32. Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz

gemäß Art. 59 Datenschutz-Grundverordnung

Berichtszeitraum: 1. Januar 2022 bis 31. Dezember 2022

Inhaltsverzeichnis

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 Eine europäische Datenstrategie

Vor einigen Jahren hat die Europäische Kommission eine neue europäische Datenstrategie vorgestellt.[1] Die Kommission stellt darin sinngemäß fest, dass die EU zwar eine hochindustrialisierte Region darstelle und deshalb auch über qualitativ hochwertige Daten verfüge, diese Daten aber im Vergleich zu Nordamerika und Asien zu wenig geteilt und genutzt würden. Vorhandene Wachstumspotenziale würden deshalb nicht ausgeschöpft. Hierfür ursächlich sind nach Einschätzung der Kommission fehlende Kompetenzen von Akteuren (namentlich bei kleinen und mittleren Unternehmen), fehlende Kapazitäten und Infrastrukturen, die unzureichende Interoperabilität vieler Daten sowie ein fehlender sektorübergreifender Governance-Rahmen für den Datenzugang und die Datennutzung.

Um diese Defizite zu beheben, verfolgt die Kommission das Ziel, einen echten **Binnenmarkt für Daten** zu schaffen. Neben Investitionen in den Aufbau technischer und personeller Ressourcen sollen neue Kommunikations-Infrastrukturen die Schaffung europäischer Datenpools unterstützen. Auf diese Weise sollen Massendatenanalysen und maschinelles Lernen erleichtert werden. Die Entstehung datengetriebener Ökosysteme soll gleichwohl mit dem Datenschutz- und dem Wettbewerbsrecht vereinbar bleiben. Die Standardisierung von Datenformaten soll die Interoperabilität verbessern. Zudem sollen **horizontale Rechtsakte** für einen sektorübergreifenden Governance-Rahmen sorgen, die den Weg zu einem europäischen Binnenmarkt für Daten ebnen. Zu diesen horizontalen Rechtsakten zählt bereits der europäische Datenschutz-Rechtsrahmen mit der Datenschutz-Grundverordnung, die Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten enthält, jedoch erklärtermaßen auch das Ziel verfolgt, auf Grundlage eines hohen Datenschutzniveaus den freien Verkehr personenbezogener Daten zu ermöglichen (vgl. Art. 1 Abs. 1 und Abs. 3 DSGVO). Neben den EU-weit geltenden Datenschutz-Rechtsrahmen sind im Berichtsjahr weitere horizontale Rechtsakte getreten, von denen unter anderem der Daten-Governance-Rechtsakt für die öffentliche Hand von herausgehobener Bedeutung ist (siehe sogleich Nr. 1.1.1).

Auf dieser Grundlage sollen **gemeinsame europäische Datenräume in strategischen Sektoren und Bereichen von öffentlichem Interesse** geschaffen werden. Auch hierzu plant die Europäische Kommission, zunächst jeweils einen Rechtsrahmen zu schaffen, der die Besonderheiten der sektorspezifischen Datenräume berücksichtigt und in den allgemeinen sektorübergreifenden Rahmen einpasst wird. Als ersten gemeinsamen europäischen Datenraum hat die Kommission einen Europäischen Gesundheitsdatenraum (European Health Data Space – EHDS) angeregt. Hierzu hat sie im Berichtszeitraum den Vorschlag einer Verordnung veröffentlicht, der sich gegenwärtig noch im Gesetzgebungsverfahren befindet (siehe dazu sogleich Nr. 1.1.2).

[1] Eine europäische Datenstrategie, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 19. Februar 2020, COM(2020) 66 final, Internet: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52020DC0066.

Der neue Binnenmarkt für Daten soll auf **europäischen Werten und Grundrechten sowie auf der Überzeugung gründen, dass der Mensch im Mittelpunkt steht und stehen sollte**. Das Bekenntnis zur Bedeutung des einzelnen Menschen und zur uneingeschränkten Achtung der europäischen Grundrechte haben das Europäische Parlament, der Rat und die Europäische Kommission jüngst in ihrer gemeinsamen Europäischen Erklärung zu den digitalen Rechten und Grundsätzen für die digitale Dekade bekräftigt.[2]

Aus datenschutzrechtlicher Sicht begrüße ich die grundsätzliche Ausrichtung der europäischen Datenstrategie an den Grundrechten. Allerdings wird man genau beobachten müssen, ob die Rechtsakte zur Umsetzung der europäischen Datenstrategie diese Ausrichtung beibehalten. Dabei scheinen die horizontalen Rechtsakte nicht vollständig aufeinander abgestimmt zu sein. Datenschutzrechtlich vor allem problematisch dürften allerdings die Initiativen zur Schaffung sektorspezifischer Datenräume sein, wie ich dies am Beispiel der Pläne zu einem gemeinsamen Gesundheitsdatenraum aufzeigen werde (Nr. 1.1.2).

1.1.1 Horizontale Rechtsakte, insbesondere Daten-Governance-Rechtsakt

Wie angedeutet, hat der **Daten-Governance-Rechtsakt**[3] (im Folgenden: DGA) eine herausgehobene Bedeutung auch für die bayerischen öffentlichen Stellen und wird deshalb in Grundzügen vorgestellt. Er ist am 30. Mai 2022 verabschiedet worden und soll ab 24. September 2023 gelten.

1.1.1.1 Weiterverwendung bestimmter Kategorien geschützter Daten im Besitz öffentlicher Stellen

Ein Kernstück des Daten-Governance-Rechtsakts betrifft die Weiterverwendung bestimmter Kategorien geschützter Daten im öffentlichen Sektor, wobei nach Art. 1 Abs. 2 UAbs. 1 DGA keine Verpflichtung der Mitgliedstaaten besteht, eine derartige Weiterverwendung zu erlauben. Sie ist im Kapitel II geregelt und ergänzt die Richtlinie (EU) 2019/1024.[4] Diese Richtlinie verpflichtet die Mitgliedstaaten seit Juli 2021 dazu, den Zugang zu offenen Daten der Verwaltung und ihre Weiterverwendung gesetzlich zu regeln. Diese Vorgabe hat der Bundesgesetzgeber mit dem Datennutzungsgesetz[5] umgesetzt. Wie angedeutet, beschränkt sich der Anwendungsbereich der Richtlinie (EU) 2019/1024 allerdings auf für jedermann frei verwendbare, „offene Daten".

Der Daten-Governance-Rechtsakt befasst sich nun auch mit der **Weiterverwendung solcher Daten, an denen rechtlich geschützte Vertraulichkeitsinteressen bestehen**. Dazu zählt Art. 3 Abs. 1 DGA die geschäftliche Geheimhaltung, die statistische Geheimhaltung, den Schutz des geistigen Eigentums Dritter und den Schutz personenbezogener Daten.

Der Daten-Governance-Rechtsakt regelt zwar nicht die Frage, ob die öffentliche Hand die Weiterverwendung von in ihrem Besitz befindlichen Daten zu erlauben hat.

2 ABl. C 23 vom 23. Januar 2023, S. 1.

3 Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt (ABl. L 152 vom 3. Juni 2022, S. 1).

4 Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (ABl. L 172 vom 26. Juni 2019, S. 56).

5 Vom 16. Juli 2021 (BGBl. I S. 2941, 2942; ber. S. 4114).

Insbesondere schafft er nach Art. 1 Abs. 3 Satz 4 DGA keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Er soll aber die Rahmenbedingungen für die gemeinsame Datennutzung im Binnenmarkt verbessern (siehe Erwägungsgrund 3 DGA). Dazu soll der Daten-Governance-Rechtsakt unter anderem die Bedingungen festlegen, unter denen Daten im Besitz öffentlicher Stellen durch Datennutzer weiterverwendet werden können. Insbesondere Art. 5 DGA sieht dazu in seinen Abs. 3 bis 6 auch Regelungen vor, mit denen datenschutzrechtliche Belange berücksichtigt werden sollen.

Artikel 5 DGA
Bedingungen für die Weiterverwendung
[…]
(3) Öffentliche Stellen sorgen gemäß dem Unionsrecht und dem nationalen Recht dafür, dass die Daten geschützt bleiben. Sie können folgende Anforderungen vorschreiben:

a) Den Zugang zur Weiterverwendung von Daten nur zu gewähren, wenn die öffentliche Stelle oder die zuständige Stelle nach Eingang des Antrags auf Weiterverwendung sichergestellt hat, dass die Daten
   i) im Falle personenbezogener Daten anonymisiert wurden und
   ii) im Falle von vertraulichen Geschäftsinformationen, einschließlich Geschäftsgeheimnisse oder durch Rechte des geistigen Eigentums geschützte Inhalte, nach einer anderen Methode der Offenlegungskontrolle verändert, aggregiert oder aufbereitet wurden,

b) der Zugang zu den Daten und deren Weiterverwendung erfolgt durch Fernzugriff in einer von der öffentlichen Stelle bereitgestellten oder kontrollierten sicheren Verarbeitungsumgebung,

c) der Zugang zu den Daten und deren Weiterverwendung erfolgt unter Einhaltung hoher Sicherheitsstandards innerhalb der physischen Räumlichkeiten, in denen sich die sichere Verarbeitungsumgebung befindet, sofern ein Fernzugriff nicht erlaubt werden kann, ohne die Rechte und Interessen Dritter zu gefährden.

(4) Die öffentlichen Stellen erlegen im Falle einer erlaubten Weiterverwendung gemäß Absatz 3 Buchstaben b und c Bedingungen auf, mit denen die Integrität des Betriebs der technischen Systeme der verwendeten sicheren Verarbeitungsumgebung gewahrt wird. Die öffentliche Stelle behält sich das Recht vor, das Verfahren, die Mittel und die Ergebnisse der vom Weiterverwender durchgeführten Datenverarbeitung zu überprüfen, um die Integrität des Datenschutzes zu wahren, und sie behält sich das Recht vor, die Verwendung der Ergebnisse zu verbieten, wenn darin Informationen enthalten sind, die die Rechte und Interessen Dritter gefährden. Die Entscheidung, die Verwendung der Ergebnisse zu verbieten, muss für den Weiterverwender verständlich und transparent sein.
(5) Sofern im nationalen Recht für die Weiterverwendung von Daten gemäß Artikel 3 Absatz 1 keine besonderen Schutzvorkehrungen bezüglich geltender Geheimhaltungspflichten vorgesehen sind, macht die öffentliche Stelle die Nutzung der gemäß Absatz 3 des vorliegenden Artikels bereitgestellten Daten davon abhängig, ob der Weiterverwender einer Geheimhaltungspflicht nachkommt, wonach ihm die Offenlegung von Informationen, die er möglicherweise trotz der getroffenen Schutzvorkehrungen erlangt hat, untersagt ist, wenn dadurch die Rechte und Interessen Dritter verletzt würden. Weiterverwendern ist es untersagt, betroffene Personen, auf die sich die Daten beziehen, erneut zu identifizieren, und sie ergreifen technische und operative Maßnahmen, um eine erneute Identifizierung zu verhindern und der öffentlichen Stelle etwaige Datenschutzverletzungen, die zu einer erneuten Identifizierung der betroffenen Personen führen könnten, mitzuteilen. Im Falle der unbefugten Weiterverwendung nicht personenbezogener Daten unterrichtet der Weiterverwender unverzüglich,

gegebenenfalls mit Unterstützung der öffentlichen Stelle, die juristischen Personen, deren Rechte und Interessen beeinträchtigt werden könnten.
(6) Kann die Weiterverwendung von Daten gemäß den in den Absätzen 3 und 4 des vorliegenden Artikels festgelegten Verpflichtungen nicht erlaubt werden und es keine andere Rechtsgrundlage für die Übermittlung der Daten gemäß der Verordnung (EU) 2016/679 gibt, bemüht sich die öffentliche Stelle, gemäß dem Unionsrecht und dem nationalen Recht, nach besten Kräften, mögliche Weiterverwender dabei zu unterstützen, die Einwilligung der betroffenen Personen oder die Erlaubnis der Dateninhaber einzuholen, deren Rechte und Interessen durch eine solche Weiterverwendung beeinträchtigt werden könnten, sofern dies ohne einen unverhältnismäßig hohen Aufwand für die öffentliche Stelle machbar ist. In den Fällen, in denen die öffentliche Stelle eine solche Unterstützung leistet, kann sie von den in Artikel 7 Absatz 1 genannten zuständigen Stellen unterstützt werden.

Die öffentlichen Stellen haben nach Art. 5 Abs. 3 Satz 1 DGA dafür zu sorgen, dass personenbezogene Daten nach Maßgabe des Unionsrechts oder des nationalen Rechts geschützt bleiben. Diese Vorgabe steht wohl grundsätzlich im Einklang mit Art. 6 Abs. 3 Satz 1 DSGVO, wonach die Rechtsgrundlage für eine Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung nach Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO sowie zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe nach Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO durch Unionsrecht oder durch das Recht der Mitgliedstaaten gesondert festgelegt wird.

Art. 5 Abs. 3 Satz 2 DGA sieht drei Möglichkeiten vor, mit denen das Unionsrecht oder das nationale Recht Anforderungen an das Wie des Schutzes personenbezogener Daten vorschreiben kann (nicht muss!). Nach Buchstabe a kann der Zugang zu personenbezogenen Daten von einer **vorherigen Anonymisierung** abhängig gemacht werden, wobei die Anonymisierung in der Verordnung nicht näher definiert wird.

Nach den Buchstaben b und c kann der Datenzugang auch unter gesicherten Zugangsbedingungen gewährt werden, wenn eine Anonymisierung nicht durchgeführt wurde – etwa weil die Bereitstellung anonymisierter Daten den Interessen der Nutzungsberechtigten nicht entsprechen würde. Damit angesprochen ist die Weiterverwendung pseudonymer Daten durch Datennutzer, die dem Regelungsregime der Datenschutz-Grundverordnung unterliegen. Art. 5 Abs. 4 DGA sieht dazu vor, dass die öffentlichen Stellen die erlaubte Weiterverwendung an Prüf- und Verbotsvorbehalte zu knüpfen haben. Art. 5 Abs. 5 DGA untersagt es den Weiterverwendern im Falle der Verwendung pseudonymer Daten, die betroffenen Personen zu reidentifizieren. Zudem müssen die Weiterverwender technisch-organisatorische Maßnahmen ergreifen, um eine Reidentifizierung zu vermeiden oder die öffentliche Stelle über Datenschutzverletzungen mit dem Risiko der unbeabsichtigten Reidentifizierung zu informieren. Da die Datenschutz-Grundverordnung vom Daten-Governance-Rechtsakt unberührt bleiben soll, bleiben die Weiterverwender nach Art. 33, 34 DSGVO weiterhin verpflichtet, Datenschutzverletzungen im Sinne des Art. 4 Nr. 12 DSGVO an die Aufsichtsbehörde zu melden und gegebenenfalls Betroffene über sie zu benachrichtigen.

Absatz 5 formuliert ein Muster für den Umgang mit pseudonymisierten Daten, das in nachfolgenden horizontalen Rechtsakten wiederholt aufgegriffen und in ihrem jeweiligen Anwendungsbereich weiterentwickelt worden ist. Ist eine Weiterverwendung nach den dargelegten Bedingungen nicht möglich, sollen die öffentlichen Stellen nach Art. 5 Abs. 6 DGA im Rahmen der Verhältnismäßigkeit mögliche Weiterverwender dabei unterstützen, die Einwilligung der betroffenen Personen einzuholen.

Um Daten erhältlich und leicht zugänglich zu machen, sollen die Mitgliedstaaten zudem **zentrale Informationsstellen** schaffen oder benennen, die entsprechende Anträge von Datennutzern auf Weiterverwendung entgegennehmen und an die fachlich zuständigen öffentlichen Stellen übermitteln. Um die Antragstellung zu erleichtern, erstellen die zentralen Informationsstellen auf elektronischem Weg eine durchsuchbare Bestandsliste mit einer Übersicht aller verfügbaren Datenressourcen, die auch über ein europaweites zentrales Zugangsportal recherchierbar gemacht werden (Art. 8 DGA). Zugleich sollen die Mitgliedstaaten Stellen schaffen, die öffentliche Stellen bei ihren Aufgaben nach Art. 5 DGA unterstützen sollen (Art. 7 DGA).

