31. Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz

gemäß Art. 59 Datenschutz-Grundverordnung

Berichtszeitraum:	1. Januar 2021 bis 31. Dezember 2021
Veröffentlichungsdatum:	25. Mai 2022

Inhaltsverzeichnis

1 Überblick 10

1.1 Pandemiebekämpfung und Datenschutz 10

1.1.1 Infektionsschutzgesetz und Bayerische Infektionsschutzmaßnahmenverordnungen 10

1.1.2 Kontaktmanagement und Datenminimierung 11

1.1.3 SORMAS 12

1.1.4 Befreiung von der Maskenpflicht 12

1.1.5 Testmanagement 14

1.1.6 Insbesondere: Testungen an Schulen 14

1.1.7 Transparenz der Verarbeitung: Positivbeispiel Impfmanagement 15

1.1.8 Zwischenbilanz 15

1.2 Schlussbemerkung 16

2 Allgemeines Datenschutzrecht 17

2.1 „Datenschutzreform 2018“ – Weiterentwicklung des Informationsangebots des Bayerischen Landesbeauftragten für den Datenschutz 17

2.2 Office-Anwendungen aus Drittstaaten bei bayerischen öffentlichen Stellen 18

2.2.1 Datenschutz-Sicherheitskonzept 19

2.2.2 Übermittlung personenbezogener Daten auf Grundlage von Art. 44 ff. DSGVO 19

2.2.3 Rechenschaftspflicht 23

2.3 Entgeltpflicht für Kontrollen bei der Auftragsverarbeitung? 24

3 Polizei und Verfassungsschutz 27

3.1 Änderung des Polizeiaufgabengesetzes 27

3.2 Zuverlässigkeitsüberprüfungen im Rahmen von Akkreditierungsverfahren 27

3.3 Erkennungsdienstliche Maßnahmen aus Anlass von Ordnungswidrigkeiten 30

3.4 Prüfung erkennungsdienstlicher Maßnahmen aufgrund einer Eingabe 32

3.5 Anlasslose Überprüfung von Speicherungen im Integrationsverfahren der Bayerischen Polizei (IGVP) 33

3.6 Speicherung im Staatsschutz-Informationssystem wegen Teilens eines Medienberichts in einem Sozialen Netzwerk 34

3.7 Prüfung Antiterrordatei (ATD) ... 35

3.8 Prüfung Rechtsextremismus-Datei (RED) ... 35

4 Justiz ... 37

4.1 Beanstandung einer Staatsanwaltschaft wegen unterbliebener Anhörung vor Gewährung einer Akteneinsicht ... 37

4.2 Unzulässige Videobeobachtung eines Untersuchungsgefangenen ... 38

4.3 Nutzung privater Mobiltelefone für erkennungsdienstliche Maßnahmen im Maßregelvollzug ... 40

4.4 Protokollierung von Zugriffen in der Haftdatei IT-Vollzug ... 40

4.5 Dokumentation von Lichtbildanforderungen im Rahmen von Verkehrsordnungswidrigkeitenverfahren ... 41

5 Allgemeine Innere Verwaltung ... 43

5.1 Datenverarbeitung bei Gutachterausschüssen zur Ermittlung von Grundstückswerten und für sonstige Wertermittlungen ... 43

5.1.1 Sachverhalt ... 43

5.1.2 Gutachterausschuss für Grundstückswerte als Verantwortlicher ... 43

5.1.3 Datenschutzrechtliche Konsequenzen ... 44

5.1.4 Behördlicher Datenschutzbeauftragter ... 45

5.1.5 Informationspflichten nach Art. 13 DSGVO ... 45

5.1.6 Auftragsverarbeitung ... 45

5.1.7 Rechtsgrundlagen für die Datenverarbeitung ... 46

5.2 Bürgerversammlungen: Veröffentlichung von Anträgen ... 46

5.3 Bauantragsunterlagen: keine regelhafte Übermittlung durch Gemeinden an Wasserzweckverbände ... 48

5.4 Datenschutz bei der Herausgabe kommunaler Mitteilungsblätter ... 50

5.5 Personenbezogene Angaben auf Parkausweisen für Gewerbetreibende oder selbständige Freiberufler ... 51

5.6 Duldung durch Ausländerbehörde: keine überschießende Datenerhebung ... 52

5.7 Luftsicherheitsassistenten: Datenübermittlungen durch Luftämter an Arbeitgeber nur im Rahmen des Erforderlichen ... 53

5.7.1 Luftsicherheitsassistentinnen und Luftsicherheitsassistenten: beleihende Stelle und Arbeitgeber nicht identisch ... 53

5.7.2 Beschwerdesachverhalt ... 54

5.7.3 Datenschutzrechtliche Bewertung der Übermittlung ... 54

5.7.4 Benennung von Datenschutzbeauftragten erforderlich ... 55

6 E-Government und öffentliche Register 56

6.1 Erneut: Gesetz über die Digitalisierung im Freistaat Bayern 56

6.1.1 Transparente Regelung der Verantwortlichkeiten 56

6.1.2 Entscheidungsmöglichkeiten der Nutzerinnen und Nutzer klargestellt 56

6.1.3 Aber: Verarbeitung von Nutzerdaten nicht an Zustimmung gebunden 57

6.1.4 Ausblick: Verarbeitung von Meldedaten begrenzen 57

6.2 BayernAtlas: gesetzgeberischer Handlungsbedarf 58

6.2.1 Auch Geodaten können personenbezogene Daten sein 59

6.2.1.1 Personenbezogenheit einer Information 59

6.2.1.2 Identifizierbarkeit 60

6.2.2 Erfordernis einer Rechtsgrundlage 60

6.2.2.1 Bloßes Einsichtsrecht nach dem Vermessungs- und Katastergesetz 61

6.2.2.2 Bayerisches Geodateninfrastrukturgesetz gilt nur für betroffene Geodaten und erfordert Abwägung 61

6.2.2.3 Anhörungserfordernis nach dem Bayerischen Umweltinformationsgesetz 62

6.2.3 Ausblick 62

7 Soziales und Gesundheit 63

7.1 Vollzug des Masernschutzgesetzes durch Kindertageseinrichtungen und Gesundheitsämter 63

7.1.1 Rechtsgrundlagen 63

7.1.2 Datenschutzkonforme Vorlage bei der Kindertageseinrichtung – Dokumentation ohne Kopie des Nachweises 64

7.1.3 Meldung an das zuständige Gesundheitsamt 64

7.1.4 Übermittlung einer Kopie des Nachweises nur mit Einwilligung 65

7.1.5 Keine Übermittlung von Listen über vorgelegte Kontraindikationsnachweise 65

7.1.6 Datenverarbeitungsbefugnisse des Gesundheitsamtes 66

7.1.7 Datenschutzkonforme Vorlage und Prüfung des Nachweises beim Gesundheitsamt 66

7.2 Vollzug des Masernschutzgesetzes in Krankenhäusern 66

7.3 Datenschutzrechtliche Anforderungen an Reihentestungen auf den Erreger SARS-CoV-2 in (Rehabilitations- und Pflege-) Einrichtungen 68

7.3.1 Datenerhebung aufgrund einer behördlichen Anordnung oder aufgrund einer datenschutzrechtlichen Einwilligung 69

7.3.2 Übermittlungsbefugnis des Gesundheitsamts auf Ersuchen der Einrichtungsleitung 71

7.3.3 Datenverarbeitung als Annex einer behördlichen Anordnung zu Zwecken von Infektionsschutz und Pandemiebekämpfung 73

7.3.4 Weitere Entwicklung und Ausblick 73

7.4 Datenweitergabe durch Impfzentrum an Arbeitgeber 74

7.4.1 Zugrundeliegender Sachverhalt 74

7.4.2 Stellungnahme des Landratsamtes 74

7.4.3 Datenschutzrechtliche Bewertung der Übermittlung ... 75
7.4.4 Erhebung von Arbeitgeberdaten ... 76

7.5 Impfzentrum: Aufbewahrung von Dokumentationen zur Impfberechtigung ... 78

7.6 Forschungsstudie ohne Einwilligung ... 79

7.7 Übermittlung von Daten zu COVID-19-Infektionsketten an Berufsgenossenschaften ... 80

7.7.1 Gesetzliche Befugnis ... 80
7.7.2 Einwilligung ... 81
7.7.3 Fazit ... 82

7.8 Unterhaltsvorschussleistungen: Datenverarbeitungen durch das Jugendamt und das Landesamt für Finanzen ... 82

7.9 Datenverarbeitung im Zusammenhang mit Kindeswohlgefährdungen ... 84

7.10 Mitteilungspflichten des Medizinischen Dienstes bei Behandlungsfehlerbegutachtungen ... 86

7.10.1 Mitteilungspflicht gegenüber Leistungserbringerinnen und Leistungserbringern ... 86
7.10.2 Mitteilungspflicht gegenüber Versicherten ... 88

7.11 Abfragen beim Ausländerzentralregister im Sozialbereich ... 89

8 Personalverwaltung ... 91

8.1 Verarbeitung des COVID-19-Impfstatus im bayerischen öffentlichen Dienst ... 91

8.2 Regelung zur Aufbewahrung von Beurteilungsunterlagen ... 92
8.2.1 Vorgaben zum Umgang mit dienstlichen Beurteilungen ... 93
8.2.2 Gebot einer umfassenden Regelung ... 93
8.2.3 Neuregelung in Abschnitt 3 Nr. 11.8 VV-BeamtR ... 93
8.2.4 Datenschutzrechtliche Bewertung der neuen Regelung ... 94
8.2.4.1 Grundsätzliches (Sätze 1 bis 3) ... 94
8.2.4.2 Allgemeine Vorgaben zu Aufbewahrung und Vernichtung (Satz 4) ... 94
8.2.4.3 Entwürfe, vorbereitende Übersichten und „andere im Entstehungsprozess befindliche Unterlagen“ (Satz 5) ... 95
8.2.4.4 Aufbewahrung „sonstiger“ Unterlagen (Satz 6) ... 95
8.2.4.5 Sonstige Unterlagen zur aktuellen dienstlichen Beurteilung (Satz 7) ... 96
8.2.4.6 Sonstige Unterlagen zu Vorbeurteilungen (Satz 8) ... 96
8.2.4.7 Aufbewahrungsort (Sätze 9 bis 10) ... 97
8.2.4.8 Maßnahmen zur rechtzeitigen Vernichtung (Satz 11) ... 98
8.2.5 Abschließende Bemerkungen ... 98

8.3 Verlängerung der Aufbewahrungsfrist für Beihilfeunterlagen ... 99
8.3.1 Sensibilität von Beihilfeunterlagen ... 99
8.3.2 Das spezifische datenschutzrechtliche „Beihilferisiko“ ... 99

8.3.3 Die Aufbewahrung von Beihilfeunterlagen nach alter und neuer Rechtslage ... 100
8.3.4 Fazit ... 102

8.4 Zugriff auf Zeiterfassungsdaten ... 102

8.5 Amtsärztliche Arbeitsfähigkeitsuntersuchungen bei Tarifbeschäftigten ... 105

8.5.1 Ausgangspunkt ... 105
8.5.2 Mitteilung der Untersuchungsergebnisse an den Arbeitgeber ... 106
8.5.2.1 Rechtsgrundlage ... 106
8.5.2.2 Mitteilungsumfang ... 107
8.5.3 Fazit ... 108

8.6 Bewerbungsunterlagen im Ratsinformationssystem ... 108

8.7 Kontodatenabgleich bei örtlicher Rechnungsprüfung ... 110

8.8 Gleichstellungsbeauftragte: Einsicht in Bewerbungsunterlagen und Teilnahme an Vorstellungsgesprächen ... 111

8.8.1 Einsichtsrecht in Bewerbungsunterlagen ... 112
8.8.2 Teilnahme an Vorstellungsgesprächen ... 114
8.8.3 Fazit ... 114

9 Schulen und Hochschulen ... 115

9.1 Datenschutz bei den SARS-CoV-2 Testungen in Schulen ... 115

9.1.1 SARS-CoV-2-Selbsttestungen in Schulen ... 115
9.1.1.1 Rechtsgrundlage zur Datenverarbeitung ... 115
9.1.1.2 Speicherung der Testergebnisse der Selbsttests ... 116
9.1.1.3 Alternative: externe PCR- oder PoC-Antigentests ... 117
9.1.2 PCR-Pooltests an Grund- und Förderschulen ... 117
9.1.2.1 Testverfahren ... 117
9.1.2.2 Wissenschaftliche Begleitstudie ... 118
9.1.2.3 Rechtsgrundlage zur Datenverarbeitung ... 118
9.1.3 Verarbeitung des Impf- oder Genesenenstatus ... 119
9.1.3.1 Status befreit von der Testobliegenheit ... 119
9.1.3.2 Rechtsgrundlage zur Datenverarbeitung ... 119
9.1.3.3 Freiwillige Offenbarung des Impf- oder Genesenenstatus ... 119

9.2 Elektronische Fernprüfungen und alternative Präsenzprüfungen bei Hochschulen ... 120

9.2.1 Sachverhalt ... 120
9.2.2 Rechtliche Bewertung ... 121
9.2.2.1 § 4 Abs. 1 Satz 1 BayFEV ... 121
9.2.2.2 Studienordnung ... 122
9.2.2.3 Einwilligung ... 122
9.2.2.4 Fortgang ... 123

10 Technik und Organisation ... 124

10.1 COVID-19-Pandemie, Digitalisierung und Datenschutz ... 124

10.2 IT-Systeme zur Bewältigung der COVID-19-Pandemie ... 126

10.2.1 SORMAS ... 127

10.2.2 BayIMCO: Software für das Bayerische Impfmanagement ... 129

10.2.3 Beschwerden zu technischen Belangen des Bayerischen Impfmanagements ... 130

10.2.3.1 Vermeintliches Hosting in einem unsicheren Drittstaat ... 130

10.2.3.2 Einwilligung zur Weitergabe von Daten an Forschungsstellen ... 130

10.2.4 Digitales Kontaktnachverfolgungssystem Luca ... 131

10.3 Elektronische Kommunikation im Rahmen des COVID19-Pandemiemanagements mit Bürgerinnen und Bürgern ... 132

10.3.1 Kommunikationsmöglichkeiten ... 133

10.3.2 Beschwerden ... 134

10.4 Social Engineering – eine nicht zu unterschätzende Gefahr ... 135

10.5 Einführung einer Ersthelfer-App ... 137

10.6 Beschäftigtendatenschutz bei der Ablage von E-Mails ... 138

10.7 Beanstandung nach dem Verlust von Bewerbungsunterlagen ... 140

10.8 Verweigerte Kfz-Ummeldung wegen Personenverwechslung ... 141

10.9 Meldungen von Verletzungen des Schutzes von personenbezogen Daten ... 142

10.10 Exchange-Sicherheitslücke ... 143

11 Datenschutzkommission ... 145

12 Ländervertreter im EDSA ... 147

13 Anhang ... 149

Abkürzungsverzeichnis ... 163

Stichwortverzeichnis ... 164

Hinweis zu Abkürzungen

Abkürzungen von Rechtstexten sind im jeweiligen Abschnitt 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), geändert durch § 6 Gesetz vom 18. Mai 2018 (GVBl. S. 301)
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, und ABl. L 127 vom 23. Mai 2018, S. 2)
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)

1 Überblick

1.1 Pandemiebekämpfung und Datenschutz

Auch im Jahr 2021 war die Pandemiebekämpfung mit erheblichen Belastungen der Menschen in Bayern verbunden.

Zu Beginn des Jahres 2021 etwa waren die bayerischen Schulen schlichtweg geschlossen; der Unterricht wurde zumeist mithilfe von Videokonferenzen und mebis organisiert. Für die Schülerinnen und Schüler bedeutete dies den zwangsläufigen Verzicht auf den Kontakt mit Gleichaltrigen – und gestresste Eltern, die oft auf beengtem Raum selbst im Homeoffice arbeiten mussten. Im Frühjahr kehrte man zwar allmählich zum Präsenzunterricht zurück, unbeschwert war dies gleichwohl nicht: Während des Präsenzunterrichts hatten die Schülerinnen und Schüler regelmäßig Masken zu tragen. Zudem mussten immer wieder ganze Klassen in Quarantäne geschickt werden. Im Frühjahr wurden regelmäßige Reihenselbsttests an Schulen, im Sommer auch für noch nicht eingeschulte Kinder eingeführt.

Der Besuch von Krankenhäusern, Heimen, Sporteinrichtungen, Freizeiteinrichtungen, personennahen Dienstleistungsbetrieben oder der Gastronomie wurde, soweit überhaupt möglich, an negative Testnachweise geknüpft und zudem von einer Kontaktdatenerfassung abhängig gemacht. Selbst- und Fremdschutz verhießen im Laufe des Jahres die Impfungen, an sie knüpften die Gesetzgeber in Bund und Ländern zudem ab dem Herbst gewisse Erleichterungen. Freilich wurden diese Erleichterungen auch an die Offenbarung des Impf- oder Teststatus geknüpft.

So notwendig diese beispielhaft genannten Maßnahmen zur Pandemiebekämpfung gewesen sein mögen: Sie schränkten grundrechtliche Freiheiten – darunter auch das Datenschutzgrundrecht – oft ganz erheblich ein. Dementsprechend führten sie bei mir zu zahlreichen Beschwerden von Bürgerinnen und Bürgern. Zugleich wandten sich Behörden mit Beratungsanfragen an mich, um eine datenschutzkonforme Ausgestaltung der Maßnahmen sicherzustellen. Diese Eingaben und Anfragen führten zu einem erheblichen Anstieg des Arbeitsaufkommens, obwohl ich im Jahr 2021 aus Gründen der Kontaktvermeidung weitgehend auf Vor-Ort-Kontrollen verzichten musste.

Im nachfolgenden Überblick werde ich auf einige datenschutzrechtlich bedeutsame Fragen zum Kontaktmanagement, zur Maskenpflicht, zum Test- und zum Impfmanagement in Bayern eingehen. Die Einzelheiten werden in den nachfolgenden Kapiteln des Tätigkeitsberichts näher beleuchtet.

1.1.1 Infektionsschutzgesetz und Bayerische Infektionsschutzmaßnahmenverordnungen

Die Regelungen zur Pandemiebekämpfung in ihrer Gesamtheit waren (und sind) komplex, zudem unterlagen sie auch im Jahr 2021 einem kontinuierlichen Wandel. Neben zahlreichen Spezialregelungen bildeten das Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen (Infektionsschutzgesetz –

IfSG)[1], und im Freistaat die Bayerischen Infektionsschutzmaßnahmenverordnungen (BayIfSMV) den rechtlichen Rahmen. Diese Regelungen bestimmten maßgeblich auch über die Zulässigkeit der Verarbeitung personenbezogener Daten im Zusammenhang mit der Bekämpfung der COVID-19-Pandemie.

Das Zusammenspiel von bundesgesetzlichen und landesrechtlichen Bestimmungen zur Pandemiebekämpfung kann vor allem am Beispiel des § 28a IfSG veranschaulicht werden, der einen Katalog besonderer Schutzmaßnahmen zur Verhinderung einer Ausbreitung von COVID-19 vorsieht. Die meisten dieser Schutzmaßnahmen setzten nicht zuletzt aufgrund ihrer Eingriffsintensität voraus, dass der Deutsche Bundestag zuvor eine „epidemische Lage von nationaler Tragweite" festgestellt hatte. Der Deutsche Bundestag traf die in § 5 Abs. 1 Satz 1 IfSG vorgesehene Feststellung einer solchen Lage mit Blick auf COVID-19 erstmals am 25. März 2020[2] und verlängerte diese Feststellung dann mehrmals. Für die Dauer der epidemischen Lage von nationaler Tragweite konnten die Länder nach § 32 in Verbindung mit § 28 Abs. 1 und § 28a Abs. 1 IfSG Rechtsverordnungen erlassen, die besondere Schutzmaßnahmen zur Verhinderung der Verbreitung von COVID-19 anordnen. Hiervon hat die Bayerische Staatsregierung Gebrauch gemacht. Im Berichtszeitraum wurden die 11., 12., 13., 14. und die 15. BayIfSMV erlassen und damit auch für die datenschutzrechtliche Beurteilung zahlreicher personenbezogener Datenverarbeitungsvorgänge relevant.

1.1.2 Kontaktmanagement und Datenminimierung

Zu Beginn der Pandemie standen bekanntlich weder Impfstoffe noch hinreichende Ressourcen für Testungen zur Verfügung. In dieser Zeit kam dem Kontaktmanagement eine besondere Rolle zu, die es weit in das Jahr 2021 hinein behielt. Zur Problematik der Kontaktdatenerfassung im Allgemeinen und zum polizeilichen Zugriff auf solche Kontaktdaten habe ich bereits im 30. Tätigkeitsbericht Stellung genommen (dort Nr. 1.1.1, 1.1.2).

Im Berichtszeitraum rückten nunmehr elektronische Hilfsmittel zum Kontaktmanagement stärker in den Vordergrund. Um die Kontaktnachverfolgung effektiver zu gestalten, beschaffte der Freistaat Bayern im Frühjahr 2021 eine Landeslizenz für die sog. Luca-App. Im Unterschied zur Corona-Warn-App (siehe dazu bereits mein 30. Tätigkeitsbericht, Nr. 1.1.3) sollte die von privater Hand entwickelte Luca-App die Kontaktverfolgung elektronisch, medienbruchfrei und insbesondere für die Gesundheitsämter leichter zugänglich durchführen. Es stellte sich allerdings bald nach ihren ersten Einsätzen heraus, dass die Luca-App erhebliche Datenschutzfragen aufwarf. Auf diese Fragen machte auch die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder wiederholt aufmerksam, zuletzt am 29. April 2021 und am 21. Mai 2021.[3]

1 Vom 20. Juli 2000 (BGBl. I S. 1045), im Berichtszeitraum zuletzt geändert durch Gesetz vom 10. Dezember 2021 (BGBl. I S. 5162).

2 Plenarprotokoll 19/154, 19169C.

3 Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Stellungnahme zu Kontaktnachverfolgungssystemen – insbesondere zu „Luca" der culture4life GmbH vom 29. April 2021, Internet: https://www.datenschutzkonferenz-online.de/media/st/20210429_DSK_Stellungnahme_LUCA.pdf; Stellungnahme zur Verantwortlichkeit bei der Nutzung von Kontaktnachverfolgungssystemen wie der Luca App vom 21. Mai 2021, Internet: https://www.datenschutzkonferenz-online.de/media/st/DSK-Stellungnahme_Luca_Verantwortlichkeit.pdf.

Zu technisch-organisatorischen Fragen im Zusammenhang mit dem Einsatz der Luca-App durch bayerische öffentliche Stellen sei auf Abschnitt Nr. 10.2.4 verwiesen.

Gegen Ende des Jahres zeigte sich zudem, dass die Luca-App den Erwartungen nicht gerecht werden konnte. Insbesondere gelang es nicht im erhofften Umfang, die Gesundheitsämter bei einer effektiven Nachverfolgung von Kontakten zu unterstützen. Mitunter mussten sich Gesundheitsämter auch mit unzutreffenden Kontaktangaben auseinandersetzen. Die datenschutzfreundlichere Corona-Warn-App (CWA) konnte die Gesundheitsämter jedenfalls bei hohen Infektionszahlen besser entlasten. Sie meldet die von ihr als kritisch identifizierten Kontakte nicht an die Gesundheitsämter, sondern ohne Personenbezug an die potentiell betroffenen Nutzerinnen und Nutzer der App.

1.1.3 SORMAS

Um die Bearbeitung von COVID-19-Kontaktfällen in den Gesundheitsämtern zu unterstützen und zu vereinheitlichen, wurde im November 2020 von Bund und Ländern der bundesweite Einsatz des elektronischen Verfahrens SORMAS (Surveillance Outbreak Response Management Analysis System) beschlossen. Ich habe die Einführung von SORMAS in Hinblick auf die bayerischen Gesundheitsämter begleitet. Die Implementierung verlief auch aus Datenschutzsicht nicht ohne Schwierigkeiten (vgl. Nr. 10.2.1).

1.1.4 Befreiung von der Maskenpflicht

Zu datenschutzrechtlichen Fragen im Zusammenhang mit einer Befreiung von der Maskenpflicht habe ich mich bereits in meinem 30. Tätigkeitsbericht 2020 unter Nr. 1.1.4 geäußert. Die Verpflichtung zum Tragen einer Mund-Nasen-Bedeckung war auch im Berichtszeitraum ein zentraler Baustein zur Eindämmung von COVID-19. In dem vom Bundesgesetzgeber festgelegten Katalog von Schutzmaßnahmen (§ 28a Abs. 1 IfSG) hat die Maskenpflicht als bewährtes Mittel einen festen Platz.

Ausnahmen von der Pflicht zum Tragen einer Maske sind insbesondere für Personen vorgesehen, denen die Verwendung wegen einer Behinderung oder aus gesundheitlichen Gründen nicht zumutbar ist. Auch im Hinblick auf die nachfolgende Darstellung der Rechtsentwicklung im Jahr 2021 möchte ich ausdrücklich klarstellen, dass ich das beschriebene Regel-Ausnahme-Verhältnis unter den Gesichtspunkten einer effektiven Pandemiebekämpfung nachvollziehen konnte und unterstützte.

Der frühen Rechtsprechung zufolge[4] erforderte die Glaubhaftmachung einer Ausnahmesituation regelmäßig die Vorlage eines aussagekräftigen Attests. Diese ärztliche Bescheinigung sollte demzufolge nachvollziehbar und detailliert unter Angabe der Diagnose die daraus resultierenden Beeinträchtigungen beschreiben, die das Tragen der Mund-Nasen-Bedeckung unzumutbar machen. Diese Anforderung floss in den Wortlaut des § 1 Abs. 2 Nr. 2 11. BayIfSMV[5] ein:

„(2) Soweit in dieser Verordnung die Verpflichtung vorgesehen ist, eine Mund-Nasen-Bedeckung zu tragen (Maskenpflicht), gilt:

[4] Vgl. etwa Bayerischer Verwaltungsgerichtshof, Beschluss vom 8. September 2020, 20 NE 20.1999, BeckRS 2020, 21902.

[5] Vom 15. Dezember 2020 (BayMBl. Nr. 737).

1. Kinder sind bis zum sechsten Geburtstag von der Tragepflicht befreit.
2. Personen, die glaubhaft machen können, dass ihnen das Tragen einer Mund-Nasen-Bedeckung aufgrund einer Behinderung oder aus gesundheitlichen Gründen nicht möglich oder unzumutbar ist, sind von der Trageverpflichtung befreit; die Glaubhaftmachung erfolgt bei gesundheitlichen Gründen insbesondere durch eine ärztliche Bescheinigung, die die fachlich-medizinische Beurteilung des Krankheitsbildes (Diagnose), den lateinischen Namen oder die Klassifizierung der Erkrankung nach ICD 10 sowie den Grund, warum sich hieraus eine Befreiung der Tragepflicht ergibt, enthält.
3. Das Abnehmen der Mund-Nasen-Bedeckung ist zulässig, solange es zu Identifikationszwecken oder zur Kommunikation mit Menschen mit Hörbehinderung oder aus sonstigen zwingenden Gründen erforderlich ist."

Die von § 1 Abs. 2 Nr. 2 11. BayIfSMV geforderte Glaubhaftmachung durch ein „sprechendes Attest" mit Beschreibung der Diagnose und der daraus resultierenden Beschwerden beim Maskentragen mag zwar im Allgemeinen dem Grundsatz der Verhältnismäßigkeit genügen, kann aber jedenfalls in Einzelfällen zu schwerwiegenden Beeinträchtigungen der Intimsphäre und damit zur unzumutbaren Offenbarung hochsensibler Daten führen. Auf diesen Umstand habe ich die Staatsregierung gemeinsam mit dem Präsidenten des Bayerischen Landesamts für Datenschutzaufsicht und dem Beauftragten für die Belange von Menschen mit Behinderung hingewiesen. Erfreulicherweise hat die Staatsregierung diese Bedenken aufgegriffen und die Anforderungen für die Befreiung von der Maskenpflicht in § 3 Abs. 1 Nr. 3 13. BayIfSMV[6] geändert. Die seitdem fortgeführte Bestimmung verpflichtet Ärztinnen und Ärzte weiterhin zu aussagekräftigen Attesten. Hochsensible Diagnosen müssen darin aber nicht mehr offenbart werden:

„(1) Soweit in dieser Verordnung Maskenpflicht vorgesehen ist, gilt:
1. Es ist eine medizinische Gesichtsmaske oder eine Mund-Nasen-Bedeckung (Maske) zu tragen.
2. Kinder sind bis zum sechsten Geburtstag von der Tragepflicht befreit.
3. Personen, die glaubhaft machen können, dass ihnen das Tragen einer Maske aufgrund einer Behinderung oder aus gesundheitlichen Gründen nicht möglich oder unzumutbar ist, sind von der Maskenpflicht befreit, solange dies vor Ort sofort insbesondere durch Vorlage eines schriftlichen ärztlichen Zeugnisses im Original nachgewiesen werden kann, das den vollständigen Namen, das Geburtsdatum und konkrete Angaben darüber enthalten muss, warum die betroffene Person von der Tragepflicht befreit ist.
4. Die Maske darf abgenommen werden, solange es zu Identifikationszwecken oder zur Kommunikation mit Menschen mit Hörbehinderung oder aus sonstigen zwingenden Gründen erforderlich ist.
5. Für Beschäftigte gilt die Verpflichtung während ihrer dienstlichen Tätigkeiten nur im Rahmen der arbeitsschutzrechtlichen Bestimmungen."

Über die veränderte Rechtslage informiert eine Gemeinsame Aktuelle Kurzinformation, die ich zusammen mit dem Bayerischen Landesamt für Datenschutzaufsicht herausgegeben habe.[7] Insbesondere haben wir darauf hingewiesen, dass der Verant-

6 Vom 5. Juni 2021 (BayMBl. Nr. 384).

7 Bayerischer Landesbeauftragter für den Datenschutz/Bayerisches Landesamt für Datenschutzaufsicht, Befreiung von der Maskenpflicht aus gesundheitlichen Gründen, Gemeinsame Aktuelle Kurz-Information 1, Stand 11/2021, Internet: https://www.datenschutz-bayern.de/datenschutzreform2018/gaki01.html.

wortliche die Kenntnisnahme der erhobenen Informationen durch Unbefugte zuverlässig zu verhindern hat. Eine Dokumentation der ärztlich attestierten Befreiung von der Maskenpflicht durch Kontrollberechtigte ist grundsätzlich nicht geboten. Sofern sie im Einzelfall vorgeschrieben ist, darf die Tatsache der Befreiung, der ausstellende Arzt sowie gegebenenfalls der Gültigkeitszeitraum des Attests in die zu führenden Unterlagen aufgenommen werden. Eine Kopie des ärztlichen Zeugnisses ist unzulässig. Sobald sie für Nachweiszwecke nicht mehr erheblich sind, sind die erfassten Daten umgehend zu vernichten oder zu löschen (zur Veröffentlichung siehe auch Nr. 2.1).

1.1.5 Testmanagement

Neben der Maskenpflicht sollen auch Testungen maßgeblich zur Eindämmung der Verbreitung von COVID-19 beitragen. Auch wenn insbesondere Schnelltests weniger ergebnissicher als PCR-Tests sind, kann so zumindest ein beträchtlicher Teil infizierter und damit in der Regel auch infektiöser Personen festgestellt werden. Aus Sicht des Verordnungsgebers leisten Schnelltests im Rahmen eines Gesamtkonzepts zur Pandemiebekämpfung einen unverzichtbaren Beitrag. Als Datenschutz-Aufsichtsbehörde habe ich diese fachliche Bewertung respektiert. Dieser Umstand ändert freilich nichts daran, dass die Verantwortlichen zentrale Datenschutzgrundsätze wie die der Datenminimierung, Zweckbindung und der Vertraulichkeit zu wahren haben (zum Problem der Datenübermittlung siehe etwa Nr. 7.3.2 und Nr. 7.7).

Auch möchte ich im Zusammenhang mit der Teststrategie der Staatsregierung auch auf eine Entschließung der Datenschutzkonferenz hinweisen, welche die Beachtung des Grundsatzes der Rechtmäßigkeit im Zusammenhang mit der Verarbeitung des Nachweises negativer Testergebnisse in Beschäftigungsverhältnissen angemahnt hat.[8]

Nicht zuletzt weise ich an dieser Stelle auch auf die anlassbezogene Reihentestung in einer Rehabilitations- und Pflegeeinrichtung hin (Nr. 7.3).

1.1.6 Insbesondere: Testungen an Schulen

Zahlreiche Beschwerden im Zusammenhang mit der Teststrategie der Staatsregierung betrafen die Testungen an den bayerischen öffentlichen Schulen. Dort kamen regelmäßig Corona-Selbsttests zum Einsatz. Diese Tests führen Schülerinnen und Schüler unter Aufsicht einer Lehrkraft durch.

In Beschwerden bei mir machten Erziehungsberechtigte geltend, durch die Selbsttestung an Schulen werde nicht nur die selbstbestimmte Entwicklung ihrer Kinder gefährdet, sondern auch das informationelle Selbstbestimmungsrecht beeinträchtigt: Bei einem Test „vor aller Augen“ würden positive Ergebnisse sogleich im Klassenverband bekannt; daran könnten soziale Repressionen anknüpfen. Das sei bei einem Test zuhause nicht der Fall.

[8] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Coronavirus: Impfnachweis, Nachweis negativen Testergebnisses und Genesungsnachweis in der Privatwirtschaft und im Beschäftigungsverhältnis gehören gesetzlich geregelt!, Entschließung vom 29. März 2021, Internet: https://www.datenschutzkonferenz-online.de/media/en/20210331_entschliessung_impfdatenverarbeitung.pdf.

Die vorgebrachten Datenschutzbedenken konnte ich zwar grundsätzlich nachvollziehen. Gleichwohl erwies sich die fragliche Datenverarbeitung nicht als unzulässig. Nach meinem Dafürhalten hat der Verordnungsgeber insoweit nachvollziehbar angenommen, dass die häusliche Testung gegenüber der Testung an der Schule kein gleich effektives Mittel darstellt. Eine ordnungsgemäße Testung in häuslicher Umgebung konnte durch die Schule nicht gewährleistet werden. In dieser Einschätzung sah ich mich im Ergebnis durch mehrere Entscheidungen des Bayerischen Verwaltungsgerichtshofs[9] bestätigt (siehe Nr. 9.1).

1.1.7 Transparenz der Verarbeitung: Positivbeispiel Impfmanagement

Der zentrale Baustein der Pandemiebekämpfung dürfte im Laufe des Jahres 2021 die Impfstrategie der Staatsregierung gewesen sein. Dementsprechend bildeten die technischen und organisatorischen Maßnahmen rund um das Bayerische Impfmanagement einen Schwerpunkt meiner aufsichtsbehördlichen Tätigkeit. Für die einzurichtenden Impfzentren in Bayern strebte das Bayerische Staatsministerium für Gesundheit und Pflege die Entwicklung einer einheitlichen bayerischen Softwarelösung für die elektronische Impfanmeldung und die Impfverwaltung (BayIMCO) an. Diese Software sollte die einheitliche Klärung der Impfberechtigung, die Erfassung des jeweiligen Impfstatus und eine für die Durchführung von Impfungen erforderliche Kommunikation mit Bürgerinnen und Bürger unterstützen. Dabei band mich das Gesundheitsministerium frühzeitig in die rechtliche wie auch technisch-organisatorische Beurteilung ein. Zudem legte es eine ausführliche Datenschutz-Folgenabschätzung vor und erstellte zudem ausführliche Datenschutzinformationen für die Bürgerinnen und Bürger; auch diese Informationen lagen mir rechtzeitig zur Prüfung vor (siehe Nr. 10.2.2).

1.1.8 Zwischenbilanz

Die vorangegangene Darstellung datenschutzrechtlicher Herausforderungen hat einen repräsentativen Ausschnitt von Verarbeitungsvorgängen aus dem Kontext der Pandemiebekämpfung in den Blick genommen. Die verstärkte Nutzung von Office-Anwendungen aus Drittländern (Nr. 2.2) oder die Durchführung elektronischer Fernprüfungen an Hochschulen (Nr. 9.2) sind Datenschutzthemen, die zwar nicht die Bekämpfung der COVID-19-Pandemie betreffen, jedoch in ihrem Verlauf unerwartet in den Mittelpunkt des Interesses gerückt sind.

Insgesamt unterstreichen meine aufsichtsbehördlichen Kontrollen, dass die verständige Beachtung der zentralen Datenschutzgrundsätze die zuständigen öffentlichen Stellen bei der Pandemiebekämpfung oft nicht behinderte, sondern bei ihrer Aufgabenerfüllung unterstützte. Das gilt namentlich für den Grundsatz der Datenminimierung, der letztlich eine Ausprägung des Erforderlichkeitsprinzips ist und vor überschießender Verarbeitung bewahrt (siehe etwa Nr. 1.1.2). Die öffentlichen Stellen sind auch gut beraten, den Grundsatz der Transparenz zu beachten, der maßgeblich zur Akzeptanz ihrer Maßnahmen beiträgt (zum Positivbeispiel BayIMCO siehe Nr. 1.1.7, Nr. 10.2.2).

[9] Vgl. etwa Bayerischer Verwaltungsgerichtshof, Beschluss vom 12. Oktober 2021, 25 NE 21.2471, BeckRS 2021, 33613, Rn. 19; Beschluss vom 28. September 2021, 25 NE 21.2372, BeckRS 2021, 30952, Rn. 51.

1.2 Schlussbemerkung

Die nachfolgenden Beiträge geben einen Überblick zu meiner Tätigkeit im Jahr 2021. Sie zeigen, dass ich auch außerhalb des Themenkreises „Datenschutz in der COVID-19-Pandemie“ zahlreiche Gesetzgebungsverfahren begleiten konnte. Das Aufkommen an behördlichen Beratungsanfragen, an Beschwerden wie auch an Meldungen von Datensicherheitsverletzungen ist unvermindert hoch, sodass ich insofern auch für diesen Berichtszeitraum nur eine kleine Zahl von Fällen auswählen konnte. Ich hoffe, dass meine Hinweise die bayerischen öffentlichen Stellen bei der Wahrnehmung ihrer datenschutzrechtlichen Verantwortung nachhaltig unterstützen.

2 Allgemeines Datenschutzrecht

2.1 „Datenschutzreform 2018“ – Weiterentwicklung des Informationsangebots des Bayerischen Landesbeauftragten für den Datenschutz

Verantwortliche können einen den rechtlichen, technischen und organisatorischen Standards entsprechenden Datenschutz nur sicherstellen, wenn sie auch über das dafür erforderliche Wissen verfügen. Vor diesem Hintergrund lege ich besonderen Wert auf ein differenziertes Angebot an **Orientierungshilfen, Arbeitspapieren, Aktuellen Kurz-Informationen** sowie sonstigen Materialien. Dieses Angebot habe ich auch im Berichtszeitraum gepflegt und weiter ausgebaut. Es steht auf meiner Internetpräsenz https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018“ zum kostenfreien Abruf bereit.

Im Berichtszeitraum habe ich zwei umfangreiche Orientierungshilfen zu zentralen Fragen des Datenschutzrechts veröffentlicht. Die meinem Aufgabenkreis entsprechend an bayerische öffentliche Stellen adressierten Papiere haben erfreulicherweise Resonanz auch im nichtöffentlichen Bereich sowie außerhalb Bayerns erfahren.

— Die Orientierungshilfe **„Die Einwilligung nach der Datenschutz-Grundverordnung“** behandelt systematisch eine wesentliche Rechtsgrundlage für die Verarbeitung personenbezogener Daten (vgl. Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO). Sie geht insbesondere auf die Frage ein, wann Staatsbehörden und Kommunen dieses Instrument einsetzen dürfen. Detailliert erläutert werden die Voraussetzungen für eine wirksame Einwilligung. Themen sind ferner Widerruf und Aufbewahrung, auch die Fortgeltung früherer Einwilligungen. Eine Checkliste für die praktische Anwendung schließt die Orientierungshilfe ab.

— Mit der Orientierungshilfe **„Bayerische öffentliche Stellen und Telemedien“** habe ich diesen Verantwortlichen bereits alsbald nach Inkrafttreten des Telekommunikation-Telemedien-Datenschutz-Gesetzes eingehende Erläuterungen zum neuen Recht zur Verfügung gestellt. Einen Schwerpunkt bilden die Regelungen zu Cookies, insbesondere was das Bedürfnis nach und die Anforderungen an Einwilligungen sowie das Verhältnis der einschlägigen Vorgaben zum allgemeinen Datenschutzrecht betrifft. Prüfraster zum Einsatz und zur Ausgestaltung von Einwilligungsbannern sowie Listen zur Abgrenzung einwilligungspflichtiger und nicht einwilligungspflichtiger Cookies zielen auf weiteren Praxisnutzen.

Im Verlauf des Berichtszeitraums habe ich zudem mehrere **Arbeitspapiere** herausgebracht. Das Arbeitspapier **„Der Sozialdatenschutz unter Geltung der Datenschutz-Grundverordnung (DSGVO)“** stellt ein bereichsspezifisches Datenschutzrecht vor. Wie das Arbeitspapier **„Datenschutz bei kommunalen Mitteilungsblättern“** (siehe Beitrag Nr. 5.4) zeigt, sind die rechtlichen Vorgaben auch bei scheinbar randseitigen Themen mitunter nicht unkompliziert. Hier habe ich den bayerischen Kommunen auch Formulare zur Verfügung gestellt, die dabei helfen sollen, die vorgestellten „Fettnäpfchen“ möglichst zu umgehen. Großer Nachfrage erfreut sich schließlich das Arbeitspapier **„Verarbeitung des COVID-19-Impfstatus im bayeri-**

schen öffentlichen Dienst“ (siehe Beitrag Nr. 8.1), das einschlägige Rechtsgrundlagen aufzeigt und zueinander in Beziehung setzt und bereits in einer überarbeiteten Version vorliegt.

Unter den bewährten **Aktuellen Kurz-Informationen** erschien im Berichtszeitraum erstmals ein vom Bayerischen Landesamt für Datenschutzaufsicht und mir gemeinsam getragenes Papier. Die **Gemeinsame Aktuelle Kurz-Information 1 „Befreiung von der Maskenpflicht aus gesundheitlichen Gründen“** befasst sich aus Datenschutzsicht insbesondere mit der Gestaltung von Befreiungsattesten, der Berechtigung, solche Atteste einzusehen, sowie der Dokumentation entsprechender Kontrollen. Ich würde mich freuen, wenn dem Papier weitere Gemeinsame Aktuelle Kurz-Informationen folgen könnten.

In alleiniger Verantwortung habe ich die **Aktuellen Kurz-Informationen 35 bis 40** publiziert; auch auf Grund der kontinuierlich hohen Nachfrage auf meiner Internetpräsenz möchte ich den Beitrag zur „3G-Zutrittsregel im bayerischen öffentlichen Dienst“ besonders hervorheben (siehe Beitrag Nr. 8.1).

Meine Veröffentlichungen im Zusammenhang mit der COVID-19-Pandemie passe ich immer wieder aufs Neue dem sich rasch ändernden rechtlichen Rahmen an. Einige bereits im Jahr 2018 bereitgestellte Papiere habe ich im Berichtszeitraum aktualisiert und teils grundlegend überarbeitet.

Bayerische öffentliche Stellen, ihre Datenschutzbeauftragten wie auch alle anderen am Datenschutz Interessierten haben die Möglichkeit, sich per **RSS-Feed** über Neuigkeiten auf meinen Internetseiten informieren zu lassen. Dieses Angebot ist eine datenschutzfreundliche Alternative zu einem Newsletter, weil es ohne eine Sammlung von Kontaktdaten auskommt. Für jede neue Publikation wird ein Hinweis mit einer kurzen Inhaltsangabe gepostet. Die Einbindung von RSS-Feeds in einen E-Mail-Client ist in der Regel nicht schwierig. Hinweise dazu sind auf https://www.datenschutz-bayern.de unter „RSS“ zu finden.

Auch für das **Jahr 2022** sind wieder mehrere neue Orientierungshilfen und Arbeitspapiere geplant. Die Reihe „Aktuelle Kurz-Informationen“ wird ebenfalls fortgesetzt.

2.2 Office-Anwendungen aus Drittstaaten bei bayerischen öffentlichen Stellen

Gegenwärtig bestehen bei zahlreichen bayerischen öffentlichen Stellen (Verantwortliche) Unsicherheiten, was den Einsatz von Office-Anwendungen aus dem Nicht-EU-Ausland, insbesondere den Vereinigten Staaten von Amerika (USA), betrifft. Den Bayerischen Landesbeauftragten für den Datenschutz haben insoweit zahlreiche Anfragen vor allem aus dem Bereich der bayerischen öffentlichen Schulen erreicht. Die Nutzung solcher Produkte bringt oftmals eine Übermittlung personenbezogener Daten in ein Drittland mit sich; Übermittlungen dieser Art sind seit Geltungsbeginn der Datenschutz-Grundverordnung allerdings strikt reglementiert (siehe im Einzelnen Art. 44 DSGVO).

Der Beitrag erläutert nach einem Hinweis zum Datenschutz-Sicherheitskonzept zunächst die aktuell bestehenden rechtlichen Rahmenbedingungen für eine Übermittlung personenbezogener Daten in ein Drittland auf Grundlage der Art. 44 ff. DSGVO. Sie zeigt ferner auf, welche Anforderungen an die Rechenschaftspflicht des Verantwortlichen zu stellen sind.

Verantwortliche sollten berücksichtigen, dass sich die Rechtsprechung und die Positionen der Datenschutz-Aufsichtsbehörden zu Fragen der Art. 44 ff. DSGVO zügig fortentwickeln. Daher sollte stets auf neue Entscheidungen und Veröffentlichungen geachtet werden.

2.2.1 Datenschutz-Sicherheitskonzept

Als eine **vorbereitende Maßnahme** sollte der Verantwortliche, der eine **Office-Anwendung aus einem Drittland** einsetzen möchte, stets ein **Datenschutz-Sicherheitskonzept** erstellen. Es sollte insbesondere auf die folgenden Fragen eingehen:

— Welches **Produkt** soll in welcher **IT-Umgebung** eingesetzt werden?

— Welche **Kategorien personenbezogener** Daten sollen mithilfe des Produkts verarbeitet werden?

— Welche **nachteiligen Folgen** können sich daraus für die Vertraulichkeit, Verfügbarkeit und Integrität von personenbezogenen Daten ergeben? Wie sind diese Folgen und deren Eintrittswahrscheinlichkeiten zu **bewerten** und mit welchen Maßnahmen ist ihnen gegebenenfalls zu **begegnen**? Zur Beantwortung dieser Fragen kann zunächst auf den einschlägigen BSI-Standard[10] zurückgegriffen werden.

2.2.2 Übermittlung personenbezogener Daten auf Grundlage von Art. 44 ff. DSGVO

Soweit eine Office-Anwendung eingesetzt werden soll, bei deren Nutzung personenbezogene Daten von Beschäftigten sowie Bürgerinnen und Bürgern in einen Staat außerhalb des Geltungsbereichs der Datenschutz-Grundverordnung übermittelt werden oder Stellen in einem solchen Staat eine Zugriffsmöglichkeit eröffnet wird, muss die Folgenbetrachtung auch die für solche Datentransfers einschlägigen gesetzlichen Vorgaben berücksichtigen. Die Bewertung nachteiliger Folgen für die Vertraulichkeit der personenbezogenen Daten wie auch die Implementierung von Maßnahmen zu ihrer Minimierung sind in diesem Fall durch die Art. 44 ff. DSGVO angeleitet.

Insbesondere ist die **Zulässigkeit der Übermittlung von personenbezogenen Daten** in das Drittland an den **Art. 44 ff. DSGVO** zu messen; die Vorschriften sollen sicherstellen, dass personenbezogene Daten nach Verlassen des räumlichen Geltungsbereichs der Datenschutz-Grundverordnung nicht in eine Verarbeitungsumgebung mit (signifikant) geringerem Datenschutzniveau geraten.

Grundlage der Übermittlung kann ein die Vergleichbarkeit des Datenschutzniveaus verbindlich feststellender, wirksamer **Angemessenheitsbeschluss** der Europäischen Kommission sein (Art. 45 Abs. 1 DSGVO). Für die USA, wo zahlreiche Anbieter von Office-Anwendungen beheimatet sind, liegt ein Angemessenheitsbeschluss ge-

[10] Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 203-3. Risikoanalyse auf der Basis von IT-Grundschutz, Internet: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.html.

genwärtig allerdings nicht vor. Die in Rede stehenden Übermittlungen können regelmäßig auch nicht auf die Ausnahmetatbestände gestützt werden, die Art. 49 Abs. 1 DSGVO für bestimmte Fälle vorsieht.

Vor diesem Hintergrund ist die **Vergleichbarkeit des Datenschutzniveaus durch den Verantwortlichen und seinen Vertragspartner sicherzustellen**, der als Datenempfänger fungieren soll. Dazu müssen geeignete Garantien vorgesehen sein und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen (Art. 46 Abs. 1 DSGVO). Vorliegend kommen hierzu insbesondere Regelungen in **Standarddatenschutzklauseln** in Betracht (Art. 46 Abs. 2 Buchst. c DSGVO). Ein entsprechendes aktuelles Klauselwerk hat die Europäische Kommission im Sommer 2021 bereitgestellt.[11]

Da das Klauselwerk grundsätzlich nicht die Heimatrechtsordnung des ausländischen Datenempfängers modifizieren kann, genügen der Verantwortliche und sein Vertragspartner jedoch den Anforderungen der Datenschutz-Grundverordnung **nicht** bereits dann, wenn sie die Geltung des Klauselwerks vereinbaren.[12]

Geeignete Garantien im Sinne von Art. 46 Abs. 1 DSGVO werden nur vermittelt, wenn das **Klauselwerk auch (tatsächlich) wirksam** ist. Dazu bedarf es einer Betrachtung der Heimatrechtsordnung des ausländischen Datenempfängers. Der Europäische Datenschutzausschuss hat für diese Betrachtung ausführliche Hinweise veröffentlicht.[13]

Soweit die Betrachtung der Heimatrechtsordnung des ausländischen Datenempfängers ergibt, dass das Klauselwerk dort nicht in vollem Umfang die beabsichtigte Wirkung zu entfalten vermag, ist eine **Kompensation durch zusätzliche Maßnahmen** zu prüfen.[14] Dazu kann auch eine **Verschlüsselung** und/oder **Pseudonymisierung** zählen.[15] Ist eine Kompensation nicht möglich, muss eine Übermittlung personenbezogener Daten an den ausländischen Datenempfänger unterbleiben.

Aus diesen grundsätzlichen Bemerkungen ergeben sich für den Einsatz konkreter Office-Anwendungen insbesondere die nachstehenden **Konsequenzen**:

— Ausgangspunkt aller Überlegungen sollte ein **Datenschutz-Sicherheitskonzept** sein, das eine datenschutzrechtliche Folgenbetrachtung vornimmt.

  Das Datenschutz-Sicherheitskonzept muss klare Aussagen darüber enthalten, welche **Kategorien personenbezogener Daten** von Beschäftigten sowie

11 Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, ABl. L 199 vom 7. Juni 2021, S. 31 ff.

12 Vgl. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Pressemitteilung vom 21. Juni 2021, Internet: https://www.datenschutzkonferenz-online.de/pressemitteilungen.html.

13 Europäischer Datenschutzausschuss, Recommendations 01/2020 vom 18. Juni 2021, Rn. 28 ff., Internet: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

14 Recommendations 01/2020, Rn. 50 ff.

15 Recommendations 01/2020, Rn. 54.

Bürgerinnen und Bürgern (in einer Schule etwa also von Schülerinnen, Schülern, Eltern, Lehrkräften und sonstigem Schulpersonal) in ein Drittland übermittelt werden oder Zugriffen von dort ausgesetzt werden sollen.

Bei der **Folgenbetrachtung** ist für die konkrete Office-Anwendung insbesondere die nachteilige Folge zu würdigen, dass Behörden aus einem Drittland auf personenbezogene Daten von Beschäftigten sowie Bürgerinnen und Bürgern Zugriff nehmen könnten (auch im Wege einer Anforderung zur Offenlegung von personenbezogenen Daten). Diese nachteilige Folge ist bereits dann zu berücksichtigen, wenn die Rechtsordnung des Drittlandes zugunsten dortiger Behörden in Bezug auf die zu übermittelnden personenbezogenen Daten Zugriffsbefugnisse vorsieht, die aus unionsrechtlicher Perspektive als unverhältnismäßig erscheinen. Die nachteilige Folge kann grundsätzlich nicht allein durch eine Wahrscheinlichkeitsbetrachtung („bisher ist ja nichts passiert") auf Grundlage von Angaben des Vertragspartners relativiert werden.

— Der Verantwortliche sollte das Rechtsverhältnis mit dem Vertragspartner in Ansehung von Datenübermittlungen in ein Drittland unter Einbezug der **aktuellen Standarddatenschutzklauseln** gestalten.

— Bei der Prüfung der **tatsächlichen Wirksamkeit des vereinbarten Klauselwerks** sind hinsichtlich des Drittlands USA zumindest diejenigen Vorgaben des US-amerikanischen Rechts zu berücksichtigen, die der Europäische Gerichtshof in seiner „Schrems II"-Entscheidung angesprochen hat.[16]

  Insofern dürfte nach der derzeitigen Auffassung des Bayerischen Landesbeauftragten für den Datenschutz die tatsächliche Wirksamkeit des vereinbarten Klauselwerks anzunehmen sein, wenn der Verantwortliche den Nachweis erbringt, dass die zu übermittelnden personenbezogenen Daten aus Rechtsgründen von vornherein nicht Gegenstand der betreffenden Zugriffsrechte US-amerikanischer Behörden werden können.

— Lässt sich dieser Nachweis nicht führen, ist als **Kompensation** eine Verschlüsselung und/oder Pseudonymisierung der personenbezogenen Daten in Betracht zu ziehen. Der Verantwortliche muss in diesem Fall zudem den Nachweis erbringen, dass eine Aufhebung der Verschlüsselung und/oder Pseudonymisierung bei dem ausländischen Vertragspartner durch Behörden seines Heimatstaats ausgeschlossen werden kann.

  Bei der Bewertung der nachteiligen Folge einer Aufhebung der Verschlüsselung und/oder Pseudonymisierung, die im Rahmen des Datenschutz-Sicherheitskonzepts durchgeführt werden kann, sollten nicht nur die Erfahrungen, die der ausländische Vertragspartner mit Zugriffsersuchen durch Behörden seines Heimatstaats gemacht hat, sondern auch alle weiteren verfügbaren Informationen[17] einbezogen werden. Entsprechendes gilt für die Bemessung kompensatorischer Maßnahmen, insbesondere für die Beantwortung der Frage, ob eine Verschlüsselung oder Pseudonymisierung ausreichend stark ist. Auch hier gilt: Dass „bisher nichts passiert ist", bedeutet nicht, dass diese Maßnahmen vernachlässigt werden dürfen.

16 Europäischer Gerichtshof, Urteil vom 16. Juli 2020, C-311/18, Rn. 177 ff.

17 Vgl. näher Recommendations 01/2020, Annex 3.

— Speziell beim Betrieb eines **Videokonferenz-Systems** fallen zumindest temporär Bild- und Tondateien an. Nach aktuellem Kenntnisstand ist eine ausreichend starke Verschlüsselung und/oder Pseudonymisierung insofern derzeit noch nicht möglich; dies gilt jedenfalls für typische Nutzungsszenarien im Schulbereich.

  Datenschutzrechtliche Bedenken betreffend eine Übermittlung in das Drittland USA können hier auch nicht dadurch ausgeräumt werden, dass auf eine dauerhafte Aufzeichnung verzichtet wird und/oder die Dateien physikalisch im Geltungsbereich der Datenschutz-Grundverordnung gespeichert werden. US-amerikanische Anbieter sind als in den USA ansässige Unternehmen Zugriffsrechten US-amerikanischer Behörden ausgesetzt; dies gilt insbesondere für Regelungen des US CLOUD Act.[18] Entsprechenden Ersuchen kann allenfalls ausnahmsweise im Einklang mit der Datenschutz-Grundverordnung nachgekommen werden.[19] Im Übrigen ist zu bedenken, dass gegebenenfalls Verkehrsdaten übermittelt werden, bei denen ein Personenbezug hergestellt werden kann.

— Bei **anderen Office-Anwendungen** als Videokonferenz-Systemen kann eine ausreichend sicher gestaltete **Pseudonymisierung** insbesondere unter den folgenden Voraussetzungen in Betracht kommen:

  (1) **Angemessen starke Pseudonymisierungsmethode:** Personenbezogene Daten werden so verarbeitet, dass sie ohne Hinzuziehung zusätzlicher Informationen weder einer spezifischen betroffenen Person zugeordnet noch dazu verwendet werden können, die betroffene Person in einer größeren Gruppe zu identifizieren. Zudem darf ein Abgleich mit sämtlichen Informationen, die Dritten zur Verfügung stehen, nicht dazu führen, dass die pseudonymisierten Daten identifizierten oder identifizierbaren natürlichen Personen zugeordnet werden können.

  (2) **Besonderer Schutz der Zuordnungsregeln:** Die Zuordnung der pseudonymisierten Daten zu Identitätsinformationen („Zuordnungsregeln", z. B. Datentabelle oder Formel) und damit die Re-Identifizierung darf nur durch den Verantwortlichen (beispielsweise: die Schule) oder einen Auftragsverarbeiter, der als Vertrauensinstanz agiert und auf den die Datenschutz-Grundverordnung anwendbar ist, möglich sein. Zudem müssen die Zuordnungsregeln grundsätzlich innerhalb der EU gehalten und einem angemessenen Schutz durch technische und organisatorische Maßnahmen gegen unbefugte Zugriffe, gegen unbefugte Veränderungen sowie gegen Störungen der erforderlichen Verfügbarkeit unterliegen.

  (3) **Stand der Technik:** Das eingesetzte Pseudonymisierungsverfahren muss grundsätzlich dem Stand der Technik entsprechen. Die Wirksam-

18 Zu diesem näher Europäischer Datenschutzausschuss/Europäischer Datenschutzbeauftragter, Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection mit Annex vom 10. Juli 2019, Internet: https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

19 Zu den Anforderungen näher a. a. O. (Fußnote 18), Annex, S. 4 ff.

keit der Pseudonymisierung als datenschutzrechtliche Schutzmaßnahme muss durch bedarfsgerechte Überprüfungen durchgängig gewährleistet sein.

– Entsprechend sind folgende Anforderungen an eine ausreichend sicher gestaltete **Verschlüsselung** zu stellen:

  (1) **Angemessen starke Verschlüsselungsmethode:** Der Verschlüsselungsalgorithmus und seine Parametrisierung (z. B. Schlüssellänge, Verschlüsselungsstärke, Betriebsmodus) müssen angemessen sein und den spezifischen Zeitraum berücksichtigen, für den die Vertraulichkeit der verschlüsselten personenbezogenen Daten sicherzustellen ist.

  (2) **Besonderer Schutz der Schlüssel:** Die Schlüssel müssen allein durch den Verantwortlichen (beispielsweise: die Schule) oder einen Auftragsverarbeiter, der als Vertrauensinstanz agiert und auf den die Datenschutz-Grundverordnung anwendbar ist, verwaltet und kontrolliert werden. Dadurch wird ein Zugriff auf unverschlüsselte Daten (Klardaten) durch unberechtigte Dritte mit Hilfe einer Ende-zu-Ende-Verschlüsselung ausgeschlossen. Zudem muss der Verschlüsselungsalgorithmus fehlerfrei durch ordnungsgemäß gepflegte Software implementiert sein, deren Konformität mit der Spezifikation des ausgewählten Algorithmus etwa durch Zertifizierung bestätigt wurde. Die Verschlüsselung muss – unter Berücksichtigung der zur Verfügung stehenden Ressourcen und technischen Möglichkeiten (z. B. Rechenleistung für Brute-Force-Angriffe) – Robustheit gegen eine eventuell durchgeführte Kryptoanalyse bieten. Ferner muss im Hinblick auf die Schlüssel, deren Generierung und Einsatz ein angemessener Schutz durch technische und organisatorische Maßnahmen gegen unbefugte Zugriffe, gegen unbefugte Veränderungen sowie gegen Störung der erforderlichen Verfügbarkeit bestehen.

  (3) **Stand der Technik:** Das eingesetzte Verschlüsselungsverfahren muss grundsätzlich dem Stand der Technik entsprechen. Die Wirksamkeit der Verschlüsselung als datenschutzrechtliche Schutzmaßnahme muss durch bedarfsgerechte Überprüfungen durchgängig gewährleistet sein.

2.2.3 Rechenschaftspflicht

Verantwortliche trifft nach Art. 5 Abs. 2 DSGVO eine Rechenschaftspflicht. Die Rechenschaftspflicht bezieht sich auch auf den Verarbeitungsgrundsatz „Rechtmäßigkeit“ (Art. 5 Abs. 1 Buchst. a DSGVO). Sie gewährleistet, dass Verantwortliche ihre Überlegungen zu den rechtlichen Grundlagen einer Verarbeitung festhalten; für die Datenschutz-Aufsichtsbehörden werden diese Überlegungen so kontrollierbar. Im Rahmen der Rechenschaftspflicht müssen Verantwortliche, die Datentransfers in Drittstaaten durchführen möchten, auch dokumentieren, dass sie die durch Art. 44 ff. DSGVO geforderte, oben näher erläuterte Prüfung vorgenommen haben. Diese gesetzlichen Anforderungen haben Anteil an dem Regelungsgefüge, das die Rechtmäßigkeit einer Verarbeitung betrifft.

Was die Beachtung von Art. 44 ff. DSGVO angeht, orientiert der Bayerische Landesbeauftragte für den Datenschutz seine Kontrollen vorrangig an den Dokumentationen, welche die Verantwortlichen zur Erfüllung der Rechenschaftspflicht erstellen.

Verantwortliche können daher nicht erwarten, dass ihnen die Datenschutz-Aufsichtsbehörde die Erfüllung der Rechenschaftspflicht abnimmt; sie können insbesondere nicht erwarten, dass die Datenschutz-Aufsichtsbehörde die Zulässigkeit durchgeführter Drittstaatentransfers würdigt, wenn keine oder keine ausreichenden Dokumentationen vorgelegt werden können.

Bei Drittstaatentransfers im Zusammenhang mit Office-Anwendungen – ausgenommen sind Videokonferenz-Systeme – akzeptiert der Bayerische Landesbeauftragte für den Datenschutz unter den oben dargelegten Anforderungen bis auf weiteres grundsätzlich auch Dokumentationen zur Erfüllung der Rechenschaftspflicht, die auf eine Prüfung der tatsächlichen Wirksamkeit von Klauselwerken verzichten. Vorausgesetzt ist dabei,

- dass das vereinbarte Klauselwerk auf den aktuellen Standarddatenschutzklauseln beruht und von diesen nicht abweicht, sowie

- dass der Verantwortliche eine ausreichend sicher gestaltete Verschlüsselung und/oder Pseudonymisierung vorsieht und anwendet.

2.3 Entgeltpflicht für Kontrollen bei der Auftragsverarbeitung?

Nach Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO hat eine Auftragsverarbeitungs-Vereinbarung vorzusehen, dass der Auftragsverarbeiter dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Seit der Datenschutzreform 2018 wird diskutiert, ob und inwieweit Auftragsverarbeitungs-Vereinbarungen für den Fall der Wahrnehmung von Kontrollrechten des Verantwortlichen – insbesondere im Fall einer Vor-Ort-Kontrolle – ein gesondertes Entgelt vorsehen können. Der Bayerische Landesbeauftragte für den Datenschutz hat den bayerischen öffentlichen Stellen empfohlen, sich für die Ausübung ihrer gesetzlichen Kontrollrechte nicht zu einem besonderen Entgelt verpflichten zu lassen (vgl. Aktuelle Kurz-Information 6 in der Fassung vom 1. August 2018).

Der Europäische Datenschutzausschuss hat im Juli 2021 nach öffentlicher Konsultation überarbeitete Leitlinien 7/2020 zu den Begriffen des Verantwortlichen und des Auftragsverarbeiters in der Datenschutz-Grundverordnung veröffentlicht, in welche zu der Frage einer Entgeltpflicht für Kontrollen bei der Auftragsverarbeitung die folgenden Erwägungen neu aufgenommen wurden:

„The issue of the allocation of costs between a controller and a processor concerning audits is not covered by the GDPR and is subject to commercial considerations. However, Article 28 (3)(h) requires that the contract include an obligation for the processor to make available all information necessary to the controller and an obligation to allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. This means in practice that parties should not insert in the contract clauses envisaging the payment of costs or fees that would be clearly disproportionate or excessive, thus having a dissuasive effect on one of the parties. Such clauses would indeed imply that the rights and obligations set out in Article 28(3)(h) would never be exercised in practice and would

become purely theoretical whereas they form an integral part of the data protection safeguards envisaged under Article 28 GDPR."[20]

Der Europäische Datenschutzausschuss weist zutreffend darauf hin, dass die wirtschaftliche Gestaltung der Austauschbeziehung zwischen dem Verantwortlichen und dem Auftragsverarbeiter durch den Markt und nicht durch die Datenschutz-Grundverordnung reguliert wird. Dies bedeutet allerdings auch, dass es dem Verantwortlichen unbenommen ist, ihm unterbreitete Angebote von Auftragsverarbeitern auf ihre Datenschutzfreundlichkeit zu prüfen und diesen Gesichtspunkt bei der Auswahl des Vertragspartners zu berücksichtigen. Der Verantwortliche wird zudem entsprechende Vorgaben in einen Ausschreibungstext aufnehmen können, wenn die benötigte Leistung in einem Vergabeverfahren beschafft wird.

Der Europäische Datenschutzausschuss gibt ferner zu bedenken, dass Kosten oder Gebühren Maßnahmen des Verantwortlichen nach Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO behindern können. Der Bayerische Landesbeauftragte für den Datenschutz hat dieses Risiko bereits kurz nach der Datenschutzreform 2018 wie folgt beschrieben (Aktuelle Kurz-Information 6 in der Fassung vom 1. August 2018):

„Ein gesondertes Entgelt würde einer Ausübung der Kontrollrechte entgegenwirken. Die Vereinbarung eines Entgelts, einer Aufwandsentschädigung oder eines sonstigen Kostenbeitrags, auch die Vereinbarung, hierzu im Bedarfsfall nachträglich eine die Auftragsverarbeitungs-Vereinbarung ergänzende Regelung zu treffen, führt dazu, dass eine Inspektion beim Auftragsverarbeiter als etwas ‚Außergewöhnliches' wahrgenommen wird, das dem Auftraggeber ‚eigentlich' nicht zusteht und gerade deshalb außerhalb der wechselseitigen Austauschbeziehung zu vergüten ist. Davon abgesehen kann ein solches Entgelt entweder auf Grund seiner bereits erkennbaren (absoluten) Höhe oder der vertraglich angelegten Unklarheit seiner Berechnung abschreckende Wirkung entfalten."

Soweit ein Auftragsverarbeiter die Besorgnis hat, dass er durch Maßnahmen des Verantwortlichen nach Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO – insbesondere Vor-Ort-Kontrollen – Belastungen ausgesetzt wird, welche den vertraglichen Leistungsaustausch aus dem Gleichgewicht bringen, kann er den erwartbaren Mehraufwand bei der Berechnung der vom Verantwortlichen geforderten Hauptleistung pauschal berücksichtigen. Ergänzend kommen dabei insbesondere vertragliche Bestimmungen in Betracht, dass eine Vor-Ort-Kontrolle grundsätzlich mit einer bestimmten Frist anzukündigen ist, oder dass anlasslose Inspektionen mengenmäßig kontingentiert sind. Diese bislang empfohlene Vorgehensweise (vgl. Aktuelle Kurz-Information 6 in der Fassung vom 1. August 2018) steht nach Auffassung des Bayerischen Landesbeauftragten für den Datenschutz auch weiterhin mit Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO in Einklang.

Soweit die neu gefassten Leitlinien 7/2020 des Europäischen Datenschutzausschusses eine Vereinbarung separater, insbesondere nicht pauschalierter Entgelte für Maßnahmen des Verantwortlichen nach Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO nicht ausschließen, sollten die bayerischen öffentlichen Stellen insbesondere die folgenden Überlegungen berücksichtigen:

[20] European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, Stand 7/2021, Rn. 145, Internet: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_de.

- Ob eine Klausel für Maßnahmen nach Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO ein eindeutig unverhältnismäßiges oder überhöhtes Entgelt vorsieht, das auf den Verantwortlichen eine abschreckende Wirkung hat, ist stets in Anbetracht der Umstände des Einzelfalls zu würdigen.

- Ein Fall eindeutiger Unverhältnismäßigkeit kann insbesondere vorliegen, wenn die während der Vertragsdauer für Maßnahmen nach Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO erwartbaren Kosten oder Gebühren die Gestalt der vom Verantwortlichen zu erbringenden Hauptleistung wesentlich verändern.

- Ein eindeutig überhöhtes Entgelt kann insbesondere darauf beruhen, dass der tatsächliche Aufwand beim Auftragsverarbeiter zu den vereinbarten Kosten oder Gebühren in einem grob unangemessenen Verhältnis steht (so etwa bei „Phantasiepreisen" für den Einsatz personeller oder sachlicher Ressourcen oder bei der „Erfindung" von Kontrollgebühren, denen der Auftragsverarbeiter einen Aufwand nicht plausibel zuordnen kann).

- Eine abschreckende Wirkung kann etwa dann in Betracht zu ziehen sein, wenn zu erwarten ist, dass der Verantwortliche Maßnahmen nach Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO auf Grund der Kostenbelastung nicht ohne Überwindung weiterer Hürden veranlassen kann. Das ist insbesondere dann der Fall, wenn bei einem kommunalen Träger nach den einschlägigen Vorschriften ein Gremienbeschluss zur Bewilligung außer- oder überplanmäßiger Ausgaben erforderlich wird.

- Soweit bayerische öffentliche Stellen im Einzelfall separate, insbesondere nicht pauschalierte Entgelte für Maßnahmen nach Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO vereinbaren möchten, sollten sie vor diesem Hintergrund zum einen auf eine strikte Kostentransparenz achten. Dazu gehört neben einer Markterkundung insbesondere eine Aufwandsprognose. Bereits vor Vertragsschluss sollte zumindest überschlägig ermittelt werden, welche Mittel während der Vertragsdauer voraussichtlich für Maßnahmen nach Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO über die Hauptleistung hinaus bereitgestellt werden müssen. Diese Mittel sollten zum anderen in der haushaltsrechtlich angezeigten Form so eingeplant werden, dass der Verantwortliche im Bedarfsfall jederzeit darauf zugreifen kann, insbesondere eine (zusätzliche) Bewilligung nicht erforderlich ist. Im Übrigen sollten kommunale Träger bei Vertragsschlüssen, die der Zustimmung des kollegialen Hauptorgans bedürfen, auch insofern für Kostentransparenz sorgen

3 Polizei und Verfassungsschutz

3.1 Änderung des Polizeiaufgabengesetzes

Die Staatsregierung hat am 12. Februar 2021 einen Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften vorgelegt (Landtags-Drucksache 18/13716). Bereits frühzeitig hat mich das Bayerische Staatsministerium des Innern, für Sport und Integration in das Gesetzgebungsverfahren einbezogen. Eine konsolidierte Fassung meiner Stellungnahmen ist im Rahmen meiner Internetpräsenz veröffentlicht.[21]

Der Ausschuss für Kommunale Fragen, Innere Sicherheit und Sport des Bayerischen Landtags hat mich als Sachverständigen zugezogen. Meine Stellungnahme zu den mir in diesem Zusammenhang übermittelten Fragen ist im Anhang zu diesem Tätigkeitsbericht dokumentiert.

