung personenbezogener Daten aus dem Kernbereich privater Lebensgestaltung wird den Benutzern des Bayerischen Behördennetzes durch Informationen auf der internen Webseite der IT-Sicherheitsbehörde erklärt. Auch bei den weiteren Datenverarbeitungen, die zur Erkennung und Abwehr von Gefahren für die Informationstechnik dienen, hat das Landesamt seine Vorgehensweise so gestaltet, dass eine Erhebung von Daten aus dem Kernbereich privater Lebensgestaltung möglichst verhindert wird.

Als Ergebnis der Prüfung war festzuhalten, dass noch keine Daten gemäß Art. 48 Abs. 5 Satz 2 BayDiG erhoben wurden und somit auch nicht zu löschen waren. Daher war auch eine Dokumentation der Erlangung und Löschung von Kernbereichsdaten gemäß Art. 48 Abs. 5 Satz 3 BayDiG bislang nicht erforderlich.

14.6 Unzureichende Schwärzung: QR-Code enthielt personenbezogene Daten

Meldungen und Beschwerden zur unzureichenden Schwärzung von personenbezogenen Daten vor der Veröffentlichung von Dokumenten erreichen mich immer wieder. Der nachfolgende kleine Fehler einer Gemeinde ist jedoch ungewöhnlich:

Ihr Bürgermeister wollte für eine anstehende Wahl mobilisieren und veröffentlichte dazu eine geschwärzte Wahlbenachrichtigung eines Bürgers. Im Gegensatz zu anderen Vorfällen im Kontext „Schwärzung“ war in diesem Fall nicht die Methode das Problem. Allerdings war der auf der Wahlbenachrichtigung angegebene QR-Code nicht mit geschwärzt. Dieser QR-Code führte zu einem Online-Formular, mit dem man Briefwahlunterlagen beantragen konnte. So aufgerufen war das Formular bereits für einen konkreten Wahlberechtigten vorausgefüllt. Somit konnte jeder, der den QR-Code aufgerufen hat, dessen Daten einsehen. Die Gemeinde hatte schlicht übersehen, dass auch der QR-Code einen Weg zu personenbezogenen Daten eröffnete.

Der Sorge, dass sich ein unberechtigter Dritter Wahlunterlagen unter falschem Namen beschaffen könnte, wird dadurch begegnet, dass per QR-Code beantragte Wahlunterlagen immer an die bei der Kommune angegebene Meldeadresse verschickt werden und damit nicht in falsche Hände geraten können. Im konkreten

Fall wurden die betreffenden Briefwahlunterlagen persönlich übergeben, so dass Transparenz gegenüber der betroffenen Person sichergestellt war.

Da das Dokument sofort nach Bekanntwerden bei der Gemeinde gelöscht wurde und der Betroffene über den Vorfall in Kenntnis und über die möglichen Folgen aufgeklärt wurde, habe ich von einer aufsichtlichen Maßnahme abgesehen.

14.7 Verwarnungen nach Art. 58 Abs. 2 Buchst. b DSGVO

14.7.1 Verwarnung aufgrund unzureichender technisch-organisatorischer Schutzmaßnahmen einer Klinik bei einem Cybervorfall

Die IT-Infrastruktur einer Klinik wurde durch Cyberkriminelle infiltriert und mittels einer Ransomware verschlüsselt. Es waren alle IT-Systeme betroffen und für die Behandlung der Patienten musste auf Papier umgestellt werden. Zentrale Systeme zur elektronischen Patientenverwaltung standen einige Monate nicht oder nur eingeschränkt zur Verfügung. Der vollständige Wiederaufbau beziehungsweise die Neustrukturierung der IT-Infrastruktur konnte nach mehr als einem Jahr noch nicht vollständig abgeschlossen werden.

Einzelheiten zum Angriff konnten aufgrund fehlender Logdateien nicht nachvollzogen werden. Aus diesem Grund wurde auch auf eine forensische Untersuchung des Vorfalls seitens der Klinik verzichtet. Logfiles liegen häufig aus dem Grund nicht mehr vor, dass sie aus Gründen des Speicherplatzes nur eine bestimmte Größe zugewiesen bekommen und nach Erreichen dieser Größe automisch – mit den ältesten Einträgen beginnend – überschrieben werden. Wird der Sicherheitsvorfall erst Wochen oder Monate später festgestellt, sind die relevanten Daten häufig bereits auf diese Weise gelöscht.

Da der Angreifer eine Datenveröffentlichung androhte, war anzunehmen, dass Daten abgeflossen waren. Dies konnte aber ebenfalls aufgrund fehlender Logdateien weder festgestellt noch ausgeschlossen werden. Der Vorfall zeigt, wie wichtig es ist, sich über den Sinn und Zweck Protokollierungsmöglichkeiten von IT-Sicherheitskomponenten Gedanken zu machen sowie die Logfiles entsprechend zu dimensionieren und regelmäßig auszuwerten, um Angriffsversuche frühzeitig erkennen zu können.

Nach Art. 24 Abs. 1, Art. 25 Abs. 1 und Art. 32 Abs. 1 DSGVO muss der Verantwortliche insbesondere die erforderlichen und geeigneten technisch-organisatorischen Schutzmaßnahmen treffen, um ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau (nach Stand der Technik) im Zusammenhang mit dem Betrieb seiner IT-Systeme zu gewährleisten und die Vertraulichkeit, Integrität, Verfügbarkeit sowie Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. Zudem ist der Verantwortliche verpflichtet, Nachweise erbringen zu können, dass die Verarbeitung gemäß den Vorgaben der Datenschutz-Grundverordnung erfolgt (vgl. Art. 24 Abs. 1 Satz 1 DSGVO). Welche technisch-organisatorischen Schutzmaßnahmen gemäß Art. 32 DSGVO zu treffen sind, richtet sich nach den einschlägigen Standards, wie beispielsweise vom Bundesverband IT-Sicherheit e. V. und

dessen Handreichung zum „Stand der Technik“[210] oder das IT-Grundschutz-Kompendium vom Bundesamt für Sicherheit in der Informationstechnik.[211]

In Anbetracht des Umstands, dass die Klinik gegen die genannten datenschutzrechtlichen Vorgaben verstoßen hat und es sich bei den betroffenen Daten überwiegend um sensible Daten – einschließlich von Daten im Sinne von Art. 9 Abs. 1 DSGVO – gehandelt hat, habe ich die Klinik nach Art. 58 Abs. 2 Buchst. b DSGVO verwarnt.