1.1.1.2 Regeln des Daten-Governance-Rechtsakts insbesondere zu Datenvermittlungsdiensten

Das dritte Kapitel des Daten-Governance-Rechtsakts beschreibt die Anforderungen an sogenannte Datenvermittlungsdienste (der Kommissionsvorschlag stellte noch durchweg auf „Dienste für die gemeinsame Datennutzung" ab[6]). Nach Art. 2 Nr. 11 DGA sind sie als Dienste zu verstehen, mit denen „durch technische, rechtliche oder sonstige Mittel Geschäftsbeziehungen zwischen einer unbestimmten Anzahl von betroffenen Personen oder Dateninhabern einerseits und Datennutzern andererseits hergestellt werden sollen, um die gemeinsame Datennutzung […] zu ermöglichen". Der Daten-Governance-Rechtsakt misst **Datenvermittlungsdiensten eine Schlüsselrolle** in der Datenwirtschaft bei, weil sie in besonderer Weise dazu beitragen können, Daten effizient zu bündeln und den bilateralen Datenaustausch zu erleichtern. Allerdings wirft die abstrakte Legaldefinition durchaus Auslegungs- und Abgrenzungsfragen auf.

Datenvermittlungsvermittlungsdienste müssen nach Art. 12 DGA eine Reihe von Bedingungen erfüllen, die das Vertrauen in solche Dienste stärken. Für bestimmte Datenvermittlungsdienste sehen Art. 10 und 11 DGA ein Anmeldeverfahren vor. Nach Art. 13 DGA haben die Mitgliedstaaten Aufsichtsbehörden für Datenvermittlungsdienste zu benennen, deren Aufgaben allerdings die Befugnisse der nationalen Aufsichtsbehörden für den Datenschutz unberührt lassen. Zugleich soll der Daten-Governance-Rechtsakt den rechtlichen Rahmen bilden, um Formen des Datenaltruismus zu fördern. So ist in Art. 25 DGA vorgesehen, dass die Kommission ein europäisches Einwilligungsformular für Datenaltruismus entwickelt, das modular aufgebaut ist und für bestimmte Sektoren und verschiedene Zwecke angepasst werden kann. Zur Unterstützung und Beratung der Europäischen Kommission wird ein **„Europäischer Dateninnovationsrat"** eingerichtet.

1.1.1.3 Weitere horizontale Rechtsakte

Ebenfalls im Berichtszeitraum in Kraft getreten ist das **Gesetz über digitale Märkte**.[7] Diese Verordnung legt Regeln für bestimmte **zentrale Plattformdienste** fest, die als „Torwächter" bezeichnet werden, wenn sie aufgrund ihrer Marktposition einen besonderen Einfluss auf den EU-Binnenmarkt für Daten entfalten.

6 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz) vom 25. November 2020, COM(2020) 767 final, Internet: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=celex:52020PC0767.

7 Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte, ABl. L 265 vom 12. Oktober 2022, S. 1).

In Teilen gilt bereits auch das **Gesetz über digitale Dienste**.[8] Es richtet sich in erster Linie an **„Datenvermittlungsdienste“**. Dieses Gesetz dient der Unterbindung illegaler Inhalte (zum Beispiel Hate Speech und – mit gewissen Abstrichen – auch Fake News) und soll für mehr Transparenz bei der Online-Werbung sorgen. Insoweit weist er Querbezüge zum Daten-Governance-Rechtsakt und zum Gesetz über Digitale Märkte auf. Auch insoweit werden Datenvermittlungsdienste reglementiert. Datenschutzrechtlich relevant ist etwa die Verpflichtung von bestimmten Vermittlungsdiensten zur Errichtung von Meldesystemen für Rechtsverstöße. Das Gesetz über digitale Dienste verfolgt einen risikobasierten Ansatz; es enthält Sondervorschriften für Hosting und Online-Plattformen. Die Datenschutz-Grundverordnung und die E-Privacy-Richtlinie sollen vom Gesetz über digitale Dienste (im Folgenden: DSA) unberührt bleiben, vgl. Art. 2 Abs. 4 Buchst. g DSA. Im Übrigen sieht das Gesetz über digitale Dienste ein grundsätzliches Verbot profilingbasierter Werbung (Art. 26 Abs. 3 DSA) und eine Schutzvorschrift zugunsten Minderjähriger bezüglich Werbeansprachen (Art. 28 Abs. 2 DSA) vor. Art. 39 DSA beschreibt die Anforderungen an Online-Archive, Art. 40 Abs. 8 Buchst. d DSA den Datenzugang zu Forschungszwecken. Art. 45 DSA betrifft Verhaltenskodizes.

Die **während des Berichtszeitraums noch nicht abgeschlossenen Gesetzgebungsverfahren** zu bedeutsamen horizontalen Rechtsakten betreffen unter anderem harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), COM (2022) 68 = 2022/0047 COD)[9], horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyber-Resilience-Act),[10] eine Verordnung über Maßnahmen für ein hohes Maß an Interoperabilität des öffentlichen Sektors[11] und ein geplantes Gesetz über Künstliche Intelligenz.[12] Da letzterer Entwurf perspektivisch auch für die bayerische öffentliche Hand relevant werden wird, wird er nachfolgend in seinen Grundzügen vorgestellt.

1.1.1.4 Insbesondere: Diskussion um eine KI-Verordnung

Ihren Entwurf für ein Gesetz über Künstliche Intelligenz stellte die Kommission am 21. April 2021 vor. Der Europäische Wirtschafts- und Sozialausschuss nahm zu diesem Vorschlag im Herbst 2021 Stellung. Der Rat hat hierzu bereits im Rahmen einer

8 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste, ABl. L 277 vom 27. Oktober 2022, S. 1).

9 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), COM(2022) 68 final, Internet: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52022PC0068.

10 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020, COM/2022/454 final, Internet: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=celex:52022PC0454

11 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes Maß an Interoperabilität des öffentlichen Sektors in der Union (Gesetz für ein interoperables Europa), COM/2022/720 final, Internet: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=celex:52022PC0720.

12 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM/2021/206 final, Internet: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=celex:52021PC0206.

sog. Allgemeinen Ausrichtung seinen vorläufigen Standpunkt festgelegt,[13] sodass der Gesetzentwurf gegenwärtig bereits im fortgeschrittenen Stadium erörtert wird.[14] Der Verordnungsentwurf hat zum Ziel, einerseits die Entwicklung von innovativen KI-Systemen zu fördern und andererseits etwaige Risiken auf ein vertretbares Maß zu begrenzen.

Im noch laufenden Gesetzgebungsverfahren ist vieles umstritten. Dies beginnt bereits mit der Frage, **was unter Künstlicher Intelligenz zu verstehen ist**. So definiert Art. 3 Nr. 1 des Verordnungsentwurfs in der Fassung des Kommissionsvorschlags als „System künstlicher Intelligenz" (KI-System) eine Software, die mit näher bestimmten Techniken und Konzepten entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren. Die relevanten Techniken und Konzepte sollen in einer Anlage aufgeführt werden. Diese Definition wird als zu unklar kritisiert. Die Allgemeine Ausrichtung des Rates stellt hingegen in Art. 3 Nr. 1 auf ein System ab, das so konzipiert ist, dass es mit Elementen der Autonomie arbeitet, und das auf der Grundlage maschineller vom Menschen erzeugter Daten und Eingaben durch maschinelles Lernen und/oder logik- und wissensgestützter Konzepte ableitet, wie eine Reihe von Zielen erreicht wird, und systemgenerierte Ergebnisse wie Inhalte (generative KI-Systeme), Vorhersagen, Empfehlungen oder Entscheidungen hervorbringt, die das Umfeld beeinflussen, mit dem die KI-Systeme interagieren. Diese Definition halte ich am ehesten für nachvollziehbar.

Als eine wesentliche Herausforderung identifiziert der Kommissionsvorschlag die Frage, wie die Risiken des Einsatzes von KI-Systemen für den Menschen beherrschbar gemacht werden können. Hierzu wird ein **risikobasierter Ansatz** diskutiert, der KI-Systeme in verschiedene Risikoklassen unterteilt. Je nach Risikostufe unterliegen KI-Systeme unterschiedlichen Bedingungen.

KI-Systeme für die Interaktion mit natürlichen Personen sollen nach Art. 52 des Verordnungsentwurfs (in allen Fassungen) besonderen Transparenzpflichten unterliegen. Damit soll sichergestellt werden, dass den betroffenen Personen bewusst ist, dass sie mit einem KI-System und nicht mit einem anderen Menschen kommunizieren.

Bestimmte Praktiken im Bereich der Künstlichen Intelligenz sollen nach Art. 5 des Verordnungsentwurfs verboten werden, etwa zur unterschwelligen Beeinflussung außerhalb des Bewusstseins einer Person. Nur teilweise untersagt sollen biometrische Echtzeit-Fernidentifizierungssysteme in öffentlichen Räumen sein, wenn sie zu Strafverfolgungszwecken eingesetzt werden.

Zugleich sieht der Kommissionsvorschlag in Art. 53 ff. des Verordnungsentwurfs vor, dass von den zuständigen Behörden **KI-Reallabore** errichtet werden können, um im Rahmen einer kontrollierten Umgebung die Entwicklung, Erprobung und Validierung

13 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union – Allgemeine Ausrichtung vom 6. Dezember 2022, ST 15698 2022 INIT, Internet: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=consil:ST_15698_2022_INIT.

14 Zum Beratungsstand im Europäischen Parlament siehe https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0106(COD)&l=en unter „Documentation gateway".

von innovativen KI-Systemen zu erleichtern, bevor sie in den Verkehr gebracht und in Betrieb genommen werden.

Angesichts der hier nur angedeuteten Herausforderungen gewinnt die **unabhängige Aufsicht** in Bezug auf KI-Systeme eine besondere Relevanz. Nach Art. 3 Nr. 42 des Verordnungsentwurfs (in allen Fassungen) sind insofern namentlich zwei Funktionen wahrzunehmen. Die Bewertung, Benennung und Notifizierung von Konformitätsbewertungsstellen hat eine **„notifizierende Behörde“** zu übernehmen. Werden KI-Systeme im Markt eingeführt, werden sie von einer **„Marktüberwachungsbehörde“** weiter kontrolliert (vgl. Art. 3 Nr. 19, 22, 42 und 43 des Verordnungsentwurfs in der Fassung des Kommissionsvorschlags sowie Art. 3 Nr. 43 der Allgemeinen Ausrichtung des Rates). Nach Art. 59 des Verordnungsentwurfs in der Fassung des Kommissionsvorschlags soll eine nationale Aufsichtsbehörde nach Möglichkeit beide Funktionen wahrnehmen. Jedenfalls die notifizierenden Stellen sind so zu organisieren, dass ihre Unparteilichkeit gewahrt ist. Gleichzeitig soll die Zuständigkeit der unabhängigen Datenschutzaufsichtsbehörden unberührt bleiben.

Da das Gesetzgebungsverfahren noch nicht abgeschlossen ist, bleibt insbesondere abzuwarten, wie die künftigen Aufsichtsstrukturen konkret aussehen werden. Allerdings scheint bereits jetzt unstreitig zu sein, dass der Europäische Datenschutzbeauftragte die aufsichtsbehördliche Zuständigkeit in Bezug auf KI-Systeme erhalten soll, die von EU-Einrichtungen eingesetzt werden. Hierfür spricht, dass der Europäische Datenschutzbeauftragte wie die Datenschutz-Aufsichtsbehörden in den Mitgliedstaaten unabhängig ist. Auch sieht der Kommissionsentwurf der Verordnung eine Reihe von aufsichtsbehördlichen Instrumenten vor, die aus dem Datenschutzrecht bekannt sind. Das gilt etwa für die Meldepflichten nach Art. 62 des Verordnungsentwurfs; die Regelung ist Art. 33 DSGVO ähnlich. Angesichts dessen und des Umstands, dass Teile der aufsichtsbehördlichen Aufgaben ausdrücklich den Datenschutz-Aufsichtsbehörden zugewiesen werden (siehe etwa Art. 63 Abs. 5 des Verordnungsentwurfs in der Fassung des Kommissionsvorschlags) ist es daher nicht auszuschließen, dass auch die Datenschutz-Aufsichtsbehörden der Mitgliedstaaten mit der Überwachung von KI-Systemen betraut werden. Nach meiner Einschätzung verfügt allerdings gegenwärtig keine Aufsichtsbehörde in Deutschland (und wohl auch in ganz Europa) über die notwendigen personellen und technischen Ressourcen, um diese Herausforderung zu bewältigen – zumal die Aufsicht über KI-Systeme spezifische Kenntnisse der Funktionsweise erfordern.

Unabhängig davon ist es notwendig und folgerichtig, wenn die Datenschutzkonferenz auf nationaler Ebene und der Europäische Datenschutzausschuss auf europäischer Ebene gleichermaßen das Thema der Künstlichen Intelligenz stärker in den Fokus rücken. Insoweit rufe ich in Erinnerung, dass bereits die 97. Konferenz der unabhängigen Datenschutz-Aufsichtsbehörden des Bundes und der Länder in ihrer Hambacher Erklärung vom 3. April 2019[15] erste Hinweise zu den datenschutzrechtlichen Anforderungen an die Nutzung von KI-Systemen gegeben hat.

1.1.1.5 Zwischenfazit

Insgesamt versuchen die horizontalen Rechtsakte eine rechtliche Grundlage für Maßnahmen zu schaffen, welche die eingangs beschriebenen Defizite an Interoperabilität, Governance und Kommunikations-Infrastrukturen beheben. Es ist allerdings nicht zu

[15] Text auf https://www.datenschutz-bayern.de, Rubrik „Konferenzen“.

übersehen, dass bereits die horizontalen Rechtsakte nicht vollständig aufeinander abgestimmt sind. So bleibt vieles im Unklaren. Beispielsweise gibt es Legaldefinitionen, die je nach Rechtsakt denselben (oder sehr ähnlichen) zentralen Begriffen unterschiedliche Bedeutungen geben.[16] Hinsichtlich anderer relevanter Begriffe fehlen Legaldefinitionen, und die horizontalen Rechtsakte verweisen insoweit auch nicht auf Begriffsbestimmungen früherer Rechtsakte. Aus datenschutzrechtlicher Sicht wäre es etwa sinnvoll gewesen, im Daten-Governance-Rechtsakt auf die Legaldefinition der „Anonymisierung" in Art. 2 Nr. 7 Richtlinie (EU) 2019/1024 zu verweisen. Insgesamt soll der Datenschutz-Rechtsrahmen überwiegend unangetastet bleiben – gleichzeitig sehen einige horizontale Rechtsakte Vorschriften vor, die sich zwangsläufig auf den Datenschutz auswirken. Vor diesem Hintergrund haben auch der Europäische Datenschutzausschuss und der Europäische Datenschutzbeauftragte im Rahmen ihrer gemeinsamen Stellungnahme 03/2021 zum Vorschlag eines Daten-Governance-Gesetzes[17] sinngemäß mehr Rechtsklarheit gefordert und verlangt, dass die weiteren horizontalen Rechtsakte das bestehende, grundrechtlich garantierte Datenschutzniveau nicht untergraben dürfen.

1.1.2 Sektorspezifische gemeinsame Datenräume: Beispiel Gesundheit

Am 3. Mai 2022 hat die EU-Kommission ihren Vorschlag einer Verordnung zum europäischen Raum für Gesundheitsdaten (**European Health Data Space – EHDS**[18] veröffentlicht. Der Vorschlag betrifft den ersten sektorspezifischen europäischen Datenraum. Der EHDS soll den Zugang zu elektronischen Gesundheitsdaten und ihren Austausch fördern. Der Vorschlag sieht neben begrüßenswerten Vorschriften zu einer besseren Interoperabilität elektronischer Gesundheitsdaten und zur Standardisierung von elektronischen Patientenakten auch Regelungen vor, die aus datenschutzrechtlicher Sicht insbesondere im Zusammenhang mit der sogenannten Sekundärnutzung dringend nachzubessern sind.

Im unmittelbaren Zusammenhang mit Gesundheitsdienstleistungen (sog. **Primärnutzung**, siehe Art. 2 Abs. 2 Buchst. d des Verordnungsentwurfs) sollen natürliche Personen eine bessere Kontrolle über die Verarbeitung ihrer elektronischen Gesundheitsdaten erlangen. Zugleich sollen Gesundheitsdienstleister für die jeweilige Gesundheitsdienstleistung relevante Daten zügiger austauschen können. Zu diesen Zwecken sollen die Mitgliedstaaten Zugangsdienste für elektronische Gesundheitsdaten einrichten, um den natürlichen Personen insbesondere die Ausübung ihrer **Rechte auf Kopie der Gesundheitsdaten** (Art. 3 Abs. 1, 2 des Verordnungsentwurfs) und **auf Datenportabilität** (Art. 3 Abs. 8 des Verordnungsentwurfs) zu ermöglichen. Zugleich sieht der Vorschlag vor, dass Angehörige der Gesundheitsberufe, wenn sie elektronische Gesundheitsdaten verarbeiten, unabhängig vom Versicherungs- und Behandlungsmitgliedstaat Zugriff auf die elektronischen Gesundheitsdaten der von ihnen behandelten natürlichen Personen erhalten (Art. 4 Abs. 1 Buchst. a

16 Zum Beispiel „Dateninhaber" in Art. 2 Nr. 9 DGA und Art. 2 Nr. 6 Entwurf eines Datengesetzes; „Datennutzer" oder „Nutzer", in Art. 2 Nr. 9 DGA, Art. 3 Buchst. b DSA, Art. 3 Nr. 4 Entwurf eines Gesetzes über künstliche Intelligenz, Art. 2 Nr. 5 Entwurf eines Datengesetzes sowie – etwas besser – in Art. 2 Nr. 20, 21 Gesetz über digitale Märkte, der den Nutzerbegriff mit erklärenden Zusätzen ergänzt.