3.2 Zuverlässigkeitsüberprüfungen im Rahmen von Akkreditierungsverfahren

In Akkreditierungsverfahren bei Großereignissen sind Zuverlässigkeitsüberprüfungen seit Jahren ein fester Bestandteil der polizeilichen Praxis. Sie waren daher in der Vergangenheit regelmäßig Gegenstand meiner Prüfungstätigkeit. Die FIFA Fußball-Weltmeisterschaft und der Papstbesuch 2006, der G8-Gipfel 2008, die Leichtathletik-Weltmeisterschaft 2009, die FIFA Frauen-Weltmeisterschaft 2011 sowie die Alpine Ski-Weltmeisterschaft 2011, die Biathlon-Weltmeisterschaft 2012, die UEFA Euro 2020 oder zuletzt die IAA Mobility 2021 sind nur einige ausgewählte Beispiele, bei denen polizeiliche Zuverlässigkeitsüberprüfungen erfolgten.

Zuverlässigkeitsüberprüfungen unter Einbindung der Polizei werden aber nicht nur anlässlich von Großveranstaltungen durchgeführt. Auch einzelne (öffentliche) Arbeitgeber fordern Bewerberinnen und Bewerber, Beschäftigte und Fremdpersonal (beispielsweise Reinigungskräfte) auf, in eine Anfrage bei der Polizei zu dort über sie etwa vorliegenden Erkenntnissen einzuwilligen.

Zuverlässigkeitsüberprüfungen führen insbesondere bei Großveranstaltungen aufgrund ihrer Bedeutung und ihres Umfangs zu schwerwiegenden Eingriffen in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz) einer Vielzahl betroffener Personen. Von besonderer Bedeutung ist dabei, dass die Polizei auch solche Daten speichert, die beispielsweise in das Bundeszentralregister erst gar nicht eingetragen werden, dort bereits getilgt sind oder aus diesem Register – sofern es um ein Führungszeugnis und nicht um eine unbeschränkte Auskunft geht –nicht übermittelt werden dürfen.

Bislang wurden zuvor abgegebene schriftliche Einwilligungserklärungen als ausschließliche Grundlage für die Einbeziehung der betroffenen Personen in das Verfahren zur Überprüfung ihrer Zuverlässigkeit herangezogen. Darin erklärte sich diese mit der Teilnahme an einem Verfahren einverstanden, bei dem die Polizei anschließend

[21] Internet: https://www.datenschutz-bayern.de/nav/0710.html.

ihre Erkenntnisse zu der jeweiligen Person überprüfte, bewertete und dem Veranstalter oder dem Arbeitgeber mitteilte, ob gegen eine Verwendung der Person Sicherheitsbedenken bestanden. Eine Datenschutzinformation unterrichtete betroffene Personen unter anderem über den Ablauf, den Umfang, die Beurteilungskriterien und die möglichen Folgen einer Überprüfung.

An der Freiwilligkeit einer Einwilligung hatte ich seit jeher erhebliche Zweifel, weil betroffene Personen oft unzumutbare Nachteile befürchten mussten, wenn sie ihre Einwilligung verweigerten. Auch im Hinblick auf den Grundsatz des Vorbehalts des Gesetzes hielt ich eine Einwilligung für problematisch. Gemäß der vom Bundesverfassungsgericht entwickelten Wesentlichkeitslehre darf der Gesetzgeber die wesentlichen Entscheidungen über die Voraussetzungen, Umstände und Folgen von Eingriffen nämlich nicht an die Verwaltung delegieren, sondern muss sie selbst treffen. Vor dem Hintergrund von Erwägungsgrund 35 RLDSJ, der im Kern besagt, dass im Verhältnis zwischen der Polizei sowie Bürgerinnen und Bürgern Einwilligungen keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten darstellen sollen, sah ich mich in meiner kritischen Haltung bestätigt.

Von Beginn an und zuletzt in meiner oben unter Nr. 3.1 dargestellten Stellungnahme zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften gegenüber dem Ausschuss für Kommunale Fragen, Innere Sicherheit und Sport des Bayerischen Landtags habe ich meine Haltung gegenüber den beteiligten Stellen deutlich gemacht und für die Zuverlässigkeitsüberprüfungen eine bereichsspezifische gesetzliche Regelung gefordert. Mit Sorge musste ich beobachten, dass Zuverlässigkeitsüberprüfungen immer mehr als Regelverfahren auf der Grundlage „informierter Einwilligungen“ durchgeführt wurden. Das Fehlen klarer gesetzlicher Regelungen führte zudem oftmals dazu, dass eine datenschutzkonforme verfahrensrechtliche Ausgestaltung der Zuverlässigkeitsüberprüfungen etwa durch hinreichende Clearing-Verfahren sowie eine transparente Ausgestaltung der Datenschutzinformationen immer wieder neu „errungen“ werden musste.

Nachdem meine Forderung nach einer ausdrücklichen Rechtsgrundlage für die Zuverlässigkeitsüberprüfungen im Rahmen der Novellierungen des Polizeiaufgabengesetzes (PAG) zum 24. Juli 2017 und zum 25. Mai 2018 (vgl. hierzu auch den 28. Tätigkeitsbericht 2018 unter Nr. 4.1.1) unberücksichtigt geblieben war, wurde im Berichtsjahr kurzfristig und nach Abgabe meiner Stellungnahme gegenüber dem Ausschuss für Kommunale Fragen, Innere Sicherheit und Sport ein neuer Art. 60a PAG geschaffen. Diese Vorschrift regelt nun seit dem 1. August 2021 den Rahmen für Zuverlässigkeitsüberprüfungen durch die Polizei.

Art. 60a PAG
Zuverlässigkeitsüberprüfung
(1) [1]Bei Anlässen, die mit erheblichen Sicherheitsrisiken verbunden sind, kann die Polizei personenbezogene Daten einer Person mit deren schriftlicher oder elektronischer Zustimmung bei öffentlichen und nichtöffentlichen Stellen erheben, übermitteln und anderweitig verarbeiten (Zuverlässigkeitsüberprüfung), soweit dies im Hinblick auf den Anlass und die Tätigkeit der betroffenen Person erforderlich und angemessen ist. [2]Die Erforderlichkeit und der Umfang der Verarbeitung sind anhand einer Gefährdungsanalyse festzulegen, wobei sich die Datenerhebung nach dem Zweck der Zuverlässigkeitsüberprüfung richtet. [3]Zuverlässigkeitsüberprüfungen können insbesondere erfolgen
1. zur Regelung der besonderen Zugangsberechtigung zu Veranstaltungen und Veranstaltungsreihen, die besonders gefährdet sind,

2. für den privilegierten Zutritt zu einem Amtsgebäude oder einem anderen gefährdeten Objekt oder Bereich,
3. für die Erbringung von Dienstleistungen zur Unterstützung behördlicher Aufgaben,
4. bei Personen, die Zugang zu Unterlagen oder ähnlichen Inhalten haben sollen, aus denen sich sicherheitsrelevante Erkenntnisse für die Tätigkeit von Polizei und Sicherheitsbehörden ergeben oder
5. zu Zwecken des Personen- und Objektschutzes.
[4]Die Polizei kann hierzu die Identität der Person feststellen, deren Zuverlässigkeit überprüft werden soll, und zu diesem Zweck auch von ihr vorgelegte Ausweisdokumente kopieren oder Kopien von Ausweisdokumenten anfordern.
(2) [1]Die Polizei ist befugt, das Ergebnis ihrer Zuverlässigkeitsüberprüfung an eine andere Stelle zu übermitteln, wenn die Beurteilung der Zuverlässigkeit der anderen Stelle obliegt. [2]Hat die Polizei dabei Zuverlässigkeitsbedenken, ist die betroffene Person vor der Datenübermittlung an die andere Stelle über die Bedenken der Polizei zu informieren, wenn die betroffene Person dies schriftlich oder in elektronischer Form gegenüber der Polizei zuvor erklärt hat. [3]In den Fällen des Satzes 2 gibt die Polizei der betroffenen Person Gelegenheit, Einwände gegen die Sicherheitsbedenken schriftlich oder in elektronischer Form vorzubringen, welche vor der Übermittlung nach Satz 1 zu prüfen sind. [4]Die betroffene Person ist von der anderen Stelle auf die Möglichkeiten nach den Sätzen 2 und 3 und über Ablauf und Inhalt des polizeilichen Überprüfungsverfahrens spätestens vor der erstmaligen Datenübermittlung an die Polizei hinzuweisen. [5]Hat die Polizei Zweifel daran, dass die andere Stelle ihrer Verpflichtung nach Satz 4 nachgekommen ist, ist die betroffene Person durch die Polizei vor der Übermittlung nach Satz 1 über das Bestehen von Sicherheitsbedenken zu informieren. [6]Von der Information des Betroffenen nach den Sätzen 2 und 5 kann unter den Voraussetzungen des Art. 65 Abs. 2 und 3 abgesehen werden. [7]Erfolgt die Mitteilung an eine nichtöffentliche Stelle, beschränkt sich die Mitteilung nach Satz 1 darauf, dass Zuverlässigkeitsbedenken bestehen.
(3) Die Polizei kann die andere Stelle dazu verpflichten, ihr mitzuteilen, wenn sie eine Person trotz bekannter Zuverlässigkeitsbedenken der Polizei gleichwohl für den Anlass verwendet, für den die Zuverlässigkeitsüberprüfung durchgeführt wurde.
(4) Art. 54 Abs. 2 Satz 6 findet keine Anwendung.
(5) [1]Die Polizei kann ferner Personen, die eine Tätigkeit in einer Behörde der Polizei oder des Verfassungsschutzes anstreben, mit deren schriftlicher oder elektronischer Zustimmung einer Zuverlässigkeitsüberprüfung nach Abs. 1 unterziehen. [2]In diesen Fällen findet Arbeits- und Beamtenrecht Anwendung.

Bereits im Gesetzgebungsverfahren habe ich die Schaffung einer bereichsspezifischen Rechtsgrundlage ausdrücklich begrüßt. Zugleich wies ich aber darauf hin, dass das Gesetzesvorhaben ausschließlich der Sicherung des über die Jahre aus datenschutzrechtlicher Sicht erarbeiteten Status quo dienen darf. Aus diesem Grund habe ich dem Bayerischen Staatsministerium des Innern, für Sport und Integration gegenüber auch deutlich gemacht, dass ich der nunmehr in Art. 60a Abs. 1 Satz 1 PAG enthaltenen Befugnis einer Datenerhebung durch die Polizei bei öffentlichen wie nichtöffentlichen Stellen kritisch gegenüber stehe. Bislang stand nämlich der Abgleich mit vorhandenen Daten im Vordergrund. Mit dieser Forderung konnte ich mich letztendlich jedoch nicht durchsetzen.

Positiv ist zu bewerten, dass nach Art. 60a Abs. 1 Satz 2 PAG bei Zuverlässigkeitsüberprüfungen die Erforderlichkeit und der Umfang der Verarbeitung anhand einer Gefährdungsanalyse festzulegen sind, wobei sich die Datenerhebung nach dem Zweck der Zuverlässigkeitsüberprüfung richtet. Hiermit wird im Wesentlichen eine

alte datenschutzrechtliche Forderung aufgegriffen (siehe mein 25. Tätigkeitsbericht 2012 unter Nr. 3.10 und mein 28. Tätigkeitsbericht 2018 in Anlage 9).

Zudem konnte ich erreichen, dass eine Verschlechterung der verfahrensrechtlichen Stellung betroffener Personen vermieden wird. Während der ursprüngliche Entwurf von Art. 60a PAG bei Sicherheitsbedenken vor einer Offenlegung gegenüber dem Veranstalter lediglich eine Information der betroffenen Person vorsah, wurde für diesen Fall auf meine Kritik hin ein Clearing-Verfahren vorgesehen, in dessen Rahmen eine betroffene Person Einwände gegen die Sicherheitsbedenken vorbringen kann. Voraussetzung hierfür ist lediglich, dass die betroffene Person vorab gegenüber der Polizei den entsprechenden Wunsch schriftlich oder elektronisch äußert. Auf diese Möglichkeit ist die betroffene Person vor der erstmaligen Datenübermittlung an die Polizei durch den Veranstalter oder den Arbeitgeber hinzuweisen. Soweit die Polizei Zweifel daran hat, dass dieser Verpflichtung Genüge getan wurde, ist die betroffene Person jedenfalls vor der Übermittlung von Sicherheitsbedenken zu informieren. Weiterhin konnte ich erreichen, dass betroffenen Personen der Ablauf und der Inhalt der Zuverlässigkeitsüberprüfung vor der erstmaligen Datenübermittlung an die Polizei bekannt zu geben sind.

Ob mit der erweiterten Befugnis zur Datenerhebung im Rahmen von Zuverlässigkeitsüberprüfungen nach Art. 60a Abs.1 Satz 1 PAG auch eine Ausweitung der polizeilichen Praxis einhergehen wird, bleibt abzuwarten. Jedenfalls konnte ich solche Tendenzen bei den Zuverlässigkeitsüberprüfungen im Rahmen der IAA Mobility 2021, die sich als erste auf Art. 60a PAG als Rechtsgrundlage stützten, nicht feststellen. Nach meinen Erkenntnissen lag der Fokus wie in den früheren Verfahren auf einem Abgleich bestehender Daten und Informationen bei der Polizei. Es zeigte sich aber, dass die Existenz einer normenklaren Rechtsgrundlage mit den von mir geforderten verfahrensrechtlichen Absicherungen (Clearing-Verfahren, Datenschutzinformation) für betroffene Personen ein großer Gewinn war. So nutzten nach meiner Kenntnis insbesondere einige Personen das Clearing-Verfahren, um gegen sie erhobene Sicherheitsbedenken auszuräumen. Nachträgliche Beschwerden über fälschlicherweise erhobene Sicherheitsbedenken haben mich im Berichtszeitraum nicht erreicht, was ich als Signal für das Funktionieren des Clearing-Systems werte.

3.3 Erkennungsdienstliche Maßnahmen aus Anlass von Ordnungswidrigkeiten

Erkennungsdienstliche Maßnahmen der Polizei sind häufiger Gegenstand meiner datenschutzrechtlichen Prüfungen und meiner Tätigkeitsberichte (siehe etwa mein 25. Tätigkeitsbericht 2012 unter Nr. 3.5.5 sowie mein 26. Tätigkeitsbericht 2014 unter Nr. 3.5.4). Die Polizei kann insbesondere aufgrund des Polizeiaufgabengesetzes sowie der Strafprozeßordnung (StPO) erkennungsdienstliche Maßnahmen durchführen. Nach meiner Erfahrung werden erkennungsdienstliche Maßnahmen in der Regel auf Grundlage von § 81b StPO vorgenommen.

§ 81b StPO
Erkennungsdienstliche Maßnahmen bei dem Beschuldigten
Soweit es für die Zwecke der Durchführung des Strafverfahrens oder für die Zwecke des Erkennungsdienstes notwendig ist, dürfen Lichtbilder und Fingerabdrücke des Beschuldigten auch gegen seinen Willen aufgenommen und Messungen und ähnliche Maßnahmen an ihm vorgenommen werden.

Die Vorschrift unterscheidet zwei Zwecke, die mit einer erkennungsdienstlichen Maßnahme verfolgt werden können: Sie dient entweder der Überführung oder Entlastung

einer beschuldigten Person in einem konkreten Strafverfahren (Alternative 1) oder sie erfolgt zu Zwecken des Erkennungsdienstes (Alternative 2).

„Erkennungsdienstliche Zwecke“ haben vorbeugende und sichernde Maßnahmen, die der Polizei bei ihrer künftigen Tätigkeit die Identifizierung tatverdächtiger Personen erleichtern sollen. So können von einer Serieneinbrecherin oder einem Serieneinbrecher Lichtbilder und Fingerabdrücke gefertigt werden, um sie oder ihn im Falle einer zukünftigen Tat anhand von Fingerspuren oder einer von Zeugen genannten Personenbeschreibung schneller identifizieren zu können. Maßnahmen nach § 81b Alt. 2 StPO dienen also der Strafverfolgungsvorsorge.

Die Rechtsprechung hat den im Wortlaut sehr knapp gehaltenen § 81b StPO im Lauf der Zeit erheblich präzisiert. Dies gilt insbesondere für die Voraussetzungen erkennungsdienstlicher Maßnahmen mit dem Ziel der Strafverfolgungsvorsorge (Alternative 2).

Eine wichtige Voraussetzung ist, dass die erkennungsdienstliche Behandlung verhältnismäßig ist. Das Bundesverwaltungsgericht führt hierzu aus:

„Das Gebot der Verhältnismäßigkeit kommt in dem gesetzlichen Erfordernis der Notwendigkeit der erkennungsdienstlichen Behandlung zum Ausdruck. Nach § 81b Alt. 2 StPO dürfen die dort aufgeführten Maßnahmen nur angeordnet und vorgenommen, die dabei gewonnenen Daten nur gespeichert werden, wenn sie für die Zwecke des Erkennungsdienstes notwendig sind. Diese Datenerhebung und -speicherung dient der Strafverfolgungsvorsorge, indem sie der Kriminalpolizei sächliche Hilfsmittel für die Erforschung und Aufklärung künftiger Straftaten zur Verfügung stellt. Notwendigkeit im Sinne des § 81b Alt. 2 StPO ist anzunehmen, wenn angesichts aller Umstände des Einzelfalles tatsächliche Anhaltspunkte die Annahme rechtfertigen, der Beschuldigte könne künftig als Verdächtiger einer Straftat in Betracht kommen, deren Aufklärung die erkennungsdienstlichen Unterlagen überführend oder entlastend fördern können. Zu den Umständen, die bei dieser Prognoseentscheidung zu berücksichtigen sind, gehören das Ermittlungsergebnis des strafprozessualen Anlassverfahrens sowie Art, Schwere und Begehungsweise der dem Beschuldigten im Anlassverfahren zur Last gelegten Straftaten, seine Persönlichkeit sowie der Zeitraum, während dessen er strafrechtlich nicht mehr in Erscheinung getreten ist. Ist das strafprozessuale Ermittlungsverfahren nach § 170 Abs. 2 StPO eingestellt worden, weil sich der Anfangsverdacht im Verlauf der Ermittlungen nicht zu einer die Anklageerhebung rechtfertigenden Verurteilungswahrscheinlichkeit konkretisiert hat, müssen Behörden und Gerichte unter Abwägung des Für und Wider sorgfältig begründen, aus welchen Gründen sie eine erkennungsdienstliche Behandlung dennoch für notwendig halten (stRspr, vgl. zuletzt BVerwG, Urteil vom 27. Juni 2018 – 6 C 39.16 [ECLI:DE:BVerwG:2018:270618U6C39.16.0] – NJW 2018, 3194 Rn. 21 bis 23).“[22]

Angesichts dieser nicht unerheblichen Hürden, die erkennungsdienstlichen Maßnahmen im Bereich der Strafverfolgungsvorsorge entgegenstehen, hat es mich verwundert, dass ein Polizeipräsidium Maßnahmen nach § 81b Alt. 2 StPO auch gegenüber Betroffenen ergriff, denen lediglich Ordnungswidrigkeiten zur Last gelegt wurden.

Ein Zeitungsartikel, der von einer polizeilichen Kontrollaktion gegen die Prostitution in einem Sperrbezirk handelte, hatte über mehrere durchgeführte erkennungsdienstliche Maßnahmen berichtet und mein Interesse geweckt. Er veranlasste mich dazu,

22 Bundesverwaltungsgericht, Beschluss vom 25. März 2019, 6 B 163/18, 6 PKH 10/18, juris, Rn. 10.

beschwerdeunabhängig das betreffende Polizeipräsidium um eine nähere Darlegung des Sachverhalts und der Rechtsgrundlage zu ersuchen.

Wie mir die Polizei schließlich berichtete, wurden erkennungsdienstliche Maßnahmen gegen mehrere Personen aus Anlass einer Ordnungswidrigkeit gemäß § 120 Gesetz über Ordnungswidrigkeiten („Verbotene Ausübung der Prostitution") durchgeführt, nachdem es in Hotelzimmern zu „Anbahnungsgesprächen" mit sogenannten Scheinfreiern der Polizei gekommen war. Weder im Rahmen dieser Kontrollaktion noch zu einem vorherigen Zeitpunkt waren die erkennungsdienstlich behandelten Personen mit einer Straftat auffällig geworden, auch stand deren Identität zweifelsfrei fest. Die erkennungsdienstliche Maßnahme solle vielmehr dazu beitragen, die „Prostitutionsszene in ihrer Gesamtheit transparent und kontrollierbar zu halten", erläuterte das Polizeipräsidium und sei deshalb recht- und verhältnismäßig.

Diese Einschätzung konnte ich nicht teilen. Bei meiner Prüfung kam ich zu dem Schluss, dass die Durchführung der in Frage stehenden erkennungsdienstlichen Maßnahmen rechtswidrig war.

Die notwendigen Voraussetzungen für eine erkennungsdienstliche Maßnahme zum Zweck der Strafverfolgungsvorsorge waren hinsichtlich der konkreten Tatumstände nicht gegeben. Insbesondere war das polizeiliche Vorgehen angesichts der – selbst für Straftaten – hohen Anforderungen an erkennungsdienstliche Maßnahmen unverhältnismäßig, da lediglich Ordnungswidrigkeiten im Raum standen. Nur aus Gründen der Vollständigkeit sei erwähnt, dass auch weite Teile der Rechtsliteratur eine Behandlung für Zwecke des Erkennungsdienstes (§ 81b Alt. 2 StPO) im Bußgeldverfahren für „ausnahmslos ausgeschlossen"[23] halten.

Zu beachten ist des Weiteren, dass bei einer solchen Vorgehensweise im Übrigen auch eine Speicherung von Fingerabdrücken, Lichtbildern usw. in den zentralen erkennungsdienstlichen Datenbanken des Bundeskriminalamts ausgeschlossen ist. Das in diesem Zusammenhang maßgebliche Bundeskriminalamtgesetz (BKAG) spricht ausdrücklich von „Straftaten" als Anlass für eine erkennungsdienstliche Maßnahme und nicht von „Ordnungswidrigkeiten" (§ 16 Abs. 5 Satz 1 Nr. 2 BKAG).

Die erhobenen erkennungsdienstlichen Daten der betroffenen Personen wurden nach kontroversen Diskussionen mit dem betreffenden Polizeipräsidium, dem Bayerischen Landeskriminalamt sowie dem Bayerischen Staatsministerium des Innern, für Sport und Integration schließlich gelöscht. Auch zukünftig werde ich meine Aufmerksamkeit insbesondere auf solche erkennungsdienstliche Maßnahmen legen, die aus Anlass einer Ordnungswidrigkeit durchgeführt wurden. Hierfür habe ich das Innenministerium für das Jahr 2022 um die Vorlage aller entsprechenden Fälle gebeten, die bei der Bayerischen Polizei im Jahresverlauf anfallen, um diese Thematik gegebenenfalls einer weiteren datenschutzrechtlichen Prüfung unterziehen zu können.

3.4 Prüfung erkennungsdienstlicher Maßnahmen aufgrund einer Eingabe

Inhalt und Voraussetzungen einer erkennungsdienstlichen Behandlung zur Strafverfolgungsvorsorge (§ 81b Alt. 2 Strafprozeßordnung) habe ich oben unter Nr. 3.3 ausführlich dargelegt. Ergänzend weise ich auf die Beiträge in meinem 25. Tätigkeitsbericht 2012 unter Nr. 3.5.5 sowie in meinem 26. Tätigkeitsbericht 2014 unter Nr. 3.5.4

[23] Vgl. Lampe, in: Karlsruher Kommentar zum OWiG, 5. Aufl. 2018, § 46 Rn. 27.

hin. Das Thema war im Berichtszeitraum auch Gegenstand einer Datenschutzbeschwerde:

Ein bislang in keiner Weise strafrechtlich in Erscheinung getretenes Ehepaar wurde beim Spazierengehen in eine Auseinandersetzung mit einer Hundehalterin verwickelt und in diesem Zusammenhang von der Polizei erkennungsdienstlich behandelt. Dem Ehepaar wurde zur Last gelegt, die Hundehalterin mit einem Taschenmesser sowie mit einem Pfefferspray bedroht (§ 241 Strafgesetzbuch) zu haben. Dies bestritten beide und sie trugen vor, Messer und Spray nur zur Abwehr des nicht angeleinten Hundes bereitgehalten zu haben. Die mit dem Vorgang befasste Staatsanwaltschaft stellte die strafrechtlichen Ermittlungen ein, da der Tatnachweis nicht mit der für eine Anklageerhebung erforderlichen Sicherheit geführt werden konnte. Gleichwohl lehnte die Polizei eine von beiden Ehepartnern beantragte Löschung der personenbezogenen Daten ab, die aufgrund der erkennungsdienstlichen Maßnahmen gespeichert worden waren.

Bei meiner datenschutzrechtlichen Prüfung des Falles konnte ich nicht ernsthaft erkennen, woraus sich vorliegend die Gefahr begründen sollte, dass die Eheleute zukünftig strafrechtlich in Erscheinung treten könnten. Mit dem Hinweis, dass eine erkennungsdienstliche Speicherung zu präventiv-polizeilichen Zwecken eine Wiederholungsgefahr voraussetzt, konnte ich schließlich die von den Beschwerdeführern erstrebte Löschung erreichen.

3.5 Anlasslose Überprüfung von Speicherungen im Integrationsverfahren der Bayerischen Polizei (IGVP)

Ein wichtiger Bestandteil für die alltägliche Arbeit der Polizei ist das Integrationsverfahren der Bayerischen Polizei (IGVP), welches vor allem der Vorgangsverwaltung beim jeweiligen Polizeiverband dient. In diesem System werden wesentliche Vorgänge dokumentiert, die bei der polizeilichen Arbeit anfallen. Die Bedeutung von IGVP-Speicherungen hat sich in den letzten Jahren stark verändert. Aufgrund der Verfügbarkeit der dort gespeicherten Informationen für die gesamte Bayerische Polizei und der Funktion dieser Informationen als Quelldaten für andere polizeiliche Datenbanken erlangt das IGVP – verbunden mit der stetig fortschreitenden automatisierten Datenverarbeitung – zunehmend einen höheren Verwendungswert.

Unter anderem aus diesem Grund habe ich im Berichtszeitraum bei einem Präsidium eine anlasslose Prüfung von IGVP-Speicherungen vorgenommen und dabei mein Augenmerk insbesondere auf die Einhaltung der Aussonderungsfristen gelegt.

Gemäß Art. 53 Abs. 5 Satz 2 Polizeiaufgabengesetz (PAG) in Verbindung mit den einschlägigen Verwaltungsvorschriften beträgt die Aufbewahrungsdauer von Speicherungen im IGVP in der Regel fünf Jahre.

Leider konnte ich bei meiner Prüfung immerhin sieben Fälle feststellen, bei denen eine Aufbewahrung über fünf Jahre hinaus stattfinden sollte, obwohl kein Grund vorlag, von der Regelfrist abzuweichen.

Die Gründe hierfür waren unterschiedlich: In fünf Fällen wurden schlicht falsche Aussonderungsfristen eingetragen. In einem Fall wurde vergessen, den Vorgang abzuschließen, was zur Folge hatte, das die Aufbewahrungsfrist von fünf Jahren nie zu laufen begann. Bei einer Speicherung kam es mutmaßlich aufgrund eines technischen Fehlers zu einer Verlängerung der Speicherungsfrist.

Alle sieben Vorgänge wurden auf meinen Hinweis hin gelöscht. Das betroffene Polizeipräsidium hat erfreulicherweise umfassende Sensibilisierungs- und Schulungsmaßnahmen zugesagt. Auch habe man innerhalb des Präsidiums auf die in den letzten Jahren stark veränderte Bedeutung von IGVP-Speicherungen hingewiesen, wie auch auf die Auswirkungen der Mängel bei IGVP-Speicherungen sowohl auf die Datenschutzrechte der gespeicherten Personen als auch auf die Qualität der polizeilichen Datenhaltung.

3.6 Speicherung im Staatsschutz-Informationssystem wegen Teilens eines Medienberichts in einem Sozialen Netzwerk

Wie schnell man durch das Teilen von internetverfügbaren Inhalten in Sozialen Netzwerken nicht nur die Aufmerksamkeit anderer Nutzerinnen und Nutzer auf sich ziehen, sondern auch die des polizeilichen Staatsschutzes und sich am Ende als beschuldigte Person in polizeilichen Datenbanken wiederfinden kann, möchte ich in diesem Beitrag aufzeigen.

Bei einer datenschutzrechtlichen Prüfung stieß ich auf zwei Speicherungen im Staatsschutz-Informationssystem. Die Sachverhalte, wegen derer die beiden betroffenen Personen in dieser Datei gespeichert wurden, waren ähnlich: Beide hatten jeweils in einem Sozialen Netzwerk unabhängig voneinander einen im Internet verfügbaren Beitrag einer öffentlich-rechtlichen Rundfunkanstalt geteilt. Auf einem Foto in diesem Beitrag war die Fahne einer Gruppierung abgebildet, die nach Erkenntnissen des Bundesministeriums des Innern und für Heimat einer verbotenen Organisation nahestehen soll.

Vor diesem Hintergrund handelte es sich bei der Fahne möglicherweise um ein Kennzeichen, dessen Verwendung oder Verbreitung ein Verbot nach § 20 Abs. 1 Satz 1 Nr. 5 Vereinsgesetz entgegenstand. Diesen Verbotstatbestand konnte die gespeicherte Person allerdings nicht verwirklichen. Zum einen ist Medienberichterstattung über die betreffende Gruppierung nach Maßgabe von § 20 Satz 2 in Verbindung mit § 9 Abs. 1 Satz 2 Vereinsgesetz von dem Verbot ausgenommen (sogenannte Sozialadäquanzklausel); dies gilt jedenfalls auch für die zielgleiche „Verlinkung“ eines entsprechenden Medienberichts durch Dritte. Zum anderen setzt ein strafbarer Verstoß gegen § 20 Abs. 1 Satz 1 Nr. 5 Vereinsgesetz ein vorsätzliches Handeln voraus. Vereinfacht gesagt bedeutet dies, dass die Täterin oder der Täter sich nach der genannten Vorschrift nur dann strafbar macht, wenn sie oder er die verbotene Organisation mit ihrer oder seiner Handlung auch unterstützen möchte.

Anhaltspunkte dafür, dass die beiden betroffenen Personen etwas anderes tun wollten als die Verbreitung des Medienberichts zu fördern, waren für mich nicht ersichtlich; es bestanden im Übrigen keinerlei Anhaltspunkte, dass die Personen mit ihrem Handeln die verbotene Organisation unterstützen wollten.

Es verwundert daher nicht, dass die Strafverfahren gegen die beiden Personen jeweils eingestellt wurden, weil ihnen eine rechtswidrige Tat nicht vorzuwerfen war (vgl. § 170 Abs. 2 Strafprozeßordnung).

Vor diesem Hintergrund habe ich das betroffene Polizeipräsidium gebeten, die beiden Speicherungen im Staatsschutz-Informationssystem zu löschen. Letztlich folgte man dort meiner Auffassung, dass die von mir herausgegriffenen Fälle nicht dem Bereich der politisch motivierten Kriminalität, sondern dem Bereich des legalen Nutzungsverhaltes in Sozialen Netzwerken zuzuordnen waren.

Wichtig ist mir im Zusammenhang mit diesem Vorgang vor allem der Hinweis, mit welchen auch alltäglichen Handlungen man die Aufmerksamkeit von Strafverfolgungsbehörden auf sich lenken kann – und sei es nur, dass man einen Online-Beitrag teilt, den seriöse Medien selbst zum Teilen angeboten haben.

3.7 Prüfung Antiterrordatei (ATD)

Seit 2007 werden in der Antiterrordatei (ATD) Erkenntnisse von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder aus dem Bereich des internationalen, vor allem islamistisch motivierten Terrorismus verarbeitet. Das Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz – ATDG), das die Voraussetzungen der betreffenden Datenverarbeitungen regelt, enthält auch die Verpflichtung, mindestens alle zwei Jahre „die Durchführung des Datenschutzes" zu kontrollieren.

Auch in diesem Berichtszeitraum habe ich eine entsprechende Vor-Ort-Prüfung beim Bayerischen Landesamt für Verfassungsschutz durchgeführt. Konkret nahm ich eine Mitteilung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu drei konkreten Abfragen des Bayerischen Landesamts für Verfassungsschutz in der ATD zum Anlass. Darüber hinaus habe ich stichprobenartig die originären Speicherungen von sogenannten „Hauptpersonen" und hierzu verknüpften „Kontaktpersonen" durch das Bayerische Landesamt für Verfassungsschutz überprüft. Als sogenannte „Kontaktperson" im Sinne des Antiterrordateigesetzes gilt jemand, bei dem tatsächliche Anhaltspunkte vorliegen, dass er oder sie mit einer „Hauptperson" nicht nur flüchtig oder in zufälligem Kontakt in Verbindung steht und durch ihn oder sie weiterführende Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus zu erwarten sind (siehe § 3 Abs. 2 Satz 1 ATDG).

Meine Prüfung gab keinen Anlass zu Beanstandungen. Die Abrufvoraussetzungen des § 5 Abs. 1 Satz 1 ATDG waren in allen drei vom Bundesbeauftragten mitgeteilten Fällen gegeben. Der Abruf erfolgte auch durch die zuständige Stelle des Bayerischen Landesamts für Verfassungsschutz. Dies ließ sich anhand von Protokolldaten nachvollziehen. Auch die von mir geprüften originären Speicherungen des Bayerischen Landesamtes für Verfassungsschutz entsprachen den gesetzlichen Vorgaben. Zugehörige Kontaktpersonen waren nicht gespeichert.

3.8 Prüfung Rechtsextremismus-Datei (RED)

Seit 2012 werden Daten zur Bekämpfung des gewaltbezogenen Rechtsextremismus in der Rechtsextremismus-Datei (RED) gespeichert. Gesetzliche Grundlage hierfür ist das Gesetz zur Errichtung einer standardisierten zentralen Datei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus (Rechtsextremismus-Datei-Gesetz – RED-G), das hinsichtlich der Rahmenbedingungen vergleichbar mit dem Antiterrordateigesetz (siehe Nr. 3.7) ist und ebenfalls mindestens alle zwei Jahre datenschutzrechtliche Pflichtprüfungen vorsieht.

Dem Rechnung tragend habe ich im Berichtszeitraum vor Ort beim Bayerischen Landesamt für Verfassungsschutz Datensätze geprüft, die von dort in die Rechtsextremismus-Datei eingespeichert wurden. Entsprechend dem Vorgehen bei der Antiterrordatei wurden auch hier stichprobenartig die Speicherungen von sogenannten

„Hauptpersonen“ und hierzu verknüpften „Kontaktpersonen“ geprüft. Im Rahmen dieser Prüfung konnte ich mich zum Beispiel bei einer Person vom Vorliegen der Speichervoraussetzungen des § 2 Satz 1 Nr. 2 REDG überzeugen (wiederholtes Verbreiten von Propagandamitteln verfassungswidriger Organisationen, Sprengstoffdelikte, Haftstrafe). Bei einer anderen Hauptperson war ich mir nach Einsichtnahme in die staatsanwaltschaftliche Ermittlungsakte ebenfalls sicher, dass die Voraussetzungen des § 2 Satz 1 Nr. 1 Buchst. b REDG vorlagen.

Insgesamt waren auch bei der RED die geprüften Speicherungen durch das Bayerische Landesamt für Verfassungsschutz nicht zu beanstanden.

4 Justiz

4.1 Beanstandung einer Staatsanwaltschaft wegen unterbliebener Anhörung vor Gewährung einer Akteneinsicht

Eine Bürgerin, die sich hilfesuchend an mich wandte, war zunächst Beschuldigte in mehreren Ermittlungsverfahren, die auf Anzeigen verschiedener Personen zurückgingen. Diese Verfahren wurden von der zuständigen Staatsanwaltschaft zu einem Verfahren verbunden. Letztlich wurde dieses Ermittlungsverfahren wegen nicht ausschließbarer Schuldunfähigkeit der Beschuldigten gemäß § 170 Abs. 2 Strafprozeßordnung (StPO) eingestellt.

Einer verletzten Person wurde nach Abschluss der Ermittlungen und nach Einstellung des Ermittlungsverfahrens vollumgänglich und uneingeschränkt Akteneinsicht in die Ermittlungsakte – und damit auch in diese Person nicht betreffende Bestandteile – sowie ferner in ein forensisch-psychiatrisches Gutachten zur Frage der Schuldunfähigkeit der Beschuldigten (vgl. §§ 20, 21 Strafgesetzbuch – StGB) gewährt. Dieses forensisch-psychiatrische Gutachten enthielt auch eine auszugsweise Schilderung des Lebens samt Familien- und Krankengeschichte der Beschuldigten.

Die Staatsanwaltschaft trug vor, dass die Akteneinsicht auf der Rechtsgrundlage des § 406e StPO gewährt worden sei. Die Gewährung von Akteneinsicht sei zeitgleich mit der Einstellung des Ermittlungsverfahrens gemäß § 170 Abs. 2 StPO wegen nicht ausschließbarer Schuldunfähigkeit verfügt worden. Grundlage für die Entscheidung einer Einstellung sei das Gutachten gewesen. Eine Anhörung der Beschwerdeführerin vor Gewährung der Akteneinsicht sei deshalb nicht erfolgt, da der verletzten Person in einem engen zeitlichen Zusammenhang mit der Übersendung der Einstellungsentscheidung eine eigene Prüfung der Einstellungsgründe ermöglicht werden sollte.

Die Staatsanwaltschaft teilte ferner mit, dass im Rahmen der Einstellungsentscheidung neben der Frage einer (nicht ausschließbaren) Schuldunfähigkeit der Beschuldigten auch zu prüfen gewesen sei, ob im Wege eines Sicherungsverfahrens eine Unterbringung in einem psychiatrischen Krankenhaus nach § 63 StGB anzustreben sei. Hierzu befänden sich im letzten Absatz der Einstellungsgründe Ausführungen, wonach in der Gesamtbetrachtung aller angezeigten Handlungen der Beschuldigten der Bereich der mittleren Kriminalität nicht erreicht gewesen sei, weshalb im Ergebnis kein Sicherungsverfahren durchzuführen gewesen sei. Man sei davon ausgegangen, dass die verletzte Person hierzu im Rahmen einer Beschwerde hätte geltend machen können, dass die Voraussetzungen einer Unterbringung in einem psychiatrischen Krankenhaus vorlägen. Zu einer solchen Bewertung habe es allerdings der Kenntnis aller angezeigten Handlungen bedurft, so dass eine Beschränkung der Akteneinsicht auf einzelne Aktenbestandteile nicht angezeigt gewesen sei.

Nach datenschutzrechtlicher Prüfung dieses Sachverhalts kam ich zu dem Ergebnis, dass die Gewährung von Akteneinsicht in die vollständige Ermittlungsakte samt Gutachten unzulässig war und die Beschwerdeführerin in ihren Datenschutzrechten verletzte. Daher habe ich die Maßnahme der Staatsanwaltschaft gemäß Art. 16 Abs. 4 BayDSG förmlich beanstandet. Ausschlaggebend für die Beanstandung war insbe-

sondere, dass die Akteneinsicht nach § 406e Abs. 1 bis 3 StPO rechtsfehlerhaft gewährt wurde, weil die Beschuldigte vor Gewährung der Akteneinsicht nicht angehört worden war.

Zwar konnte ich im konkreten Fall die Argumente der Staatsanwaltschaft zur Gewährung einer vollumfänglichen Akteneinsicht sowohl in die Ermittlungsakte als auch in das forensisch-psychiatrische Gutachten im Grundsatz nachvollziehen.

Jedoch verlangt die Rechtsprechung zu § 406e StPO, dass die betroffene Person vor einer Akteneinsichtsgewährung anzuhören ist; sie stützt dies auf eine entsprechende Anwendung von § 33 Abs. 3 StPO, das Rechtsstaatsprinzip sowie das Gebot der Sachaufklärung.[24] Von einer Anhörung kann entsprechend § 33 Abs. 4 StPO nur dann abgesehen werden, wenn sie den Zweck der Anordnung gefährden würde oder wenn der Anhörung tatsächliche Gründe entgegenstehen, beispielsweise der Aufenthaltsort der beschuldigten Person unbekannt ist. Keiner dieser Fälle war vorliegend einschlägig. Die Staatsanwaltschaft begründete die unterbliebene Anhörung damit, dass der verletzten Person zeitnah zur Übersendung der Einstellungsentscheidung eine eigene Prüfung der Gründe ermöglicht werden sollte. In dieser Begründung kann ich keine Ausnahme nach § 33 Abs. 4 StPO feststellen. Mangels Anhörung konnte die betroffene Person auch keine Stellung zur Gewährung einer Einsicht – insbesondere in das Gutachten – nehmen.

Die Staatsanwaltschaft räumte schließlich ein, dass dieses durch die Rechtsprechung entwickelte Recht auf Anhörung der beschuldigten Person vor einer Akteneinsicht an verletzte Personen vorliegend nicht beachtet worden sei. Auf die Beachtung dieses Rechts seien nun die Dezernentinnen und Dezernenten bereits mündlich hingewiesen worden. In Ergänzung würden alle mit der Gewährung von Akteneinsicht befassten Mitarbeiterinnen und Mitarbeiter nochmals schriftlich hierfür sensibilisiert.

Vor allem bei der Gewährung von Einsicht in forensisch-psychiatrische Gutachten, die überwiegend besondere Kategorien personenbezogener Daten enthalten und tiefe Einblicke in das Leben eines Menschen samt Krankheitsgeschichte zulassen können, ist sorgfältig zu prüfen, ob Einsicht gewährt werden darf. Ferner ist sicherzustellen, dass bei Gewährung von Akteneinsicht gemäß § 406e StPO die betroffene Person im Rahmen einer Anhörung ihren Rechten nachkommen kann und gegebenenfalls auch Gründe vorbringen kann, weshalb keine Einsicht gewährt werden soll beziehungsweise gewährt werden darf. Der Staatsanwaltschaft obliegt dann eine Abwägung der Interessen der verletzten Person mit den Interessen der beschuldigten Person.

4.2 Unzulässige Videobeobachtung eines Untersuchungsgefangenen

Eine Justizvollzugsanstalt meldete mir nach Art. 33 DSGVO in Verbindung mit Art. 205 Abs. 3 Bayerisches Strafvollzugsgesetz (BayStVollzG), Art. 28 Abs. 1, Abs. 2 Satz 1 Nr. 3, Abs. 2 Satz 2 BayDSG folgenden Fall: Versehentlich wurde ein Untersuchungsgefangener für knapp zwei Wochen in seinem Einzelhaftraum videoüberwacht (Live-Beobachtung), ohne dass die dafür erforderlichen rechtlichen Voraussetzungen vorlagen. Dieses Versehen fiel erst auf, nachdem der Untersuchungsgefangene in eine andere Abteilung verlegt wurde.

[24] Bundesverfassungsgericht, Beschluss vom 30. Oktober 2016, 1 BvR 1766/14, BeckRS 2016, 55370.

Ursächlich für den Fehler war, dass der Untersuchungsgefangene aus gesundheitlichen Gründen während der COVID-19-Pandemie in einem Einzelhaftraum untergebracht werden musste. Der einzig verfügbare Einzelhaftraum in der Zugangsabteilung war jedoch derjenige, welcher üblicherweise für Personen vorgesehen ist, die als besondere Sicherungsmaßnahme videoüberwacht werden. Bei der Belegung dieses Einzelhaftraums mit dem betroffenen Untersuchungsgefangenen war schlicht übersehen worden, die Videoüberwachung zu unterbinden.

Die Justizvollzugsanstalt teilte mir mit, sie habe den betroffenen Untersuchungsgefangenen über den Datenschutzverstoß informiert und die Bediensteten der betroffenen Abteilung ausdrücklich auf die Einhaltung datenschutzrechtlicher Bestimmungen, insbesondere auf die gesetzlichen Voraussetzungen der Videoüberwachung als besondere Sicherungsmaßnahme, hingewiesen. Ferner entwickelte die Justizvollzugsanstalt eine Abdeckungsvorrichtung für die Videoüberwachungsanlage, um den Einzelhaftraum im Einzelfall – ohne Vorliegen der Voraussetzungen einer besonderen Sicherungsmaßnahme – künftig belegen zu können.

Justizvollzugsanstalten können gegenüber sich in Strafhaft und in Untersuchungshaft befindenden Personen verschiedene, sogenannte besondere Sicherungsmaßnahmen anordnen, wenn nach ihrem Verhalten oder aufgrund ihres seelischen Zustands in erhöhtem Maß Fluchtgefahr oder die Gefahr von Gewalttätigkeiten gegen Personen oder Sachen oder die Gefahr des Selbstmords oder der Selbstverletzung besteht. Gleiches gilt für Jugendarrestanstalten und Einrichtungen für Sicherungsverwahrung.

Als eine besondere Sicherungsmaßnahme kann die ständige Beobachtung, auch mit technischen Mitteln, angeordnet werden. Rechtsgrundlage hierfür ist Art. 96 Abs. 1 und Abs. 2 Nr. 2 BayStVollzG gegebenenfalls in Verbindung mit Art. 27 Bayerisches Untersuchungshaftvollzugsgesetz beziehungsweise Art. 22 Abs. 2 Bayerisches Jugendarrestvollzugsgesetz. Im Rahmen der Sicherungsverwahrung findet sich die Rechtsgrundlage in Art. 74 Abs. 1 und Abs. 2 Nr. 2 Bayerisches Sicherungsverwahrungsvollzugsgesetz.

Wird als besondere Sicherungsmaßnahme eine ständige Beobachtung mit technischen Mitteln angeordnet, so ist zu berücksichtigen, dass beim Einsatz technischer Mittel, beispielsweise in Form einer Videokamera, keine Aufzeichnung von Videosequenzen erfolgen darf. Zulässig ist allein eine Live-Beobachtung.

Ich habe den gemeldeten Vorfall zum Anlass genommen, um stichprobenartig weitere zehn Justizvollzugsanstalten zu dieser Thematik zu prüfen. Die Justizvollzugsanstalten wurden um Mitteilung gebeten, ob in der jeweiligen Anstalt eine Nutzung der videoüberwachten Einzelhafträume erfolgte, um aufgrund der Auswirkungen der COVID-19-Pandemie auf die Unterbringungssituation reagieren und eine vermehrte Unterbringung in Einzelhafträumen ermöglichen zu können, ohne dass die Voraussetzungen für eine besondere Sicherungsmaßnahme vorlagen. Ferner wurden die Justizvollzugsanstalten im Falle der Bejahung dieser Frage gebeten, mitzuteilen, welche (technischen) Vorkehrungen getroffen wurden, um in diesen Fällen eine Videobeobachtung auszuschließen.

Alle zehn Justizvollzugsanstalten teilten mit, dass eine Nutzung der videoüberwachten Einzelhafträume ohne Vorliegen der Voraussetzungen für eine besondere Sicherungsmaßnahme nicht erfolgte – auch unabhängig von der Unterbringungssituation während der COVID-19-Pandemie. Eine Justizvollzugsanstalt teilte mir überdies ergänzend mit, dass die Kameras mit blickdichten Abdeckhauben für den Fall bedeckt werden, dass eine Belegung des Einzelhaftraums ohne gleichzeitige Anordnung einer

ständigen Beobachtung erfolgt. So ist zugleich für die Personen, die in einem solchen Einzelhaftraum untergebracht werden, nachvollziehbar und prüfbar, dass eine Beobachtung mit technischen Mitteln ausgeschlossen ist.

4.3 Nutzung privater Mobiltelefone für erkennungsdienstliche Maßnahmen im Maßregelvollzug

Nach Art. 34 Bayerisches Maßregelvollzugsgesetz (BayMRVG), Art. 205 Abs. 3 Bayerisches Strafvollzugsgesetz (BayStVollzG), Art. 2 Satz 1 BayDSG, Art. 28 Abs. 2 Satz 2 BayDSG in Verbindung mit Art. 33 DSGVO besteht auch im Bereich des Maßregelvollzugs eine Pflicht des Verantwortlichen, der Aufsichtsbehörde Verletzungen des Schutzes personenbezogener Daten zu melden.

Über mein Online-Formular hat mich eine solche Meldung einer forensischen Klinik erreicht. Nach Art. 28 BayMRVG können zur Sicherung des Vollzugs der Unterbringung, zur Identitätsfeststellung und zur Aufrechterhaltung der Sicherheit oder des geordneten Zusammenlebens in der Maßregelvollzugseinrichtung von Patientinnen und Patienten Lichtbilder aufgenommen werden. In dem gemeldeten Fall nutzte ein Mitarbeiter dafür einfachheitshalber ein privates Handy; die Bilder ließ er anschließend der Klinik über seine private E-Mail-Adresse zukommen.

Wie ich bereits in meinem 25. Tätigkeitsbericht 2012 unter Nr. 7.3 dargelegt habe, halte ich die Nutzung privater Endgeräte im Krankenhaus grundsätzlich für nicht zulässig. Auch wenn der Mitarbeiter beauftragt war, erkennungsdienstliche Aufnahmen für den Maßregelvollzug anzufertigen und er nach dem Versand an die Klinik selbständig die besagte E-Mail sowie die Lichtbilder von seinem privaten Handy gelöscht hatte, hat er das Verbot der Klinik missachtet, private Endgeräte zu nutzen. Aus diesem Grund wurde er von der Klinik arbeitsrechtlich ermahnt sowie datenschutzrechtlich geschult.

Der Vorfall unterstreicht nochmals, wie wichtig das Zur-Verfügung-Stellen klinikeigener Geräte und die regelmäßige Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für datenschutzrechtliche Belange ist.

4.4 Protokollierung von Zugriffen in der Haftdatei IT-Vollzug

Die Haftdatei IT-Vollzug ist ein Fachverfahren für die Datenverarbeitung im bayerischen Justizvollzug. Sie dient der Erfassung und Dokumentation und der Daten von Gefangenen und Sicherungsverwahrten; sie unterstützt die Bediensteten in den Justizvollzugsanstalten bei der Durchführung vollzuglicher Maßnahmen und bei Verwaltungsvorgängen durch die Bereitstellung von Informationen.

Bedienstete der Justizvollzugsanstalten haben dabei in der Regel nur Zugriff auf die Daten derjenigen Gefangenen, die sich in der jeweiligen Anstalt befinden. Eine bayerweite Personensuche in IT-Vollzug ist nur ausgewählten Personengruppen für dienstlich notwendige Tätigkeiten vorbehalten. Unter diese ausgewählten Personengruppen fallen beispielsweise die Leiterinnen und Leiter der Justizvollzugsanstalten, aber auch Angehörige der allgemeinen Justiz wie Staatsanwältinnen und Staatsanwälte. Im Rahmen der bayernweiten Personensuche in IT-Vollzug wird deshalb zwischen sogenannten internen und externen Nutzerinnen und Nutzern unterschieden. Während Bedienstete der Justizvollzugsanstalten sogenannte interne Nutzerinnen und Nutzer sind, werden Bedienstete der allgemeinen Justiz als externe Nutzerinnen

und Nutzer angesehen. Ihnen wird dabei regelmäßig ein Zugriff in abgestuftem Umfang gewährt.

In IT-Vollzug wurden zunächst nur die Eingabe, die Änderung sowie die Löschung von Daten protokolliert. Der lesende Zugriff interner Nutzerinnen und Nutzer wurde nicht protokolliert. Hingegen erfolgte und erfolgt eine Protokollierung lesender Zugriff externer Nutzerinnen und Nutzer bei der bayernweiten Personensuche in IT-Vollzug.

Im Rahmen einer datenschutzrechtlichen Prüfung der Protokollierung von Verarbeitungsvorgängen in IT-Vollzug machte ich das Bayerische Staatsministerium der Justiz auf die mit Wirkung vom 1. August 2018 eingeführte gesetzliche Protokollierungspflicht in Art. 199 Abs. 3 Satz 1 Nr. 3 Bayerisches Strafvollzugsgesetz (BayStVollzG) aufmerksam. Diese Regelung sieht seit dem 1. August 2018 – mit der Möglichkeit der Inanspruchnahme einer Übergangsfrist bis 6. Mai 2023 (Art. 205 Abs. 4 BayStVollzG) – vor, dass jeder Abruf von personenbezogenen Daten in IT-Vollzug zu protokollieren ist. Die Praxis, nur Abrufe durch externe Nutzerinnen und Nutzer zu protokollieren, genügt daher nicht den neuen gesetzlichen Anforderungen.

Das Justizministerium teilte mir daraufhin mit, dass man zwischenzeitlich eine Protokollierung sämtlicher lesender und verarbeitender Zugriffe vornehme.

Im Verlauf der Prüfung wies ich auch darauf hin, dass die Protokolle von Abrufen auch die für den Abruf maßgeblichen Gründe nennen, Datum und Uhrzeit des Abrufs enthalten und, soweit möglich, die Feststellung der Identität der abrufenden Person sowie des Empfängers ermöglichen müssen (Art. 199 Abs. 3 Satz 2 BayStVollzG). Zwischenzeitlich berichtete das Justizministerium, dass diesbezüglich die technische Programmierung und Umsetzung erfolgt sei.

4.5 Dokumentation von Lichtbildanforderungen im Rahmen von Verkehrsordnungswidrigkeitenverfahren

Die Ordnungswidrigkeitenbehörden, die für die Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten zuständig sind, dürfen im Rahmen der Ermittlung der betroffenen Fahrzeugführerin oder des betroffenen Fahrzeugführers Lichtbilder von den Personalausweis- und Passbehörden zum Abgleich anfordern. Voraussetzung für die Zulässigkeit der Lichtbildanforderung ist stets, dass die gesetzlichen Voraussetzungen hierfür vorliegen. In meinem 30. Tätigkeitsbericht 2020 unter Nr. 2.4.2 habe ich die Rechtslage hierzu ausführlich dargestellt.

Dürfen Ordnungswidrigkeitenbehörden bei den Personalausweis- und Passbehörden Daten, insbesondere Lichtbilder, anfordern, müssen sie den Anlass des Ersuchens und die Herkunft der übermittelten Daten und Unterlagen aktenkundig machen, siehe § 24 Abs. 3 Satz 3 Personalausweisgesetz (PAuswG) und § 22 Abs. 3 Satz 3 Passgesetz (PassG).

§ 24 PAuswG
Verwendung im Personalausweisregister gespeicherter Daten
[...]
(3) Die ersuchende Behörde trägt die Verantwortung dafür, dass die Voraussetzungen des Abs. 2 vorliegen. Ein Ersuchen nach Abs. 2 darf nur von Bediensteten gestellt werden, die vom Behördenleiter dazu besonders ermächtigt sind. Die ersuchende Behörde hat den Anlass des Ersuchens und die Herkunft der übermittelten Daten und Unterlagen zu dokumentieren. Wird die Personalausweisbehörde vom Bundesamt für

Verfassungsschutz, den Landesbehörden für Verfassungsschutz, dem Militärischen Abschirmdienst, dem Bundesnachrichtendienst, dem Bundeskriminalamt oder dem Generalbundesanwalt oder der Generalbundesanwältin um die Übermittlung von Daten ersucht, so hat die ersuchende Behörde den Familiennamen, die Vornamen und die Anschrift des Betroffenen unter Hinweis auf den Anlass der Übermittlung aufzuzeichnen. Die Aufzeichnungen sind gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Übermittlung folgt, zu vernichten.
[...]

Im Rahmen meiner Prüfungstätigkeit habe ich fünf große Zweckverbände, die für die kommunale Verkehrsüberwachung zuständig sind, um Erläuterung ihrer Dokumentation gemäß § 24 Abs. 3 Satz 3 PAuswG und § 22 Abs. 3 Satz 3 PassG gebeten.

Die fünf Zweckverbände kamen dieser Aufforderung nach. Regelmäßig wird zur Anforderung von Lichtbildern ein Vordruck genutzt, den die Zweckverbände an die zuständige Personalausweis- oder Passbehörde senden. Ein Abdruck dieser Anfrage wird zur jeweiligen Akte genommen. Die Vordrucke dokumentieren in der Regel, auf welcher Rechtsgrundlage und aus welchen Gründen ein Lichtbild der betroffenen Person angefordert wird. Diese Vordrucke legten mir die Zweckverbände vor. Daneben geht aus den Anforderungen und den entsprechenden Antworten der Personalausweis- und Passbehörden hervor, woher die übermittelten Daten stammen.

Im Ergebnis konnte ich feststellen, dass alle fünf Zweckverbände die Dokumentationspflichten gesetzeskonform einhalten. Die zur jeweiligen Akte genommene Anforderung samt entsprechender Antwort sind geeignet, die Dokumentationspflicht aus § 24 Abs. 3 Satz 3 PAuswG und § 22 Abs. 3 Satz 3 PassG praktisch umzusetzen. Allerdings waren die Vordrucke für Auskunftsersuchen – Lichtbildanforderungen – teils nicht (mehr) gesetzeskonform ausgestaltet, da beispielsweise veraltete Rechtsgrundlagen angegeben waren.

Die einzelnen Zweckverbände wurden im Hinblick auf die Vordrucke und den jeweiligen Anpassungsbedarf um Überarbeitung gebeten. Dem kamen die Zweckverbände nach und legten mir die überarbeiteten Vordrucke anschließend zur Prüfung vor. Sämtliche mir vorgelegten Vordrucke entsprechen nun vollständig den gesetzlichen Anforderungen.

5 Allgemeine Innere Verwaltung

5.1 Datenverarbeitung bei Gutachterausschüssen zur Ermittlung von Grundstückswerten und für sonstige Wertermittlungen

5.1.1 Sachverhalt

Im Berichtszeitraum wurde ich aufgrund einer Eingabe mit folgendem Sachverhalt befasst: Ein Bürger hat nach dem Erwerb eines Grundstücks einen Fragebogen von einem Gutachterausschuss gemäß § 192 Baugesetzbuch (BauGB) erhalten. Gutachterausschüsse werden als selbständige und unabhängige Einrichtung mit einer Geschäftsstelle zur Ermittlung von Grundstückswerten und für sonstige Wertermittlungen gebildet (§ 192 Abs. 1, Abs. 4 BauGB). Sie bestehen aus einer oder einem Vorsitzenden und ehrenamtlichen weiteren Gutachterinnen und Gutachtern (vgl. § 192 Abs. 2 BauGB). Der Gutachterausschuss erstattet Gutachten über den Verkehrswert von bebauten und unbebauten Grundstücken sowie Rechten an Grundstücken (§ 193 BauGB). Zudem führt er eine Kaufpreissammlung, wertet sie aus und ermittelt Bodenrichtwerte und sonstige zur Wertermittlung erforderliche Daten (§ 193 BauGB).

Mit dem Fragebogen wurden neben Informationen zum Kaufobjekt selbst auch der Name des Grundstückserwerbers und seine Adress-/Kontaktdaten vom Gutachterausschuss erhoben. Der Bürger bat mich um die Prüfung der Datenverarbeitung des Gutachterausschusses. Dem bin ich nachgekommen und hebe folgende Punkte von allgemeinem Interesse hervor:

5.1.2 Gutachterausschuss für Grundstückswerte als Verantwortlicher

Der Gutachterausschuss ist für die von ihm veranlasste Verarbeitung personenbezogener Daten – insbesondere Namen und Adressdaten der Grundstückseigentümer und der Vertragsparteien des Immobiliengeschäfts – als sonstige öffentliche Stelle gemäß Art. 1 Abs. 1 BayDSG Verantwortlicher nach Art. 4 Nr. 7 DSGVO. Maßgeblich für diese Einschätzung sind folgende Erwägungen:

Verantwortlicher ist nach Art. 4 Nr. 7 DSGVO 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. Wie aus dieser gesetzlichen Definition folgt, muss der Verantwortliche nicht selbst eine natürliche oder juristische Person sein, sondern kann auch eine Behörde, Einrichtung oder andere Stelle sein. In Anlehnung an den verwaltungsverfahrensrechtlichen Behördenbegriff[25] kommt es somit vor allem darauf an, dass eine Einrichtung vorliegt, die eine gewisse organisatorische Selbstständigkeit aufweist. Das heißt, sie muss vom Wechsel der Amtsinhaber unabhängig und nach der einschlägigen Zuständigkeitsregelung berufen sein, unter eigenem Namen nach außen hin eigenständige

[25] Vgl. Bundesverwaltungsgericht, Urteil vom 24. Januar 1991, 2 C 16/88, NJW 1991, 2980; Schmitz, in: Stelkens/Bonk/Sachs, Verwaltungsverfahrensgesetz, 9. Aufl. 2018, § 1 Rn. 238 ff.

Aufgaben der öffentlichen Verwaltung wahrzunehmen.[26] Als Verantwortlicher beziehungsweise öffentliche Stelle kommen daher grundsätzlich nicht in Betracht bloße nach außen nicht in Erscheinung tretende Arbeitseinheiten von Behörden wie Referate in Ministerien, Dezernate in nachgeordneten Behörden, Projektgruppen, Beauftragte und dergleichen.[27]

Beim Gutachterausschuss handelt es sich um ein Kollegialorgan, das aus einer oder einem Vorsitzenden, ihren oder seinen Stellvertreterinnen oder Stellvertretern und weiteren ehrenamtlichen Gutachterinnen und Gutachtern besteht (vgl. § 192 Abs. 1, Abs. 2 BauGB, § 2 Verordnung über die Gutachterausschüsse, die Kaufpreissammlungen und die Bodenrichtwerte nach dem Baugesetzbuch — Gutachterausschussverordnung – BayGaV). Der Gutachterausschuss ist nach dem Gesetz selbstständig und unabhängig (§ 192 Abs. 1 BauGB). Das heißt, er steht außerhalb der Hierarchie der Organisationseinheit, bei der er angesiedelt ist — dem Landratsamt oder der kreisfreien Gemeinde (§ 1 Abs. 1 BayGaV) — unterliegt also nicht deren Weisungen.[28]

Der Gutachterausschuss verfügt über eine Geschäftsstelle (§ 192 Abs. 4 BauGB). Diese ist die Kreisverwaltungsbehörde (§ 9 Abs. 1 BayGaV). Dieser Umstand steht aber nicht einer Einordung des Gutachterausschusses als datenschutzrechtlich Verantwortlicher beziehungsweise öffentliche Stelle entgegen. Denn die Geschäftsstelle unterliegt bei der Führung der Geschäfte des Gutachterausschusses dessen Weisungen (§§ 9 Abs. 2 und 10 Abs. 2 Satz 1 BayGaV). Dementsprechend wird das Handeln der Geschäftsstelle dem Gutachterausschuss zugrechnet.[29]

Durch Gesetz sind dem Gutachterausschuss in §§ 192 ff. BauGB und § 1 Abs. 2, Abs. 3 BayGaV die Erfüllung öffentlicher Aufgaben in eigener Zuständigkeit zugewiesen. Als unabhängige Einrichtung tritt der Gutachterausschuss dabei im eigenen Namen nach außen auf. So ist es unter anderem eine Aufgabe der oder des Vorsitzenden, den Gutachterausschuss nach außen zu vertreten (§ 8 Abs. 1 BayGaV). Zu beachten ist auch, dass die einschlägigen Vorschriften, insbesondere mit datenschutzrechtlich relevantem Gehalt wie § 197 BauGB und §§ 10, 11 BayGaV, ausdrücklich den Gutachterausschuss oder dessen Geschäftsstelle adressieren, wodurch ebenfalls dessen (datenschutzrechtliche) Eigenständigkeit zum Ausdruck kommt. Hieraus folgt, dass der Gutachterausschuss Mittel und Zwecke der Datenverarbeitung bei der Erfüllung seiner Aufgaben nach § 192 ff. BauGB, § 1 Abs. 2 BayGaV bestimmt und mithin datenschutzrechtlich verantwortlich ist.

5.1.3 Datenschutzrechtliche Konsequenzen

Auswirkungen hat diese Einordnung vor allem bei der Benennung eines behördlichen Datenschutzbeauftragten, bei der Erfüllung von Informationspflichten und bei der Auftragsverarbeitung. Allerdings ist der den Gutachterausschuss treffende „Aufwand“ überschaubar.

26 Vgl. Schmitz, in: Stelkens/Bonk/Sachs, Verwaltungsverfahrensgesetz, 9. Aufl. 2018, § 1 Rn. 231, 238.

27 Vgl. Schmitz, in: Stelkens/Bonk/Sachs, Verwaltungsverfahrensgesetz, 9. Aufl. 2018, § 1 Rn. 240; siehe auch Wilde/Ehmann/Niese/Knoblauch, Datenschutz in Bayern, Stand 6/2018, Art. 1 BayDSG Rn. 12.

28 Vgl. Reidt, in: Battis/Krautzberger/Löhr, Baugesetzbuch, 14. Aufl. 2019, § 192 Rn. 2.

29 Vgl. Federwisch, in: Spannowsky/Uechtritz, Beck'scher Online-Kommentar Baugesetzbuch, Stand 11/2018, § 192 Rn. 16.

5.1.4 Behördlicher Datenschutzbeauftragter

Als öffentliche Stelle muss der Gutachterausschuss eine oder einen behördlichen Datenschutzbeauftragten benennen (Art. 37 Abs. 1 Buchst. a DSGVO). Als solche oder solcher können beispielsweise datenschutzrechtlich geschulte Bedienstete der Geschäftsstelle des Gutachterausschusses benannt werden. Es ist aber auch möglich, externe Datenschutzbeauftragte zu benennen (Art. 37 Abs. 6 Var. 2 DSGVO). So kann der Gutachterausschuss zum Beispiel den behördlichen Datenschutzbeauftragten oder die behördliche Datenschutzbeauftragte der Kreisverwaltungsbehörde, bei welcher der Gutachterausschuss angesiedelt ist, oder einen sonstigen (datenschutzrechtlich geschulten) Mitarbeiter oder eine Mitarbeiterin der Kreisverwaltungsbehörde als (externe) behördliche Datenschutzbeauftragte oder (externen) behördlichen Datenschutzbeauftragten benennen. Grundlage wäre dann ein Dienstleistungsvertrag (Geschäftsbesorgungsvertrag) zwischen dem Gutachterausschuss und der Kreisverwaltungsbehörde, welcher regelt, dass der Gutachterausschuss einen Bediensteten oder eine Bedienstete der Kreisverwaltungsbehörde als behördliche Datenschutzbeauftragte oder behördlichen Datenschutzbeauftragten benennen darf.

5.1.5 Informationspflichten nach Art. 13 DSGVO

Art 13 DSGVO begründet für den Verantwortlichen die Pflicht, den betroffenen Personen die in Art. 13 Abs. 1 und Abs. 2 DSGVO im Einzelnen aufgeführten Informationen zu geben, wenn personenbezogene Daten erhoben werden. Zu einer solchen Datenerhebung kommt es etwa, wenn der Gutachterausschuss gemäß § 197 BauGB Auskünfte oder Unterlagen von den betroffenen Personen einfordert.

Art. 13 Abs. 1 Buchst. a DSGVO sieht vor, dass die personenbezogene Daten erhebende öffentliche Stelle die betroffene Person insbesondere über den Namen und die Kontaktdaten des Verantwortlichen informiert. Somit muss der Gutachterausschuss seine Kontaktdaten als Verantwortlicher angeben, wenn er Informationen nach Art. 13 DSGVO zur Verfügung stellt.

Betreibt der Gutachterausschuss eine eigene Homepage, so ist zu beachten, dass auch insoweit die Informationspflichten nach Art. 13 Abs. 1 und 2 DSGVO zu erfüllen sind. Das heißt, der Gutachterausschuss hat auf seiner Homepage die Informationen zur Erhebung von personenbezogenen Daten beim Betrieb der Homepage unter einer aussagekräftigen Rubrik, etwa einer Datenschutzerklärung, mitzuteilen. Das Bayerische Staatsministerium des Innern, für Sport und Integration hat auf seiner Homepage[30] ein – mit mir abgestimmtes – Muster für ein Impressum und eine Datenschutzerklärung im Internetauftritt bayerischer öffentlicher Stellen zur Verfügung gestellt. Ich rate insoweit nachdrücklich, die Datenschutzerklärung inhaltlich nach diesem Muster zu gestalten.

5.1.6 Auftragsverarbeitung

Schaltet ein Verantwortlicher bei der Verarbeitung personenbezogener Daten einen Dienstleister als Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO ein, so ist regelmäßig ein Vertrag zur Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO zu schließen.

30 Internet: https://www.stmi.bayern.de/sus/datensicherheit/datenschutz/reform_arbeitshilfen.

Da der Gutachterausschuss selbst Verantwortlicher ist, wäre es grundsätzlich denkbar, sein Verhältnis zu seiner Geschäftsstelle – der Kreisverwaltungsbehörde – mit der Folge der eingangs dargestellten Konsequenz als Auftragsverhältnis nach Art. 28 Abs. 1 DSGVO anzusehen. Hierfür spräche, dass auch die Kreisverwaltungsbehörde – das Landratsamt oder die kreisfreie Gemeinde (vgl. § 1 Abs. 1 BayGaV) – eigenständiger Verantwortlicher ist. Allerdings bestimmt der Gesetzgeber bereits selbst in § 9 Abs. 1 BayGaV ausdrücklich, dass die Geschäftsstelle des Gutachterausschusses die Kreisverwaltungsbehörde ist. Da § 9 Abs. 1 BayGaV insoweit nicht zwischen den einzelnen Organisationseinheiten der Kreisverwaltungsbehörde unterscheidet, halte ich es für vertretbar, Dienstleistungen etwa der IT-Abteilung der Kreisverwaltungsbehörde für den Gutachterausschuss als Teil der Geschäftsstelle des Gutachterausschusses selbst anzusehen, so dass insoweit kein Auftragsverhältnis im Sinne von Art. 28 Abs. 1 DSGVO vorliegt.

Dies gilt jedoch nicht, wenn die Kreisverwaltungsbehörde ihre IT-Dienste nicht mehr selbst betreibt, sondern beispielsweise an eine privatrechtlich organisierte Gesellschaft ausgelagert hat. In diesem Fall wird regelmäßig ein Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO zwischen dem Gutachterausschuss und der privatrechtlich (etwa als GmbH) organisierten Gesellschaft zu schließen sein.