Ergänzend begleite ich den datenschutzkonformen Wiederaufbau der IT-Infrastruktur bis zur vollständigen Behebung der festgestellten datenschutzrechtlichen Mängel.

14.7.2 Verwarnung wegen unzureichender Nutzertrennung bei Nutzung eines Gastzuganges in einem Online-Antragsverfahren

Eine öffentliche Stelle meldete einen Datenschutzvorfall im Rahmen eines Onlineantragsverfahrens, bei dem Nutzer aufgrund eines Systemfehlers unberechtigterweise auf Daten anderer Nutzer zugreifen konnten. Das Online-Antragsverfahren nutzte zur Authentifizierung die Zugangsmöglichkeiten des BayernPortals. Bei der Anmeldung über das BayernPortal wird normalerweise für jeden Nutzer eine individuelle bereichsspezifische Personenkennziffer (bPK) generiert, die zur eindeutigen Identifikation dient. Im vorliegenden Fall stellte sich jedoch heraus, dass bei Nutzung eines Gastzugangs für alle Anwender eine identische bPK vergeben wurde, die ausschließlich aus Nullen bestand. Dies führte dazu, dass das System alle Nutzer mit Gastzugang als ein und dieselbe Person behandelte und diesen Nutzern die begonnenen Anträge sämtlicher anderer Gastzugangs-Nutzer anzeigen ließ.

Technisch war das Problem darauf zurückzuführen, dass die verantwortliche Stelle bei der Verarbeitung der vom BayernPortal übermittelten Authentifizierungsdaten nicht vorhandene Werte durch einheitliche Platzhalter ersetzte. Dies führte bei der Übernahme der Daten in das Online-Antragsverfahren zu einer Uneindeutigkeit, die eine korrekte Nutzerzuordnung unmöglich machte.

Die datenschutzrechtliche Bewertung des Vorfalls ergab, dass die verantwortliche Stelle ihre Pflichten nach Art. 25 und Art. 32 DSGVO verletzt hatte. Nach diesen Vorschriften hat der Verantwortliche unter Berücksichtigung des Stands der Technik geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Der Einsatz einer für alle Gastnutzer identischen ID widerspricht grundlegenden Prinzipien sicherer Softwarearchitektur, wie sie etwa im BSI IT-Grundschutz-Kompendium[212] nieder-

[210] Internet: https://www.teletrust.de/publikationen/broschueren/stand-der-technik.

[211] Internet: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html.

[212] Internet: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html.

gelegt sind. In modernen Softwarearchitekturen werden IDs gerade dazu eingesetzt, um Datensätze eindeutig zu unterscheiden und insbesondere bei nutzerbezogenen Daten eine korrekte Zuordnung sicherzustellen.

Eine Implementierung, bei der alle Nutzer dieselbe ID erhalten, macht eine Nutzerunterscheidung unmöglich und widerspricht damit elementaren Sicherheitsgrundsätzen.

Erschwerend kommt hinzu, dass die Dokumentation zur Anbindung von Drittanwendungen an das Bayernportal explizit darauf hinweist, dass bei Nutzung bestimmter Anmeldeoptionen, insbesondere des temporären Logins, die bPK und andere Werte entfallen können. Die Dokumentation stellt ausdrücklich klar, dass das Error-Handling in solchen Fällen bei der Drittanwendung stattfinden muss und nicht im Nutzerkonto selbst. Die verantwortliche Stelle hätte demnach bei der Implementierung vorsehen müssen, dass fehlende oder ungültige bPK-Werte erkannt und entsprechend behandelt werden.

Auch die im Rahmen der Entwicklung des Onlineverfahrens durchgeführten Tests erwiesen sich als unzureichend. Zwar wurden entwicklungsbegleitende Tests durchgeführt, jedoch wurden offenbar nicht alle Grenzfälle und nicht von der Spezifikation umfasste Eingaben abgeprüft. Gerade bei der Verwendung externer Komponenten ist zu beachten, dass sich schnelle Änderungen an den Spezifikationen ergeben können, auf die die eigene Softwareentwicklung reagieren können muss. Unit-Tests, die auch Grenzfälle abdecken, hätten das Problem frühzeitig aufdecken können. Mit der dargestellten Verarbeitung hat die verantwortliche Stelle die Integrität und Vertraulichkeit personenbezogener Daten im Sinne von Art. 5 Abs. 1 Buchst. f DSGVO verletzt. Besonders schwerwiegend ist, dass es sich bei den betroffenen Daten unter anderem um besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO handelte, die einem erhöhten Schutzbedürfnis unterliegen.

Als Sofortmaßnahme wurde der Gastzugang deaktiviert und eine zusätzliche Prüfung der bPK auf Nicht-Null-Werte implementiert, um künftige unberechtigte Zugriffe zu verhindern. Aufgrund der Schwere des Verstoßes und der Versäumnisse bei der technischen Umsetzung wurde eine Verwarnung ausgesprochen.

Dieser Vorfall zeigt, wie wichtig die korrekte Implementierung von Schnittstellen bei der Einbindung von Komponenten anderer Stellen für Digitalisierungsverfahren ist. Diese Thematik wird zukünftig an Relevanz gewinnen, wenn im Rahmen der Digitalisierung und Staatsmodernisierung zunehmend von anderen Stellen entwickelte (Standard-)Komponenten („Einer-für-alle-Prinzip“) eingebunden werden sollen.