17 Internet: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_de.

18 Vorschlag für Verordnung des Europäischen Parlaments und des Rates über den europäischen Raum für Gesundheitsdaten, COM/2022/197 final, Internet: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=COM:2022:197:FIN.

des Verordnungsentwurfs). Eine Zustimmung der natürlichen Personen in den Datenzugang ist im Grundsatz nicht vorgesehen; die natürlichen Personen haben lediglich das Recht, den Datenzugang zu beschränken (vgl. Art. 3 Abs. 9, Art. 4 Abs. 4 des Verordnungsentwurfs[19]). Die wechselseitige Gewährung des Datenzugangs soll über eine **gemeinsame Infrastruktur für die Primärnutzung elektronischer Gesundheitsdaten** realisiert werden (MyHealth@EU, siehe Art. 12 ff. des Verordnungsentwurfs).

Das vorgeschlagene Konzept der Datenverarbeitung zur Primärnutzung steht in einem erheblichen Spannungsverhältnis zur ärztlichen Schweigepflicht, wonach jede Preisgabe von personenbezogenen Patientendaten – auch die gegenüber anderen Schweigepflichtigen – einer ausdrücklichen Entbindung durch die Patientin oder den Patienten bedarf. Art. 8 Abs. 2 Satz 1 Charta der Grundrechte der Europäischen Union (im Folgenden: GRCh) bestimmt, dass personenbezogene Daten nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden dürfen. Jede Verarbeitung personenbezogener Daten ohne Einwilligung der betroffenen natürlichen Person bewirkt einen Grundrechtseingriff, der sich nach Art. 52 Abs. 1 GRCh auf das unbedingt Notwendige zu beschränken hat. Da die Zugangsberechtigung der Gesundheitsdienstleister davon abhängt, dass sie die betreffenden natürlichen Personen behandeln (siehe Art. 4 Abs. 1 Buchst. a des Verordnungsentwurfs), ist es nicht ersichtlich, warum eine vorherige Zustimmung in die Verarbeitung nicht einholbar sein soll. Allerdings muss ich einschränkend hinzufügen, dass das Erfordernis einer Schweigepflichtentbindungserklärung wohl ein deutsches Spezifikum ist, das in den weitaus meisten Mitgliedstaaten der EU keine Entsprechung hat.

Ohnehin viel problematischer sind die Vorschläge zur sonstigen Nutzung von elektronischen Gesundheitsdaten (sog. **Sekundärnutzung**, siehe Art. 2 Abs. 2 Buchst. e des Verordnungsentwurfs). Der Vorschlag sieht dazu vor, dass die Mitgliedstaaten Zugangsstellen für Gesundheitsdaten benennen (Art. 36 Abs. 1 des Verordnungsentwurfs). Sie sollen Anträge auf Zugang zu elektronischen Gesundheitsdaten entgegennehmen, prüfen und verbescheiden (Art. 37 des Verordnungsentwurfs). Der Vorschlag sieht ein breites Spektrum von Verarbeitungszwecken vor, für die Sekundärnutzung zulässig ist (siehe Art. 34 des Verordnungsentwurfs).

Dateninhaber sind grundsätzlich verpflichtet, ihre elektronischen Gesundheitsdaten für die Sekundärnutzung zur Verfügung zu stellen (vgl. Art. 33 Abs.1 des Verordnungsentwurfs). Dazu sollen sie verpflichtet werden, den Zugangsstellen für Gesundheitsdaten Metadaten („allgemeine Beschreibung des Datensatzes", Art. 41 Abs. 2 des Verordnungsentwurfs) zu übermitteln, die dann veröffentlicht werden. Im Fall eines berechtigten Antrags auf Sekundärnutzung fordern die Zugangsstellen bei relevanten Dateninhabern die beantragten elektronischen Gesundheitsdaten als Klardaten an (siehe Art. 41 Abs. 4 des Verordnungsentwurfs). Erst nachdem die elektronischen Gesundheitsdaten von verschiedenen Dateninhabern gesammelt und kompiliert worden sind, werden sie von der Zugangsstelle pseudonymisiert oder anonymisiert, um sie so an den Antragsteller weiterzuleiten (Art. 37 Abs. 1 Buchst. g, Art. 44 Abs. 2, 3 und Art. 45 Abs. 2 Buchst. c und d des Verordnungsentwurfs). Die Weiterverarbeitung durch die Nutzer soll zweckgebunden bis zu maximal zehn Jahren (siehe Art. 46 Abs. 9 des Verordnungsentwurfs) erfolgen – eine Wiederherstellung des unmittelbaren Personenbezugs ist den Nutzungsberechtigten nicht gestattet (siehe Art. 44 Abs. 3 Sätze 3, 4 des Verordnungsentwurfs). Ist die Zugangsstelle nicht willens

[19] Art. 4 Abs. 4 Satz 1 des Verordnungsentwurfs sieht nur für den Fall der Einschränkung des Zugangs durch natürliche Personen einen Zustimmungsvorbehalt vor.

oder nicht in der Lage, einen Antrag auf Sekundärnutzung innerhalb von zwei Monaten – bei komplexen Fällen binnen vier Monaten – zu bescheiden, gilt der Antrag als genehmigt (vgl. Art. 46 Abs. 3 des Verordnungsentwurfs). Bei grenzüberschreitenden Antragsfällen können Nutzer ihren Antrag bei einer beliebigen Zugangsstelle für Gesundheitsdaten stellen, die für die Weiterleitung zuständig ist (siehe Art. 45 Abs. 3 des Verordnungsentwurfs). Die Anträge werden dann über nationale Kontaktstellen auf dem Weg der grenzüberschreitenden Infrastruktur HealthData@EU weitergeleitet (siehe im Einzelnen Art. 52 des Verordnungsentwurfs). Fordern öffentliche Stellen elektronische Gesundheitsdaten an, soll eine Datengenehmigung nicht erforderlich sein (vgl. Art. 48 des Verordnungsentwurfs).

Es ist zwar nicht zu übersehen, dass der Vorschlag zahlreiche Vorgaben für die Sicherheit der bereitzustellenden elektronischen Gesundheitsdaten macht. Sieht man davon ab, dass die Wirksamkeit dieser Vorkehrungen bei bestimmten Datenkategorien – wie etwa genetischen Daten oder Bilddaten – fraglich sein kann, bestehen aus datenschutzrechtlicher Sicht schwerwiegende, auch grundrechtliche Bedenken gegenüber dem vorgeschlagenen Konzept der Sekundärnutzung. Von diesen grundrechtlichen Bedenken abgesehen, würde die Verordnung eine massive Mehrbelastung von Dateninhabern (etwa Krankenhäusern, großen Arztpraxen, Herstellern von Medizinprodukten, gesetzlichen Krankenkassen, öffentlichen Archiven, Ämtern für Statistik usw.) begründen, soweit sie verpflichtet werden, den Zugangsstellen Metadaten und – im Falle von positiven Zugangsentscheidungen – Klardaten zur Verfügung zu stellen. Diesen erheblichen bürokratischen Aufwänden stehen ungeachtet einiger Kostendämpfungsmaßnahmen für Unternehmen keine unmittelbaren Vorteile gegenüber, soweit Kliniken und Arztpraxen nicht selbst zu den Datennutzern gehören. Die gesetzliche Pflicht zur Bereitstellung elektronischer Gesundheitsdaten greift damit nicht unerheblich in die Unternehmensfreiheit der kommerziellen Dateninhaber aus Art. 16 GRCh ein.

Ob derartige Eingriffe aus Gründen der Datenverkehrsfreiheit gerechtfertigt sind, habe ich allerdings aufgrund meiner Aufgabenstellung nicht zu beurteilen. Schwerwiegende grundrechtliche Bedenken mit datenschutzrechtlicher Relevanz bestehen jedoch auch und vor allem im Hinblick auf die Grundrechte der Patientinnen und Patienten auf Achtung ihres Privatlebens und auf Datenschutz, Art. 7 und Art. 8 GRCh. Die Pflicht zur Bereitstellung der elektronischen Gesundheitsdaten soll **unabhängig von der Einwilligung der betroffenen natürlichen Personen** eingreifen. Der Vorschlag der Kommission sieht sogar vor, dass elektronische Gesundheitsdaten selbst dann uneingeschränkt übermittelt werden müssen, wenn sie vom Dateninhaber zuvor lediglich auf Grundlage einer Einwilligung erhoben wurden (siehe Art. 33 Abs. 5 des Verordnungsentwurfs). Derartige gesetzliche Übermittlungspflichten gibt es auf nationaler Ebene in Deutschland zwar punktuell auch in anderen Zusammenhängen, etwa im Bereich der Bekämpfung von Straftaten. Dort besteht eine Pflicht zur Offenbarung von Patientendaten aber nicht generell, sondern lediglich in konkreten Ermittlungsfällen. Demgegenüber sieht der Vorschlag der Kommission vor, dass die Zugangsstellen für Gesundheitsdaten generell allgemeine Beschreibungen der elektronischen Gesundheitsdaten zu veröffentlichen haben, um einen effektiven Datenzugang zu ermöglichen. Damit wird der Zugang zu elektronischen Gesundheitsdaten systematisch eröffnet. Daten und die ärztliche Schweigepflicht werden damit grundsätzlich infrage gestellt.

Hochproblematisch und in Entgegensetzung zum Grundsatz der Datenminimierung aus Art. 5 Abs. 1 Buchst. c DSGVO ist die geplante Verpflichtung der Dateninhaber nach Art. 33 des Verordnungsentwurfs, auf Anforderung regelmäßig **Klardaten** den

Zugangsstellen für Gesundheitsdaten zuzuleiten. Zunächst ist es nicht nachvollziehbar, aus welchen praktischen Gründen die Übermittlung von pseudonymisierten Daten nicht möglich sein soll, zumal entsprechende Modelle in den Mitgliedstaaten existieren – und funktionieren. Dieser Mangel wird dadurch verstärkt, dass der Verordnungsvorschlag keine konkreten Vorgaben zur organisatorischen Ausgestaltung der Zugangsstellen macht. Beispielsweise hätte es gravierende Folgen, wenn kriminelle Organisationen im Rahmen erfolgreicher Hackerangriffe die gesammelten Gesundheitsdatenprofile einer Zugangsstelle ableiten würden. Zwar dürften die technisch-organisatorischen Vorgaben der Datenschutz-Grundverordnung wohl gelten – aufgrund der Konzeption der Datenschutz-Grundverordnung als allgemeines Datenschutzgesetz sind sie aber zu unspezifisch, um insoweit rechtsklare Vorgaben an die Zugangsstellen zu formulieren.

Bedenken löst auch der Umfang der bereitzustellenden Daten aus, der neben elektronischen Patientenakten sensible elektronische Gesundheitsdaten unter anderem aus psychiatrischen Behandlungen, genetische Daten, Material aus der bildgebenden Diagnostik oder gesundheitsrelevante Verhaltensdaten umfasst (vgl. Art. 33 des Verordnungsentwurfs). Vor allem aber ist problematisch, dass der Vorschlag einen weit gefassten Katalog von berechtigten Sekundärnutzungszwecken für den Datenzugang vorsieht – **ohne dass der betroffenen Person insoweit ein wie auch immer geartetes Mitspracherecht hinsichtlich der Weiterverwendung ihrer Gesundheitsdaten eingeräumt wird.** Das begründet erhebliche grundrechtliche Bedenken, weil die aufgeführten berechtigten Datenzugangsinteressen hinsichtlich ihrer Legitimität höchst unterschiedliche Gewichte haben, aber auf der legislativen Ebene gleich behandelt werden. Beispielsweise soll das Datenzugangsinteresse „Pandemiebekämpfung“ auf der Ebene des Vorschlags genauso behandelt (Art. 34 Abs. 1 Buchst. a des Verordnungsentwurfs) werden wie „Bildungs- und Lehrtätigkeiten im Gesundheits- und Pflegesektor“ (Art. 34 Abs. 1 Buchst. d des Verordnungsentwurfs). Dabei ist es offensichtlich, dass in dem einen Fall eine flächendeckende Erhebung von pseudonymisierten Gesundheitsdaten im substantiellen Interesse der Gesamtbevölkerung liegt, während es in dem anderen Fall nicht ansatzweise ersichtlich ist, wieso eine solche Verarbeitung nicht auf eine ausdrückliche Einwilligung der betroffenen Personen gestützt werden soll. Schon allein um eine unterschiedliche Handhabung in den Mitgliedstaaten zu vermeiden, muss die Verordnung insoweit selbst eine unterschiedliche Gewichtung der Datenzugangsinteresse vornehmen, anstatt dies dem Verwaltungsvollzug durch die nationalen Zugangsstellen für Gesundheitsdaten zu überlassen. Mit anderen Worten müsste der Katalog des Art. 34 Abs. 1 des Verordnungsentwurfs durch eine Regelung ersetzt werden, bei der nur zum Schutz vor schwerwiegenden Gesundheitsgefahren der Bevölkerung von der Mitgestaltung der betroffenen natürlichen Personen abgesehen wird. Im Übrigen sollten die natürlichen Personen ihre Zustimmung zur Sekundärnutzung geben müssen oder zumindest ein voraussetzungsfreies Recht zum Widerspruch erhalten. Hochproblematisch ist zudem die in Art. 46 Abs. 3 des Verordnungsentwurfs vorgesehene Genehmigungsfiktion, nach der Grundrechtseingriffe ohne eine entsprechende Prüfung und Entscheidung der zuständigen Behörde legitimiert werden sollen.

Mittlerweile hat das Europäische Parlament erfreulicherweise einen Teil der Kritik aufgegriffen. Es bleibt daher zu hoffen, dass dem Grundrechtsschutz der betroffenen Personen im weiteren Verlauf des Gesetzgebungsverfahrens ein größeres Gewicht beigemessen wird. Auf die datenschutzrechtlichen Anforderungen im Zusammenhang mit dem Europäischen Gesundheitsdatenraum hat jüngst auch eine Stellungnahme der Datenschutzkonferenz aufmerksam gemacht (Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

vom 27. März 2023, Nutzung von Gesundheitsdaten braucht Vertrauen – Der Europäische Gesundheitsdatenraum darf das Datenschutzniveau der Datenschutz-Grundverordnung nicht aushöhlen[20]). Diese Stellungnahme habe ich unterstützt. Selbstverständlich kann ich das grundsätzliche Anliegen nachvollziehen, dass elektronische Gesundheitsdaten wirtschaftlich interessant sind. Ihre effektivere Nutzung kann zu einer Wertschöpfung beitragen. Auch soweit der geplante Gesundheitsdatenraum die wissenschaftliche Forschung bei der Nutzung von Gesundheitsdaten unterstützen soll, ist dies im Grundsatz nachvollziehbar. Allerdings hebt die Europäische Erklärung zu den digitalen Rechten und Grundsätzen für die digitale Dekade ausdrücklich hervor, dass der Mensch im Mittelpunkt des digitalen Wandels stehen soll. Ein zentraler Aspekt ist dabei die **uneingeschränkte Achtung der Grundrechte**. Dies kann nach meinem Verständnis nur bedeuten, dass gerade beim Teilen und Nutzen von sensiblen Gesundheitsdaten die betroffenen Personen die sie betreffenden Verarbeitungsvorgänge mitgestalten können.