5.1.7 Rechtsgrundlagen für die Datenverarbeitung

Wenn der Gutachterausschuss personenbezogene Daten, wie Namen und Adress-/Kontaktdaten verarbeitet, benötigt er hierfür eine Rechtsgrundlage (vgl. Art. 6 Abs. 1 DSGVO). In dem von mir geprüften Fall konnte sich der Gutachterausschuss für seine Datenverarbeitungen auf Art. 4 Abs. 1 BayDSG in Verbindung mit § 197 Abs. 1 BauGB und § 10 BayGaV stützen. Der Gutachterausschuss legte insoweit dar, dass die Adressen der Vertragsparteien erfasst würden, um von ihnen erforderlichenfalls weitere Informationen einholen zu können. Im konkreten Fall des Eingabeführers sei nur noch dessen Nachname gespeichert gewesen. Dies sei erforderlich, um bei der weiteren Verarbeitung der Kauffälle und Nutzung der Immobiliendaten, beispielsweise bei Auskunftsersuchen aus der Kaufpreissammlung, die richtigen Datensätze zusammenstellen zu können. Die Namen seien etwa erforderlich, um Verwandtenverkäufe zu erkennen, welche Auswirkungen auf die Preisgestaltung haben können. Dies konnte ich nachvollziehen.

5.2 Bürgerversammlungen: Veröffentlichung von Anträgen

Bürgerversammlungen bieten Gelegenheit zum Austausch zwischen der ersten Bürgermeisterin oder dem ersten Bürgermeister sowie Bürgerinnen und Bürgern zu gemeindlichen Angelegenheiten. Bürgerversammlungen sind ein wichtiges Element der Bürgerbeteiligung. Insbesondere können dort von Bürgerinnen und Bürgern auch Anträge eingebracht werden.

Durch eine bei mir im Berichtszeitraum eingereichte Beschwerde eines Bürgers habe ich erfahren, dass eine bayerische Kommune derartige Anträge seit vielen Jahren im öffentlich zugänglichen Teil ihres Ratsinformationssystems speichert und so weltweit zugänglich macht. Hiervon waren im Fall der von der konkreten Beschwerde betroffenen Kommune bei Anträgen bis zum Jahr 2015 auch persönliche Daten der Antragstellerinnen und Antragsteller wie deren Anschrift, Telefonnummer und teilweise sogar Nationalität umfasst. Zwar hatte die Kommune von den Betroffenen in der Vergangenheit Einwilligungen zur Veröffentlichung gerade auch im Internet eingeholt. So

hatte auch im konkreten Beschwerdefall der betreffende Bürger der Veröffentlichung durch entsprechenden Vermerk in den Antragsunterlagen zunächst zugestimmt. Jedoch war ihm nach eigener Aussage dabei nicht hinreichend bewusst gewesen, dass die Unterlagen dann mittels Suchmaschinen weltweit dauerhaft abgerufen werden können. Er widerrief daher seine Einwilligung, nachdem er dies erkannt hatte, woraufhin die Kommune den Antrag zwar löschte, jedoch übersah, dass dieser auch in einem weiteren Dokument enthalten war. Die personenbezogenen Daten konnten so weiterhin mittels einfacher Suchmaschinenrecherche abgerufen werden.

Ich habe einen **Verstoß gegen datenschutzrechtliche Vorgaben** festgestellt. Die Veröffentlichung der personenbezogenen Daten des Betroffenen bedurfte einer Rechtsgrundlage. Eine solche lag grundsätzlich zunächst in der seinerzeit freiwillig erteilten Einwilligung mittels Ankreuzen des entsprechenden Vermerks in den Antragsunterlagen. Diese war jedoch unwidersprochen zwischenzeitlich **widerrufen** worden. Unabhängig von der konkreten Beschwerde erscheint es zudem zweifelhaft, ob sich öffentliche Stellen bei der dauerhaften Internetbereitstellung von Anträgen aus Bürgerversammlungen einschließlich personenbezogener Daten überhaupt auf– gegebenenfalls schon vor langer Zeit erteilte – Einwilligungen stützen können. Hierzu habe ich der betroffenen Kommune folgende **Hinweise** gegeben:

Maßgeblicher Zeitpunkt für die Beurteilung der Zulässigkeit der Datenverarbeitung ist nicht (nur) der des Hochladens der Daten beispielsweise in ein Ratsinformationssystem. Vielmehr kommt die Veröffentlichung in einem öffentlichen Internetportal einer dauerhaften Übermittlung personenbezogener Daten an eine Vielzahl (unbestimmter) Dritter gleich. Eine zulässige dauerhafte Übermittlung setzt aber voraus, dass **die erforderlichen Voraussetzungen für die Übermittlung zu jedem Zeitpunkt der Online-Verfügbarkeit vorliegen müssen**.

Weiterhin habe ich klargestellt, dass einmal eingeholte **Einwilligungen** in eine Internetveröffentlichung **kein „Blanko-Scheck" für eine Zurverfügungstellung auf unbestimmte Zeit** sind. Zwar werden gemäß Erwägungsgrund 171 Satz 3 DSGVO zuvor eingeholte Einwilligungen mit Geltungsbeginn der Datenschutz-Grundverordnung nicht automatisch unwirksam, sondern sind weiter gültig, soweit sie den aktuellen Vorgaben entsprechen. Außerdem ist auch unter Geltung der Datenschutz-Grundverordnung kein festes Verfallsdatum für eingeholte Einwilligungen vorgesehen.[31] Jedoch wird man insbesondere bei zeitlich unbefristet eingeholten Einwilligungen davon ausgehen müssen, dass diese den Grundsätzen der **Datensparsamkeit** und der **Zweckbindung in besonderem Maße unterliegen** und daher nicht mehr benötigte Daten zu löschen sind sowie die Einwilligungen selbst in angemessenen Zeitabständen erneuert werden müssen.[32] Maßgeblich für die Gültigkeit „alter" Einwilligungen ist auch, ob die seinerzeit Einwilligenden nach heutigem Maßstab **hinreichend informiert** entscheiden konnten. Dies setzt unter anderem voraus, dass die **betroffene Person wusste, in welchem Umfang sie ihre Einwilligung erteilt**. Wie vom Europäischen Gerichtshof zu Recht betont, müssen klare und umfassende Informationen die Einwilligenden in die Lage versetzen, die Konsequenzen einer etwaigen Einwilligung leicht zu bestimmen und gewährleisten, dass die Einwilligung in voller Kenntnis der Sachlage erteilt wird.[33] Insoweit ist es aber fraglich, ob eine Person, die

31 Stemmer, in: Wolf/Brink, Beck'scher Online-Kommentar Datenschutzrecht, Stand 5/2021, Art. 7 DSGVO Rn. 85.

32 Heckmann/Paschke, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 7 Rn. 43.

33 Europäischer Gerichtshof, Urteil vom 1. Oktober 2019, C-673/17.

beispielsweise in den Jahren 2005 bis 2010 eine Einwilligung zur Veröffentlichung ihres Antrags auch im Internet erteilt hat, damit rechnen konnte, dass dieser Antrag noch 15 Jahre später für Jedermann abrufbar ist. Einzubeziehen sind auch die erheblichen (kommunikations-) technologischen Veränderungen der letzten Jahre. Insoweit ist kritisch zu hinterfragen, ob sich Einwilligende zum damaligen Zeitpunkt der Tragweite einer Internetveröffentlichung, insbesondere hinsichtlich der einerseits nur eingeschränkten Löschmöglichkeiten und der andererseits permanenten Zugriffsmöglichkeiten mittels Smartphone bewusst sein konnten. Seit Geltungsbeginn der Datenschutz-Grundverordnung sieht Art. 13 Abs. 2 Buchst. a DSGVO ausdrücklich vor, dass der Verantwortliche die betroffene Person über die Dauer einer Verarbeitung zu informieren hat, soweit dies für eine faire und transparente Verarbeitung notwendig ist.

Klargestellt habe ich bei dieser Gelegenheit auch, dass es eine **gesetzliche Befugnis** zur Veröffentlichung von Anträgen zu Bürgerversammlungen im Internet **nicht gibt**. Finden sich die Wörter „Veröffentlichung" oder „Bekanntgabe" im kommunalrechtlichen Kontext, so sind grundsätzlich lediglich ortsübliche Veröffentlichungen gemeint, eine Internetveröffentlichung kennt die Gemeindeordnung hingegen (noch) nicht. Auch auf die allgemeine Übermittlungsbefugnis aus Art. 5 Abs. 1 BayDSG kann eine Internetveröffentlichung regelmäßig nicht gestützt werden. Eine kommunale Aufgabe, die eine pauschale und dauerhafte Übermittlung einer Vielzahl personenbezogener Daten an Jedermann erfordert (vgl. Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG), ist nicht ersichtlich. Auch ist Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG für eine solche eigeninitiative Datenbereitstellung durch eine öffentliche Stelle schon vom Wortlaut her offensichtlich nicht ausgelegt.

Mit der im konkreten Fall betroffenen Kommune habe ich mich daher darauf verständigt, dass Anträge zu Bürgerversammlungen, auf denen persönliche Kontaktdaten von Antragstellerinnen und Antragstellern einsehbar sind, – trotz in der Vergangenheit freiwillig erteilter Einwilligungen – generell aus dem öffentlichen Teil des Ratsinformationssystems entfernt werden.

5.3 Bauantragsunterlagen: keine regelhafte Übermittlung durch Gemeinden an Wasserzweckverbände

Bauanträge sind gemäß Art. 64 Abs. 1 Satz 1 Bayerische Bauordnung (BayBO) schriftlich bei der Gemeinde einzureichen. Gemäß Art. 64 Abs. 2 Satz 1 BayBO sind mit dem Bauantrag alle für die Beurteilung des Bauvorhabens und die Bearbeitung des Bauantrags erforderlichen Unterlagen (Bauvorlagen) einzureichen.

Art. 64 BayBO
Bauantrag, Bauvorlagen
(1) [1]Der Bauantrag ist schriftlich bei der Gemeinde einzureichen. [2]Diese legt ihn, sofern sie nicht selbst zur Entscheidung zuständig ist, mit ihrer Stellungnahme unverzüglich bei der Bauaufsichtsbehörde vor. [3]Die Gemeinden können die Ergänzung oder Berichtigung unvollständiger oder unrichtiger Bauanträge verlangen.
(2) [1]Mit dem Bauantrag sind alle für die Beurteilung des Bauvorhabens und die Bearbeitung des Bauantrags erforderlichen Unterlagen (Bauvorlagen) einzureichen. [2]Es kann gestattet werden, dass einzelne Bauvorlagen nachgereicht werden.

Durch die Eingabe eines Bürgers bin ich auf folgende Praxis aufmerksam geworden: In Gemeinden, in denen ein örtlicher Wasserzweckverband mit der Wasserversorgung betraut wurde, werden regelhaft die gesamten Bauantragsunterlagen an diesen weitergeleitet. Als Grund hierfür wurde mir genannt, dass Bauherrinnen und Bauherrn

es oftmals pflichtwidrig unterlassen würden, selbst die erforderlichen Anzeigen der für die Beitragsbemessung relevanten baulichen Änderungen beim Wasserzweckverband vorzunehmen. Auf gemeindlicher Seite habe sich daher die Übung entwickelt, den Wasserzweckverbänden die gesamten Bauantragsunterlagen eigeninitiativ weiterzuleiten.

Aus datenschutzrechtlicher Sicht ist ein solches Vorgehen jedoch kritisch zu bewerten.

Zunächst einmal stellt die Übersendung der Bauantragsunterlagen an den Wasserzweckverband jedenfalls bei Bauanträgen natürlicher Personen unzweifelhaft eine Verarbeitung personenbezogener Daten dar, für die bayerische Gemeinden einer Rechtsgrundlage bedürfen (vgl. Art. 6 Abs. 1 DSGVO). Mangels einer ersichtlichen spezialgesetzlichen Befugnis für die eingangs geschilderte Praxis war deren Zulässigkeit anhand der allgemeinen Verarbeitungsbefugnisse aus dem Bayerischen Datenschutzgesetz zu beurteilen. Nach dem insoweit allein in Betracht kommenden Art. 5 Abs. 1 Satz 1 Nr. 1 Var. 2 BayDSG ist eine Übermittlung personenbezogener Daten zulässig, wenn sie zur Erfüllung einer der **empfangenden** öffentlichen Stelle obliegenden Aufgabe **erforderlich** ist. Insoweit war aus datenschutzrechtlicher Sicht jedoch Folgendes zu bedenken:

Zwar ist die öffentliche Wasserversorgung gemäß § 50 Abs. 1 Wasserhaushaltsgesetz eine Aufgabe der Daseinsvorsorge und als kommunale Aufgabe im eigenen Wirkungskreis der Kommune (vgl. Art. 83 Abs. 1 Verfassung des Freistaates Bayern und Art. 57 Abs. 2 Gemeindeordnung) eine solche, die im öffentlichen Interesse liegt. Diese Aufgabe wurde in den vorgenannten Konstellationen einem Wasserzweckverband – der empfangenden öffentlichen Stelle – übertragen und damit zur (eigenen) Aufgabe des Wasserzweckverbands. Dem Aufgabenbereich des Wasserzweckverbands zuzurechnen ist auch die Bemessung von Beiträgen. Zur Sicherstellung der Wasserversorgung erhebt der Zweckverband nämlich für die Deckung seines Aufwands einen Beitrag für bebaute Grundstücke. Zur Berechnung des durch die Grundstückseigentümer konkret zu begleichenden Beitragssatzes ist auch regelmäßig die Kenntnis der genauen Grundstücks- und Geschossflächen der versorgten Häuser und Wohnungen erforderlich.

Die Erfüllung dieser Aufgaben **erfordert jedoch regelmäßig nicht die Übermittlung der gesamten Bauantragsunterlagen an den Wasserzweckverband.** Doch auch eine Übermittlung bloß der notwendigen Daten – also der zur Bemessung der Beiträge notwendigen Parameter – ist **nur dann** im Sinne des Art. 5 Abs. 1 Satz 1 Nr. 1 Var. 2 BayDSG **erforderlich, wenn die Meldung nicht bereits durch die Bauherrin oder den Bauherrn selbst erfolgt ist**. Um dies beurteilen zu können, müsste der Gemeinde jedoch bekannt sein, ob nicht beim Wasserzweckverband bereits eine Änderungsmeldung eingegangen oder eine solche gegebenenfalls entbehrlich ist (möglich bei selbstverwalteten Kläranlagen und Brunnen). In der Praxis werden diese Fragen jedoch offenbar gar nicht erst gestellt. Vielmehr werden in den oben geschilderten Konstellationen die gesamten Bauantragsunterlagen regelhaft und damit gleichsam „auf Vorrat“ übermittelt. Eine solche Datenübermittlung hält freilich dem Erforderlichkeitsgrundsatz **nicht** stand.

Ich bin daher an das Bayerische Staatsministerium des Innern, für Sport und Integration als oberste Aufsichtsbehörde über die bayerischen Kommunen herangetreten. Erfreulicherweise hat das Innenministerium umgehend reagiert und die bayerischen Kommunen über die datenschutzrechtliche Problematik informiert sowie eine vorherige konkrete Einzelfallprüfung vor etwaigen Datenübermittlungen angemahnt.

5.4 Datenschutz bei der Herausgabe kommunaler Mitteilungsblätter

Art. 26 Abs. 2 Gemeindeordnung enthält die gemeindliche Befugnis zur Veröffentlichung von Amtsblättern. Unter einem Amtsblatt ist ein regelmäßig erscheinendes Druckwerk zu verstehen, das dazu bestimmt ist, Vorschriften, Verfügungen oder Mitteilungen amtlich bekanntzumachen.

Nach meinem Eindruck möchten viele Gemeinden aber darüber hinausgehen und örtlichen Vereinen oder Institutionen wie etwa Kirchen, Parteien und sonstigen Verbänden ein gemeindliches Medium bieten, in welchem diese auf eigene Veranstaltungen hinweisen oder darüber berichten können. Hinzu kommt, dass auch die Gemeinde selbst kraft ihres kommunalen Selbstverwaltungsrechts die allgemeine Aufgabe hat, (datenschutzkonforme) Öffentlichkeitsarbeit zu betreiben, also die Gemeindeangehörigen etwa über Vorgänge aus der Gemeindeverwaltung oder über Aktivitäten der ersten Bürgermeisterin oder des ersten Bürgermeisters sowie des Gemeinderats zu informieren (siehe insoweit auch meine Ausführungen im 23. Tätigkeitsbericht 2008 unter Nr. 21.4). Aus diesen Gründen beschränken sich nach meinem Eindruck viele bayerische Gemeinden inzwischen nicht mehr auf die Herausgabe eines bloßen Amtsblatts, sondern erweitern dieses um sonstige Mitteilungen zu einem übergreifenden kommunalen Mitteilungsblatt. Ein solches Medium enthält typischerweise neben amtlichen Bekanntmachungen weitere redaktionelle und informatische Inhalte, oftmals verbunden mit einem Anzeigenteil. Dies wirft eine Vielzahl datenschutzrechtlicher Fragen und Probleme auf, die im Folgenden kurz angerissen werden sollen:

Zunächst werden die Gemeinden regelmäßig Herausgeber des kommunalen Mitteilungsblattes sein, weil die Gesamtleitung des Druckerzeugnisses und die redaktionelle Verantwortung bei ihnen liegen. Diese Stellung hat aber auch datenschutzrechtliche Auswirkungen. Aus Datenschutzsicht ist vor allem relevant, ob eine Gemeinde Verantwortlicher im Sinne der Datenschutz-Grundverordnung ist (vgl. Art. 4 Nr. 7 DSGVO) ist. Wenn die Gemeinde Herausgeber des kommunalen Mitteilungsblatts ist, also letztlich allein bestimmt, welche Beiträge in dem Druckwerk veröffentlicht werden, oder etwa selbst Beiträge verfasst beziehungsweise Inhalte beisteuert, so ist ihre datenschutzrechtliche Verantwortlichkeit grundsätzlich zu bejahen.

Hieran knüpfen sich datenschutzrechtliche Folgefragen an, da in solchen Mitteilungsblättern regelmäßig personenbezogene Daten von Bürgerinnen und Bürgern sowie von Bediensteten verarbeitet werden. Wird etwa ein Foto veröffentlicht, auf dem eine natürliche Person identifizierbar abgebildet ist, so stellt dieser Vorgang aus Datenschutzperspektive eine rechtfertigungsbedürftige Datenübermittlung an eine unbestimmte Zahl von Empfängern, also an nichtöffentliche Stellen (die Leserinnen und Leser des Mitteilungsblatts), dar. Entsprechendes gilt, wenn die Gemeinde einen Beitrag veröffentlicht, in dem eine Person namentlich erwähnt wird oder etwa einer konkreten Person zuordenbare (Kontakt-)Daten enthalten sind.

Die Gemeinden können sich bei solchen Datenverarbeitungen jedoch nur in einem sehr begrenzten Umfang auf gesetzliche Befugnisse stützen. Vor allem steht der Gemeinde als Teil der staatlichen Gewalt für ihre kommunalen Druckerzeugnisse nicht das in Art. 38 BayDSG und Art. 85 DSGVO enthaltene Presseprivileg zu. Oftmals müssen die Gemeinden daher wirksame Einwilligungen nach Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 7 DSGVO von den jeweils betroffenen Personen einholen. Dabei ist es aufgrund der gemeindlichen Verantwortung für das kommunale Mitteilungsblatt nicht ausreichend, wenn (wie wohl von einigen bayerischen Kommunen praktiziert) etwa auf den Fotos abgebildete Personen gegenüber ihrem Verein erklären, dass sie in die

Veröffentlichung einwilligen. Denkbar ist insoweit allenfalls, dass der Vereinsvorstand als (Erklärungs-)Bote für die Gemeinde eingeschaltet wird.

Um den Gemeinden Hilfestellungen zur Lösung datenschutzrechtlicher Fragen bei der Herausgabe von Mitteilungsblättern zu geben, habe ich das Arbeitspapier „Datenschutz bei kommunalen Mitteilungsblättern" veröffentlicht.[34] Das Arbeitspapier erläutert die zu beachtenden datenschutzrechtlichen Vorgaben und geht auf typische Fallkonstellationen wie etwa die Bekanntgabe von Eheschließungen oder Jubiläumsgratulationen in einem kommunalen Mitteilungsblatt ein. Des Weiteren sind auch datenschutzkonforme Mustereinwilligungsformulare enthalten. Diese können dazu verwendet werden, das Vorliegen wirksamer Einwilligungen in die Verarbeitung personenbezogener Daten in einem kommunalen Mitteilungsblatt zu dokumentieren.

5.5 Personenbezogene Angaben auf Parkausweisen für Gewerbetreibende oder selbständige Freiberufler

Im Berichtszeitraum war ich erneut mit personenbezogenen Angaben auf Parkausweisen befasst (siehe zuletzt meinen 28. Tätigkeitsbericht 2018 unter Nr. 7.7). Konkret ging es diesmal um Parkausweise für Gewerbetreibende oder selbständige Freiberuflerinnen und Freiberufler, mit welchen diesem Personenkreis Ausnahmegenehmigungen gemäß § 46 Abs. 1 Nr. 4a und 11 Straßenverkehrs-Ordnung (StVO) erteilt werden.

§ 46 StVO
Ausnahmegenehmigung und Erlaubnis
(1) Die Straßenverkehrsbehörden können in bestimmten Einzelfällen oder allgemein für bestimmte Antragsteller Ausnahmen genehmigen
[…]
4a. von der Vorschrift, an Parkuhren nur während des Laufens der Uhr, an Parkscheinautomaten nur mit einem Parkschein zu halten (§ 13 Absatz 1);
[…]
11. von den Verboten oder Beschränkungen, die durch Vorschriftzeichen (Anlage 2), Richtzeichen (Anlage 3), Verkehrseinrichtungen (Anlage 4) oder Anordnungen (§ 45 Absatz 4) erlassen sind;
[…]

Durch das Auslegen von Parkausweisen hinter der Windschutzscheibe eines Kraftfahrzeugs werden auf dem Dokument vermerkte personenbezogene Daten öffentlichen Stellen zu Kontrollzwecken bereitgestellt. Die hierdurch unvermeidbar vermittelte Möglichkeit der Kenntnisnahme durch die Allgemeinheit ist nach meiner Einschätzung grundsätzlich eine datenschutzrechtlich hinzunehmende Nebenfolge. Diese Nebenfolge sollte in Anbetracht des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) aber so wenig belastend ausfallen wie möglich.

In diesem Zusammenhang habe ich im Rahmen der Bearbeitung einer bei mir eingereichten Bürgereingabe erfahren, dass die betroffene öffentliche Stelle auf derartigen Parkausweisen nicht nur detaillierte Angaben zur Art des Gewerbes oder der Art der

[34] Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz bei kommunalen Mitteilungsblättern, Stand 7/2021, Internet: https://datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Einzelthemen".

selbstständigen freiberuflichen Tätigkeit machte, sondern auch die vollständigen Namen der betroffenen natürlichen Personen aufführte.

Die betroffene öffentliche Stelle habe ich daher darauf hingewiesen, dass die Offenlegung der **vollständigen Namen** betroffener natürlicher Personen und der **genauen Art der selbständigen oder gewerblichen Tätigkeit** insoweit auch für berechtigte Kontrollzwecke **nicht erforderlich ist.** Erfreulicherweise hat die betroffene öffentliche Stelle umgehend reagiert. Zukünftig werden daher auf derartigen Parkausweisen neben der Ausweisnummer nur noch die Bezeichnung „Selbständiger Freiberufler" und gegebenenfalls die Anschrift aufgeführt sein. **Auf die Angabe des Namens und der Art der selbständigen Tätigkeit wird die öffentliche Stelle auf den neu ausgestellten Parkausweisen dagegen verzichten.** Dies habe ich ausdrücklich begrüßt.

Die geänderte Handhabung **gewährleistet weiterhin eine wirksame Überprüfung der rechtmäßigen Nutzung der Ausnahmegenehmigung** sowohl auf Seiten des Überwachungspersonals der öffentlichen Stelle als auch der Polizei. Ich empfehle daher Parkausweisen nach § 46 Abs. 1 Nr. 4a und 11 StVO ausstellenden Behörden, für gewerbliche oder selbständige Anlieger nur eine abstrakte Tätigkeitsbezeichnung wie etwa „Selbständiger Freiberufler" und gegebenenfalls die Anschrift aufzuführen.

5.6 Duldung durch Ausländerbehörde: keine überschießende Datenerhebung

Nach § 60a Abs. 2 Satz 1 Aufenthaltsgesetz (AufenthG) ist die Abschiebung von vollziehbar ausreisepflichtigen Ausländern vorübergehend auszusetzen, solange die Abschiebung aus tatsächlichen oder rechtlichen Gründen unmöglich ist und keine Aufenthaltserlaubnis erteilt wird. Hierbei handelt es sich um eine nicht nur auf Antrag, sondern auch von Amts wegen vorzunehmende Prüfung. Die Duldung ist dabei eine gegenüber der geduldeten Person begünstigende Entscheidung. Diese Person ist daher nach Maßgabe von § 82 Abs. 1 Satz 1 AufenthG verpflichtet, ihre Belange und für sie günstige Umstände, soweit sie nicht offenkundig oder bekannt sind, unter Angabe nachprüfbarer Umstände geltend zu machen und soweit möglich auch nachzuweisen. Für die betroffenen Personen günstige Sachverhalte, die ein Abschiebehindernis begründen und für die Ausländerbehörden weder offenkundig noch bereits während eines laufenden Asylverfahrens vollständig bekannt sind, können beispielsweise das Vorhandensein von Angehörigen im Bundesgebiet, oder eine stattgefundene Integration durch Schulbesuch, Arbeit oder Praktika sein. Weitere exemplarisch aufgezählte Duldungsgründe finden sich in § 60a Abs. 2 AufenthG. Außerdem können sich bislang nicht mitgeteilte Veränderungen ergeben haben oder die geduldeten Personen können Angaben machen, die nicht bereits von den vorher an anderer Stelle erfragten Auskünften erfasst sind. Rechtsgrundlage für Datenerhebungen in diesem Kontext ist § 86 AufenthG:

„[1]Die mit der Ausführung dieses Gesetzes betrauten Behörden dürfen zum Zweck der Ausführung dieses Gesetzes und ausländerrechtlicher Bestimmungen in anderen Gesetzen personenbezogene Daten erheben, soweit dies zur Erfüllung ihrer Aufgaben nach diesem Gesetz und nach ausländerrechtlichen Bestimmungen in anderen Gesetzen erforderlich ist. [2]Personenbezogene Daten, deren Verarbeitung nach Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 untersagt ist, dürfen erhoben werden, soweit dies im Einzelfall zur Aufgabenerfüllung erforderlich ist."

Zwar enthält § 86 AufenthG keine konkreten Vorgaben zur Form der Erhebung (schriftlich, mündlich oder etwa mittels Formular) und sieht daher auch keine konkreten Bestimmungen zum Inhalt von etwa verwendeten Formularen vor. Jedoch ist unabhängig von der gewählten Form der Datenerhebung maßgeblich, dass diese nur dann zur Aufgabenerfüllung erforderlich ist, wenn die personenbezogenen Daten zur Vorbereitung einer konkreten ausländerrechtlichen Entscheidung oder Maßnahme erhoben werden. Bei Verwendung schriftlich auszufüllender Formulare als Alternative zu einer mündlichen Befragung ist aus datenschutzrechtlicher Sicht darauf zu achten, dass **nicht mehr Angaben erfragt werden, als für die beantragte Entscheidung nach den für diese maßgeblichen Vorschriften benötigt werden**. Freiwillige Angaben (zum Beispiel eine Telefonnummer) sind als solche auf dem Vordruck zu kennzeichnen.

Im Berichtszeitraum habe ich erfahren, dass die bayerischen Regierungen in ihrer Zuständigkeit als Zentrale Ausländerbehörden bei Gesuchen auf Erteilung oder Verlängerung einer Bescheinigung über die Aussetzung der Abschiebung nicht bayernweit einheitliche Angaben erheben. Ursächlich hierfür war nach meinem Eindruck, dass die Zentralen Ausländerbehörden nicht dasselbe Formular verwenden. Je nach verwendetem Formular wurden dabei mehr oder auch weniger Daten erhoben. Ich habe mich deshalb an das Bayerische Staatsministerium des Innern, für Sport und Integration als Aufsichtsbehörde über die Zentralen Ausländerbehörden gewandt, um auf einheitliche Vorgaben hinsichtlich des Umfangs der Datenerhebung hinzuwirken.

Erfreulicherweise hat das Innenministerium bereits angekündigt, die Ausländerbehörden ausdrücklich dazu anhalten, **in den verwendeten Formularen nur die erforderlichen Daten zu erheben und andere Daten wie etwa die Handynummer als freiwillig zu kennzeichnen.** Mit Blick auf das in Art. 5 Abs. 1 Buchst. c DSGVO verankerte Gebot der Datensparsamkeit bestätigte mir das Innenministerium außerdem, dass die Formulare, sofern sie über die Identität und Anschrift hinausgehende Fragen (zum Beispiel zu Angehörigen, zum Arbeitsverhältnis, zu Krankheiten) umfassen, in Zukunft den **allgemeinen Zusatz „bitte nur die auf Sie zutreffenden Fragen beantworten“** enthalten sollen.

5.7 Luftsicherheitsassistenten: Datenübermittlungen durch Luftämter an Arbeitgeber nur im Rahmen des Erforderlichen

Eine Beschwerde im Berichtszeitraum gab Anlass, ein nach meiner Einschätzung bislang nur unzureichend beleuchtetes Thema näher zu betrachten, nämlich die Zulässigkeit von Datenübermittlungen zwischen bayerischen Luftsicherheitsbehörden und den von diesen nach § 16a Abs. 1 Luftsicherheitsgesetz (LuftSiG) beliehenen natürlichen Personen (Luftsicherheitsassistentinnen und Luftsicherheitsassistenten) beziehungsweise deren Arbeitgebern. Zum besseren Verständnis möchte ich zunächst die rechtliche Einbettung der Luftsicherheitsassistentinnen und Luftsicherheitsassistenten in das System der Luftsicherheit veranschaulichen.

5.7.1 Luftsicherheitsassistentinnen und Luftsicherheitsassistenten: beleihende Stelle und Arbeitgeber nicht identisch

§ 16a Abs. 1 LuftSiG ermöglicht es der zuständigen Luftsicherheitsbehörde (entweder das Luftamt Südbayern bei der Regierung von Oberbayern oder das Luftamt Nordbayern bei der Regierung von Mittelfranken), auch natürlichen Personen als Be-

liehenen die Wahrnehmung bestimmter luftsicherheitsrechtlicher Aufgaben zu übertragen. Dies betrifft nach Nummer 1 der Vorschrift gerade auch die Übertragung bestimmter Aufgaben bei der Durchführung von Sicherheitsmaßnahmen nach § 5 Abs. 1 bis 3 LuftSiG. In der Praxis umfasst diese Beleihung regelmäßig insbesondere die Aufgabe, Fluggäste und deren Handgepäck auf verbotene Gegenstände zu kontrollieren. Aus der öffentlich-rechtlichen Beleihungssituation resultiert dabei gemäß § 16a Abs. 5 LuftSiG eine unmittelbare Aufsichtsbefugnis der beleihenden Luftsicherheitsbehörde (Luftamt) gegenüber den Luftsicherheitsassistentinnen und Luftsicherheitsassistenten.

Als Arbeitgeber für die nach § 16 a Abs. 1 LuftSiG durch die Luftämter beliehenen Luftsicherheitsassistentinnen und Luftsicherheitsassistenten fungieren zwei allein vom Freistaat getragene Unternehmen, nämlich die Sicherheitsgesellschaft am Flughafen München mbH und die Sicherheitsgesellschaft am Flughafen Nürnberg mbH. Aufgabe der beiden Gesellschaften ist es, Arbeitsverträge mit den jeweils zu beleihenden Personen zu schließen und hierdurch die personellen Ressourcen bereitzustellen, welche die zuständigen Luftsicherheitsbehörden zur Erfüllung ihrer Aufgaben, insbesondere nach § 5 LuftSiG, benötigen. Da sie insoweit Aufgaben der öffentlichen Verwaltung wahrnehmen, sind beide Unternehmen als öffentliche Stellen im Sinne des Art. 1 Abs. 2 BayDSG anzusehen. Selbst mit luftsicherheitsrechtlichen Aufgaben durch die Luftämter beliehen sind die beiden Sicherheitsgesellschaften aber nicht.

5.7.2 Beschwerdesachverhalt

Eine nach § 16a Abs. 1 LuftSiG beliehene Person wandte sich mit einer Anfrage an die sie beleihende Luftsicherheitsbehörde. Inhaltlich ging es um die Ankündigung, aus Gründen des Eigenschutzes bestimmte (gefährliche) Gegenstände in den Sicherheitsbereich des Flughafens mitzunehmen. Die Luftsicherheitsbehörde leitete die betreffende Nachricht – unter Offenlegung des Absenders – an den Arbeitgeber weiter, was zu erheblichen Verwerfungen im Arbeitsverhältnis führte.

5.7.3 Datenschutzrechtliche Bewertung der Übermittlung

Im Rahmen meiner datenschutzrechtlichen Überprüfung des Vorgangs konnte mir die Luftsicherheitsbehörde entgegen der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO nicht darlegen, dass die betreffende Übermittlung auf eine Rechtsgrundlage gestützt werden konnte.

Da es an spezialgesetzlichen Verarbeitungsvorschriften für die hier vorliegende Fallgestaltung fehlte, war die Zulässigkeit der Datenübermittlung anhand der allgemeinen Übermittlungsvorschrift des Art. 5 Abs. 1 Nr. 1 BayDSG zu beurteilen. Danach ist eine Übermittlung personenbezogener Daten zulässig, wenn sie zur Erfüllung einer der übermittelnden oder der empfangenden öffentlichen Stelle obliegenden Aufgabe erforderlich ist.

Eine **Erforderlichkeit** der Übermittlung **zu eigenen (luftsicherheitsrechtlichen) Aufgaben** wurde dabei von Seiten der betreffenden Luftsicherheitsbehörde aber gerade **nicht** vorgetragen. Diese nahm die mitgeteilten Informationen gerade nicht zum Anlass, Maßnahmen hinsichtlich der Beleihung oder andere sicherheitsrechtliche Maßnahmen zu ergreifen. Die Übermittlung erfolgte auch nicht zur Prüfung oder Vorbereitung solcher Maßnahmen. Vielmehr nahm die Luftsicherheitsbehörde an, die

Übermittlung sei für die Erfüllung der Aufgaben der betroffenen Sicherheitsgesellschaft erforderlich. Nach Auffassung der Luftsicherheitsbehörde berührten die von der betroffenen Person mitgeteilten Informationen deren Arbeitsverhältnis nämlich in so erheblichem Umfang, dass dies der Sicherheitsgesellschaft als Arbeitgeberin zur Kenntnis gebracht werden sollte, um dieser gegebenenfalls eine arbeitsrechtliche Sanktionierung zu ermöglichen.

Tatsächlich legte der geschilderte Sachverhalt meines Erachtens aber einen **deutlichen Bezug zu den luftsicherheitsrechtlichen Aufgaben nahe, die der betroffenen Person im Rahmen der Beleihung übertragen worden waren**, und weniger zu ihren davon unabhängigen arbeitsvertraglichen Pflichten. Eigene sicherheitsrechtliche Aufgaben, zu deren Erfüllung die Übermittlung erforderlich gewesen wäre, sind der insoweit lediglich als Arbeitgeberin der beliehenen Luftsicherheitsassistentinnen und Luftsicherheitsassistenten fungierenden Sicherheitsgesellschaft dabei – anders als der Luftsicherheitsbehörde selbst – jedoch gerade nicht zugewiesen. Ein „Abwälzen" sicherheitsrechtlicher Aufgaben der Luftsicherheitsbehörde mit Verweis auf die Personalhoheit der Sicherheitsgesellschaft an diese kam insoweit nicht in Betracht.

Hätte die Luftsicherheitsbehörde im Zusammenhang mit der an sie gerichteten Anfrage die Schwelle einer Gefahr für die öffentliche Sicherheit oder die Luftsicherheit überschritten gesehen, hätte sie im Rahmen ihrer eigenen luftsicherheitsrechtlichen Befugnisse vielmehr selbst (beispielsweise hinsichtlich der von ihr selbst ausgesprochenen Beleihung) tätig werden müssen, oder – sofern eigene Zuständigkeiten an dieser Stelle überschritten waren – die zuständige Sicherheitsbehörde informieren können.

Wegen der fehlenden Rechtsgrundlage für die Datenübermittlung habe ich gegenüber der Luftsicherheitsbehörde einen datenschutzrechtlichen Verstoß festgestellt. Da diese mir zugesagt hat, Handlungsanweisungen zum Umgang mit personenbezogenen Daten in derartigen Fällen zu erarbeiten, habe ich von weitergehenden Maßnahmen abgesehen.

5.7.4 Benennung von Datenschutzbeauftragten erforderlich

Anlässlich meiner datenschutzrechtlichen Überprüfung habe ich die Luftsicherheitsbehörde zudem darauf aufmerksam gemacht, dass die von ihr mit hoheitlichen Aufgaben beliehenen Luftsicherheitsassistentinnen und Luftsicherheitsassistenten bei Ausübung dieser Tätigkeit aus datenschutzrechtlicher Sicht gemäß Art. 1 Abs. 4 BayDSG als Beliehene (eigenständige) öffentliche Stellen sind. Für Behörden und öffentliche Stellen ist jedoch nach Art. 37 Abs. 1 Buchst. a DSGVO die Benennung von Datenschutzbeauftragten obligatorisch. Diese Anforderung trifft auch die Luftsicherheitsassistentinnen und Luftsicherheitsassistenten; diese müssen ebenfalls Datenschutzbeauftragte benennen. Vor dem Hintergrund der großen Zahl betroffener Beliehener habe ich eine Koordinierung diesbezüglicher Benennungen durch die beleihende Luftsicherheitsbehörde angeregt.

6 E-Government und öffentliche Register

6.1 Erneut: Gesetz über die Digitalisierung im Freistaat Bayern

Auch in diesem Berichtszeitraum war ich wieder intensiv mit datenschutzrechtlichen Fragen der Verwaltungsmodernisierung befasst. Fortführen möchte ich wegen seiner grundsätzlichen Bedeutung meinen Bericht über das zum aktuellen Zeitpunkt noch laufende Gesetzgebungsverfahren für ein Gesetz über die Digitalisierung im Freistaat Bayern (Bayerisches Digitalgesetz – BayDiG, siehe hierzu bereits meinen 30. Tätigkeitsbericht 2020 unter Nr. 7.1). Im Rahmen meiner Beteiligung an dem Gesetzgebungsverfahren habe ich die für die Bürgerinnen und Bürger aus meiner Sicht zentralen Datenschutzgesichtspunkte wiederholt an das federführende Bayerische Staatsministerium für Digitales herangetragen. Erfreulicherweise haben meine Stellungnahmen Wirkung gezeigt. Das Digitalministerium berücksichtigte bereits einige meiner Forderungen. Exemplarisch möchte ich auf die folgenden, für die Bürgerinnen und Bürger aus meiner Sicht besonders relevanten Datenschutzaspekte näher eingehen.

6.1.1 Transparente Regelung der Verantwortlichkeiten

Das Zusammenspiel des geplanten Portalverbunds Bayern mit seinen Unterportalen BayernPortal und Organisationsportal Bayern sowie des geplanten Nutzerkontos mit seinen Unterkonten Bürger- und Organisationskonto bringt – mitunter sehr komplexe – Datenverarbeitungen mit sich. In meinem 30. Tätigkeitsbericht 2020 unter Nr. 7.1.2 habe ich detailliert erläutert, warum es einer transparenten und für die Nutzerinnen und Nutzer nachvollziehbaren Zuordnung dieser Datenverarbeitungen zu konkreten Verantwortlichen im Sinne des Art. 4 Nr. 7 DSGVO bedarf. Eine besondere Schwierigkeit einer solchen Lösung liegt insbesondere in dem Zusammenspiel der Portallösung mit der Schaffung einer digitalen Identität, welche jeder natürlichen Person das Recht auf staatliche Bereitstellung digitaler Dienste einräumen soll.

Der aktuelle Gesetzentwurf enthält nunmehr eine Regelung, die Klarheit hinsichtlich der Frage bringt, welche öffentliche Stelle datenschutzrechtlich Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO für welchen (Teil-) Datenverarbeitungsvorgang innerhalb des Gesamtsystems ist. Insbesondere wird nach einem Regel-Ausnahme-Verhältnis zukünftig zwischen Basisdiensten (Verantwortung bei der nutzenden Behörde) und zentralen Diensten (Verantwortung beim bereitstellenden Ressort) unterschieden, wobei die Basisdienste den Regelfall bilden. Dies trägt in der praktischen Umsetzung des Bayerischen Digitalgesetzes dazu bei, dass die Bürgerinnen und Bürger bei der Inanspruchnahme digitaler Verwaltungsleistungen schnell und eindeutig jeweiligen Verantwortlichen identifizieren können sollten.

6.1.2 Entscheidungsmöglichkeiten der Nutzerinnen und Nutzer klargestellt

In meinem 30. Tätigkeitsbericht 2020 unter Nr. 7.1.4 habe ich gefordert, die Unterschiede zwischen einer bloßen Zustimmung und einer datenschutzrechtlichen Einwilligung klarzustellen. Zwar entsprechen die insoweit im aktuellen Gesetzentwurf ver-

wendeten Begriffe vom Wortlaut her weiterhin nicht durchgängig dem datenschutzrechtlichen Verständnis. Demnach wäre nämlich zwischen einer Einwilligung als eigenständiger Rechtsgrundlage für Datenverarbeitungen und einer Zustimmung als bloßem Tatbestandmerkmal einer gesetzlichen Befugnis zu unterscheiden. Die Gesetzesbegründung weist jedoch – insoweit im Einklang mit der von mir im Laufe des Gesetzgebungsverfahrens hilfsweise vorgebrachten Forderung – ausdrücklich darauf hin, wie die Begriffe im datenschutzrechtlichen Sinne jeweils zu verstehen sind. Gegen diese Regelungstechnik habe ich keine grundlegenden Einwände erhoben.

In diesem Kontext weise ich auch auf die neu aufgenommene Möglichkeit für die Nutzerinnen und Nutzer eines Nutzerkontos hin, eine Zustimmung zur Durchführung digitaler Verwaltungsverfahren „für bestimmte Gruppen von Behördenkontakten" zu erteilen. Nun ist es neben der von mir grundsätzlich kritisierten generellen Zustimmung auch möglich, eine nach eigenem Bedarf beschränkte Zustimmung zu erteilen. Damit wurde meiner Forderung Rechnung getragen, dass die Bürgerinnen und Bürger ihren Interessen entsprechend im Vorfeld der Datenverarbeitungen den Umfang erteilter Zustimmungen genau bestimmen können müssen. Im Ergebnis haben die Bürgerinnen und Bürger jetzt die Wahl, ihre Zustimmung zu einzelnen Verwaltungsverfahren, zu bestimmten Gruppen von Behördenkontakten oder generell zu erteilen.

6.1.3 Aber: Verarbeitung von Nutzerdaten nicht an Zustimmung gebunden

Der Gesetzentwurf in der zum Berichtszeitpunkt aktuellen Version erlaubt bei Einsatz des Nutzerkontos die Verarbeitung von Nutzerdaten schon dann, wenn dies zur Durchführung eines Verwaltungsverfahrens oder zur Inanspruchnahme sonstiger Leistungen der öffentlichen Verwaltung erforderlich ist. Die Vorschrift stellt damit für die Zulässigkeit von Datenverarbeitungen – entgegen meinen mehrmals geäußerten datenschutzrechtlichen Bedenken – ausschließlich auf die Frage der Erforderlichkeit ab. Auf die in früheren Fassungen des Bayerischen Digitalgesetzes vorgesehene Zustimmung zu der Datenverarbeitung soll es dagegen insofern nicht mehr ankommen.

Haben die Nutzerinnen und Nutzer (zugegebenermaßen freiwillig) einmal ein Nutzerkonto erstellen lassen, verlieren sie bei dem verfolgten Regelungsansatz nach meinem Verständnis damit die Entscheidungshoheit darüber, ob die hinterlegten Daten weiterverarbeitet werden oder nicht. Es ist vielmehr die verarbeitende Stelle, die (zumindest faktisch) die Entscheidung darüber trifft, ob bestimmte Nutzerdaten etwa zur Inanspruchnahme sonstiger Leistungen der öffentlichen Verwaltung erforderlich sind. Dies widerspricht nach meinem Verständnis den übergreifenden Zielen des Bayerischen Digitalgesetzes, nämlich der freiwilligen Nutzung der digitalen Identität und der fortdauernden Entscheidungshoheit der Nutzerinnen und Nutzer über deren Einsatz. Hierauf habe ich das federführende Digitalministerium (leider erfolglos) mehrfach eindringlich hingewiesen und um Korrektur gebeten.

6.1.4 Ausblick: Verarbeitung von Meldedaten begrenzen

Der Gesetzentwurf lässt leider auch in der zum Berichtszeitpunkt aktuellen Version weiterhin offen, welche Datenkategorien in welchem Umfang für die digitale Identität, insbesondere das Nutzerkonto konkret verwendet werden sollen. Die Gesetzesbegründung und die bisherige Entstehungsgeschichte lassen mich weiterhin vermuten, dass primär Meldedaten im Sinne des Bundesmeldegesetzes betroffen sein werden. Hierzu habe ich meine kritische Haltung in meinem 30. Tätigkeitsbericht 2020 unter

Nr. 7.1.1 bereits umfassend dargestellt. Daran halte ich nach wie vor fest. Insbesondere die Forderung, den Datenfluss nach Aktivierung der Nutzerkonten für die Bürgerinnen und Bürger transparent zu gestalten und vor allem auf das (jeweils) konkret erforderliche Ausmaß zu begrenzen, behält ihre Gültigkeit. Die konkrete Regelung dieser Frage soll jedoch nun wohl nicht mehr im Bayerischen Digitalgesetz selbst, sondern in einer gesondert zu erlassenden Verordnung erfolgen. Insoweit werde ich die Umsetzung des Bayerischen Digitalgesetzes auch auf dieser Ebene weiterhin aufmerksam begleiten und soweit veranlasst, hierzu berichten.

6.2 BayernAtlas: gesetzgeberischer Handlungsbedarf

„Der BayernAtlas ist eine Internetanwendung zum Betrachten amtlicher Karten und Luftbilder der Bayerischen Vermessungsverwaltung. Für Privatanwender, Fachanwender und Smartphone-Nutzer oder als Anfahrtsplan für die eigene Homepage: Der BayernAtlas liefert für jeden Anwendungsbereich eine Lösung. Er enthält Luftbilder, eine nahtlos zoombare Webkarte, amtliche topographische Karten mit und ohne Schummerung sowie eine inhaltsreduzierte Ausgabe der Flurkarte (Parzellarkarte), historische Karten, dreidimensionale Gelände- und Gebäudedaten, saisonale Themenkarten und vieles mehr.“ [35]

Mit dem BayernAtlas verfügt der Freistaat Bayern über eine Internetplattform, die der breiten Öffentlichkeit eine umfassende Palette an Geodaten zur Verfügung stellt. Geodaten sind alle Daten mit direktem oder indirektem Bezug zu einem bestimmten Standort oder geografischen Gebiet (vgl. Art. 3 Nr. 2 Richtlinie 2007/2/EG – INSPIRE-Richtlinie).[36] Das Spektrum so zugänglicher Daten ist sehr breit und betrifft nahezu jeden Lebensbereich: von Geologie- und Umweltdaten sowie Daten zu Naturgefahren bis hin zu Daten über die Bauleitplanung. Der in den BayernAtlas integrierte (kostenpflichtige) BayernAtlas-plus erweitert das bereitgestellte Angebot um weitere beziehungsweise genauere Daten, wie etwa Flurstücksnummern, Luftbilder mit einer höheren Auflösung oder Bodenschätzungsdaten.

Art. 3 INSPIRE-Richtlinie
Im Sinne dieser Richtlinie bezeichnet der Ausdruck
[…]
2. „Geodaten“ alle Daten mit direktem oder indirektem Bezug zu einem bestimmten Standort oder geografischen Gebiet;
[…].

Im Berichtszeitraum war ich aufgrund von Beratungsanfragen mehrerer Ressorts der Bayerischen Staatsregierung, aber auch aufgrund von Bürgerbeschwerden damit befasst, die Datenschutzkonformität der Bereitstellung von Geodaten im BayernAtlas näher zu beleuchten. Exemplarisch nennen möchte ich insoweit die Themen Solarpotentialdaten (vgl. dazu schon meinen 24. Tätigkeitsbericht 2010 unter Nr. 6.5) und Daten zur Denkmaleigenschaft von privaten Gebäuden.

35 Aus der Beschreibung des BayernAtlas auf der Internetpräsenz des Landesamts für Digitalisierung, Breitband und Vermessung, Internet: https://www.ldbv.bayern.de/produkte/dienste/bayernatlas.html.

36 Richtlinie (EG) 2007/2 des Europäischen Parlaments und des Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Union (ABl. L 108 vom 25. April 2007, S. 1), zuletzt geändert durch die Verordnung (EU) 2019/1010 des Europäischen Parlaments und des Rates vom 5. Juni 2019 (ABl. L 170 vom 25. Juni 2019, S. 115).

Allen diesen Fällen war gemeinsam, dass die Infrastruktur des BayernAtlas (entweder über separate Anwendungen oder über damit verknüpfte Dienste) genutzt wird oder werden sollte. Ich hatte jeweils insbesondere zu beurteilen, ob die über den BayernAtlas und den BayernAtlas-plus abrufbaren Geodaten als personenbezogene Daten (Art. 4 Nr. 1 DSGVO) zu werten sind und – wenn dies der Fall ist – Rechtsgrundlagen für die einschlägigen Datenverarbeitungen zur Verfügung stehen. Insofern waren Defizite festzustellen, so dass nach meinem derzeitigen Eindruck gesetzgeberischer Handlungsbedarf besteht. Insofern habe ich den betroffenen Ressorts bereits folgende Hinweise gegeben:

6.2.1 Auch Geodaten können personenbezogene Daten sein

Personenbezogene Daten sind nach Art. 4 Nr. 1 DSGVO alle Informationen, die sich **auf eine identifizierte oder identifizierbare natürliche Person beziehen.** Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

6.2.1.1 Personenbezogenheit einer Information

Geodaten haben qua Definition nach Art. 3 Nr. 2 INSPIRE-Richtlinie einen direkten oder indirekten Bezug zu einem bestimmten Standort. Von daher liegt es nahe, sie als bloße Sachdaten zu bewerten, also als Daten, die sich nur auf ein Objekt (etwa ein Gebäude oder ein Grundstück) beziehen und dieses beschreiben. Jedoch können auch solche Sachdaten mittelbar einen **Personenbezug** erhalten, wenn sie zugleich **eine Information enthalten,** die sich auf eine (identifizierbare) natürliche Person bezieht. Dies ist dann der Fall, wenn sie die Identität, die Merkmale oder das Verhalten dieser Person betreffen oder wenn sie verwendet werden, um die Art festzulegen oder zu beeinflussen, in der die Person behandelt oder beurteilt wird.[37] Damit muss der Information ein Inhalts-, Zweck- oder Ergebniselement innewohnen. Der Bezug zu einer natürlichen Person kann aufgrund **individualisierender Identifikationsmerkmale**, des **Detaillierungsgrads oder der Einzigartigkeit der Sache** hergestellt werden.[38]

So sind etwa Angaben über die Zugehörigkeit eines Grundstücks zu einer bestimmten Gemeinde bei isolierter Betrachtung Informationen, bei denen kein Inhalts-, Zweck- oder Ergebniselement feststellbar ist. Anders zu beurteilen sind aber beispielsweise Angaben über die wirtschaftliche Nutzung und Verwertung eines Grundstücks, da sie sich auf die Rechte und Interessen einer Person auswirken können (Ergebniselement), wenn ein Personenbezug durch die Verknüpfung mit einer punktbezogenen georeferenzierten Kennziffer, wie etwa Hausnummer, Flurstücksnummer oder konkreten Geokoordinaten hergestellt wird. Entsprechendes gilt auch für Flächendaten, wenn diese einen grundstücksgenauen Detaillierungsgrad erreichen, anhand dessen der – eine natürliche Person darstellende — Grundstückseigentümer

[37] Artikel-29-Datenschutzgruppe, Stellungnahme zum Begriff „personenbezogene Daten“, Stand 4/2007, WP 136, S.11, Internet: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_de.pdf.

[38] Klar/Kühling, in: Kühling/Buchner, Datenschutz-Grundverordnung/Bundesdatenschutzgesetz, 3. Aufl. 2020, Art. 4 Abs. 1 Rn. 13.

festgestellt werden kann (vgl. zum Ganzen schon meinen 21. Tätigkeitsbericht 2004 unter Nr. 14.1). Entfällt im Hinblick auf die Information hingegen das erforderliche Identifikationsmerkmal oder lässt der angebotene Detaillierungsgrad das Grundstück in einer größeren Menge anderer Grundstücken untergehen, so handelt es sich hierbei regelmäßig um ein bloßes Sachdatum.[39] In Übereinstimmung damit nimmt auch Erwägungsgrund 24 INSPIRE-Richtlinie an, dass Geodaten personenbezogene Daten sein können.

Daher stellt etwa die über den BayernAtlas-plus abrufbare Flurstücksnummer eines (durch die Anzeige des Standortes auf der Karte) bestimmten Grundstücks eine Information über die natürliche Person des Grundstückseigentümers und dessen Vermögen dar. Aber auch im Übrigen enthält der BayernAtlas sachbezogene Informationen, welche durch eine unschwer mögliche Verschneidung mit weiteren Informationen (zum Beispiel aus der Parzellenkarte oder Adressenangaben usw.) Aussagen über die persönlichen und sachlichen Verhältnisse bestimmbarer natürlicher Person zulassen können. Dies scheint mir etwa der Fall zu sein bei der flurstücks- bzw. grundstücksgenauen Darstellung von Überschwemmungsgebieten oder auch der Denkmaleigenschaft konkreter Gebäude. In Zweifelsfällen rate ich daher, von einer Personenbeziehbarkeit auszugehen.[40]

6.2.1.2 Identifizierbarkeit

Die natürliche Person, auf die sich die bereitgestellten Informationen (mittelbar) beziehen, muss aber auch zumindest **identifizierbar** sein. Hierfür ist es nach Erwägungsgrund 26 DSGVO nicht notwendig, dass der Verantwortliche selbst die Identifizierung durchführen kann. Es ist vielmehr ausreichend, dass irgendein Dritter nach allgemeinem Ermessen diese wahrscheinlich durchführen kann[41].

Umgekehrt gilt aber auch: Ist bei einem gezieltermaßen auf einen massenhaften Datenabruf ausgerichteten System bei dem Verantwortlichen selbst das Wissen über die konkret betroffene Person unproblematisch vorhanden, so ist das Merkmal der Identifizierbarkeit generell — und damit auch aus der Perspektive der unbestimmten Vielzahl der die Daten Abrufenden — erfüllt. Dies trifft in besonderer Weise für die der Öffentlichkeit im BayernAtlas bereitgestellten Geodaten zu. Insoweit können die betroffenen Grundstückseigentümer durch den Verantwortlichen (hier: das Landesamt für Digitalisierung, Breitband und Vermessung) problemlos über das Liegenschaftskataster identifiziert werden, worauf dieser Zugriff hat. Hierbei kommt der Flurstücksnummer eine Doppelbedeutung zu. Bezogen auf ein konkretes Grundstück ist sie selbst ein personenbezogenes Datum. Im Hinblick auf weitere sich auf das Grundstück beziehende Informationen dient sie als individualisierendes Identifikationsmerkmal.

6.2.2 Erfordernis einer Rechtsgrundlage

Werden personenbezogene Geodaten im BayernAtlas proaktiv und generell bereitgestellt (zum Beispiel durch Anzeige auf einer Karte oder durch Einblenden von detaillierten Informationen in einem separaten Fenster nach Anklicken des jeweiligen

39 Schild, in: Wolff/Brink, Beck'scher Online-Kommentar Datenschutzrecht, Stand 11/2021, Art. 4 DSGVO Rn. 23, 24.

40 Vgl. insoweit auch Verwaltungsgericht Wiesbaden, Urteil vom 4. November 2019, 6 K 460/16. WI, BeckRS 2019, 33849, Rn. 52.

41 Klabunde, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 4 Rn. 17.

Objekts) werden diese gemäß Art. 4 Nr. 2 DSGVO verarbeitet. Diese Verarbeitung bedarf einer Rechtsgrundlage gemäß Art. 6 Abs. 1 DSGVO. Insoweit besteht jedoch nach meinem derzeitigen Eindruck gesetzgeberischer Handlungsbedarf. Insbesondere habe ich die betroffenen Ressorts bereits auf folgende Defizite der aktuellen Rechtslage aufmerksam gemacht:

6.2.2.1 Bloßes Einsichtsrecht nach dem Vermessungs- und Katastergesetz

Art. 11 Abs. 1 Satz 1 bis 3 Vermessungs- und Katastergesetz (VermKatG) vermitteln – bei vorhandenem berechtigten Interesse – ein **Einsichtsrecht** in – personenbezogene – Daten des Liegenschaftskatasters beziehungsweise ein entsprechendes Recht auf Auskunft sowie Erstellung von Auszügen. Diese individuell durchsetzbaren Rechte können jedoch bereits aufgrund der hiermit verbundenen tatsächlichen höheren Hürden bei deren Geltendmachung **nicht** mit **einer proaktiven, anlasslosen und generellen Veröffentlichung** in einem frei zugänglichen Portal **gleichgestellt werden.** Diesen qualitativen Unterschied hat der Gesetzgeber im Übrigen selbst anerkannt, indem er in Art. 3 Abs. 2 Bayerisches Umweltinformationsgesetz (BayUIG) zwischen einer Akteneinsicht beziehungsweise Auskunft und einer proaktiven Unterrichtung der Öffentlichkeit nach Art. 10 BayUIG unterscheidet. Zusammengefasst erlaubt das Vermessungs- und Katastergesetz daher bereits von seiner Rechtsfolge her keine Veröffentlichung von Daten.

Art. 11 VermKatG
Einsicht, Auskunft und Benutzung des Liegenschaftskatasters, Verordnungsermächtigung
(1) [1]Jedem wird Einsicht in das Liegenschaftskataster gewährt und Auskunft erteilt, soweit nicht Interessen des öffentlichen Wohls entgegenstehen. [2]Auszüge aus dem Liegenschaftskataster werden auf Antrag erstellt. [3]Für die Einsicht in personenbezogene Daten sowie für Auskünfte und Auszüge aus Verzeichnissen, die personenbezogene Daten enthalten, ist ein berechtigtes Interesse darzulegen; das gilt nicht für die Bezeichnung von Flurstücken sowie für die in Art. 6 Abs. 3 genannten Inhalte des Liegenschaftskatasters. […]

Das Gleiche gilt im Übrigen auch für das Gesetz zum Schutz und zur Pflege der Denkmäler (Bayerisches Denkmalschutzgesetz – BayDSchG), welches in dessen Art. 2 Abs. 1 Satz 5 BayDSchG nur eine Einsicht in die Denkmalliste, nicht aber die praktizierte Veröffentlichung der (kartengebundenen) Denkmalliste im Internet erlaubt.

6.2.2.2 Bayerisches Geodateninfrastrukturgesetz gilt nur für betroffene Geodaten und erfordert Abwägung

Das Bayerische Geodateninfrastrukturgesetz (BayGDIG) sieht für sogenannte **betroffene Geodaten** im Sinne des Art. 2 Abs. 1 BayGDIG zwar die Verpflichtung vor, diese öffentlich zur Verfügung zu stellen. Der Zugang erfolgt auch durch ein Geoportal des Landes. Jedoch ist bei personenbezogenen Daten nach Art. 8 Abs. 3 Satz 2 Nr. 1 BayGDIG 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 (siehe dazu schon meinen 23. Tätigkeitsbericht 2008 unter Nr. 24.2). Die hiernach erforderliche **Interessenabwägung** wird aber oftmals dazu führen, dass die betroffenen Grundstückseigentümer ein **überwiegendes schutzwürdiges Interesse** daran haben, dass Daten zur Nutzung oder Werthaftigkeit ihres Grundstücks

nicht ohne ihre Einwilligung im Internet weltweit veröffentlicht werden und in der Folge gewerblich genutzt werden können.

Art. 8 BayGDIG
Nutzung
(3) [1][…]. [2]Soweit
1. durch den Zugang zu Geodaten personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt würden,
2. Betriebs- oder Geschäftsgeheimnisse zugänglich gemacht würden,
ist der Zugang zu beschränken, 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. [3][…].

Daneben habe ich derzeit aber auch erhebliche Zweifel daran, dass alle über den BayernAtlas und den BayernAtlas-plus abrufbaren Daten sogenannte betroffene Geodaten nach Art. 2 Abs. 1 BayGDIG sind, also eines oder mehrere Themen nach den Anhängen I, II oder III der INSPIRE-Richtlinie betreffen. Dies gilt insbesondere für die Flurstücksnummer, Daten zur Bodenschätzung oder die Eigenschaft als Baudenkmal.

6.2.2.3 Anhörungserfordernis nach dem Bayerischen Umweltinformationsgesetz

Auch das gegenüber dem Bayerischen Geodateninfrastrukturgesetz nach Art. 8 Abs. 3 Satz 2 Halbsatz 2 Var. 3 BayGDIG vorrangige Bayerische Umweltinformationsgesetz (BayUIG) sieht im Hinblick auf die Veröffentlichung von Umweltdaten in Art. 8 Abs. 1 Nr. 1 BayUIG eine ähnliche **Einzelfallabwägung der Interessen** vor. Darüber hinaus verpflichtet die Norm in deren Satz 3 aber zusätzlich dazu, die Betroffenen vor der Entscheidung über die Offenbarung der Informationen **anzuhören.**

6.2.3 Ausblick

Um einer sich derzeit abzeichnenden Zersplitterung entsprechender Veröffentlichungsbefugnisse in verschiedenen Fachgesetzen vorzubeugen, habe ich mich gegenüber den betroffenen Ressorts für eine übergreifende und zukunftsoffene gesetzliche Lösung eingesetzt. Hierfür wäre nach meiner derzeitigen Auffassung eine Überarbeitung und Ergänzung des Bayerischen Geodateninfrastrukturgesetzes gut geeignet. Soweit veranlasst, werde ich hierzu erneut berichten.

7 Soziales und Gesundheit

7.1 Vollzug des Masernschutzgesetzes durch Kindertageseinrichtungen und Gesundheitsämter

Im Berichtszeitraum haben mich zahlreiche Bürgeranfragen zum Vollzug des Masernschutzgesetzes im Zusammenhang mit dem Besuch von Kindertageseinrichtungen in öffentlich-rechtlicher Trägerschaft erreicht. Die Anfragen bezogen sich auf Datenverarbeitungen zum einen durch die Kindertageseinrichtungen, zum anderen durch die bayerischen Gesundheitsämter.

7.1.1 Rechtsgrundlagen

Seit 1. März 2020 gilt bundesweit das Masernschutzgesetz. In Gemeinschaftseinrichtungen wie Kindertagesstätten besteht nach § 20 Infektionsschutzgesetz (IfSG) für dort Betreute und Beschäftigte die Pflicht, einen Nachweis bezüglich ihres Masernimmunstatus zu erbringen. Wenn eine verpflichtete Person minderjährig ist, müssen die Sorgeberechtigten den Nachweis erbringen. Die Leitung der Einrichtung hat den Nachweis zu prüfen und unter bestimmten Umständen das Gesundheitsamt zu informieren.

Dies bedeutet, dass für alle Kinder, die ab dem 1. März 2020 in eine Kindertageseinrichtung aufgenommen werden, vor dem Beginn der Betreuung ein Nachweis gemäß Masernschutzgesetz vorgelegt werden muss (§ 20 Abs. 8 IfSG). Für alle Kinder, die am 1. März 2020 bereits eine Kindertageseinrichtung besuchen, muss der Nachweis bis zum Ablauf des 31. Juli 2022 erbracht werden (§ 20 Abs. 10 IfSG). Entsprechendes gilt für in den Kindertageseinrichtungen tätige Personen, sofern sie nach 1970 geboren sind.

Den Nachweis kann die betreffende Person gemäß § 20 Abs. 9 IfSG erbringen

- durch Vorlage eines Impfausweises oder eines ärztlichen Zeugnisses (auch in Form einer Anlage zum Untersuchungsheft für Kinder) darüber, dass bei ihr ein altersentsprechender Impfschutz gegen Masern besteht,
- durch ein ärztliches Zeugnis darüber, dass bei ihr eine Immunität gegen Masern vorliegt (durch eine Titerbestimmung), oder
- durch ein ärztliches Zeugnis darüber, dass sie aufgrund einer dauerhaften medizinischen Kontraindikation nicht geimpft werden kann.

Zum Inhalt eines Kontraindikationsattests hat das Bayerische Staatsministerium für Gesundheit und Pflege mir gegenüber geäußert, dass darin lediglich Angaben zur zeitlichen Dauer von Kontraindikationen enthalten sein müssen (Feststellung, dass die betreffende Person aufgrund einer medizinischen Kontraindikation nicht gegen Masern geimpft werden kann), nicht aber Angaben zum medizinischen Grund der Kontraindikation.

Alternativ kommt auch eine Bestätigung einer staatlichen Stelle oder der Leitung einer anderen vom Gesetz betroffenen Einrichtung darüber in Betracht, dass ein Nachweis bereits vorgelegen hat.

7.1.2 Datenschutzkonforme Vorlage bei der Kindertageseinrichtung – Dokumentation ohne Kopie des Nachweises

Es wurde wiederholt die Frage an mich herangetragen, wie bei Kindern in Kindertageseinrichtungen die Vorlage des Nachweises zum Masernimmunstatus zu dokumentieren sei, insbesondere, ob die Kindertageseinrichtung den Nachweis kopieren und zum Kinderakt nehmen dürfe.

Die Frage ist in Hinblick auf den Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) dahin zu beantworten, dass der Nachweis durch die (auf das Erforderliche beschränkte) Gewährung der Einsicht in den Impfpass (beziehungsweise das Kinderuntersuchungsheft) oder durch Vorlage einer ärztlichen Bescheinigung geführt werden kann. Die Einsicht in den vollständigen Impfpass (beziehungsweise das vollständige Nachweisheft) ist grundsätzlich nicht erforderlich und daher unzulässig.

Die Vorlage des Impfpasses bezieht sich grundsätzlich auf das Originaldokument. Geschwärzte Fotos oder Scans des Impfpasses müssen von der Einrichtung nicht akzeptiert werden, da aufgrund des fehlenden Personenbezugs der Einzelseiten des Impfpasses im Fall von Fotokopien die Zuordnung zu einer konkreten Person nicht hinreichend gewährleistet ist.

Die für den Nachweis bei der Kindertageseinrichtung vorgelegten Dokumente sind nur zur Prüfung der Voraussetzungen notwendig. Die Aufbewahrung von Kopien der vorgelegten Nachweise ist nach Abschluss der Prüfung regelmäßig nicht erforderlich und damit unzulässig.

Der Nachweis soll lediglich im erforderlichen Umfang (Erfüllung oder Nichterfüllung der Voraussetzungen des § 20 Abs. 9 IfSG) schriftlich – idealerweise in der hierfür vorgesehenen Dokumentationshilfe – dokumentiert und in dieser Form zu den Akten genommen werden.[42]

Mir wurde ebenfalls davon berichtet, dass verschiedene Gesundheitsämter Kindertageseinrichtungen zur Kopie und Aufbewahrung des Nachweises in den Unterlagen der Gemeinschaftseinrichtung aufgefordert hätten. Aus den genannten Gründen halte ich auch eine solche Aufforderung für nicht datenschutzkonform.

7.1.3 Meldung an das zuständige Gesundheitsamt

Das Masernschutzgesetz sieht vor, dass die Leitung der Kindertageseinrichtung das zuständige Gesundheitsamt unverzüglich zu benachrichtigen hat, wenn ein im Einzelfall zu führender Nachweis nach dem Masernschutzgesetz nicht vorgelegt wird, oder wenn sich ergibt, dass ein Impfschutz gegen Masern erst zu einem späteren Zeitpunkt

[42] Bayerisches Staatsministerium für Gesundheit und Pflege, Dokumentationshilfe für Einrichtungen bzw. Übermittlungsbogen an das zuständige Gesundheitsamt, Internet: https://www.lgl.bayern.de/gesundheit/praevention/impfen/masernschutzgesetz.htm.

möglich ist oder vervollständigt werden kann. Dabei ist zu beachten, dass bei Nichtvorlage des Nachweises eine Datenübermittlung erst mit Ablauf des im Gesetz benannten Stichtages zulässig ist.

Die Anforderungen nach dem Masernschutzgesetz können auch dann als nicht erfüllt bewertet werden, wenn die vorgelegten Nachweise/Bescheinigungen nicht eindeutig waren oder die Einrichtungsleitung auf Tatsachen basierte Zweifel an der Glaubwürdigkeit des Attests hat. Auch in diesen Fällen erscheint daher eine Datenübermittlung an das Gesundheitsamt datenschutzrechtlich zulässig (siehe § 20 Abs. 9 Satz 2, § 20 Abs. 9a Satz 2 IfSG).

7.1.4 Übermittlung einer Kopie des Nachweises nur mit Einwilligung

Sofern die Voraussetzungen für eine Meldung an das Gesundheitsamt vorliegen, umfasst die Benachrichtigungspflicht nach § 20 Abs. 9 und Abs. 9a IfSG lediglich die Übermittlung der im Gesetz genannten personenbezogenen Angaben (Name und Vorname, Geschlecht, Geburtsdatum, Anschrift der Hauptwohnung oder des gewöhnlichen Aufenthaltsortes und, falls abweichend, Anschrift des derzeitigen Aufenthaltsortes der betroffenen Person sowie, soweit vorliegend, Telefonnummer und E-Mail-Adresse, vgl. § 2 Nr. 16 IfSG) und den Grund für die Meldung gemäß der Dokumentationshilfe. Die Dokumentationshilfe dient dabei zugleich als Übermittlungsbogen an das zuständige Gesundheitsamt.

Für das Anfertigen einer Kopie des Nachweises durch die Gemeinschaftseinrichtung und die Übersendung an das Gesundheitsamt existiert keine gesetzliche Datenverarbeitungsbefugnis. Nur bei Vorliegen einer ausdrücklichen Einwilligung der betroffenen Person gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 9 Abs. 2 Buchst. a DSGVO ist dieses Vorgehen datenschutzrechtlich zulässig. Die nach Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 4 Nr. 11, Art. 7 DSGVO für die Einwilligung geltenden Voraussetzungen, insbesondere die Freiwilligkeit der Erteilung, sind dabei strikt zu beachten. In der Vollzugspraxis dürfte dies in erster Linie Fälle betreffen, in denen Eltern von sich aus den Einrichtungen Nachweise überlassen. Nach Art. 7 Abs. 1 DSGVO muss die verantwortliche Einrichtung dann insoweit nachweisen können, dass eine wirksame Einwilligung vorliegt.

Aufforderungen der Gesundheitsämter an die Kindertageseinrichtungen, Kopien der Nachweise zu übermitteln, sind daher ebenfalls datenschutzrechtlich unzulässig, sofern das Erfordernis der Einwilligung dabei nicht beachtet wird.