14.7.3 Zwei Landratsämter wurden wegen wiederholter Missachtung datenschutzrechtlicher Vorgaben bei der E-Mail-Kommunikation verwarnt

Im ersten Fall hat ein Landratsamt trotz mehrfacher Hinweise in den Jahren 2020 und 2022 zur datenschutzkonformen Verarbeitung bei der E-Mail-Kommunikation erneut Gesundheitsdaten unverschlüsselt und somit ungesichert per E-Mail versendet. Die Ursache lag vor allem darin, dass die Sensibilität der versandten Da-

ten nicht erkannt wurde. Dies zeigte, dass offenbar immer noch kein ausreichendes Verständnis für die besonderen Anforderungen bei der Verarbeitung sensibler Daten in der digitalen Kommunikation bestand.

Nach den geltenden datenschutzrechtlichen Bestimmungen besteht die Verpflichtung, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko für die Rechte und Freiheiten der betroffenen Personen angemessenes Schutzniveau zu gewährleisten. Dazu zählt insbesondere die Verschlüsselung der Daten bei der digitalen Übermittlung. Diese Verschlüsselung muss nicht nur technisch bereitgestellt werden, sondern die Beschäftigten müssen auch hinsichtlich der Risiken eines E-Mail-Versands sowie der Nutzung von Verschlüsselungstools geschult werden.

Im vorliegenden Fall waren zwar geeignete Verschlüsselungslösungen vorhanden, jedoch wurde die besondere Kategorie der personenbezogenen Daten (Gesundheitsdaten) bei der E-Mail-Kommunikation nicht berücksichtigt. Dies führte zu einem Verstoß gegen die Verpflichtungen nach Art. 24 Abs. 1, Art. 25 Abs. 1 und Art. 32 Abs. 1 in Verbindung mit Art. 9 Abs. 1 DSGVO.

Somit war trotz der vorhandenen technischen Möglichkeiten und der gesetzlichen Vorgaben kein angemessener, datenschutzkonformer Umgang mit den sensiblen personenbezogenen Daten gewährleistet. Aufgrund der wiederholten Verstöße und des fehlenden Verständnisses für den Schutz besonders sensibler Daten habe ich eine Verwarnung gegen das Landratsamt ausgesprochen.

In einem weiteren Fall informierte das Gesundheitsamt eines Landratsamtes per E-Mail betroffene Bürgerinnen und Bürger über einen Krankheitsfall mit einer ansteckenden Leberentzündung. Diese E-Mail wurde unverschlüsselt und ungesichert sowie unter Verwendung der offenen Adressfelder „An“ oder „Cc“ an neun Empfänger versandt, sodass alle Empfänger die E-Mail-Adressen der anderen sehen konnten. Aufgrund der offenen Adressierung und der örtlichen Verhältnisse war es wahrscheinlich, dass die Empfänger die Identität des Erkrankten und seiner Familie indirekt erkennen konnten.

Auch hier handelt es sich bei den übermittelten Informationen um sensible personenbezogene Daten (Gesundheitsdaten), die nach der Datenschutz-Grundverordnung besonderen Schutz genießen. Die Offenlegung dieser Daten erfolgte unrechtmäßig, da keine Rechtsgrundlage für die Verarbeitung ersichtlich war. Zudem wurden die E-Mail-Adressen der Empfänger unbefugt offengelegt.

Das Landratsamt war bereits 2022 auf die Notwendigkeit einer datenschutzkonformen E-Mail-Kommunikation hingewiesen worden, insbesondere auf die Verschlüsselung sensibler Daten und die Nutzung des BCC-Feldes. Trotz vorhandener technischer Möglichkeiten und einer Geschäftsanweisung zur sicheren Datenverarbeitung kam es auch hier erneut zu einem Verstoß.

Auch hier gelangte ich bei der Bewertung des Sachverhalts zu dem Ergebnis, dass das Landratsamt die Verpflichtungen, geeignete technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten zu treffen, insbesondere bei der digitalen Übermittlung von Gesundheitsdaten, missachtet hat. Die wiederholten Verstöße zeigten, dass im Landratsamt kein durchgängiges Verständnis für den datenschutzkonformen Umgang mit sensiblen Daten in der elektronischen Kommunikation bestand.

Aus diesem Grund habe ich eine Verwarnung gegen das Landratsamt ausgesprochen. Zudem habe ich das Landratsamt aufgefordert, die datenschutzrechtlichen Vorgaben künftig strikt einzuhalten und die technischen sowie organisatorischen Maßnahmen konsequent umzusetzen, um ein angemessenes Schutzniveau für die Rechte und Freiheiten der betroffenen Personen sicherzustellen.

In diesem Zusammenhang möchte ich erneut darauf hinweisen, wie wichtig regelmäßige Datenschutz-Schulungen für aller Beschäftigten sind. Es zeigt sich immer wieder, dass gerade auch in stressigen Situationen Fehler beim E-Mail-Versand passieren. Deswegen sollten die richtigen Verhaltensweisen nicht nur erklärt, sondern auch praktisch geübt werden.

Hilfreich können hierbei Checklisten für die wichtigsten Punkte sein, wie etwa

— BCC verwendet?
— Richtige Adressaten eingegeben?
— Bei Auto-Vervollständigen: Richtiger Adressat automatisch eingefügt?
— Verschlüsselung eingeschaltet?