1.2 Vertretung der Länderinteressen im Europäischen Datenschutzausschuss (EDSA)

Seit 25. Juni 2021 ist der Bayerische Landesbeauftragte für den Datenschutz der „Stellvertreter des gemeinsamen Vertreters“ im Europäischen Datenschutzausschuss (EDSA). Der EDSA ist eine Einrichtung der Europäischen Union, in der die Mitgliedstaaten jeweils durch den Leiter einer nationalen Datenschutz-Aufsichtsbehörde vertreten sind. Er soll insbesondere die einheitliche Anwendung der Datenschutz-Grundverordnung sicherstellen. In diesem Rahmen stellt der EDSA einheitliche Dokumente, wie 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 EDSA in Kohärenzverfahren Beschlüsse fassen. Ferner fördert er die Zusammenarbeit zwischen den nationalen Datenschutz-Aufsichtsbehörden. Da in Deutschland mehrere Datenschutz-Aufsichtsbehörden bestehen, sieht § 17 Bundesdatenschutzgesetz vor, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die Funktion des gemeinsamen Vertreters im EDSA wahrnimmt. Sein vom Bundesrat zu wählender Stellvertreter nimmt die Stimme Deutschlands im Europäischen Datenschutzausschuss nicht nur im Verhinderungsfall wahr. Der gemeinsame Vertreter überträgt vielmehr auch in bestimmten, für die Länder wichtigen Angelegenheiten seinem Stellvertreter die Verhandlungsführung und das Stimmrecht im Europäischen Datenschutzausschuss. In diesem Sinne nimmt der Vertreter des gemeinsamen Vertreters vor Allem die Interessen der Datenschutzaufsichtsbehörden der Länder wahr. Der EDSA erfüllt seine Aufgaben, indem er auf der Grundlage von mittelfristigen Strategien jährliche Arbeitsprogramme aufstellt. Die erste **EDSA-Strategie** wurde vor meiner Wahl angenommen (am 15. Dezember 2020) und betrifft den Zeitraum 2021 bis 2023. Sie bietet keinen umfassenden Überblick über die Arbeit des EDSA, sondern legt vier „tragende Säulen“ und „Schlüsselaktionen“ fest, mit denen er seine strategischen Ziele erreichen will. Die vier tragenden Säulen bestehen in der Förderung der Harmonisierung und Erleichterung der Einhaltung datenschutzrechtlicher Vorschriften, der Unterstützung einer wirksamen Rechtsdurchsetzung und einer effizienten Zusammenarbeit zwischen nationalen Aufsichtsbehörden, der Wahl eines grundrechtlichen Ansatzes für neue Technologien sowie der Förderung des EU-Datenschutzes als globales Modell in der Welt.

20 Text auf https://www.datenschutz-bayern.de, Rubrik „Konferenzen“.

Im Berichtsjahr hat der EDSA 15-mal in Videokonferenzen und in Präsenz getagt. Zudem fand im April 2022 in Wien ein Treffen der Mitglieder des EDSA statt, um die grundsätzliche Ausrichtung des Gremiums zu überprüfen und eine verbesserte Zusammenarbeit in der Durchsetzung des Datenschutzes in den Blick zu nehmen. Das Plenum wird durch seine Arbeitsgruppen unterstützt, die in zahlreichen Sitzungen die Entscheidungen des EDSA vorbereiten. In diesem Zusammenhang danke ich herzlich allen Mitarbeiterinnen und Mitarbeitern der Datenschutz-Aufsichtsbehörden von Bund und Ländern, die mit großem Engagement und großer Fachkunde dem Plenum und den Arbeitsgruppen zugearbeitet haben.

Ein Hauptschwerpunkt der EDSA-Arbeit bestand auch im Berichtszeitraum in der Annahme von Leitlinien, Empfehlungen und Stellungnahmen. Daneben hat der EDSA im Jahr 2022 mehrere Entscheidungen in Streitbeilegungsverfahren gefällt. Soweit die angenommenen Dokumente für die Länder und damit auch für die bayerischen öffentlichen Stellen besonders relevant sind, werden sie an gesonderter Stelle vorgestellt (siehe Nr. 14). Im Übrigen wird auf die auf der Webseite des EDSA veröffentlichten Dokumente verwiesen.[21]

1.3 Über diesen Tätigkeitsbericht

Die europäische Datenstrategie und die in ihr wurzelnden Unionsrechtsakte werden in den nächsten Jahren auch die Arbeit der Datenschutz-Aufsichtsbehörden in den Mitgliedstaaten, in Deutschland wie in Bayern zunehmend prägen. Bei alldem ist jedoch auch die „klassische" Datenschutzarbeit zu leisten: Nach Art. 15 Abs. 1 Satz 1 BayDSG habe ich die Einhaltung der Datenschutz-Grundverordnung, des Bayerischen Datenschutzgesetzes sowie anderer Vorschriften über den Datenschutz bei den bayerischen öffentlichen Stellen zu überwachen. Dabei verfolge ich stets einen präventiven Ansatz: Guter Datenschutz reagiert nicht in erster Linie mit harten Sanktionen auf spektakuläre Datenschutzverletzungen, sondern versucht, zu deren Vermeidung anzuleiten.

Ein zentrales Instrument ist dabei die Vermittlung von Wissen. Ich möchte möglichst viele bayerische öffentliche Stellen in die Lage versetzen, Verarbeitungen personenbezogener Daten in ihrem jeweiligen Aufgabenbereich rechtskonform zu gestalten. Daher habe ich im Berichtszeitraum mein im innerdeutschen Vergleich mittlerweile wohl führendes **Informationsangebot für den öffentlichen Sektor** weiter ausgebaut und aktualisiert. Beitrag Nr. 2.1 gibt dazu einen Überblick. Aus dem allgemeinen Datenschutzrecht möchte ich als Beispiele die Beiträge Nr. 2.2 und 2.3 nennen, in denen bayerische öffentliche Stellen erfahren, was beim **Versand von Hybridbriefen** und beim **Einsatz externer Schriftarten auf Webseiten** zu beachten ist.

Zum präventiven Datenschutz gehört die **Beratung an der Gesetzgebung beteiligter Stellen**, insbesondere der Staatsministerien. Meine Einbindung in die entsprechenden Verfahren gestaltet sich in Einklang mit Art. 16 Abs. 3 BayDSG und § 7 Abs. 4 Satz 1 Geschäftsordnung der Bayerischen Staatsregierung meist reibungslos. Ich werde frühzeitig beteiligt, und meine Hinweise werden gehört, meine Optimierungsvorschläge erfreulich oft aufgegriffen. Im Berichtszeitraum findet sich allerdings auch ein Gegenbeispiel. Bei der **Novelle des Bayerischen Universitätsklinikagesetzes** hat sich das zuständige Staatsministerium meinen eingehend begründeten datenschutzrechtlichen Monita gegenüber weitgehend verschlossen und Verarbeitungs-

[21] Internet: https://edpb.europa.eu/edpb_de.

vorschriften eingebracht, die Patientenrechte einseitig zugunsten von Forschungsinteressen verkürzen. Die Neuregelung erscheint in Anbetracht der gegenwärtigen Regulierung des europäischen Gesundheitsdatenraums zudem als übereilt.

Bei der Bayerischen Polizei habe ich weiterhin die Bemühungen zur Einführung einer **Verfahrensübergreifenden Recherche- und Analyseplattform** (VeRA) kritisch begleitet. In meinem Eintreten für einen rechtsstaatlich erträglichen Handlungsrahmen habe ich Unterstützung durch das Bundesverfassungsgericht erfahren. In einer Entscheidung zum Polizeirecht einiger anderer Bundesländer griff das Gericht Argumente auf, die ich seit jeher auch der Bayerischen Polizei entgegenhalte (Beitrag Nr. 3.1). „Kleinere" Erfolge konnte ich etwa bei der **Beschleunigung von Auskunftsverfahren** sowie bei der **Nutzung privater Smartphones** durch Polizeibeamte erreichen (Beiträge Nr. 3.2 und 3.4). Im Bereich des Verfassungsschutzes habe ich gegenüber dem Bayerischen Landtag zu **Löschmoratorien** Stellung genommen, welche die Arbeit des **NSU-Untersuchungsausschusses** erleichtern sollen, jedoch datenschutzrechtliche Fragen aufwerfen (Beitrag Nr. 3.5). Bei der Justiz erstreckt sich meine Aufsichtskompetenz zwar nicht auf richterliche Tätigkeiten; zu überprüfen hatte ich jedoch etwa **Datenübermittlungen von Staatsanwaltschaften an Jugendämter und Ausländerbehörden** (Beiträge Nr. 4.2 und 4.3). Gegenüber einem **Notar** habe ich wegen **unzulässiger Einsichtnahme in ein Grundbuch** eine förmliche **Beanstandung** ausgesprochen (Beitrag Nr. 4.5).

Was den kommunalen Bereich betrifft, habe ich mich grundsätzlich zu den Regelungsmöglichkeiten geäußert, die Gemeinden bei **Datennutzungssatzungen** zustehen (Beitrag Nr. 5.1). Gemeinden können sich zwar kein eigenes Datenschutzrecht schaffen, das als einengend empfundene Vorgaben einfach beiseiteschiebt. Sie sollten aber einige Spielräume kennen, die durch Ortsrecht ausgefüllt werden dürfen. Einer eingehenden Prüfung habe ich das **E-Ticket-System** eines kommunalen Verkehrsunternehmens unterzogen (Beitrag Nr. 5.2). In einigen Details konnten hier Optimierungsbedarfe aufgezeigt werden. Die Gemeinden als Meldebehörden möchte ich darauf aufmerksam machen, dass **Melderegisterauskünfte** nur aus dem **örtlichen Meldedatenbestand** erteilt werden dürfen und ein **automatisierter Abruf aus dem Ausländerzentralregister** auch zum Zweck der Verwaltungsvereinfachung nicht eingerichtet werden darf (Beiträge Nr. 6.2 und 6.3). Meine Beratungstätigkeit bei der Schaffung einheitlicher Regelungen für die Inanspruchnahme **staatlicher Rechenzentren als Auftragsverarbeiter** habe ich auch im Berichtszeitraum fortgeführt. (Beitrag Nr. 6.1).

Im Bereich der Sozial- und Gesundheitsverwaltung sind viele Datenschutzfragen im Zusammenhang mit der COVID-19-Pandemie mittlerweile geklärt, teilweise haben sie auch an Interesse verloren; Themen waren insofern noch die **Symptomabfrage durch Gesundheitsämter** oder die **Impfstatusabfrage** bei Besucherinnen und Besuchern **in öffentlichen Krankenhäusern** (Beträge Nr. 7.2 und 7.4). Daneben waren „coronafreie" Datenschutzfragen wie die **Evaluierung des Bayerischen Krebsregistergesetzes** oder die **datenschutzrechtliche Verantwortlichkeit in Bereitschaftspraxen** der Kassenärztlichen Vereinigung Bayerns zu würdigen (Beiträge Nr. 7.3 und 7.5).

Bei der Steuer- und Finanzverwaltung ist die Funktion der Datenschutz-Aufsichtsbehörde weithin dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zugewiesen; dies gilt auch für die bayerischen Finanzämter. Das Steuerrecht setzt mit einer Sonderregelung auf eine bundesweite Zentralisierung. Neue Fragen der Abgrenzung zu meinen Zuständigkeiten stellten sich im Berichtszeitraum durch

Einführung der **bayerischen Grundsteuer**. In Bezug auf die Verwaltung dieser Landessteuer sehe ich derzeit mich als zuständige Datenschutz-Aufsichtsbehörde an (Beitrag Nr. 8.1). Meine ersten Erfahrungen mit der Wahrnehmung dieser Zuständigkeit habe ich für einige Fallgruppen dargestellt (Beitrag Nr. 8.2).

Im Bereich des Personaldatenschutzes standen Fragen der Verarbeitung von **Immunitätsnachweisen bei der einrichtungsbezogenen Impfpflicht** (Beitrag Nr. 9.1) noch im Zusammenhang mit der COVID-19-Pandemie. In gleich zwei beachtenswerten Einzelfällen kam es zu förmlichen **Beanstandungen** allzu dokumentationsfreudiger öffentlicher Arbeitgeber; hier ging es um eine **verdeckte Tonaufzeichnung** der Äußerungen einer Beschäftigten **während einer Videokonferenz** (Beitrag Nr. 9.3) und – wieder einmal – um den illegalen **Einsatz von Ortungssystemen in Dienstkraftfahrzeugen** (Beitrag Nr. 9.4). Ein grundsätzlicher Beitrag (Nr. 9.5) widmet sich dem Schicksal des dienstlichen E-Mail-Accounts eines verstorbenen Professors, der im Ruhestand noch an seiner Hochschule tätig war.

Was den Datenschutz an Schulen und Hochschulen betrifft, habe ich im Berichtszeitraum eine Überarbeitung der einschlägigen Bestimmungen des **Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen,** der **Bayerischen Schulordnung** sowie der zugehörigen **Verwaltungsvorschriften** beratend unterstützt (Beitrag Nr. 10.1). Eingehend habe ich mich mit der Verarbeitung personenbezogener Daten im Rahmen der **Videoaufsicht bei Fernprüfungen** an bayerischen Hochschulen auseinandergesetzt (Beitrag Nr. 10.2). Eine nicht unerhebliche Anzahl von Eingaben erreichte mich im Zuge des **Zensus 2022**; die wichtigsten Fragen habe ich in einem Überblicksbeitrag dargestellt (Nr. 11.1).

Zum technisch-organisatorischen Datenschutz gibt mein Tätigkeitsbericht für das Jahr 2022 wieder eine Vielzahl von Impulsen: Mein Angebot an Materialien zur **Datenschutz-Folgenabschätzung** – einem in der Datenschutz-Grundverordnung zentralen Instrument des systematischen Auffindens und Bewältigens von Risiken – hat die nächsthöhere Ausbaustufe erreicht (Beitrag Nr. 12.2); grundsätzlich habe ich mich mit den datenschutzrechtlichen Anforderungen an sog. **Penetrationstests** befasst, welche die Sicherheit von IT-Systemen gezielt auf die Probe stellen (Beitrag Nr. 12.1). Die **unbeabsichtigte Veröffentlichung personenbezogener Daten im Internet** kommt leider auch bei bayerischen öffentlichen Stellen vor; zu einigen im Rahmen meiner Aufsichtstätigkeit wiederkehrenden Fallgruppen erläutere ich Maßnahmen der Fehlervermeidung (Beitrag Nr. 12.4). In einer **Umfrage bei den bayerischen Gesundheitsämtern** zur Datenverarbeitung im Zusammenhang mit der COVID-19-Pandemie konnte ich einige neue Erkenntnisse gewinnen (Beitrag Nr. 12.5).

Die **Datenschutzkommission beim Bayerischen Landtag**, die nach Art. 17 Abs. 1 Satz 1 BayDSG meine Arbeit unterstützt, hat im Berichtszeitraum drei Mal getagt. Dem Gremium, einer bayerischen Besonderheit, deren Tradition bis zum Bayerischen Datenschutzgesetz von 1978 zurückreicht, gehören sechs Mitglieder aus der Mitte des Landtags sowie vier externe Mitglieder an. Den mit den Sitzungen der Datenschutzkommission verbundenen intensiven Austausch über aktuelle datenschutzpolitische wie datenschutzrechtliche Fragen, über Gesetzesvorhaben, auch über Maßnahmen, die ich im Rahmen meiner Aufsichtstätigkeit getroffen habe, empfinde ich stets als bereichernd. Ich möchte daher die Gelegenheit nutzen, den Mitgliedern der Datenschutzkommission für ihre nicht im Fokus der Öffentlichkeit stehende Arbeit meinen ganz herzlichen Dank auszusprechen.

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 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.

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

– Die Orientierungshilfe **„Das Recht auf Löschung nach der Datenschutz-Grundverordnung“** widmet sich Art. 17 DSGVO, einem wichtigen Betroffenenrecht. Voraussetzungen und Rechtsfolge werden Schritt für Schritt anhand zahlreicher Beispiele erläutert; eine ausführliche Behandlung erfahren auch die Ausschlussgründe. Bayerische öffentliche Stellen finden so Anleitung bei der Bearbeitung von Löschungsanträgen; Bürgerinnen und Bürger können nachlesen, wie Löschungsansprüche zu verwirklichen sind.

– Die Orientierungshilfe **„Risikoanalyse und Datenschutz-Folgenabschätzung“** bildet einen wesentlichen Baustein in einem größeren Informationspaket, das in Beitrag Nr. 12.2 näher vorgestellt ist.

Das im Berichtszeitraum veröffentlichte Arbeitspapier **„Datenschutz bei der Nutzung von Telefax-Diensten“** nimmt ein bereits etwas betagtes, im öffentlichen Sektor jedoch noch immer beliebtes Kommunikationsmittel in den Blick und formuliert auf aktuellem Stand datenschutzrechtliche Anforderungen an einen sicheren Einsatz. Fortgesetzt habe ich die Reihe der **Aktuellen Kurz-Informationen**; vier dieser Papiere erschienen neu, fünf bereits früher publizierte wurden dem aktuellen Rechtsstand angepasst.

Ferner habe ich im Berichtsjahr den Newsletter **„Privacy in Bavaria“** neu eingeführt, der stets auf nur einer DIN A4-Seite neueste aufsichtsbehördliche Veröffentlichungen, Judikatur und Hinweise auf praxisrelevante Fachbeiträge vorstellt, jeweils mit einer kurzen Information zum datenschutzrechtlichen „Nährwert“. Ab Juni erschienen in unregelmäßigen Abständen sieben Ausgaben in deutscher und englischer Sprache. So erhalten nicht nur bayerische öffentliche Stellen und ihre behördlichen Datenschutzbeauftragten alle paar Wochen ein Update zur Entwicklung des Datenschutzrechts im öffentlichen Sektor; auch jenseits der Landesgrenzen ist die Möglichkeit eröffnet, bei geringem Aufwand Blicke auf die bayerische – und deutsche – Datenschutzwelt zu werfen.