7.1.5 Keine Übermittlung von Listen über vorgelegte Kontraindikationsnachweise

Vereinzelt wurden mir Fälle geschildert, in denen Gesundheitsämter bei Kindertageseinrichtungen Listen mit personenbezogenen Angaben zu Kindern angefordert haben, für die eine ärztliche Bescheinigung über das Bestehen einer vorübergehenden oder dauerhaften Kontraindikation vorgelegt wurde. Meiner vom Gesundheits- und vom Sozialministerium geteilten Ansicht nach ist weder eine solche Datenerhebung des Gesundheitsamtes noch die Datenübermittlung durch die Kindertageseinrichtung von einer gesetzlichen Grundlage gedeckt und daher datenschutzrechtlich unzulässig. In dieser Fallkonstellation offenkundig nicht einschlägig ist insbesondere § 20 Abs. 9 IfSG, auf die sich einzelne Gesundheitsämter berufen hatten.

7.1.6 Datenverarbeitungsbefugnisse des Gesundheitsamtes

Als Folge der Benachrichtigungspflicht kann das zuständige Gesundheitsamt nach § 20 Abs. 12 IfSG die zum Nachweis verpflichtete Person zu einer Beratung laden und gegebenenfalls weitere Maßnahmen anordnen (förmliches Auffordern zur Nachholung der Impfung bis hin zum Erlass eines Betretungsverbotes der Einrichtung).

§ 20 Abs. 12 IfSG enthält generell die Befugnis des Gesundheitsamtes, sich auf Anforderung die entsprechenden Nachweise von Personen vorlegen zu lassen, die in Kindertageseinrichtungen betreut werden. Von welchen Personen das Gesundheitsamt einen solchen Nachweis anfordert, steht in seinem Ermessen. Die Gesundheitsämter dürfen ihn daher selbst kontrollieren – unabhängig von der durch die Einrichtung vorgenommenen Bewertung des Nachweises und auch dann, wenn sie keine Benachrichtigung durch die Leitung der Einrichtung erhalten haben.

7.1.7 Datenschutzkonforme Vorlage und Prüfung des Nachweises beim Gesundheitsamt

Zu der Frage, was unter Vorlage des Nachweises im Sinne von § 20 Abs. 12 IfSG zu verstehen ist, vertrete ich die Auffassung, dass eine Vorlage des Nachweises die (kurzfristige) Aushändigung des Originals einschließt. Dies gilt jedenfalls für eine vorübergehende Entgegennahme etwa zur Überprüfung des Dokuments.

Möglicherweise kann eine Entscheidung, ob das ärztliche Attest als Nachweis im Sinne des § 20 Abs. 9 Satz 1 IfSG anerkannt werden kann, im Zeitpunkt der Vorlage nicht abschließend getroffen werden. Das Gesundheitsamt darf nach meinem Dafürhalten in diesem Fall im Rahmen der Erforderlichkeit zur Erfüllung seiner gesetzlich vorgegebenen (Prüf-)Aufgaben ausnahmsweise eine Kopie des vorgelegten Attestes anfertigen. Die rechtlichen Grundlagen dafür finden sich in § 20 Abs. 12 IfSG in Verbindung mit Art. 6 Abs. 1 UAbs. 1 Buchst. c in Verbindung mit Abs. 3 Satz 1 Buchst. b, Art. 9 Abs. 2 Buchst. i DSGVO (dies ist abzugrenzen von der Aufforderung von Gesundheitsämtern gegenüber Kindertageseinrichtungen, Kopien von Nachweisen pauschal bzw. präventiv zu übermitteln; insoweit ist eine gesetzliche Befugnis zu verneinen, siehe Nr. 7.1.4.).

Die Kopie des Attestes darf grundsätzlich nur so lange aufbewahrt werden, bis der Zweck, für den die Kopie angefertigt wurde, erfüllt ist. Grundsätzlich besteht danach ein Recht auf Löschung nach Art. 17 Abs. 1 Buchst. a DSGVO.

7.2 Vollzug des Masernschutzgesetzes in Krankenhäusern

Im Berichtszeitraum haben mich Anfragen zum Vollzug des Masernschutzgesetzes in Krankenhäusern öffentlich-rechtlicher Träger erreicht. Die Anfragen betrafen Patientinnen und Patienten, die in den entsprechenden Einrichtungen betreut wurden, aber auch in der und für die Einrichtung tätige Personen.

Gemäß § 20 Abs. 8 und 9 Infektionsschutzgesetz (IfSG) müssen Personen, die nach dem 31. Dezember 1970 geboren sind und in bestimmten Einrichtungen wie zum Beispiel Krankenhäusern **betreut werden oder tätig sind**, den Nachweis eines Impfschutzes oder der Immunität gegen Masern erbringen oder den Nachweis, dass aufgrund einer medizinischen Kontraindikation nicht geimpft werden kann.

Der Nachweis ist bei Neuaufnahmen seit dem 1. März 2020 vor Beginn der Betreuung beziehungsweise vor Aufnahme der Tätigkeit zu erbringen. Gemäß § 20 Abs. 10 IfSG haben Personen, die am 1. März 2020 bereits in Einrichtungen betreut wurden oder dort tätig waren, der Leitung der jeweiligen Einrichtung einen Nachweis **bis zum Ablauf des 31. Juli 2022** vorzulegen.

Zu klären waren insbesondere folgende Fragestellungen:

1. Sind Kopien des Impfpasses bzw. der ärztlichen Bescheinigung bei der Einrichtung zulässig?

2. Wie weit ist der Personenkreis zu fassen, der in diesen Einrichtungen „tätig" ist und wie ist der Nachweis zu erbringen?

Zu 1.: Zur Frage der **Kopien** vertrete ich die Auffassung, dass der Nachweis durch die (auf das Erforderliche beschränkte) Gewährung der Einsicht in den Impfpass oder durch Vorlage einer ärztlichen Bescheinigung geschehen kann. Die Einsicht in den vollständigen Impfpass sowie das Fertigen von Kopien sind daher ebenso wie die anschließende Aufbewahrung datenschutzrechtlich nicht erforderlich und daher unzulässig.

Zur Erfüllung der Dokumentationspflicht der im Masernschutzgesetz genannten Einrichtungen sehe ich es als ausreichend an, wenn die verantwortliche Einrichtungsleitung schriftlich dokumentiert, dass einer der im Masernschutzgesetz genannten Nachweise vorgelegt wurde, und diese Dokumentation zu den Akten nimmt.

Zu 2.: Mich beschäftigte darüber hinaus insbesondere die Frage, **welcher Personenkreis als „tätig"** im Sinne des § 20 Abs. 8 und 9 IfSG anzusehen ist. Ein großer Sozialträger verlangte von allen Geschäftspartnern vorab in Kopie einen Impfnachweis ihrer Beschäftigten (Handwerker, Installateure, Kundendienstmonteure usw.) und drohte damit, andernfalls die externen Dienstleister nicht in das Haus zu lassen und dem Gesundheitsamt zu melden.

Ich habe die Auffassung vertreten, dass diese Auslegung der genannten Vorschriften zu weitgehend ist. Nach der Gesetzesbegründung sollen zwar auch Personen erfasst sein, die nicht unmittelbar mit den Bewohnern der Einrichtung in Kontakt sind, allerdings ist erkennbar, dass es sich um Personen handeln soll, die in einer engen Verbindung zur Einrichtung stehen. Folgende Personen werden vom Gesetzgeber genannt:[43]

— medizinisches Personal (Einrichtungen nach § 23 Abs. 3 Satz 1 IfSG);

— Lehr- und Erziehungspersonal (Einrichtungen nach § 33 Nr. 1 bis 4 IfSG);

— Pflege- oder Aufsichtspersonal (Einrichtungen nach § 36 Abs. 1 Nr. 4 IfSG);

— Hausmeisterinnen und Hausmeister;

— Transportpersonal;

— Küchenpersonal;

[43] Vgl. Bundestags-Drucksache 19/13452, S. 28 zu § 20 Abs. 8 Nr. 3 IfSG.

- Reinigungspersonal;
- ehrenamtlich Tätige;
- Praktikanten.

In Abstimmung mit dem Bayerischen Staatsministerium für Gesundheit und Pflege habe ich dem Sozialträger folgende Hinweise gegeben, die dabei helfen sollen, die Verarbeitung von Gesundheitsdaten im Rahmen des Masernschutzgesetzes nur auf das erforderliche Maß zu beschränken:

Bei externen Dienstleistern (wie etwa Handwerkerinnen und Handwerkern, Installateurinnen und Installateuren oder Kundendienstmonteurinnen und Kundendienstmonteuren) ist nicht nur pauschal, sondern **im Einzelfall** vom verantwortlichen Träger zu beurteilen, ob eine Nachweispflicht besteht.

Die Nachweispflicht nach § 20 Abs. 8, Abs. 9 IfSG gilt für alle Personen, die in der Einrichtung **regelmäßig und zeitlich nicht nur vorübergehend** tätig sind.

„Regelmäßig" ist eine Tätigkeit insbesondere dann, wenn sie **nicht nur für wenige Tage** verrichtet wird. „Nicht nur zeitlich vorübergehend" ist eine Tätigkeit dann, wenn sie nicht nur jeweils wenige Minuten, **sondern über einen längeren Zeitraum** anhält.

Nicht nachweispflichtige Tätigkeiten im Sinne des Masernschutzgesetzes sind insbesondere:

- Einzelaufträge bis zu 14 Tagen („absolute Grenze");
- wiederkehrende Tätigkeiten bis zu 1 Tag pro Monat (also pro Jahr maximal 12 × 1 Tag);
- Tätigkeiten, die ausschließlich auf den außerhalb der Räumlichkeiten bestehenden Baustellen stattfinden.

Bei Dienstleistern, die regelmäßig und zeitlich nicht nur vorübergehend in der Einrichtung tätig sind, genügt es zur Erfüllung der Nachweispflicht, wenn die verantwortliche Einrichtungsleitung belegen kann, dass sie die eingesetzten Dienstleister privatrechtlich verpflichtet hat, nur den Anforderungen des Masernschutzgesetzes entsprechende Personen in der Einrichtung einzusetzen. Es genügt auch, dass sie diese Verpflichtung an die Stellen kommuniziert hat, die die Verträge mit externen Dienstleistern abgeschlossen haben und dies bei einer Kontrolle durch das Gesundheitsamt belegen kann. Die verantwortliche Einrichtungsleitung kann sich die Nachweise im Einzelfall aber auch selbst vorlegen lassen, eine Verpflichtung hierzu besteht jedoch nicht.

7.3 Datenschutzrechtliche Anforderungen an Reihentestungen auf den Erreger SARS-CoV-2 in (Rehabilitations- und Pflege-) Einrichtungen

Im Verlauf der COVID-19-Pandemie erreichte mich die Beratungsanfrage der behördlichen Datenschutzbeauftragten einer Kreisverwaltungsbehörde im Zusammenhang mit gesundheitsbehördlich angeordneten Reihentestungen von Bewohnerinnen, Bewohnern und des Personals in Rehabilitations- und Pflegeeinrichtungen auf den Erreger SARS-CoV-2.

7.3.1 Datenerhebung aufgrund einer behördlichen Anordnung oder aufgrund einer datenschutzrechtlichen Einwilligung

Zunächst wurde die Frage aufgeworfen, ob es im Wirkungsbereich einer gesundheitsbehördlich angeordneten Reihentestung in einer konkreten Pflegeeinrichtung hinsichtlich der damit beabsichtigten, umfassenden Erhebung von Testergebnissen einer datenschutzrechtlichen Einwilligung der betroffenen Personen bedarf. Dabei wurde innerhalb des verantwortlichen Landratsamtes im Austausch mit der behördlichen Datenschutzbeauftragten diskutiert, ob es insofern maßgeblich auf eine Abwägung des (möglicherweise als vorrangig zu beurteilenden) öffentlichen Interesses gegenüber dem Interesse der betroffenen Personen ankommen könnte.

Dazu habe ich die folgenden datenschutzrechtlichen Hinweise gegeben:

Tritt in Einrichtungen, wie zum Beispiel einem Senioren- oder Pflegeheim, ein COVID-19-Fall auf, ist aufgrund der Art der Übertragung von SARS-CoV-2 (angesichts der seinerzeit im November/Dezember 2020 noch mangelnden Verfügbarkeit eines Impfstoffs) von einem allgemeinen Ansteckungsverdacht in Bezug auf das (Pflege-) Personal sowie die Bewohnerinnen und Bewohner auszugehen. In der Regel legitimiert dieser Ansteckungsverdacht gemäß § 25 Abs. 1, Abs. 3 Satz 2 Infektionsschutzgesetz (IfSG) die behördliche Anordnung der Reihenuntersuchung (im Gegensatz zu einer anlasslosen Reihentestung, die nach § 25 IfSG nicht erlaubt wäre).

§ 25 IfSG
Ermittlungen
(1) Ergibt sich oder ist anzunehmen, dass jemand krank, krankheitsverdächtig, ansteckungsverdächtig oder Ausscheider ist oder dass ein Verstorbener krank, krankheitsverdächtig oder Ausscheider war, so stellt das Gesundheitsamt die erforderlichen Ermittlungen an, insbesondere über Art, Ursache, Ansteckungsquelle und Ausbreitung der Krankheit. Das Gesundheitsamt kann auch Ermittlungen anstellen, wenn sich ergibt oder anzunehmen ist, dass jemand durch eine Schutzimpfung oder andere Maßnahme der spezifischen Prophylaxe eine gesundheitliche Schädigung erlitten hat.
(2) Für die Durchführung der Ermittlungen nach Absatz 1 gilt § 16 Absatz 1 Satz 2, Absatz 2, 3, 5 und 8 entsprechend. Das Gesundheitsamt kann eine im Rahmen der Ermittlungen im Hinblick auf eine bedrohliche übertragbare Krankheit erforderliche Befragung in Bezug auf die Art, Ursache, Ansteckungsquelle und Ausbreitung der Krankheit unmittelbar an eine dritte Person, insbesondere an den behandelnden Arzt, richten, wenn eine Mitwirkung der betroffenen Person oder der nach § 16 Absatz 5 verpflichteten Person nicht oder nicht rechtzeitig möglich ist; die dritte Person ist in entsprechender Anwendung von § 16 Absatz 2 Satz 3 und 4 zur Auskunft verpflichtet.
(3) Die in Absatz 1 genannten Personen können durch das Gesundheitsamt vorgeladen werden. Sie können durch das Gesundheitsamt verpflichtet werden,

1. Untersuchungen und Entnahmen von Untersuchungsmaterial an sich vornehmen zu lassen, insbesondere die erforderlichen äußerlichen Untersuchungen, Röntgenuntersuchungen, Tuberkulintestungen, Blutentnahmen und Abstriche von Haut und Schleimhäuten durch die Beauftragten des Gesundheitsamtes zu dulden, sowie
2. das erforderliche Untersuchungsmaterial auf Verlangen bereitzustellen.

Darüber hinausgehende invasive Eingriffe sowie Eingriffe, die eine Betäubung erfordern, dürfen nur mit Einwilligung des Betroffenen vorgenommen werden; § 16 Absatz 5 gilt nur entsprechend, wenn der Betroffene einwilligungsunfähig ist. Die bei den Untersuchungen erhobenen personenbezogenen Daten dürfen nur für Zwecke dieses Gesetzes verarbeitet werden.
[…]

Gemäß § 25 Abs. 2 Satz 1 IfSG in Verbindung mit § 16 Abs. 1 Satz 2 IfSG kann die zuständige Behörde im Rahmen ihrer sogenannten Ermittlungsmaßnahmen personenbezogene Daten erheben.

§ 16 IfSG
Allgemeine Maßnahmen zur Verhütung übertragbarer Krankheiten
(1) Werden Tatsachen festgestellt, die zum Auftreten einer übertragbaren Krankheit führen können, oder ist anzunehmen, dass solche Tatsachen vorliegen, so trifft die zuständige Behörde die notwendigen Maßnahmen zur Abwendung der dem Einzelnen oder der Allgemeinheit hierdurch drohenden Gefahren. Im Rahmen dieser Maßnahmen können von der zuständigen Behörde personenbezogene Daten erhoben werden; diese dürfen nur von der zuständigen Behörde für Zwecke dieses Gesetzes verarbeitet werden.
[…]

Die Datenschutz-Grundverordnung lässt derartige, auf Fachrecht beruhende Anordnungen, die eine datenschutzrechtliche Verarbeitungsbefugnis vermitteln, auf nationaler Ebene zu (siehe Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2, Abs. 3 UAbs. 1 Buchst. b DSGVO).

Neben einer solchen nationalen Regelung, welche die zweckgebundene Verarbeitung von Gesundheitsdaten erlaubt, bleibt für eine datenschutzrechtliche Einwilligung grundsätzlich kein Raum. Dies verdeutlicht beispielsweise Erwägungsgrund 54 Satz 1 DSGVO.

„Aus Gründen des öffentlichen Interesses in Bereichen der öffentlichen Gesundheit kann es notwendig sein, besondere Kategorien personenbezogener Daten auch ohne Einwilligung der betroffenen Person zu verarbeiten."

Für das Zusammenspiel zwischen Einwilligung und gesetzlichen Erlaubnistatbeständen wird hier deutlich, dass die Einwilligung nicht als Ergänzung neben die gegebene Anordnungsbefugnis treten soll. Denn grundsätzlich ist nicht zu empfehlen, eine Verarbeitung sowohl auf eine datenschutzrechtliche Einwilligung als auch auf einen gesetzlichen Verarbeitungstatbestand zu stützen. Unzulässig sind Einwilligungen regelmäßig auch dann, wenn die Anwendung eines im Grunde einschlägigen gesetzlichen Verarbeitungstatbestands an einem Grundsatz der Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 DSGVO) scheitert. Dabei soll zugleich vermieden werden, dass die datenverarbeitende Stelle etwa im Falle der Verweigerung, des Widerrufs oder der Unwirksamkeit einer Einwilligung doch wieder auf einen gesetzlichen Erlaubnistatbestand zurückgreifen könnte.[44]

Dies ist auch unter dem Aspekt der Freiwilligkeit der Einwilligung folgerichtig. Gemäß Art. 4 Nr. 11 DSGVO ist die Einwilligung eine freiwillige Willensbekundung.

Art. 4 DSGVO
Begriffsbestimmungen
Im Sinne dieser Verordnung bezeichnet der Ausdruck:
[…]
11. „Einwilligung" der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in

[44] Siehe Buchner/Petri, in: Kühling/Buchner, Datenschutz-Grundverordnung/Bundesdatenschutzgesetz, 3. Aufl. 2020, Art. 6 DSGVO Rn. 23.

Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;
[…].

Von Freiwilligkeit kann jedoch keine Rede sein, sofern die betroffene Person zu einem bestimmten Tun, Dulden oder Unterlassen aufgrund einer behördlichen Anordnung verpflichtet ist.

Im Ergebnis ist festzuhalten, dass die Erhebung personenbezogener Testergebnisse durch die zuständige Behörde im Rahmen einer von ihr gemäß § 25 IfSG angeordneten Reihenuntersuchung auf den Erreger SARS-CoV-2 in einer (Rehabilitations- und Pflege-) Einrichtung keiner zusätzlichen Einwilligung der betroffenen Personen bedarf. Auf die in diesem Zusammenhang seitens des zuständigen Landratsamtes mir gegenüber als Argument in Betracht gezogene Abwägung des öffentlichen Interesses mit den privaten Interessen des Betroffenenkreises kommt es insofern **nicht** an.

7.3.2 Übermittlungsbefugnis des Gesundheitsamts auf Ersuchen der Einrichtungsleitung

Im Anschluss wurde von Seiten der behördlichen Datenschutzbeauftragten des verantwortlichen Landratsamtes die Frage an mich herangetragen, ob das betreffende Gesundheitsamt die Ergebnisse sämtlicher aufgrund entsprechender Anordnung getesteten Personen (sowohl der Beschäftigten als auch der Bewohnerinnen und Bewohner und gegebenenfalls der Patientinnen und Patienten) an die Einrichtungsleitung (auf deren Ersuchen hin) übermitteln darf.

Aus datenschutzrechtlicher Sicht ist in Fällen dieser Art Folgendes zu beachten:

Wie ich in meinem 30. Tätigkeitsbericht 2020 unter Nr. 3.3 ausgeführt habe, darf das Gesundheitsamt Testergebnisse unmittelbar an die Einrichtungsleitung übermitteln, wenn dies zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist und die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben (Art. 6 Abs. 1 UAbs. 1 Buchst. d, Art. 9 Abs. 2 Buchst. c DSGVO). Naturgemäß können diese Tatbestandsmerkmale nicht allgemein und pauschal für alle betroffenen Personenkategorien in einer Einrichtung bejaht werden; vielmehr bedarf es grundsätzlich einer eigenständigen Prüfung in jedem Einzelfall.

Diese Voraussetzungen sind bei Mitarbeiterinnen und Mitarbeitern der Einrichtung, die weder aus körperlichen noch aus rechtlichen Gründen außerstande sind, ihre Einwilligung zu erteilen, nicht gegeben. Es stellt sich dann die Frage, ob es nach geltendem Datenschutzrecht der Einwilligung jeder oder jedes einzelnen Beschäftigten bedarf, um das jeweilige Testergebnis an die Einrichtungsleitung übermitteln zu dürfen, oder ob eine anderweitige Rechtsgrundlage für die Übermittlung existiert.

Gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2, Abs. 3 UAbs. 1 Buchst. b, Art. 9 Abs. 2 Buchst. i DSGVO kann die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren, zulässig sein, wenn dies erforderlich und in einem nationalen Gesetz vorgesehen ist, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Personen, insbesondere des Berufsgeheimnisses, vorsieht.

Nachdem sich die betroffenen Personen vorliegend nicht freiwillig, sondern aufgrund einer verpflichtenden Anordnung des Gesundheitsamtes einem Test auf SARS-CoV 2 unterzogen hatten, ist die Verbotsnorm des Art. 30 Abs. 1 Satz 3 Gesundheitsdienst- und Verbraucherschutzgesetz (GDVG) – mangels Freiwilligkeit der Testung – nicht einschlägig. Folglich ist der Anwendungsbereich des Art. 30 Abs. 2 GDVG, der Ausnahmen von diesem Verarbeitungsverbot regelt, ebenfalls nicht eröffnet.

Da sich meines Erachtens darüber hinaus auch aus dem Infektionsschutzgesetz (insbesondere aus § 27 IfSG) keine Unterrichtungs- oder Übermittlungsbefugnisse gegenüber (der Leitung von) Pflege- und Rehabilitationseinrichtungen ergeben (und ein Rückgriff auf Verarbeitungsbefugnisse aus dem BayDSG am Vorrang des spezialgesetzlichen Regelungsregimes des GDVG und des IfSG scheitert), verbleibt nurmehr die Einwilligung gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 9 Abs. 2 Buchst. a, Art. 4 Nr. 11, Art. 7 DSGVO als mögliche Rechtsgrundlage für eine entsprechende Datenübermittlung durch das Gesundheitsamt.

Allerdings sind im Rahmen eines „klaren Ungleichgewichts" zwischen dem Verantwortlichen und der betroffenen Person generell besonders hohe Anforderungen an die **Freiwilligkeit** der Einwilligung zu stellen (siehe Erwägungsgrund 43 Satz 1 DSGVO)[45].

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

Dies gilt speziell im Verhältnis der Mitarbeiterinnen und Mitarbeiter zur Einrichtungsleitung. Angesichts des im Beschäftigungsverhältnis typischerweise bestehenden Abhängigkeitsverhältnisses dürfte die Freiwilligkeit einer Einwilligung im Sinne des Art. 4 Nr. 11 DSGVO daher regelmäßig zweifelhaft sein. So könnte allenfalls dann, wenn es möglich wäre, sicherzustellen, dass bei einer Einwilligungsverweigerung keinerlei Nachteile entstehen, die Unfreiwilligkeit der Einwilligung vermieden werden. Wie das konkret gelingen kann, erscheint jedoch fraglich.

Vor diesem Hintergrund dürfte es aus meiner Sicht effektiv kaum gelingen, bei Patientinnen und Patienten, bei Bewohnerinnen und Bewohnern wie auch bei Beschäftigten einer (Rehabilitations- und Pflege-) Einrichtung geeignete Maßnahmen vorzusehen, die den betroffenen Personen den Einwilligungsdruck nehmen und folglich eine Freiwilligkeit der Einwilligung im Rechtssinne gewährleisten könnten. Ohne tatsächlich belegbare Maßnahmen zur Herbeiführung der Freiwilligkeit verblieben erhebliche Zweifel an der Wirksamkeit einer solchen Einwilligung.

Somit kann die Einrichtungsleitung ihre an das Gesundheitsamt gerichtete Bitte um Übermittlung sämtlicher Ergebnisse einer gesundheitsbehördlich angeordneten Reihentestung nicht auf eine wirksame Einwilligung der betroffenen Personen stützen, da es der Einrichtungsleitung regelmäßig nicht gelingen dürfte, besondere Maßnahmen zur Gewährleistung der Freiwilligkeit nachzuweisen.

[45] Siehe zur Unfreiwilligkeit in sozialen Abhängigkeitsverhältnissen: Klement, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DSGVO Rn. 64.

7.3.3 Datenverarbeitung als Annex einer behördlichen Anordnung zu Zwecken von Infektionsschutz und Pandemiebekämpfung

Nach den obigen Erwägungen wird es somit in aller Regel (mangels derart weitreichender Übermittlungsbefugnisse) unzulässig sein, (standardmäßig) eine vollständige Liste des Gesundheitsamtes, die alle Testergebnisse sämtlicher betroffener Patientinnen und Patienten, Bewohnerinnen und Bewohner sowie Mitarbeiterinnen und Mitarbeiter umfasst, an die Einrichtungsleitung zu übermitteln. Unabhängig davon kann dem Gesundheitsamt im Rahmen seines Auswahlermessens als zuständige Stelle und nach Maßgabe des Grundsatzes der Erforderlichkeit (Art. 5 Abs. 1 Buchst. c DSGVO) die Befugnis zur Übermittlung eines positiven Testergebnisses **im Einzelfall** zustehen. Dies wird dann der Fall sein, wenn damit infektionsschutzrechtliche Zwecke verfolgt werden, die sich auf andere Weise (etwa durch Anordnung umfassender Schutzmaßnahmen ohne Personenbezug) nicht erreichen lassen. Infektionsschutz und die Pandemiebekämpfung (beziehungsweise Pandemieeindämmung, vgl. § 28 Abs. 1 IfSG) wären zugleich Anlass und Zweck einer solchen „Annex-Datenverarbeitung", wobei sich die Offenbarung des Personenbezugs als eine notwendige Begleiterscheinung der behördlichen Anordnung darstellt.

7.3.4 Weitere Entwicklung und Ausblick

Seit dem 24. November 2021 gilt eine bundesweite 3G-Regelung am Arbeitsplatz (§ 28b IfSG), insbesondere auch für Beschäftige und ehrenamtlich Tätige mit Patientenkontakt in Krankenhäusern und Pflegeeinrichtungen. Zunächst bedeutete dies, dass auch Beschäftigte und ehrenamtlich Tätige mit Patientenkontakt ohne Geimpften- oder Genesenenstatus für die genannten Einrichtungen (anfangs grundsätzlich zweimal wöchentlich) einen negativen Testnachweis als Zugangserfordernis erbringen mussten. Soweit ersichtlich, sind für auskunftspflichtige geimpfte, genesene und getestete Beschäftigte angeordnete Reihentestungen in Pflegeeinrichtungen in der Folge entfallen und insoweit auch das Ersuchen von Einrichtungsleitungen an das Gesundheitsamt um Übermittlung von Testergebnissen.

Gegenwärtig sind die geltenden Bestimmungen regelmäßigen, pandemiebedingten Aktualisierungen unterworfen. Durch erneute Anpassung des Infektionsschutzgesetzes am 10. Dezember 2021 besteht nun gemäß § 20a IfSG ab dem 16. März 2022 eine einrichtungsbezogene Impfpflicht für Arbeitnehmerinnen und Arbeitnehmer in Kliniken, Pflegeheimen, Arzt- und Zahnarztpraxen, Rettungs- und Pflegediensten, Geburtshäusern und anderen medizinisch-pflegerischen Einrichtungen.

Für Bewohnerinnen und Bewohner von Alten- und Pflegeeinrichtungen geht das Robert Koch-Institut ausweislich seiner unter dem Datum des 21. Januar 2022 auf seiner Homepage veröffentlichten Empfehlungen mit dem Titel „Prävention und Management von COVID-19 in Alten- und Pflegeeinrichtungen und Einrichtungen für Menschen mit Beeinträchtigungen und Behinderungen"[46] von der weiteren Durchführung regelmäßiger Reihentestungen aus (siehe Ziffer 3.9 der Veröffentlichung). Für diese Fälle gelten die obigen datenschutzrechtlichen Erwägungen fort.

[46] Internet: https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Alten_Pflegeeinrichtung_Empfehlung.html.

7.4 Datenweitergabe durch Impfzentrum an Arbeitgeber

Zu Beginn des Berichtszeitraums war die Impfkampagne gegen COVID-19 gerade aufgenommen worden; zunächst stand nicht genügend Impfstoff für alle impfwilligen Bürgerinnen und Bürger zur Verfügung. Impfungen zum Schutz vor COVID-19 waren mangels ausreichender Verfügbarkeit in erster Linie Bewohnerinnen und Bewohnern von Senioren- und Pflegeeinrichtungen sowie dem Personal in medizinischen Einrichtungen vorbehalten. Außerhalb dieser Einrichtungen wurden Impfungen ausschließlich in Impfzentren und nur bei nachweislich erfüllten Priorisierungskriterien verabreicht.

Vor diesem Hintergrund befasste ich mich unter anderem mit folgender Beschwerde gegen die Weitergabe von personenbezogenen Gesundheitsinformationen an ein Krankenhaus in seiner Funktion als Arbeitgeber der betroffenen Person.

7.4.1 Zugrundeliegender Sachverhalt

Nach ihrer Online-Registrierung im digitalen Impfportal der Bayerischen Staatsregierung erhielt die betroffene Person zunächst einen Termin für eine COVID-19-Schutzimpfung im Impfzentrum, welches vom örtlichen Landratsamt betrieben wurde. Dort wurde die impfwillige Person zunächst nach ihrer Arbeitsstätte befragt. Nach wahrheitsgemäßer Angabe, dass sie in einem Krankenhaus beschäftigt sei, wurde der betroffenen Person die Impfung verwehrt, weil sie sich bei ihrem Arbeitgeber impfen lassen könne.

Die betroffene Person beschwerte sich daraufhin beim Landratsamt. Sie bat um Mitteilung der Rechtsgrundlage für die Erhebung der Arbeitsstätte durch das Impfzentrum und für die Stornierung ihres Termins. Dabei wies sie ausdrücklich darauf hin, dass sie sich aufgrund einer chronischen Erkrankung nicht an ihrer Arbeitsstätte impfen lassen wolle. Sie befürchte, im Impf-Anamnesebogen Vorerkrankungen und Diagnosen gegenüber Arbeitskolleginnen oder Arbeitskollegen beziehungsweise gegenüber ihrem Arbeitgeber transparent machen zu müssen. Zusätzlich bat sie um einen umgehenden Ersatztermin für die COVID-19-Schutzimpfung.

Anstatt der Beschwerde abzuhelfen nahm das Landratsamt telefonisch Kontakt mit dem Arbeitgeber auf. Er hinterließ wenig später auf dem Anrufbeantworter der betroffenen Person eine Nachricht an ihrer Arbeitsstätte, mit der er verschiedene Reihenimpftermine für Beschäftigte des Krankenhauses zur Auswahl anbot. Die betroffene Person machte von diesem Angebot keinen Gebrauch, weil sie sich nach wie vor nicht an ihrer Arbeitsstätte impfen lassen wollte. Stattdessen wandte sie sich mit einer Beschwerde an mich. Parallel bemühte sie sich nochmals um einen Impftermin im örtlichen Impfzentrum, den sie im weiteren Verlauf erhielt und wahrnahm.

7.4.2 Stellungnahme des Landratsamtes

Auf meine Aufforderung zur Stellungnahme räumte das zuständige Landratsamt zwar ein, dass der Anruf beim Arbeitgeber der betroffenen Person, soweit er die Beschwerde der betroffenen Person beim Landratsamt zum Gegenstand gehabt hatte, nicht zur Aufgabenerfüllung erforderlich gewesen sei. Allerdings vertrat die Behörde im Übrigen die Auffassung, dass die Weitergabe der personenbezogenen Daten an den Arbeitgeber durch Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG legitimiert gewesen sei.

Art. 5 BayDSG
Übermittlung
(1) [1]Eine Übermittlung personenbezogener Daten ist zulässig, wenn
1. sie zur Erfüllung einer der übermittelnden oder der empfangenden öffentlichen Stelle obliegenden Aufgabe erforderlich ist oder
2. 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.
[2]Bei einer Übermittlung nach Satz 1 Nr. 2 darf der Empfänger die übermittelten Daten nur für den Zweck verarbeiten, zu dem sie ihm übermittelt wurden.

Ferner habe es zur Bewältigung der COVID-19-Pandemie, insbesondere zum Zwecke der Koordinierung und Organisation der Impfkampagne, einer Kommunikation zwischen den verschiedenen impfenden Einrichtungen bedurft. Nachdem die betroffene Person zum Personal des betreffenden Krankenhauses gehört habe, sei insoweit eine Abklärung zwischen dem Impfzentrum und ihrer Arbeitsstelle erforderlich gewesen. Insofern seien dem Arbeitgeber der betroffenen Person außer der Nennung des Namens, der Anschrift und des Geburtsdatums keine weiteren personenbezogenen Daten telefonisch mitgeteilt worden.

7.4.3 Datenschutzrechtliche Bewertung der Übermittlung

Der Rechtsauffassung des Landratsamtes konnte ich mich aus folgenden Gründen nicht anschließen:

Bei der Bereitschaft, sich impfen zu lassen, handelt es sich um ein Gesundheitsdatum im Sinne des Art. 4 Nr. 15 DSGVO, da diese Information einen Rückschluss auf eine begehrte und regelmäßig auch bevorstehende medizinische Behandlung einer Person erlaubt. Im gegebenen Einzelfall wurde nicht nur der Name, die Anschrift und das Geburtsdatum der betroffenen Person, sondern auch deren Bereitschaft, sich im Impfzentrum impfen zu lassen, offenbart. Somit lag der Rückschluss auf eine begehrte und wohl auch bevorstehende medizinische Behandlung – nämlich eine Impfung – auf der Hand. Gesundheitsdaten wurden also übermittelt. Diese unterliegen gemäß Art. 9 Abs. 1 DSGVO einem generellen Verarbeitungsverbot, das nur unter besonderen Voraussetzungen (siehe Art. 9 Abs. 2 DSGVO, Art. 8 BayDSG) durchbrochen werden kann. Nach Erwägungsgrund 51 Satz 6 DSGVO sollten Ausnahmen von diesem allgemeinen Verarbeitungsverbot **ausdrücklich** vorgesehen werden, unter anderem bei ausdrücklicher Einwilligung der betroffenen Person oder bei bestimmten Notwendigkeiten[47].

„Ausnahmen von dem allgemeinen Verbot der Verarbeitung dieser besonderen Kategorien personenbezogener Daten sollten ausdrücklich vorgesehen werden, unter anderem bei ausdrücklicher Einwilligung der betroffenen Person oder bei bestimmten Notwendigkeiten, insbesondere wenn die Verarbeitung im Rahmen rechtmäßiger Tätigkeiten bestimmter Vereinigungen oder Stiftungen vorgenommen wird, die sich für die Ausübung von Grundfreiheiten einsetzen."

[47] Siehe Weichert, in: Kühling/Buchner, Datenschutz-Grundverordnung/Bundesdatenschutzgesetz, 2. Aufl. 2018, Art. 9 DSGVO Rn. 1 bis 6.

Mit Blick darauf habe ich verdeutlicht, dass Beschäftigte im Verantwortungsbereich des Landratsamtes **nachdrücklich zu sensibilisieren** sind, damit sie zukünftig Gesundheitsdaten als solche erkennen und den schutzwürdigen datenschutzrechtlichen Interessen der betroffenen Personen umfänglich Rechnung tragen können.

Im Übrigen ergibt sich aus dem dargelegten Zweck der Koordinierung und Organisation der Impfkampagne ebenfalls keine datenschutzrechtlich tragfähige Grundlage für die stattgefundene Übermittlung. Insoweit liegt vielmehr ein **Verstoß gegen den Grundsatz der Datenminimierung** nach Art. 5 Abs. 1 Buchst. c DSGVO vor.

Art. 5 DSGVO
Grundsätze für die Verarbeitung personenbezogener Daten
(1) Personenbezogene Daten müssen
[…]
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
[…].

Die konkreten Umstände des Einzelfalles einschließlich der Gesundheitsdaten hätten nicht unter Offenbarung der Identität der beschwerdeführenden Person mit deren Arbeitgeber erörtert werden dürfen, da sie ersichtlich für den dargelegten Zweck nicht erheblich sind. Zur Legitimation der Weitergabe von personenbezogenen Gesundheitsdaten genügt es nicht, wenn der Verantwortliche die Erforderlichkeit zur Aufgabenerfüllung pauschal behauptet. Vielmehr hätte die deutliche Beschwerde der betroffenen Person das Landratsamt dazu veranlassen müssen, die Erforderlichkeit für die Aufgabenerfüllung kritisch zu hinterfragen und letztlich die Entscheidung zu treffen, in diesem Zusammenhang keine personenbezogenen Daten zu offenbaren.

Richtigerweise ist bei Abstimmungen über die Organisation und Koordinierung von Impfungen in den impfberechtigten Einrichtungen – etwa mit dem Ziel, eine doppelte Impfterminvergabe zu vermeiden – zu fordern, dass diese zunächst ohne Personenbezug, das heißt insbesondere **ohne Offenlegung von Gesundheitsdaten** (etwa der Impfbereitschaft einer bestimmten Person) erfolgen.

Vorliegend ist es der verantwortlichen Stelle nicht gelungen, plausibel darzulegen, weshalb die allgemeine Aufgabe der Organisation und Koordinierung von Impfungen für eine Vielzahl von Impfberechtigten, gerade von der spezifischen Weitergabe der personenbezogenen Daten einer bestimmten Person abhängen sollte. Solche Gründe konnte ich auch in Anbetracht der generell ausgestalteten Vorschriften der bundesrechtlichen Coronavirus-Impfverordnung in der Fassung vom 8. Februar 2021 (BAnz. AT vom 8. Februar 2021, V1, im Folgenden: CoronaImpfV 2/2021) sowie der landesrechtlichen Vollzugsvorgaben nicht erkennen.

7.4.4 Erhebung von Arbeitgeberdaten

Im Zusammenhang mit der Organisation von Terminen in den Impfzentren halte ich demgegenüber die Erhebung von Informationen über medizinische Einrichtungen als Arbeitgeber nicht allgemein für beanstandenswert. Denn der Verordnungsgeber hat beispielsweise in § 3 Abs. 1 Nr. 4 CoronaImpfV 2/2021 ausdrücklich vorgesehen, dass Personen, die in stationären oder teilstationären Einrichtungen zur Behandlung, Betreuung oder Pflege geistig oder psychisch behinderter Menschen tätig sind oder

im Rahmen ambulanter Dienste regelmäßig geistig oder psychisch behinderte Menschen behandeln, betreuen oder pflegen, mit hoher Priorität Anspruch auf eine Schutzimpfung haben.

§ 3 CoronaImpfV 2/2021
Schutzimpfungen mit hoher Priorität
(1) Folgende Personen haben mit hoher Priorität Anspruch auf Schutzimpfung:

1. Personen, die das 70. Lebensjahr vollendet haben,
2. folgende Personen, bei denen ein sehr hohes oder hohes Risiko für einen schweren oder tödlichen Krankheitsverlauf nach einer Infektion mit dem Coronavirus SARS-CoV-2 besteht:
  a) Personen mit Trisomie 21,
  b) Personen nach Organtransplantation,
  c) Personen mit einer Demenz oder mit einer geistigen Behinderung oder mit schwerer psychiatrischer Erkrankung, insbesondere bipolare Störung, Schizophrenie oder schwere Depression,
  d) Personen mit malignen hämatologischen Erkrankungen oder behandlungsbedürftigen soliden Tumorerkrankungen, die nicht in Remission sind oder deren Remissionsdauer weniger als fünf Jahre beträgt,
  e) Personen mit interstitieller Lungenerkrankung, COPD, Mukoviszidose oder einer anderen, ähnlich schweren chronischen Lungenerkrankung,
  f) Personen mit Diabetes mellitus (mit HbA1c ≥ 58 mmol/mol oder ≥ 7,5%),
  g) Personen mit Leberzirrhose oder einer anderen chronischen Lebererkrankung,
  h) Personen mit chronischer Nierenerkrankung,
  i) Personen mit Adipositas (Personen mit Body-Mass-Index über 40),
  j) Personen, bei denen nach individueller ärztlicher Beurteilung aufgrund besonderer Umstände im Einzelfall ein sehr hohes oder hohes Risiko für einen schweren oder tödlichen Krankheitsverlauf nach einer Infektion mit dem Coronavirus SARS-CoV-2 besteht,
3. bis zu zwei enge Kontaktpersonen
  a) von einer nicht in einer Einrichtung befindlichen pflegebedürftigen Person nach den Nummern 1 und 2 und nach § 2 Absatz 1 Nummer 1, die von dieser Person oder von einer sie vertretenden Person bestimmt werden,
  b) von einer schwangeren Person, die von dieser Person oder von einer sie vertretenden Person bestimmt werden,
4. Personen, die in stationären Einrichtungen zur Behandlung, Betreuung oder Pflege geistig oder psychisch behinderter Menschen tätig sind oder im Rahmen ambulanter Pflegedienste regelmäßig geistig oder psychisch behinderte Menschen behandeln, betreuen oder pflegen,
5. Personen, die in Bereichen medizinischer Einrichtungen mit einem hohen oder erhöhten Expositionsrisiko in Bezug auf das Coronavirus SARS-CoV-2 tätig sind, insbesondere Ärzte und sonstiges Personal mit regelmäßigem unmittelbarem Patientenkontakt, Personal der Blut- und Plasmaspendedienste und in SARS-CoV-2-Testzentren,
6. Polizei- und Ordnungskräfte, die in Ausübung ihrer Tätigkeit zur Sicherstellung der öffentlichen Ordnung, insbesondere bei Demonstrationen, einem hohen Infektionsrisiko ausgesetzt sind, sowie Soldatinnen und Soldaten, die bei Einsätzen im Ausland einem hohen Infektionsrisiko ausgesetzt sind,
6a. Personen, die in Kinderbetreuungseinrichtungen, in der Kindertagespflege und in Grundschulen, Sonderschulen oder Förderschulen tätig sind,

7. Personen, die im öffentlichen Gesundheitsdienst oder in besonders relevanter Position zur Aufrechterhaltung der Krankenhausinfrastruktur tätig sind,
8. Personen, die in Einrichtungen nach § 36 Absatz 1 Nummer 3 oder Nummer 4 des Infektionsschutzgesetzes untergebracht oder tätig sind,
9. Personen, die im Rahmen der nach Landesrecht anerkannten Angebote zur Unterstützung im Alltag im Sinne des § 45a des Elften Buches Sozialgesetzbuch regelmäßig bei älteren oder pflegebedürftigen Menschen tätig sind.

(2) § 2 Absatz 2 sowie, für Personen nach Absatz 1 Nummer 1, § 2 Absatz 3 gelten entsprechend.

Grundsätzlich erscheint somit die Erhebung von Arbeitgeberdaten im gegebenen Kontext nicht als unzulässig. Denn es besteht ein Sachzusammenhang mit der Priorisierung impfwilliger Personen. Im Einklang damit ist auch die „Datenschutzinformation zur Digitalen Impfverwaltung" in Bayern verfasst, so hieß es dort seinerzeit beispielsweise unter Nr. 4.1.1:

„Zu Ihrem Account geben sie zunächst folgende Datenarten an:
[…]
Angaben zu Ihrer beruflichen Tätigkeit /Wohnsituation:
‚Ich arbeite in einer Pflege- oder medizinischen Einrichtung, in […]' (z. B. Alten- und Pflegeheim, med. Einrichtung mit sehr hohem Expositionsrisiko) […]"

Auch die Erläuterung unter Nr. 4.1.3 bestätigt die Erheblichkeit des beruflichen Umfelds für die Priorisierungskriterien:

„Personen mit höherem Kennwert gelten als gefährdeter und/oder risikobehafteter (weil sie beispielsweise berufsmäßig mit vielen anderen Menschen in Kontakt sind) und erhalten daher vorrangig einen Impftermin."

Vorliegend hat allerdings die Antwort auf die zulässige Frage nach dem Arbeitgeber letztlich dazu geführt, dass der bereits zugeteilte Impftermin im Impfzentrum storniert worden ist. Dieser Entscheidung vor Ort liegt jedoch keine datenschutzrechtlich relevante Verarbeitung zugrunde, sondern eine Anwendung bzw. Auslegung des Fachrechts (das heißt insbesondere der fachrechtlichen Vorgaben zur Priorisierung der Corona-Schutzimpfungen). Deshalb habe ich den Sachverhalt auch nicht hinsichtlich der weiteren rein fachrechtlichen Aspekte überprüft, etwa der Frage, ob zum damaligen Zeitpunkt Tatsachen vorgelegen haben, die bereits für sich genommen und damit unabhängig vom Beschäftigungsverhältnis die Voraussetzungen für eine hohe Priorisierung der betroffenen Person im Sinne des § 3 Abs. 1 CoronaImpfV 2/2021 erfüllten.

Im Ergebnis stellt die vom Impfzentrum vorgenommene Erhebung von Informationen über medizinische Einrichtungen als Arbeitgeber im gegebenen Kontext der Impfpriorisierung keinen Verstoß gegen Datenschutzrecht dar.

7.5 Impfzentrum: Aufbewahrung von Dokumentationen zur Impfberechtigung

Zu Beginn der Impfkampagne gegen das Coronavirus SARS-CoV-2 war der Zugang zu den Impfungen reglementiert. Gemäß der bis zum 6. Juni 2021 geltenden Coronavirus-Impfverordnung vom 31. März 2021 (BAnz. AT vom 1. April 2021), mussten anspruchsberechtigte Personen vor der Schutzimpfung einen Nachweis der Anspruchsberechtigung und zur Prüfung der Priorisierung vorlegen.

Ich wurde im Rahmen eines Beschwerdeverfahrens darauf aufmerksam, dass ein Impfzentrum sich die Unterlagen nicht nur vorlegen ließ, sondern teilweise auch die Originale einbehielt oder Kopien anfertigte. Das Impfzentrum hatte angenommen, dass die Nachweise ähnlich einem Beweismittel aufzubewahren seien.

Mein Einwand, dass nach Art. 5 Abs. 1 Buchst. c DSGVO der Grundsatz der Datenminimierung zu beachten sei und daher nach Vorlage der entsprechenden Nachweise ein interner Aktenvermerk ausreichend sein sollte, wurde kooperativ aufgenommen und umgesetzt.

Art. 5 DSGVO
(1) Personenbezogene Daten müssen
[…]
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung");
[…].

Dies führte im Ergebnis dazu, dass ab diesem Zeitpunkt die Verarbeitung nach dem Grundsatz der Datensparsamkeit durchgeführt wurde sowie auch 60.000 Impfakten im Nachhinein bereinigt und die nicht erforderlichen Unterlagen datenschutzgerecht vernichtet wurden.

7.6 Forschungsstudie ohne Einwilligung

Im Rahmen einer anerkannten medizinischen Screeningstudie zur Prostatakrebsvorsorge wurden personenbezogene Daten von etwa 45.000 Probanden für eine Zusatzstudie (Sexualstudie) verarbeitet, ohne dass hierfür eine ausreichende Einwilligung der betroffenen Personen vorlag. Im Ergebnis führte dies zu einer förmlichen Beanstandung.

Die Einwilligung zur Datenverarbeitung in einem Forschungsvorhaben unterliegt bestimmten Anforderungen. Hierzu zählt neben der Freiwilligkeit insbesondere auch die Transparenz der Verarbeitung. Der Proband muss anhand der ihm gegebenen Informationen erkennen können, in welche Datenverarbeitung er einwilligt und zu welchem Zweck seine Daten verarbeitet werden sollen.

In den Fragebögen befand sich jedoch ein erheblicher Teil an zusätzlichen, sehr intimen Fragen sexueller Natur, die für die Basisstudie nicht relevant waren, sondern einer darüber hinausgehenden Sexualstudie dienten.

Diese äußerst sensiblen Daten wurden erhoben, ohne dass die für die Basisstudie eingeholte Einwilligung ergänzt worden war und den weitergehenden Zweck der Sexualstudie umfasste.

Ich stellte daher fest, dass sowohl die Erhebung als auch die weitere Verwendung der zusätzlichen Daten für die Sexualstudie, welche im Rahmen der Basisstudie erhoben wurden, mangels wirksamer Einwilligungen unzulässig waren. Daher hatte die Forschungseinrichtung gegen datenschutzrechtliche Vorgaben gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 9 Abs. 1 und Art. 9 Abs. 2 Buchst. a DSGVO verstoßen.

Der Datenschutzverstoß wog umso schwerer, da die betroffenen Personen im Glauben waren, für einen rein medizinischen Zweck ihre Daten freiwillig zur Verfügung zu stellen.

Da es sich um einen Datenschutzverstoß von erheblichem Gewicht handelte, habe ich eine Beanstandung ausgesprochen und hierüber die Rechtsaufsichtsbehörde der Forschungseinrichtung verständigt.

Im Ergebnis löschte die Forschungseinrichtung sämtliche im Zusammenhang mit der Zusatzstudie erhobenen Daten und zog die Veröffentlichungen zur Sexualstudie zurück.

7.7 Übermittlung von Daten zu COVID-19-Infektionsketten an Berufsgenossenschaften

Angehörige von Heil- und Pflegeberufen haben den Verdacht einer Erkrankung, die Erkrankung sowie den Tod in Bezug auf die Krankheit COVID-19 an die Gesundheitsämter zu melden (siehe § 6 Abs. 1 Satz 1 Nr. 1 Buchst. t Infektionsschutzgesetz – IfSG). Die Gesundheitsämter sollen dadurch in die Lage versetzt werden, die zur Überwachung und Eindämmung der Krankheit notwendigen Maßnahmen zu ergreifen. Hierzu gehört es beispielsweise, eine sogenannte Infektionskette – also die Quelle einer Infektion, deren Übertragungsweg sowie mögliche weitere infizierte Personen (Kontaktpersonen) – zu ermitteln.

Wenn sich eine Person in ihrem **beruflichen Umfeld** infiziert hat, so kann dies grundsätzlich einen Versicherungsfall der **gesetzlichen Unfallversicherung** darstellen. Um prüfen zu können, ob die Voraussetzungen für eine Leistungspflicht der gesetzlichen Unfallversicherung bestehen, wurden in einigen Fällen die Gesundheitsämter von den insoweit zuständigen Berufsgenossenschaften gebeten, dort vorhandene Erkenntnisse, insbesondere aus dem Kontext einer Kontaktnachverfolgung, zu übermitteln. Mehrere Gesundheitsämter haben mich gefragt, ob sie einem solchen Übermittlungsersuchen nachkommen dürfen oder gar nachkommen müssen.

Für die Beantwortung dieser Frage ist zunächst zu beachten, dass Anfragen von Berufsgenossenschaften zu etwaigen Infektionsketten nicht nur Daten der versicherten Person, sondern auch Daten Dritter betreffen. Das Gesundheitsamt hat insoweit zu prüfen, wann eine **Rechtsgrundlage** für eine Datenübermittlung eingreift.

7.7.1 Gesetzliche Befugnis

Personenbezogene Daten dürfen gemäß Art. 6 Abs. 1 DSGVO nur verarbeitet, also auch übermittelt werden (vgl. Art. 4 Nr. 2 DSGVO), wenn es dafür eine Rechtsgrundlage gibt. Zu denken wäre insbesondere an Art. 6 Abs. 1 UAbs. 1 Buchst. c oder e DSGVO in Verbindung mit einer nationalen Befugnisnorm. Des Weiteren dürften die seitens des Gesundheitsamtes verarbeiteten Daten überwiegend **Gesundheitsdaten** im Sinne von Art. 4 Nr. 15 DSGVO darstellen, die gemäß Art. 9 Abs. 1 DSGVO grundsätzlich einem strikten **Verarbeitungsverbot** unterliegen und daher nur ausnahmsweise (Art. 9 Abs. 2 DSGVO) verarbeitet werden dürfen. Zu beachten ist ferner, dass diese Daten ursprünglich allein zum Zweck der Verhütung und Bekämpfung der COVID-19-Erkrankung durch das Gesundheitsamt erhoben worden sind.

Bei einer etwaigen Übermittlung an eine Berufsgenossenschaft würde es sich folglich um eine **zweckändernde Weiterverarbeitung** handeln, für die das Gesundheitsamt eine ausdrückliche Rechtsgrundlage benötigt. Eine allein für die Berufsgenossenschaft im Recht der gesetzlichen Unfallversicherung vorhandene Verarbeitungs-, ins-

besondere Erhebungsbefugnis reicht hier nicht aus. Denn nach dem im Datenschutzrecht relevanten sogenannten **Doppeltürmodell**[48] müssen sowohl die übermittelnde Behörde als auch die empfangende Stelle sich jeweils auf eine Rechtsgrundlage für ihre Datenverarbeitung stützen können. Außerdem muss eine Zweckänderungserlaubnis bestehen.

So kann eine Übermittlung von Gesundheitsdaten grundsätzlich nach Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 UAbs. 1 Buchst. b, Art. 9 Abs. 2 Buchst. h, Abs. 3 DSGVO zulässig sein. Hiernach ist die Verarbeitung unter anderem für Zwecke der Versorgung oder Behandlung im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedsstaats erlaubt. Ein solches nationales Gesetz ist in Bayern das Gesundheitsdienst- und Verbraucherschutzgesetz (GDVG). Insbesondere bei den Vorschriften der Art. 30 und 31 GDVG handelt es sich um sogenannte bereichsspezifische Rechtsnormen, die gegenüber den allgemeinen Bestimmungen des Bayerischen Datenschutzgesetzes vorrangig sind.

Dem Gesundheitsdienst- und Verbraucherschutzgesetz lässt sich allerdings derzeit **keine** Rechtsvorschrift entnehmen, die eine Datenübermittlung zugunsten der gesetzlichen Unfallversicherung ausdrücklich gestattet; dies gilt ebenso für das Infektionsschutzgesetz und das Siebte Buch Sozialgesetzbuch – Gesetzliche Unfallversicherung –.

Die Berufsgenossenschaften führten insoweit die Vorschriften über die Amtshilfe (§§ 3 ff. Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – SGB X) sowie die Vorschrift des § 69 Abs. 1 Nr. 1 SGB X als Rechtsgrundlagen für die Datenübermittlung durch das Gesundheitsamt an. Die allgemeinen Vorschriften über die Amtshilfe stellen allerdings keine datenschutzrechtlichen Befugnisnormen dar.[49] Auch kann die eine Übermittlung von Sozialdaten regelnde Bestimmung des § 69 Abs. 1 Nr. 1 Var. 3 SGB X nicht unmittelbar herangezogen werden. Denn personenbezogene Gesundheitsdaten werden erst dann zu Sozialdaten, wenn sie in den Herrschaftsbereich des Sozialleistungsträgers gelangt sind (siehe die Begriffsbestimmung des § 67 Abs. 2 Satz 1 SGB X).

Sofern es sich bei den beim Gesundheitsamt gespeicherten Informationen auch um Daten im Sinne von § 28a Abs. 1 Nr. 17 IfSG (sogenannte Kontaktdaten) handeln sollte, steht die Vorschrift des § 28a Abs. 4 Satz 6 IfSG einer zweckändernden Verarbeitung sogar ausdrücklich entgegen.

7.7.2 Einwilligung

Ist demnach keine gesetzliche Grundlage für eine Datenübermittlung durch das Gesundheitsamt vorhanden, verbleibt allenfalls die Einholung einer Einwilligung betroffener Personen.

[48] Siehe beispielsweise Bundesverfassungsgericht, Beschluss vom 24. Januar 2012, 1 BvR 1299/05, BeckRS 2012, 47556, Rn. 123; Bayerischer Verwaltungsgerichtshof, Beschluss vom 20. Mai 2020, 12 B 19.1648, BeckRS 2020, 10398, Rn. 46 f.

[49] Vgl. Bayerisches Oberstes Landesgericht, Beschluss vom 6. August 2020, 1 VA 33/20, BeckRS 2020, 18859, Rn. 43.

Sofern es sich dabei um **Daten der versicherten Person** selbst handelt, muss diese in die Übermittlung **ausdrücklich** einwilligen (Art. 9 Abs. 2 Buchst. a DSGVO). Hinsichtlich der Bedingungen für die Einwilligung möchte ich auf Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 4 Nr. 11 und Art. 7 DSGVO[50] hinweisen. Die Gesundheitsämter müssen die ersuchte Datenübermittlung auf diejenigen Gesundheitsdaten beschränken, die von der Einwilligung der versicherten Person abgedeckt sind.

Bei **Daten Dritter** muss jeweils deren eigene Einwilligung zusätzlich eingeholt werden (sofern diesbezüglich keine anderweitige Rechtsgrundlage ersichtlich ist), um die Übermittlung von deren Gesundheitsdaten, zum Beispiel im Zusammenhang mit einer eigenen COVID-19-Erkrankung, zu rechtfertigen.

Demnach könnte **beispielsweise** nach Einholung einer Einwilligungserklärung der versicherten Person der anfragenden Berufsgenossenschaft zwar mitgeteilt werden, dass es sich um eine Ansteckung im Betrieb gehandelt habe; eine Offenlegung – falls überhaupt möglich –, welche Person der konkrete Überträger gewesen ist, wäre dagegen ohne deren eigene Einwilligung nicht zulässig.

Daten im Sinne von § 28a Abs. 1 Nr. 17 IfSG können schon deshalb **nicht** auf Grundlage einer Einwilligung übermittelt werden, weil die Gesundheitsämter sich damit über das in § 28a Abs. 4 Satz 6 IfSG bestimmte Weitergabeverbot hinwegsetzen würden.

7.7.3 Fazit

Abschließend lässt sich festhalten, dass bei einer etwaigen Datenübermittlung durch die Gesundheitsämter zu berücksichtigen ist, dass unterschiedliche Kategorien von Daten unterschiedlichen rechtlichen Vorgaben unterliegen können. Auch ist besonders darauf zu achten, dass von einem Übermittlungsersuchen nicht nur Daten der versicherten Person, sondern auch Daten Dritter betroffen sein können.

Zusammenfassend ist derzeit **keine gesetzliche Befugnis** erkennbar, die es den Gesundheitsämtern erlaubt, die erbetenen Daten an Berufsgenossenschaften zu übermitteln. Eine solche Datenübermittlung kann allenfalls auf eine datenschutzrechtliche **Einwilligungserklärung** der jeweils betroffenen Personen gestützt werden, wobei die Einwilligung nicht die vom Gesetzgeber im Zusammenhang mit der Kontaktdatenerfassung bewusst gezogenen Verarbeitungsgrenzen überspielen darf.

Im Übrigen **empfehle** ich, vor einer Datenübermittlung an die anfragende Berufsgenossenschaft die behördliche Datenschutzbeauftragte oder den behördlichen Datenschutzbeauftragten des Gesundheitsamts zu beteiligen.

7.8 Unterhaltsvorschussleistungen: Datenverarbeitungen durch das Jugendamt und das Landesamt für Finanzen

Im Zusammenhang mit der Gewährung von Unterhaltsvorschussleistungen für Kinder alleinstehender Mütter und Väter auf Grundlage des Unterhaltsvorschussgeset-

[50] Siehe hierzu ausführlich Bayerischer Landesbeauftragter für den Datenschutz, Die Einwilligung nach der Datenschutz-Grundverordnung, Stand 9/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Überblick".

zes (UhVorschG) war ich mehrfach mit der Frage beschäftigt, ob das jeweils zuständige Jugendamt und das Landesamt für Finanzen über ausreichende Verarbeitungsbefugnisse verfügen.

Gegenstand meiner Prüfung waren vor allem Datenübermittlungen des Jugendamts im Zusammenhang mit der Auszahlung der Hilfeleistung sowie mit einer gerichtlichen Vertretung des Freistaates Bayern bei der Durchsetzung von Ansprüchen nach § 7 UhVorschG.

In der Verwaltungspraxis bewilligen zwar die Jugendämter Unterhaltsvorschussleistungen, ausgezahlt werden diese jedoch durch die beim Landesamt für Finanzen eingerichtete Staatsoberkasse Bayern. Dies setzt eine Übermittlung der insoweit notwendigen Daten durch das Jugendamt voraus. Ähnlich verhält es sich auch in Erstattungs- beziehungsweise Regressverfahren. Diese führt das Landesamt für Finanzen (gerichtlich) durch, welches die hierfür benötigten Daten wiederum von den Jugendämtern erhält.

Ich bezweifelte, dass es für die jeweiligen Datenübermittlungen durch die Jugendämter eine Rechtsgrundlage gibt. Die Prüfung erfolgte anhand der Regelungen im Sozialgesetzbuch, da das Unterhaltsvorschussgesetz gemäß § 68 Nr. 14 Erstes Buch Sozialgesetzbuch – Allgemeiner Teil – als ein besonderer Teil dieses Gesetzbuches gilt. Dies hat zur Folge, dass vor allem die allgemeinen leistungsbereichsübergreifenden Regelungen des Sozialgesetzbuches – im Wesentlichen seines Ersten und Zehnten Buches – auch in diesem Bereich Anwendung finden. Problematisch war dabei eine bayerische Regelung im Gesetz zur Ausführung der Sozialgesetze (AGSG), wonach die Jugendämter in Bayern für den Vollzug des Unterhaltsvorschussgesetzes für zuständig erklärt wurden.[51] Der Wortlaut dieser Vorschrift war meines Erachtens dahingehend zu verstehen, dass nur die Jugendämter – nicht also die Staatsoberkasse – für die Gewährung von Unterhaltsvorschussleistungen, das heißt von der Bewilligung, Auszahlung bis hin zu einer eventuellen Geltendmachung eines Erstattungs- oder Regressanspruchs, zuständig sind.

Da ich die tatsächliche Handhabung in der Praxis, die so wohl auch vom Bundesgesetzgeber gebilligt wird,[52] nachvollziehen konnte, die Rechtslage in Bayern diese Vorgehensweise allerdings nicht hinreichend widerspiegelte, regte ich gegenüber dem Bayerischen Staatsministerium für Familie, Arbeit und Soziales sowie dem Bayerischen Staatsministerium der Finanzen und für Heimat eine Änderung des Gesetzes zur Ausführung der Sozialgesetze an. Die Bayerische Staatsregierung hat diese Anregung aufgegriffen und eine entsprechende Änderung initiiert.[53] Mit dem Gesetz zur Änderung des Bayerischen Kinderbildungs- und -betreuungsgesetzes und des Gesetzes zur Ausführung der Sozialgesetze vom 23. April 2021[54] wurde nunmehr in Art. 62 AGSG mit einem neuen Satz 3 die bisherige Praxis kodifiziert.

Art. 62 AGSG
Zuständigkeit nach dem Unterhaltsvorschussgesetz
[1]Die Jugendämter sind zuständig für den Vollzug des Unterhaltsvorschussgesetzes. [2]…] [3]Satz 1 gilt jedoch nicht für die Kassenaufgaben nach Art. 79 der Bayerischen Haushaltsordnung mit Ausnahme der für die rechtzeitige und vollständige Entrichtung der Einzahlungen erforderlichen Maßnahmen und für die gerichtliche Vertretung des

51 Siehe Art. 62 AGSG in der bis zum 30. April 2021 geltenden Fassung.
52 Siehe Bundestags-Drucksache 17/8802, S. 11.
53 Siehe Landtags-Drucksache 18/11716.
54 GVBl. 2021 S. 196.

Freistaates Bayern zur Durchsetzung von Ansprüchen nach § 7 des Unterhaltsvorschussgesetzes.

Nach Satz 1 sind die bayerischen Jugendämter zwar weiterhin für den Vollzug des Unterhaltsvorschussgesetzes zuständig; allerdings nicht für die Kassenaufgaben nach Art. 79 Bayerische Haushaltsordnung und für die Durchsetzung von Ansprüchen nach § 7 UhVorschG, was sich jetzt eindeutig aus Satz 3 ergibt.

Damit erfolgte die von mir gewünschte gesetzliche Klarstellung der Aufgabenverteilung beim Vollzug des Unterhaltsvorschussgesetzes. Die Datenübermittlungsbefugnisse der Jugendämter ergeben sich auf dieser Basis aus dem Zehnten Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X). In der Gesetzesbegründung ist aufgrund meiner weiteren Anregung der Hinweis aufgenommen worden, dass das Landesamt für Finanzen (einschließlich der Staatsoberkasse Bayern) als Empfänger der Daten von den Jugendämtern die Zweckbindung sowie die Geheimhaltungspflichten nach § 78 SGB X zu beachten hat.[55]

7.9 Datenverarbeitung im Zusammenhang mit Kindeswohlgefährdungen

Im Berichtszeitraum war ich mit der datenschutzrechtlichen Bewertung eines Sachverhaltes befasst, bei dem die Frage der Zulässigkeit einer Datenerhebung von Fotoaufnahmen durch ein Jugendamt zu klären war.

Ein Veterinäramt und ein Jugendamt eines Landratsamtes hatten gemeinsam einen Hausbesuch bei einer Familie durchgeführt. Parallel im Raum standen eine nicht artgerechte Hundehaltung und eine Kindeswohlgefährdung. Nachdem das Jugendamt die Örtlichkeit in Augenschein genommen hatte, nahm es das betroffene Kind sogleich in Obhut. An zwei weiteren Terminen führte das Veterinäramt allein Vor-Ort-Kontrollen durch, um nochmals die Hundehaltung zu überprüfen. Bei allen drei Terminen machte das Veterinäramt Fotoaufnahmen von den räumlichen Gegebenheiten und stellte sie dem Jugendamt auf Nachfrage zur Verfügung.

Das Jugendamt darf zwar im Zuge der Prüfung einer Kindeswohlgefährdung personenbezogene Daten des betroffenen Kindes sowie dessen Eltern im erforderlichen Umfang erheben (auch etwa im Rahmen eines Vor-Ort-Termins). Allerdings sieht das Achte Buch Sozialgesetzbuch – Kinder und Jugendhilfe – (SGB VIII) anders als das Tierschutzgesetz (TierSchG) nicht vor, dass Fotoaufnahmen von häuslichen Situationen ohne Einwilligung der betroffenen Personen angefertigt werden dürfen. Dem kommt es gleich, wenn solche Fotos bei einer anderen Stelle angefordert werden.

Eine Rechtsgrundlage für das Anfertigen von Fotoaufnahmen durch das Veterinäramt findet sich in § 16 Abs. 3 Satz 1 Nr. 2 Buchst. b TierSchG:

§ 16 TierSchG
(3) Personen, die von der zuständigen Behörde beauftragt sind, sowie in ihrer Begleitung befindliche Sachverständige der Europäischen Kommission und anderer Mitgliedstaaten dürfen zum Zwecke der Aufsicht über die in Absatz 1 bezeichneten Personen und Einrichtungen und im Rahmen des Absatzes 2
[. . .]
1. zur Verhütung dringender Gefahren für die öffentliche Sicherheit und Ordnung

55 Vgl. Landtags-Drucksache 18/11716, S. 9.

a) die in Nummer 1 bezeichneten Grundstücke, Räume, Gebäude und Transportmittel außerhalb der dort genannten Zeiten,
b) Wohnräume des Auskunftspflichtigen
betreten, besichtigen sowie zur Dokumentation Bildaufzeichnungen, mit Ausnahme von Bildaufzeichnungen von Personen, anfertigen; das Grundrecht der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) wird insoweit eingeschränkt,
[…].

Diese Vorschrift kann allerdings eine Datenerhebung durch das Jugendamt aufgrund der damit verbundenen Beeinträchtigung der Unverletzlichkeit der Wohnung nicht legitimieren. Ich konnte zwar die Zielrichtung des Vorgehens des Jugendamtes – auch unter Berücksichtigung der gesetzlichen Wertungen hinsichtlich in Raum stehender Kindeswohlgefährdungen – grundsätzlich nachvollziehen. Allerdings konnte ich bei meiner Bewertung nicht außer Acht lassen, dass dem Jugendamt nur eine Hilfe- und Schutzfunktion und nicht die Rolle einer Ermittlungsbehörde – mit Beweissicherung, etwa durch Fotoaufnahmen – zukommt. Auch § 8a Abs. 1 Satz 2 SGB VIII spricht derzeit unter anderem nur davon, sich „einen unmittelbaren Eindruck von dem Kind und von seiner persönlichen Umgebung zu verschaffen".

Das Anfertigen und somit Erheben von Fotoaufnahmen – auch von der häuslichen Situation eines Kindes – könnte folglich allenfalls auf Basis von Einwilligungen der betroffenen Personen erfolgen;[56] dies gilt auch für die Erhebung solcher Fotoaufnahmen von einer anderen Stelle. Die Bedingungen für die Einwilligung sind Art. 7 DSGVO zu entnehmen.[57] Ohnehin kommt die Einwilligung als Legitimationsgrundlage für Verarbeitungen im öffentlichen Sektor nur ausnahmsweise in Betracht, wenn sie nicht in einem Spannungsverhältnis zum Vorbehalt des Gesetzes steht.

Bei dem von mir bewerteten Sachverhalt habe ich nach Ausübung des mir zustehenden Ermessens letztendlich doch von datenschutzaufsichtlichen Maßnahmen abgesehen. Denn das Jugendamt hatte grundsätzlich die Befugnis, eine Inaugenscheinnahme der Wohnung vorzunehmen. Aufgrund dessen wog die Beeinträchtigung durch das Erheben von Bildaufnahmen der Wohnung weniger schwer als in anderen Fallkonstellationen, in denen eine Behörde überhaupt keine Befugnis zur Wohnungsbesichtigung hat.

Da jedoch bei Vergleich der oben genannten tierschutzrechtlichen Regelung mit den Datenverarbeitungsbefugnissen im Achten Buch Sozialgesetzbuch ein gewisser Wertungswiderspruch erkennbar wird, habe ich das Bayerische Staatsministerium für Familie, Arbeit und Soziales gewandt und auf die Problematik hingewiesen.

56 So auch Deutsches Institut für Jugendhilfe und Familienrecht, Zulässigkeit von Fotoaufnahmen von Wohnung bzw. Kind gegen den Willen der Eltern zur Dokumentation des Vorgehens bei Kindeswohlgefährdungen?, Rechtsgutachten vom 8. Januar 2008, JAmt 2008, S. 23 f.

57 Nähere Ausführungen dazu bei Bayerischer Landesbeauftragter für den Datenschutz, Die Einwilligung nach der Datenschutz-Grundverordnung, Stand 10/2018, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Einwilligung".