14.8 Beanstandung auf Grund mehrfacher Datenschutzverstöße im Rahmen des Streamings einer Stadtratssitzung

Eine Stadt übertrug den öffentlichen Teil der Stadtratssitzung als Livestream über das Portal YouTube. Dabei wurde ein externer Dienstleister mit der Bereitstellung von Video- und Tonstreams für die Hybridsitzung des Stadtrates beauftragt. Auch der nicht-öffentliche Teil der Stadtratssitzung wurde als Bild- und Ton-Übertragung übertragen. Insgesamt wurden 15 Minuten und 40 Sekunden der nicht-öffentlichen Sitzung live veröffentlicht. Im nicht-öffentlichen Teil der Sitzung standen unter anderem Personalangelegenheiten auf der Tagesordnung. Das Video des betroffenen Sitzungsteils war auch nach Beendigung des Livestreams noch über das Internet zugreifbar und wurde erst später – nach Hinweis einer dritten Person – durch die Pressestelle aus dem YouTube-Kanal der Stadt entfernt. Die Veröffentlichung der nicht-öffentlichen Stadtratssitzung als Livestream sowie als nachträglich abrufbares Video über YouTube war nicht beabsichtigt. Lediglich der öffentliche Sitzungsteil sollte ausschließlich als Livestream veröffentlicht werden.

Die Stadt konnte nicht abschließend klären, wie die Wiederaufnahme des Livestreams ausgelöst wurde. Geklärt werden konnte lediglich, dass ein menschlicher Fehler bei einem Dienstleister mit ursächlich war.

Für die Veröffentlichung der nicht-öffentlichen Sitzung gab es keine Rechtsgrundlage – weder für einen Livestream noch für eine längerfristige Bereitstellung der Aufzeichnung. Da im nicht-öffentlichen Teil der Sitzung personenbezogene Daten besprochen wurden, lag hier ein Datenschutzverstoß vor.

Die Stadt hat nach dem Vorfall zahlreiche technisch und organisatorische Maßnahmen zur Wahrung der IT-Sicherheit sowie die Erstellung und Aktualisierung notwendiger Dokumentationen nachgeholt. Hier gab es einiges zu tun. Begrüßenswert war insbesondere die Einführung einer OnAir-Lampe, durch die Teilnehmer nun transparent erkennen können, dass gerade eine Aufzeichnung stattfindet.

Bei der Auswahl von YouTube als Plattform zur Veröffentlichung des Livestreams hatte die Stadt keine Risikobetrachtung vorgenommen. Nach Angabe der Stadt sei YouTube auf Grund des Bekanntheitsgrades gewählt worden. Eine datenschutzfreundliche Voreinstellung, bei der der Livestream standardmäßig auf „privat“ eingestellt werden kann, wodurch zumindest die nachträgliche öffentliche Verfügbarkeit verhindert worden wäre, sei bei YouTube nicht möglich gewesen.

Ich habe den Verstoß auf Grund der unrechtmäßigen Veröffentlichung, des Unterschreitens der allgemein anerkannten Regeln der Technik, des Fehlens eines Berechtigungs- und Löschkonzepts und auf Grund von fehlenden datenschutzfreundlichen Voreinstellungen zur Vermeidung der Veröffentlichung beanstandet.

Ergänzend habe ich die Stadt darauf hingewiesen, dass unter Abwägung aller Risiken bei einer Verarbeitung der Bekanntheitsgrad eines Dienstes ausschließlich dann in die Abwägung mit einbezogen werden sollte, wenn das Risiko durch den Einsatz des Dienstes nicht steigt.

Dieser Vorfall macht deutlich, welche technischen Tücken selbst bei der Umsetzung mit Hilfe eines Dienstleisters bestehen können. Ich rate daher dringend, zum einem im Rahmen der Konzeption des Livestreamings mögliche technische und organisatorische Probleme und Gefahren etwa im Rahmen einer Risikoanalyse umfassend zu betrachten. Zum anderen sollte auch während des Livestreamings nicht-öffentlicher Sitzungsteile kontrollierbar sein und überwacht werden, ob tatsächlich keine Übertragung und/oder Aufzeichnung stattfindet.

14.9 Meldungen von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DSGVO

14.9.1 Patientin irrtümlich von der Krankenkasse als verstorben gemeldet

Ein besonders gearteter Fall, der zu schwerwiegenderen Auswirkungen für die betroffene Person führte, wurde mir von einem bayerischen öffentlichen Klinikum gemeldet:

In diesem Klinikum wurden die Stammdaten einer Patientin A aufgrund einer Verwechslung versehentlich mit den Stammdaten der Patienten B überschrieben. In der Folge wurde bei der Patientin A irrtümlich der Behandlungsfall der anderen Patientin B erfasst. Diese Patientin B verstarb. Ihr Tod wurde jedoch im IT-System bei Patientin A eingetragen. Daraufhin wurde das mutmaßliche Ableben der Patientin A von der Klinik an deren Krankenkasse gemeldet. Die Versicherte wurde in Folge von ihrer Krankenkasse informiert, dass sie verstorben sei und abgemeldet wurde.

Es ist durchaus vorstellbar, dass eine irrtümliche Für-Tod-Erklärung zu größeren finanziellen, gesundheitlichen oder immateriellen Schäden für die betroffene Patienten A führen kann, wenn beispielsweise

— erforderliche Leistungen von der Krankenkasse nicht mehr erbracht werden, gegebenenfalls andere Stellen (wie zum Beispiel die Rentenversicherung) im automatischen Datenabgleich über den Tod informiert werden und ebenfalls ihre Leistungen einstellen,

— psychische Belastungen durch die Nachricht vom eigenen Tod entstehen oder

— ein erhöhter organisatorischer Aufwand für die Richtigstellung der Daten erforderlich wird.

Glücklicherweise konnte der Vorfall im Klinikum auf Basis der vorhandenen Protokollierung des IT-Systems nachvollzogen werden; die Daten für beide Patientinnen konnten mit Hilfe des Backups korrigiert werden.

Damit wird erneut die Bedeutung eines gut funktionierenden Datenschutzmanagementsystems, einer verlässlichen Umsetzung von Basis-IT-Sicherheitsmaßnahmen sowie eines stets verfügbaren Backup-Systems, ferner einer angemessenen Protokollierung von Zugriffen und Änderungen von Daten deutlich.