Zudem habe ich mich im Berichtsjahr entschlossen, eine Präsenz in den Sozialen Medien aufzubauen. Dabei wird es nicht überraschen, dass ich besonders darauf geachtet habe, ein datenschutzkonform zu nutzendes Instrument auszusuchen. Meine Wahl fiel auf den Microblogging-Dienst **Mastodon**, der auch vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit genutzt wird. Ich freue mich, dass mein Account **https://social.bund.de/@BayLfD** dort einen Host gefunden hat. Ich nutze den Kanal derzeit schwerpunktmäßig dafür, über meine aktuellen Publikationen zu informieren; er bietet so neben dem seit Langem bestehenden RSS-Feed eine weitere Option, datenschutzfachlich auf dem Laufenden zu bleiben.

Der Kanal bringt darüber hinaus auch Mastodon-exklusive Informationen. Dazu gehört etwa die **„Datenschutzfrage der Woche“** (#DPQW): Außerhalb der bayerischen Schulferien gibt es seit Dezember jeden Donnerstag eine Frage und eine Antwort – beides grundsätzlich höchstens 500 Zeichen lang. Datenschutzwissen so knapp zu verpacken, ist manches Mal eine Herausforderung. Erfreulicherweise haben mir auch Nutzende des Kanals bereits Vorschläge für dieses Format zukommen lassen. Die Mastodon-Aktion **„Wie bekomme ich die Cookies auf meiner Homepage unter Kontrolle?“** leitete fünf Tage lang in 17 Posts mit zahlreichen verlinkten Materialien durch ein Prüfprogramm, das zur datenschutzrechtlichen Optimierung von Webseiten nicht nur bayerischer öffentlicher Stellen beitragen kann.

Für das **Jahr 2023** ist ein weiterer Ausbau des Informationsangebots in den klassischen Formen von Orientierungshilfen, Arbeitspapieren und Aktuellen Kurz-Informationen, mit dem Newsletter sowie auf meinem Mastodon-Kanal geplant.

2.2 Versand von Hybridbriefen durch bayerische öffentliche Stellen

Im Zuge der fortschreitenden Digitalisierung entstehen neue, ganz oder teilweise elektronische Postdienstleistungen. Dies gilt auch für den Bereich der Briefübermittlung. Bayerische öffentliche Stellen können insbesondere Angebote sogenannter Hybridbriefe nutzen. Hybridbriefe verbinden elektronische und papierförmige Kommunikation. Das Dokument wird vom Absender elektronisch verfasst und mitsamt den notwendigen Adressdaten elektronisch an einen Postdienstleister oder einen mit diesem kooperierenden Dienstleister übermittelt. Dort wird der Brief ausgedruckt, kuvertiert und frankiert; anschließend wird er durch den Postdienstleister dem Empfänger analog zugeleitet.

Mich erreichen immer wieder Anfragen bayerischer öffentlicher Stellen, die den Hybridbrief gerade für Massenverwaltungsverfahren nutzen möchten, jedoch unsicher sind, was dabei datenschutzrechtlich zu beachten ist. Die vorliegende Aktuelle Kurz-Information zeigt auf, welche Rolle das Datenschutzrecht auf den einzelnen Abschnitten des Weges spielt, den ein Hybridbrief von seinem Absender zum Empfänger nimmt (Nr. 2.2.1 bis 2.2.3). Sie geht auf das Verhältnis zwischen dem Absender und „seinem“ Postdienstleister ein (Nr. 2.2.4) und gibt Hinweise zur Gewährleistung eines angemessenen Schutzniveaus während des Kommunikationsprozesses (Nr. 2.2.5).

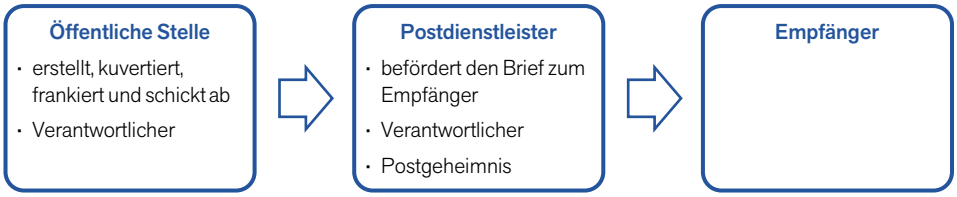
2.2.1 Verarbeitung personenbezogener Daten beim Hybridbrief

Briefe enthalten mit obligatorischen Angaben der Absender- und Empfängeradresse, aber auch inhaltlich („im Umschlag“) regelmäßig eine Vielzahl personenbezogener Daten. Beim herkömmlichen Briefversand verfasst und verschickt eine bayerische öf-

fentliche Stelle den Brief und verarbeitet dabei die personenbezogenen Daten aufgrund der jeweiligen – gegebenenfalls fachgesetzlichen – Rechtsgrundlagen. Der konventionelle Brief- und Pakettransport durch einen Postdienstleister wird datenschutzrechtlich üblicherweise als eine Datenverarbeitung durch einen eigenständigen Verantwortlichen angesehen. Dahinter steht die Überlegung, dass die Postdienstleistung im Kern keine Verarbeitung personenbezogener Daten zum Gegenstand habe, sondern diese Verarbeitung nur eine unvermeidliche „Begleiterscheinung" sei, und der Postdienstleister daher nicht im Auftrag und nach Weisung Daten verarbeite, wie dies bei der Auftragsverarbeitung der Fall sei.[22]

Der Postdienstleister nimmt zum Zweck der Zustellung von den Adressdaten Kenntnis, grundsätzlich jedoch nicht vom Inhalt der Postsendung, der durch das Postgeheimnis geschützt ist. Postdienstleistung ist gemäß § 4 Nr. 1 Postgesetz (PostG) die gewerbsmäßige Sendungsbeförderung. Als eigenständiger Verantwortlicher muss der Postdienstleister die Verarbeitung personenbezogener Daten auf eine Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 DSGVO stützen können. Gesetzliche Verarbeitungsbefugnisse, die sich auf die Verarbeitung der Adressdaten zum Zwecke der ordnungsgemäßen Zustellung von Postsendungen beziehen, enthält § 41a PostG.

Klassischer Briefversand

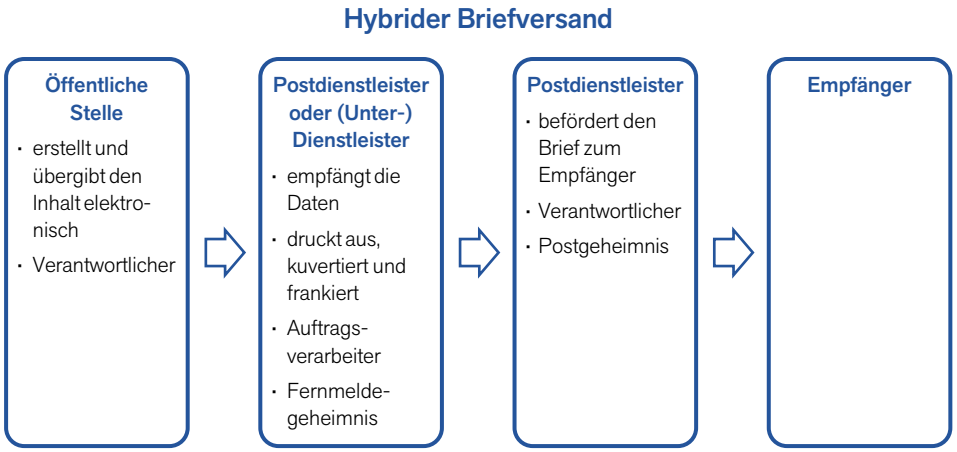


Der Versand von Hybridbriefen unterscheidet sich vom klassischen Briefversand durch seine Mehrstufigkeit. Das Dokument wird zunächst vom Absender elektronisch verfasst, dann aber nicht selbstständig ausgedruckt, kuvertiert und abgeschickt, sondern elektronisch an den Postdienstleister oder ein mit diesem kooperierendes Unternehmen übermittelt. Dieser Datentransfer ist der anknüpfenden klassischen Briefzustellung vorgelagert. Er unterliegt – soweit im Rahmen einer Telekommunikationsdienstleistung erbracht – dem Fernmeldegeheimnis, während die anschließende Beförderung des fertiggestellten Briefs als Postdienstleistung – wie bei der klassischen Briefzustellung – dem Postgeheimnis unterfällt.[23]

Die Besonderheit des Hybridbrief-Versands liegt also darin, dass die eigentliche Erstellung des papierförmigen Briefs aus den übermittelten elektronischen Daten als (zusätzliche) Dienstleistung an den Postdienstleister oder ein kooperierendes Unternehmen ausgelagert wird. Soweit es bei Hybridbriefen zum Transport des fertiggestellten Briefs kommt, ergeben sich keine Unterschiede hinsichtlich der datenschutzrechtlichen Verantwortlichkeit im Vergleich zum klassischen Brieftransport: Der fertiggestellte Hybridbrief wird durch den Postdienstleister, der als eigenständiger Verantwortlicher fungiert, zugestellt.

22 Vgl. Arning/Rothkegel, in: Taeger/Gabel, DSGVO/BDSG/TTDSG, 4. Aufl. 2022, Art. 4 DSGVO Rn. 258.

23 Vgl. Altenhain, in: Münchener Kommentar zum StGB, 4. Aufl. 2021, § 206 StGB Rn. 33.



Die eingeschobene Phase der elektronischen Datenübertragung und Brieferstellung hält auch rechtliche Besonderheiten bereit:

Hier wird die – wenngleich automatisierte (vgl. Art 4 Nr. 2 DSGVO) – Verarbeitung von Inhaltsdaten Gegenstand der Dienstleistung. Für diese Verarbeitung personenbezogener Daten durch den Postdienstleister oder ein mit diesem kooperierendes Unternehmen existiert keine gesetzliche Verarbeitungsbefugnis. Die Leistung kann allerdings im Rahmen eines Auftragsverarbeitungs-Verhältnisses (Art. 4 Nr. 8, Art. 28 DSGVO) für den Absender erbracht werden. Aufgrund der Privilegierung der Auftragsverarbeitung – die Verarbeitung des Auftragsverarbeiters leitet sich letztlich von der Rechtsgrundlage des Verantwortlichen ab[24] – bedarf der jeweilige Dienstleister für diese Phase des Hybridbriefversands keiner eigenständigen Rechtsgrundlage. Die bayerische öffentliche Stelle als Auftraggeber muss dann sicherstellen, dass die gesetzlichen Vorgaben für eine Auftragsverarbeitung eingehalten werden.

Abzugrenzen vom Hybridbrief-Versand ist die medienbruchfreie und somit durchgängig elektronische Briefübermittlung, wie sie beispielweise im De-Mail-Gesetz (DeMailG) geregelt ist.

Ob und zu welchen Bedingungen der Einsatz von Hybridbriefen in Betracht kommt, ist vom Verantwortlichen unter Beachtung der nachstehenden Ausführungen zu entscheiden.

2.2.2 Normative Übermittlungsregelungen

Existieren für die betrachtete Übermittlung – von eventuell vorhandenen, spezialgesetzlichen Regelungen zu einer Auftragsverarbeitung abgesehen (dazu Nr. 2.2.4) – einschlägige Übermittlungsvorschriften, etwa Regelungen zur elektronischen Kommunikation, so ist deren Einhaltung vorab zu prüfen. Zu berücksichtigen sind insbesondere Anforderungen an die Form der zu übermittelnden Dokumente oder an Übermittlungsmodalitäten.

Da Hybridbriefe letztlich ausgedruckt werden, kommen sie jedenfalls dann nicht in Betracht, wenn auch der herkömmliche Postversand ausscheidet, also wenn etwa gesetzlich eine rein elektronische Kommunikation geboten ist, vgl. etwa Art. 20 Abs. 3

[24] Vgl. Bayerischer Landesbeauftragter für den Datenschutz, Auftragsverarbeitung, Orientierungshilfe, Stand 4/2019, S. 7, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Auftragsverarbeitung".

Bayerisches Digitalgesetz. Gesetzliche Vorgaben, elektronische Kommunikationsformen zu nutzen (vgl. etwa die „Soll"-Vorschrift des § 67 Abs. 1 Fünftes Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung –), sollten daher nicht als Aufforderung zur Nutzung von Hybridbriefverfahren missverstanden werden. Nicht abschließend geklärt ist, ob Hybridbriefe geeignet sind, verwaltungsverfahrensrechtliche Anforderungen an die Schriftform zu erfüllen.[25]

2.2.3 Informationspflichten

Eine weitere Besonderheit ergibt sich hinsichtlich der Informationspflichten des datenschutzrechtlich Verantwortlichen, der ein Hybridbrief-Angebot nutzt. Eine bayerische öffentliche Stelle hat als Absender im Rahmen ihrer Informationspflichten gemäß Art. 13 Abs. 1 Buchst. e DSGVO und Art. 14 Abs. 1 Buchst. e DSGVO auf den jeweiligen Postdienstleister und/oder dessen Kooperationspartner als Empfänger von personenbezogenen Daten hinzuweisen. Schließlich können auch Auftragsverarbeiter „Empfänger" im Sinne von Art. 4 Nr. 9 DSGVO sein. Zwar werden auch beim klassischen Briefversand die personenbezogenen Adressdaten des Briefempfängers dem Postunternehmen als Datenempfänger offenbart. Die Tatsache der Offenbarung von Adressdaten gegenüber dem Postunternehmen zum Zwecke der Briefzustellung ist der empfangenden betroffenen Person allerdings regelmäßig bereits bekannt, so dass sich eine gesonderte Information gegebenenfalls gemäß Art. 13 Abs. 4 DSGVO, Art. 14 Abs. 5 Buchst. a DSGVO erübrigt. Der betroffenen Person ist aber von sich aus regelmäßig nicht bekannt, ob die absendende bayerische öffentliche Stelle vom Hybridbriefverfahren Gebrauch macht oder nicht und in diesem Rahmen nicht nur Adressdaten, sondern auch den Briefinhalt dem Dienstleistungsunternehmen offenbart.

2.2.4 Auftragsverarbeitung und bereichsspezifische Sonderregelungen

Kommt der Postversand mittels Hybridbrief grundsätzlich in Betracht, müssen die Voraussetzungen der Auftragsverarbeitung gemäß Art. 4 Nr. 8, Art. 28 DSGVO eingehalten werden. Die allgemeinen Anforderungen zur Zulässigkeit von Auftragsverarbeitungen sind umfassend in der Orientierungshilfe „Auftragsverarbeitung" dargestellt.[26] Insbesondere muss ein Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter geschlossen werden, der den Anforderungen von Art. 28 Abs. 3 DSGVO genügt.

Möchte sich der Postdienstleister bei der Brieferstellung eines weiteren Dienstleisters als Unter-Auftragsverarbeiter bedienen, so sind insbesondere die Art. 28 Abs. 2 und 4 DSGVO einzuhalten (vgl. auch Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchst. d DSGVO). Dabei ist zu beachten, dass die Einbeziehung eines Unter-Auftragsverarbeiters gemäß Art. 28 Abs. 2 DSGVO stets der Genehmigung des Verantwortlichen bedarf. Der Auftragsverarbeiter muss dem Unter-Auftragsverarbeiter gemäß Art. 28 Abs. 4 DSGVO dieselben vertraglichen Datenschutzpflichten auferlegen, die ihn vertraglich binden.

25 Dafür Schulz, in: Mann/Sennekamp/Uechtritz, Verwaltungsverfahrensgesetz, 2. Aufl. 2019, § 3a VwVfG Rn. 47; kritisch Schmitz, in: Stelkens/Bonk/Sachs, Verwaltungsverfahrensgesetz, 9. Aufl. 2018, § 3a VwVfG Rn. 38h.

26 Vgl. Bayerischer Landesbeauftragter für den Datenschutz, Auftragsverarbeitung, Orientierungshilfe, Stand 4/2019, S. 13 ff., Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Auftragsverarbeitung".

Grundsätzlich muss der Auftragsverarbeitungsvertrag gemäß Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchst. b DSGVO auch gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Dies ist relevant, weil es trotz einer weitgehend automatisierten Datenverarbeitung beim Ausdruck seitens des Auftragsverarbeiters zur Kenntnisnahme durch Beschäftigte kommen kann, wenn etwa bei Wartungsarbeiten oder zur Störungsbehebung technisches Personal Einsicht in Briefe nimmt oder dies stichprobenartig zur Qualitätssicherung erfolgt.