7.10 Mitteilungspflichten des Medizinischen Dienstes bei Behandlungsfehlerbegutachtungen

Bereits mehrmals habe ich mich mit den Mitteilungspflichten des Medizinischen Dienstes[58] Bayern gemäß § 277 Fünftes Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (SGB V) befasst (siehe meine Ausführungen im 25. Tätigkeitsbericht 2012 unter Nr. 8.13 und im 18. Tätigkeitsbericht 1998 unter Nr. 4.8.1). Dieses Mal lag der Schwerpunkt meiner Prüfung bei den Mitteilungspflichten des Medizinischen Dienstes gegenüber den Leistungserbringern und krankenversicherten Personen, konkret im Zusammenhang mit der Begutachtung von Behandlungsfehlern.

In der dafür maßgeblichen, bis zum 20. Juli 2021 geltenden Vorschrift in § 277 Abs. 1 Satz 1 SGB V-alt hieß es:

„[1]Der Medizinische Dienst hat dem an der vertragsärztlichen Versorgung teilnehmenden Arzt, sonstigen Leistungserbringern, über deren Leistungen er eine gutachtliche Stellungnahme abgegeben hat, und der Krankenkasse das Ergebnis der Begutachtung und der Krankenkasse die erforderlichen Angaben über den Befund mitzuteilen."

7.10.1 Mitteilungspflicht gegenüber Leistungserbringerinnen und Leistungserbringern

Nach § 277 Abs. 1 Satz 1 SGB V-alt war der Medizinische Dienst verpflichtet, Leistungserbringerinnen oder Leistungserbringern, über deren Leistungen er eine gutachtliche Stellungnahme abgegeben hat, das Ergebnis seiner Begutachtung mitzuteilen. Ich habe diesbezüglich die Auffassung vertreten, dass diese Vorschrift auch in Fällen zur Anwendung kommen solle, in denen der Medizinische Dienst beauftragt ist, etwaige von Ärztinnen und Ärzten verursachte Behandlungsfehler zu begutachten.

§ 277 SGB V knüpft nämlich, bereits aus gesetzessystematischen Gründen, an die Aufgabenzuweisung des Medizinischen Dienstes in § 275 SGB V an. Nach § 275 Abs. 1 Satz 1 Nr. 1 SGB V sind die Krankenkassen in den gesetzlich bestimmten Fällen, oder wenn es nach Art, Schwere, Dauer oder Häufigkeit der Erkrankung oder nach dem Krankheitsverlauf erforderlich ist, verpflichtet, bei Erbringung von Leistungen, insbesondere zur Prüfung von Voraussetzungen sowie Art und Umfang der Leistung, eine gutachtliche Stellungnahme des Medizinischen Dienstes einzuholen. Unter Art und Umfang der Leistung ist meines Erachtens auch die Prüfung von Regressansprüchen der Krankenkasse zu verstehen.[59] Bei diesen Regressansprüchen handelt es sich um Schadensersatzansprüche, die auf die Krankenkasse gemäß § 116 Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X) übergegangen sind. Somit kommt bei einer Beauftragung des Medizinischen Dienstes durch die Krankenkasse zur Überprüfung eines Behandlungsfehlers zum Zweck der Geltendmachung von Regressansprüchen § 275 Abs. 1 Satz 1 Nr. 1 SGB V und infolgedessen § 277 Abs. 1 SGB V zur Anwendung.

[58] Neue Bezeichnung durch das MDK-Reformgesetz vom 14. Dezember 2019, BGBl. I S. 2789 ff. – vormals: Medizinischer Dienst der Krankenversicherung.

[59] So im Ergebnis auch Sichert/Seifert: in Becker/Kingreen, SGB V, Gesetzliche Krankenversicherung, 7. Aufl. 2020, § 275 SGB V Rn. 9; Nebendahl in: Spickhoff, Medizinrecht, 3. Aufl. 2018, § 275 SGB V Rn. 6.

Für die von Versicherten (allein) geltend gemachten Schadensersatzansprüche wegen Behandlungsfehlern, die **nicht** auf die jeweilige Krankenkasse gemäß § 116 SGB X übergegangen sind,[60] kann eine Beauftragung des Medizinischen Dienstes durch die Krankenkasse (ergänzend[61]) nach § 275 Abs. 3 Satz 1 Nr. 4, § 66 SGB V erfolgen. In diesen Fällen wird dementsprechend die Mitteilungspflicht gemäß § 277 Abs. 1 SGB V ausgelöst.

Der Medizinische Dienst Bayern sowie das Bayerische Staatsministerium für Gesundheit und Pflege teilten meine Rechtsauffassung. Eine meiner Zuständigkeit unterliegende Krankenkasse war dagegen anderer Ansicht. Sie führte an, dass die Mitteilung gegenüber beteiligten und insbesondere eines Behandlungsfehlers beschuldigten Leistungserbringerinnen oder Leistungserbringern der Zielsetzung des Gesetzes widerspreche. Eine Mitteilung an die Leistungserbringerin oder den Leistungserbringer wäre bei einer Leistungsbegutachtung sinnvoll; bei der Begutachtung eines Behandlungsfehlers würde eine solche jedoch zu einer Schwächung der Verhandlungsposition der krankenversicherten Personen (in den Fällen des § 66 SGB V) sowie der Krankenkassen (in den Fällen des § 116 SGB X) führen.

Diese Befürchtung war zwar grundsätzlich plausibel. Gleichwohl war ich der Meinung, dass eine Mitteilung der Prüfergebnisse zu mehr Transparenz für den betroffenen Leistungserbringer führen und deshalb eher zu einem für alle Beteiligten ausgewogenen Verfahren beitragen kann. Schließlich geht es bei der betreffenden Begutachtung durch den Medizinischen Dienst um die von der Leistungserbringerin oder dem Leistungserbringer selbst erbrachte und gegebenenfalls von ihr oder ihm verschuldete Schlechtleistung. Vor diesem Hintergrund sollte sie oder er dann auch die Bewertung ihrer oder seiner Leistung durch den Medizinischen Dienst unmittelbar erfahren. Diese Vorgehensweise stand im Einklang mit den allgemeinen Vorgaben der Datenschutz-Grundverordnung zur Transparenz, insbesondere den Art. 12 ff. DS-GVO.

Im Ergebnis bestand daher für den Medizinischen Dienst auch bei einem etwaigen Behandlungsfehler die Pflicht, der Leistungserbringerin oder dem Leistungserbringer das Prüfungsergebnis mitzuteilen.

Der Gesetzgeber hat auf diese Situation reagiert und mit dem Gesetz zur Weiterentwicklung der Gesundheitsversorgung vom 11. Juli 2021[62] § 277 Abs. 1 Satz 1 bis 3 SGB V neu gefasst:

„[1]Der Medizinische Dienst hat der Krankenkasse das Ergebnis der Begutachtung und die wesentlichen Gründe für dieses Ergebnis mitzuteilen. [2]Der Medizinische Dienst ist befugt und in dem Fall, dass das Ergebnis seiner Begutachtung von der Verordnung, der Einordnung der erbrachten Leistung als Leistung der gesetzlichen Krankenversicherung oder der Abrechnung der Leistung mit der Krankenkasse durch den Leistungserbringer abweicht, verpflichtet, diesem Leistungserbringer das Ergebnis seiner Begutachtung mitzuteilen; dies gilt bei Prüfungen nach § 275 Absatz 3 Satz 1 Nummer 4 nur, wenn die betroffenen Versicherten in die Übermittlung an den Leistungserbringer eingewilligt haben. [3]Fordern Leistungserbringer nach der Mitteilung nach

60 Beispielsweise die Geltendmachung eines Anspruchs auf Schmerzensgeld.

61 § 275 Abs. 3 Satz 1 Nr. 4 SGB V hat wohl gegenüber § 275 Abs. 1 Satz 1 Nr. 1 SGB V nur klarstellende Funktion, siehe Sichert/Seifert: in Becker/Kingreen, SGB V, Gesetzliche Krankenversicherung, 7. Aufl. 2020, § 275 SGB V Rn. 9; Nebendahl in: Spickhoff, Medizinrecht, 3. Aufl. 2018 § 275 SGB V, Rn. 6.

62 BGBl. I S. 2754 ff.

Satz 2 erster Halbsatz mit Einwilligung der Versicherten die wesentlichen Gründe für das Ergebnis der Begutachtung durch den Medizinischen Dienst an, ist der Medizinische Dienst zur Übermittlung dieser Gründe verpflichtet."

Diese Gesetzesänderung führt im Ergebnis dazu, dass der Medizinische Dienst nicht mehr verpflichtet ist, den Leistungserbringern nach Begutachtung eines etwaigen Behandlungsfehlers das Prüfungsergebnis mitzuteilen. Eine grundsätzliche Befugnis zur Weitergabe dieses Ergebnisses dürfte allerdings dem Wortlaut von § 277 Abs. 1 Satz 2 Halbsatz 1 SGB V weiterhin zu entnehmen sein. Bei Prüfungen nach § 275 Abs. 3 Satz 1 Nr. 4 SGB V bedarf es jedoch vor einer solchen freiwilligen Übermittlung an die Leistungserbringerin oder den Leistungserbringer der Einwilligung der betroffenen versicherten Person (§ 277 Abs. 1 Satz 2 Halbsatz 2 SGB V). Die Information darüber, ob eine solche Einwilligung vorliegt, hat die Krankenkasse dem Medizinischen Dienst im Rahmen der Beauftragung mitzuteilen, da es sich um eine für die Begutachtung erforderliche Angabe handelt (§ 276 Abs. 1 Satz 1 SGB V).[63] Falls eine Leistungserbringerin oder ein Leistungserbringer mit Einwilligung der versicherten Person die wesentlichen Gründe für das Ergebnis der Begutachtung durch den Medizinischen Dienst anfordern sollte, ist der Medizinische Dienst zur Übermittlung dieser Gründe dann auch weiterhin verpflichtet (siehe § 277 Abs. 1 Satz 3 SGB V).

7.10.2 Mitteilungspflicht gegenüber Versicherten

Darüber hinaus wurde ich gefragt, ob der Medizinische Dienst in Bayern verpflichtet ist, einer versicherten Person das über einen möglicherweise zu ihren Lasten begangenen Behandlungsfehler erstellte Gutachten direkt zu übersenden. Eine solche Pflicht bestand zunächst nicht. Dem Wortlaut von § 277 Abs. 1 SGB V-alt konnte ich eine solche Pflicht zur Übersendung zumindest nicht entnehmen.

Dies bedeutete aber nicht, dass sich die versicherte Person nur an die eigene Krankenkasse, die behandelnde Ärztin oder den behandelnden Arzt wenden musste, um das über ihre Person erstellte Gutachten zu erhalten. Denn eine versicherte Person hatte ebenfalls gegenüber dem Medizinischen Dienst Auskunfts- und Akteneinsichtsrechte (zum Beispiel § 276 Abs. 3 SGB V).

Inzwischen enthält § 277 Abs. 1 Satz 5 SGB V eine ausdrückliche Regelung, wonach der Medizinische Dienst verpflichtet ist, den versicherten Personen zumindest die sie betreffenden Gutachten nach § 275 Abs. 3 Satz 1 Nr. 4 SGB V in vollständiger Form zu übermitteln. Bei Begutachtungen des Medizinischen Dienstes zu Behandlungsfehlervorwürfen haben diese Personen häufig ein nachvollziehbares Interesse, das vollständige Gutachten zu erhalten, um dies in die Prüfung der weiteren Vorgehensweise einzubeziehen. Um den Interessen der versicherten Personen ausreichend Rechnung zu tragen, haben diese daher nunmehr einen direkten Anspruch auf Übermittlung dieses Gutachtens durch den Medizinischen Dienst.[64]

63 Siehe Bundesrats-Drucksache 12/21, S. 127; Bundestags-Drucksache 19/26822, S. 112.
64 Siehe Bundesrats-Drucksache 12/21, S. 127; Bundestags-Drucksache 19/26822, S. 112.

7.11 Abfragen beim Ausländerzentralregister im Sozialbereich

Das Ausländerzentralregister ist eine vom Bundesverwaltungsamt im Auftrag des Bundesamtes für Migration und Flüchtlinge betriebene Datenbank, in der personenbezogene Daten von Ausländerinnen und Ausländern gespeichert sind. Mit rund 26 Millionen Datensätzen ist das Ausländerzentralregister eines der großen automatisierten Register der öffentlichen Verwaltung in der Bundesrepublik Deutschland.[65] Das Ausländerzentralregister dient auch in Bayern vielen Behörden als Informationsquelle und unterstützt diese bei vielfältigen Aufgaben (beispielsweise im asylrechtlichen Bereich).

Im zurückliegenden Berichtszeitraum habe ich eine anlasslose Prüfung in Bezug auf Abfragen beim Ausländerzentralregister eingeleitet. Hiervon betroffen waren verschiedene Stellen aus dem Sozialbereich (insbesondere Jobcenter, Jugendämter, Sozialämter).

Die bei der Prüfung gewonnenen Erkenntnisse haben mich insbesondere zu den folgenden Hinweisen für die Nutzung des Ausländerzentralregisters veranlasst:

— Abfragen beim Ausländerzentralregister finden in unterschiedlichen Bereichen in der Sozialverwaltung statt. Begründet wurden diese regelmäßig mit der Überprüfung oder Vervollständigung von Angaben sowie der Klärung etwaiger Leistungsberechtigungen.

  Diesbezüglich ist zu beachten, dass im (Sozial-)Datenschutzrecht der Grundsatz besteht, dass Daten zunächst bei der betroffenen Person selbst zu erheben sind (sog. Grundsatz der Ersterhebung[66]). Deshalb sind die für die Sachbearbeitung notwendigen Daten bei der betroffenen Person grundsätzlich selbst zu erheben.

  Eine Datenerhebung bei Dritten, also auch der Abruf beim Ausländerzentralregister, ist dagegen nur ausnahmsweise zulässig (vgl. zum Beispiel § 67a Abs. 2 Satz 2 Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – SGB X). Deshalb ist bei einem Abruf beim Ausländerzentralregister im Einzelfall immer zu prüfen, ob eine Befugnis vorhanden ist, die eine damit verbundene Drittdatenerhebung ausdrücklich gestattet.

— Des Weiteren ist mir einerseits dargelegt worden, dass zwar Abfragen beim Ausländerzentralregister erfolgt seien. Beispielsweise sei der Aufenthaltsstatus eingesehen worden. Allerdings sei anschließend kein Ausdruck in der Akte hinterlegt worden, was ich ausdrücklich begrüßt habe.

  Andererseits ist mir aber auch erläutert worden, dass unter gewissen Umständen zur weiteren Bearbeitung Ausdrucke aus dem Ausländerzentralregister zur Akte genommen werden müssten. Dabei gilt es zu beachten, dass die auf den Ausdrucken vorhandenen, für die Aufgabenerfüllung nicht erforderlichen Daten zu schwärzen oder in anderer Form unkenntlich zu machen sind. Denn es dürfen nur die Daten erhoben und zur Akte in Papier- oder elektronischer

65 Bundesverwaltungsamt, Aufgaben von A-Z, Ausländerzentralregister, Internet: https://www.bva.bund.de/DE/Das-BVA/Aufgaben/A/Auslaenderzentralregister/azr_node.html.

66 Siehe ausführlich Bayerischer Landesbeauftragter für den Datenschutz, Der Sozialdatenschutz unter Geltung der Datenschutz-Grundverordnung, Stand 3/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Einzelthemen“.

Form genommen werden, die zur konkreten Aufgabenerfüllung im Einzelfall erforderlich sind. Eine Datensammlung auf Vorrat ist dagegen nicht zulässig.

– Darüber hinaus ist mir hinsichtlich der Verwendung von Fachverfahren (wie beispielsweise Prosoz) mitgeteilt worden, dass sich dabei das Problem stellen würde, dass darin Datenfelder (zum Beispiel zur Religionszugehörigkeit) vorgesehen sind, die zwar von der Sachbearbeitung nach vorheriger Abfrage aus dem Ausländerzentralregister der Vollständigkeit halber ausgefüllt worden seien, die jedoch für die Aufgabenerfüllung nicht notwendig seien.

  Die sich im Einsatz befindlichen Fachverfahren sind daher einer kritischen Prüfung hinsichtlich der Erforderlichkeit der Datenfelder zu unterziehen und die einsetzenden Stellen müssten sich gegebenenfalls mit dem Verfahrenshersteller bezüglich einer Möglichkeit zur Löschung von Datenfeldern in Verbindung setzen. Falls eine Anpassung des Fachverfahrens nicht möglich sein sollte, sind die Sachbearbeitungen dahingehend zu sensibilisieren, dass nur die für die Aufgabenerfüllung erforderlichen Daten beim Ausländerzentralregister erfragt und anschließend in das Fachverfahren eingetragen werden dürfen; gegebenenfalls verbleiben dann gewisse Datenfelder ohne Inhalt.

– In Bezug auf meine Nachfrage nach Erfüllung der Informationspflichten im Sinne von Art. 13 f. DSGVO habe ich die Rückmeldung erhalten, dass Informationen bislang (grundlos) unterblieben seien.

  Im Zuge der Erfüllung der Informationspflichten ist – falls keine diesbezügliche Ausnahmevorschrift, beispielsweise Art. 14 Abs. 5 Buchst. a DSGVO, eingreifen sollte – sorgfältig zu prüfen, ob den Vorgaben der Datenschutz-Grundverordnung nachgekommen wird. Dabei sollte im Rahmen der Erfüllung der Informationspflichten die Abfrage beim Ausländerzentralregister als Möglichkeit, Daten bei Dritten zu erheben, ausdrücklich benannt sein.

  Im Einzelfall kann auch ein Ausnahmetatbestand gegeben sein, wonach Informationen unterbleiben dürfen. Dieser Umstand ist auf Art. 23 DSGVO zurückzuführen, der den Mitgliedstaaten unter anderem erlaubt, das Recht einer betroffenen Person auf Informationserteilung einzuschränken. Hierfür bedarf es jedoch einer gesetzlichen Regelung. Eine solche findet sich zum Beispiel im Zehnten Buch Sozialgesetzbuch. Danach kann eine Information bei einer Datenerhebung bei Dritten unterbleiben, soweit die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten geheim gehalten werden müssen und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss (§ 82a Abs. 1 Nr. 2 SGB X). Der Verantwortliche hat allerdings schriftlich festzuhalten, aus welchen Gründen er von einer Information abgesehen hat.

  Falls ein solcher Ausnahmetatbestand greifen sollte, sind eine sorgfältige Prüfung der dazugehörigen Voraussetzungen sowie eine entsprechende (interne) Dokumentation vorzunehmen.

Diese Hinweise sollten von allen Sozialbehörden, die die Abfragemöglichkeit beim Ausländerzentralregister nutzen, beachtet werden.

8 Personalverwaltung

8.1 Verarbeitung des COVID-19-Impfstatus im bayerischen öffentlichen Dienst

Vor dem Hintergrund der fortdauernden COVID-19-Pandemie hat mich im Berichtszeitraum eine Vielzahl an Anfragen und Beschwerden zu der Frage erreicht, ob – und gegebenenfalls in welchen Fällen – bayerische Dienstherren und öffentliche Arbeitgeber den **COVID-19-Impf- oder Genesenenstatus** ihrer Beschäftigten verarbeiten dürfen.

Diese Information kann Dienstherren und Arbeitgebern einerseits dabei behilflich sein, einen ordnungsgemäßen Dienstbetrieb sicherzustellen und ihren beamten- und arbeitsrechtlichen (Fürsorge-)Pflichten den Beschäftigten gegenüber nachzukommen. Auf der anderen Seite ist die Verarbeitung dieser Daten durch Dienstherren und Arbeitgeber mit **Risiken** für die Beschäftigten verbunden. Insbesondere besteht die Gefahr, dass Dienstherren und Arbeitgeber die erhobenen Daten „zweckentfremdet" verwenden, und dass neben dem Impf- oder Genesenenstatus weitere sensible (Gesundheits-)Daten der Beschäftigten erhoben werden – etwa zu der Frage, weshalb sich Beschäftigte gegen eine mögliche Schutzimpfung entschieden haben. In der Folge können den Beschäftigten Diskriminierungen im Arbeitsumfeld oder berufliche Nachteile in der Zeit nach Bewältigung der Pandemie drohen.

Ausgangspunkt für die datenschutzrechtliche Bewertung ist die Feststellung, dass Angaben zum Impf- oder Genesenenstatus Gesundheitsdaten im Sinne von Art. 4 Nr. 15 DSGVO sind und damit zu den **besonderen Kategorien** personenbezogener Daten nach Art. 9 Abs. 1 DSGVO gehören. Eine Verarbeitung des Impf- oder Genesenenstatus Beschäftigter (einschließlich entsprechender Nachweise) durch Dienstherren und Arbeitgeber ist daher nur erlaubt, wenn eine Verarbeitungsbefugnis nach Art. 6 Abs. 1 DSGVO und (zusätzlich) ein Zulässigkeitstatbestand nach Art. 9 Abs. 2 DSGVO – jeweils gegebenenfalls in Verbindung mit nationalem Durchführungsrecht – dies gestatten. Die Verarbeitung von Gesundheitsdaten Beschäftigter durch Dienstherren oder Arbeitgeber ist somit nur bei Vorliegen der entsprechenden gesetzlichen Voraussetzungen zulässig.

Es ist deshalb zuvorderst Sache des mitgliedstaatlichen Gesetzgebers festzulegen, in welchen Bereichen und zu welchen Zwecken Dienstherren und Arbeitgeber den Impf- oder Genesenenstatus von Beschäftigten verarbeiten dürfen. Die Risiken, welche mit der Arbeit ungeimpfter Mitarbeiterinnen und Mitarbeiter für diese selbst, jedoch auch für andere verbunden sind, variieren nach Einsatzstelle und Tätigkeit, nach dem Kontakt zu Bürgerinnen und Bürgern, Kolleginnen und Kollegen ganz erheblich. Das Recht muss die Frage des Dienstherrn oder Arbeitgebers nach dem Impfschutz daher **differenziert** beantworten.

Den damit zusammenhängenden datenschutzrechtlichen Fragen habe ich mich umfassend in meinem **Arbeitspapier „Verarbeitung des COVID-19-Impfstatus im bayerischen öffentlichen Dienst"** gewidmet. Das Arbeitspapier stellt unter anderem Voraussetzungen und Reichweite von bereichsspezifischen Verarbeitungsbefugnissen dar – eine solche besteht mit § 23a Infektionsschutzgesetz (IfSG) etwa im Hinblick auf Beschäftigte in bestimmten medizinischen Einrichtungen. Auch wird die

Frage beantwortet, inwieweit die Verarbeitung des Impfstatus Beschäftigter durch Arbeitgeber im Rahmen von Erstattungsleistungen nach § 56 IfSG zulässig sein kann. Ferner führt das Papier aus, dass eine Verarbeitung des Impf- oder Genesenenstatus auf Grundlage datenschutzrechtlicher **Einwilligungen** (Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 9 Abs. 2 Buchst a DSGVO) im Beschäftigungsverhältnis **nur in Ausnahmefällen** in Betracht kommen kann. Denn vielfach wird es hier angesichts des bestehenden Machtungleichgewichts zwischen Arbeitgebern und Dienstherren auf der einen und Beschäftigten auf der anderen Seite an der nach Art. 4 Nr. 11 DSGVO erforderlichen **Freiwilligkeit fehlen**.

Insgesamt war die Rechtsentwicklung zu dieser Thematik im Berichtszeitraum von einer **hohen Dynamik** geprägt. Im Laufe des Pandemiegeschehens besondere Bedeutung erlangt hat dabei die Verarbeitung des Impf- oder Serostatus von Beschäftigten in Bezug auf COVID-19 im Rahmen von 3G-Zutrittsregelungen. **„3G am Arbeitsplatz“** bedeutet, dass betroffene Beschäftigte Arbeitsstätten grundsätzlich nur dann betreten dürfen, wenn sie im Hinblick auf COVID-19 **geimpft, genesen oder getestet** sind und dies auch nachweisen können. Entsprechende Regelungen sind zunächst auf Grundlage des Infektionsschutzgesetzes in der Bayerischen Infektionsschutzmaßnahmenverordnung, später dann bundesweit im Infektionsschutzgesetz selbst getroffen worden. Zur Umsetzung gesetzlicher 3G-Zutrittsregelungen verarbeiten Arbeitgeber und Dienstherrn neben Impf- oder Genesenennachweisen auch Testnachweise Beschäftigter. Letztere enthalten ebenfalls Gesundheitsdaten im Sinne von Art. 4 Nr. 15 DSGVO, da sie Rückschlüsse auf den Gesundheitszustand der betroffenen Person (infiziert oder nicht infiziert) zulassen. Aufgrund ihrer herausgehobenen Bedeutung habe ich die Thematik „3G am Arbeitsplatz“ gesondert in einer **Aktuellen Kurz-Information 38 „3G-Zutrittsregel im bayerischen öffentlichen Dienst“** dargestellt.

Bedingt durch die dynamische Rechtsentwicklung habe ich sowohl das Arbeitspapier als auch die Aktuelle Kurz-Information 38 zwischenzeitlich **mehrfach aktualisiert**. Die jeweils gültigen Fassungen sind auf meiner Internetseite https://www.datenschutz-bayern.de in der Rubrik „Corona-Pandemie“ abrufbar.

8.2 Regelung zur Aufbewahrung von Beurteilungsunterlagen

In meinem 29. Tätigkeitsbericht 2019 habe ich unter Nr. 12.8.2 über die Beanstandung einer bayerischen öffentlichen Stelle wegen des unbeabsichtigten Versands einer Excel-Datei mit Personaldaten berichtet. Die öffentliche Stelle hatte einer Gruppe von 45 Beamtinnen und Beamten mit einer E-Mail unbeabsichtigt eine Excel-Datei zugeleitet, die Übersichten über frühere dienstliche Beurteilungen und weitere beurteilungsbezogene Informationen enthielt. Die Übersicht betraf zahlreiche Personen, darunter auch solche, die der Gruppe nicht mehr angehörten.

Diesen Vorgang habe ich nicht nur gemäß Art. 16 Abs. 4 BayDSG förmlich beanstandet, sondern unter anderem auch zum Anlass genommen, mich für eine umfassende Regelung zum datenschutzgerechten Umgang mit beurteilungsbezogenen Unterlagen einzusetzen. Nach meiner Vorstellung sollte eine solche Regelung möglichst alle Dokumente und Dateien erfassen, die im Zusammenhang mit dienstlichen Beurteilungen stehen und sensible personenbezogene Daten enthalten können.

8.2.1 Vorgaben zum Umgang mit dienstlichen Beurteilungen

Die dienstliche Beurteilung als solche ist datenschutzrechtlich gut abgesichert. Sie zählt zur Personalakte im Sinne von § 50 Satz 2 Beamtenstatusgesetz (BeamtStG), da sie in unmittelbarem inneren Zusammenhang mit dem Dienstverhältnis steht. Das Personalaktenrecht garantiert besondere Vertraulichkeit. Insbesondere gewährt und begrenzt es Einsichts- und Auskunftsrechte (vgl. § 50 BeamtStG und Art. 103 ff. Bayerisches Beamtengesetz – BayBG).

8.2.2 Gebot einer umfassenden Regelung

In die Personalakte wird grundsätzlich allerdings nur die endgültige dienstliche Beurteilung aufgenommen; Vorarbeiten bleiben ausgeschlossen. Unterlagen, die sich auf Beurteilungen mehrerer Personen beziehen – etwa Ranglisten zur Erfüllung bestimmter Beurteilungsquoten, für Auswahlentscheidungen oder Beförderungen – können ebenfalls nicht in die Personalakte aufgenommen werden, da diese immer nur für jeweils eine Person geführt wird. Nur die dienstliche Beurteilung selbst unterfällt deshalb dem umfassenden Schutz des Personalaktenrechts. Demgegenüber ist der Umgang mit anderen Unterlagen, die in Zusammenhang mit dienstlichen Beurteilungen stehen, weitgehend nicht spezifisch geregelt. Eine wichtige Ausnahme bildet Art. 107 Abs. 1 BayBG, der das personalaktenrechtliche Auskunftsrecht der Beamtinnen und Beamten auf andere Akten erstreckt, die personenbezogene Daten über sie enthalten und für das Dienstverhältnis verarbeitet werden.

Da der Inhalt solcher Unterlagen ebenso schutzwürdig wie eine dienstliche Beurteilung sein kann, sollte nach meiner Auffassung der Umgang mit diesen Unterlagen ausführlicher geregelt werden. Notwendig erschienen mir insbesondere Regelungen zu Aufbewahrung, Vernichtung und Zugriffsberechtigungen. Zugleich sollte auch das Auskunftsrecht der Beamtinnen und Beamten gemäß Art. 107 BayBG für außerhalb der Personalakte aufbewahrte Unterlagen wirksam abgesichert werden.

8.2.3 Neuregelung in Abschnitt 3 Nr. 11.8 VV-BeamtR

Ich habe daher das für das Beamtenrecht einschließlich des Personalaktenrechts innerhalb der Bayerischen Staatsregierung federführend zuständige Bayerische Staatsministerium der Finanzen und für Heimat mehrfach und zunehmend nachdrücklich zur Regelung dieser Fragen aufgefordert.

Als Ergebnis einer mehrmonatigen, intensiven Fachdiskussion hat das Finanzministerium schließlich die Verwaltungsvorschriften zum Beamtenrecht (VV-BeamtR) überarbeitet. Abschnitt 3 Nr. 11.8 VV-BeamtR behandelt nun ausführlich Dauer und Ort der Aufbewahrung von Beurteilungsunterlagen. Die Vorschrift lautet:

„[1]Unterlagen, die in Zusammenhang mit Beurteilungen stehen, beinhalten häufig sensible personenbezogene Daten. [2]Sie sind deshalb mit der gebotenen datenschutzrechtlichen Sorgfalt aufzubewahren. [3]Die Beurteilung selbst sowie formelle Beurteilungsbeiträge sind zu den Personalakten zu nehmen und unterliegen den personalaktenrechtlichen Regelungen. [4]Alle anderen Unterlagen, die in Zusammenhang mit Beurteilungen stehen, sind sorgsam aufzubewahren, vor unbefugtem Zugriff Dritter zu schützen und so bald als rechtlich zulässig zu vernichten. [5]Vorbereitende Unterlagen wie z. B. Entwürfe, vorbereitende Übersichten sowie andere im Entstehungspro-

zess befindliche Unterlagen sind unmittelbar nach Anfertigung des endgültigen Dokuments zu vernichten. [6]Sonstige in Zusammenhang mit Beurteilungen stehende Dokumente wie z. B. Ranglisten, Übersichten oder informelle Beurteilungsbeiträge sind zu vernichten, wenn ihre Vorhaltung nicht mehr erforderlich ist. [7]Eine unter Nachweisgesichtspunkten gebotene Aufbewahrungspflicht besteht stets für die die aktuelle Beurteilung betreffenden Unterlagen. [8]Gleiches gilt für Unterlagen zu Vorbeurteilungen, soweit diese noch für Auswahlentscheidungen herangezogen werden können. [9]Die Aufbewahrung soll in der Verantwortung des zuständigen Beurteilers oder der zuständigen Personalstelle erfolgen. [10]Dies erleichtert die Erfüllung der Rechte aus Art. 107 BayBG und Art. 12 Abs. 3 Satz 1 der Datenschutz-Grundverordnung. [11]Die rechtzeitige Vernichtung ist durch geeignete Maßnahmen sicherzustellen."

In Abschnitt 18 Nr. 1.1 VV-BeamtR wird im Übrigen auch den Gemeinden und den sonstigen der Aufsicht des Freistaates Bayern unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts empfohlen, entsprechend dieser Bekanntmachung zu verfahren.

8.2.4 Datenschutzrechtliche Bewertung der neuen Regelung

Die neue Verwaltungsvorschrift regelt den Umgang mit beurteilungsbezogenen Unterlagen umfassend und detailliert. Grob unterteilt regelt Abschnitt 3 Nr. 11.8 VV-BeamtR in den Sätzen 1 bis 8 die Dauer der Aufbewahrung verschiedener Typen von Dokumenten, die in Zusammenhang mit dienstlichen Beurteilungen stehen, und in den Sätzen 9 bis 11 eher organisatorische Aspekte.

8.2.4.1 Grundsätzliches (Sätze 1 bis 3)

Die Verwaltungsvorschrift misst dem Schutz der Beurteilungsunterlagen grundsätzlich angemessene Bedeutung zu, wie Abschnitt 3 Nr. 11.8 Sätze 1 und 2 VV-BeamtR zeigen. Zutreffend zieht Abschnitt 3 Nr. 11.8 Satz 1 VV-BeamtR den Kreis der zu schützenden Unterlagen weit. Entscheidend ist der Zusammenhang mit einer dienstlichen Beurteilung. Es kommt nicht darauf an, ob ein Dokument vor oder nach einer bestimmten Beurteilung erstellt wurde. Die Vorschrift erfasst somit etwa auch Tabellen, die für Konkurrenzentscheidungen erstellt werden und auf Beurteilungen Bezug nehmen, da auch sie „in Zusammenhang mit Beurteilungen stehen". Diese Unterlagen sind mit der „gebotenen datenschutzrechtlichen Sorgfalt" aufzubewahren (vgl. Abschnitt 3 Nr. 11.8 Satz 2 VV-BeamtR).

Hervorheben möchte ich Abschnitt 3 Nr. 11.8 Satz 3 VV-BeamtR, wonach formelle Beurteilungsbeiträge zu den Personalakten genommen werden und deshalb auch dem vollen Schutz des Personalaktenrechts unterfallen. Nach Auffassung des Finanzministeriums stehen diese Dokumente ebenso wie die Beurteilung, zu der sie beitragen, in einem unmittelbaren inneren Zusammenhang mit dem Dienstverhältnis im Sinne von § 50 Satz 2 BeamtStG. Aus Datenschutzsicht ist das zu begrüßen.

8.2.4.2 Allgemeine Vorgaben zu Aufbewahrung und Vernichtung (Satz 4)

Nach Abschnitt 3 Nr. 11.8 Satz 4 VV-BeamtR sind „[a]lle anderen Unterlagen, die in Zusammenhang mit Beurteilungen stehen," sorgsam aufzubewahren, vor unbefugtem Zugriff Dritter zu schützen und so bald wie rechtlich zulässig zu vernichten. Aus dem Kontext ergibt sich, dass damit alle im Zusammenhang mit einer Beurteilung erstellten Unterlagen mit Ausnahme der dienstlichen Beurteilung selbst und der in Ab-

schnitt 3 Nr. 11.8 Satz 3 VV-BeamtR geregelten formellen Beurteilungsbeiträge gemeint sind. Sie sollen ebenso wie Personalakten besonders geschützt und frühestmöglich vernichtet werden.

Datenschutzrechtlich ist die Vernichtung von Unterlagen regelmäßig geboten, wenn sie für den Zweck, zu dem sie angefertigt worden sind, nicht mehr gebraucht werden (vgl. Art. 17 Abs. 1 Satz 1 Buchst. a DSGVO). Dementsprechend gestattet Art. 103 Satz 1 BayBG die Verarbeitung von personenbezogenen Unterlagen, wozu auch die Aufbewahrung zählt, nur im Rahmen der Erforderlichkeit zu bestimmten dienstlichen Zwecken. Werden diese Zwecke nicht oder nicht mehr verfolgt oder haben sie sich erledigt, wird die Verarbeitung (Aufbewahrung) unzulässig und sind die entsprechenden Dokumente ganz oder teilweise zu vernichten. Vor diesem Hintergrund regeln die folgenden Sätze 5 bis 8 die Aufbewahrungsdauer für verschiedene Arten von Unterlagen.

8.2.4.3 Entwürfe, vorbereitende Übersichten und „andere im Entstehungsprozess befindliche Unterlagen“ (Satz 5)

Abschnitt 3 Nr. 11.8 Satz 5 VV-BeamtR sieht die Vernichtung vorbereitender Unterlagen „wie z. B. Entwürfe, vorbereitende Übersichten sowie andere im Entstehungsprozess befindliche Unterlagen“ vor, sobald das endgültige Dokument erstellt ist.

Diese Vernichtungsanordnung erscheint sachgerecht. Datenschutzrechtlich ist die Aufbewahrung überholter Dokumente regelmäßig nicht mehr erforderlich und damit grundsätzlich unzulässig. So wird ein Beurteilungsentwurf nicht mehr benötigt, wenn die Beurteilung fertiggestellt ist. Entsprechendes gilt für noch nicht fertiggestellte vorbereitende Übersichten in Auswahlverfahren und ähnliche unfertige Dokumente.

8.2.4.4 Aufbewahrung „sonstiger“ Unterlagen (Satz 6)

Für „sonstige“ in Zusammenhang mit Beurteilungen stehende Unterlagen „wie z. B. Ranglisten, Übersichten oder informelle Beurteilungsbeiträge“ bestimmt Abschnitt 3 Nr. 11.8 Satz 6 VV-BeamtR die Vernichtung, wenn „ihre Vorhaltung nicht mehr erforderlich ist“. Regelungssystematisch sind in Abgrenzung zu den Sätzen 3 und 5 damit wohl Unterlagen gemeint, die über das Entwurfsstadium hinausgelangt sind, etwa fertiggestellte nicht formelle Beurteilungsbeiträge oder endgültige Übersichten über einen Bewerbendenkreis. Erfasst werden wohl vor allem auch Unterlagen, die – bislang – häufig in den Handakten von Vorgesetzten, auch elektronisch, aufbewahrt werden.

Wie lange die Aufbewahrung dieser Unterlagen im Einzelfall erforderlich und damit zulässig ist, kann nur in Kenntnis des konkreten Zwecks der Aufbewahrung beantwortet werden. Nach Ansicht des Finanzministeriums geht es vor allem darum, in Gerichtsverfahren Beurteilungen zu verteidigen und Auswahlentscheidungen in Konkurrenzsituationen zu begründen. In derartigen Verfahren könne es auf Informationen ankommen, die zwar nicht in den Beurteilungen selbst, aber in damit zusammenhängenden Unterlagen enthalten sind.

Dieses Argument ist zwar an sich nachvollziehbar. Sind dienstliche Beurteilungen in Gerichtsverfahren nicht anders als durch Rückgriff auf „sonstige“ Beurteilungsunterlagen „zu halten“, spricht das für die Erforderlichkeit der Aufbewahrung. Voraussetzung ist jedoch, dass kein milderes, ebenso geeignetes Mittel erkennbar ist, das den

Bestand dienstlicher Beurteilungen in gleicher Weise absichern könnte, etwa sorgfältigere Beurteilungsbegründungen, wenn Beurteilungen dadurch weniger streitanfällig würden, so dass ein Rückgriff auf „sonstige“ Unterlagen seltener nötig wäre.

Die datenschutzrechtliche Erforderlichkeit der Aufbewahrung von Unterlagen darf schließlich nicht nur behauptet werden. Ebenso wenig kann es genügen, wenn die Unterlagen nur vielleicht einmal gebraucht werden könnten. Die Aufbewahrung könnte dann im Einzelfall zwar nützlich sein; sie wäre aber angesichts ihrer enormen praktischen Reichweite rechtlich kaum als zwingend erforderlich zu bewerten. Lässt sich die Erforderlichkeit der Aufbewahrung aber nicht belegen, könnte bezweifelt werden, ob die Aufbewahrung der sonstigen Beurteilungsunterlagen nahezu aller Beamtinnen und Beamten noch verhältnismäßig (angemessen) ist oder ob die Daten ohne konkrete Aussicht auf praktische Verwendung letztlich nur auf Vorrat gespeichert werden.

Aus Datenschutzsicht wäre es deshalb wichtig zu wissen, wie oft „sonstige Unterlagen“ zu den genannten gerichtlichen Zwecken tatsächlich benötigt werden. Leider konnte mir das Finanzministerium auch auf wiederholte Aufforderung hin keine Auskunft dazu erteilen, wie oft „sonstige“ Unterlagen im Sinne von Abschnitt 3 Nr. 11.8 Satz 6 VV-BeamtR in Gerichtsverfahren entscheidungserheblich sind. Daher halte ich derzeit die datenschutzrechtliche Zulässigkeit dieser Regelung für zweifelhaft.

8.2.4.5 Sonstige Unterlagen zur aktuellen dienstlichen Beurteilung (Satz 7)

Nach Abschnitt 3 Nr. 11.8 Satz 7 VV-BeamtR müssen die Unterlagen zu laufenden Beurteilungen „unter Nachweisgesichtspunkten“ stets aufbewahrt werden. Ich nehme an, dass auch diese Regelung für Gerichtsverfahren gedacht ist, und die aktuelle Beurteilung wesentlich häufiger gerichtlich überprüft wird als frühere Beurteilungen. Ich halte es daher für möglich, dass die angesprochenen Unterlagen bei der Plausibilisierung von Leistung, Eignung und Befähigung im Zusammenhang mit der Überprüfung von Personalmaßnahmen in einer im Verhältnis zur Gesamtzahl der Beurteilungen relevanten Zahl von Fällen gebraucht werden. Ob diese Einschätzung zutrifft, wäre aber noch zu belegen. Dabei sollte sich ergeben, dass ein prozentual relevanter Teil der Beurteilungen und Auswahlentscheidungen angegriffen und die Entscheidung regelmäßig durch Rückgriff auf „sonstige Unterlagen“ beeinflusst wird. Das Finanzministerium konnte hierzu ebenfalls keine Angaben machen.

8.2.4.6 Sonstige Unterlagen zu Vorbeurteilungen (Satz 8)

Noch schwieriger zu bewerten ist Abschnitt 3 Nr. 11.8 Satz 8 VV-BeamtR. Demnach sollen Unterlagen zu Vorbeurteilungen aufbewahrt werden, soweit diese noch für Auswahlentscheidungen herangezogen werden können. Bei der in erster Linie vorzunehmenden Würdigung von Leistung, Eignung und Befähigung des Bewerbendenkreises können frühere Beurteilungen grundsätzlich einbezogen werden, da sie nach der Rechtsprechung des Bundesverwaltungsgerichts Hinweise auf die nach Art. 33 Abs. 2 Grundgesetz bedeutsamen Gesichtspunkte der dienstlichen Erfahrung, der Verwendungsbreite und der Leistungsentwicklung geben können.[67]

Abschnitt 3 Nr. 11.8 Satz 8 VV-BeamtR zielt aber offenbar nicht darauf ab, alle sonstigen Unterlagen, die in Zusammenhang mit einer früheren dienstlichen Beurteilung

[67] Vgl. etwa Bundesverwaltungsgericht, Urteil vom 19. Februar 2002, 2 C 31.01, BeckRS 2003, 21261; Urteil vom 21. August 2003, 2 C 14/02, BeckRS 25254; Urteil vom 4. November 2010, 2 C 16.09, BeckRS 2011, 45441; Urteil vom 30. Juni 2011, 2 C 19.10, BeckRS 2011, 53364.

einer aktiven Beamtin oder eines aktiven Beamten gefertigt wurden, dauerhaft aufzubewahren. Dann hätte es der besonderen Aufbewahrungsanordnung in Abschnitt 3 Nr. 11.8 Satz 7 VV-BeamtR für die aktuelle Beurteilung nicht bedurft. Abschnitt 3 Nr. 11.8 Satz 8 VV-BeamtR sei vielmehr – wie mir das Finanzministerium erläutert hat – vor dem Hintergrund der Auswahl- und Beförderungsrichtlinien der einzelnen Ressorts der Bayerischen Staatsregierung zu sehen. Nach diesen Richtlinien könne bei der Auswahl zwischen mehreren im Wesentlichen nach Leistung, Eignung und Befähigung gleich geeigneten Personen auf Hilfskriterien zurückgegriffen werden, zu denen auch eine oder mehrere Vorbeurteilungen zählen könnten. Um diese Vorbeurteilungen – als Hilfskriterien – umfassend einzuschätzen, sehe Abschnitt 3 Nr. 11.8 Satz 8 VV-BeamtR die Aufbewahrung der Unterlagen vor.

Unter der Annahme eines dreijährigen Beurteilungsturnus und der hilfsweise möglichen Berücksichtigung von zwei Vorbeurteilungen sieht Abschnitt 3 Nr. 11.8 Satz 8 VV-BeamtR somit im Ergebnis eine Aufbewahrungsdauer von rund neun Jahren vor. Das halte ich mit Blick auf die noch nicht nachgewiesene praktische Bedeutung der Unterlagen für Gerichtsverfahren, auf die für die Aufbewahrung abgestellt wird, für bedenklich. Angesichts der langen Aufbewahrungsdauer wäre es besonders wichtig zu wissen, wie häufig es in Gerichtsverfahren auf sonstige Unterlagen zu Vorbeurteilungen ankommt, die bei Auswahlentscheidungen als Hilfskriterien herangezogen wurden. Nach meiner Einschätzung werden Vorbeurteilungen ohnehin allenfalls selten im Rahmen ihrer Verwendung als Hilfskriterien überprüft. Noch seltener dürfte in solchen Verfahren der Rückgriff auf ergänzende Unterlagen sein.

8.2.4.7 Aufbewahrungsort (Sätze 9 bis 10)

Nach Abschnitt 3 Nr. 11.8 Satz 9 VV-BeamtR sollen die Beurteilungsunterlagen, soweit sie nicht nach Abschnitt 3 Nr. 11.8 Satz 3 VV-BeamtR zu den Personalakten zu nehmen oder nach Abschnitt 3 Nr. 11.8 Satz 5 VV-BeamtR zu vernichten sind, in der Verantwortung des zuständigen Beurteilers oder der zuständigen Personalstelle aufbewahrt werden. Zuständiger Beurteiler ist im Regelfall des Art. 60 Abs. 1 Satz 1 Leistungslaufbahngesetz die Leitung der Beschäftigungsbehörde. Abschnitt 3 Nr. 11.8 Satz 9 VV-BeamtR bezweckt also, dass sämtliche Beurteilungsunterlagen, die eine bestimmte Person betreffen, bei der beurteilenden Dienststelle zentral aufbewahrt werden, entweder bei der Behördenleitung oder bei der Personalstelle. Die Regelung bedeutet zugleich, dass sämtliche Unterlagen, die im Zusammenhang mit einer Beurteilung oder einem Auswahlverfahren erstellt wurden, unverzüglich an die Leitung der Beschäftigungsbehörde oder an die Personalabteilung zu schicken sind, insbesondere die „sonstigen" Unterlagen im Sinne von Abschnitt 3 Nr. 11.8 Satz 6 VV-BeamtR, auch soweit sie in Handakten enthalten sein sollten. Das ist plausibel, wenn man davon ausgeht, dass diese Unterlagen tatsächlich für Gerichtsverfahren relevant sind. Dann müssen sie bei Bedarf auch schnell an der Stelle verfügbar sein, die das Gerichtsverfahren betreut. Das wird regelmäßig die Personalstelle sein.

Wie Abschnitt 3 Nr. 11.8 Satz 10 VV-BeamtR zutreffend ausführt, erleichtert eine gebündelte Aufbewahrung auch die Erfüllung der Auskunftsrechte aus Art. 107 BayBG und weiterer Datenschutzrechte entsprechend Art. 12 Abs. 3 Satz 1 DSGVO. Tatsächlich ist es schwer vorstellbar, datenschutzrechtliche Pflichten vollständig und kurzfristig zu erfüllen, wenn die einschlägigen Unterlagen bei verschiedenen Dienststellen oder früheren Vorgesetzten erst mühsam zusammengesucht werden müssten. Auch die rechtzeitige, datenschutzrechtlich nachzuweisende (vgl. Art. 5 Abs. 2 DSGVO) Vernichtung von Unterlagen lässt sich anders als durch eine zentrale Aufbewahrung praktisch kaum verwirklichen. Die Regelung harmoniert damit mit Art. 103 Satz 2 BayBG, wonach der Kreis der auf Personaldaten Zugriffsberechtigten möglichst eng

zu ziehen ist. Eine gestreute, dezentrale Aufbewahrung der personenbezogenen Unterlagen wäre damit grundsätzlich nicht vereinbar. Bei den Personalabteilungen dürfte zumeist auch der größte Sachverstand hinsichtlich der regelmäßigen Prüfungen der weiteren Erforderlichkeit der Aufbewahrung oder der Vernichtung der einzelnen Dokumente zu verorten sein.

8.2.4.8 Maßnahmen zur rechtzeitigen Vernichtung (Satz 11)

Gemäß Abschnitt 3 Nr. 11.8 Satz 11 VV-BeamtR ist die rechtzeitige Vernichtung der Unterlagen durch geeignete Maßnahmen sicherzustellen. Die Verwaltungsvorschrift lässt offen, wie diese Maßnahmen aussehen könnten oder sollten. Ich gehe davon aus, dass eine halbjährliche Sichtung der Unterlagen durch die aufbewahrende Stelle datenschutzrechtlichen Anforderungen (noch) genügen dürfte. Dabei ist auch zu prüfen, inwieweit Unterlagen teilweise zu vernichten (schwärzen) sind.

8.2.5 Abschließende Bemerkungen

Die Verwaltungsvorschrift bestimmt umfassende Aufbewahrungspflichten für Unterlagen, die in Zusammenhang mit dienstlichen Beurteilungen stehen. Zugleich wird die Notwendigkeit der rechtzeitigen Vernichtung betont. Zuständig für die Aufgaben sind in der Regel die Personalstellen (vgl. Abschnitt 3 Nr. 11.8 Satz 9 VV-BeamtR).

Meine rechtlichen Zweifel hinsichtlich der Aufbewahrungspflichten habe ich angedeutet. Sie betreffen insbesondere sonstige Unterlagen zu Vorbeurteilungen (siehe oben zu Abschnitt 3 Nr. 11.8 Satz 8 VV-BeamtR). Die hier in einer Verwaltungsvorschrift vorgesehenen Aufbewahrungsfristen können sich über gesetzliche Löschungspflichten, die insbesondere aus Art. 103 Satz 1 BayBG folgen können, normenhierarchisch jedenfalls nicht durchsetzen. Die Verwaltungsvorschrift selbst kann die Notwendigkeit der Aufbewahrung daher nicht begründen.

Die angesprochenen datenschutzrechtlichen Zweifel auszuräumen ist grundsätzlich Sache des – insbesondere staatlichen oder kommunalen – Verantwortlichen, der entsprechend Art. 5 Abs. 2 DSGVO zu dokumentieren hat, welche Maßnahmen er zur Prüfung der Erforderlichkeit der Aufbewahrung der Dokumente oder zu ihrer Vernichtung ergriffen hat. Dazu zählt nach meiner Auffassung vor allem eine Übersicht über die Gerichtsverfahren, in denen „sonstige Unterlagen“ entscheidungserheblich waren, aufgegliedert nach Unterlagen zur aktuellen Beurteilung, erster Vorbeurteilung und gegebenenfalls weiteren Vorbeurteilungen. Ich erwarte insofern den Nachweis, dass diese Unterlagen eine hinreichende Anzahl von gerichtlichen Entscheidungen tatsächlich beeinflussen, so dass die weitreichende Aufbewahrungspflicht gerechtfertigt werden kann. Eine solche Übersicht kann grundsätzlich auch von einer übergeordneten Stelle für ihren Bereich vorgelegt werden.

Trotz einiger kritischer Anmerkungen begrüße ich im Ergebnis aber die Neuregelung. Bei entsprechender Anwendung kann sie den Datenschutz im Umgang mit Beurteilungsunterlagen deutlich stärken. Das gilt besonders für die Regelung der Vernichtung von Entwürfen und vergleichbaren Dokumenten sowie der Aufbewahrung der Unterlagen bei Leitung oder Personalstelle der Beschäftigungsbehörde. Damit wird zumindest der Versuch unternommen, die weit verbreitete Praxis abzustellen, dass (ehemalige) Vorgesetzte Beurteilungsentwürfe und sonstige Beiträge oder Übersichten dauerhaft in Papierform oder elektronisch, etwa als Muster, aufbewahren.

Auch das Risiko einer Wiederholung des eingangs geschilderten Szenarios – versehentlicher Versand einer Beurteilungsübersicht – sollte durch die konsequente Anwendung der neuen Verwaltungsvorschrift erheblich reduziert werden.

8.3 Verlängerung der Aufbewahrungsfrist für Beihilfeunterlagen

Eine aus Datenschutzsicht unerfreuliche Entwicklung hat sich im Berichtszeitraum im Hinblick auf das bayerische Beihilferecht ergeben. Nach bisheriger Rechtslage waren **Beihilfeunterlagen**, aus denen die **Art der Erkrankung** ersichtlich ist, unverzüglich zurückzugeben oder zu vernichten, sobald die Beihilfestelle sie nicht mehr benötigte. Nunmehr sind diese Unterlagen gesetzlich **fünf Jahre** aufzubewahren. Vergleichbares gilt für Unterlagen über **Heilfürsorge und Heilverfahren**, deren generelle Aufbewahrungsfrist nun ebenfalls fünf Jahre beträgt.

Gegen diese Rechtsänderung habe ich im Laufe des Gesetzgebungsverfahrens **erhebliche Bedenken** vorgebracht. Leider ist meinen Bedenken nur teilweise Rechnung getragen worden. Gerade für aktive bayerische Beamtinnen und Beamte bedeutet die Neuregelung in datenschutzrechtlicher Hinsicht eine **klare Verschlechterung**.

8.3.1 Sensibilität von Beihilfeunterlagen

Die Gewährung von Beihilfen nach Art. 96 Bayerisches Beamtengesetz (BayBG) hat für den berechtigten Personenkreis – der insbesondere aktive und ehemalige Beamtinnen und Beamte sowie gegebenenfalls deren Angehörige umfasst – Vorteile: Im Umfang des Beihilfebemessungssatzes (in der Regel 50 v.H. oder 70 v.H., vgl. Art. 96 Abs. 3 Sätze 2 und 3 BayBG) gewährt der Dienstherr Beihilfeleistungen zu medizinisch notwendigen und angemessenen Aufwendungen in Krankheits-, Geburts- und Pflegefällen sowie zur Gesundheitsvorsorge. Berechtigte Personen müssen sich daher nur zu dem Teil ergänzend (privat) versichern, der nicht von der Beihilfe abgedeckt ist.

Die Gewährung von Beihilfe setzt voraus, dass die entsprechenden Aufwendungen von den Beamtinnen und Beamten nachgewiesen werden (vgl. Art. 96 Abs. 2 Satz 1 BayBG). Die hiernach zu erbringenden **Nachweise** enthalten allerdings regelmäßig eine Vielzahl **hochsensibler Gesundheitsdaten** der betreffenden Beschäftigten und gegebenenfalls deren Angehöriger – insbesondere in Form medizinischer (Krankheits-)Diagnosen und sonstiger Feststellungen. Beamtinnen und Beamte haben daher ein gewichtiges Interesse daran, dass diese sensiblen Gesundheitsdaten – die als besondere Kategorie personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO unter erhöhtem Schutz stehen – **strikt zweckgebunden** für Leistungen der Krankenfürsorge verwendet werden, und eine **Nutzung für anderweitige Verwendungsinteressen** des Dienstherrn (etwa für Dienstfähigkeitsbeurteilungen) **unterbleibt**.

8.3.2 Das spezifische datenschutzrechtliche „Beihilferisiko“

Hier birgt das System der Beihilfe insbesondere für aktive Beamtinnen und Beamte ein **spezifisches Risiko**: Die Festsetzung der Beihilfen obliegt nämlich den obersten Dienstbehörden; diese können ihre Befugnisse auf andere Dienststellen übertragen (Art. 96 Abs. 4 Sätze 1 und 2 BayBG). Für den staatlichen Bereich setzt grundsätzlich

das Landesamt für Finanzen mit seinen Dienststellen als zentrale Landesbehörde die Beihilfe der Berechtigten fest (Art. 96 Abs. 4 Satz 3 BayBG).

Während also in Fällen von Leistungen der gesetzlichen oder privaten Krankenversicherung hochsensible Unterlagen (Arztbriefe, Arzneimittelverschreibungen etc.) über die betreffenden Personen an eine vom Dienstherrn oder Arbeitgeber vollständig getrennte und von diesem unabhängige Stelle gehen, liegt bei der Beihilfe grundsätzlich eine **dienstherrnmäßige Identität** von Beschäftigungs-/Personalstelle und Krankenfürsorgestelle vor. Mit anderen Worten gelangen im Rahmen der Beihilfegewährung Gesundheitsdaten von Beamtinnen und Beamten regelmäßig in den **Verfügungsbereich des Dienstherrn**. (Anders ist dies etwa in Konstellationen der „Beihilfeversicherung" nach Art. 96 Abs. 4 Satz 5 BayBG, die jedoch im staatlichen Bereich gesetzlich nicht zulässig ist).

Der Gesetzgeber hat dieses spezifische „Beihilferisiko" erkannt und verschiedene **risikomindernde Maßnahmen** gesetzlich vorgesehen. Hierzu zählen seit jeher eine strenge Zweckbindung von Beihilfeunterlagen (vgl. Art. 105 Abs. 2 BayBG), die organisatorische Abschottung der Beihilfesachbearbeitung von der übrigen Personalverwaltung (vgl. Art. 105 Abs. 1 BayBG), aber auch möglichst **kurze Aufbewahrungs- und Speicherfristen**. Die diesbezüglichen Vorgaben in Art. 110 Abs. 2 BayBG hat der Gesetzgeber durch das Gesetz zur Änderung dienstrechtlicher Vorschriften vom 23. Dezember 2021 (GVBl. S. 663) leider zwischenzeitlich erheblich „aufgeweicht".

8.3.3 Die Aufbewahrung von Beihilfeunterlagen nach alter und neuer Rechtslage

Die Aufbewahrung von Beihilfeunterlagen war in Art. 110 Abs. 2 BayBG-alt bislang im Wesentlichen wie folgt geregelt:

„[1]Unterlagen über Beihilfen, Heilfürsorge, Heilverfahren, Unterstützungen, Erholungsurlaub, Erkrankungen sowie Umzugs- und Reisekosten sind fünf Jahre nach Ablauf des Jahres, in dem die Bearbeitung des einzelnen Vorgangs abgeschlossen wurde, aufzubewahren. [2]Sofern aus ihnen die Art der Erkrankung ersichtlich ist, sind sie unverzüglich zurückzugeben oder zu vernichten, wenn sie für den Zweck, zu dem sie vorgelegt worden sind, nicht mehr benötigt werden. [3]Elektronisch gespeicherte Beihilfebelege sind spätestens ein Jahr nach Ablauf des Jahres, in dem die Unterlagen elektronisch erfasst wurden, zu löschen, sofern sie nicht darüber hinaus für die Bearbeitung oder auf Grund sonstiger gesetzlicher Vorschriften benötigt werden. […]"

Die Vorschrift sah somit zwar bereits eine grundsätzliche Aufbewahrungsdauer für Beihilfeunterlagen von fünf Jahren vor (Art. 110 Abs. 2 Satz 1 BayBG-alt). Ausgenommen hiervon waren allerdings **Beihilfeunterlagen**, aus denen die **Art der Erkrankung** ersichtlich ist – diese waren **unverzüglich zurückzugeben oder zu vernichten**, sobald die Beihilfestelle sie nicht mehr benötigte (Art. 110 Abs. 2 Satz 2 BayBG-alt). Elektronisch gespeicherte Beihilfebelege waren grundsätzlich spätestens ein Jahr nach Ablauf des Jahres, in dem die Unterlagen elektronisch erfasst wurden, zu löschen, Art. 105 Abs. 2 Satz 3 BayBG-alt.

Demgegenüber sieht der neu gefasste, zum 1. Januar 2022 in Kraft getretene Art. 110 Abs. 2 BayBG nunmehr Folgendes vor:

„[1]Unterlagen über Beihilfen, Heilfürsorge, Heilverfahren, Unterstützungen, Erholungsurlaub, Erkrankungen sowie Umzugs- und Reisekosten sind fünf Jahre nach Ablauf des Jahres, in dem die Bearbeitung des einzelnen Vorgangs abgeschlossen

wurde, aufzubewahren. [2]Sofern aus Unterlagen über Unterstützungen, Erholungsurlaub, Erkrankungen sowie Umzugs- und Reisekosten die Art der Erkrankung ersichtlich ist, sind sie unverzüglich zurückzugeben oder zu vernichten, wenn sie für den Zweck, zu dem sie vorgelegt worden sind, nicht mehr benötigt werden. […]“

Beihilfeunterlagen sind – ebenso wie Unterlagen über Heilfürsorge und Heilverfahren – in Art. 110 Abs. 2 Satz 2 BayBG nicht mehr genannt. Die spezifische Regelung für elektronisch gespeicherte Beihilfebelege ist entfallen. In der Folge erstreckt sich die **fünfjährige Aufbewahrungsfrist** nach Art. 110 Abs. 2 Satz 1 BayBG **generell auf Beihilfeunterlagen** – und damit auch auf solche, aus denen die Art der Erkrankung ersichtlich ist.

Der Gesetzgeber hat diese Änderung insbesondere mit der zwischenzeitlich auf drei Jahre verlängerten Beantragungsfrist für die Beihilfe (vgl. Art. 96 Abs. 3a BayBG) begründet. Bei Beibehaltung der bisherigen, kürzeren Aufbewahrungsfristen entstehe eine Divergenz, die „ein Einfallstor für Fehlerstattungen und Missbrauch“ biete. Des Weiteren ergebe sich aus den bisherigen Aufbewahrungsfristen „ein erhebliches Betrugsrisiko“ (vgl. Landtags-Drucksache 18/17828, Seite 1). Letztlich verfolgt die Fristverlängerung das Anliegen, Fälle des Beihilfemissbrauchs besser erkennen und verfolgen zu können.

Dieses Anliegen kann ich zwar grundsätzlich nachvollziehen. Die von der Bayerischen Staatsregierung vorgebrachte Begründung zu dieser Gesetzesänderung konnte mich allerdings **nicht überzeugen** – im Hinblick auf die verlängerte Antragsfrist für die Beihilfe schon deshalb nicht, weil insoweit eine Angleichung der Aufbewahrungsfrist auf ebenfalls drei Jahre ausgereicht hätte. Insbesondere aber hat der Gesetzentwurf einen tatsächlichen Handlungsbedarf im Hinblick auf (mögliche) Fehlleistungen der Beihilfestellen **nicht substantiiert nachgewiesen**. Valide tatsächliche Erkenntnisse über das (angenommene) Ausmaß des Beihilfemissbrauchs hat mir das innerhalb der Bayerischen Staatsregierung insoweit federführend zuständige Bayerische Staatsministerium der Finanzen und für Heimat auch auf mehrfache Nachfrage hin nicht mitteilen können. Die der Gesetzesänderung zugrunde liegenden Annahmen bleiben somit letztlich **weitgehend spekulativ**.

Beihilfeunterlagen, aus denen die Art der Erkrankung ersichtlich ist, sind in **höchstem Maße sensibel**. Mitgliedstaatliches Recht kann zwar die Verarbeitung von Gesundheitsdaten Beschäftigter durch den Dienstherrn zulassen, soweit dies zur Erfüllung dienstrechtlicher Pflichten und Rechte erforderlich ist – dann muss dieses Recht allerdings „geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsehen“, vgl. Art. 9 Abs. 2 Buchst. b DSGVO.

Die nun Gesetz gewordene Verlängerung der Aufbewahrungsdauer für Unterlagen über Beihilfe, Heilfürsorge und Heilverfahren, aus denen die Art der Erkrankung ersichtlich ist, dürfte im Ergebnis – jedenfalls im staatlichen Bereich – zum Aufbau einer aussagekräftigen **Gesundheitsdatenbank** über alle aktiven und ehemaligen bayerischen Beamtinnen und Beamten sowie deren beihilfeberücksichtigungsfähige Angehörigen führen. Eine **belastbare Grundlage** für diesen **intensiven Grundrechtseingriff** ist für mich unverändert nicht erkennbar. Zwar hat der Gesetzentwurf schon in einem frühen Stadium als „Kompensation“ für diesen Eingriff entsprechende Zugriffsbeschränkungen vorgesehen (vgl. Art. 105 Abs. 3 BayBG). Diese allein waren und sind jedoch aus meiner Sicht insoweit nicht ausreichend. Ich bin dieser Gesetzesänderung daher – auch im Gespräch mit dem Finanzministerium – **entschieden entgegen getreten**.

Die dargestellte Gesetzesänderung hat letztlich ein **Vorhaben aufgegriffen**, das die Bayerische Staatsregierung bereits vor einigen Jahren verfolgt hatte. Damals war – mit einer vergleichbaren Begründung – vorgesehen gewesen, die Aufbewahrungsfrist für Beihilfeunterlagen sogar auf **zehn Jahre** zu verlängern. Auf meine Intervention hin hatte die Bayerische Staatsregierung von diesem Vorhaben allerdings wieder Abstand genommen (siehe hierzu meine Ausführungen im 28. Tätigkeitsbericht 2018 unter Nr. 12.1.1).

Leider konnte ich mit meinen datenschutzrechtlichen Bedenken, die ich im Laufe des Gesetzgebungsverfahrens erneut vorgebracht habe, diesmal nicht vollständig durchdringen. Immerhin ist die Aufbewahrungsfrist für Beihilfeunterlagen, aus denen die Art der Erkrankung ersichtlich ist, statt auf die ursprünglich einmal angedachten zehn auf nunmehr „nur" fünf Jahre verlängert worden. Ferner wurde meinen Vorbehalten insoweit Rechnung getragen, als Art. 105 Abs. 2 Satz 2 BayBG nunmehr ausdrücklich klarstellt, dass Beihilfeakten **in keinem Fall an personalverwaltende Stellen weitergegeben** werden dürfen.

8.3.4 Fazit

Seit dem 1. Januar 2022 sind Unterlagen über Beihilfen – ebenso wie Unterlagen über Heilfürsorge und Heilverfahren – auch dann fünf Jahre aufzubewahren, wenn aus diesen Unterlagen die Art der Erkrankung ersichtlich ist. Diese gegenüber dem bisherigen Recht **erhebliche Verlängerung der Aufbewahrungsdauer ist aus Datenschutzsicht zu bedauern**. Im Vergleich zu einem diesbezüglichen Regelungsvorhaben der Bayerischen Staatsregierung vor einigen Jahren konnte ich immerhin teilweise datenschutzrechtliche Verbesserungen durchsetzen. Die Einhaltung der gesetzlichen Vorgaben in der Beihilfepraxis werde ich im Rahmen meiner Aufsichtszuständigkeit genau im Blick behalten.

8.4 Zugriff auf Zeiterfassungsdaten

Ein Landratsamt hat mich nach den Möglichkeiten und Grenzen interner Zuständigkeitsregelungen für den Zugriff auf Zeiterfassungsdaten der Beschäftigten, sei es bei Beamtinnen und Beamten, sei es bei Tarifbeschäftigten, gefragt. Konkret sollte eine Regelung getroffen werden, wonach die Funktion der oder des Arbeitszeitbeauftragten dezentral für jeden Arbeitsbereich von der jeweiligen Arbeitsbereichsleitung übernommen wird.

Den Umgang mit Zeiterfassungsdaten habe ich bereits in meinem 20. Tätigkeitsbericht 2002 unter Nr. 13.1.3, in meinem 22. Tätigkeitsbericht 2006 unter Nr. 19.3, in meinem 24. Tätigkeitsbericht 2010 unter Nr. 11.2.2, in meinem 25. Tätigkeitsbericht 2012 unter Nr. 11.8.3 und in meinem 27. Tätigkeitsbericht 2016 unter Nr. 11.10 erörtert.

Zeiterfassungsdaten von Beschäftigten sind grundsätzlich Personalaktendaten. Der Dienstherr muss bei der Verarbeitung von Personalaktendaten die Voraussetzungen der Art. 103 ff. Bayerisches Beamtengesetz (BayBG) und § 50 Beamtenstatusgesetz (BeamtStG) beachten. Diese Vorschriften sind gemäß Art. 145 Abs. 2 BayBG auch auf die nicht-verbeamteten Beschäftigten des bayerischen öffentlichen Dienstes im Grundsatz entsprechend anzuwenden.

Nach Art. 103 Satz 1 Nr. 1 BayBG, § 50 Satz 4 BeamtStG darf der Dienstherr personenbezogene Daten nur verarbeiten, soweit dies zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere zu Zwecken der Personalverwaltung oder Personalwirtschaft erforderlich ist. Die Verarbeitung darf gemäß Art. 103 Satz 2 BayBG außerdem nur durch Beschäftigte erfolgen, die vom Dienstherrn mit der Bearbeitung von Personalangelegenheiten betraut sind. Der Kreis der mit Personaldaten befassten Beschäftigten ist dabei möglichst eng zu begrenzen.

Zur Ausfüllung der gesetzlichen Vorgaben im Rahmen der Arbeitszeitermittlung ist insbesondere Abschnitt 11 der Verwaltungsvorschriften zum Beamtenrecht (VV-BeamtR) zu beachten. Für Gemeinden und sonstige der Aufsicht des Freistaates Bayern unterstehende Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts gilt die Anwendungsempfehlung gemäß Abschnitt 18 Nr. 1.1 VV-BeamtR.

Im Hinblick auf den Zugang zu den Zeiterfassungsdaten enthält Abschnitt 11 Nr. 1.7 VV-BeamtR die Regelung, dass die Dienststellenleitung die Arbeitszeiterfassung und die Einhaltung der Dienstvereinbarung durch geeignete Maßnahmen zu überwachen hat. Abschnitt 11 Nr. 1.9 VV-BeamtR regelt, dass die Dienststellenleitung die ihr nach den vorstehenden Verwaltungsvorschriften zugewiesenen Befugnisse und Verpflichtungen allgemein oder im Einzelfall delegieren kann, soweit dies zweckmäßig erscheint.

In der Praxis wird hierzu meist eine Bedienstete oder ein Bediensteter zur oder zum sog. Arbeitszeitbeauftragten bestellt. Aus datenschutzrechtlicher Sicht möglich und zulässig ist es zwar auch, der oder dem (unmittelbaren) Vorgesetzten die Aufgabe der Kontrolle der Arbeitszeiterfassung für ihren oder seinen jeweiligen Verwaltungsbereich zu übertragen. **Idealerweise** bestellt der Dienstherr aber eine **zentrale Arbeitszeitbeauftragte oder** einen **zentralen Arbeitszeitbeauftragten**. Andernfalls sehen sich die Beschäftigten leicht einer umfassenden Verhaltens- und Leistungskontrolle durch ihre unmittelbare Vorgesetzte oder ihren unmittelbaren Vorgesetzten ausgesetzt. Soweit verwaltungsorganisatorisch umsetzbar, ist es stets vorzugswürdig, die Überwachung der Arbeitszeiterfassung sowie die Einhaltung einer diesbezüglichen Dienstvereinbarung anderen Beschäftigten zu übertragen.

Eine Regelung, wonach die Funktion der oder des Arbeitszeitbeauftragten für jeden Arbeitsbereich von der jeweiligen **Arbeitsbereichsleitung** übernommen wird, ist zwar grundsätzlich zulässig. Allerdings halte ich auch im Falle der Bestellung einer oder eines Fachvorgesetzten zur oder zum (Teil-)Arbeitszeitbeauftragten ein jederzeitiges anlassloses Einsichtsrecht etwa in die Monatsübersichten ihrer oder seiner Mitarbeiterinnen und Mitarbeiter für nicht erforderlich. Insoweit erscheint mir ein Zugriff allenfalls zu bestimmten Stichpunkten (etwa regelmäßig zu Beginn eines Monats für die Übersichten des Vormonats) mit der von Art. 103 BayBG aufgestellten doppelten Zugangsbeschränkung, wonach gerade der jeweilige Zugriff auf Personalaktendaten im Einzelfall erforderlich sein muss, vereinbar.