14.9.2 Automatisierter Abruf von Grundbuchdaten ohne erforderliche Zustimmung

Im Berichtszeitraum wurde eine Meldung über eine Verletzung des Schutzes personenbezogener Daten im automatisierten Grundbuchabrufverfahren bekannt. Bei einer Stichprobenkontrolle des IT-Servicezentrums der bayerischen Justiz ergab sich der Verdacht, dass sich eine zugelassene Teilnehmerin unrechtmäßig Daten ohne die erforderliche Zustimmung der Eigentümer verschafft hatte.

Eine Kanzlei hatte eine Auskunft aus dem Grundbuch abgerufen. Auf Nachfrage wurde ein berechtigtes Interesse als Rechtsgrundlage genannt, eine Zustimmung der betroffenen Eigentümer konnte jedoch nicht vorgelegt werden. Dies lässt darauf schließen, dass die Voraussetzungen des § 133 Abs. 4 Satz 3 Grundbuchordnung (GBO) für den automatisierten Abruf nicht erfüllt waren.

Rechtlich beruht das automatisierte Abrufverfahren auf § 133 GBO, wonach Teilnehmende auf Grundlage einer Zulassung und unter Angabe der erforderlichen Parameter Auskünfte automatisiert abrufen können. Die zulassende Stelle überprüft dabei regelmäßig die Einhaltung der rechtlichen Voraussetzungen im Rahmen von Stichprobenkontrollen.

Im konkreten Fall wurde der Teilnehmerin aufgezeigt, dass das Berechtigungsinteresse im Sinne des § 12 GBO allenfalls für eine manuelle Einsichtnahme in Betracht kommt, nicht jedoch für die Nutzung des automatisierten Abrufs. Für den automatisierten Abruf ist zwingend die Zustimmung der Eigentümer oder eine ausdrückliche gesetzliche Grundlage erforderlich.

Die unbegründete Nutzung des automatisierten Abrufs stellt eine Verletzung datenschutzrechtlicher Vorgaben dar, da es sich um eine unbefugte Offenlegung personenbezogener Daten handelt.

Die Kontrollmechanismen zur Sicherstellung der Rechtskonformität automatisierter Abrufe haben sich im vorliegenden Fall als wirkungsvoll erwiesen. Die betroffene Kanzlei wurde von der bayerischen Justiz belehrt und entsprechend informiert, dass künftige Abrufe nur auf rechtmäßiger Grundlage erfolgen dürfen.

14.10 Zuletzt: Aufregung wegen öffentlich zugänglicher Briefe vom Christkind

Ein Bürger hatte mich angeschrieben, weil in einer Gemeinde die Postkisten mit Briefen vom Christkind an die Kinder vor der Rathaustüre standen. Die Kisten waren nur mit einem Klappdeckel verschlossen, sodass jeder neugierige Weihnachtswichtel hätte hineinschauen oder Briefe entwenden können. Datenschutz? Im ganzen Stress nicht dran gedacht! Jeder hätte sehen können, wer dem Christkind etwas ins Ohr geflüstert hat.

Die Gemeinde erklärte, dass die Kisten nur kurz vor der Abholung draußen standen, damit die Post schnell wegkommt. Das Christkind konnte also aufatmen: Die Briefe kamen sicher an. Damit im nächsten Jahr keine neugierigen Weihnachtswichtel an die Briefe herankommen, werden sie in Zukunft bis zur Abholung im Gebäude verwahrt. Der sicheren Kommunikation des Christkinds mit den Kindern steht also nichts mehr im Wege!

15 Datenschutzkommission

Der Datenschutzkommission beim Bayerischen Landtag gehörten im Berichtszeitraum folgende Mitglieder und stellvertretende Mitglieder an:

Aus dem Landtag:

Mitglieder:

Peter Tomaschko, CSU
Tobias Beck, FREIE WÄHLER
Benjamin Adjei, BÜNDNIS 90/DIE GRÜNEN
Horst Arnold, SPD
Dr. Alexander Dietrich, CSU
Thomas Holz, CSU
Gerd Mannes, AfD

Stellvertretende Mitglieder:

Leo Dietz, CSU
Felix Locke, FREIE WÄHLER
Verena Osgyan, BÜNDNIS 90/DIE GRÜNEN
Katja Weitzel, SPD
Josef Heisl, CSU
Thorsten Schwab, CSU
Roland Magerl, AfD

Auf Vorschlag der Staatsregierung:

Mitglied:

Leitende Ministerialrätin Christina Rölz, Datenschutzbeauftragte des Bayerischen Staatsministeriums des Innern, für Sport und Integration

Stellvertretendes Mitglied:

Leitende Ministerialrätin Ilka Bürger, Datenschutzbeauftragte des Bayerischen Staatsministeriums für Wirtschaft, Landesentwicklung und Energie

Auf Vorschlag der kommunalen Spitzenverbände in Bayern:

Mitglied:

Rudolf Schleyer, Vorstandsvorsitzender der Anstalt für Kommunale Datenverarbeitung in Bayern

Stellvertretendes Mitglied:

Cynthia Derra, Datenschutzbeauftragte des Bayerischen Landkreistags

Auf Vorschlag des Staatsministeriums für Gesundheit, Pflege und Prävention aus dem Bereich der gesetzlichen Sozialversicherungsträger:

Mitglied:

Werner Krempl, Erster Direktor und Geschäftsführer der Deutschen Rentenversicherung Nordbayern

Stellvertretendes Mitglied:

Dr. Irmgard Stippler, Vorsitzende des Vorstandes der AOK Bayern – Die Gesundheitskasse

Auf Vorschlag des Verbands Freier Berufe in Bayern e. V.:

Mitglied:

Dr. Till Schemmann, Notar

Stellvertretendes Mitglied:

Dr. Thomas Kuhn, Rechtsanwalt

Herr Peter Tomaschko, MdL, führte den Vorsitz in der Datenschutzkommission; stellvertretender Vorsitzender war Herr Tobias Beck, MdL.