Defizite können hier nicht nur datenschutzrechtliche, sondern – mit Blick auf § 203 Strafgesetzbuch (StGB) – auch strafrechtliche Konsequenzen haben. Beschäftigte bayerischer öffentlicher Stellen können als Amtsträger (vgl. § 11 Abs. 1 Nr. 2 StGB) gemäß § 203 Abs. 2 Satz 1 Nr. 1 StGB Geheimnisträger sein. Eine gesetzliche Offenbarungsbefugnis hat der Gesetzgeber in Bezug auf externe Dienstleister zwar in § 203 Abs. 3 Satz 2 StGB geschaffen. Somit hält sich das Strafbarkeitsrisiko des Amtsträgers bei der Weitergabe entsprechend geschützter Geheimnisse im Rahmen einer zulässigen Auftragsverarbeitung in Grenzen, soweit Auftragsverarbeiter „mitwirkende Personen" im Sinne von § 203 Abs. 3 Satz 2 StGB sein können.[27] Gleichwohl ist auch mit Blick auf die Straftatbestände des § 203 Abs. 4 StGB ein exaktes Vorgehen im Bereich der Informationsweitergabe angezeigt.

Zu beachten sind neben den allgemeinen Vorgaben der Datenschutz-Grundverordnung auch bereichsspezifische Sonderregelungen zur Auftragsverarbeitung, die der Gesetzgeber in besonders sensiblen Fällen eingeführt hat. Sonderregelungen für Auftragsverarbeitungen finden sich etwa im Melderecht, im Steuerrecht, im Sozialrecht und im Personaldatenschutzrecht.[28]

Beispielsweise gilt bei der Verwaltung von Realsteuern (nach § 3 Abs. 2 Abgabenordnung – AO – Grundsteuer und Gewerbesteuer), kommunalen Steuern und Fremdenverkehrsbeiträgen – gegebenenfalls nach Maßgabe von Art. 13 Abs. 1 Nr. 1 Buchst. c Kommunalabgabengesetz – das steuerliche Offenbarungsverbot (§ 30 AO). Nach § 30 Abs. 9 AO dürfen die Finanzbehörden sich bei der Verarbeitung geschützter Daten nur dann eines Auftragsverarbeiters bedienen, wenn diese Daten ausschließlich durch Personen verarbeitet werden, die zur Wahrung des Steuergeheimnisses verpflichtet sind. Soweit diese Personen nicht bereits Amtsträger (vgl. §§ 7, 30 Abs. 1 AO) oder Gleichgestellte (vgl. § 30 Abs. 3 AO) sind, ist eine Verpflichtung nach dem Verpflichtungsgesetz (VerpflG)[29] erforderlich.[30]

Gemäß § 1 Abs. 1 Nr. 2 VerpflG soll auf die gewissenhafte Erfüllung seiner Obliegenheiten verpflichtet werden, wer unter anderem bei einem Betrieb oder Unternehmen, das für eine Behörde oder sonstige Stelle Aufgaben der öffentlichen Verwaltung ausführt, beschäftigt ist. Dies wird bei Beschäftigten eines privaten Dienstleistungsunternehmens, das mit der Erstellung von Hybridbriefen für bayerische öffentliche Stellen

27 Vgl. Weichert, in: Kühling/Buchner, DSGVO/BDSG, 3. Aufl. 2020, Art. 9 DSGVO Rn. 149.

28 Vgl. zu einzelnen Regelungen Bayerischer Landesbeauftragter für den Datenschutz, Leitfaden zum Outsourcing kommunaler IT, Stand 3/2021, S. 6 ff., Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Auftragsverarbeitung".

29 Vgl. allgemein zur Verpflichtung nach dem Verpflichtungsgesetz: Bayerischer Landesbeauftragter für den Datenschutz, Die förmliche Verpflichtung als Instrument des Datenschutzes, Arbeitspapier, Stand 10/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Einzelthemen".

30 Vgl. Rüsken, in: Klein, AO, 15. Aufl. 2020, § 30 AO Rn. 224.

betraut ist, regelmäßig der Fall sein. Im Vertrag über die Auftragsverarbeitung muss zudem festgelegt werden, dass ausschließlich diese besonders verpflichteten Personen tätig werden und der Einsatz von nicht verpflichtetem Personal auch bei Beteiligung von weiteren Auftragsverarbeitern ausgeschlossen ist.

2.2.5 Nachweis eines angemessenen Schutzniveaus

Nach der Datenschutz-Grundverordnung ist jeder Verantwortliche (und grundsätzlich auch jeder Auftragsverarbeiter) verpflichtet, mittels der wirksamen Umsetzung von Schutzmaßnahmen ein dem Verarbeitungsrisiko angemessenes Schutzniveau zu gewährleisten. Welche Schutzmaßnahmen dem Risiko entsprechend wirksam umgesetzt werden müssen, wird grundsätzlich durch eine datenschutzrechtliche Risikoanalyse ermittelt und nachgewiesen.[31]

Bei einer solchen Risikoanalyse sind in dem hier betrachteten Verfahren für den hybriden Briefversand insbesondere folgende Aspekte eingehend zu behandeln:

- **Vertraulichkeit:** Beim Hybridbrief muss die vertrauliche Behandlung der übermittelten personenbezogenen Daten durchgängig gewährleistet werden. Insbesondere bei der elektronischen Übermittlung, bei der Datenaufbewahrung, bei dem (automatisierten) Ausdruck sowie bei der (automatisierten) Kuvertierung sind angemessene Schutzmaßnahmen gegen die unbefugte Kenntnisnahme beim Auftragsverarbeiter wirksam umzusetzen.

- **Datenminimierung:** Zu gewährleisten ist auch, dass nach der Erreichung des Verarbeitungszwecks die Briefdaten – insbesondere der Briefinhalt – beim Auftragsverarbeiter zuverlässig wieder gelöscht werden. Bei Versäumnissen in diesem Bereich kann rasch ein umfangreicher illegaler Datenbestand anwachsen.

- **Nichtverkettung:** Beim Hybridbrief-Verfahren werden nicht nur die Adressdaten, sondern auch die vollständigen Inhalte der Hybridbriefe, die unterschiedliche und sensible Informationen enthalten können, in elektronischer Form beim Auftragsverarbeiter verarbeitet. Die Verarbeitung dieser Daten kann etwa für Werbezwecke des Auftragsverarbeiters sehr gewinnbringend sein. Daher sind Vorkehrungen zu treffen, dass die Daten eines Hybridbriefes vom Auftragsverarbeiter nur für den Versandzweck verarbeitet werden können.

2.2.6 Fazit

Bayerischen öffentlichen Stellen ist es grundsätzlich gestattet, unter Einhaltung datenschutzrechtlicher und technisch-organisatorischer Vorgaben Hybridbriefe zu versenden. Die insoweit erfolgende Verarbeitung personenbezogener Daten muss den Verarbeitungsgrundsätzen gemäß Art. 5 DSGVO entsprechen. Vor Durchführung des

[31] Vgl. Bayerischer Landesbeauftragter für den Datenschutz, Risikoanalyse und Datenschutz-Folgenabschätzung, Orientierungshilfe, Stand 5/2022, Internet: https://www.datenschutz-bayern.de, Rubrik „DSFA“.

Hybridbriefversands ist insbesondere die Einhaltung allgemeiner und bereichsspezifischer Vorgaben zur Auftragsverarbeitung zu prüfen und der Nachweis eines angemessenen Schutzniveaus zu erbringen.

2.3 Externe Schriftarten auf Webseiten bayerischer öffentlicher Stellen

Zur Attraktivität einer Webseite kann auch die typografische Gestaltung beitragen. Viele Webseitenanbieter sind dabei mit den überall verfügbaren Standard-Schriftarten (etwa Times New Roman, Arial, Verdana) nicht zufrieden; sie möchten etwa die „Hausschrift" aus dem eigenen Corporate Design nutzen oder überhaupt eine individuellere Wirkung erzielen. In diesem Zusammenhang kommen neben lizensierten Schriftarten oftmals solche zum Einsatz, die im Internet frei verfügbar bereitgestellt werden, insbesondere in Gestalt von Web Fonts. Auch auf den Internetpräsenzen bayerischer öffentlicher Stellen finden solche Web Fonts Verwendung. Das kann aus Datenschutzsicht Probleme mit sich bringen. Die vorliegende Aktuelle Kurz-Information erläutert, was insofern zu beachten ist.

2.3.1 Was sind Web Fonts?

Web Fonts sind Vektorschriften, die auf einem Bildschirm unabhängig von Plattform (Desktop-PC, Smartphone, Tablet), Betriebssystem und Browser einheitlich dargestellt werden können. Der Browser greift dabei ergänzend zur internen Schriftenbibliothek auf eine im Netz hinterlegte Schriftdatei zu. Im Internet gibt es viele Angebote von Web Fonts. Einer der bekanntesten Drittanbieter dürfte Google mit der Dienstleistung „Google Fonts" sein, in deren Rahmen über 1.000 Schriftarten bereitstehen.

2.3.2 Wie werden Web Fonts in eine Webseite integriert?

Web Fonts können in eine Webseite auf zweierlei Art eingebunden werden: Sie können auf dem eigenen Server des Webseitenbetreibers gehostet werden (Selbsthosting) oder auf dem Server eines Drittanbieters (Fremdhosting).

Üblicherweise werden Web Fonts auf Webseiten in Form des Fremdhostings **extern** integriert. Beim Aufruf der Webseite wird eine Verbindung zum Server des Drittanbieters aufgebaut; der Browser der Nutzerin oder des Nutzers lädt von dort die für die Darstellung der Webseite benötigte Schriftdatei. Technisch wird die Einbindung regelmäßig durch eine Anweisung im HTML-Code der Webseite erreicht. Beim Verbindungsaufbau zum Server des Drittanbieters wird zumindest die IP-Adresse der Nutzerin oder des Nutzers übermittelt. Der Drittanbieter hat damit die Möglichkeit, diese Information – etwa zu Analysezwecken – weiterzuverarbeiten.

Alternativ können Webseitenbetreiber die benötigten Web Fonts **lokal** einsetzen, indem sie die Schriftdateien auf dem eigenen Server verfügbar machen. Ruft eine Nutzerin oder ein Nutzer die Webseite auf, wird der Browser für die Schriftdatei auf die Schriftbibliothek des Webseitenbetreibers verwiesen; eine Verbindung zu einem Drittanbieter wird nicht aufgebaut. Diese Variante erfreut sich allerdings geringerer Beliebtheit als die externe Einbindung, weil ihr längere Ladezeiten zugeschrieben werden.

2.3.3 Dynamische Einbindung nur mit wirksamer Einwilligung

Werden aufgrund der externen Einbindung von Web Fonts Nutzerdaten, etwa die IP-Adresse, an einen Drittanbieter übermittelt, benötigt der Webseitenbetreiber dafür eine Rechtsgrundlage (vgl. Art. 6 Abs. 1 DSGVO).

Der Webseitenbetreiber ist im Falle der Einbindung von Web Fonts als Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO anzusehen, da er über die Mittel und Zwecke der Datenverarbeitung (mit-)entscheidet. Mit der externen Einbettung von Drittdiensten (wie Web Fonts) in die Webseite veranlasst er, dass der Drittanbieter personenbezogene Daten der Nutzerinnen und Nutzer erhält.[32] Zum Erheben und Übermitteln der Nutzerdaten (als Zwischenziel) setzt er Web Fonts wie ein „Werkzeug" ein.[33] Die Verantwortlichkeit ist dem Webseitenbetreiber auch nicht mit der Erwägung abzusprechen, dass er keinerlei Einfluss auf die (Weiter-)Verarbeitung beim Drittanbieter habe.[34] Allerdings ist die Verantwortlichkeit des Webseitenbetreibers auf das Erheben und Übermitteln der Nutzerdaten beschränkt, weil er nur insofern über die Mittel und Zwecke der Verarbeitung bestimmen kann.

Als Rechtsgrundlage kommt bei den Webangeboten bayerischer öffentlicher Stellen in aller Regel nur die Einwilligung (Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO) in Betracht. Diese Stellen können sich – anders als nichtöffentliche – wegen Art. 6 Abs. 1 UAbs. 2 DSGVO nicht auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO berufen. Auch nichtöffentlichen Stellen bliebe die Begründung eines berechtigten Interesses allerdings verwehrt, wenn mit der Möglichkeit einer lokalen Einbindung eine vorzugswürdige Alternative besteht.[35]

Hinweis: Werden beim Abruf von externen Schriftarten im Browser Cookies von Drittanbietern gesetzt oder ausgelesen (Third-Party-Cookies) oder ähnliche Technologien genutzt, ist dafür (zusätzlich) eine Einwilligung nach § 25 Abs. 1 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) erforderlich. Insbesondere greift keine von diesem Erfordernis befreiende Ausnahme nach § 25 Abs. 2 TTDSG ein.[36] Kommen Cookies oder ähnliche Technologien nicht zum Einsatz, ist der Anwendungsbereich des § 25 TTDSG nicht tangiert. Die Rechtmäßigkeit der Datenverarbeitung richtet sich in diesem Fall ausschließlich nach den Bestimmungen der Datenschutz-Grundverordnung.

Wird die Einwilligung mittels eines Einwilligungsbanners oder einer sogenannten Consent Management Plattform (CMP) eingeholt, muss sie den Anforderungen der Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 4 Nr. 11 und Art. 7 DSGVO genügen.[37] Sie muss danach insbesondere freiwillig (Art. 4 Nr. 11 DSGVO), informiert (Art. 4 Nr. 11 DSGVO), auf einen bestimmten Zweck (Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO) und

32 Europäischer Gerichtshof, Urteil vom 29. Juli 2019, C-40/17, NJW 2019, 2755, Rn. 64 ff., 85.
33 Europäischer Gerichtshof, Urteil vom 29. Juli 2019, C-40/17, NJW 2019, 2755, Rn. 77.
34 Europäischer Gerichtshof, Urteil vom 29. Juli 2019, C-40/17, NJW 2019, 2755, Rn. 82.
35 Landgericht München, Urteil vom 20. Januar 2022, 3 O 17493/20, BeckRS 2022, 612, Rn. 8.
36 Näher Bayerischer Landesbeauftragter für den Datenschutz, Bayerische öffentliche Stellen und Telemedien, Stand 12/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018".
37 Dazu im Einzelnen Bayerischer Landesbeauftragter für den Datenschutz, Die Einwilligung nach der Datenschutz-Grundverordnung, Stand 9/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018".

auf eine bestimmte Verarbeitung bezogen (Art. 4 Nr. 11 DSGVO) sowie unmissverständlich (Art. 4 Nr. 11 DSGVO) sein. Die Einwilligung wirkt grundsätzlich bis zu ihrem Widerruf (Art. 7 Abs. 3 Satz 1, 2, Abs. 4 DSGVO).

Für die Einbindung von externen Schriftarten bedeutet dies insbesondere,

— dass keine Daten (IP-Adresse) an Server der Drittanbieter übermittelt werden dürfen, bevor eine Einwilligung mittels Einwilligungsbanners oder CMP erteilt wurde, sowie

— dass insbesondere klar und deutlich anzugeben ist, welche Daten (etwa die IP-Adresse) verarbeitet werden, an wen (Name des Drittanbieters) sie übermittelt werden und zu welchem Zweck dies geschieht.

Stammt der Web Font-Anbieter aus dem Nicht-EU-Ausland, sind auch die Anforderungen von Art. 44 ff. DSGVO zu erfüllen. Der Webseitenbetreiber muss im Rahmen seiner Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) gegenüber der Datenschutz-Aufsichtsbehörde einen entsprechenden Nachweis führen können.[38] Der Aufwand bei der Erfüllung dieser Pflicht sollte nicht unterschätzt werden.[39]

Bindet eine bayerische öffentliche Stelle externe Web Fonts auf ihrer Webseite ein, ohne dafür eine wirksame Einwilligung und erforderlichenfalls die Einhaltung der Art. 44 ff. DSGVO nachweisen zu können, ist die Übermittlung der IP-Adresse wie auch weiterer personenbezogener Daten von Nutzerinnen und Nutzern nicht rechtmäßig. Nach Auffassung des Landgerichts München I kommt in einem Fall dieser Art ein Anspruch gegen den Webseitenbetreiber auf Unterlassen der Weitergabe der IP-Adresse (§ 823 Abs. 1 in Verbindung mit § 1004 Bürgerliches Gesetzbuch analog) sowie auf Schadensersatz (Art. 82 Abs. 1 DSGVO) in Betracht.