Zu beachten ist ferner, dass zu (Teil-)Arbeitszeitbeauftragten bestellte Fachvorgesetzte nur auf die Zeiterfassungsdaten der Mitarbeiterinnen und Mitarbeiter ihres Bereichs zugreifen dürfen. Datennutzungen, die darüber hinausgehen, sind nur mit einer freiwilligen und informierten Einwilligung der jeweiligen Beschäftigten zulässig (vgl. § 50 Satz 4 BeamtStG).

Soweit die örtliche Regelung des Landratsamts vorsah, dass außerhalb der Arbeitsbereiche (also in hierarchisch höheren Organisationseinheiten, etwa auf Abteilungs-

oder Sachgebietsebene) die Funktion der oder des Arbeitszeitbeauftragten nicht gesondert besetzt ist, sollten Sachgebiets- und Abteilungsleitungen zwar formell keine derartige Funktion übernehmen, gleichwohl aber in die Zeiterfassungsdaten der Beschäftigten ihrer jeweiligen Organisationseinheiten (Abteilung oder Sachgebiet) gegebenenfalls anlasslos Einsicht nehmen können.

Insoweit ist allerdings die personelle Zugangsbeschränkung des Art. 103 Satz 2 BayBG zu beachten. Fachvorgesetzten dürfen personenbezogene Daten für Zwecke der Personalverwaltung oder Personalwirtschaft nur zugänglich gemacht werden, soweit dies für ihre Aufgabenerfüllung erforderlich ist. Nicht zu beanstanden ist es etwa, wenn **Fachvorgesetzte (ohne Arbeitszeitbeauftragte zu sein)** den aktuellen An- oder Abwesenheitsstatus der Beschäftigten ihrer Organisationseinheit und den Grund der Abwesenheit (etwa Krankheit, Urlaub, Dienstbefreiung) kennen, um arbeitsorganisatorische Maßnahmen treffen zu können. Auch die Kenntnis von künftigen urlaubsbedingten Abwesenheiten ist aus organisatorischen Gründen sinnvoll, ebenso wie die Kenntnis von etwaigem Resturlaub. Zu weitgehend erscheint mir aber ein jederzeitiges, anlassloses Einsichtsrecht in die „Kommt- und Geht-Buchungen" der Beschäftigten oder Abwesenheitszeiten in der Vergangenheit. Derartige Kenntnisse über die Abwesenheiten in der Vergangenheit benötigt die Personalverwaltung, nicht hingegen die oder der Fachvorgesetzte. Auch die Übertragung von Resturlaub ist keine Angelegenheit, an der die oder der jeweilige Fachvorgesetzte ein unmittelbares dienstliches Interesse hat, sofern sie oder er nicht weitergehende personalverwaltende Funktionen wahrnimmt.

Schließlich ergab sich die Möglichkeit des **Datenzugriffs durch Sachgebiets-/Abteilungsleitungen auch auf Beschäftigte in nachgeordneten Arbeitsbereichen**. Insoweit hatten die Arbeitsbereichsleitungen die Funktion als Arbeitszeitbeauftragte bereits inne, sodass zusätzliche entsprechende Verarbeitungsbefugnisse der Sachgebiets- oder Abteilungsleitungen neben die Befugnisse der Arbeitsbereichsleitungen als Arbeitszeitbeauftragte getreten wären. Dies hätte die personellen Zugriffsmöglichkeiten stark erweitert und war mit der engen personellen Begrenzung des Art. 103 Satz 2 BayBG nicht zu vereinbaren. Die Verfolgung von Verstößen gegen arbeitszeitrechtliche Vorschriften ist keine Aufgabe der Fachvorgesetzten, sondern der Personalverwaltung. Insofern arbeitet diese mit gegebenenfalls bestehenden Arbeitszeitbeauftragten zusammen.

Die Landrätin oder der Landrat als **Dienstvorgesetzte oder Dienstvorgesetzter** der Kreisbeamtinnen und Kreisbeamten (vgl. Art. 38 Abs. 3 Satz 1 Landkreisordnung) hat nur, soweit dies im Einzelfall erforderlich ist, den vollen Zugriff auf die Personalakte und Personalaktendaten. Im Hinblick auf den gesetzlich vorgegebenen strengen Schutz von Personalaktendaten war die Möglichkeit eines ständigen Zugriffsrechts der konkreten Amtsinhaberin oder des konkreten Amtsinhabers auf das bei der Zeiterfassung anfallende Datenmaterial kritisch zu betrachten. Zwar kann sich eine Landrätin oder ein Landrat in der Wahrnehmung ihrer oder seiner Funktion als Dienstvorgesetzte oder Dienstvorgesetzter jederzeit anlassbezogen und im Einzelfall Zeiterfassungsdaten vorlegen lassen. In Bezug auf Zeiterfassungsdaten können weitergehende Zugriffsrechte jedoch nur bestehen, soweit der Landrätin oder dem Landrat als Dienststellenleitung mangels Delegation – etwa in Bezug auf unmittelbar zugeordnete Beschäftigte – die Überwachung der Arbeitszeiterfassung obliegt (vgl. Abschnitt 11 Nr. 1.7 VV-BeamtR).

8.5 Amtsärztliche Arbeitsfähigkeitsuntersuchungen bei Tarifbeschäftigten

Datenschutzrechtliche Fragen im Zusammenhang mit Untersuchungen der Dienstfähigkeit bayerischer Beamtinnen und Beamter haben mich bereits wiederholt beschäftigt, vgl. etwa den Beitrag Nr. 9.3 in meinem 29. Tätigkeitsbericht 2019, den Beitrag Nr. 11.4 in meinem 25. Tätigkeitsbericht 2012 oder den Beitrag Nr. 16.3.3 in meinem 21. Tätigkeitsbericht 2004.

Im Berichtszeitraum habe ich mich anlässlich einer Beschwerde vertieft mit dem Datenschutz bei **amtsärztlichen Untersuchungen der Arbeitsfähigkeit** Tarifbeschäftigter befasst. Dabei ging es um die Frage, auf welcher Rechtsgrundlage und in welchem Umfang ein Gesundheitsamt dem beauftragenden Arbeitgeber Untersuchungsergebnisse mitteilen darf. Was den Mitteilungsumfang betraf, trug die Praxis den rechtlichen Vorgaben jedenfalls im konkreten Fall nicht hinreichend Rechnung.

8.5.1 Ausgangspunkt

Verschiedene, im Wesentlichen gleichlautende tarifvertragliche Regelungen sehen vor, dass Arbeitgeber Tarifbeschäftigte unter gewissen Voraussetzungen dazu verpflichten können, einen **Nachweis** über ihre **Arbeitsfähigkeit** zu erbringen. Der Nachweis hat dabei in Form einer entsprechenden **ärztlichen Bescheinigung** zu erfolgen. Mit der vorangehenden Untersuchung können **unter anderem Amtsärzte** beauftragt werden (vgl. nur § 3 Abs. 5 Sätze 1 und 2 Tarifvertrag für den öffentlichen Dienst der Länder – TV-L; § 3 Abs. 4 Sätze 1 und 2 Tarifvertrag für den öffentlichen Dienst – TVöD).

§ 3 TV-L
Allgemeine Arbeitsbedingungen
(5) [1]Der Arbeitgeber ist bei begründeter Veranlassung berechtigt, Beschäftigte zu verpflichten, durch ärztliche Bescheinigung nachzuweisen, dass sie zur Leistung der arbeitsvertraglich geschuldeten Tätigkeit in der Lage sind. [2]Bei dem beauftragten Arzt kann es sich um einen Betriebsarzt, Personalarzt oder Amtsarzt handeln, soweit sich die Betriebsparteien nicht auf einen anderen Arzt geeinigt haben. […]

§ 3 TVöD
Allgemeine Arbeitsbedingungen
(4) [1]Der Arbeitgeber ist bei begründeter Veranlassung berechtigt, die/den Beschäftigte/n zu verpflichten, durch ärztliche Bescheinigung nachzuweisen, dass sie/er zur Leistung der arbeitsvertraglich geschuldeten Tätigkeit in der Lage ist. [2]Bei der beauftragten Ärztin/dem beauftragten Arzt kann es sich um eine Betriebsärztin/einen Betriebsarzt handeln, soweit sich die Betriebsparteien nicht auf eine andere Ärztin/einen anderen Arzt geeinigt haben. […]

Für eine solche amtsärztliche Untersuchung sind gemäß Art. 3 Abs. 2 Gesundheitsdienst- und Verbraucherschutzgesetz (GDVG) grundsätzlich die unteren Behörden für Gesundheit, Veterinärwesen und Verbraucherschutz (Gesundheitsämter) zuständig. Das Ergebnis der Untersuchung wird meist in einem Gesundheitszeugnis festgehalten. Dieses Zeugnis ist für die personalverwaltende Stelle bestimmt, welche den Untersuchungsauftrag erteilt hat.

8.5.2 Mitteilung der Untersuchungsergebnisse an den Arbeitgeber

8.5.2.1 Rechtsgrundlage

Tarifrechtliche Regelungen wie etwa § 3 Abs. 5 TV-L verpflichten Beschäftigte (lediglich) dazu, ihre Arbeitsfähigkeit durch ärztliche Bescheinigung nachzuweisen. Ausgehend vom Wortlaut dieser Vorschriften ist es insoweit ausreichend, wenn die Amtsärztin oder der Amtsarzt nach Abschluss der Untersuchung das Gesundheitszeugnis dem betroffenen Beschäftigten oder der betroffenen Beschäftigten **aushändigt**. Der oder dem Beschäftigten obliegt es dann, das Gesundheitszeugnis ihrem oder seinem Arbeitgeber vorzulegen. Wohl aus Gründen der Verfahrensvereinfachung und -beschleunigung sind die Gesundheitszeugnisse in den von mir geprüften Fällen allerdings direkt vom Gesundheitsamt an den beauftragenden Arbeitgeber **übermittelt** worden.

Dies wirft die Frage nach einer entsprechenden **Übermittlungsbefugnis** der Gesundheitsämter in diesen Fällen auf. Dabei sind insbesondere die Vorgaben des Art. 30 GDVG zu beachten:

Art. 30 GDVG
Datenschutz, Geheimhaltungspflichten
(1) [1]Die Behörden für Gesundheit, Veterinärwesen und Verbraucherschutz dürfen Geheimnisse, die Amtsangehörigen in der Eigenschaft als Arzt, Tierarzt oder als andere gemäß § 203 Abs. 1 oder 3 des Strafgesetzbuchs (StGB) zur Wahrung des Berufsgeheimnisses verpflichtete Person
1. in Wahrnehmung der in Art. 13 und 14 genannten Aufgaben,
2. im Zusammenhang mit einer Untersuchung oder Begutachtung, der sich der Betroffene freiwillig unterzogen hat oder
3. bei einer Beratung von Tierhaltern
anvertraut oder sonst bekannt geworden sind, bei der Erfüllung einer anderen Aufgabe als der, bei deren Wahrnehmung die Erkenntnisse gewonnen wurden, nicht verarbeiten. [2]Ebenso dürfen die Behörden für Gesundheit, Veterinärwesen und Verbraucherschutz Geheimnisse, die den in Satz 1 genannten Personen außerhalb ihres dienstlichen Aufgabenbereichs anvertraut oder sonst bekannt geworden sind, bei der Erfüllung ihrer Aufgaben nicht verarbeiten. [3]Die Behörden für Gesundheit, Veterinärwesen und Verbraucherschutz dürfen Geheimnisse nach den Sätzen 1 und 2 nicht offenbaren oder an andere Teile der öffentlichen Stelle, deren Bestandteil die Behörde für Gesundheit, Veterinärwesen und Verbraucherschutz ist, übermitteln. […]
(2) [1]Abs. 1 gilt nicht, soweit
1. die Verarbeitung durch Rechtsvorschrift ausdrücklich zugelassen ist,
2. die betroffene Person in die Verarbeitung ausdrücklich eingewilligt hat.
[…]

Der Arbeitgeber kann die Untersuchung der Arbeitsfähigkeit einer oder eines Beschäftigten nicht erzwingen. Es handelt sich mithin um eine Untersuchung bzw. Begutachtung, der sich die betroffenen Beschäftigten im Sinne des Art. 30 Abs. 1 Satz 1 Nr. 2 GDVG freiwillig unterziehen.[68] Dies hat zur Folge, dass die Ergebnisse einer solchen Untersuchung dem besonderen **Geheimnisschutz** des Art. 30 GDVG unterliegen. Gesundheitsämter dürfen diese Untersuchungsergebnisse daher nur übermitteln, wenn eine **Rechtsvorschrift** dies **ausdrücklich zulässt** oder die betroffenen

[68] Vgl. hierzu die Gesetzesbegründung zur Vorgängernorm des Art. 30 GDVG, Landtags-Drucksache 10/8972, S. 14.

Personen zuvor in die Übermittlung **ausdrücklich eingewilligt** haben (Art. 30 Abs. 1 Satz 3 in Verbindung mit Abs. 2 Satz 1 GDVG).

Für Untersuchungen der Dienstfähigkeit bei Beamtinnen und Beamten normiert Art. 67 Abs. 1 Bayerisches Beamtengesetz (BayBG) unter gewissen Voraussetzungen eine ausdrückliche Übermittlungsbefugnis. Diese Vorschrift findet auf Tarifbeschäftigte jedoch keine Anwendung. Eine dem Art. 67 Abs. 1 BayBG vergleichbare Regelung für tarifrechtlich vorgesehene Arbeitsfähigkeitsuntersuchungen existiert nicht. Insbesondere bietet Art. 5 Abs. 1 Nr. 1 BayDSG in diesem Zusammenhang keine hinreichende ausdrückliche Rechtsgrundlage im Sinne des Art. 30 Abs. 2 Satz 1 Nr. 1 GDVG: Denn ein Rückgriff auf die generalklauselhaften Übermittlungstatbestände dieser Vorschrift würde den gesetzlich normierten besonderen Geheimnisschutz des Art. 30 Abs. 1 GDVG im Ergebnis leerlaufen lassen.

Die Übermittlung der Ergebnisse einer Arbeitsfähigkeitsuntersuchung durch die Gesundheitsämter an Arbeitgeber ist somit gemäß Art. 30 Abs. 2 Satz 1 Nr. 2 GDVG nur auf Grundlage einer zuvor erteilten **ausdrücklichen Einwilligung** der betroffenen Beschäftigten zulässig. Die Anforderungen an eine wirksame Einwilligung nach Art. 4 Nr. 11, Art. 7 und Art. 9 Abs. 2 Buchst. a DSGVO sind dabei zu beachten. Einen Verstoß gegen diese Vorgaben habe ich im konkreten Beschwerdefall nicht feststellen können.

8.5.2.2 Mitteilungsumfang

Klärungsbedarf bestand allerdings, was den Umfang der Mitteilung des Gesundheitsamtes an den Arbeitgeber angeht. In dem an mich herangetragenen Sachverhalt hatte das beauftragte Gesundheitsamt dem Arbeitgeber neben Feststellungen zur eingeschränkten Arbeitsfähigkeit der betroffenen Person auch die zugrunde liegende **„Funktionsstörung“** mitgeteilt. Gemeint sind damit recht abstrakte Angaben wie etwa „Störung des Bewegungsapparates“, „(chronische) seelische Störung“ oder „Störung aus dem psychiatrischen Formenkreis“. Nach Darstellung des Gesundheitsamtes war die Mitteilung der „Funktionsstörung“ an den Arbeitgeber unter Verwendung einer entsprechenden „Standard-Formulierung“ erfolgt. Es bestand daher Anlass zu der Annahme, dass die Weitergabe diesbezüglicher Angaben durch die Gesundheitsämter verbreitet praktiziert wird.

Zwar handelt es sich bei der Angabe einer „Funktionsstörung“ nicht um eine medizinische Diagnose im engeren Sinn. Gleichwohl stellt diese Angabe ein Gesundheitsdatum dar, welches im Regelfall zumindest abstrakt auf die „Art“ einer Erkrankung hinweist. Die Mitteilung einer „Funktionsstörung“ gegenüber einem Arbeitgeber muss daher ebenfalls durch eine Rechtsgrundlage gedeckt sein. Dies war in vorliegendem Zusammenhang allerdings nicht der Fall.

Auch bei Vorliegen einer ausdrücklichen Einwilligung der betroffenen Person in die Weitergabe der Ergebnisse einer Arbeitsfähigkeitsuntersuchung an den Arbeitgeber gilt der datenschutzrechtliche Erforderlichkeitsgrundsatz: Das Gesundheitsamt darf dem Arbeitgeber personenbezogene Daten nur mitteilen, wenn und soweit dies zur Erfüllung des jeweiligen Gutachtensauftrags **erforderlich** ist. Denn die gesetzliche Erhebungsbefugnis des Arbeitgebers ist durch den Maßstab des Erforderlichen begrenzt (vgl. Art. 103 Satz 1 BayBG in Verbindung mit Art. 145 Abs. 2 BayBG).

Der zulässige Rahmen eines Begutachtungsauftrags ergibt sich aus den jeweils **einschlägigen rechtlichen Bestimmungen**. Zumindest mittelbar **konkretisieren und**

begrenzen diese Bestimmungen zugleich **Inhalt und Umfang** der ärztlichen Begutachtung sowie der damit zusammenhängenden Datenverarbeitung durch das Gesundheitsamt; dies gilt insbesondere auch im Hinblick auf die Übermittlung von Ergebnissen der Begutachtung an den jeweiligen Auftraggeber. Die Einwilligung der betroffenen Person legitimiert in diesem Zusammenhang (allein) den Übermittlungsvorgang (siehe bereits oben); sie führt aber nicht dazu, dass die gesetzliche Erhebungsbefugnis des Arbeitgebers nach Art. 103 Satz 1 BayBG in Verbindung mit Art. 145 Abs. 2 BayBG über das zur Zweckerreichung Erforderliche hinaus „ausgeweitet" wird. Bezüglich der Untersuchung der Arbeitsfähigkeit Tarifbeschäftigter bedeutet das: Schon nach dem Wortlaut der einschlägigen Vorschriften (vgl. etwa § 3 Abs. 5 Satz 1 TV-L, § 3 Abs. 4 Satz 1 TVöD) sind betroffene Beschäftigte (allein) dazu verpflichtet, durch eine ärztliche Bescheinigung nachzuweisen, dass sie zur Leistung der arbeitsvertraglich geschuldeten Tätigkeit in der Lage sind.

Erforderlich im Sinne von Art. 103 Satz 1 BayBG sind in einer entsprechenden Bescheinigung daher nur Angaben, die in **direktem Zusammenhang** mit der Frage der **Arbeitsfähigkeit** stehen. Dies betrifft etwa den Umfang der Arbeitsfähigkeit, gegebenenfalls auch präzisierende Ausführungen zu Tätigkeitsbereichen, in denen Arbeitsfähigkeit (nicht) besteht. Demgegenüber war für mich nicht erkennbar, weshalb in einer solchen ärztlichen Bescheinigung darüber hinausgehende Informationen zu einer vorhandenen Erkrankung (sei es auch nur durch die abstrakte Angabe einer „Funktionsstörung") notwendig sein sollten.[69]

Aufgrund der Aussage des Gesundheitsamtes, im Hinblick auf die „Funktionsstörung" auf eine „Standard-Formulierung" zurückgegriffen zu haben, hatte ich Grund zu der Annahme, dass die Regelungssystematik nicht allen Gesundheitsämtern hinreichend deutlich geworden ist. Daher habe ich das Bayerische Staatsministerium für Gesundheit und Pflege gebeten, den Gesundheitsämtern die dargestellte Rechtslage noch einmal zu verdeutlichen. Das Gesundheitsministerium ist meiner Bitte zwischenzeitlich nachgekommen.

8.5.3 Fazit

Tarifbeschäftigte haben unter gewissen Voraussetzungen einen Nachweis über ihre Arbeitsfähigkeit zu erbringen. Eine Übermittlung der Untersuchungsergebnisse durch die Gesundheitsämter an Arbeitgeber ist nur zulässig, wenn die betroffenen Beschäftigten zuvor ausdrücklich hierin eingewilligt haben. Im Hinblick auf den zulässigen Mitteilungsumfang gilt der datenschutzrechtliche Erforderlichkeitsgrundsatz: Mitgeteilt werden dürfen daher nur Angaben, die in direktem Zusammenhang mit der Frage der Arbeitsfähigkeit stehen. Auf die Mitteilung einer Diagnose oder auch (nur) einer „Funktionsstörung" trifft dies allerdings nicht zu – eine solche Angabe hat daher in einem Gesundheitszeugnis zur Arbeitsfähigkeit zu unterbleiben.

8.6 Bewerbungsunterlagen im Ratsinformationssystem

Im Berichtszeitraum hat mich eine Gemeinde gefragt, ob sie den Gemeinderatsmitgliedern zur Sitzungsvorbereitung im Rahmen von Bewerbungsverfahren den Zugriff

[69] Vgl. hierzu auch Landesarbeitsgericht Berlin-Brandenburg, Urteil vom 24. August 2012, 6 Sa 568/12, BeckRS 2012, 75192, Nr. 3.2.1.2.2.1.

auf Bewerbungsunterlagen durch Einstellen in das elektronische Ratsinformationssystem ermöglichen darf.

Die Zulässigkeit einer solchen Datenverarbeitung richtet sich nach Art. 103 Satz 1 Bayerisches Beamtengesetz (BayBG), der gemäß Art. 145 Abs. 2 BayBG auch auf die nicht-verbeamteten Beschäftigten des bayerischen öffentlichen Dienstes im Grundsatz entsprechend anzuwenden ist. Gemäß Art. 103 Satz 1 Nr. 1 BayBG darf der Dienstherr personenbezogene Daten über Bewerber und Bewerberinnen sowie aktive und ehemalige Beamte und Beamtinnen verarbeiten, soweit dies zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere zu Zwecken der Personalverwaltung oder Personalwirtschaft erforderlich ist. Soweit die Entscheidung über die Einstellung einer Bewerberin oder eines Bewerbers gemäß Art. 43 Abs. 1 Gemeindeordnung (GO) in der Zuständigkeit des Gemeinderats liegt, kann eine Information seiner Mitglieder über die Bewerbungen vom Grundsatz her auf Art. 103 BayBG – gegebenenfalls in Verbindung mit Art. 145 Abs. 2 BayBG – gestützt werden.

Dies bedeutet allerdings nicht, dass beliebig Bewerbungsdaten bekannt gegeben werden dürfen. Maßgebend ist insoweit das Kriterium der „Erforderlichkeit". Für die Beurteilung der Erforderlichkeit im Einzelfall ist dabei entscheidend, dass es sich bei Personalangelegenheiten um besonders sensible – und daher auch von Gesetzes wegen grundsätzlich in nicht-öffentlicher Sitzung zu behandelnde – Beratungsgegenstände handelt (vgl. Art. 52 Abs. 2 GO). Datenverarbeitungen sind entsprechend dem Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 Buchst. c DSGVO auf das zur Erreichung des konkreten Verarbeitungszwecks notwendige Maß zu begrenzen.

In Übereinstimmung mit dem Bayerischen Staatsministerium des Innern, für Sport und Integration vertrete ich die Auffassung, dass Sitzungsunterlagen zu derartigen Tagesordnungspunkten nicht mit der Tagesordnung versandt werden dürfen. Aus Datenschutzsicht ist es in Personalangelegenheiten vielmehr regelmäßig angezeigt, erforderliche Unterlagen lediglich für die Dauer der Sitzung als – möglichst nummerierte – Tischvorlagen zur Verfügung zu stellen und anschließend wieder einzusammeln. Zur Aufgabenerfüllung des Gemeinderats ist es demgegenüber nicht erforderlich, dass dessen Mitglieder Sitzungsunterlagen über Personalangelegenheiten – etwa postalisch oder elektronisch – schon zusammen mit der Tagesordnung erhalten. Hier besteht die Gefahr, dass in den Sitzungsunterlagen enthaltene vertrauliche Informationen unbefugt an Dritte gelangen oder weitergegeben werden können (vgl. meinen 21. Tätigkeitsbericht 2004 unter Nr. 16.2 am Ende). Zur Frage des Akteneinsichtsrechts des Gemeinderats und seiner Mitglieder habe ich mich an anderer Stelle ausführlich geäußert.[70]

Da die Einführung von Bewerbungsunterlagen in die Gemeinderatssitzung „auf analogem Wege" allenfalls im Rahmen temporärer Tischvorlagen in Betracht kommt, scheidet schon aus diesem Grund die Einstellung in ein elektronisches Ratsinformationssystem aus. Probleme ergäben sich hier insbesondere auch dadurch, dass die Unterlagen heruntergeladen und offline verwendet werden könnten, so dass die Gefahr der Reproduzierbarkeit und unbefugter Zugriffe gegeben wäre, die durch die Beschränkung auf Tischvorlagen minimiert wird. Die Begrenzung der Datenverarbeitung auf das zu Zwecken der Personalverwaltung oder Personalwirtschaft Erforderli-

[70] Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz für bayerische Gemeinderatsmitglieder, 2020, Frage 16, Internet: https://www.datenschutz-bayern.de, Rubrik „Broschürenbestellung".

che gemäß Art. 103 Satz 1 Nr. 1 BayBG könnte mit der Datenbereitstellung im elektronischen Ratsinformationssystem nicht sichergestellt werden. Der Gemeinderat ist vielmehr angehalten, seine Aufgaben ohne überschießende Datenverarbeitung zu erfüllen. Im Rahmen einer Güterabwägung ist das Interesse der betroffenen Person an der vertraulichen Behandlung ihrer sensiblen Daten dem Interesse des Gemeinderats an einer Verfahrensvereinfachung vorzuziehen.

Insoweit halte ich es für nicht erforderlich im Sinne von Art. 103 Satz 1 BayBG, zur Sitzungsvorbereitung von Gemeinderatsmitgliedern Bewerbungsunterlagen in das elektronische Ratsinformationssystem einzustellen.

8.7 Kontodatenabgleich bei örtlicher Rechnungsprüfung

Ein Landratsamt erkundigte sich im Berichtszeitraum bei mir nach der rechtlichen Bewertung eines geplanten anonymisierten Abgleichs, der zwischen Bankkontodaten von bestimmten Landkreisbeschäftigten und den Bankkontodaten der Empfängerinnen und Empfänger von Sozialleistungen durchgeführt werden sollte. Mit dem Datenabgleich wollte der Rechnungsprüfungsausschuss des Kreistags herausfinden, ob sich Landkreisbeschäftigte auf Kosten der öffentlichen Hand ungerechtfertigt bereicherten.

Soweit Organe der Rechnungsprüfung des Landkreises gemäß Art. 89 Abs. 1 Landkreisordnung (LKrO) personenbezogene Daten erheben, können sie sich grundsätzlich auf Art. 92 Abs. 6 Satz 1 LKrO als Rechtsgrundlage stützen. Art. 92 Abs. 6 Satz 1 LKrO steht allerdings unter dem Vorbehalt des Verhältnismäßigkeitsgrundsatzes, so dass nur solche Unterlagen vorgelegt werden dürfen, die das Organ der Rechnungsprüfung zur Erfüllung seiner Aufgaben für erforderlich hält. Zur Parallelvorschrift in Art. 106 Abs. 6 Satz 1 Gemeindeordnung (GO) habe ich mich bereits in meinem 28. Tätigkeitsbericht 2018 unter Nr. 12.5 geäußert.

Auch reine Bankkontodaten von Landkreisbeschäftigten sowie Empfängerinnen und Empfängern von Sozialleistungen habe ich in dem vorgelegten Fall als personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO gewertet, selbst wenn der Rechnungsprüfungsausschuss diese zunächst ohne Namen und Anschriften der betroffenen Personen verarbeiten wollte. Die Bankkontodaten der eigenen Beschäftigten waren für den Landkreis jedenfalls personenbeziehbar, weil ihm im Rahmen der Personalverwaltung die für eine Zuordnung erforderlichen Informationen zur Verfügung standen. Im Fall eines konkreten Missbrauchsverdachts war eine Zuordnung sogar von vornherein geplant.

Zu beachten war außerdem, dass Bankkontodaten von Landkreisbeschäftigten notwendiger Bestandteil ihrer Personalakten sind, vgl. § 50 Satz 2 Beamtenstatusgesetz (BeamtStG). Für die Verarbeitung von Personalaktendaten bestimmt Art. 103 Satz 3 Bayerisches Beamtengesetz (BayBG), dass diese auch zu Zwecken der Rechnungsprüfung verarbeitet werden dürfen. Auf vertraglich Beschäftigte im öffentlichen Dienst sind § 50 BeamtStG und Art. 103 BayBG gemäß Art. 145 Abs. 2 BayBG im Grundsatz entsprechend anwendbar. Ebenso wie im Rahmen von Art. 92 Abs. 6 LKrO muss aber auch eine auf Art. 103 Satz 3 BayBG gestützte Datenverarbeitung verhältnismäßig sein.

Im Einzelnen war ein Abgleich der Bankkontodaten von allen mit der Bewilligung von Sozialleistungen beauftragten Beschäftigten des Landkreises mit den Bankkontodaten der Empfängerinnen und Empfänger von Sozialleistungen ohne konkreten Anlass

geplant. Dazu sollten offenbar erhebliche Datenmengen in einem automatisierten Abgleich verarbeitet werden, um Übereinstimmungen auszufiltern. Damit sollte ein Verfahren eingesetzt werden, das **einer Rasterfahndung vergleichbar** ist.

Derartige Datenverarbeitungen sind aufgrund der Reichweite und der Intensität des Grundrechtseingriffs jedoch nur in sehr engen Grenzen und nur aufgrund einer ausreichend bestimmten, klar gefassten gesetzlichen Rechtsgrundlage möglich, vgl. etwa § 98a Strafprozeßordnung (StPO). Dabei kann ein Richtervorbehalt zu beachten sein (vgl. § 98b Abs. 1 Satz 1 StPO).

Soweit die anfragende Stelle die Verarbeitung der personenbezogenen Daten (auch) auf Art. 4 Abs. 1 BayDSG stützen wollte, habe ich ausgeführt, dass Art. 4 Abs. 1 BayDSG als allgemeine, nicht bereichsspezifische Verarbeitungsbefugnis allenfalls Eingriffe von geringer bis mittlerer Eingriffstiefe legitimieren kann. Sie sieht schon auf der Rechtsfolgenseite nicht einen automatisierten Abgleich von Bankdaten vor; auf der Tatbestandsseite fehlen zudem Merkmale, welche eine hinreichende Begrenzungswirkung entfalten könnten. Die Vorschrift erreicht daher letztlich nicht das im Zusammenhang mit der beabsichtigten Maßnahme erforderliche Maß an Normbestimmtheit. Derart spezifische Grundrechtseingriffe auf allgemeine, funktionell unbestimmte Verarbeitungsbefugnisse zu stützen, wäre angesichts der Reichweite und Eingriffsintensität verfassungsrechtlich nicht zulässig. Nach den verfassungsgerichtlichen Vorgaben sind vielmehr Anlass, Zweck und Grenzen des Rechtseingriffs entsprechend dem Grundsatz der Normenbestimmtheit und Normenklarheit bereichsspezifisch, präzise und normenklar festzulegen, so dass die gesetzesausführende Verwaltung für ihr Verhalten steuernde und begrenzende Handlungsmaßstäbe vorfindet.[71]

Art. 92 Abs. 6 Satz 1 LKrO kann demgegenüber lediglich eine Anforderung von Informationen – bei personenbezogenen Daten: eine Datenerhebung – rechtfertigen. Eine Befugnis zum Datenabgleich ist nicht eingeräumt. Art. 103 Satz 3 BayBG schließlich ist ein Zweckänderungstatbestand, der im Zusammenspiel mit einer Verarbeitungsbefugnis auch eine zweckändernde Verarbeitung gestattet. Die Vorschrift hilft aber nicht weiter, wenn es bereits an einer (hinreichend bestimmten) Verarbeitungsbefugnis fehlt.

Ein Datenabgleich kann somit äußerstenfalls in einem Einzelfall in Betracht kommen, wenn eine bestimmte Person – etwa aufgrund einer Stichprobenuntersuchung – konkret verdächtig ist und der Abgleich einer Klärung des Verdachts dienen soll. Ich habe dem Landratsamt daher geraten, von den Planungen eines umfassenden elektronischen Kontodatenabgleichs im Rahmen der örtlichen Rechnungsprüfung abzusehen. Mangels ausreichender Rechtsgrundlage verstößt eine derartige Datenverarbeitung gegen den Grundsatz der Rechtmäßigkeit gemäß Art. 5 Abs. 1 Buchst. a DSGVO. Das Landratsamt ist meinem Rat im Ergebnis gefolgt und hat den ursprünglich geplanten Kontodatenabgleich letztlich nicht vorgenommen.

8.8 Gleichstellungsbeauftragte: Einsicht in Bewerbungsunterlagen und Teilnahme an Vorstellungsgesprächen

Zur Erfüllung ihrer gesetzlich zugewiesenen Aufgaben sind Gleichstellungsbeauftragte vielfach auf Informationen ihrer jeweiligen Dienststelle angewiesen. Weisen

[71] Vgl. etwa zur Anforderung bei der Videoüberwachung Bundesverfassungsgericht, Beschluss vom 23. Februar 2007, 1 BvR 2368/06, BeckRS 2007, 22066.

solche Informationen einen Personenbezug auf, können die Informationsbedürfnisse der Gleichstellungsbeauftragten mit den Grundrechten betroffener Personen auf Datenschutz (Art. 8 Charta der Grundrechte der Europäischen Union) und informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz) in Konflikt geraten. Bestehen und Reichweite von Informationsrechten der Gleichstellungsbeauftragten haben mich in der Vergangenheit daher bereits mehrfach beschäftigt.

Anlässlich einer entsprechenden Beratungsanfrage hatte ich erneut Gelegenheit, mich zu dieser Thematik zu äußern. Gegenstand der Betrachtung war dabei zum einen ein etwaiges Einsichtsrecht der Gleichstellungsbeauftragten in Bewerbungsunterlagen, zum anderen die Teilnahme von Gleichstellungsbeauftragten an Vorstellungsgesprächen.

8.8.1 Einsichtsrecht in Bewerbungsunterlagen

Mit Einsichtsrechten von Gleichstellungsbeauftragten in Bewerbungsunterlagen, Bewerberlisten und Personalakten habe ich mich bereits im Beitrag Nr. 12.3 meines 19. Tätigkeitsberichts 2000 befasst. Dabei bin ich zu dem Ergebnis gekommen, dass Gleichstellungsbeauftragte nur dann Einsicht in Bewerbungsunterlagen nehmen dürfen, wenn ihre Beteiligung in Personalangelegenheiten gesetzlich vorgesehen ist. Dies setzt nach Art. 18 Abs. 3 Satz 2 Bayerisches Gleichstellungsgesetz (BayGlG) entweder einen **entsprechenden Antrag der betroffenen Personen oder der Gleichstellungsbeauftragten** voraus; im letztgenannten Fall müssen Gleichstellungsbeauftrage allerdings hinreichende Anhaltspunkte dafür vortragen, dass die Ziele des Bayerischen Gleichstellungsgesetzes nicht beachtet werden.

An dieser Rechtsauffassung halte ich auch nach Geltungsbeginn der Datenschutz-Grundverordnung fest, da sich die maßgeblichen gesetzlichen Vorgaben nicht wesentlich geändert haben. Bei meiner Bewertung habe ich die einschlägigen Regelungen im Bayerischen Personalvertretungsgesetz (BayPVG) vergleichend in den Blick genommen – die Frage eines Einsichtsrechts in Bewerbungsunterlagen stellt sich nämlich auch für Personalräte.

Im Einzelnen:

Wie weit Informationsrechte von Gleichstellungsbeauftragten reichen (können), bemisst sich anhand einer Abwägung. In diese einzustellen sind die legitimen Informationsbedürfnisse der Gleichstellungsbeauftragten einerseits und die Grundrechte betroffener Personen auf Datenschutz und informationelle Selbstbestimmung andererseits. Vorzunehmen hat diese Abwägung im Rahmen vorhandener Regelungsspielräume zunächst der bayerische Gesetzgeber. Für die vorliegende Konstellation hat er dies in Art. 18 Abs. 2 und 3 BayGlG getan. Dort heißt es:

„(2) [1]Die Gleichstellungsbeauftragten sind zur Durchführung ihrer Aufgaben rechtzeitig und umfassend zu unterrichten, bei Personalangelegenheiten spätestens gleichzeitig mit der Einleitung eines personalvertretungsrechtlichen Beteiligungsverfahrens. [2]Die hierfür erforderlichen Unterlagen sind frühzeitig vorzulegen und die erbetenen Auskünfte zu erteilen.
(3) [1]Die Gleichstellungsbeauftragten sind frühzeitig an wichtigen gleichstellungsrelevanten Vorhaben zu beteiligen. [2]Eine Beteiligung in Personalangelegenheiten findet auf Antrag der Betroffenen statt; die Gleichstellungsbeauftragten sind auf Antrag ferner zu beteiligen, wenn sie hinreichende Anhaltspunkte dafür vortragen, daß die Ziele

dieses Gesetzes nicht beachtet werden. [3]Eine Beteiligung an Vorstellungsgesprächen findet nur auf Antrag der Betroffenen statt. [4]Die Personalakten dürfen nur mit Zustimmung der Betroffenen eingesehen werden."

Art. 18 Abs. 2 BayGlG knüpft das Unterrichtungsrecht der Gleichstellungsbeauftragten an deren Aufgabendurchführung (Art. 18 Abs. 2 Satz 1 BayGlG) und begrenzt es zugleich durch das Kriterium der Erforderlichkeit (Art. 18 Abs. 2 Satz 2 BayGlG). Die Vorschrift entspricht insoweit Art. 69 Abs. 2 Sätze 1 und 2 BayPVG.

Die Aufgaben der Gleichstellungsbeauftragten ergeben sich allgemein aus Art. 17 BayGlG:

„(1) [1]Die Gleichstellungsbeauftragten fördern und überwachen den Vollzug dieses Gesetzes und des Gleichstellungskonzepts und unterstützen dessen Umsetzung. [2]Die Gleichstellungsbeauftragten fördern zusätzlich mit eigenen Initiativen die Durchführung dieses Gesetzes und die Verbesserung der Situation von Frauen sowie die Vereinbarkeit von Familie und Erwerbstätigkeit für Frauen und Männer.
(2) Die Gleichstellungsbeauftragten wirken im Rahmen ihrer Zuständigkeit an allen Angelegenheiten des Geschäftsbereichs mit, die grundsätzliche Bedeutung für die Gleichstellung von Frauen und Männern, die Vereinbarkeit von Familie und Erwerbstätigkeit und die Sicherung der Chancengleichheit haben können.
(3) [1]Zu den Aufgaben der Gleichstellungsbeauftragten gehört auch die Beratung zu Gleichstellungsfragen und Unterstützung der Beschäftigten in Einzelfällen. [2]Die Beschäftigten können sich unmittelbar an die Gleichstellungsbeauftragten wenden."

Gleichstellungsbeauftragte sind allerdings – ebenso wie Personalräte – kein allgemeines Kontrollorgan der jeweiligen Dienststelle. Ein **Informationsanspruch** setzt daher in der Regel einen **konkreten Aufgabenbezug** voraus. Ein solcher kann sich insbesondere aus einem einschlägigen **Beteiligungstatbestand** ergeben. In diesem Fall sind Gleichstellungsbeauftragte in einem Umfang zu unterrichten, der ihnen die ordnungsgemäße Ausübung ihres Beteiligungsrechts ermöglicht.

Einstellungen zählen zu den „Personalangelegenheiten" (vgl. Art. 75 Abs. 1 Satz 1 Nr. 1 BayPVG); diese umfassen insbesondere verschiedene personelle Einzelmaßnahmen (vgl. den diesbezüglichen Katalog in Art. 75 Abs. 1 Satz 1 BayPVG). Die Datenschutz-Grundrechte betroffener Personen sind bei der Bearbeitung von einzelfallbezogenen Personalangelegenheiten in einem besonderen Maße berührt, da hierbei sehr spezifische, vielfach auch sensible Daten der betroffenen Personen verarbeitet werden.

Der Gesetzgeber hat daher zu entscheiden, ob und gegebenenfalls welchen Stellen er in diesem Zusammenhang Beteiligungsrechte einräumt.

Personalräte haben gemäß Art. 75 Abs. 1 BayPVG umfangreiche Beteiligungsrechte in Personalangelegenheiten. Zu deren Wahrnehmung sind sie rechtzeitig und umfassend – auch durch die Vorlage erforderlicher Unterlagen – zu unterrichten (Art. 69 Abs. 2 Sätze 1 und 2 BayPVG). Im Unterschied zum Bayerischen Gleichstellungsgesetz enthält das Bayerische Personalvertretungsgesetz mit Art. 69 Abs. 2 Satz 3 BayPVG sogar eine Regelung, die sich unter anderem bei der Personalangelegenheit „Einstellung" ausdrücklich auf die Vorlage von Bewerbungsunterlagen bezieht. Art. 69 Abs. 2 BayPVG lautet:

„(2) [1]Der Personalrat ist zur Durchführung seiner Aufgaben rechtzeitig und umfassend zu unterrichten. [2]Ihm sind die hierfür erforderlichen Unterlagen zur Verfügung zu

stellen. [3]Bei einer Einstellung, Beförderung und Übertragung der Dienstaufgaben eines anderen Amtes mit höherem Endgrundgehalt oder höherer Amtszulage für eine Dauer von mehr als sechs Monaten kann der Personalrat auch die zur Erfüllung seiner Aufgaben erforderliche Vorlage von Bewerbungsunterlagen verlangen. […]"

In der Gesetzesbegründung zum jetzigen Art. 69 Abs. 2 Satz 3 BayPVG hat der Gesetzgeber in diesem Zusammenhang klargestellt, dass bei einem (für Personalräte nur ausnahmsweisen) Ausschluss des Mitbestimmungsrechts (folgerichtig) auch eine Vorlegungs- bzw. Unterrichtungsverpflichtung ausgeschlossen ist, weil es insoweit „bereits an einer konkreten Aufgabe des Personalrats fehlt".[72]

Die **Beteiligungsrechte der Gleichstellungsbeauftragten bei Personalangelegenheiten** sind gegenüber denjenigen der Personalräte allerdings **deutlich eingeschränkt**: Sie bestehen nur, wenn die betroffene Person es beantragt (Art. 18 Abs. 3 Satz 2 Halbsatz 1 BayGlG) oder wenn der oder die Gleichstellungsbeauftragte einen „qualifizierten" Antrag stellt (Art. 18 Abs. 3 Satz 2 Halbsatz 2 BayGlG). Nur in diesen Fällen kann für Gleichstellungsbeauftragte in der Personalangelegenheit „Einstellung" ein korrespondierendes Einsichtsrecht in Bewerbungsunterlagen auf Grundlage von Art. 18 Abs. 2 Sätze 1 und 2 BayGlG bestehen. Art. 18 Abs. 2 Satz 1 Halbsatz 2 BayGlG trifft in diesem Zusammenhang (lediglich) Vorgaben zum Zeitpunkt der Information.[73]

8.8.2 Teilnahme an Vorstellungsgesprächen

Die Frage, unter welchen Voraussetzungen den Gleichstellungsbeauftragten ein Recht auf Teilnahme an Vorstellungsgesprächen zusteht, lässt sich dagegen recht schnell beantworten:

Gemäß Art. 18 Abs. 3 Satz 3 BayGlG setzt die Beteiligung von Gleichstellungsbeauftragten an Vorstellungsgesprächen einen entsprechenden **Antrag der betroffenen Personen** voraus.

Ein **generelles Teilnahmerecht** der Gleichstellungsbeauftragten an Vorstellungsgesprächen ist im Bayerischen Gleichstellungsgesetz hingegen **nicht vorgesehen**.

8.8.3 Fazit

Gleichstellungsberechtigte dürfen nach derzeitiger Rechtslage nur dann Einsicht in Bewerbungsunterlagen nehmen, wenn betroffene Personen dies beantragen oder die Gleichstellungsbeauftragten einen „qualifizierten" Antrag stellen.

Die Teilnahme an Vorstellungsgesprächen setzt zwingend einen entsprechenden Antrag betroffener Personen voraus.

72 Vgl. Landtags-Drucksache 15/6238, S. 11.

73 Vgl. die Gesetzesbegründung zu dieser Vorschrift, Landtags-Drucksache 15/4735, S. 9.

9 Schulen und Hochschulen

9.1 Datenschutz bei den SARS-CoV-2 Testungen in Schulen

Auch im Schulbereich war das Jahr 2021 stark von der COVID-19-Pandemie und den daraus resultierenden Herausforderungen geprägt. Während der Infektionswellen im vorangegangenen Berichtszeitraum standen aus schuldatenschutzrechtlicher Sicht neben Fragen rund um die Befreiung von der Pflicht zum Tragen einer Mund-Nasen-Bedeckung (siehe hierzu den Beitrag Nr. 1.1.4) insbesondere die Durchführung und Gestaltung des Distanzunterrichts im Vordergrund (siehe hierzu auch die Ausführungen in meinem 30. Tätigkeitsbericht 2020 unter Nr. 10.1.2). Im Berichtszeitraum verfolgte die Bayerische Staatsregierung zunehmend den **Ansatz**, den **Präsenzunterricht** in den Schulen bei Wahrung der Sicherheit und Gesundheit aller Angehörigen der Schulfamilie möglichst lange auch unter den Bedingungen eines dynamischen Infektionsgeschehens **zu gewährleisten**. Eine **zentrale Maßnahme** bildete dabei eine **regelmäßige und kontinuierliche Testung** der Lehrkräfte, des sonstigen schulischen Personals sowie der Schülerinnen und Schüler. Diese politische und schulfachliche Grundentscheidung war auch bei der Anwendung des Datenschutzrechtes in der Schule zu berücksichtigen. Im Berichtszeitraum erreichten mich, insbesondere als zunächst eine grundsätzliche Testobliegenheit sowie später der PCR-Pooltest als neues Testverfahren eingeführt wurden, eine **Vielzahl von Beschwerden und Zuschriften Erziehungsberechtigter**, die im Hinblick auf den Schutz der personenbezogenen Daten ihrer Kinder besorgt waren. Die an mich herangetragenen Fragestellungen habe ich – neben einigen Einzelkonstellationen, deren Darstellung den Rahmen dieses Berichts sprengen würde – im Wesentlichen so beantwortet, wie ich nachfolgend zusammengefasst habe.

9.1.1 SARS-CoV-2-Selbsttestungen in Schulen

Im Laufe des Berichtszeitraums kamen an den bayerischen öffentlichen Schulen regelmäßig Corona-Selbsttests zum Einsatz. Diese Tests führten Schülerinnen und Schüler unter Aufsicht einer Lehrkraft durch.

Die in Zuschriften an mich geäußerten Datenschutzbedenken zu diesem Verfahren konnte ich zwar nachvollziehen, weil so regelmäßig Mitschülerinnen und Mitschüler von einem positiven Testergebnis erfahren. Gleichwohl führte dies nicht dazu, dass eine Datenverarbeitung unzulässig war.

9.1.1.1 Rechtsgrundlage zur Datenverarbeitung

Nach Art. 6 Abs. 1 DSGVO darf auch eine Schule personenbezogene Daten der Schülerinnen und Schüler nur aufgrund einer Rechtsgrundlage verarbeiten. Dies gilt auch dann, wenn Schulen im Rahmen einer Testobliegenheit für den Präsenzunterricht personenbezogene Daten verarbeiten, wie etwa ein negatives Ergebnis eines PCR- oder PoC-Antigentests oder das Testergebnis des in der Schule unter Aufsicht durchgeführten Selbsttests. Auch Gesundheitsdaten dürfen aufgrund von gesetzlichen Rechtsgrundlagen verarbeitet werden (vgl. Art. 9 Abs. 2 Buchst. g oder i DSGVO).

Der Gesetzgeber hat in den im Berichtszeitraum erlassenen Bayerischen Infektionsschutzmaßnahmenverordnungen die rechtlichen Voraussetzungen für eine Datenverarbeitung durch die Schulen geschaffen. Hierzu habe ich das Bayerische Staatsministerium für Unterricht und Kultus teils sehr kurzfristig datenschutzrechtlich beraten.

Zwar wurden die Bestimmungen der Bayerischen Infektionsschutzmaßnahmenverordnungen kontinuierlich fortgeschrieben und in Details geändert. Jedoch lassen sich die **zentralen normativen Vorgaben zu den Selbsttests** in der Schule während des Berichtszeitraums wie folgt beschreiben:

„Die Teilnahme am Präsenzunterricht, an sonstigen Schulveranstaltungen oder schulischen Ferienkursen in Präsenz sowie an der Mittags- und Notbetreuung ist Schülerinnen und Schülern nur erlaubt, wenn sie drei Mal wöchentlich einen in der jeweiligen Bayerischen Infektionsschutzmaßnahmenverordnung näher geregelten Testnachweis (PCR-Test, PoC-PCR-Test, PoC-Antigentest) erbringen oder in der Schule unter Aufsicht einen über die Schule zur Verfügung gestellten und dort zu verwendenden Selbsttest mit negativem Ergebnis vorgenommen haben.
Die Schule verarbeitet das Testergebnis für die Zwecke der Aufrechterhaltung des Präsenzunterrichts. Eine Übermittlung von Testdaten an Dritte findet im Übrigen vorbehaltlich von Meldepflichten nach dem Infektionsschutzgesetz nicht statt. Das Testergebnis wird höchstens 14 Tage aufbewahrt.“ [74]

Die Schulen konnten sich somit auf die gesetzliche Befugnis zur Datenverarbeitung nach Art. 85 Abs. 1 Satz 1 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG) in Verbindung mit dieser Regelung der jeweils geltenden Bayerischen Infektionsschutzmaßnahmenverordnung berufen.

Beim **Selbsttest im Klassenverband** konnten Schülerinnen und Schüler bemerken, wenn bei einer oder einem anderen ein positives Testergebnis vorlag. In diesem Fall sollte sich die betroffene Person sofort absondern, und der Schulbesuch durfte nicht weiter fortgesetzt werden. Spätestens bei Abholung einer positiv getesteten Schülerin oder eines positiv getesteten Schülers durch einen Erziehungsberechtigten erfuhren die übrigen Schülerinnen und Schüler faktisch das Testergebnis.

Selbst wenn man in dieser eben geschilderten Möglichkeit der Kenntnisnahme nicht nur einen faktischen Umstand sieht, sondern rechtlich eine Datenverarbeitung der Schule, so war sie durch die gesetzliche Befugnis im Grundsatz nach Art. 85 Abs. 1 Satz 1 BayEUG in Verbindung mit der oben genannten Regelung der jeweiligen Bayerischen Infektionsschutzmaßnahmenverordnung gedeckt.

Soweit eine gesetzliche Befugnis die Datenverarbeitung – wie hier – erlaubt, ist die Einholung einer Einwilligung der betroffenen Personen nicht erforderlich.

9.1.1.2 Speicherung der Testergebnisse der Selbsttests

Abgesehen von der eben erwähnten zeitlichen Vorgabe zur Speicherung der Testergebnisse für **höchstens 14 Tage** machten die Bayerischen Infektionsschutzmaßnahmenverordnungen keine weiteren Vorgaben zur Aufbewahrung der Testergebnisse. Insofern gelten die allgemeinen Vorgaben des Datenschutzrechts. Nach dem Grund-

[74] Vgl. etwa § 12 Abs. 2 15. BayIfSMV vom 23. November 2021 (BayMBl. Nr. 816). Die dortigen Normverweise wurden im Zitat paraphrasiert.

satz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 Buchst. f DSGVO) müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

Nach Art. 32 Abs. 1 DSGVO trifft der Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen **geeignete technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Sachgerechte Lösungen waren vor dem Hintergrund dieser Vorgaben an den Schulen vor Ort zu entwickeln. Hierbei sollte die oder der behördliche Datenschutzbeauftragte eingebunden werden. Neben der Aufbewahrung der Dokumentation der Testergebnisse im Schultresor kam auch eine Ablage der Informationen zum Beispiel in einem verschließbaren Aktenschrank an einem allgemein nicht beliebig zugänglichen beziehungsweise absperrbaren Ort, etwa dem Sekretariat oder dem Büro der Schulleitung, in Betracht.

9.1.1.3 Alternative: externe PCR- oder PoC-Antigentests

In diesem Zusammenhang ist noch hervorzuheben, dass die oben dargestellten Regelungen der Bayerischen Infektionsschutzmaßnahmenverordnungen als **Alternative zum Selbsttest in der Schule** die Möglichkeit boten, ein aktuelles negatives Ergebnis eines außerhalb der Schule durchgeführten PCR- oder PoC-Antigentests vorzuweisen. Somit konnte jeder, der keinen Selbsttest in der Schule im Klassenverband durchführen wollte, selbst **außerhalb der Schule einen PCR- oder PoC-Test durchführen lassen** und dessen aktuelles (negatives) Ergebnis in der Schule vorweisen, um den Präsenzunterricht besuchen zu können. Das Ergebnis war von der Schule in geeigneter Weise zu dokumentieren (zum Beispiel durch einen Aktenvermerk). Die Aufbewahrung des Originals oder einer Kopie des PCR- oder PoC-Testergebnisses, etwa in der Schülerakte, war jedoch nicht erforderlich und somit datenschutzrechtlich grundsätzlich nicht zulässig (Art. 5 Abs. 1 Buchst. e DSGVO).

9.1.2 PCR-Pooltests an Grund- und Förderschulen

9.1.2.1 Testverfahren

Im Schuljahr 2021/22 wurden in den Jahrgangsstufen 1 bis 4 sowie an Förderschulen mit den Schwerpunkten geistige Entwicklung, körperliche und motorische Entwicklung sowie Sehen die Corona-Selbsttests in den Schulen grundsätzlich durch das PCR-Pooltestverfahren abgelöst. Bei einem PCR-Pooltest werden Speichelproben von mehreren Personen gemeinsam in einer Gesamtprobe (dem „Pool“) untersucht. Dies geschieht, indem die Schülerinnen und Schüler für 30 Sekunden an einem Abstrichtupfer lutschen (wie an einem Lolli). Alle Abstrichtupfer einer Klasse kommen gemeinsam in einen Behälter. Es entsteht eine anonyme Sammelprobe. Im Anschluss werden die Speichelproben in ein Labor transportiert und mithilfe des PCR-Verfahrens ausgewertet. Zusätzlich zur Poolprobe wird noch eine Einzelprobe genommen. Diese wird ausschließlich dann ausgewertet, wenn der Pooltest positiv ausfällt. In die-

sem Fall kann schnell ermittelt werden, welches Kind betroffen ist. Ist der Pooltest negativ, werden die Proben entsorgt. **Auch zu den PCR-Pooltests** erreichten mich **viele Anfragen und allgemeine Beschwerden.** Insbesondere wurde dabei die **Freiwilligkeit eingeholter datenschutzrechtlicher Einwilligungen** und die Übermittlung der anonymisierten Daten von den Laboren an das Institut für Medizinische Informationsverarbeitung Biometrie und Epidemiologie (IBE) an der Ludwig-Maximilians-Universität München (LMU) thematisiert.

9.1.2.2 Wissenschaftliche Begleitstudie

Das Kultusministerium hat auf seiner Webseite[75] weitergehende umfangreiche Informationen insbesondere zum Testverfahren, zur Ergebnisübermittlung an die Erziehungsberechtigten, zur Einwilligungserklärung und zum Datenschutz sowie **zur wissenschaftlichen Begleitstudie** veröffentlicht. Danach werde die Speichelprobe der Schülerinnen und Schüler selbst nicht an die Forschungsgruppe weitergegeben. Das Forschungsinstitut erhalte nur die Auswertungsergebnisse der Poolproben und gegebenenfalls der Einzelproben. Diese Daten würden vollständig anonymisiert an das Forschungsinstitut weitergegeben, eine Rückverfolgung hin zu den Poolteilnehmerinnen und Poolteilnehmern sei dem IBE oder der LMU nicht möglich. Es werde somit nicht – wie in einigen an mich herangetragenen Anfragen und Beschwerden befürchtet wurde – mit der DNA der Schülerinnen und Schüler geforscht.

9.1.2.3 Rechtsgrundlage zur Datenverarbeitung

Die Teilnahme an zwei wöchentlichen PCR-Pooltests, die nun an die Stelle der Selbsttestungen treten konnte, war – ebenso wie die Teilnahme an den vorstehend bereits beschriebenen Selbsttests – für die Schülerinnen und Schüler freiwillig. Schülerinnen und Schülern, die nicht am PCR-Pooltest teilnehmen wollten, blieb auch hier die Möglichkeit, den geforderten negativen Testnachweis alternativ durch die Vorlage externer PCR- oder PoC-Antigentests zu erbringen. Diese Tests waren für die betroffenen Schülerinnen und Schüler kostenlos (§ 4a Coronavirus-Testverordnung – TestV).

Die Verarbeitung der personenbezogenen Daten der Schülerinnen und Schüler bei der Teilnahme an den PCR-Pooltests wurde, auch im Hinblick auf die Beteiligung von Laboren, auf **eingeholte datenschutzrechtliche Einwilligungen** der betroffenen Schülerinnen und Schüler beziehungsweise der Erziehungsberechtigten gestützt. Die **Freiwilligkeit** dieser Einwilligungen habe ich wegen der verbleibenden alternativen Nachweismöglichkeiten grundsätzlich als **gewährleistet** angesehen. Bei der erfolgten Ausgestaltung habe ich im Berichtszeitraum somit **keinen Anlass zu aufsichtsrechtlichen Maßnahmen** gesehen.[76]

Gleichwohl werde ich auch das Verfahren der PCR-Pooltests im Rahmen meiner Aufsichtszuständigkeit für die Verarbeitung personenbezogener Daten durch bayerische öffentliche Stellen **weiter aufmerksam verfolgen**.

75 Internet: https://www.km.bayern.de/allgemein/meldung/7451/haeufig-gestellte-fragen-faq-zu-den-pooltests.html.

76 Siehe auch Bayerischer Verwaltungsgerichtshof, Beschluss vom 11. Oktober 2021, 25 NE 21.2525, BeckRS 2021, 30069, Rn. 14, 26, 30; Verwaltungsgericht Regensburg, Beschluss vom 21. Oktober 2021, RN 5 E 21.1961, BeckRS 2021, 32314, insbesondere Rn. 37.

9.1.3 Verarbeitung des Impf- oder Genesenenstatus

Mit zunehmendem Fortschritt der Impfkampagne und der Zulassung von Corona-Impfstoffen für jüngere Alterskohorten stellte sich auch die Frage, ob und wie die Schulen den Impf- oder Genesenenstatus der Schülerinnen und Schüler verarbeiten durften. Die hierzu im Berichtszeitraum eingegangenen **Anfragen und Beschwerden** habe ich auf Grundlage folgender Erwägungen beantwortet:

9.1.3.1 Status befreit von der Testobliegenheit

Die COVID-19-Schutzmaßnahmen-Ausnahmenverordnung stellte geimpfte Personen und genesene Personen mit negativ getesteten Personen gleich, wenn eine landesrechtliche Vorschrift vorgibt oder voraussetzt, dass eine Person negativ auf eine Infektion mit dem Coronavirus SARS-CoV-2 getestet ist. Somit konnten sich geimpfte oder genesene Schülerinnen und Schüler im Berichtszeitraum **von der Testobliegenheit beziehungsweise Nachweispflicht** eines negativen PCR- oder POC-Antigentests nach der oben genannten Regelung der jeweiligen Bayerischen Infektionsschutzmaßnahmenverordnung **befreien**, wenn sie der Schule ihren Impfstatus oder ihren Genesenenstatus offenbarten. Ohne entsprechend negative Testung oder einen gleichgestellten Status konnte der Präsenzunterricht nicht besucht werden.

9.1.3.2 Rechtsgrundlage zur Datenverarbeitung

Bayerische öffentliche Schulen konnten im Berichtszeitraum nach Art. 85 Abs. 1 Satz 1 BayEUG in Verbindung mit der oben genannten Regelung der jeweiligen Bayerischen Infektionsschutzmaßnahmenverordnung und der COVID-19-Schutzmaßnahmen-Ausnahmenverordnung die Daten von Schülerinnen und Schülern verarbeiten, die erforderlich waren, um die bestehende Ausnahme vom Erfordernis eines negativen Testnachweises aufgrund des Status „geimpft“ oder „genesen“ festzustellen. Auch wenn es sich um Gesundheitsdaten handelte, konnten sie aufgrund von gesetzlichen Rechtsgrundlagen verarbeitet werden (vgl. Art. 9 Abs. 2 Buchst. g oder i DSGVO). Eine Einwilligung war nicht notwendig.

Aufgrund der Beschulung im **Klassenverband** war eine Kenntnisnahme des Status der anderen Schülerinnen und Schüler bereits durch die Abläufe nicht vermeidbar und insoweit auch von der gesetzlichen Regelung mitumfasst. Wer im Klassenverband nicht an der Testung teilnahm und auch keinen Testnachweis vorlegte, jedoch den Unterricht besuchte, war für die Mitschülerinnen und Mitschüler regelmäßig bereits dadurch als „geimpft“ oder „genesen“ erkennbar.

Datenschutzrechtlich war auch nichts dagegen einzuwenden, wenn die Schule **Einsicht in den Nachweis des Impf- oder Genesenenstatus** nahm und hierüber einen Aktenvermerk zwecks **Dokumentation des Status** in Bezug auf die Befreiung von der Testpflicht nach den Bayerischen Infektionsschutzmaßnahmenverordnungen anfertigte. Dies konnte etwa auch in Form der Führung einer Klassenliste (mit entsprechenden Markierungen zum Namen) geschehen. Eine solche Liste durfte aus Datenschutzsicht freilich nicht allgemein offen einsehbar sein.

9.1.3.3 Freiwillige Offenbarung des Impf- oder Genesenenstatus

Eine Auskunftspflicht der Schülerinnen und Schüler oder ihrer Erziehungsberechtigten über den Impf- oder Genesenenstatus gegenüber der Schule konnte ich allerdings nicht erkennen. Vielmehr erfolgte die Angabe des Impf- oder Genesenenstatus

freiwillig. Für die Befreiung von der Testobliegenheit nach der jeweiligen Bayerischen Infektionsschutzmaßnahmenverordnung war die (freiwillige) Offenbarung des Impf- oder Genesenenstatus gleichwohl die Bedingung.

Aus Datenschutzsicht konnten mit diesem Befund daher grundsätzlich auch keine Einwände dagegen erhoben werden, wenn die Schule die Erziehungsberechtigten oder die Schülerinnen und Schüler nach dem Nachweis eines Impf- oder Genesenenstatus **fragte**, um auf diese Weise festzustellen, ob eine Befreiung von der Testobliegenheit vorliegt. Selbstverständlich sollte die Schule dabei nicht den Eindruck erwecken, dass eine **Pflicht** zur Offenbarung des Impf- oder Genesenenstatus bestehe. Den Schulen war daher zu empfehlen, die Erziehungsberechtigten vorab entsprechend zu informieren.

9.2 Elektronische Fernprüfungen und alternative Präsenzprüfungen bei Hochschulen

In meinem 30. Tätigkeitsbericht 2020 habe ich unter Nr. 10.1.4 über die Einführung von Regelungen für die Durchführung von elektronischen Fernprüfungen durch Hochschulen und meine diesbezügliche Beratung des zuständigen Bayerischen Staatsministeriums für Wissenschaft und Kunst berichtet. Auch im Jahr 2021 führten Hochschulen elektronische Fernprüfungen durch. Dies brachte es mit sich, dass einzelne Studierende **Beschwerden** bei mir eingereicht haben. Die Prüfung dieser Beschwerden gestaltet sich anspruchsvoll. Denn zum einen waren anzuwendende Gesetze, insbesondere die Bayerische Fernprüfungserprobungsverordnung (BayFEV), für alle Beteiligten neu. Hierzu bestehende Rechtsfragen müssen also erstmals geklärt werden. Zum anderen waren auch die Sachverhalte und die dadurch aufgeworfenen datenschutzrechtlichen Probleme teilweise komplex. **Eine** der von mir durchgeführten Untersuchungen einer elektronischen Fernprüfung und einer alternativen Präsenzprüfung an einer Hochschule **greife ich im Folgenden heraus**.

9.2.1 Sachverhalt

Eine Hochschule führte eine **Prüfung unter Einsatz einer speziellen Prüfungssoftware** durch. Die Prüfung konnte auf zwei Arten absolviert werden: **zum einen als elektronische Fernprüfung und zum anderen als Präsenzprüfung im Hörsaal.** Bei der Präsenzprüfung gab es zwar eine Aufsicht vor Ort. Gleichwohl fand auch die Prüfung im Hörsaal auf dem eigenen Rechner des jeweiligen Prüflings statt. **Sowohl für die Fern- als auch für die Präsenzprüfung** installierten die Prüflinge die **Prüfungssoftware** auf ihrem jeweils eigenen Rechner. Dabei konnten **mittels dieser Software dort jedenfalls folgende Verarbeitungen durch die Hochschule vorgenommen werden**:

- **Verifizieren der technischen Funktionalitäten des Prüfungsrechners**, das heißt die Software prüft die korrekte Funktionalität, bevor die Prüfung beginnt;
- **Aufnahme-Werkzeuge** (Bildschirm-Aufzeichnung, Nachweis der Aktivitäten auf dem Bildschirm des Prüflings; Webtraffic [Erkennen von angesteuerten Internet-Seiten]);
- **Sperr-Funktionalitäten** (Full-Screen-Modus, nur 1 Bildschirm, zusätzliche Browser-Tabs verhindern, offene Tabs schließen, Drucken deaktivieren, Zwischenablage deaktivieren, Downloads verhindern, Cache [Zwischenspeicher]

leeren, Rechtsklick der Computermaus verhindern, Wiedereintritt in die Prüfung ermöglichen).

Bei der elektronischen Fernprüfung kamen zu diesen Verarbeitungsvorgängen **noch weitere** hinzu (Verifizierung von Video und Audio, Identifizierung des Prüflings sowie Videoaufnahme des Prüflings und Audioaufnahme des Prüfungsraumes zum Nachweis von Gesprächen).

9.2.2 Rechtliche Bewertung

Aufgrund meiner Prüfung stellte ich mehrere **Datenschutzverstöße der Hochschule** fest. Diese betrafen den Einsatz der Software **bei der Präsenzprüfung** im Hörsaal **sowie bei der elektronischen Fernprüfung**. So konnte ich für einen Teil der dabei veranlassten Datenverarbeitungen keine Rechtsgrundlage nach der Bayerische Fernprüfungserprobungsverordnung erkennen, die Vorgaben der Bayerischen Fernprüfungserprobungsverordnung wurden überschritten oder die Hochschule hat deren Einhaltung bislang nicht nachgewiesen. Daneben wurden mehrere Mängel bei der Erfüllung der Informationspflichten nach Art. 13 DSGVO sowie der Gestaltung des vorgelegten Vertrags zur Auftragsverarbeitung (Art. 28 Abs. 3 DSGVO) offenbar. Auch gegenüber der Hochschule habe ich betont, dass eine umfassende und abschließende Prüfung des Einsatzes dieser Software durch die Hochschule mit meiner Untersuchung nicht verbunden war.

Die umfassende Darstellung der Datenschutzmängel würde den Rahmen dieses Berichts sprengen. Meine **nachfolgenden Erläuterungen beschränke ich** daher **auf** die zur **elektronischen Präsenzprüfung** festgestellten Defizite. Diese lagen darin begründet, dass **keine Befugnis** der Hochschule **für die Datenverarbeitung auf den Rechnern der Prüfungsteilnehmerinnen und Prüfungsteilnehmer in der Präsenzprüfung** bestand.

9.2.2.1 § 4 Abs. 1 Satz 1 BayFEV

Zwar erlaubt § 4 Abs. 1 Satz 1 BayFEV, dass die Hochschulen im Rahmen elektronischer Fernprüfungen personenbezogene Daten verarbeiten, soweit dies zur ordnungsgemäßen Durchführung der Prüfung zwingend erforderlich ist. In § 4 Abs. 4 BayFEV heißt es konkretisierend weiterhin:

„Bei elektronischen Fernprüfungen sind Lernmanagementsysteme, Prüfungsplattformen, Videokonferenzsysteme und andere technische Hilfsmittel so zu verwenden, dass notwendige Installationen auf den elektronischen Kommunikationseinrichtungen der Studierenden nur unter den folgenden Voraussetzungen erfolgen:

1. Die Funktionsfähigkeit der elektronischen Kommunikationseinrichtung wird außerhalb der Prüfung nicht und währenddessen nur in dem zur Sicherstellung der Authentifizierung sowie der Unterbindung von Täuschungshandlungen notwendigen Maße beeinträchtigt,

[…]“

§ 4 Abs. 4 Nr. 1 BayFEV setzt den Einsatz technischer Hilfsmittel auf elektronischen Kommunikationseinrichtungen der Studierenden voraus; die Vorschrift kann im Zusammenspiel mit § 4 Abs. 1 Satz 1 BayFEV als Befugnis der Hochschulen verstanden werden, zur Sicherstellung der Authentifizierung sowie der Unterbindung von Täuschungshandlungen notwendige Installationen auf den Kommunikationseinrichtungen der Studierenden vorzuschreiben.

Die **Vorschrift findet** allerdings ausdrücklich **nur auf Prüfungen Anwendung, die als elektronische Fernprüfungen durchgeführt werden**. Als solche bestimmt § 1 Abs. 1 Satz 2 BayFEV Prüfungen, die ihrer Natur nach dafür geeignet sind, in elektronischer Form und ohne die Verpflichtung, persönlich in einem vorgegebenen Prüfungsraum anwesend sein zu müssen, durchgeführt werden. Die von der Hochschule alternativ angebotene und durchgeführte Präsenzprüfung im Sinne von § 8 Abs. 1 Satz 2 BayFEV stellte jedoch gerade keine solche elektronische Fernprüfung dar. Dies gilt auch dann, wenn diese nicht schriftlich, also auf Papier, sondern elektronisch auf einem PC oder Laptop abgenommen wird.

Mit anderen Worten: Für Eingriffe in die Datenverarbeitung auf Rechnern der Prüflinge, die diese **bei der Präsenzprüfung** im Hörsaal als Prüfungsmittel mitbringen, stellt § 4 BayFEV **keine Grundlage** dar.