Die Datenschutzkommission beim Bayerischen Landtag tagte im Berichtszeitraum drei Mal.

16 Ländervertreter im EDSA

Im Europäischen Datenschutzausschuss (EDSA) nehme ich als vom Bundesrat gewählter Vertreter gemeinsam mit dem oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit das deutsche Stimmrecht wahr (allgemein zum EDSA und zu meinen Aufgaben als Ländervertreter siehe meinen 31. Tätigkeitsbericht 2021 unter Nr. 12).

Der EDSA hat 2025 zwölfmal getagt. Schwerpunkt der Tätigkeit war die Arbeit an Leitlinien zum Verhältnis des Datenschutzrechts zu den sogenannten europäischen Digitalrechtsakten. Dazu zählen insbesondere das Gesetz über digitale Dienste (Digital Services Act, DSA), das Gesetz über digitale Märkte (Digital Markets Act, DMA) oder die Verordnung über künstliche Intelligenz (AI Act).

Die Digitalrechtsakte zielen auf die Ermöglichung und Förderung einer innovativen, wirtschaftlichen und gemeinwohlorientierten Nutzung von Daten. Im Interesse des europäischen Binnenmarkts legen sie Regeln für die Datennutzung fest und schaffen insbesondere zugunsten des freien Datenverkehrs neue Zugangsrechte zu bei verschiedenen Akteuren vorhandenen Daten.

Somit verfolgen die Digitalrechtsakte zum Teil ganz andere Ziele als das Datenschutzrecht. Dieses schützt primär das individuelle Grundrecht auf informationelle Selbstbestimmung und setzt klare Grenzen für die Verarbeitung personenbezogener Daten durch Prinzipien wie Zweckbindung, Datenminimierung und das Erfordernis einer Rechtsgrundlage für jeden Umgang mit personenbezogenen Daten.

Um beide Rechtsmaterien miteinander in Einklang zu bringen, erarbeitet der EDSA Leitlinien – im aktuellen Berichtszeitraum 2025 erstmals auch gemeinsam mit der Europäischen Kommission.

Die **Leitlinien 03/2025 zum Verhältnis zwischen der Datenschutz-Grundverordnung und dem Gesetz über digitale Dienste**[213] zielen auf eine kohärente Anwendung der sich teilweise überschneidenden Vorschriften ab. Das Gesetz über digitale Dienste will ein sicheres Online-Umfeld und einen umfassenden Grundrechtsschutz aller Nutzer sicherstellen. Im Vordergrund der Leitlinien stehen daher vor allem Fragen der Altersprüfung, des Minderjährigenschutzes und spezifische Maßnahmen zur Vermeidung manipulativer Praktiken. Die Leitlinien von EDSA und Europäischer Kommission sollen unter anderem dazu dienen, eine widerspruchsfreie Anwendung der Vorschriften des Gesetzes über digitale Dienste und der Datenschutz-Grundverordnung sicherzustellen.

Hervorzuheben sind auch die **gemeinsamen Leitlinien der Europäischen Kommission und des EDSA zum Verhältnis zwischen der Datenschutz-Grundverordnung und dem Gesetz über digitale Märkte**.[214] Ziele des Gesetzes über

[213] Internet: https://www.edpb.europa.eu/system/files/2025-09/edpb_guidelines_202503_interplay-dsa-gdpr_v1_en.pdf (Fassung nach Abschluss der öffentlichen Konsultation).

[214] Internet: https://www.edpb.europa.eu/system/files/2025-10/joint_com-edpb_gls_

digitale Märkte sind die Sicherstellung des Wettbewerbs im digitalen Raum und fairer Bedingungen für alle Marktteilnehmer. Das Gesetz legt Regeln für große Online-Plattformen fest, die als sogenannte Gatekeeper (deutsch: „Torwächter") fungieren. Die Leitlinien von EDSA und Europäischer Kommission sollen unter anderem die Gatekeeper bei der Umsetzung ihrer Verpflichtungen unterstützen.

Der EDSA wird sich auch künftig intensiv mit dem Verhältnis der Digitalrechtsakte und dem Datenschutz befassen. Weitere Leitlinien sind zu erwarten, vor allem allgemein mit Blick auf die Verordnung über künstliche Intelligenz (KI-Verordnung/AI Act) oder auch speziell zum Thema „Data Scraping", bei dem Daten aus dem Internet systematisch gesammelt und beispielsweise als Grundlage für das Training künstlicher Intelligenz genutzt werden.[215]

Aus der sonstigen Tätigkeit des EDSA im Jahr 2025[216] ist noch die Verabschiedung von **Leitlinien 02/2025 zur Verarbeitung personenbezogener Daten bei der Blockchain-Technologie**[217] besonders erwähnenswert. Diese Leitlinien empfehlen zahlreiche Maßnahmen zum datenschutzkonformen Einsatz dieser neuen Technologie. Die **Guidelines 01/2025 zur Pseudonymisierung**[218] schließlich konnten zur öffentlichen Konsultation vorgelegt werden. Zusätzliche Leitlinien zur **Anonymisierung von personenbezogenen Daten** sind weiterhin in Arbeit und waren unter anderem Gegenstand eines Stakeholder-Events im November 2025 in Brüssel.

interplay_dma_gdpr_for_public_consultation_en.pdf (Fassung nach Abschluss der öffentlichen Konsultation).

215 Vgl. das Arbeitsprogramm des EDSA für 2026 und 2027, Internet: https://www.edpb.europa.eu/news/news/2026/edpb-work-programme-2026-2027-easing-compliance-and-strengthening-cooperation-across_de.

216 Für einen umfassenderen Überblick über die Tätigkeit des EDSA siehe seine im Internet unter https://www.edpb.europa.eu/about-edpb/about-edpb/annual-reports_de veröffentlichten jährlichen Tätigkeitsberichte.