Der Verstoß gegen datenschutzrechtliche Vorgaben – etwa gegen Art. 5 Abs. 1 Buchst. a DSGVO, wenn die für eine Verarbeitung eingeholte Einwilligung nicht wirksam ist – kann nur unter den Voraussetzungen von Art. 4 Nr. 12 DSGVO[40] eine Meldepflicht nach Art. 33 Abs. 1 DSGVO auslösen, jedoch unabhängig vom Entstehen einer solchen Pflicht datenschutzaufsichtliche Maßnahmen nach sich ziehen.

2.3.4 Einfache Alternative: Lokale Einbindung

Eine einfache Lösung, Schriftarten in datenschutzrechtlicher Hinsicht rechtssicher und risikofrei in eine Webseite einzubinden, ist das Selbsthosting. Insbesondere bei Schriftarten US-amerikanischer Anbieter sollte diese Alternative erwogen werden.[41]

38 In Landgericht München, Urteil vom 20. Januar 2022, 3 O 17493/20, BeckRS 2022, 612, kam es auf Art. 44 ff. DSGVO nicht an, weil eine wirksame Einwilligung fehlte und die Datenübermittlung an den Web Font-Anbieter bereits aus diesem Grunde rechtswidrig war.

39 Vgl. in diesem Zusammenhang Bayerischer Landesbeauftragter für den Datenschutz, Office-Anwendungen aus Drittstaaten bei bayerischen öffentlichen Stellen, Aktuelle Kurz-Information 39, Stand 12/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018".

40 Zu den Anforderungen an eine Datensicherheitsverletzung im Einzelnen Bayerischer Landesbeauftragter für den Datenschutz, Meldepflicht und Benachrichtigungspflicht des Verantwortlichen, Stand 6/2019, Rn. 4 ff., Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018".

41 Vgl. auch die entsprechende Empfehlung der österreichischen Datenschutzbehörde, Newsletter 4/2022, Internet: https://www.dsb.gv.at/newsletter/dsb-newsletter-4-2022.html, die zur datenschutzrechtlichen Zulässigkeit von Google Fonts ein Prüfverfahren eingeleitet hat.

Hier wird gerade keine Verbindung der Plattform der Nutzerin oder des Nutzers mit dem Server eines Drittanbieters hergestellt; die IP-Adresse und gegebenenfalls auch andere Daten werden nicht übermittelt und es kommen auch keine Third-Party-Cookies zum Einsatz. Die Einholung einer dafür benötigten Einwilligung ist somit entbehrlich.

Entscheidet sich eine bayerische öffentliche Stelle für die Nutzung von Web Fonts, sollte sie diese daher möglichst selbst hosten. Hierzu muss sie die gewünschte Schriftart unter Beachtung der lizenzrechtlichen Rahmenbedingungen auf dem eigenen Server zur Verfügung stellen und von dort in die Webseite einbinden.

Soweit ein Webseitenbetreiber längere Ladezeiten befürchtet,[42] sollte er auch bedenken, dass die gewünschte Schriftart bei einer externen Einbindung bis zur Erteilung der Einwilligung nicht geladen werden darf und die Webseite bis zu diesem Zeitpunkt ebenfalls nur provisorisch (mit der dem Browser verfügbaren Schriftart) dargestellt werden kann.

2.4 Externe behördliche Datenschutzbeauftragte: Transparenzanforderungen

Öffentliche Stellen nehmen bei der Erfüllung ihrer datenschutzrechtlichen Verpflichtungen zunehmend die Unterstützung durch externe behördliche Datenschutzbeauftragte, welche im Rahmen von Dienstleistungsverträgen beauftragt werden, in Anspruch.[43] Dies kann jedoch zu Schwierigkeiten führen, wenn der Einsatz dieser externen behördlichen Datenschutzbeauftragten für die Bürgerinnen und Bürger nicht hinreichend transparent erfolgt. Im Berichtszeitraum war ich mehrfach mit folgender Problematik befasst:

Von den Datenverarbeitungen einer öffentlichen Stelle betroffene Personen hatten Auskunftsansprüche nach Art. 15 DSGVO geltend gemacht und wurden sodann von den externen Datenschutzbeauftragten der öffentlichen Stelle aufgefordert, ihre Identität nachzuweisen, um einen Zugriff von Unbefugten auf personenbezogene Daten zu vermeiden.[44] Dabei hatten sich die externen behördlichen Datenschutzbeauftragten entweder gar nicht als solche identifiziert bzw. nach Änderung des Kommunikationsweges nicht nochmals als solche identifiziert. Beispielsweise hatte der externe behördliche Datenschutzbeauftragte den betroffenen Bürger zunächst per E-Mail kontaktiert und dabei seine Funktion offengelegt, bei der nächsten Kontaktaufnahme per Briefpost jedoch darauf verzichtet und war insoweit nur unter dem Namen des

42 Längere Ladezeiten sollen primär dadurch vermieden werden, dass der externe Web Font bereits für andere Webseiten geladen wurde, somit im Cache des Browsers der Nutzerin oder des Nutzers verfügbar ist und nicht erneut abgerufen werden muss. Zu beachten ist hier aber, dass aktuelle Browser aus Datenschutzgründen den Cache partitionieren (Cache Partitioning), so dass auch externe Ressourcen erneut geladen werden müssen und damit dieser vermeintliche Vorteil in Verbindung mit anderen technischen Rahmenbedingungen (zum Beispiel http/2) häufig sogar zu längeren Ladezeiten führen kann.

43 Vgl. für nähere Informationen dazu Bayerischer Landesbeauftragter für den Datenschutz, Der behördliche Datenschutzbeauftragte, Stand 5/2018, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen".

44 Vgl. näher zu dieser Thematik Bayerischer Landesbeauftragter für den Datenschutz, Identifizierung bei der Geltendmachung von Betroffenenrechten, Aktuelle Kurz-Information 22, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Aktuelle Kurz-Informationen".

Privatunternehmens, bei dem der angestellt war, aufgetreten. Gegen diese Praxis haben sich betroffene Personen bei mir beschwert.

Aus datenschutzrechtlicher Sicht habe ich diese Praxis wie folgt bewertet:

Zwar ist auch für öffentliche Stellen der Einsatz externer behördlicher Datenschutzbeauftragter gemäß Art. 37 Abs. 6 DSGVO möglich. Werden diese jedoch für öffentliche Stellen tätig, so muss aus ihren Handlungen, insbesondere aus ihren Schreiben und Nachrichten, für die betroffenen Bürgerinnen und Bürger **jederzeit klar und eindeutig erkennbar sein, dass die handelnde Person externer behördlicher Datenschutzbeauftragter der öffentlichen Stelle ist.** Dies gilt nicht nur bei der erstmaligen Kontaktaufnahme, sondern auch für den Fall, dass bei laufender Kommunikation das Medium gewechselt wird. Wird dies nicht beachtet, verstößt die öffentliche Stelle gegen ihre Transparenzpflichten aus Art. 5 Abs. 1 Buchst. a DSGVO und gegen Art. 38 Abs. 4 DSGVO, da hierdurch den Betroffenen ihr Konsultationsrecht beim Datenschutzbeauftragten erschwert wird.

Da in den von mir zu bewertenden Fällen aus der E-Mail-Adresse oder E-Mail-Signatur des externen behördlichen Datenschutzbeauftragten bzw. zumindest aus dem später per Brief versandten Schreiben nicht hervorging, dass dieser in solcher Funktion für die öffentliche Stelle handelte, habe ich jeweils einen Verstoß gegen datenschutzrechtliche Vorschriften festgestellt. Ich habe die betreffenden öffentlichen Stellen aufgefordert, zukünftig auf ein jederzeitiges transparentes Auftreten des externen behördlichen Datenschutzbeauftragten zu achten.

Nach meiner Auffassung können externe behördliche Datenschutzbeauftragte dem Transparenzerfordernis unkompliziert dadurch genügen, dass sie in Schreiben oder E-Mails ihrer Unterschrift einen die Funktion kennzeichnenden Zusatz beifügen. Unterhält die öffentliche Stelle ein Webangebot und ist die oder der behördliche Datenschutzbeauftragte dort in den Datenschutzhinweisen namentlich bezeichnet, kann zusätzlich ein entsprechender Link angeboten werden. Dann haben betroffene Personen die Möglichkeit, Angaben in Schreiben oder E-Mails ohne größeren Aufwand zu verifizieren.

3 Polizei und Verfassungsschutz

3.1 Verfahrensübergreifende Recherche- und Analyseplattform der Bayerischen Polizei (VeRA)

Im Juli 2019 informierte mich das Innenministerium erstmals über das „Projekt zur Einführung einer verfahrensübergreifenden Recherche- und Analyseplattform bei der Bayerischen Polizei (VeRA)". Ziel des Projekts sei es, die begrenzten personellen Ressourcen im Bereich der Bekämpfung der Schwerstkriminalität, organisierten Kriminalität und der Terrorismusbekämpfung effizient und zielgerichtet, unter Nutzung vorhandener technischer Möglichkeiten, einzusetzen. Die Automatisierung von Prozessen solle hierbei insbesondere zu einer Entlastung des eingesetzten Personals, Beschleunigung der Ermittlungen und damit der Gewährleistung der Handlungsfähigkeit der Bayerischen Polizei führen.

Den Informationen konnte ich entnehmen, dass das Projekt im Kern die Schaffung sehr umfangreicher softwarebasierter Recherche- und Analysemöglichkeiten bedeutet, um polizeiliche Dateien, angebundene Datenbanken anderer Behörden, offen im Internet verfügbare Daten und Informationen aus sichergestellten Datenträgern in bisher nicht gekannter Effektivität und Effizienz zu durchsuchen und auszuwerten.

Schon die Mitteilung erster Zielvorstellungen zu „VeRA" ließen nicht nur eine neue Dimension polizeilicher Datenverarbeitung erahnen, sondern zugleich ein völlig neues Eingriffsniveau. Nach meiner ersten Einschätzung kam ich aufgrund zahlreicher offener Fragestellungen und der absehbar hohen Eingriffsintensität nicht umhin, dem Bayerischen Staatsministerium des Innern, für Bau und Verkehr im September 2019 meine erheblichen datenschutzrechtlichen Bedenken mitzuteilen. Während und nach einer ersten Informationsveranstaltung im Landeskriminalamt konkretisierte und verdeutlichte ich diese Bedenken nochmals. Dabei wies ich insbesondere auf eine meines Erachtens fehlende Rechtsgrundlage für den Einsatz einer solch hocheffizienten Recherche- und Analysesoftware hin und empfahl vor Durchführung eines Vergabeverfahrens dringend die Durchführung einer Datenschutz-Folgenabschätzung (DSFA). Ebenso erinnerte ich das Landeskriminalamt an meine kurz davor geäußerte Kritik an der dort bereits eingesetzten Anwendung „iFinder" (siehe auch meinen 28. Tätigkeitsbericht 2018 unter Nr. 4.1.4), die– im Vergleich zum geplanten Vorhaben „VeRA" mit deutlich reduzierteren – Fähigkeiten eine dokumenten- und verzeichnisübergreifende Volltextsuche in polizeilichen Datenbeständen ermöglicht.

Generell konnte ich in den letzten Jahren zunehmend den Eindruck gewinnen, dass die Schwierigkeit der modernen Polizeiarbeit oftmals nicht mehr wie in früheren Jahren darin besteht, an Informationen zu gelangen, sondern die Vielzahl der bereits vorhandenen und verfügbaren Daten ungeachtet ihrer Qualität noch überblicken zu können. Die Verknüpfung und effiziente Analyse von unterschiedlichen Daten in unterschiedlichen Datenquellen in kurzer Zeit ist daher eine der zentralen Herausforderungen für „VeRA".

Nach meiner Wahrnehmung hatte sich das Projekt „VeRA" in der Beurteilung der Ausgangslage in erster Linie mit den fachlichen Bedürfnissen und dem technischen Status quo befasst und dabei die wesentliche Frage ausgespart, warum überhaupt

voneinander getrennte „Datentöpfe“ existieren. Der Grund hierfür ist jedoch ein wesentliches Grundprinzip des Datenschutzes: die sogenannte Zweckbindung. Danach dürfen rechtmäßig erhobene Daten nur für die bei der Erhebung festgelegten, eindeutigen und legitimen Zwecke verwendet und in der Folge gerade nicht voraussetzungslos für jedwede anderweitigen Zwecke weiterverarbeitet werden. Dieser Grundsatz ist auch im Polizeirecht ausdrücklich verankert, zum Beispiel in Art. 53 Abs. 2 PAG:

„[1]Die Speicherung und anderweitige Verarbeitung darf nur zu dem Zweck erfolgen, zu dem diese Daten erhoben worden sind. [2]Die Verarbeitung einschließlich einer erneuten Speicherung und einer Veränderung sowie die Übermittlung zu einem anderen polizeilichen Zweck ist zulässig, soweit die Polizei die Daten zu diesem Zweck erheben dürfte oder dies anderweitig besonders gestattet ist.“

Auch aufgrund der Zweckbindung hat die Polizei daher nicht nur eine, sondern viele verschiedene Datenbanken. So gibt beispielsweise der Kriminalaktennachweis (KAN) Auskunft über alle Personen, bei denen die Polizei strafverfahrensrechtliche Ermittlungen aufgenommen hat. Das sogenannte Vorgangsverwaltungssystem IGVP hingegen betrifft die Verwaltung aller Vorgänge – also auch solcher, die unter Umständen überhaupt keinen Bezug zur Kriminalität haben, sondern beispielsweise nur das polizeiliche Vorgehen dokumentieren sollen (etwa die Feststellung von Zeugen bei einem einfachen Verkehrsunfall). Daneben gibt es eine Fülle an Spezialdatenbanken, die unterschiedlichen Zwecken dienen. Diese Unterscheidung nach dem Zweck hat mehrere Funktionen, insbesondere aber gibt sie der Polizei eine Orientierung, wofür sie die Daten gerade konkret verwenden darf und wofür nicht.

Wenn die Polizei jedoch Verfahren und Methoden einsetzt, um mit deren Hilfe bereits vorhandene, große Datenbestände zu recherchieren und selbständig auf Zusammenhänge zu analysieren, um auf diesem Wege „neues Wissen“ zu generieren, bewegt sie sich nach der Rechtsprechung des Bundesverfassungsgerichts[45] im Bereich des sogenannten Data-Mining.

Das bedeutet, dass die Polizei aus den zur Verfügung stehenden Daten mit praktisch allen informationstechnisch möglichen Methoden weitreichende Erkenntnisse abschöpfen sowie aus der Datenauswertung neue Zusammenhänge erschließen kann. Mit der Verknüpfung von Daten könnten etwa mehrstufige Analysen angestoßen werden, die neue Verdachtsmomente erst erzeugen. Weitere Analyseschritte oder auch daran anschließende operative Maßnahmen wären möglich. Die Nachteile, die Betroffenen auf Grund einer solchen Maßnahme drohten, könnten aus Sicht des Bundesverfassungsgerichts daher erheblich sein und das Gewicht der individuellen Beeinträchtigung bedeutend erhöhen. Hinzu käme, dass von den betreffenden Datenverarbeitungen durch „VeRA“ in erheblichem Maße solche Personen betroffen wären, die in keinem Bezug zur anlassgebenden Situation stünden. Die Streubreite des mit „VeRA“ verbundenen Eingriffs wäre daher enorm und bewegte sich im Bereich der Rasterfahndung.

Auch wenn die oben genannten Feststellungen des Bundesverfassungsgerichts im Zusammenhang mit der informationellen Kooperation zwischen Polizeibehörden und Nachrichtendiensten getroffen wurden, ist ihr Grund- und Schutzgedanke auch auf innerpolizeiliche Data-Mining-Systeme übertragbar. Damit brächte „VeRA“ eine er-

45 Bundesverfassungsgericht, Beschluss vom 10. November 2020, 1 BvR 3214/15, BeckRS 2020, 34607.

heblich höhere Eingriffsintensität gegenüber herkömmlichen Datenabgleichen/-verarbeitungen mit sich. Nach ständiger Rechtsprechung des Bundesverfassungsgerichts müssen Befugnisse mit einem derartig hohen Eingriffsgewicht dem Schutz von besonders gewichtigen Rechtsgütern dienen und auf Grundlage präzise bestimmter und normenklarer Regelungen an hinreichende Eingriffsschwellen gebunden sein.

Das ursprüngliche Ansinnen des Landeskriminalamts und des Innenministeriums, die Recherche- und Analyseplattform „VeRA" ohne Schaffung einer spezifischen Rechtsgrundlage betreiben zu wollen, kritisierte ich daher mehrfach. Zudem wies ich deutlich auf die Notwendigkeit einer Datenschutzfolgenabschätzung hin.

Im März 2022 musste ich schließlich einer Pressemitteilung des Landeskriminalamts entnehmen, dass bezüglich „VeRA" bereits der Zuschlag zugunsten des Unternehmens „Palantir Technologies GmbH" erfolgte.