9.2.2.2 Studienordnung

Auch der Studienordnung der Hochschule für das betroffene Studienfach war **keine Rechtsgrundlage für diese Datenverarbeitungen** zu entnehmen. Es wäre im Übrigen mit Blick auf die verfassungsrechtliche Wesentlichkeitstheorie auch sehr zweifelhaft, ob die Hochschulen überhaupt über die Befugnis verfügen, in Studienordnungen Rechtsgrundlagen für diese Datenverarbeitung zu schaffen (siehe hierzu bereits meinen 30. Tätigkeitsbericht 2020 unter Nr. 10.1.4). Diese verfassungsrechtliche Frage brauchte hier allerdings nicht weiter vertieft werden, da die in Rede stehende Studienordnung keine spezifisch datenschutzrechtliche Regelung, insbesondere keine datenschutzrechtliche Verarbeitungsbefugnis, enthielt.

9.2.2.3 Einwilligung

Zwar hatte die Hochschule zudem auch Einwilligungserklärungen der Prüfungsteilnehmerinnen und Prüfungsteilnehmer eingeholt. Diese waren nach dem Ergebnis meiner datenschutzrechtlichen Überprüfung jedoch **unwirksam**.

Nach der gesetzlichen Konzeption der Bayerischen Fernprüfungserprobungsverordnung soll die Präsenzprüfung nach § 8 Abs. 1 Satz 2, Abs. 2 BayFEV als „analoge" Alternative für die elektronische Fernprüfung verbleiben. Durch diese Alternative soll sichergestellt werden, dass die Absolvierung der elektronischen Fernprüfung für die Studierenden freiwillig ist (vgl. § 8 Abs. 1 Satz 1 BayFEV). Eine Alternative zur elektronischen Fernprüfung liegt jedoch nur dann vor, wenn sich die Präsenzprüfung von der elektronischen Fernprüfung – im Hinblick auf die betroffenen Grundrechte – deutlich unterscheidet. Diesem gesetzlichen Konzept widerspricht es jedoch, wenn die Hochschule die Präsenzprüfung durch die Einholung von Einwilligungen zu einer „halben" elektronischen Fernprüfung nach § 4 Abs. 4 und § 6 Abs. 4 BayFEV macht, indem sie mittels Software die Datenverarbeitung des privaten PCs des Studenten beeinflusst und blockiert und gegebenenfalls automatisiert überwacht (Bildschirm-Aufzeichnung, Webtraffic-Erkennen). Mit diesem Befund **verstieß die Einholung von Einwilligungen zu dieser Art der Datenverarbeitung** auf privaten Rechnern der Studierenden bereits **gegen das Konzept des § 8 Abs. 1 Satz 2, Abs. 2 BayFEV**.

Zugleich lag auch ein Verstoß gegen die **„Sperrwirkung" der gesetzlich geregelten Datenverarbeitungsbefugnisse** und den Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) vor. Soweit der Zweck und der Umfang der Datenverarbeitung nicht im gesetzlichen Aufgabenbereich der Hochschule liegen, das heißt

nicht von der Bayerischen Fernprüfungserprobungsverordnung gedeckt sind, scheidet auch eine flächendeckende allgemeine Verarbeitung auf der Grundlage einer Einwilligung (Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO in Verbindung mit Art. 4 Nr. 11 DSGVO und Art. 7 DSGVO) aus. Die Verarbeitung personenbezogener Daten auf Grundlage von Einwilligungen soll bei bayerischen öffentlichen Stellen (weiterhin) nur in Ausnahmefällen erfolgen. Sie stellt gerade kein Mittel dar, um den öffentlichen Stellen die Möglichkeit zu geben außerhalb ihres gesetzlich festgelegten Aufgabenbereiches tätig zu werden. Wurde die konkrete Datenverarbeitung bewusst aus Gründen der Datensparsamkeit nicht gesetzlich geregelt, verbietet sich mit dem Grundsatz der Datenminimierung nach Art. 5 Abs. 1 Buchst. c DSGVO regelmäßig ein Rückgriff auf eine Einwilligung.

Unabhängig davon, dass Einwilligungen hier aus den genannten Gründen von vornherein nicht als Rechtsgrundlage herangezogen werden konnten, konnte ich bei der konkreten Verfahrensweise auch nicht feststellen, dass die Einwilligungen von allen Betroffenen freiwillig erklärt und ausreichend informiert eingeholt worden sind.

9.2.2.4 Fortgang

Die von der Hochschule angeforderte Stellungnahme zu meinen Feststellungen sowie zu erfolgten Änderungen und Anpassungen im Falle eines beabsichtigten weiteren Einsatzes dieser Software habe ich zum Redaktionsschluss dieses Berichts noch nicht erhalten. Die Thematik werde ich jedenfalls weiter im Blick behalten.

Über meine Feststellungen gegenüber der Hochschule habe ich das Wissenschaftsministerium mit Blick auf die gesetzlich vorgesehene Evaluation durch das Wissenschaftsministerium spätestens zum Jahresende 2024 sowie den Bericht hierzu an den Landtag (Art. 61 Abs. 10 Satz 4 Bayerisches Hochschulgesetz) informiert. Zudem hat das Wissenschaftsministerium gemäß Art. 3 Abs. 1 BayDSG in seinem Bereich die rechtskonforme Ausführung der Datenschutzvorschriften sicherzustellen.

10 Technik und Organisation

10.1 COVID-19-Pandemie, Digitalisierung und Datenschutz

Immer wieder ist aus Politik und Medien zu hören, dass notwendige Digitalisierungen im Gesundheitswesen sowie die Nutzung von Datenbeständen zur Bekämpfung der COVID-19-Pandemie auf Grund des Datenschutzes nicht möglich seien. Zudem wird in diesem Zusammenhang nicht selten darauf verwiesen, dass andere Länder in Europa, wie etwa Spanien oder die skandinavischen Länder, bereits „viel weiter" seien. Schon dieser Hinweis widerlegt die grundsätzliche Kritik, dass zukunftsträchtige Projekte an strengen Datenschutzregeln scheitern: Denn auch in den als Vorbild genannten Ländern gilt die Datenschutz-Grundverordnung.

Gerade bei der Bekämpfung der COVID-19-Pandemie bietet die Digitalisierung große Chancen, die auch aus Datenschutzsicht genutzt werden sollten. Gleichwohl geben Beratungsanfragen aus Anlass einschlägiger Projekte mitunter Gelegenheit, auf eine datenschutzrechtliche Optimierung hinzuwirken. So begegnen mir neben datenschutzrechtlich offenkundig nicht tragfähigen Ansätzen auch immer wieder Projekte, die als Insellösungen ohne eine mir erkennbare Gesamtkonzeption und ohne gründliche Prüfung der Bedarfe sowie der Gegebenheiten vor Ort initiiert werden. In meiner Beratungs- und Prüfungspraxis zeigen sich insbesondere folgende Probleme, die eine übergreifende Digitalisierung im Gesundheitswesen in Deutschland vergleichsweise schwerer machen als in anderen europäischen Ländern:

– **Fehlende Nutzung von Synergien und Schnittstellen zum Datenaustausch**

  Im Gegensatz zu Ländern mit einer hoch zentralisierten Gesundheitsversorgung existiert in Deutschland, auch in Bayern, eine Vielzahl unterschiedlicher Träger für Krankenhäuser, Pflegeheime und andere Gesundheitseinrichtungen, die alle jeweils selbständig agieren und somit auch selbst über ihre IT-Ausstattung, Prozesse und Methoden der Datenverarbeitung entscheiden. Dies führt beispielsweise dazu, dass selbst bei Verwendung des gleichen Krankenhausinformationssystems in verschiedenen Krankenhäusern Unterschiede in der Auswahl der verwendeten Module, der Gestaltung der Arbeitsumgebung, der Prozesse und somit auch der gespeicherten Daten entstehen. Dies hat zur Folge, dass jedes Krankenhaus selbst Konzepte zur IT-Sicherheit, zum Berechtigungs- sowie Löschmanagement oder ähnlichen Rahmenbedingungen erstellen muss und in den meisten Fällen schon bayernweit über die gesetzlich vorgegebenen Abrechnungsformate hinaus keine einheitlichen Datenaustauschformate vorhanden sind. Dies erschwert es, die notwendigen Datensätze für die Forschung, statistische oder auch epidemiologische Auswertungen unkompliziert zur Verfügung zu stellen.

  Im Rahmen der Pandemiebekämpfung wurden zwar Meldepflichten – und damit verbunden elektronische Meldewege und Datenformate – für einzelne Informationen, etwa die Belegung der Intensivbetten oder die Anzahl der behandelten COVID-19 Fälle, festgelegt. Je länger die COVID-19-Pandemie andauert, zeigt sich jedoch, dass deutlich mehr Daten, wie beispielsweise zum

Impfstatus oder zum Gesundheitszustand für die Bewertung der Pandemielage, die Einladung zur Impfung oder für Forschungsfragen benötigt würden. Hierzu ist mir bisher kein Vorschlag für ein Gesamtkonzept bekannt geworden, das ich aus Datenschutzsicht hätte prüfen können. Es wäre aus meiner Sicht Aufgabe der Politik sowie der Selbstverwaltung im Gesundheitswesen, einheitliche Datenaustauschformate sowohl semantisch als auch technisch klar zu definieren, so dass diese von den Software-Anbietern und Krankenhäusern einheitlich und standardisiert umgesetzt werden können.

— **Fehlende Gesamtstrategie und Integration von Anwendungen zur digitalen Unterstützung der Pandemiebekämpfung**

Bereits in meinem 30. Tätigkeitsbericht 2020 unter Nr. 3.5 habe ich mich zur fehlenden einheitlichen technischen Basis hinsichtlich der Möglichkeit der sicheren elektronischen Kommunikation der an der Pandemiebekämpfung beteiligten Stellen geäußert.

Im Berichtszeitraum wurden zur IT-technischen Unterstützung der Pandemiebekämpfung zwar einzelne Lösungen wie SORMAS (siehe Nr. 10.2.1) oder Luca (siehe Nr. 10.2.4) eingeführt. Aber auch hier handelt es sich um punktuelle IT-Einzellösungen, ohne dass zuvor eine geeignete Gesamtkonzeption für die Digitalisierung der Gesamtabläufe deutschlandweit, zumindest aber bayernweit, erstellt worden wäre.

Die Praxis zeigt, dass sich sowohl bei der Einführung von SORMAS als auch von Luca in den Gesundheitsämtern gerade die Integration in die bestehenden Prozesse und IT-Systeme als schwierig erwies und auch vor der politischen Entscheidung zum verpflichtenden Einsatz nicht hinreichend getestet wurde. Die bayerischen Gesundheitsämter erhielten zwar von den Systemanbietern Unterstützung bei der Installation und Inbetriebnahme der Anwendungen selbst, jedoch blieb die Frage der Integration in bestehende Prozesse, Anwendungen und die IT-Landschaften den einzelnen Gesundheitsämtern selbst überlassen. Auch die von den Anbietern mitgelieferten Schnittstellen zwischen beiden Anwendungen erwiesen sich in der Praxis als nur schwer nutzbar. Wie sich herausstellte, wurde für den Export aus Luca und den anschließenden Import in SORMAS in der Praxis hauptsächlich die Microsoft Office-Anwendung Excel ohne ausreichende Sicherheitsmaßnahmen genutzt, so dass es Sicherheitsforscherinnen und Sicherheitsforschern gelang, bei dieser Schnittstelle Schadcode einzuschleusen.

Des Weiteren musste für den Datenabruf durch die Gesundheitsämter ein gesondertes, von Luca bereitgestelltes Portal genutzt werden, was für die Gesundheitsämter zu zusätzlichem Schulungsaufwand, zur Einrichtung einer gesonderten Benutzerverwaltung und zu weiteren Sicherheitsmaßnahmen geführt hat. Eine direkte Nutzung der Luca-Daten aus SORMAS heraus war nicht möglich.

Diese Beispiele unterstreichen die Wichtigkeit einer systematischen Gesamtkonzeption für die Digitalisierung von Abläufen. Denn nur so können Systembrüche, Doppelarbeiten aufgrund inkompatibler Einzelanwendungen sowie Sicherheitsprobleme vermieden werden. Derartige konzeptionelle Arbeiten können die einzelnen Gesundheitsämter in der Pandemiesituation nicht leisten. Die bestehenden Synergiepotenziale müssten daher genutzt und die notwendigen Konzepte auf Landes- oder Bundesebene erstellt werden.

– **Fehlende einheitliche technische Möglichkeiten zur Kommunikation mit Bürgerinnen und Bürgern**

  Wie unter Nr. 10.3 ausführlicher dargestellt, bestehen für die beteiligten Stellen und insbesondere die Gesundheitsämter nach wie vor große Schwierigkeiten, mit Bürgerinnen und Bürgern sicher und rechtzeitig elektronisch in Kontakt zu treten. Üblicherweise muss nach der mittlerweile in der Regel elektronisch erfolgenden „Erstmeldung" beispielsweise durch ein Labor, eine Teststation oder die digitale Einreiseanmeldung die weitere Abwicklung (zum Beispiel Vorlage von weiteren Dokumenten) in jedem Gesundheitsamt selbständig umgesetzt werden, da Luca und SORMAS die gesamten weiteren Kommunikationswege der „Contact Tracing Teams" nicht mit umfassen. Hier wären bayernweit einheitliche Lösungen, etwa auf Basis des schon bestehenden BayernPortals, wichtig, die jedoch nicht auf der Ebene der Gesundheitsämter konzipiert werden können.

Insgesamt ist festzuhalten, dass die Digitalisierung und die Akzeptanz digitaler Anwendungen sowohl im Rahmen der Pandemiebekämpfung als auch sonst nur dann erfolgreich sein werden, wenn hierfür systematische und plausible Gesamtkonzepte erstellt und diese flächendeckend und strukturiert umgesetzt werden. Es wäre wünschenswert, dass die auftraggebenden oder beschaffenden Stellen derartige Aspekte von Anfang an mit berücksichtigen. Denn so können die grundsätzlichen Auswirkungen auf die Datenschutzrechte betroffener Personen wie auch der Aufwand und der Nutzen für die einsetzenden Stellen von Anfang an die notwendige Beachtung finden. Doppelerfassungen, fehlende Schnittstellen und ineffiziente Prozesse könnten dadurch vermieden werden und sich nicht zu Datenschutzproblemen entwickeln. Die Geschwindigkeit bei der Einführung von Verfahren sollte gerade außerhalb kurzfristiger Handlungszwänge der Pandemiebekämpfung nicht das Hauptkriterium für die Beurteilung von neuen Anwendungen und IT-Systemen sowie die Entscheidungsfindung sein.

10.2 IT-Systeme zur Bewältigung der COVID-19-Pandemie

Auf Grund der COVID-19-Pandemie habe ich mich eingehend mit den datenschutzrechtlichen Grundlagen und den technisch-organisatorischen Maßnahmen der Kontaktnachverfolgung bei Infektionsgeschehen sowie dem Impfmanagement beschäftigt. Hierzu wurden im Berichtszeitraum bayernweit neue IT-Systeme für die Gesundheitsämter und Impfzentren eingeführt, die eine intensive Befassung aus Datenschutzsicht erforderlich machten. Solche Systeme verarbeiten Gesundheitsdaten, die nach Art. 9 DSGVO besonderen Schutz genießen (personenbezogene Speicherung von Quarantäne-Anordnungen, Test-Ergebnissen, Impfungen, Vorerkrankungen usw.). In den nächsten Abschnitten kommen zur Sprache:

– die Einführung von SORMAS (Surveillance Outbreak Response Management Analysis System) in allen bayerischen Gesundheitsämtern zur Kontaktverfolgung (siehe Nr. 10.2.1),

– BayIMCO (Bayerisches Impfmanagement gegen Corona) für die Impfzentren zum Impfmanagement und zur Impfanmeldung für die Bürgerinnen und Bürger (siehe Nr. 10.2.2) sowie

– die Luca-App zur elektronischen Kontaktdatenverfassung bei Veranstaltern zum Abruf durch die Gesundheitsämter (siehe Nr. 10.2.4).

Zudem war ich in die technische Bewertung von IT-Systemen auf Bundesebene eingebunden, so bei der Corona-Warn-App (CWA) oder dem digitalen Impfnachweis.

10.2.1 SORMAS

Um die Bearbeitung von COVID-19-Kontaktfällen in den Gesundheitsämtern zu unterstützen und zu vereinheitlichen, wurde im November 2020 von Bund und Ländern der bundesweite Einsatz des elektronischen Verfahrens SORMAS (Surveillance Outbreak Response Management Analysis System) beschlossen. Dies wurde von mir in Hinblick auf die bayerischen Gesundheitsämter ausführlich begleitet.

Ursprünglich wurde das Verfahren vom Robert-Koch-Institut (RKI), dem Helmholtz-Zentrum für Infektionsforschung (HZI) und weiteren Partnern für die Infektionsüberwachung und das Ausbruchsmanagement in den Schwellen-Ländern entwickelt. Eine erste Version kam bereits 2014 in Westafrika beim Ausbruch von Ebola und später 2017 in Nigeria bei Ausbruch der Affenpocken erfolgreich zum Einsatz. Bei diesen Epidemien konnten mit Hilfe des Verfahrens Infektionsherde sowie Infektionsüberträgerinnen und Infektionsüberträger frühzeitig und zeitnah verfolgt und dokumentiert werden. Mittlerweile befindet sich SORMAS weltweit im Einsatz.

Das HZI hat SORMAS speziell für den öffentlichen Gesundheitsdienst in Deutschland angepasst. Da sich SORMAS bereits in der Praxis bewährt hatte, wurde es als Basis gewählt, auf der aufbauend ein gemeinsames Verfahren bundesweit zur Kontaktnachverfolgung entstehen konnte. Bei SORMAS handelt sich jedoch nicht um ein Zentralsystem, bei dem alle Daten nur bei einer Stelle gespeichert werden; vielmehr ist eine dezentrale Datenspeicherung entweder bei den Gesundheitsämtern selbst oder beim Informationstechnikzentrum Bund (ITZBund, zentraler IT-Dienstleister für die deutsche Bundesverwaltung) als Dienstleister möglich. In einem solchen Fall wird für jedes Gesundheitsamt ein eigener Mandant angelegt.

Mit einem einheitlichen Verfahren kann auf den Einsatz unterschiedlicher proprietärer Eigenentwicklungen in den verschiedenen Bundesländern und Gesundheitsämtern verzichtet werden, die untereinander inkompatibel sind und dadurch zu Problemen beim Datenaustausch führen können. Zudem bringen lokale Einzelsysteme häufig Schwierigkeiten hinsichtlich der Datensicherheit mit sich, da bei proprietären Lösungen häufig eine umfassende Betrachtung hinsichtlich der IT-Sicherheit und der erforderlichen Maßnahmen unterbleibt. Für SORMAS wurde dagegen eine zentrale Datenschutz-Folgenabschätzung (DSFA) erstellt, die dem Bundesbeauftragen für den Datenschutz und die Informationsfreiheit und den Datenschutz-Aufsichtsbehörden der Länder zur Beurteilung vorlag.

Aus Datenschutzsicht traten während des schrittweisen Roll-Outs von SORMAS an den bayerischen Gesundheitsämtern insbesondere folgende Fragen auf:

— Die sogenannten Contact-Tracing-Teams (CTT) hatten bereits vor dem Einsatz von SORMAS überwiegend elektronische Verfahren genutzt. Ein wesentliches Werkzeug war hier neben Standard-Bürosoftware (vor allem Microsoft Office-Produkten) insbesondere das bayerische Online-Portal „BaySIM“ (Bayerisches System für Infektionskettenmanagement).

  Neben der Einführung von SORMAS stellte sich auch die Frage des Umgangs mit dem bereits vorhandenen Datenbestand. Die Daten wurden weiter benötigt; zugleich mussten Anforderungen an die Datensicherheit erfüllt werden.

Hierfür bietet SORMAS spezielle REST-Schnittstellen (Representational State Transfer) zum Datenimport, bei welchen allerdings noch Klärungsbedarf bzgl. der Umsetzung bestand.

Zudem besteht die Möglichkeit, ein digitales Symptom-Tagebuch für die betroffenen Kontaktpersonen anzubinden. Hierfür hat das Bundesministerium für Gesundheit in Zusammenarbeit mit der Firma Climedo Health GmbH unter Einbezug des RKI, des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit eine Lösung entwickelt. Auch hier war die Schnittstellenbeschreibung zunächst unvollständig.

Ebenso waren die Schnittstellendefinitionen zum Datenaustausch zwischen den Gesundheitsämtern sowie mit dem RKI nicht von Anfang an verfügbar, so dass aus Datenschutzsicht auch hier Klärungsbedarf bestand.

– Ein weiterer offener Punkt war die zum Einführungszeitpunkt von SORMAS noch unvollständige Datenschutz-Folgenabschätzung. Insbesondere das Risiko- und Zielerfüllungsmanagement entsprach noch nicht vollumfänglich den Anforderungen des Art. 35 DSGVO und musste entsprechend nachgebessert werden.

  Zudem ist bei zentral bereitgestellten Datenschutz-Folgenabschätzungen immer zu beachten, dass diese nicht die örtlichen Gegebenheiten und technisch-organisatorischen Maßnahmen umfassen können, da sich diese von Gesundheitsamt zu Gesundheitsamt unterscheiden. Die entsprechende Analyse der Risiken für die Rechte und Freiheiten der betroffenen Personen musste daher zusätzlich vor Ort durchgeführt werden.

– Schließlich mussten die weiteren von Seiten des HZI vorgelegten Unterlagen, etwa das Datenschutz- und Sicherheitskonzept sowie das Löschkonzept, im Hinblick auf die Vorgaben der Datenschutz-Grundverordnung angepasst werden.

  Beispielweise erweckten diese Unterlagen den Eindruck, dass eine automatisierte Löschung gewisser Daten nicht vorgesehen sein soll. Unter dem Blickwinkel des Grundsatzes der Speicherbegrenzung (Art. 5 Abs. 1 Buchst. e DSGVO) habe ich mich daher dafür eingesetzt, dass systemseitig Voreinstellungen für Löschfristen vorgesehen werden.

Zuletzt rückte SORMAS erneut in den Fokus, als in den Medien Schwachstellen der Software aufgedeckt wurden. Unter anderem seien anfänglich bei jeder Installation des Programms ungesicherte Standard-Test-Accounts angelegt worden, in deren Quellcode nicht änderbare Passwörter gespeichert worden wären. Solche Standard-Accounts mit statischen Passwörtern verstoßen gegen die in Art. 32 DSGVO geforderte Einhaltung der Sicherheit der Verarbeitung, insbesondere wird das in Erwägungsgrund 78 DSGVO als Konkretisierung für „geeignete technische und organisatorische Maßnahmen“ empfohlene Mittel der datenschutzfreundlichen Voreinstellung (data protection by default) unterwandert.

Mittlerweile hat das HZI die Konfiguration so geändert, dass keine Default-Logins mehr angelegt werden. Allerdings ändert dies nichts an der Problematik, die bei bereits bestehenden Installationen vorliegt.

Die deutschen Gesundheitsämter wären zudem nach Angaben des HZI von diesem Problem in der Regel gar nicht betroffen, wenn sie die vom Bundesministerium für Gesundheit ausgelieferte und beim ITZBund betriebene SORMAS-Instanz verwenden würden. Diese wird von einem Dienstleister zentral betrieben und verzichtet auf Standard-Accounts.

Da SORMAS nach wie vor weiterentwickelt wird, werde ich das Projekt auch weiterhin kritisch begleiten.

10.2.2 BayIMCO: Software für das Bayerische Impfmanagement

Einen Schwerpunkt sowohl hinsichtlich der technisch-organisatorischen Beratung bayerischer öffentlicher Stellen als auch bezüglich der Beschwerden von Bürgerinnen und Bürgern stellten im Berichtszeitraum die technischen und organisatorischen Maßnahmen rund um das Bayerische Impfmanagement dar.

Als Ende 2020 in den kreisfreien Städten und Landkreisen mit der Planung und Einrichtung von Impfzentren begonnen wurde, gab das Bayerische Staatsministerium für Gesundheit und Pflege die Entwicklung einer einheitlichen bayerischen Softwarelösung für die elektronische Impfanmeldung und die Impfverwaltung (BayIMCO) in Auftrag. Ich begrüße, dass mich das Gesundheitsministerium frühzeitig in die rechtliche wie auch technisch-organisatorische Beurteilung eingebunden und eine ausführliche Datenschutz-Folgenabschätzung vorgelegt hat. Das Gesundheitsministerium erstellte zudem frühzeitig ausführliche Datenschutzinformationen für die Bürgerinnen und Bürger; diese lagen mir rechtzeitig zur Prüfung vor.

Seit dem 11. November 2021 ist BayIMCO in allen bayerischen Impfzentren im Einsatz und somit auch das Portal zur Impfanmeldung (https://impfzentren.bayern) online. Teilweise schon zuvor vorhandene regionale Impfanmeldungssysteme sollten seit diesem Zeitpunkt deaktiviert sein.

Die Impfanmeldung und Impfabwicklung erfolgt aus Datenverarbeitungssicht in zwei Schritten: Beim Anlegen eines Accounts in BayIMCO werden zwar sowohl die Kontaktdaten als auch die Daten, die zur Ermittlung der Impfpriorität erforderlich sind (wie etwa Vorerkrankungen, Wohnsituation, berufliche Situation) erfasst, aber nur die Kontaktdaten tatsächlich gespeichert. Die übrigen zu diesem Zeitpunkt eingegebenen Daten werden aus Gründen der Datensparsamkeit noch nicht gespeichert, da es sich teilweise um Daten mit hohem Schutzbedarf handelt (insbesondere Gesundheitsdaten im Sinne von Art. 4 Nr. 15 DSGVO), die erst erforderlich sind, wenn tatsächlich eine Impfung erfolgt. Dies hat zur Folge, dass diese Daten im Zuge der späteren, konkreten Terminfestlegung noch einmal angegeben werden müssen.

Nach Abschluss beider Impfungen stehen die in BayIMCO gespeicherten Daten nicht mehr zum Abruf durch die Impfzentren zur Verfügung, sondern werden in ein Impfarchiv überführt, in dem die Daten bis zum Ende der Aufbewahrungspflicht für gesetzlich vorgegebene Zwecke (Haftung, Forschung) aufbewahrt werden. Dabei erfolgt eine Trennung zwischen den identifizierenden Daten der Impflinge und den sonstigen Impfdaten, so dass ein Zugriff mit Personenbezug nur unter Beteiligung einer gesonderten Vertrauensstelle nach einem festgelegten Verfahren möglich ist. Für Forschungszwecke darf ein derartiger Zugriff zur Ermöglichung einer anschließenden Kontaktaufnahme mit dem Impfling nur erfolgen, wenn dieser darin bei seiner Impf-

anmeldung eingewilligt hat. Das Impfarchiv ist organisatorisch dem Bayerischen Landesamt für Gesundheit und Lebensmittelsicherheit zugeordnet, der technische Betrieb liegt beim IT-Dienstleistungszentrum des Freistaats Bayern.

Zudem werden die Daten in pseudonymisierter Form in einer gesonderten Datenbank zum Zweck des Impfmonitorings gespeichert.

Abhängig von der Gesamtentwicklung der COVID-19-Pandemie ist auch zukünftig mit Erweiterungsbedarf bei BayIMCO zu rechnen. Beispielsweise mussten im Juni 2021 Ergänzungen vorgenommen werden, um eine Ausstellung digitaler Impfnachweise zu ermöglichen. Auch hier hat mich das Gesundheitsministerium frühzeitig eingebunden. Weiterer Änderungsbedarf könnte sich beispielsweise aus dem Wegfall der Impfpriorität oder den Erfordernissen weiterer Folgeimpfungen ergeben.

10.2.3 Beschwerden zu technischen Belangen des Bayerischen Impfmanagements

Im Berichtszeitraum sind eine Vielzahl von Beschwerden und Anfragen von Bürgerinnen und Bürgern zum Impfportal eingegangen. Konnten Mängel festgestellt werden, hat das Gesundheitsministerium stets eine rasche Anpassung veranlasst. Im technischen Bereich betrafen Beschwerden insbesondere die folgenden Themen:

10.2.3.1 Vermeintliches Hosting in einem unsicheren Drittstaat

Mehrere Beschwerden vertraten die Auffassung, dass BayIMCO in den Vereinigten Staaten von Amerika (USA) gehostet sei. So wurde der IP-Adresse von BayIMCO über die Geolokation die geographische Herkunft „USA“ bescheinigt. Die Datenschutzerklärung von BayIMCO gab allerdings ein Hosting in Deutschland an. Nicht nur dieser Widerspruch, sondern auch die Sorge um die Speicherung von Gesundheitsdaten in einem unsicheren Drittland begründeten die Beschwerden.

Eine von mir eingeholte Stellungnahme des Gesundheitsministeriums hebt hervor, dass personenbezogene Daten in BayIMCO niemals außerhalb Deutschlands gespeichert worden seien. Lediglich die IP-Range, zu der die verwendete IP-Adresse gehört, wurde in den USA erstanden. Inzwischen hat das Gesundheitsministerium veranlasst, dass die Geolokation den korrekten Standort des Rechenzentrums ausweist.

10.2.3.2 Einwilligung zur Weitergabe von Daten an Forschungsstellen

Im Rahmen der Anmeldung zur Impfung über BayIMCO wird die Einwilligung zur Weitergabe von Daten an Forschungseinrichtungen abgefragt. In einer frühen Software-Version wurde wohl nicht eindeutig auf die Freiwilligkeit dieser Einwilligung hingewiesen, so dass es zu Beschwerden beim Gesundheitsministerium kam.

Auch mir teilte ein Beschwerdeführer mit, dass bei der Impfanmeldung die Einwilligung in eine solche Weitergabe in Bezug auf Kontaktdaten bereits vorab ausgewählt war. Da der Petent diesen Umstand bei der Impfanmeldung erkannte, er seine Einwilligung jedoch nicht geben wollte, bat er im Impfzentrum um Entfernung der vorangekreuzten Einwilligung. Das Impfpersonal vor Ort konnte diese Vorauswahl aus technischen Gründen allerdings nicht aus dem Datensatz entfernen. Stattdessen wurde dem Impfwilligen mitgeteilt, dass eine Impfung ohne diese Einwilligung nicht möglich sei, er aber im Nachgang die Einwilligung widerrufen könne.

Die Einwilligung ist allerdings nur dann wirksam, wenn sie die Anforderungen aus Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 4 Nr. 11 und Art. 7 Abs. 2 und 3 DSGVO erfüllt. Insbesondere muss die Einwilligung freiwillig erteilt sein. Die Freiwilligkeit war in der konkreten Situation allerdings ausgeschlossen, da auf den Impfling mit der Aussage, sonst keine Impfung zu erhalten, Druck ausgeübt wurde.

In der Folge ließ das Gesundheitsministerium den Anmeldedialog anpassen und die Freiwilligkeit hinsichtlich der Erklärung einer Einwilligung deutlicher hervorheben. Ebenso wurde der Ausdruck des Impfbogens dahingehend verbessert, dass auch dort ein Hinweis zur Freiwilligkeit klar ersichtlich ist. So sollte nun allen Beteiligten verständlich sein, dass kein Zusammenhang zwischen dieser Einwilligung und der Durchführung der Impfung besteht.

10.2.4 Digitales Kontaktnachverfolgungssystem Luca

Für die Luca-App zur Kontaktnachverfolgung wurde Anfang des Jahres 2021 vom Freistaat Bayern eine Landeslizenz beschafft, die es privaten und öffentlichen Stellen in Bayern – insbesondere Veranstalterinnen und Veranstaltern sowie Gesundheitsämtern – ermöglicht, die App kostenlos einzusetzen. Damit sollte zum Ende des „Lockdowns“ im Mai 2021 die eigentlich begrüßenswerte Möglichkeit bestehen, die Kontaktverfolgung elektronisch, medienbruchfrei und insbesondere für die Gesundheitsämter leichter zugänglich durchzuführen. Neben den unter Nr. 10.1 dargestellten grundsätzlichen Problemen haben sich hierzu auch einige praktische Schwierigkeiten ergeben, die teilweise den Nutzen der von Luca erfassten Daten in Frage stellen:

— **Fehlende technische Detailprüfung, Sicherheitslücken**

Aufgrund des sehr kurz bemessenen zeitlichen Vorlaufs bei der Einführung von Luca und der Komplexität von App und Nutzungsszenario konnte weder von den Datenschutz-Aufsichtsbehörden noch von IT-Sicherheitsbehörden vor Einsatzbeginn eine detaillierte Prüfung hinsichtlich der IT-Sicherheit durchgeführt werden. Dies führte dazu, dass während des schon laufenden Betriebs Schwachstellen und Probleme entdeckt und mit großer Medienwirkung diskutiert wurden. Der Anbieter von Luca musste bezüglich der IT-Sicherheit mehrfach nachbessern. Auch Änderungsforderungen der Datenschutz-Aufsichtsbehörden im technischen Bereich konnten nicht vor dem Einsatz umgesetzt werden, sondern sind Ende 2021 immer noch in Bearbeitung. Die gewählte Herangehensweise führte letztendlich zu einem deutlichen Vertrauensverlust bei den Bürgerinnen und Bürgern, was die Nutzung von Luca betrifft.

— **Fragliche Brauchbarkeit der Daten**

Wie in meiner frühzeitig veröffentlichten Sonderinformation zu Luca[77] dargelegt, muss der Personenkreis beim Veranstalter möglichst so raum- und zeitbezogen erfasst werden, dass in Luca nur ansteckungsrelevante Personenkontakte verarbeitet werden. Hierzu sind beispielsweise an mehreren Stellen eines Veranstaltungsorts verschiedene QR-Codes erforderlich. Die Praxis zeigt jedoch, dass QR-Codes häufig mit zu großflächigem „Geltungsbereich“ angebracht werden, etwa für ganze Biergärten, große Restaurants oder Kantinen. Damit ist für das Gesundheitsamt nicht mehr ersichtlich, welche Personen

77 Internet: https://www.datenschutz-bayern.de/corona/sonderinformation-luca.html.

sich tatsächlich in infektionstauglicher Nähe befanden und somit als Kontaktpersonen gelten. Stattdessen liefert in diesen Fällen ein Datenabruf aus Luca eine große Anzahl vermeintlicher Kontakte, deren Verfolgung weder vom Aufwand noch vom Ertrag als angemessen erscheint.

— **Fehlende Planung des Maßnahmenendes**

Bereits bei der Konzeption und spätestens bei der Einführung neuer Systeme und Anwendungen zur digitalen Pandemiebekämpfung sollte geklärt sein, wie ein „Ausstieg" vonstattengehen soll. So wurde beispielsweise in der 14. Bayerischen Infektionsschutzmaßnahmenverordnung (14. BayIfSMV) mit Wirkung ab dem 15. Oktober 2021 die Pflicht zur Kontaktdatenerfassung auf Schwerpunktbereiche mit einem hohen Risiko von Mehrfachansteckungen, wie zum Beispiel große Veranstaltungen, beschränkt. Trotz dieser wesentlichen Änderung waren noch Ende November 2021 an einer Vielzahl von Stellen – sogar in einer staatseigenen Kantine – QR-Codes zur Luca-Kontaktdatenerfassung angebracht, verbunden mit Hinweisen an die Besucherinnen und Besucher, sich bei Luca zu registrieren. Hierdurch besteht das Risiko, dass auch weiterhin in großem Umfang Daten erhoben werden, die jedoch von den Gesundheitsämtern nicht mehr verarbeitet werden dürfen. Zudem setzt bei den Bürgerinnen und Bürgern ein Gewöhnungseffekt ein, sich beim Zugang zu beliebigen Stellen „einzuchecken".

Wie in vielen anderen Bundesländern stand auch in Bayern zu Jahresbeginn die Frage nach der Verlängerung des Vertrags mit dem Betreiber von Luca um ein weiteres Jahr an. Aufgrund der oben geschilderten Probleme begrüße ich es, dass das Gesundheitsministerium Anfang 2022 entschieden hat, den Vertrag auslaufen zu lassen.

10.3 Elektronische Kommunikation im Rahmen des COVID19-Pandemiemanagements mit Bürgerinnen und Bürgern

Bereits in meinem 30. Tätigkeitsbericht unter Nr. 3.5 habe ich mich mit der elektronischen Kommunikation mit Bezug auf COVID-19-Fälle zwischen öffentlichen Stellen befasst. Gerade die Gesundheitsämter kommunizieren häufig auch mit Bürgerinnen und Bürgern in elektronischer Form, beispielsweise im Rahmen von Testanmeldungen und Ergebnisübermittlungen, des Impfmanagements oder bei Quarantänemaßnahmen.

Inhalte der Kommunikation sind häufig Gesundheitsdaten. Diese stehen nach Art. 9 DSGVO unter besonderem Schutz und müssen insbesondere ausreichend vor unbefugtem Zugriff gesichert werden.

Gesundheitsdaten sind nicht immer auf den ersten Blick als solche zu erkennen. So mag eine Benachrichtigung des Gesundheitsamts, dass sich eine Bürgerin oder ein Bürger auf Grund einer Einreise aus einem Risikogebiet in Quarantäne begeben muss, keine unmittelbaren Informationen über den konkreten Gesundheitszustand der betroffenen Person enthalten. Gleichwohl sind Quarantänebenachrichtigungen als Gesundheitsdaten im Sinne von Art. 4 Nr. 15 DSGVO zu werten, weil sie immerhin

mittelbar Rückschlüsse auf den Gesundheitszustand der betroffenen Person ermöglichen,[78] was eine mögliche Infektion mit dem Erreger SARS-CoV-2 betrifft.

10.3.1 Kommunikationsmöglichkeiten

Von Bedeutung sind insbesondere die folgenden Kommunikationswege:

— **BayernPortal**

Ist eine Bürgerin oder ein Bürger im BayernPortal registriert, steht ihr oder ihm dort ein Postfach zur verschlüsselten Kommunikation zur Verfügung, das auch für den Austausch mit dem Gesundheitsamt genutzt werden kann.

Da nicht alle Bürgerinnen und Bürger diese Option nutzen können oder wollen, kommt sie hauptsächlich für individuelle Kommunikationsbeziehungen in Betracht. Soll eine größere Zahl von Bürgerinnen und Bürgern auf einmal angesprochen werden, ist das BayernPortal derzeit noch im Nachteil.

— **Cloud-Speicher**

Mehrere Anbieter stellen Cloud-Speicher bereit, in denen Dokumente für Bürgerinnen und Bürger zum Download hinterlegt und dann abgerufen werden können. Ebenso können Bürgerinnen und Bürger dort Dokumente hochladen. Über den Down- oder Uploadlink kann mittels E-Mail informiert werden.

Downloads, die sensible Daten enthalten, müssen grundsätzlich über ein ausreichend komplexes Passwort geschützt werden. Das Passwort muss auf einem anderen Kommunikationsweg übermittelt werden als die Nachricht, die mit ihm entschlüsselt werden soll. Das Passwort kann bei einem persönlichen Kontakt ausgehändigt werden. Für die Übermittlung von Testergebnissen wäre dies beispielsweise etwa anlässlich der Probenentnahme umsetzbar.

Auch bei der Auswahl eines Anbieters für Cloud-Speicher ist auf dessen grundsätzliche Eignung sowie ausreichende Sicherheit zu achten. Meine Orientierungshilfe zur Auftragsverarbeitung[79] sowie (für Kommunen) der Leitfaden zum Outsourcing kommunaler IT[80] enthalten dazu wichtige Hinweise. Kommunen, die bereits Kunden von Anbietern kommunaler Software sind, können unter diesen Maßgaben auch ein Cloud-Angebot dieses Anbieters einsetzen. Das IT Dienstleistungszentrum des Freistaats Bayern (IT-DLZ) bietet kommunalen Verwaltungen außerdem die BayernBox als Cloud-Lösung an.

78 Vgl. Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 9 DSGVO Rn. 11; Weichert, in: Kühling/Buchner, Datenschutz-Grundverordnung/Bundesdatenschutzgesetz, 2. Aufl. 2018, Art. 9 DSGVO Rn. 37.

79 Bayerischer Landesbeauftragter für den Datenschutz, Auftragsverarbeitung, Orientierungshilfe, Stand 4/2019, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018".

80 Bayerischer Landesbeauftragter für den Datenschutz, Leitfaden zum Outsourcing kommunaler IT, Stand 3/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018".

– **E-Mail**

Der Versand von Gesundheitsdaten per E-Mail erfordert grundsätzlich eine Verschlüsselung. Im Idealfall kommt eine Ende-zu-Ende-Verschlüsselung zum Einsatz; eine Transportverschlüsselung, die eine öffentliche Einrichtung gemäß der Richtlinie TR 02102-2 des Bundesamts für Sicherheit in der Informationstechnik[81] einzurichten hat, kann im Einzelfall ausreichen.

Kann auch eine Transportverschlüsselung nicht sichergestellt werden, besteht die Möglichkeit, verschlüsselte Anhänge zu versenden.

Verschlüsselte Anhänge sind allerdings nicht ganz ohne Tücken. Wurde früher gerne eine Datei in eine verschlüsselte ZIP-Datei gepackt, ist heutzutage damit zu rechnen, dass E-Mails mit derartigen Anhängen häufig durch den SPAM- und Schadcodefilter markiert und somit nicht zugestellt werden. Für Office-Dateien und PDF-Dateien besteht die Möglichkeit der direkten Verschlüsselung in der Anwendungssoftware. Für Office-Dokumente ist zu bedenken, dass der Empfänger die jeweiligen Office-Dokumente auch wieder öffnen können sollte. Daher muss ein Dateiformat gewählt werden, das mit unterschiedlichen Office-Anwendungen kompatibel ist. Dies kann auf Grund der heterogenen Software-Produkte, Empfangsgeräte und Empfangsgerätekonfigurationen zu Schwierigkeiten führen. Auf fast jedem Gerät sollten allerdings PDF-Dateien zu öffnen sein, so dass sich mit einem Passwort verschlüsselte PDF-Dateien für den Versand sensibler Informationen eignen. Allerdings müssen aktuelle und sichere Verschlüsselungsverfahren und ausreichend sichere Passworte zum Einsatz kommen.

Auch hier muss das Passwort über einen gesonderten Kommunikationskanal mitgeteilt werden. In meiner Prüfpraxis konnte ich feststellen, dass das Passwort mitunter in einer zweiten E-Mail zugeleitet wurde oder die E-Mail mit dem vermeintlich verschlüsselten Anhang die Information enthielt, dass das Geburtsdatum das Passwort sei. Beide Verfahren erhöhen die Sicherheit nicht wesentlich und sind daher zum Schutz sensibler Inhalte ungeeignet.

Unabhängig vom Einsatz verschlüsselter E-Mails oder verschlüsselter Anhänge ist in jeden Fall darauf zu achten, dass beim E-Mail-Versand immer gewisse Informationen wie etwa der Betreff unverschlüsselt übertragen werden. Diese Teile der E-Mail dürfen daher keine sensiblen Daten enthalten oder Rückschlüsse auf solche Daten zulassen. Das gilt insbesondere auch für „sprechende“ Aktenzeichen.

10.3.2 Beschwerden

Im Berichtszeitraum erreichten mich einige Beschwerden zur elektronischen Kommunikation im Rahmen der Coronavirus-Einreiseverordnung.

Beispielsweise teilte mir ein Bürger mit, dass er von einem bayerischen Gesundheitsamt per E-Mail eine Quarantänebenachrichtigung vom zuständigen Gesundheitsamt

[81] Bundesamt für Sicherheit in der Informationstechnik, BSI TR-02102-2 „Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)“, Stand 1/2021, Internet: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.html.

erhalten habe. Adressat der E-Mail waren neben ihm ca. 100 weitere betroffene Personen. Dies erkannte er daran, dass die weiteren E-Mail-Adressen im Cc-Feld eingetragen waren.

Das Gesundheitsamt hat hier gleich unter zwei Gesichtspunkten gegen Datenschutzrecht verstoßen:

Bereits unabhängig vom Inhalt der Nachricht dürfen einem Bürger in der Kommunikation mit einer Behörde keine weiteren E-Mailadressen bekannt werden. Eine Adressierung an mehrere Personen ist daher nur im Bcc-Feld möglich.

Als noch kritischer ist aber die unverschlüsselte Kommunikation per E-Mail zu werten, wenn Gesundheitsdaten betroffen sind – das gilt eben auch bei einer Quarantänebenachrichtigung (siehe Nr. 10.3.2). Leider musste ich immer wieder feststellen, dass viele Gesundheitsämter über keine geeignete technische Ausstattung verfügen, um überhaupt verschlüsselt kommunizieren zu können.

Das Gesundheitsamt gab an, dass sie die Versendung der Quarantänebenachrichtigung mit der Adressierung im Cc-Feld sehr bedauere und die Beschäftigten entsprechend erneut sensibilisiert habe. Auf Grund meines Hinweises zur Einordnung der Quarantänebenachrichtigung als Gesundheitsdatum stellte die Behörde zudem auf eine verschlüsselte Versendung per E-Mail mit verschlüsselten Word-Dateien im Anhang um.

Ein anderer Petent teilte mir mit, er sei von einem Gesundheitsamt im Rahmen der Coronavirus-Einreiseverordnung aufgefordert worden, seinen Impfpass oder ein PCR-Testergebnis via E-Mail unverschlüsselt einzusenden.

Eine gezielte Aufforderung zur Einsendung von Gesundheitsdaten per unverschlüsselter E-Mail ist nicht zulässig. Dem Bürger kann die Möglichkeit geboten werden, die geforderten Dokumente via Ende-Zu-Ende-verschlüsselter E-Mail einzusenden. Allerdings muss eine Behörde auch mindestens einen anderen sicheren Kommunikationsweg eröffnen. Hierzu zählt insbesondere der Postweg, der immer als Möglichkeit angeführt werden sollte, da nicht alle Betroffenen über elektronische Zugangsmöglichkeiten verfügen.

10.4 Social Engineering – eine nicht zu unterschätzende Gefahr

Der Blick auf die Sicherheit bei der Verarbeitung von personenbezogenen Daten muss stets umfassend und lückenlos sein. Schon kleinste „blinde Flecken“ bei der Analyse von Schwachstellen der Verarbeitung können – wie die Vergangenheit zeigt – Datenschutzverstöße mit nicht unerheblichen Folgen für betroffene Personen zur Folge haben. Nach dem Erfahrungssatz „Gefahr erkannt – Gefahr gebannt“ tut man gut daran, neben der immer komplexer werdenden Technik auch den Menschen mit seinen Besonderheiten zu betrachten.

Beim Social Engineering nutzen Angreifer den „Faktor Mensch“ als vermeintlich schwächstes Glied der Sicherheitskette aus, um ihre kriminellen Absichten zu verwirklichen.[82] Im Berichtszeitraum wurden mir insbesondere folgende Fallkonstellationen hierzu gemeldet:

Ein Beschäftigter einer bayerischen öffentlichen Stelle arbeitete im Homeoffice und wurde von einem angeblichen Service-Mitarbeiter von Microsoft angerufen. Wegen zahlreicher bei Microsoft eingegangener Fehlermeldungen sowie auslaufender Lizenzen benötige er einen Remote-Zugriff auf den Rechner des Behördenbediensteten. Die Ausführungen des vermeintlichen Microsoft-Mitarbeiters waren so überzeugend, dass sein „Opfer“ einen Remote-Zugriff auf seinen Rechner zuließ und dadurch dem unbekannten Angreifer für eine längere Zeit auch Zugriff auf dienstlich verarbeitete personenbezogene Daten gewährte.

Der zweite Fall ereignete sich in einem bayerischen Notariat. Dort rief eine unbekannte Person an und gab sich als Eigentümer einer Wohnung aus, deren Verkauf gerade im Notariat bearbeitet wurde. Der angebliche Eigentümer erbat für seine Unterlagen die Übersendung einer eingescannten Kaufvertragsurkunde per E-Mail. Dazu gab er eine E-Mail-Adresse an. Überzeugt, dass alles mit rechten Dingen zugehe, übersandte die angerufene Notariatsmitarbeiterin ohne weitere Kontrollen die gewünschte Datei an die ihr genannte E-Mail-Adresse.

Nach diesem Anruf erhielt das Notariat eine Nachricht des echten Verkäufers. Der Verkäufer informierte darüber, dass in den vergangenen Wochen mehrfach versucht worden sei, bei unterschiedlichen Institutionen und Behörden telefonisch in seinem Namen auf vertrauliche und persönliche Daten zuzugreifen. Der Anrufer habe eine ähnliche männliche Stimme, kenne Geburtsdatum, Geburtsort, Wohnadresse sowie Handynummer des Verkäufers und verfüge anscheinend über weitere persönliche Daten.

Auf Rückfrage des Notariats gab der Verkäufer an, dass er nicht der Anrufer gewesen sei. Die von der täuschenden Person angegebene E-Mail-Adresse wurde auch bei anderen Institutionen von der Person verwendet, die persönliche Informationen über den Verkäufer zu erlangen suchte.

Die beiden Fälle zeigen, dass auch bayerische öffentliche Stellen Ziele von Social Engineering sind. Daher müssen auch dort Schutzmaßnahmen getroffen werden, die solchen Angriffen wirksam entgegenwirken. Da beim Social Engineering insbesondere Hilfsbereitschaft, Vertrauen, Überraschung, Angst oder Respekt vor Autorität ausgenutzt werden, um Personen geschickt zu manipulieren, reduzieren insbesondere folgende Maßnahmen das datenschutzrechtliche Risiko:

— **Klare Handlungsanweisungen**

  Insbesondere in Bereichen, die anfällig für Social Engineering sind, sollten klare Handlungsanweisungen erstellt und deren wirksame Umsetzung bedarfsgerecht überprüft werden. Grundlage hierfür können beispielsweise die Handlungsempfehlungen des Bundesamts für Sicherheit in der Informationstechnik sein.

[82] Internet: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.

– **Sensibilisierung**

  Das Vorgehen bei Social Engineering kann sehr vielseitig und für angegriffene Personen unerwartet sein. Daher sollten die Beschäftigten und gegebenenfalls weitere relevante Personen im Allgemeinen und auch speziell hinsichtlich der relevanten und aktuell beobachteten Vorgehensweisen informiert werden.

– **Fehlerkultur**

  Eine gelebte offene Fehlerkultur wirkt schadensmindernd. Denn je früher ein Social Engineering-Angriff erkannt wird, desto früher können geeignete Gegenmaßnahmen ergriffen werden.

10.5 Einführung einer Ersthelfer-App

Eine bayerische öffentliche Stelle hat sich an mich mit der Bitte gewandt, sie bei der Implementierung einer Ersthelfer-App beratend zu unterstützen. Beabsichtigt war, eine Ersthelfer-App in einer bayerischen Region einzurichten, um damit das sogenannte „therapiefreie Intervall" bis zum Eintreffen des öffentlich-rechtlichen Rettungsdienstes zu überbrücken. Insbesondere in Fällen von Bewusstlosigkeit soll über das „Ersthelfer-System" rasch Hilfe geleistet werden, um dauerhafte gesundheitliche Schäden sowie Todesfälle nach Möglichkeit zu vermeiden. Hierzu werden geeignete freiwillige Helferinnen und Helfer geworben, geschult und mit der Ersthelfer-App auf ihren Smartphones ausgestattet.

Die Alarmierung von Ersthelferinnen und Ersthelfern, die sich örtlich ausreichend nahe bei der hilfsbedürftigen Person befinden, wird durch die Integrierte Leitstelle angestoßen. Die Ermittlung der in der konkreten Einsatzsituation verfügbaren Ersthelferinnen und Ersthelfer, die Anfrage, ob diese einsatzfähig sind, sowie die Beantwortung der Einsatzfrage und die Routenführung zur hilfsbedürftigen Person übernimmt das Ersthelfer-System größtenteils automatisiert.

Bei meiner Beratung standen im Wesentlichen folgende Aspekte im Vordergrund der Betrachtung:

– **Datenschutzrechtliche Vereinbarungen**

  Bei dem konkreten Projekt haben eine Stadt, ein Rettungszweckverband, Träger der Integrierten Leitstellen sowie ein nicht-öffentliches Unternehmen als Anbieter des Ersthelfer-Systems miteinander kooperiert; auf Seiten des Unternehmens waren zudem Unterauftragsverarbeiter eingebunden. Die Kooperation erforderte ein komplexes Regelwerk. Ein wichtiger erster Schritt bestand darin, die datenschutzrechtlichen Rollen der einzelnen Stellen klar herauszuarbeiten und die Vereinbarung der datenschutzrechtlich notwendigen Vorgaben zu gewährleisten (insbesondere in einem Vertrag zur gemeinsamen Verantwortung nach Art. 26 DSGVO und in einem Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO).

– **Standortüberwachung der Ersthelfer**

  Für das Funktionieren der Ersthelfer-App sind aktuelle Standortdaten zu den Ersthelferinnen und Ersthelfern unverzichtbar. Nur mit diesen Daten kann das Ersthelfer-System den besten Weg zum jeweiligen Notfall weisen. Allerdings

ist es datenschutzrechtlich nicht erforderlich, die Standorte der an der App angemeldeten Ersthelferinnen und Ersthelfer laufend im Ersthelfersystem genau zu erfassen. Daher werden nach Einschaltung der App durch eine Ersthelferin oder einen Ersthelfer die Daten zu ihrem oder seinem Standort vergröbert verarbeitet und nur bei größeren Ortsbewegungen aktualisiert. Bei einer Alarmierung kann auf dieser Datenbasis nur eine erste Auswahl von Ersthelferinnen und Ersthelfern im Alarmierungsradius getroffen werden. Da die vergröberten Standortinformationen nur für die automatisierte Verarbeitung der Notfallalarmierung benötigt werden, haben Anwender des Ersthelfer-Systems keinen Zugriff auf diese Standortdaten.

Erst bei der Alarmierung und nach der aktiven Annahme des Einsatzes durch eine Ersthelferin oder einen Ersthelfer werden genaue Standortdaten an das System und die Integrierte Leitstelle übermittelt. Ferner erhält die Ersthelferin oder der Ersthelfer erst nach der Annahme die notwendigen Einsatzinformationen. Nach Beendigung des Einsatzes werden die Standortdaten wieder vergröbert verarbeitet und nur bei Bedarf aktualisiert.

– **Erforderlichkeit der verarbeiteten Daten**

Ursprünglich geplant war, dass jede Ersthelferin und jeder Ersthelfer nach dem Einsatz einen sogenannten „Notfallbericht“ erstellt, der den Erstbefund der Notfallpatientin oder des Notfallpatienten, die durchgeführten Maßnahmen sowie den Patientenbefund bei Übergabe an den Rettungsdienst enthalten sollte. Dieser Bericht sollte im Ersthelfer-System gespeichert werden. Da hierfür jedoch keine datenschutzrechtlich tragfähige Befugnis erkennbar war, wird stattdessen nur noch – nach einer entsprechenden Einwilligung der Ersthelferin oder des Ersthelfers – die Zeitspanne zwischen deren oder dessen Alarmierung und dem Eintreffen am Ort des Notfalls erfasst.

Die Prüfung der Erforderlichkeit einer Verarbeitung setzt (unter anderem) den Grundsatz der Datenminimierung um. Der Grundsatz der Datenminimierung verpflichtet die Verantwortlichen, bei Verarbeitungen mit personenbezogenen Daten möglichst sparsam umzugehen, insbesondere nur so viele Daten zu erheben, wie für die Wahrnehmung der jeweiligen Aufgabe als dem Verarbeitungszweck benötigt werden.

Anhand dieses Projekts wurde ein weiteres Mal deutlich, wie wichtig es ist, schon zu Beginn einer Verarbeitung die datenschutzrechtlichen Rollen mehrerer beteiligter Stellen zu klären.

Vorhaben dieser Art sollten von Anfang an durch Ansprechpartnerinnen und Ansprechpartner begleitet werden, die das erforderliche datenschutzrechtliche Know-how bereitstellen können. Im Übrigen ist zu bemerken, dass einheitliche Standards für die Organisation und die technische Vernetzung der unterschiedlichen Ersthelfer-Systeme eine zweckgerechte Implementierung erheblich erleichtern könnten. Solche Standards können von regionalen Akteuren allerdings nicht geschaffen werden.

10.6 Beschäftigtendatenschutz bei der Ablage von E-Mails

Eine bayerische öffentliche Stelle hat sich mit der Frage an mich gewandt, was bei einer Ablage von E-Mails hinsichtlich des Beschäftigtendatenschutzes zu beachten ist.

Die Stelle druckt relevante E-Mails aus und nimmt diese danach zu den (Papier-)Akten. Dabei können die E-Mail-Ausdrucke Beschäftigtendaten enthalten (etwa in Form von Absender-, Empfängerangaben oder zur Identität der Person, die die E-Mail ausgedruckt hat). Bei einer späteren Einsicht in die Akten können diese Informationen gegebenenfalls offengelegt werden.

In diesem Kontext führte die öffentliche Stelle aus, dass insbesondere ein vollständiger Ausdruck von E-Mails stets die Inhalte der E-Mail-Adressfelder „Von", „An" und „Cc" umfasst. Außerdem ist immer auch der vollständige Benutzername des E-Mail-Systems für die Person angegeben, die die E-Mail ausgedruckt hat. Die Konfiguration des genutzten E-Mail-Systems bietet keine Möglichkeit an, die Ausgabe dieser Informationen zu unterdrücken.

Inhalte der Adressfelder „Von", „An" und „Cc" können auch personalisierte E-Mail-Adressen und Namen von Beschäftigten der Stelle, also personenbezogene Beschäftigtendaten sein. Die Bedenken der anfragenden Stelle konnte ich ausräumen.

Rechtlicher Ausgangspunkt meiner Bewertung war Art. 4 Abs. 1 BayDSG: Eine öffentliche Stelle darf personenbezogene Daten hiernach verarbeiten, soweit dies zur Aufgabenerfüllung erforderlich ist. Diese Befugnis umfasst grundsätzlich auch die Verarbeitung von Beschäftigtendaten in Sachakten. Die Erforderlichkeit einer Datenverarbeitung ließ sich in vorliegendem Zusammenhang mit den nachfolgenden Erwägungen begründen.

Die in den aufgeführten E-Mail-Adressfeldern gespeicherten personenbezogenen Beschäftigtendaten dokumentieren hausinterne Absender und Empfänger der jeweiligen E-Mail und können insbesondere bei internen Weiterleitungen den sonst üblichen sachleitenden Verfügungen, wie sie auf papiergebundenen Schreiben angebracht sind, gleichgestellt werden.

Da E-Mails, die zum Akt verfügt werden, als Teil eines Vorgangs auch die Art der Bearbeitung, die wesentlichen Schritte des Geschäftsgangs und die Erledigung in ihrer zeitlichen Reihenfolge nachvollziehbar, vollständig und dauerhaft erkennen lassen müssen (vgl. § 18 Allgemeine Geschäftsordnung für die Behörden des Freistaates Bayern), sind hinsichtlich der Verarbeitung dieser Adressfelder datenschutzrechtlich keine durchgreifenden Einwände erkennbar.

Bei der anfragenden Stelle werden relevante E-Mails ausgedruckt und zur Papierakte verfügt; danach wird die digitale E-Mail gelöscht. Die Angabe des Namens der Person, die die E-Mail ausgedruckt hat, wird dabei vom verwendeten E-Mail-System auf dem E-Mail-Ausdruck automatisiert mit angebracht.

Die datenschutzrechtliche Zulässigkeit hierfür ergibt sich aus dem Grundsatz des „ersetzenden Druckens", der sich analog zum Grundsatz des ersetzenden Scannens ergibt. Beim sogenannten „ersetzenden Scannen" wird eine digitale Kopie aus Papierdokumenten erzeugt und die Papieroriginale werden nach dem Scannen vernichtet. Da die digitale Kopie mit dem Papierdokument inhaltlich sowie bildlich übereinstimmen und für nutzende Personen lesbar sein muss, kann als typische technische

Lösung für die Sicherung der Integrität das Aufbringen einer elektronischen Signatur auf der digitalen Kopie geboten sein.[83]

Beim „ersetzenden Drucken“ wird bei einer papiergebundenen Aktenführung die elektronische Form einer E-Mail ersetzend in ihre papiergebundene Form überführt. Dabei muss die öffentliche Stelle analog zum Scannen sicherstellen, dass der Ausdruck inhaltlich mit der E-Mail übereinstimmt. Der auf dem Ausdruck enthaltene Name der ausdruckenden Person ermöglicht es, im Zweifelsfall bei dieser nachzufragen bzw. möglichen Unstimmigkeiten gezielt nachzugehen und stellt dadurch einen wichtigen, mit der E-Mail fest verbundenen Hauptbestandteil des Transfervermerks „ersetzendes Drucken“ dar.

Allerdings habe ich der Stelle aufgetragen, risikoorientiert zu prüfen und zu bewerten, ob in den dargestellten Konstellationen die Beschäftigtenangaben in einer datenschutzfreundlicheren, etwa pseudonymisierten Form verarbeitet werden können.

10.7 Beanstandung nach dem Verlust von Bewerbungsunterlagen

Eine bayerische öffentliche Stelle erhielt nach Ausschreibung einer zu besetzenden Stelle über 100 Bewerbungen, in denen sich unter anderem Lokalisationsdaten (Wohnort, Wegstrecke), Daten über die Verfolgung von Straftaten und Ordnungswidrigkeiten, Daten zu religiösen oder weltanschaulichen Überzeugungen sowie Gesundheitsdaten befanden.

Nach zentralen Vorarbeiten sollten die Bewerbungsunterlagen an die im Stellenbesetzungsverfahren beteiligten Organisationseinheiten weitergegeben werden. Hierfür wurden die Bewerbungsunterlagen in einen Transportbehälter gelegt, dieser wurde an eine zentrale Versandstelle adressiert und – wie üblich – gemeinsam mit anderer Hauspost für die Abholung durch den regelmäßigen Fahrdienst im Untergeschoss des Dienstgebäudes bereitgestellt. Seit dieser Bereitstellung ist der Behälter mit den Bewerbungsunterlagen trotz intensiver Nachforschung spurlos verschwunden.

Die in dieser Konstellation notwendige Meldung einer Datenpanne habe ich über das Meldeformular auf meiner Homepage von der verantwortlichen Stelle deutlich verspätet erhalten; die gesetzlich vorgeschriebene Begründung dafür fehlte.

Die Meldung ist nach Art. 33 Abs. 1 Satz 1 DSGVO unverzüglich, mithin ohne schuldhaftes Zögern, zu erstatten. Dies gilt insbesondere für ein – wie in der hier zu beurteilenden Fallkonstellation gegebenes – leicht zu erkennendes und leicht zu beschreibendes Ereignis.

Die in Art. 33 Abs. 1 Satz 1 DSGVO enthaltene 72-Stunden-Frist ist eine Richtgröße, an deren Überschreitung eine Begründungspflicht (Art. 33 Abs. 1 Satz 2 DSGVO) anknüpft. Aus aufsichtsbehördlicher Sicht kann bei Datenschutzverletzungen, die nicht auf den ersten Blick – und sei es auch nur vorläufig – einzuordnen sind, eine Aufklä-

[83] Vgl. Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie 03138 „Ersetzendes Scannen“ (RESISCAN), Internet: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/Ersetzendes-ScannenTR-Resiscan/ersetzendes-scannentr-resiscan_node.html.

rungsphase von höchstens 24 Stunden ab dem Auftreten hinreichender Anhaltspunkte in Anspruch genommen werden. Die Dauer hängt von den erforderlichen Aufklärungsmaßnahmen ab. Wird mehr Zeit benötigt, ist dies in der Meldung zu erläutern. Art. 33, 34 DSGVO sind in meiner Orientierungshilfe „Meldepflicht und Benachrichtigungspflicht des Verantwortlichen“ eingehend erläutert.[84]

Gehen Unterlagen von über 100 Bewerberinnen und Bewerbern auf dem regelmäßig genutzten und üblichen Transportweg verloren, liegt grundsätzlich nahe, dass die gebotenen Schutzmaßnahmen gegen Verlust (vgl. Art. 32 Abs. 1 DSGVO) nicht getroffen waren. Dies und die deutlich verspätete Meldung führten zu einer Beanstandung.

Den offenkundigen Handlungsbedarf hat die öffentliche Stelle erkannt und als Reaktion auf diesen Vorfall insbesondere folgende Abhilfemaßnahmen festgelegt:

— **Verschließbare Transportbehältnisse**

  Der Aktentransport zwischen einzelnen Dienstgebäuden wird nunmehr in verschließbaren Aluminiumkisten durchgeführt. Die Mitarbeiter des Botendienstes sind angewiesen, die Alukisten auch tatsächlich zu verschließen. Zudem können diese Aluminiumkisten nur von den dazu berechtigten Personen in den einzelnen Dienstgebäuden geöffnet werden.

— **Spezialbehälter für Entsorgung**

  Das für die Entsorgung bestimmte Schriftgut muss seit dem Vorfall deutlicher gekennzeichnet werden und wird in speziellen, nur für diesen Zweck verwendeten Behältern transportiert.

— **Sensibilisierung**

  In Schulungen werden die Mitarbeiterinnen und Mitarbeiter bezüglich des Umgangs mit Verletzungen des Schutzes personenbezogener Daten sensibilisiert.

— **Aktentransportkonzept**

  In einem Aktentransportkonzept werden die datenschutzrechtlichen Risiken sowie die umgesetzten Abhilfemaßnahmen dargestellt. Zu diesen Maßnahmen zählen etwa die Absicherung der Ablageorte beim Transport, die Verwendung von Transportbegleitunterlagen für eine Vollständigkeitsfeststellung sowie Kontrollmechanismen, die einen (drohenden) Verlust rasch erkennen und die Ursache vereinfacht aufdecken helfen. Dies ermöglicht eine regelmäßige Kontrolle der entsprechenden Routinen im Verwaltungsalltag.

10.8 Verweigerte Kfz-Ummeldung wegen Personenverwechslung

Eine Bürgerin hat sich an mich gewandt, da ihr bei einer Zulassungsstelle aufgrund von angeblichen Steuerschulden zunächst die Ummeldung ihres Kraftfahrzeuges verweigert worden war. Konkret wurde ihr im Beisein mehrerer anderer Kundinnen und Kunden der Zulassungsstelle mitgeteilt, dass sie ihr Kfz erst ummelden könne,

[84] Bayerischer Landesbeauftragter für den Datenschutz, Meldepflicht und Benachrichtigungspflicht des Verantwortlichen, Stand 6/2019, https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018“.

wenn sie ihre Schulden bei der Stadtverwaltung beglichen habe. Eine telefonische Rücksprache der betroffenen Bürgerin mit dem Steueramt der Kommune brachte eine Verwechslung ans Licht, so dass der Ummeldung ihres Fahrzeuges nichts mehr entgegenstand.

Die Bürgerin erlebte eine sehr unangenehme und peinliche Situation, da sie sich zu Unrecht „an den Pranger gestellt" fühlte und andere Personen, die sich in der Zulassungsstelle befanden, den Vorhalt mitbekamen. Wie sich schließlich herausstellte, hatte es die Zulassungsstelle versäumt, die Identität der Bürgerin ausreichend zu überprüfen.

Ich habe die verantwortliche Stelle im Hinblick auf die Datenrichtigkeit gemäß Art. 5 Abs. 1 Buchst. d DSGVO unmissverständlich darauf hingewiesen, dass sie alle ihr zur Verfügung stehenden personenbezogenen Daten nutzen muss, wenn Personen (hier: säumige Steuerschuldner) eindeutig identifiziert und zudem behördlichen Maßnahmen (hier: Verweigerung der Zulassung) ausgesetzt werden sollen. Zwar gilt grundsätzlich immer der Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO), was aber nicht dazu führen darf, dass dadurch der Grundsatz der Datenrichtigkeit ausgehebelt wird.

Für die sachliche Richtigkeit der verarbeiteten personenbezogenen Daten ist nach Art. 5 Abs. 2 DSGVO die zuständige öffentliche Stelle als datenverarbeitende Stelle verantwortlich.

Insbesondere ist auch die Klärung der Frage, ob die bei der Zulassungsstelle vorliegenden personenbezogenen (ggf. falschen, weil unvollständigen) Daten mit denen des von einer Maßnahme betroffenen Bürgers übereinstimmen, nicht Aufgabe der Bürgerinnen und Bürger, sondern der für die Datenverarbeitung zuständigen öffentlichen Stelle. Dies umso mehr, als in Abhängigkeit vom Ausgang der Identitätsprüfung eine für den betroffenen Bürger nicht ganz unerhebliche Maßnahme getroffen wurde.

Daneben habe ich die betroffene Stelle zur Wahrung der Diskretion im Rahmen der Kfz-Zulassung angehalten. Die Kommune hat technische und organisatorische Vorkehrungen zu treffen, damit künftig ähnliche oder vergleichbare Fälle einer beiläufigen Bloßstellung vor anwesenden Personen vermieden werden. Öffentliche Stellen sind nach Art. 32 Abs. 1 DSGVO auch beim Bürgerkontakt verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau im Zusammenhang mit der Verarbeitung personenbezogener Daten zu gewährleisten.

10.9 Meldungen von Verletzungen des Schutzes von personenbezogen Daten

Seit Inkrafttreten der Datenschutz-Grundverordnung im Mai 2018 berichte ich über die bei mir eingehenden Meldungen von Datenpannen. Besonders ausführlich habe ich dieses Thema in meinem 30. Tätigkeitsbericht 2020 unter Nr. 12.10 beleuchtet. Da nach wie vor zur Bekämpfung der COVID-19-Pandemie in großem Umfang medizinische Informationen wie Quarantänebescheide, Testergebnisse oder Kontaktlisten versandt werden müssen, stammen zahlreiche Meldungen aus dem Gesundheitsbereich. Insgesamt standen Verletzungen des Schutzes der Vertraulichkeit von personenbezogenen Daten im Vordergrund, doch waren auch zahlreiche Verletzungen der weiteren Schutzziele Integrität und Verfügbarkeit zu verzeichnen. Etwas ärgerlich ist, dass zu den regelmäßig wiederkehrenden Konstellationen auch einige zählen, die ich unter anderem in meinen letzten Tätigkeitsbericht bereits behandelt habe.

Das Aufkommen an Meldungen nach Art. 33 DSGVO hat sich im Vergleich zum letzten Berichtszeitraum noch einmal deutlich erhöht. Dies lässt allerdings nicht ohne Weiteres den Rückschluss auf einen Trend zu mehr Datenpannen zu; nicht wenigen öffentlichen Stellen ist es im Berichtszeitraum gelungen, die Meldung an die Datenschutz-Aufsichtsbehörden in ihre Geschäftsprozesse einzubauen. Hier zahlt sich aus, dass ich gerade bei Stellen, die in großem Umfang sensible Daten verarbeiten, auf ein effektives Datenschutzmanagement hinwirke.

In diesem Jahr möchte ich nur einen etwas skurrilen Fall aufgreifen, der ein spezifisches Risiko der Arbeit im Homeoffice aufzeigt, wenn große bayerische Flüsse im Spiel sind.

Eine kommunale Beschäftigte fuhr mit dem Fahrrad vom Büro ins Homeoffice. Die für die Weiterarbeit benötigten Papierakten hatte sie lose in ihren Fahrradkorb gelegt; sie enthielten personenbezogene Daten von Bürgerinnen und Bürgern. Auf einer Donaubrücke wurde die Beschäftigte samt Fahrrad und Aktenstapel von einem heftigen Windstoß erfasst. Die Meldung nach Art. 33 DSGVO teilt mit: „Ca. 10 Blätter flogen [...] über das Geländer in die Donau, den Rest konnte [die Beschäftigte] mühsam und unter Hilfe zweier Passanten einsammeln und retten." Hinsichtlich der verlorenen Blätter stellt die Meldung nüchtern fest: „Theoretisch können die Papiere im Uferbereich[..] angespült werden. Die Qualität und Lesbarkeit dürfte im Lauf der Zeit erheblich abnehmen."