217 Internet: https://www.edpb.europa.eu/system/files/2025-11/edpb_guidelines_202402_article48_v2_de.pdf.

218 Internet: https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf.

Abkürzungsverzeichnis

ABl.	Amtsblatt der Europäischen Union
Abs.	Absatz
a. a. O.	am angegebenen Ort (Verweis auf die zuvor angeführte Quelle)
a. F.	alte Fassung
AfD	Alternative für Deutschland
Art.	Artikel
Aufl.	Auflage
BayDSG	Bayerisches Datenschutzgesetz
BeckRS	Beck-Rechtsprechung (Datenbank)
BDSG	Bundesdatenschutzgesetz
BGBl.	Bundesgesetzblatt
Buchst.	Buchstabe
CSU	Christlich-Soziale Union in Bayern
DSFA	Datenschutzfolgenabschätzung
DSGVO	Datenschutz-Grundverordnung
EDV	Elektronische Datenverarbeitung
EG	Erwägungsgrund
FDP	Freie Demokratische Partei
ff.	(nach)folgende
GVBl.	Bayerisches Gesetz- und Verordnungsblatt
https	Hyper Text Transfer Protocol Secure
IP	Internet Protocol
IT	Informationstechnik
MdL	Mitglied des Landtages
Nr.	Nummer
PC	Personalcomputer
RLDSJ	Datenschutz-Richtlinie für Polizei und Strafjustiz
Rn.	Randnummer
sog.	sogenannt
SPD	Sozialdemokratische Partei Deutschlands
SSL	Secure Socket Layer
u. a.	unter anderem/und andere
UAbs.	Unterabsatz
vgl.	vergleiche
www	World Wide Web

Stichwortverzeichnis

Aktiengesellschaft
    Öffentliche Stelle 72
Anfrage (vertrauliche)
    Weiterleitung 156
Arbeitssicherheitsfachkraft
    Unfallanzeigen 133
Arztbrief
    Berichtigung 102
    Korrektur 102
Aufbewahrungsfrist
    Patientendaten 99
Auskunft
    Verfassungsschutz 54
Auskunft
    CD-ROM 104
Auskunft (Art 39 BayDSG)
    Personenbezogene Daten 162
Auskunftsanspruch
    Spielbank 15
Ausländerbehörde
    Datenanforderung an Sozialbehörde 131
    Übermittlung von Jobcenter 130
Ausschreibung zur polizeilichen Beobachtung 48
Automatisierte Entscheidungsfindung
    KI 39
Bauleitplanung
    Digitalisierung 81
    Einsicht in Vorarbeiten 161
BCC-Feld
    E-Mail 180
Behördennetz
    Kernbereichsdaten (Beschäftigte) 176
Beitragsservice
    Meldedaten 83
Beobachtung (polizeiliche) 48
Beratungsangebote
    Gesundheitsamt 90
Berichtigung
    Arztbrief 102
    Diagnosedaten (Krankenkasse) 114
Beschäftigtennamen
    Schreiben 149
Betroffenenrechte
    KI 39
Bewerber (öffentlicher Dienst)
    Verfassungstreue 144
Bezirkskrankenhaus
    Bodycam (polizeiliche) 50

Bodycam
Polizei 50
Bodycam (polizeiliche)
Bezirkskrankenhaus 50
Briefversand
Datenschutz 169
Bürgerantrag
Einsichtnahme 61
Unterschriftenauswertung 61
Unterschriftenliste 61
Unterschriftennutzung 61
Zweckbindung 61
Bürgerbegehren
Einsichtnahme 61
Unterschriftenauswertung 61
Unterschriftenliste 61
Unterschriftennutzung 61
Zweckbindung 61
Bürgerversammlung
Einsichtnahme 61
Unterschriftenauswertung 61
Unterschriftenliste 61
Unterschriftennutzung 61
Zweckbindung 61
CC-Feld
E-Mail 180
CD-ROM
Auskunftsmittel (Krankenhaus) 104
Cybervorfall
Klinik 178
Datenabruf
Grundbuch 184
Datenpannenmeldung
Hackerangriff 19
Datenschutzkonzept
Digitalisierung 174
Diagnose
Patientenquittung 112
Diagnosedaten
Berichtigung (Krankenkasse) 114
Dienstfähigkeitsuntersuchung
Externer Gutachter 92
Dienstfähigkeitszusatzbegutachtung 92
Digitales & KI (Stabsstelle) 28
Digitalisierung
Bauleitplanung 81
Datenschutzkonzept 174
Planfeststellung 81
Raumordnung 81
Wasserbuch 79
Digitalisierungsprojekte
Datenschutzgerechte Planung 174

Drittlandtransfer
KI-Produkte 40
Drohne
Kommunale Aufgaben 66
Eignungsprüfung
Kindertagespflegeperson 126
Elterninformation
Volljährige Beschuldigte 52
E-Mail
BCC-Feld 180
CC-Feld 180
E-Mail-Verschlüsselung 180
Entscheidungsfindung (automatisierte)
KI 39
Ermittlungsverfahren
Offenlegung nicht mehr beschuldigte Person 56
Fachkraft für Arbeitssicherheit
Unfallanzeigen 133
Gastzugang
Unzureichende Nutzertrennung 179
Geldwäscheprävention
Spielbank 15
Gemeinde
Drohnenbefliegung 66
Jubiläumsfeier 64
Öffentlichkeitsarbeit 64
Ortschronik 64
Streaming (nichtöffentliche Gemeinderatssitzung) 182
Geoportale
Legislativer Handlungsbedarf 76
Gesundheitsamt
Beratungsangebote 90
Dienstfähigkeitsuntersuchung 92
Freiwillige Beratungsangebote 90
Gleichstellungsbeauftragten
Informationsrechte 141
Gleichstellungsgesetz
Novellierung 139
Gleichstellungskonzepte 139
Grundbuch
Datenabruf (illegaler) 184
Grundsicherung
Einkommenserforschung wegen Verwandtenunterhalt 124
Gutachter
Dienstfähigkeitsuntersuchung 92
Hackerangriff
Datenpannenmeldung 19
Strafanzeige 22
Hausmeister
Kein Ermittlungsgehilfe 157
Informationsfreiheit
Datenschutz 162
Vorarbeiten von Bauleitplanung 161