Dieser Fall zeigt einmal mehr die Notwendigkeit ausreichender Sicherungsmaßnahmen beim Aktentransport. Wie ich bereits in meinem 29. Tätigkeitsbericht 2019 unter Nr. 12.7 dargestellt habe, sollten Papierakten in verschließbaren Behältern transportiert werden; ferner sollte dafür Sorge getragen werden, dass diese Behältnisse nicht unbeaufsichtigt abgestellt oder ganz vergessen werden.

10.10 Exchange-Sicherheitslücke

Durch Informationen von Microsoft sowie des Bundesamts für Sicherheit in der Informationstechnik (BSI) wurde Anfang März 2021 bekannt, dass vier Zero-Day-Sicherheitslücken in Microsoft Exchange-Servern existierten. Diese Lücken machten auch zahlreiche öffentliche Stellen über das Internet angreifbar, sobald sie Microsoft Exchange-Server in einer bestimmten Konfiguration einsetzten. Das BSI stufte die Gesamtsituation als kritisch ein, da bereits eine flächendeckende Ausnutzung stattfand und somit die Wahrscheinlichkeit einer Kompromittierung der verwundbaren Systeme als realistisch anzusehen war. Zudem zeigte die Medienberichterstattung, dass es im Nachgang der Kompromittierung auch zu weiteren Angriffen auf Basis dieser Sicherheitslücke kam.

Mich erreichte im März und April 2021 eine sehr hohe Anzahl an Meldungen nach Art. 33 DSGVO. In diesen Fällen konnte jeweils eine Kompromittierung nachgewiesen werden. Es handelte sich um eine akute Gefährdung, bei der zeitnahes Handeln erforderlich war. Microsoft stellte sowohl Patches zum Schließen der Sicherheitslücken zur Verfügung als auch Anleitungen und Möglichkeiten, die eigenen Server gezielt auf eine Infektion hin zu prüfen. Das BSI fordert für gezielte persistente Angriffe (Advanced Persistent Threat – APT) wie bei der Bedrohungslage für Exchange-Server eine Neuinstallation für betroffene, infizierte oder kompromittierte IT-Systeme. Dieser Forderung habe ich mich uneingeschränkt angeschlossen und allen öffentlichen Stellen in Bayern dringend empfohlen, entsprechende technische Maßnahmen

ohne zeitlichenVerzug umzusetzen. Zur Unterstützung der Verantwortlichen in Bayern haben das Bayerische Landesamt für Datenschutzaufsicht und ich umfangreiche Informationen erarbeitet und auf unseren Homepages zur Verfügung gestellt. Diese Dokumente beziehen sich zwar auf spezielle Sicherheitslücken, enthalten aber auch grundlegende Maßnahmen, die unabhängig vom konkreten Vorfall umgesetzt werden sollten.

Die Kompromittierung der Microsoft Exchange-Server hat gezeigt, dass Verantwortliche und Auftragsverarbeiter auch in Anbetracht hochdynamischer digitaler Prozesse ihren gesetzlichen Verpflichtungen nach Art. 32 DSGVO uneingeschränkt nachzukommen haben. Insbesondere vor dem Hintergrund der Exchange-Sicherheitslücke müssen die Verantwortlichen und Auftragsverarbeiter im öffentlichen Sektor die eingesetzten IT-Systeme durch internes oder externes IT-Fachpersonal dauerhaft und regelmäßig auf Schwachstellen überprüfen lassen, diese Systeme unter Berücksichtigung des Stands der Technik aktualisieren (etwa durch bereitgestellte Patches) und erforderlichenfalls alte, angreifbare IT-Systeme durch neue ersetzen.

11 Datenschutzkommission

Der Datenschutzkommission beim Bayerischen Landtag gehörten am Ende des Berichtszeitraums folgende Mitglieder und stellvertretende Mitglieder an:

Aus dem Landtag:

Mitglieder:

Peter Tomaschko, CSU
Benjamin Adjei, BÜNDNIS 90/DIE GRÜNEN
Alfred Grob, CSU
Dr. Helmut Kaltenhauser, FDP
Gerd Mannes, AfD
Gerald Pittner, FREIE WÄHLER
Florian Ritter, SPD

Stellvertretende Mitglieder:

Tanja Schorer-Dremel, CSU
Verena Osgyan, BÜNDNIS 90/DIE GRÜNEN
Andreas Jäckel, CSU
Matthias Fischbach, FDP
Roland Magerl, AfD
Wolfgang Hauber, FREIE WÄHLER
Christian Flisek, SPD

Auf Vorschlag der Staatsregierung:

Mitglied:

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:

Gudrun Aschenbrenner, Mitglied des Vorstands der Anstalt für Kommunale Datenverarbeitung in Bayern

Auf Vorschlag des Staatsministeriums für Gesundheit und Pflege aus dem Bereich der gesetzlichen Sozialversicherungsträger:

Mitglied:

Werner Krempl, Erster Direktor und Vorsitzender der Geschäftsführung der Deutschen Rentenversicherung Nordbayern

Stellvertretendes Mitglied:

Dr. Irmgard Stippler, Vorstandsvorsitzende 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 Benjamin Adjei, MdL.

Die Datenschutzkommission beim Bayerischen Landtag tagte im Berichtszeitraum zwei Mal.

12 Ländervertreter im EDSA

Der Bundesrat hat mich in seiner 1006. Sitzung am 25. Juni 2021 gemäß § 17 Abs. 1 Satz 2 und 3 Bundesdatenschutzgesetz (BDSG) zum Stellvertreter des gemeinsamen Vertreters im Europäischen Datenschutzausschuss (EDSA) gewählt.

Der Europäische Datenschutzausschuss (siehe Art. 68 ff. DSGVO) ist eine Einrichtung der Europäischen Union. Er besteht aus dem Leiter einer Datenschutz-Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten oder ihren jeweiligen Vertretern. Auch die Europäische Kommission sowie die Aufsichtsbehörden der EWR-/EFTA-Staaten dürfen an den Sitzungen teilnehmen, haben dort jedoch kein Stimmrecht. Eine wesentliche Aufgabe des Europäischen Datenschutzausschusses liegt darin, die einheitliche Anwendung der Datenschutz-Grundverordnung sicherzustellen. In diesem Rahmen stellt der Europäische Datenschutzausschuss einheitliche Dokumente, etwa Leitlinien und Empfehlungen, zur Verfügung. Er berät die Europäische Kommission in allen Fragen des Schutzes personenbezogener Daten, insbesondere auch bei der Rechtsetzung. Zu grenzüberschreitenden Einzelfällen kann der Europäische Datenschutzausschuss Beschlüsse fassen. Ferner fördert er die Zusammenarbeit zwischen den nationalen Datenschutz-Aufsichtsbehörden.

Da in Deutschland mehrere Behörden dieser Art bestehen, sieht das Bundesdatenschutzgesetz in § 17 Abs. 1 Satz 1 BDSG vor, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die Funktion des gemeinsamen Vertreters im Europäischen Datenschutzausschuss ausübt. Sein vom Bundesrat zu wählender Stellvertreter nimmt die Stimme Deutschlands im Europäischen Datenschutzausschuss nicht nur im Verhinderungsfall wahr. Auch in bestimmten, für die Länder wichtigen Angelegenheiten überträgt der gemeinsame Vertreter seinem Stellvertreter die Verhandlungsführung und das Stimmrecht (siehe § 17 Abs. 2 BDSG).

Deutschland muss im Europäischen Datenschutzausschuss grundsätzlich einheitlich auftreten. Vor allem bei verbindlichen Abstimmungen können der gemeinsame Vertreter oder der gewählte Stellvertreter regelmäßig nur für oder gegen einen Vorschlag stimmen oder sich der Abstimmung enthalten, auch wenn die deutschen Datenschutz-Aufsichtsbehörden zu einem bestimmten Thema unterschiedliche Auffassungen vertreten. Die Datenschutz-Grundverordnung sieht in diesen Fällen jedoch eine einheitliche Position jedes Mitgliedstaats vor. Eine Hauptaufgabe des Ländervertreters besteht deshalb darin, im Vorfeld der Ausschusssitzungen gemeinsam mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit den jeweiligen Standpunkt der deutschen Datenschutz-Aufsichtsbehörden zu ermitteln, der den europäischen Verhandlungen zugrunde gelegt wird. Unterstützt wird dieser Prozess durch die Zentrale Anlaufstelle (ZASt), die beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit eingerichtet, von diesem aber organisatorisch getrennt ist.

Seit meiner Wahl zum Ländervertreter hat der EDSA bereits zahlreiche, nicht nur für die Bürgerinnen und Bürger, sondern gerade auch für bayerische öffentliche Stellen wichtige Themen behandelt, an denen ich mitgewirkt habe oder noch mitwirke. Hervorheben möchte ich nur die folgenden Beratungsgegenstände:

- Leitlinien zum Recht auf Auskunft (betrifft Art. 15 DSGVO);
- Löschung personenbezogener Daten auch ohne Antrag der betroffenen Person (betrifft Art. 17 DSGVO);
- Einsatz von Cookies und Google Analytics;
- Umsetzung der Entscheidung des Gerichtshofs der Europäischen Union vom 16. Juli 2020, Rechtssache C-311/18 – „Schrems II“ (betrifft Datenübermittlungen in die Vereinigten Staaten von Amerika);
- Evaluierung der Datenschutzrichtlinie im Bereich Justiz und Inneres;
- Koordinierte Untersuchung der EDSA-Mitglieder zum Einsatz von Cloud-Diensten durch öffentliche Stellen;
- Verbesserung der Zusammenarbeit der europäischen Datenschutzaufsichtsbehörden.

Nähere Informationen zum Europäischen Datenschutzausschuss sind im Internet unter https://edpb.europa.eu/edpb_de zu finden.

13 Anhang

Stellungnahme zur Anhörung des Ausschusses für Kommunale Fragen, Innere Sicherheit und Sport des Bayerischen Landtags am 19. Mai 2021 zum Gesetzentwurf der Staatsregierung zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften (Drs. 18/13716)

1. Inwieweit ist der Gesetzentwurf geeignet, die im Abschlussbericht der PAG-Expertenkommission genannten Reformempfehlungen umzusetzen?

Der Gesetzentwurf setzt einen Teil der Empfehlungen des Abschlussberichts[1] der PAG-Expertenkommission um. Teilweise werden aber Empfehlungen – insbesondere aus datenschutzrechtlicher Sicht – nicht oder nur unzureichend umgesetzt. Ferner wird der Gesetzentwurf auch zur Erweiterung polizeilicher Befugnisse genutzt.

2.1 Wie bewerten Sie die grundsätzliche Beibehaltung des Gefahrenbegriffs der „drohenden Gefahr“ und die konkrete Änderung des Art. 11 PAG sowie die Einfügung eines Art. 11a PAG-E?

Nach wie vor habe ich große Vorbehalte gegenüber dem Gefahrenbegriff der „drohenden Gefahr“. Bereits im Gesetzgebungsverfahren zum Gesetz zur effektiveren Überwachung gefährlicher Personen vom 24. Juli 2017[2] habe ich die Einführung stark kritisiert. Große Sorge bereitet mir, dass mit der drohenden Gefahr eine Herabsenkung der Einschreitschwelle bei polizeilichen Standardmaßnahmen wie etwa der Identitätsfeststellung oder der Durchsuchung einer Person bewirkt wirkt, auch wenn eine Beschränkung auf bedeutende Rechtsgüter i.S.d. Art. 11a Abs. 2 PAG-E erfolgt. Dies birgt die Gefahr, dass durch die Beibehaltung – man darf nicht außer Acht lassen, dass die Einführung des Begriffs der „drohenden Gefahr“ ursprünglich der Bekämpfung des Terrorismus und Extremismus dienen soll(te)[3] – in erster Linie in die Freiheitsrechte der „Normalbürger“ eingreift und damit über das Ziel hinaus schießt.

Die Gesetzesbegründung[4] geht davon aus, dass das *BVerfG* mit der Entscheidung vom 27. Mai 2020[5] die drohende Gefahr als neue Gefahrenkategorie anerkannt und gleichzeitig klargestellt habe, dass diese Gefahrenkategorie nicht auf Fälle der Terrorismusabwehr beschränkt sei. Diese Auffassung teile ich nicht.

Die Entscheidung des *BVerfG* zum BKA-Gesetz[6] bezieht sich im Zusammenhang mit der „drohenden Gefahr“ auf Maßnahmen der Gefahraufklärung (heimliche Überwachungsmaßnahmen) und nicht auf Eingriffe in den Kausalverlauf, mithin Beseitigungs- bzw. Verhinderungsmaßnahmen. Auch in seiner Entscheidung vom 27. Mai 2020[7] behandelt das *BVerfG* Maßnahmen ausschließlich zur Gefahraufklärung. Art. 11a PAG-E geht allerdings über die reine Gefahraufklärung hinaus und schafft

1 PAG-Kommission, Abschlussbericht, 2019, Internet: https://www.pag.bayern.de.
2 GVBl. 2017, S. 388.
3 Landtags-Drucksache 17/12699.
4 Landtags-Drucksache 18/13716, S. 22.
5 *BVerfG* vom 27. Mai 2020, Az. 1 BvR 1873/13 und 1 BvR 2618/13 – Bestandsdatenauskunft II.
6 *BVerfGE* 141, 220, 270 ff. Rn. 108 ff. – BKAG.
7 *BVerfG* vom 27. Mai 2020, Az. 1 BvR 1873/13 und 1 BvR 2618/13 – Bestandsdatenauskunft II.

eine Generalklausel in Form von Beseitigungs- bzw. Verhinderungsmaßnahmen, die einen Eingriff in den Kausalverlauf zulassen.

Gleichwohl begrüße ich aus Gründen der Rechtssicherheit die Ergänzung des Art. 11 PAG-E um eine Legaldefinition der konkreten Gefahr.

2.2 In welchen praktischen Fällen sehen Einsatzleiter die Möglichkeit, von den erweiterten Befugnissen und dem Begriff der „drohenden Gefahr" Gebrauch zu machen?

Hierzu kann keine Aussage getroffen werden.

3. Der Begriff der „konkreten Gefahr" wird nunmehr im Gesetz selbst definiert (Art. 11 Abs. 1 Satz 2 PAG-E). Das Verhältnis zwischen „konkreter" und „drohender" Gefahr wird zudem durch die gesonderte Verortung der drohenden Gefahr in einem neuen Art. 11a sowie einer klareren Formulierung in Art. 11a Abs. 1 PAG-E deutlich gemacht.

3.1 Sehen Sie durch diese Anpassungen die Prüfungsreihenfolge der Gefahrenkategorien als hinreichend konkretisiert an?

Die Empfehlung[8] der PAG-Kommission geht dahin, ein Stufen- bzw. Rangverhältnis herzustellen und damit das Einschreiten aufgrund einer drohenden Gefahr für nachrangig zu erklären. Dies dürfte nun mit dem gewählten Wortlaut und der gewählten Systematik der beiden Generalklauseln in Art. 11 PAG-E und Art. 11a PAG-E erfüllt sein.

Ein solches Rangverhältnis zwischen konkreter und drohender Gefahr soll nach Vorstellung[9] der PAG-Kommission aber auch sämtliche Spezialbefugnisse betreffen, die ein Einschreiten entweder aufgrund einer konkreten oder einer drohenden Gefahr legitimieren. Auch wenn nach der Gesetzesbegründung[10] das *„dargestellte Regel-Ausnahme-Verhältnis zwischen konkreter und drohender Gefahr [gilt] auch für alle Spezialbefugnisse, bei denen eine entsprechende Abgrenzung vorzunehmen ist, entsprechend"* gelten solle, kann ich persönlich die Umsetzung dieser Absicht im Gesetz selbst nicht erkennen. Der Wortlaut der Spezialbefugnisse – die ein Einschreiten aufgrund einer konkreten wie auch drohenden Gefahr zulassen *(„einer Gefahr oder einer drohenden Gefahr")* – impliziert vielmehr ein Nebeneinander beider Gefahrenkategorien.

3.2 Sind die in Art. 11a Abs. 1 PAG-E enthaltenen unbestimmten Rechtsbegriffe „in absehbarer Zeit" und „Angriffe von erheblicher Intensität oder Auswirkungen" aus Ihrer Sicht für die Praxis und Rechtsanwendung hinreichend bestimmt.

Aus Sicht für die Praxis und die Rechtsanwendung sind die Rechtsbegriffe „in absehbarer Zeit" und „Angriffe von erheblicher Intensität oder Auswirkungen" nicht hinreichend bestimmt.

8 PAG-Kommission, Abschlussbericht, 2019, S. 36, Internet: https://www.pag.bayern.de.
9 PAG-Kommission, Abschlussbericht, 2019, S. 37, Internet: https://www.pag.bayern.de.
10 Landtags-Drucksache 18/13716, S. 21.

Die Staatsregierung brachte 2017 einen Gesetzesentwurf zu effektiveren Überwachung gefährlicher Personen[11] in den Landtag ein, der den Begriff der drohenden Gefahr in Art. 11 Abs. 3 PAG lediglich auf gefährliche Personen im Sinne von mutmaßlichen Terroristen, Amokläufern und vergleichbaren Anlasspersonen bezog. In diesem Sinne bezog sich der Begriff der drohenden Gefahr ausschließlich auf in absehbarer Zeit zu erwartende Gewalttaten von erheblicher Intensität und Auswirkung.

Mit einem Änderungsantrag[12] wurde das Tatbestandsmerkmal „Gewalttaten" durch „Angriffe" ersetzt. Bereits hierzu habe ich erhebliche Bedenken hinsichtlich der Bestimmtheit geäußert. Insbesondere lässt der Begriff „Angriff" weitere Begehungsweisen auch der Alltagskriminalität und im IT-Bereich zu. Der Anwendungsbereich der Vorschrift wird daher deutlich erweitert und geht damit über das ursprüngliche Ansinnen, insbesondere terroristische Anschläge und Amoktaten zu verhindern, hinaus.

4. Aufgrund der Entscheidung des BVerfG vom 18.12.2018 (Az. 1 BvR 142/15 – Kfz-Kennzeichenkontrollen 2) wurde Art. 13 Abs. 1 Nr. 4 PAG-E angepasst.

   Wie bewerten Sie die Befugnisse der Polizei unter verfassungsgerichtlichen Gesichtspunkten und hier insbesondere die Formulierung „(1) Die Polizei kann die Identität einer Person feststellen … 4. an einer polizeilichen Kontrollstelle, die eingerichtet worden ist, *a) … b) zum Schutz von gefahrenträchtigen Großereignissen oder c) eingebunden in spezifische polizeiliche Ermittlungsstrategien der Gefahrenabwehr*" im Hinblick auf das verfassungsrechtliche Bestimmtheitsgebot?

Diese Befugnisausweitung sehe ich unter verfassungsrechtlichen und datenschutzrechtlichen Gesichtspunkten als äußerst problematisch an. Mit den Ergänzungen werden die polizeilichen Befugnisse deutlich erweitert. So bestünde – vor allem im großstädtischen Bereich – die Möglichkeit, insbesondere an Wochenenden, an denen Fußballspiele oder Konzerte stattfinden, die Identität jeder Person festzustellen oder das Kfz-Kennzeichen jedes PKW's automatisiert zu erfassen und abzugleichen (Art. 13 Abs. 1 Nr. 4 PAG-E i.V.m. Art. 39 PAG), die bzw. das sich im näheren Umkreis einer solchen Veranstaltung aufhält bzw. bewegt. Das Erfordernis einer solchen Regelung aus polizeilicher Sicht ist – jedenfalls derzeit – nicht erkennbar.

Im Hinblick auf das verfassungsrechtliche Bestimmtheitsgebot sind die Ergänzungen um Buchst. b und c zu unbestimmt und es fehlt an der Erforderlichkeit für den Erlass dieser gesetzlichen Regelungen. Ein wesentlicher Teil der in der Gesetzesbegründung[13] aufgezeigten Beispiele kann bereits unter die bestehende Vorschrift subsumiert werden. Art. 13 Abs. 1 Nr. 4 Buchst. a PAG-E bzw. Art. 13 Abs. 1 Nr. 4 PAG derzeitige Fassung regelt jedenfalls die angesprochenen Kriminalitätsschwerpunkte, wie Menschenhandel, serienmäßig begangene Brandstiftungen oder gehäuft auftretende Wohnungseinbruchdiebstähle, vgl. § 100a Abs. 2 Nr. 1 Buchst. i, j, u Strafgesetzbuch (StGB). Ferner sehe ich es als kritisch an, dass unter ein „gefahrenträchtiges Großereignis" eine Vielzahl von Veranstaltungen gefasst werden kann. Damit werden die Möglichkeiten einer Identitätsfeststellung massiv ausgeweitet, ohne dass bislang die polizeipraktischen Bedürfnisse hierfür in nachvollziehbarere Weise dargelegt worden sind.

11 Landtags-Drucksache 17/16299.
12 Landtags-Drucksache 17/17058.
13 Landtags-Drucksache 18/13716, S. 25.

Intransparent ist überdies, was man sich unter „spezifische polizeiliche Ermittlungsstrategien der Gefahrenabwehr“ vorzustellen hat. Nicht zuletzt deshalb, da davon auszugehen ist, dass derartige Strategien als Verschlusssache eingestuft sind, ist eine Ausweitung des Art. 13 PAG an dieser Stelle aus datenschutzrechtlicher Sicht nicht akzeptabel.

5.1 Wie beurteilen Sie die geänderten Regelungen zur DNA-Analyse nach Art. 14 Abs. 3 bis 6, Art. 32a PAG-E zu Gefahrenabwehrzwecken?

(1) Art. 14 Abs. 3 bis 6 PAG-E

Zu Art. 14 Abs. 3 bis 6 PAG-E ist generell Folgendes anzumerken: Die PAG-Kommission hat in ihrem Abschlussbericht[14] herausgearbeitet, dass der Befugnis ein eher geringer praktischer Anwendungsbereich inne wohnt. Die Empfehlung der PAG-Kommission[15] geht vorrangig dahingehend, die Befugnis aufgrund ihrer geringen Bedeutung aufzuheben.

Ich habe im Jahr 2020 zusätzlich zur Überprüfung durch die PAG-Kommission den Vollzug der neu eingeführten Befugnis des Art. 14 Abs. 3 und 4 PAG – über den Berichtszeitraum der PAG-Kommission hinaus – geprüft. Insgesamt wurden mir auf meine Anfrage durch die Polizeipräsidien neben den neun Fällen, die bereits im Abschlussbericht der PAG-Kommission[16] beschrieben sind, weitere vier Fälle aus dem präventivpolizeilichen Anwendungsbereich mitgeteilt. In insgesamt elf der 13 Fälle stützte die Polizei die Befugnis zur Entnahme der DNA auf eine Freiwilligkeits-/Einverständniserklärung. Die betreffenden Körperzellen wurden in allen 13 Fällen nach Übersendung an das Bayerische Landeskriminalamt und dortiger Auswertung vernichtet. Alle Polizeiverbände wiesen einstimmig darauf hin, dass Art. 14 Abs. 5 PAG keine feste Speicherdauer vorsehe, weswegen die verantwortlichen Polizeidienststellen jeweils eine Einzelfallprüfung in Bezug auf eine etwaige Löschung betreffender Daten durchzuführen hätten, sobald die Voraussetzungen des Art. 14 Abs. 3 PAG nicht mehr vorlägen.

Die Prüfung zeigt, dass die überwiegend geübte Praxis des Rückgriffs auf Freiwilligkeitserklärungen den in Art. 14 Abs. 3 Satz 4 PAG geregelten Richtervorbehalt umgeht. Sie widerspricht zudem Erwägungsgrund 35 RLDSJ[17]. Danach können die zuständigen Behörden bei der Wahrnehmung der ihnen übertragenen Aufgaben, Straftaten zu verhüten, zwar natürliche Personen auffordern oder anweisen, ihren Anordnungen nachzukommen. Kommt die betroffene Person dieser Anweisung nach, stellt eine solche Einwilligung aber keine rechtliche Grundlage für die Verarbeitung personenbezogener Daten dar. Denn wenn eine betroffene Person aufgefordert wird, einer rechtlichen Verpflichtung nachzukommen, hat sie keine echte Wahlfreiheit, weshalb ihre Reaktion nicht als freiwillig abgegebene Willensbekundung betrachtet werden kann.

14 PAG-Kommission, Abschlussbericht, 2019, S. 41 f., Internet: https://www.pag.bayern.de.
15 PAG-Kommission, Abschlussbericht, 2019, S. 43, Internet: https://www.pag.bayern.de.
16 PAG-Kommission, Abschlussbericht, 2019, S. 40 f., Internet: https://www.pag.bayern.de.
17 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.

Die nun vorgenommene Gesetzesänderung zieht den Richtervorbehalt aus Transparenzgründen in Art. 14 Abs. 3 Satz 1 PAG-E vor. Ich befürchte allerdings, dass selbst die Regelung des Richtervorbehalts an einer präsenteren Stelle im Gesetz die geübte Vollzugspraxis nicht wesentlich ändert.

Ferner hatte ich bereits bei der Beteiligung im Rahmen des PAG-Neuordnungsgesetzes des bayerischen Polizeirechts (erfolglos) darauf hingewiesen[18], dass angesichts des mit der molekulargenetischen Untersuchung einhergehenden erheblichen Eingriffs in das Recht auf informationelle Selbstbestimmung eine Regelung zur Speicherdauer erforderlich ist. Art. 14 Abs. 6 Satz 1 PAG-E regelt nun die Aufbewahrungsdauer der entnommenen Körperzellen. Art. 14 Abs. 6 Satz 2 PAG-E regelt die Speicherdauer der ED-Unter- lagen, wozu auch die DNA-bezogenen Feststellungen gehören[19]. Allerdings sieht Art. 14 Abs. 6 Satz 2 PAG-E – wie auch die derzeitige Regelung des Art. 14 Abs. 5 PAG – vor, dass die erkennungsdienstlichen Unterlagen dann zu vernichten sind, wenn die Voraussetzungen nach Art. 14 Abs. 1, 3 oder Abs. 4 PAG-E entfallen sind. Wann nun die Voraussetzungen nach Art. 14 Abs. 1, 3 oder 4 PAG-E entfallen sind, wird nicht geregelt. Angesichts der Eingriffsintensität der Maßnahmen und der vom *BVerfG* entwickelten Wesentlichkeitslehre sollten meines Erachtens weitere flankierende Schutzmaßnahmen im Gesetz selbst geregelt werden und nicht etwaigen Vollzugsvorschriften vorbehalten bleiben.

Zu Art. 14 Abs. 4 PAG-E vgl. Antwort zu Frage 5.2.

(2) Art. 32a PAG-E

Zu begrüßen ist die Streichung des derzeit noch enthaltenen Untersuchungszwecks der biogeographischen Herkunft.

Unklar ist aber die Relevanz dieser Maßnahme in Abgrenzung zur strafprozessualen Parallelvorschrift des § 81e Abs. 2 Strafprozessordnung (StPO)[20].

Die Befugnis in Art. 32a PAG-E geht in der beabsichtigten Fassung über die derzeitige Fassung des Art. 32 Abs. 1 Satz 2 PAG hinaus. So fehlt es der Entwurfsfassung an der einschränkenden Subsidiaritätsklausel *„…wenn die Abwehr der Gefahr auf andere Weise aussichtslos oder wesentlich erschwert wäre."* Demnach ist bei Vorliegen einer bloßen abstrakten Gefahr bereits die Durchführung einer solchen Maßnahme zulässig.

Zudem lassen die verfahrensrechtlichen Regelungen nach wie vor weitere bedeutende grundrechtsflankierende Vorschriften vermissen. Für die nun neu eingeführte Speicherung der DNA-Identifizierungsmuster in Dateien, vgl. Art. 32a Abs. 2 PAG-E, ist die gesetzliche Regelung zur Speicherdauer der DNA-Identifizierungsmuster unzureichend.

18 Vgl. meine Stellungnahme unter https://www.datenschutz-bayern.de/nav/0710.html.

19 Landtags-Drucksache 17/20425, S. 42.

20 Vgl. auch PAG-Kommission, Abschlussbericht, 2019, S. 48, Internet: https://www.pag.bayern.de.

5.2 Wurden die Voraussetzungen für die Identifizierung eines Verstorbenen oder einer hilflosen Person mittels molekulargenetischer Untersuchung außerhalb strafrechtlicher Ermittlungsverfahren Ihrer Einschätzung nach hinreichend geregelt (Art. 14 Abs. 4 PAG-E)?

Eine hinreichende Regelung liegt – sofern man deren praktische Relevanz anerkennt – in Art. 14 Abs. 4 PAG-E nicht vor.

Im Falle des Auffindens einer unbekannten Leiche ist eine solche Befugnis nicht erforderlich. So ist eine Identifizierung nach § 88 StPO möglich, auch wenn kein Anfangsverdacht für eine Straftat im Raum steht. *„Bestehen bei einem Todesfall Anhaltspunkte für einen nicht natürlichen Tod oder wird eine unbekannte Leiche gefunden, so läuft (auch bei einem zunächst noch fehlenden Straftatverdacht) ein Todesermittlungserfahren i.e.S. an. Dieses basiert im Wesentlichen auf § 159 StPO und stellt noch kein übliches strafprozessuales Ermittlungsverfahren dar; vielmehr handelt es sich dabei um ein Verfahren eigener Art (so BGHSt 49, 29). Zweck dieses besonderen Verfahrens ist die vorsorgliche Beweissicherung für den hypothetisch möglichen Fall, dass der Tod durch die Straftat eines anderen herbeigeführt worden sein sollte. Ferner ist die genaue Todesursache abzuklären und ggf. die Identität des Verstorbenen festzustellen."*[21] Gem. § 159 StPO besteht die Pflicht von Polizei- und Gemeindebehörden zur sofortigen Anzeige an die Staatsanwaltschaft oder an das Amtsgericht, wenn *„der Leichnam eines Unbekannten gefunden"* wird.

Zu berücksichtigen ist in diesem Zusammenhang auch, dass eine dem Polizeirecht typisch innewohnende Gefahrenlage bei der Identifizierung von Leichen nicht gegeben ist. In der Regel handelt es sich hier nicht um eine Form der Gefahrenabwehr.

6. Die zulässige Höchstdauer einer Gewahrsamsanordnung soll unter Berücksichtigung der Vorschläge der PAG-Kommission und der Erfordernisse der Polizeipraxis auf längstens einen Monat reduziert werden und der Präventivgewahrsam soll künftig nur bis zu einer Gesamtdauer von zwei Monaten verlängert werden dürfen (Art. 20 Abs. 2 Satz 2 PAG-E).

6.1 Sind Ihrer Auffassung nach durch diese Änderungen die geäußerten verfassungsrechtlichen Bedenken ausgeräumt?

Art. 20 Abs. 2 PAG-E ist im Vergleich zur derzeitigen Gesetzeslage zu begrüßen und setzt auch teils die Empfehlung der PAG-Kommission[22] um.

Allerdings sind die grundrechtsflankierenden Vorschriften nur unzureichend. Art. 97 Abs. 2 PAG-E sieht vor, dass die richterliche Entscheidung ohne persönliche Anhörung der in Gewahrsam genommenen Person ergehen kann, wenn diese rauschbedingt nicht in der Lage ist, den Gegenstand der persönlichen Anhörung ausreichend zu erfassen und zur Feststellung der entscheidungserheblichen Tatsachen beizutragen. Art. 97 Abs. 2 Satz 2 PAG-E regelt im Anschluss daran, dass in diesen Fällen die richterliche Entscheidung mit Erlass wirksam wird und es hierzu keiner Bekanntgabe an die in Gewahrsam genommene Person bedarf. Diese Regelung begegnet erheblichen Bedenken. Der Bundesgesetzgeber hat zwar in § 422 Abs. 2 Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG) vorgesehen, dass ein Beschluss – abweichend von § 422 Abs. 1 FamFG – nicht erst mit Rechtskraft, sondern bereits aufgrund sofortiger Anordnung

21 *Kastner* in Möllers Polizei-WB, 3. Auflage 2018, Todesermittlungsverfahren.

22 PAG-Kommission, Abschlussbericht, 2019, S. 59 f., Internet: https://www.pag.bayern.de.

wirksam werden kann. Der Bundesgesetzgeber überantwortet diese Entscheidung aber dem Gericht und ordnet nicht von Gesetzes wegen die sofortige Wirksamkeit an. Ich gehe davon aus, dass die bundesrechtlichen Ausnahmeregelung des § 422 Abs. FamFG abschließend und eng auszulegen ist. Sie lässt daher keine landesrechtliche Durchbrechung – zumal zu Lasten des Betroffenen – zu. Auch die Einfügung des Satzes 3 in Art. 97 Abs. 2 PAG-E sehe ich kritisch. § 419 Abs. 1 Satz 2 FamFG erachtet die Bestellung eines Verfahrenspflegers gerade für erforderlich, *„wenn von der persönlichen Anhörung des Betroffenen abgesehen werden soll. Die Vorschrift betrifft damit die Fälle, in denen die Anhörung wegen erheblicher gesundheitlicher Gefahren für den Betroffenen unterbleiben soll oder der Betroffene nicht ansprechbar ist."*[23]

6.2 Ist die Regelung geeignet, um die von einem terroristischen Gefährder ausgehende Gefahr zu beseitigen?

Hierzu kann keine Aussage getroffen werden.

6.3 Wie beurteilen Sie darüber hinaus die Änderungen zum anwaltlichen Beistand?

Die Einfügung des Art. 97 Abs. 4 PAG-E ist begrüßenswert.

7. Art. 33 Abs. 4 Satz 5 PAG-E führt im Zusammenhang mit dem Einsatz der Body-Cam in Wohnungen einen Richtervorbehalt für die Verwertung der erlangten Erkenntnisse zum Zwecke der Gefahrenabwehr ein (Art. 33 Abs. 4 Satz 5 PAG-E).

7.1 Wie beurteilen Sie diesen zusätzlichen Rechtsschutz für die Betroffenen dieser Maßnahme?

Zunächst möchte ich hervorheben, dass die PAG-Kommission in ihrem Abschlussbericht[24] empfiehlt, *„Aufzeichnungen nach Art. 33 Abs. 4 PAG in Wohnungen unter den Vorbehalt einer unverzüglich nachzuholenden richterlichen Entscheidung zu stellen. Zudem sollte im Gesetz vorgesehen werden, dass die von der Maßnahme betroffenen Personen eine rechtsmittelfähige Bescheinigung ausgehändigt bekommen, etwa in Anlehnung an die Regelung nach Art. 24 Abs. 4 und 6 PAG…"*. Dieser Empfehlung möchte der Gesetzentwurf mit Art. 33 Abs. 4 Satz 4 und 5 PAG-E nachgekommen sein. Diese Einschätzung teile ich persönlich nicht.

Der Gesetzentwurf stellt auf die Verwertbarkeit der erlangten Aufnahmen in Wohnungen ab und zwar lediglich zum Zwecke der Gefahrenabwehr. Die Empfehlung der PAG-Kommission geht aber dahin, die Zulässigkeit der Aufnahme in Wohnungen per se einer richterlichen Entscheidung zu unterstellen. Demnach mangelt es der Norm nach wie vor am verfassungsrechtlich zwingend erforderlichen Richtervorbehalt. Art. 33 Abs. 4 Satz 3 PAG unterfällt – entgegen der Annahme in der Gesetzesbegründung[25] – dem Maßstab des Art. 13 Abs. 4 Grundgesetz (GG). Vielmehr müsste daher – da eine richterliche Entscheidung in vielen Fällen erst nachholbar sein wird – die Maßnahme nach Art. 33 Abs. 4 Satz 3 PAG einer unverzüglichen richterlichen Entscheidung zugeführt werden.

23 *Günter,* in BeckOK FamFG, 34. Ed. 1.4.2020, § 419 Rn. 7.

24 PAG-Kommission, Abschlussbericht, 2019, S. 65, Internet: https://www.pag.bayern.de.

25 Landtags-Drucksache 18/13716, S. 29.

Zudem liefe die richterliche Überprüfung mit dem beabsichtigten Wortlaut des Art. 33 Abs. 4 Satz 5 PAG-E in zahlreichen Fällen ins Leere. Denn eine Überprüfung ist nur für Fälle der Verwertbarkeit der Erkenntnisse zum Zwecke der Gefahrenabwehr vorgesehen; dass im Regelfall aber eine Verwertung der Erkenntnisse im Rahmen der Strafverfolgung vorliegen wird, bleibt unberücksichtigt und ungeregelt.

Die Geräte dienen überwiegend dem Eigenschutz der Polizeibeamteninnen und -beamten.[26] Daraus wird deutlich, dass im Regelfall eine Verwertung im Rahmen der Strafverfolgung erfolgen soll. Der Hinweis in der Gesetzesbegründung[27], dass im Hinblick auf die Verwertung im Rahmen des Strafverfahrens die allgemeinen Regelungen der Strafprozessordnung gelten sollen und es deshalb keiner gesonderten Aufnahme einer nachträglichen richterlichen Überprüfung auch für diese Fälle bedurfte, geht fehl. Art. 13 Abs. 4 GG sieht nicht lediglich eine richterliche Überprüfung der Verwertbarkeit der Aufnahmen vor, sondern bereits einen Richtervorbehalt für die Maßnahme an sich – also einen Richtervorbehalt für die Erhebung personenbezogener Daten. Eine Strafrichterin/ein Strafrichter überprüft nicht die Zulässigkeit der Maßnahme als solche, sondern entscheidet ausschließlich über die Verwertbarkeit der gewonnenen Bildaufzeichnungen als Beweismittel nach strafprozessualen Regeln, was sich in der Regel nach ganz anderen Maßstäben richtet. In diesem Zusammenhang ist auch zwingend Art. 95 Abs. 5 Satz 2 PAG-E anzupassen. Denn die jedenfalls einzuholende richterliche Bestätigung i.S.v. Art. 95 Abs. 5 Satz 1 PAG-E läuft regelmäßig wegen Art. 95 Abs. 5 Satz 2 PAG-E ins Leere.

Zudem ist der Katalog des Art. 52 Abs. 1 Satz 1 PAG um den Body-Cam-Einsatz in Wohnungen nach Art. 33 Abs. 4 Satz 3 PAG zu ergänzen. Denn die Verwendung von Body-Cams in Wohnungen ist am Maßstab des Art. 13 Abs. 4 GG zu messen mit der Folge, dass der Landtag – entsprechend Art. 13 Abs. 6 GG – regelmäßig über diese eingriffsintensive Maßnahme zu unterrichten ist.

7.2 Wie bewerten Sie diesbezüglich die besondere Mitteilung an den Betroffenen über den Einsatz von Body-Cams in Wohnungen (Art. 33 Abs. 4 Satz 4 PAG-E)?

Der Gesetzentwurf geht auf die Empfehlung der PAG-Kommission[28] nach einer rechtsmittelfähigen Bescheinigung in Anlehnung an die Regelung des Art. 24 Abs. 4 und 5 PAG nur unzureichend ein.

Eine Umsetzung dieser Dokumentation kann nach der Gesetzesbegründung[29] *„etwa durch die Übergabe oder Einwurf eines Informationsblattes“* erfolgen. Ein Informationsblatt ist nicht mit einer rechtsmittelfähigen Bescheinigung gleichzusetzen. Die Empfehlung der PAG-Kommission zielt nach meinem Verständnis darauf ab, der oder den betroffenen Personen die Möglichkeit einer gerichtlichen Überprüfung einzuräumen. Mit der Aushändigung eines Informationsblattes wird diese Empfehlung nur unzureichend umgesetzt.

26 Landtags-Drucksache 17/20425, S. 51.
27 Landtags-Drucksache 18/13716, S. 29.
28 PAG-Kommission, Abschlussbericht, 2019, S. 65, Internet: https://www.pag.bayern.de.
29 Landtags-Drucksache 18/13716, S. 29.

Würde aber die richterliche Entscheidung – Anordnung oder in Eilfällen die richterliche Bestätigung – für Aufnahmen in Wohnungen per se und nicht nur für deren Verwertbarkeit umgesetzt werden, so würde dem Betroffenen auch eine Rechtsmittel an die Hand gegeben, da ein rechtsmittelfähiger richterlicher Beschluss vorläge.

7.3 Wie beurteilen Sie darüber hinaus die Beibehaltung der Prerecording-Funktion (Art. 33 Abs. 4 Satz 5 = Art. 33 Abs. 4 Satz 7 PAG-E) insbesondere im Lichte des LS 1 der Entscheidung des BVerfG v. 18.12.2018 (Az. 1 BvR 142/15 – Kfz-Kennzeichenkontrollen 2)?

Im Lichte des Leitsatzes 1 der Entscheidung des *BVerfG* vom 18. Dezember 2018 (Az. 1 BvR 142/15) ist die Prerecording-Funktion als Eingriff in das Grundrecht auf informationelle Selbstbestimmung zu sehen. Die Prerecording-Funktion kann nach der Entscheidung des *BVerfG* damit nicht mehr als grundrechtneutral eingestuft werden. Dies wirft verfassungsrechtliche Fragen auf.

8. Welche Bedeutung haben die Regelungen zum Richtervorbehalt im vorliegenden Gesetz und sind sie praxisnah umsetzbar?

Hierzu kann keine Aussage getroffen werden.

9. Neben der Einführung neuer Richtervorbehalte erfolgt zusätzlich eine Aufzählung derjenigen Maßnahmen, die einem grundsätzlichen Richtervorbehalt unterliegen, gebündelt an einer zentralen Stelle im Gesetz (Art. 94 PAG-E). Ergänzend wird der grundsätzliche Richtervorbehalt auch in den jeweiligen Befugnisnormen hervorgehoben. Wie wirkt sich diese Gestaltung Ihrer Ansicht nach auf die Rechtsanwendung aus?

Laut Gesetzesbegründung[30] soll hiernach eine erhöhte Anwenderfreundlichkeit und Übersichtlichkeit erreicht werden. Ob dies gelingt, wird die Praxis zeigen.

10. Wie bewerten Sie die Ergänzung und Zusammenfassung der verfahrensrechtlichen Vorschriften in einem neuen Abschnitt an zentraler Stelle im Gesetz (IX. Abschnitt „Gerichtliches Verfahren"), insbesondere hinsichtlich der Kohärenz und der Erleichterung der Anwendung?

Hierzu kann derzeit noch keine Aussage getroffen werden. Ob eine Erleichterung der Anwendung damit einhergehen wird, wird die Praxis zeigen.

11. Wie ist die Möglichkeit der Rechtsbeschwerde beim Bayerischen Obersten Landesgericht zu bewerten?

Hierzu kann keine Aussage getroffen werden.

12. Ist der Schutz des anwaltlichen Berufsgeheimnisses durch das Gesetz ausreichend gewährt, obgleich eine Generalklausel entsprechend § 62 BKAG fehlt?

Eine dem § 62 BKAG ähnelnde Vorschrift findet sich in Art. 49 PAG. Art. 49 PAG regelt aber den Schutz des anwaltlichen Berufsgeheimnisses nur unzureichend. Art. 49 Abs. 1 PAG (Erhebungsebene) lässt einige verdeckte Maßnahmen (Art. 42 Abs. 2 PAG, Art. 45 Abs. 2 PAG, Art. 37 Abs. 1 PAG, Art. 38 Abs. 1 PAG) unberücksichtigt,

30 Landtags-Drucksache 18/13716, S. 37.

obwohl diese ebenfalls intensiv in das Vertrauensverhältnis eingreifen können. Ähnlich verhält es sich mit Art. 49 Abs. 2 PAG, der bislang nur den Abruf der Vorratsdaten nach Art. 43 Abs. 2 Satz 2 PAG speziell regelt. Eine entsprechende Ausschlussregelung ist jedoch auch für das Auskunftsverlangen gegenüber Diensteanbietern vorzusehen, wenn dieses Verkehrsdaten nach Art. 43 Abs. 2 Satz 1 PAG zum Gegenstand hat. Schließlich ist auch der Katalog des Art. 49 Abs. 5 PAG (Auswertungsebene) um Art. 42 Abs. 2 PAG zu ergänzen.

13. Die im Zeugenschutz bereits etablierten Grundsätze und Standards für umfassende Schutzmaßnahmen werden in Art. 92 PAG-E für den Bereich des operativen Opferschutzes festgeschrieben. Somit besteht nun die explizite Rechtsgrundlage, die (auch unbeabsichtigte) Preisgabe personenbezogener Daten zu schützender Personen an Dritte zu verhindern. Wie bewerten Sie diese Ergänzungen hinsichtlich des Ziels eines möglichst effektiven Opferschutzes?

Grundsätzlich sind Vorschriften zum Schutz personenbezogener Daten in diesem Zusammenhang zu begrüßen. Nicht ganz klar ist der Anwendungsbereich dieser Vorschrift; denn handelt es sich um schützenswerte Zeugen gilt das Zeugenschutz-Harmonisierungsgesetz (ZSHG). Wann nun eine Person zu einer „zu schützenden Person“ wird, kann weder dem Gesetzestext noch der Begründung[31] entnommen werden.

Ob die Vorschrift in der Praxis einen effektiven Opferschutz ermöglicht, kann derzeit (noch) nicht beurteilt werden.

14. Welche Regelungen des PAG sind ihrer Auffassung nach darüber hinaus reformbedürftig? Können Sie dies kurz begründen bspw. an den Regelungen über die Vorladung (Art. 15 PAG), die Durchsuchung von Speichermedien (Art. 22 Abs. 2 PAG), Sicherstellung (Art. 25 PAG), die Videoüberwachung (Art. 33 PAG), die Postsicherstellung (Art. 35 PAG), die Besonderen Mittel der Datenerhebung (Art. 36 PAG), den Einsatz von VE und VP (Art. 37, 38 PAG), die Ausschreibung zur polizeilichen Beobachtung (Art. 40 PAG), den Einsatz technischer Mittel in Wohnungen (Art. 41 PAG), die Betreten und Durchsuchung der Wohnung des Betroffenen bei Telekommunikationsüberwachungsmaßnahmen (Art. 44 Abs. 1 Satz 5 PAG), die Online-Durchsuchung (Art. 45 PAG), den Einsatz von unbemannten Luftfahrtsystemen (Art. 47 PAG), das Verarbeitungsverbot nach Übermittlung (Art. 55 Abs. 3 Satz 5 PAG), den Abruf nachrichtendienstlicher Daten durch die Polizei (Art. 60 Abs. 3 PAG)?

Im Rahmen des Gesetzgebungsverfahrens zum Gesetz zur Neuordnung des bayerischen Polizeirechts (PAG-Neuordnungsgesetz) vom 18. Mai 2018[32] habe ich bereits ausführlich aus datenschutzrechtlicher Sicht Stellung zum Reformbedarf einzelner Vorschriften genommen. Meine Stellungnahme zum PAG-Neuordnungsgesetz ist auf meiner Homepage[33] abrufbar. Insbesondere möchte ich aber folgende Aspekte nochmals hervorheben:

(1) Akkreditierung

Immer wieder – zuletzt bei den Vorbereitungen zur UEFA EURO 2020 in München – spielt die Thematik der Akkreditierung zu Großveranstaltungen eine Rolle. Wiederholt

31 Landtags-Drucksache 18/13716, S. 36 f.
32 GVBl. 2018, S. 301.
33 https://www.datenschutz-bayern.de/nav/0710.html.

habe ich die Schaffung einer bereichsspezifischen Rechtsgrundlage für sämtliche Fallkonstellationen eines Akkreditierungsverfahrens gefordert.

Art. 32 Abs. 1 Satz 1 Nr. 1b) PAG regelt nunmehr zwar ausdrücklich die Datenerhebung zu Zwecken des Personenschutzes, insbesondere die Überprüfung von Dienstleistungspersonal im Zusammenhang mit Veranstaltungen. Ausweislich der Gesetzesbegründung[34] zu Art. 32 Abs. 1 Satz 1 Nr. 1b) PAG wurde diese Alternative als besondere Form der Datenerhebung gerade für Überprüfungen bei *„Veranstaltungen, bei denen polizeiliche Schutzpersonen zugegen sind"* geschaffen. Die Rechtsgrundlage kann damit nur zur Anwendung kommen, wenn tatsächlich entsprechende polizeiliche Schutzpersonen zugegen sind oder zumindest damit zu rechnen ist.

Da Akkreditierungsverfahren einen erheblichen Eingriff in Grundrechte der Betroffenen darstellen, insbesondere in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1, Art. 1 Abs. 1 GG) und letztlich auch in die durch Art. 12 Abs. 1 GG geschützte Berufsausübungsfreiheit – gegebenenfalls auch in Art. 5 Abs. 1 GG –, müssen die Rechte und Freiheiten der betroffenen Personen durch ein gesetzlich geregeltes transparentes Verfahren mit entsprechenden Informations- und Anhörungsrechten gewährleistet werden. Es muss dabei der betroffenen Person rechtzeitig die Möglichkeit eröffnet werden, sich persönlich zu den für die Entscheidung erheblichen Tatsachen zu äußern. Dies ist schon aus verfassungsrechtlicher Sicht und aufgrund des Rechts der betroffenen Person an einem geordneten, rechtsstaatlichen Verfahren unerlässlich.

(2) Durchsuchung von Speichermedien (Art. 22 Abs. 2 PAG)

Nach Art. 22 Abs. 2 Satz 1 PAG können vom Durchsuchungsobjekt räumlich getrennte Speichermedien durchsucht werden, wenn die Durchsuchung ein „elektronisches Speichermedium" betrifft. Art. 22 Abs. 2 Satz 1 PAG geht demnach davon aus, dass eine Durchsuchung elektronischer Speichermedien unter den Voraussetzungen des Art. 22 Abs. 1 PAG zulässig ist. Diese Rechtsauffassung teile ich nicht. Art. 22 Abs. 1 PAG erlaubt lediglich die Durchsuchung von „Sachen". Sachen in diesem Sinne sind nur „körperliche Gegenstände" gemäß § 90 BGB[35]. Elektronische Daten sind als solche keine Sachen, da ihnen die für den Sachbegriff kennzeichnende abgrenzbare Körperlichkeit fehlt[36]. Auch das Polizeiaufgabengesetz selbst geht von der mangelnden Sacheigenschaft von Daten aus (siehe Art. 25 Abs. 3 Satz 4 PAG: *„Die Bestimmungen … gelten unter Berücksichtigung der unkörperlichen Natur von Daten sinngemäß."*). Nur der Datenträger ist eine Sache i.S.v. § 90 BGB. Dies rechtfertigt aber keine Durchsuchung der darauf abgelegten Daten. Es stellt sich ferner die Frage nach der Relevanz dieser Befugnis neben der repressiven Befugnis nach § 110 Abs. 3 Satz 1 StPO.

Eine Durchsuchung ist daher nur unter strengen Voraussetzungen, insbesondere nur zur „Abwehr einer Gefahr für ein bedeutendes Rechtsgut" zuzulassen. Zudem dürfen auf vom Durchsuchungsobjekt räumlich getrennte Speichermedien nur zugegriffen werden, „wenn andernfalls der Verlust der gesuchten Daten zu besorgen ist" (eine gleichlautende Einschränkung enthält auch § 110 Abs. 3 Satz 1 StPO, dem Art. 22 Abs. 2 PAG nachgebildet ist). Denn nur wenn ein Daten- und Beweismittelverlust zu

34 Landtags-Drucksache 17/20425, S. 50.

35 Siehe *Schmidbauer*, in: Schmidbauer/Steiner, PAG, 5. Aufl., 2020, Art. 22 Rn. 4.

36 Siehe *Stresemann*, in: MüKo BGB, 8. Aufl., 2018, § 90 Rn. 25; *Fritzsche*, in BeckOK BGB, 57. Ed., Stand 1.11.2020, § 90 Rn. 25, 27.

befürchten ist, also das externe Speichermedium (z.B. Daten in der Cloud) nicht rechtzeitig gesichert werden kann, ist ein derart weitgehender Eingriff vertretbar. Weiterhin sieht die Regelung des Art. 22 Abs. 2 PAG bislang keinerlei Vorkehrungen zum Schutz von Daten vor, über deren Inhalt nach §§ 53, 53a StPO das Zeugnis verweigert werden könnte oder die dem Kernbereich privater Lebensgestaltung unterfallen. Ein Verweis auf Art. 49 BayPAG fehlt insoweit.

Darüber hinaus ist die Befugnis zur Durchsuchung elektronischer Speichermedien und Clouds unter einen Richtervorbehalt zu stellen. Zwar handelt es sich bei der Durchsuchung um eine offene Maßnahme. Aufgrund deren Eingriffsintensität hat jedoch grundsätzlich eine Richterin/ein Richter darüber zu entscheiden. Insbesondere die systematische Durchsuchung und Auswertung von Festplatten und Clouds mit Analysetools stellt einen erheblichen Grundrechtseingriff dar, der einem Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nahekommt. Mit der Durchsuchung von Sachen kann eine derart eingriffsintensive Maßnahme nicht gleichgesetzt werden. Auch § 110 Abs. 3 StPO setzt grundsätzlich eine von der Ermittlungsrichterin/von dem Ermittlungsrichter angeordnete Durchsuchung (§ 105 Abs. 1 StPO) voraus.

Zudem sollten Maßnahmen nach Art. 22 Abs. 2 PAG aufgrund ihrer Eingriffsintensität protokolliert und die betroffenen Inhaber im Falle ihrer Abwesenheit hierüber benachrichtigt werden.

(3) Sicherstellung (Art. 25 PAG)

Die in Art. 25 Abs. 3 PAG vorgesehene Befugnis zur Sicherstellung von Daten soll unter denselben Voraussetzungen zulässig sein wie die Sicherstellung von Sachen (Art. 25 Abs. 1 PAG) und Vermögensrechten (Art. 25 Abs. 2 PAG). Das halte ich jedoch für unvertretbar, da mit der Sicherstellung personenbezogener Daten und Zugangsdaten in das Grundrecht auf informationelle Selbstbestimmung eingegriffen wird, was nur in engen Grenzen erlaubt werden kann.

Die Befugnis ist unter einen Richtervorbehalt zu stellen. Zwar handelt es sich hierbei – ebenso wie bei der Durchsuchung nach Art. 22 Abs. 2 PAG – um eine offene Maßnahme. Aufgrund deren Eingriffsintensität hat jedoch grundsätzlich auch hierüber eine Richterin/ein Richter zu entscheiden. Denn der Entzug der Verfügungsgewalt des Inhabers über seine personenbezogenen Daten und Zugangsdaten stellt einen erheblichen Grundrechtseingriff dar, zumal mit der Sicherstellung der Daten regelmäßig auch eine Kenntnisnahme hiervon durch die Polizei einhergeht.

(4) Besonderen Mittel der Datenerhebung (Art. 36 PAG)

Über die bisherige Erweiterung des Richtervorbehalts hinaus ist auch der Einsatz technischer Mittel nach Art. 36 Abs. 1 Nr. 2 c), d) und e) PAG-E, sofern diese durchgehend länger als 24 Stunden oder an mehr als zwei Tagen durchgeführt werden sollen, unter einen Richtervorbehalt zu stellen (siehe auch § 64 Abs. 3 Nr. 2 BKAG).

(5) Abruf nachrichtendienstlicher Daten durch die Polizei (Art. 60 Abs. 3 PAG)

Die Abrufbefugnis des Art. 60 Abs. 3 Nr. 1 PAG sieht vor, dass die Polizei die Verfassungsschutzbehörden um die Übermittlung von mit nachrichtendienstlichen Mitteln erhobenen Daten *„zur Abwehr einer im Einzelfall bestehenden Gefahr oder einer drohenden Gefahr für ein bedeutendes Rechtsgut“* ersuchen darf. Die Datenübermittlungsbefugnis des Art. 25 Abs. 2 Satz 1 Nr. 1 Bayerisches Verfassungsschutzgesetz

(BayVSG) erlaubt eine Datenübermittlung hingegen nur *„zur Abwehr einer im Einzelfall bestehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben, Gesundheit oder Freiheit einer Person oder für Sachen von erheblichem Wert, deren Erhaltung im öffentlichen Interesse geboten ist“*. Diese vorgenannten Rechtsgüter entsprechen den Rechtsgütern des Art. 11a Abs. 2 Nr. 1, Nr. 2 und Nr. 4 PAG-E. Darüber hinaus sieht Art. 60 Abs. 3 Nr. 1 PAG jedoch auch die „drohende Gefahr“ als zulässigen Gefahrengrad vor. Demnach geht die Abrufbefugnis des Art. 60 Abs. 3 Nr. 1 PAG deutlich über die Voraussetzungen der Übermittlungsbefugnis des Art. 25 Abs. 2 Satz 1 Nr. 1 BayVSG hinaus und verstößt damit bereits gegen die Vorgaben des *BVerfG* zum sog. Doppeltür-Modell im wegweisenden Bestandsdatenauskunfts-Urteil vom 24. Januar 2014[37].

15. Welche Bedeutung hat der Einsatz von unbemannten Luftfahrtsystemen (Drohnen), insbesondere im Bereich der drohenden Gefahr für die praktische polizeiliche Arbeit?

Hierzu kann keine Aussage getroffen werden.

16. Ist das vorliegende Gesetz in der Gesamtschau seiner Befugnisse und Regelungen mit der vom Bundesverfassungsgericht im Urteil zur Vorratsdatenspeicherung erstmals geforderten „Überwachungsgesamtrechnung“ vereinbar?

Ich stelle mir die Frage, ob mit den über die letzten Jahre immer mehr erweiterten Befugnissen der vom *BVerfG* im Urteil zur Vorratsdatenspeicherung[38] erstmals geforderten „Überwachungsgesamtrechnung“ noch Genüge getan wird.

Das *BVerfG* hat 2010 ausgeführt, dass eine Gesetzgebung, *„die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielte, … von vornherein mit der Verfassung unvereinbar“*[39] sei. Nur wenn sichergestellt sei, dass durch alle Überwachungsmaßnahmen zusammen nicht alle Aktivitäten der Bürger erfasst und rekonstruiert werden können, sei eine Vorratsdatenspeicherung überhaupt rechtfertigungsfähig.

Auch im BKAG-Urteil mahnt das *BVerfG* an, keine Totalüberwachung zu ermöglichen: *„Mit der Menschenwürde unvereinbar ist es, wenn eine Überwachung sich über einen längeren Zeitraum erstreckt und derart umfassend ist, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden können… Beim Einsatz moderner, insbesondere dem Betroffenen verborgener Ermittlungsmethoden müssen die Sicherheitsbehörden mit Rücksicht auf das dem „additiven“ Grundrechtseingriff innewohnende Gefährdungspotenzial koordinierend darauf Bedacht nehmen, dass das Ausmaß der Überwachung insgesamt beschränkt bleibt…“*[40]. Dieser Hinweis des Gerichts ist zwar unmittelbar an die Sicherheitsbehörden adressiert, ist aber auch bei der gesetzlichen Ausgestaltung von Überwachungsmaßnahmen zu berücksichtigen.

Neben der Einführung neuer Befugnisse ist dabei auch das Zusammenwirken und Überschneiden z.B. mit bundespolizeilichen Befugnissen in den Blick zu nehmen.

37 *BVerfGE* 130, 151, 184 – Bestandsdatenauskunft; ähnlich bereits *BVerfGE* 125, 260, 355 f. – Vorratsdatenspeicherung.

38 *BVerfGE* 125, 260, 323 f. – Vorratsdatenspeicherung.

39 *BVerfGE* 125, 260, 323 – Vorratsdatenspeicherung.

40 *BVerfGE* 141, 220, 280 f. – BKAG.

Auch mit der nun erneuten Erweiterung polizeilicher Befugnisse (vgl. Frage 4) besteht, insbesondere im großstädtischen Bereich, die Gefahr, dass man weg von einer anlassbezogenen Überwachung hin zur Überwachung des Alltagslebens rückt.

Vor diesem Hintergrund ist fraglich, ob mit der Erweiterung der Befugnisse, insbesondere im Bereich verdeckter Maßnahmen, die Überwachungsgesamtbilanz noch gewahrt oder nicht bereits darüber hinausgegangen wird. Es darf darauf hingewiesen, dass das Max-Planck-Institut kürzlich ein „Konzept für ein periodisches Überwachungsbarometer“[41] veröffentlicht hat. Hierzu fand am 22. Februar 2021 eine Anhörung des Deutschen Bundestags statt.

17. Die vorangegangenen Novellierungen des PAG haben im Jahr 2018 zu massiven zivilgesellschaftlichen Protesten in Bayern geführt; die Bürgerinnen und Bürger brachten ihre Sorgen vor einem ausufernden Überwachungsstaat darin friedlich zum Ausdruck. Ist der vorliegende Gesetzentwurf ihrer Auffassung nach dazu geeignet, die damals formulierten Bedenken der Bayerischen Bürgerinnen und Bürger aufzugreifen und das Vertrauen in eine angemessene Balance des Polizeirechts zwischen Freiheits- und Sicherheitsrechten wiederherzustellen?

Die PAG-Expertenkommission hat mit ihren Untersuchungen und daraus entwickelten Empfehlungen einen wesentlichen Beitrag zur Evaluierung einzelner – insbesondere umstrittener Vorschriften – des Polizeiaufgabengesetzes geleistet. Viele dieser Empfehlungen wurden mit dem aktuellen Gesetzentwurf umgesetzt. Zu bedenken gebe ich aber, dass die Empfehlungen aus datenschutzrechtlicher Sicht teilweise nur unzureichend umgesetzt werden und der Gesetzesentwurf überdies auch dazu genutzt wird, abermals Befugnisse der Bayerischen Polizei auszuweiten.

41 Abrufbar unter https://csl.mpg.de/de/aktuelles/konzept-fuer-ein-periodischesueberwachungs-barometer/.

Abkürzungsverzeichnis

ABl.	Amtsblatt der Europäischen Union
Abs.	Absatz
AfD	Alternative für Deutschland
App	Application, Anwendungsprogramm auf Smartphone
Art.	Artikel
BayDSG	Bayerisches Datenschutzgesetz
BeckOK	Beck'scher Online-Kommentar
BeckRS	Beck-Rechtsprechung
BDSG	Bundesdatenschutzgesetz
Buchst.	Buchstabe
CSU	Christlich-Soziale Union in Bayern
DNA	Desoxyribonuclein Acid, Träger der Erbinformation
DSFA	Datenschutzfolgenabschätzung
DSGVO	Datenschutz-Grundverordnung
EDV	Elektronische Datenverarbeitung
EU	Europäische Union
EuGH	Europäischer Gerichtshof
FDP	Freie Demokratische Partei
ff.	(nach)folgende
GVBl.	Bayerisches Gesetz- und Verordnungsblatt
https	Hyper Text Transfer Protocol Secure
IP	Internet Protocol
IT	Informationstechnik
lit.	Buchstabe
MdL	Mitglied des Landtages
m. w. N.	mit weiteren Nachweisen
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
z. B.	zum Beispiel

Stichwortverzeichnis

Akkreditierungsverfahren
    Zuverlässigkeitsüberprüfung 27
Akteneinsicht
    Anhörung 37
Anhörung
    Akteneinsicht 37
Antiterrordatei (ATD) 35
Arbeitgeber
    Datenweitergabe durch Impfzentrum 74
Arbeitsfähigkeitsuntersuchungen
    amtsärztliche bei Tarifbeschäftigten 105
Aufbewahrung von Beurteilungsunterlagen
    Regelung 92
Aufbewahrungsfrist für Beihilfeunterlagen
    Verlängerung 99
Ausländerbehörde
    Duldung 52
Ausländerzentralregister
    Abfragen im Sozialbereich 89
Bauantragsunterlagen
    Weiterleitung an Wasserzweckverband 48
Baurecht
    Gutachterausschuss zur Ermittlung von Grundstückswerten und für sonstige
    Wertermittlungen 43
Bauvorlagen
    Weiterleitung an Wasserzweckverband 48
Bayerisches Digitalgesetz 56
Bayerisches Geodateninfrastrukturgesetz
    BayernAtlas 58
Bayerisches Umweltinformationsgesetz
    BayernAtlas 58
BayIMCO 15, 126
    Software 129
Beamte
    Bewerbungsunterlagen im Ratsinformationssystem 108
    Zugriff auf Zeiterfassungsdaten 102
Behandlungsfehlerbegutachtungen
    Mitteilungspflichten des Medizinischen Dienstes 86
Beihilfeunterlagen
    Verlängerung der Aufbewahrungsfrist 99
Beschäftigtendatenschutz
    Ablage von E-Mails 138
Beurteilungsunterlagen
    Regelung zur Aufbewahrung 92
Bewerbungsunterlagen
    Verlust 140
Bürgerversammlungen
    Veröffentlichung von Anträgen 46

Clearing-Verfahren
Akkreditierungsverfahren 27
COVID-19-Pandemie 10
Bayerische Infektionsschutzmaßnahmenverordnungen 10
BayIMCO 15, 126
Datenweitergabe durch Impfzentrum an Arbeitgeber 74
Digitalisierung 124
elektronische Kommunikation 132
externer Test in Schulen 117
Impfmanagement 15
Infektionsschutzgesetz 10
Kontaktmanagement 11
Lollitest 117
Maskenpflicht 12
PCR-Pooltest in Schulen 117
Selbsttest in Schulen 115
SORMAS 12, 126
Testmanagement 14
Testung in Schulen 115
Testungen an Schulen 14
Verarbeitung des COVID-19-Impfstatus im bayerischen öffentlichen Dienst 91
Denkmalliste
BayernAtlas 58
Digitalgesetz 56
Digitalisierung
Digitalisierung COVID-19-Pandemie 124
Duldung
Ausländerbehörde 52
Einwilligung
Akkreditierungsverfahren 27
Forschungsstudie 79
Erkennnungsdienstliche Maßnahmen
Maßregelvollzug 40
Erkennungsdienstliche Maßnahmen
Ordnungswidrigkeiten 30
Strafverfolgungsvorsorge 32
Strafverfolgungsvorsorge 30
Ersthelfer-App 137
Exchange-Sicherheitslücke 143
Fernprüfungen 120
Formular 52
Duldung durch Ausländerbehörde 52
Forschungsstudie ohne Einwilligung 79
Gemeinde
Amtsblatt 50
Mitteilungsblatt 50
Öffentlichkeitsarbeit 50
Geodaten
BayernAtlas 58
Gesetz über die Digitalisierung im Freistaat Bayern 56
Gesetz über die elektronische Verwaltung in Bayern
Digitalgesetz 56
Gesundheitsamt
Arbeitsfähigkeitsuntersuchungen bei Tarifbeschäftigten 105

Gesundheitsämter
Vollzug des Masernschutzgesetzes 63
Gewerbetreibende
Parkausweis 51
Großveranstaltungen
Akkreditierungsverfahren 27
Grundstückswerte
Gutachterausschuss 43
Gutachterausschuss zur Ermittlung von Grundstückswerten und für sonstige Wertermittlungen 43
Haftdatei IT-Vollzug
Protokollierung 40
Hochschulen
Fernprüfungen 120
IGVP
Anlasslose Überprüfung 33
Impfmanagement 15
Impfstatus
Verarbeitung im bayerischen öffentlichen Dienst 91
Impfzentrum
Datenweitergabe an Arbeitgeber 74
Impfzentrum
Aufbewahrung von Dokumentationen zur Impfberechtigung 78
INSPIRE-RL
BayernAtlas 58
Integrationsverfahren der Bayerischen Polizei
Anlasslose Überprüfung 33
IT-Vollzug (Haftdatei)
Protokollierung 40
Justizvollzug
Videoüberwachung in Untersuchungshaft 38
Kfz-Ummeldung
Personenverwechslung 141
Kindertageseinrichtungen
Vollzug des Masernschutzgesetzes 63
Kindeswohlgefährdungen
Datenverarbeitung 84
Kontaktmanagement 11
Kontodatenabgleich
örtliche Rechnungsprüfung 110
Krankenhäuser
Vollzug des Masernschutzgesetzes 66
Lichtbildanforderung
Dokumentation 41
Luftamt 53
Luftsicherheitsassistenten 53
Luftsicherheitsgesetz 53
Masernschutzgesetz
Vollzug durch Kindertageseinrichtungen und Gesundheitsämter 63
Vollzug in Krankenhäusern 66
Maskenpflicht 12
Maßregelvollzug
erkennungsdienstliche Maßnahmen 40

Medizinischer Dienst
Mitteilungspflichten bei Behandlungsfehlerbegutachtungen 86
Meldedaten
Digitalgesetz 56
Meldungen von Datenpannen
Übersicht 2021 142
Onlinezugangsgesetz
Digitalgesetz 56
Ordnungswidrigkeiten
Erkennungsdienstliche Maßnahmen 30
Parkausweis 51
Personaldaten
Bewerbungsunterlagen im Ratsinformationssystem 108
Verarbeitung des COVID-19-Impfstatus im bayerischen öffentlichen Dienst 91
Verlängerung der Aufbewahrungsfrist für Beihilfeunterlagen 99
Verlust von Bewerbungsunterlagen 140
Verwaltungsvorschrift zur Aufbewahrung von Beurteilungsunterlagen 92
Zugriff auf Zeiterfassungsdaten 102
Personaldatenschutz
Ablage von E-Mails 138
Personenverwechslung
verweigerte Kfz-Ummeldung 141
Polizeiaufgabengesetz 27
Änderung 2021 27
Ratsinformationssystem
Bewerbungsunterlagen 108
Rechnungsprüfung, örtliche
Kontodatenabgleich 110
Rechtsextremismus-Datei (RED) 35
Reihentestungen auf SARS-CoV-2 in Einrichtungen 68
SARS-CoV-2
Reihentestungen in Einrichtungen 68
Schulen
externer Test auf SARS-CoV-2 117
Lollitest 117
PCR-Pooltest 117
Selbsttest auf SARS-CoV-2 115
Testung auf SARS-CoV-2 115
Selbständige Freiberufler
Parkausweis 51
Social Engineering 135
Solarpotential
BayernAtlas 58
SORMAS 12, 126
Staatsschutz-Informationssystem 34
Tarifbeschäftigte
amtsärztliche Arbeitsfähigkeitsuntersuchungen 105
Bewerbungsunterlagen im Ratsinformationssystem 108
Zugriff auf Zeiterfassungsdaten 102
Testmanagement 14
Testungen an Schulen 14
Umweltinformationsgesetz, Bayerisches
BayernAtlas 58

Unterhaltsvorschussleistungen
Datenverarbeitungen durch das Jugendamt und das Landesamt für Finanzen 82
Untersuchungshaft
Videoüberwachung 38
Verkehrsordnungswidrigkeiten
Lichtbildanforderung 41
Vermessungs- und Katastergesetz
BayernAtlas 58
Videoüberwachung
Untersuchungshaft 38
Wasserzweckverband
Weiterleitung von Bauantragsunterlagen durch Gemeinden 48
Zeiterfassungsdaten
Zugriff 102
Zuverlässigkeitsüberprüfung
Akkreditierungsverfahren 27