Informationssicherheit
Datenschutz (Synergien) 175
IT-Sicherheit
Datenschutz (Synergien) 175
Jobcenter
Übermittlung an Ausländerbehörde 130
Jugendämter
Sammelermächtigungen 152
Kameras
Parken 70
Kartenviewer
Legislativer Handlungsbedarf 76
Kernbereichsdaten (Beschäftigte)
Prüfung 176
KI
Automatisierte Entscheidungsfindung 39
Betroffenenrechte 39
Drittlandsprodukte 40
Entscheidungsfindung (automatisierte) 39
Rechenschaftspflicht (datenschutzrechtliche) 32
Rollenmodell (datenschutzrechtliches) 30
Transparenz 39
Kindertagespflege
Eignungsfeststellung 126
KI-Verordnung 27
Kommune
Drohnenbefliegung 66
Kommunen
Wärmeplanung 58
Kontaktfomular
Mammografie-Screening 117
Kopie
CD-ROM 104
Korrektur
Arztbrief 102
Krankenhaus
Todesmeldung (irrtümliche) 183
Krankenhaus
CD-ROM als Auskunftsmittel 104
Videoüberwachung 108
Krankenkasse
Berichtigung von Diagnosedaten 114
Löschung
Patientendaten 99
Verfassungsschutz 55
Mammografie-Screening 117
Online-Kontaktformular 117
Medizinische Untersuchungsstelle (Regierung) 92
Meldedaten
Beitragsservice 83
Rundfunk 83
Meldedatenübermittlung
Rundfunkfinanzierung 83

Meldung (Datenpanne)
Hackerangriff 19
Mithören
Telefongespräch 158
Namen (Beschäftigte)
Schreiben 149
Nutzertrennung (unzureichende)
Gastzugang 179
Offenlegung
Staatsanwaltschaft 56
Öffentliche Stelle
Aktiengesellschaft 72
Online-Kontaktfomular
Mammografie-Screening 117
Ordnungswidrigkeitenverfahren
Einbindung Arbeitgeber 53
Freiwillige Angaben 52
Ortschronik 64
Paketversand
Datenschutz 169
Parken
Automatisierte Kennzeichenerfassung 70
Kameraparken 70
Patientendaten
Aufbewahrungsfrist 99
Löschung 99
Patientenquittung
Diagnose 112
Patientenzimmer
Videoüberwachung 108
Planfeststellung
Digitalisierung 81
Planungkonzept
Einsicht 161
Polizei
Bodycam 50
Verdeckte Ermittler 47
Vertrauenspersonen 47
Polizeiliche Beobachtung 48
Pressearbeit
Versammlungsbehörde 54
Psychiatrie
Videoüberwachung 108
QR-Code
Schwärzung 177
Ransomware
Klinik 178
Raumordnung
Digitalisierung 81
Rechenschaftspflicht (datenschutzrechtliche)
KI 32
Recht auf Auskunft
CD-ROM 104

Verfassungsschutz 54
Recht auf Auskunft (Art 39 BayDSG)
Personenbezogene Daten 162
Recht auf Berichtigung
Diagnosedaten (Krankenkasse) 114
Recht auf Kopie
CD-ROM 104
Recht auf Löschung
Verfassungsschutz 55
Rechtsnachfolge
Zuordnung von Instituten 95
Rollenmodell (datenschutzrechtliches)
KI 30
Rundfunk
Meldedaten 83
Rundfunkfinanzierung
Meldedatenübermittlung 83
Sammelermächtigungen
Jugendämter 152
Schneckenpost
Datenschutz 169
Schreiben (dienstliche)
Beschäftigtennamen 149
Schulaufsicht
Kommunikation mit Schule 156
Schule
Hausbesuch vom Hausmeister 157
Mithören (Telefongespräch) 158
Schulpflichtverstoß 157
Telefongespräch (Mithören) 158
Werbung (Landheim) 159
Schullandheim
Werbung 159
Schulrecht
Änderungen 2025 155
Schwärzung
QR-Code 177
Überprüfung (Art. 39 BayDSG) 161
Weißung 119
Solarpotenzialkataster 76
Sozialbehörde
Datenanforderung von Ausländerbehörde 131
Spielbank
Auskunftsanspruch 15
Staatsanwaltschaft
Offenlegung 56
Strafakte (Aufbewahrung) 57
Strafakte
Aufbewahrung 57
Staatsanwaltschaft 57
Strafanzeige
Hackerangriff 22
Technisch-organisatorische Maßnahme 22

Streaming (nichtöffentliche Gemeinderatssitzung) 182
Telefongespräch
Mithören 158
Todesmeldung (irrtümliche)
Krankenhaus 183
Transparenz
KI 39
Umgliederung
Universität – Universitätsklinikum 95
Unfallanzeigen 133
Universität
Übergabe Institut 95
Universitätsklinikum
Übernahme Institut 95
Unkenntlichmachen personenbezogener Daten
Weißung 119
Verdeckte Ermittler
Polizei 47
Verfassungsschutz
Auskunft 54
Löschung 55
Recht auf Auskunft 54
Recht auf Löschung 55
Verfassungstreue
Bewerber (öffentlicher Dienst) 144
Versammlungsbehörde
Pressearbeit 54
Vertrauenspersonen (Polizei) 47
Vertrauliche Anfrage
Weiterleitung 156
Verwandtenunterhalt
Verhältnis zur Grundsicherung 124
Videoüberwachung
Krankenhaus 108
Patientenzimmer 108
Psychiatrie 108
Wärmeplanung
Kommunen 58
Wasserbuch
Digitalisierung 79
Webarchive
Datenschutz 165
Weißung
Schwärzung 119