Ich nahm dies zum Anlass, den Sachverhalt und die damit verbundenen datenschutzrechtlichen Problemstellungen nochmals zusammenfassend aus meiner Perspektive dem Innenministerium zu erläutern.

In der Folge zeigten sich Landeskriminalamt und Innenministerium offener für die Schaffung einer Befugnis zum Betrieb von „VeRA" und die Durchführung einer tragfähigen DSFA. Schließlich wurde ich über die beabsichtigte Schaffung einer neuen, spezifischen Rechtsgrundlage für den Einsatz von „VeRA" innerhalb des Polizeiaufgabengesetzes informiert. In diesem Zusammenhang wies ich unter anderem auf folgende Punkte hin:

- In Hamburg und Hessen, wo für den vergleichbaren Einsatz der Palantir-Software bereits Rechtsgrundlagen geschaffen wurden, stehen diese zur Überprüfung durch das Bundesverfassungsgericht an. Aus Gründen der Rechtssicherheit wäre es empfehlenswert, die Entscheidungen zu diesen beiden Verfassungsbeschwerden abzuwarten.

- Die mit VeRA verbundenen Datenverarbeitungen weisen – insbesondere im Vergleich zu einer händischen Auswertung – ein enormes Eingriffsgewicht mit immenser Streubreite auf und erlangen auch im Rahmen einer Überwachungsgesamtrechnung[46] Bedeutung.

- Die Anwendung von VeRA ist grundsätzlich auf solche Daten zu beschränken, die die Polizeibehörden unter besonderen Voraussetzungen für Zwecke der vorbeugenden Gefahrenabwehr speichern. Eine Einbeziehung von Daten aus der polizeilichen Vorgangsverwaltung IGVP, die einen enormen Umfang hat und größtenteils Daten von unbescholtenen Bürgern enthält, lehne ich ab.

- Das Eingriffsgewicht bei der Nutzung von VeRA ist mit dem einer Rasterfahndung zumindest vergleichbar. In diesem Fall wird den verfassungsrechtlichen Anforderungen nur genügt, wenn die Ermächtigung eine konkrete Gefahr für hochrangige Rechtsgüter vorsieht. Eine „drohende Gefahr" reicht dafür nicht aus.

[46] Dazu im Überblick Schwabenbauer, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Kap. G Rn. 348 f.

Die Sicherheitslage scheint sich nahezu jährlich zu verbessern. So wurde für die Polizeiliche Kriminalstatistik (PKS) im Jahr 2021 in Bayern die niedrigste Kriminalitätsbelastung seit 44 Jahren und gleichzeitig die höchste Aufklärungsquote seit 27 Jahren vermeldet. Darüber hinaus nimmt das Projekt „Polizei 20/20", das die Sicherheitsarchitektur der Polizeien des Bundes und der Länder in den kommenden Jahren gravierend verändern und weitest möglich vernetzen soll, zunehmend Fahrt auf (siehe auch meinen 30. Tätigkeitsbericht 2020 unter Nr. 5.1).

All dies führt schlussendlich zu der Fragestellung, ob angesichts dieser Sachlage noch ein derart eingriffsintensives Instrument wie „VeRA" zusätzlich erforderlich ist und wenn ja, wie der Einsatz verhältnismäßig ausgestaltet werden kann.

Am 16. Februar 2023 hat das Bundesverfassungsgericht ein Urteil zu den oben erwähnten Regelungen in Hessen und Hamburg erlassen.[47] Es bleibt nun abzuwarten, wie der bayerische Gesetzgeber bei der beabsichtigten Schaffung einer Rechtsgrundlage die dort aufgestellten verfassungsrechtlichen Rahmenbedingungen umsetzen wird.

3.2 Dauer der Bearbeitung von Auskunftsersuchen

Nach Art. 65 Polizeiaufgabengesetz (PAG) hat die Polizei einer Person auf Antrag unter anderem mitzuteilen, ob und welche personenbezogenen Daten sie über die antragstellende Person verarbeitet.

Art. 65 PAG
Auskunftsrecht
(1) [1]Die Polizei teilt einer Person auf Antrag mit, ob sie betreffende personenbezogene Daten, einschließlich Bild- und Tonaufnahmen, verarbeitet werden. [2]Ist dies der Fall, erhält die Person ihrem Antrag entsprechend Auskunft über sie betreffende personenbezogene Daten und über

1. *die Rechtsgrundlage und die Zwecke der Verarbeitung,*
2. *verfügbare Informationen zur Herkunft der Daten oder, falls dies im Einzelfall nicht möglich ist, zu den Kategorien personenbezogener Daten, die verarbeitet werden,*
3. *die Empfänger, gegenüber denen die personenbezogenen Daten offengelegt wurden,*
4. *die für deren Speicherung vorgesehene Dauer oder, falls dies im Einzelfall nicht möglich ist, die Kriterien für deren Festlegung,*
5. *die bestehenden Rechte auf Berichtigung, Löschung oder Verarbeitungseinschränkung und*
6. *die Kontaktdaten des Landesbeauftragten und die Möglichkeit, bei ihm Beschwerde einzulegen.*

[3]Bestehen begründete Zweifel an der Identität der antragstellenden Person, kann die Erteilung der Auskunft von der Erbringung geeigneter Nachweise abhängig gemacht werden. [4]Auskunft zur Herkunft personenbezogener Daten von oder zu deren Übermittlung an Verfassungsschutzbehörden des Bundes oder der Länder, den Bundesnachrichtendienst oder den Militärischen Abschirmdienst, wird nur mit Zustimmung dieser Stellen erteilt.
(2) [1]Die Auskunft kann unterbleiben, soweit und solange andernfalls

[47] Bundesverfassungsgericht, Urteil vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, BeckRS 2023, 1828.

1. die Erfüllung polizeilicher Aufgaben gefährdet oder wesentlich erschwert würde,
2. die öffentliche Sicherheit oder Ordnung gefährdet würde oder
3. die im Einzelfall, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, erforderliche Geheimhaltung verarbeiteter Daten gefährdet würde und das Interesse der antragstellenden Person an der Auskunftserteilung nicht überwiegt.

[2]Art. 50 bleibt unberührt.

(3) [1]Art. 62 Abs. 5 gilt entsprechend. [2]Die Gründe für die Ablehnung eines Antrags sind von der Polizei zu dokumentieren. [3]Sie sind dem Landesbeauftragten für dessen Kontrolle in auswertbarer Weise zur Verfügung zu stellen, soweit nicht das Staatsministerium des Innern, für Sport und Integration im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. [4]Eine Mitteilung des Landesbeauftragten an den Betroffenen im Beschwerdeverfahren darf keine Rückschlüsse auf den Erkenntnisstand der Polizei zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(4) Art. 62 Abs. 6 gilt entsprechend.

Dieses Auskunftsrecht ist aus datenschutzrechtlicher Sicht von sehr großer Bedeutung, da betroffene Personen häufig erst durch die Kenntnis, was über sie gespeichert ist, in die Lage versetzt werden, weitere Rechte, wie etwa das Recht auf Löschung, auszuüben. Auskunftsersuchen nach Art. 65 PAG sind für mich daher ein datenschutzrechtliches Dauerthema im Austausch mit der Bayerischen Polizei. Dementsprechend häufig sind sie auch in meinen Tätigkeitsberichten präsent (siehe zuletzt meinen 28. Tätigkeitsbericht 2018 unter Nr. 4.6).

Aufgrund von Beschwerden rückte in der Vergangenheit neben der Frage des Umfangs der Auskunft immer wieder der Aspekt in den Mittelpunkt, welche Zeit die Polizei für die Bearbeitung derartiger Anträge in Anspruch nehmen darf.

Schon im Berichtszeitraum 2015/2016 (siehe meinen 27. Tätigkeitsbericht 2016 unter Nr. 3.10.2) hatte ich dem Bayerischen Landeskriminalamt mitgeteilt, dass die Bearbeitung sowohl von Auskunfts- als auch von Löschungsanträgen in der Regel nicht länger als drei Monate dauern darf. Maßgeblich hierfür ist zum einen die allgemeine Entscheidung des Gesetzgebers, nach drei Monaten grundsätzlich den Weg für eine Untätigkeitsklage zu öffnen (siehe § 75 Verwaltungsgerichtsordnung). Zum anderen sieht die Datenschutz-Richtlinie für Polizei und Strafjustiz im Speziellen vor, dass derartige Anträge grundsätzlich unverzüglich zu beantworten sind (siehe Erwägungsgrund 40 RLDSJ).

In der Folge erreichten mich dennoch immer wieder begründete Eingaben zur Bearbeitungsdauer bei Auskunftsersuchen. So wandten sich wiederholt betroffene Personen an mich, die mehr als vier Monate nach Stellung eines Auskunftsantrags lediglich eine Eingangsbestätigung, aber keine endgültige Antwort oder Zwischennachricht erhalten hatten. Vor diesem Hintergrund bat ich das Landeskriminalamt, mir zu bestimmten Zeitpunkten über die Zahl der drei Monate nach Antragsstellung noch unerledigten Auskunftsersuchen zu berichten.

Auf meine erste diesbezügliche Anfrage hin teilte mir das mir das Landeskriminalamt mit, dass einige Anträge noch nicht abgeschlossen seien. Ich habe dies gegenüber dem Landeskriminalamt kritisiert und sinngemäß darauf hingewiesen, dass die Polizei bei der Bearbeitung von Auskunftsanträgen einer gesetzlichen Verpflichtung nachzukommen habe, die nicht ohne Weiteres zugunsten anderer Schwerpunkte zurückge-

stellt werden könne. Auch habe ich gegenüber dem Landeskriminalamt deutlich gemacht, dass der in den letzten Jahren zu verzeichnende kontinuierliche Anstieg bei den an die Polizei gerichteten Auskunftsanträgen mit Blick auf das stetig wachsende gesellschaftliche Interesse und Bewusstsein für die Thematik Datenschutz durchaus vorhersehbar gewesen sei.

In der Folge konnte mir das Landeskriminalamt erfreulicherweise berichten, dass man entsprechende Maßnahmen ergriffen habe und die Fälle mit einer überlangen Bearbeitungsdauer (also länger als drei Monate) „auf null" habe reduzieren können. Gleichwohl werde ich beim Landeskriminalamt weiterhin regelmäßig entsprechende Berichte einholen, um den weiteren Verlauf dieser – zuletzt wieder positiven – Entwicklung zu verfolgen.

3.3 Unsachgemäßer E-Mail-Versand durch die Polizei im Rahmen eines Ermittlungsverfahrens

Die E-Mail ist zum Standard-Kommunikationsmittel unserer Zeit geworden. Jeder bzw. jede schätzt die damit verbundenen Vorzüge eines direkten und schnellen Informationsaustauschs. Allzu häufig wird dabei jedoch vergessen, dass der Inhalt einer E-Mail grundsätzlich nicht gesichert ist. Nur durch eine Verschlüsselung der Daten lassen sich wichtige Sicherheitsstandards gewährleisten (siehe hierzu etwa meinen 26. Tätigkeitsbericht 2014 unter Nr. 3.6.6).

Dass aber nicht nur dies beim Umgang mit E-Mails datenschutzrechtlich problematisch sein kann, zeigt folgendes Beispiel:

Im Wege einer Eingabe beschwerte sich ein Bürger über folgenden Sachverhalt: Im Rahmen eines Online-Betrugsverfahrens kontaktierte eine Polizeiinspektion alle Geschädigten mittels E-Mail. Diese Nachricht, welche auch Fragen zum betreffenden Warenkauf enthielt, wurde an den Petenten und gleichzeitig an etwa 20 weitere Geschädigte gesandt. Da die E-Mail-Adressen im für alle Empfängerinnen und Empfänger einsehbaren Adressfeld und nicht unter „BCC" aufgeführt wurden, erhielten alle angeschriebenen Geschädigten Kenntnis von den E-Mail-Adressen der übrigen, ihnen unbekannten Geschädigten.

Ich habe das zuständige Polizeipräsidium darauf hingewiesen, dass der Schutz personenbezogener Daten auch im E-Mail-Verkehr Berücksichtigung finden muss. Das betrifft neben den Informationen in Form von Texten und Anhängen auch die Adressen der Empfängerinnen und Empfänger. Insbesondere ist darauf zu achten, dass bei Nachrichten an mehrere Personen das „BCC"-Feld genutzt wird, um die Offenlegung der einzelnen E-Mail-Adressen an alle Empfängerinnen und Empfänger zu verhindern.

Nach Prüfung des Sachverhaltes räumte das Polizeipräsidium ein, dass die gewählte Vorgehensweise zweifelsfrei nicht die richtige gewesen und dem Schutz der personenbezogenen Daten der Geschädigten nur unzureichend Rechnung getragen worden sei. Es habe sich um einen Fehler im Einzelfall und keineswegs um eine gängige Ermittlungsmethode der betreffenden Polizeiinspektion gehandelt.

Um künftig derartige Fälle zu vermeiden, sei eine Sensibilisierung aller Beschäftigten der Polizeiinspektion erfolgt. Der Rückmeldung des Polizeipräsidiums war zu entnehmen, dass die Einhaltung datenschutzrechtlicher Aspekte auch im Zusammenhang mit dem E-Mail-Verkehr weiterhin im Fokus behalten werde.

Im Ergebnis diente die Beschwerde somit dazu, auf einen datenschutzrechtlich korrekten Umgang mit dem Kommunikationsmittel E-Mail im Rahmen polizeilicher Ermittlungstätigkeit aufmerksam zu machen.

3.4 Unzulässiges Abfotografieren eines Ausweises mittels eine privaten Smartphones

Im Berichtszeitraum monierte eine Beschwerde die Vorgehensweise der Polizei im Zusammenhang mit einer Identitätsfeststellung. Eine lautstarke Auseinandersetzung hatte einen Polizeieinsatz zur Folge gehabt. Im Verlauf des Einsatzes stellte die Polizei die Identität der anwesenden Personen fest. Hierzu ließen sich die Beamten auch einen Ausweis der Petentin aushändigen. Ein Polizeibeamter fotografierte den Ausweis mit seinem privaten Smartphone, um in der Situation vor Ort handlungsbereit zu bleiben und später am Schreibtisch eine sorgfältige Sachbearbeitung zu ermöglichen.

Durch die Verwendung des privaten Smartphones war allerdings die Sicherheit der Verarbeitung personenbezogener Daten auf dem Ausweis nicht gewährleistet; gleichzeitig wurde gegen eine entsprechende polizeiinterne Richtlinie verstoßen, die eine Nutzung privater EDV-Anlagen zu dienstlichen Zwecken untersagt (Art. 66 Polizeiaufgabengesetz in Verbindung mit Art. 28 Abs. 1, Abs. 2 Satz 2, Art. 32 BayDSG und Art. 32 Abs. 1 DSGVO).

Das betroffene Polizeipräsidium räumte ein, dass das Vorgehen des Polizeibeamten fehlerbehaftet war. Auch teilte es mir auf mein entsprechendes Schreiben mit, dass das Foto nach der Sachbearbeitung umgehend sowohl vom privaten Smartphone als auch aus dem dazugehörigen Cloud-Speicher gelöscht worden sei. Weiterhin werde die Problematik im Rahmen einer Dienstbesprechung mit den nachgeordneten Dienststellen erörtert. Vor diesem Hintergrund habe ich von weiteren Maßnahmen abgesehen.

3.5 Parlamentarische Untersuchungsausschüsse und Löschmoratorien

Im Zusammenhang mit der Tätigkeit parlamentarischer Untersuchungsausschüsse habe ich die Zunahme von Löschmoratorien bereits in meinem 27. Tätigkeitsbericht 2016 kritisch gewürdigt. Dabei habe ich auf zahlreiche Aspekte einer möglichst datenschutzfreundlichen Verfahrensweise hingewiesen. Dies betraf insbesondere die strikte Zweckbindung von über die eigentliche Speicherdauer hinausgehend aufbewahrten Daten, die ausschließlich dem Zweck des Untersuchungsausschusses dienen dürfen, sowie eine Einschränkung des zugriffsberechtigten Personenkreises. Gleichzeitig hatte ich meine datenschutzrechtlichen Bedenken gegenüber den umfassenden Speicherungs- und Aufbewahrungsverlängerungen gerade auch im Hinblick auf die verfassungsrechtlich gebotene Aufklärungsarbeit von Untersuchungsausschüssen vorerst zurückgestellt.

Vor diesem Hintergrund bin ich im Juni 2021 gerne der Aufforderung aus den Beschlüssen des Bayerischen Landtags (Landtags-Drucksache 18/14524 und 18/14525) nachgekommen, zur Frage der Fortführung oder Aufhebung des bestehenden Löschmoratoriums „NSU“ Stellung zu nehmen. Im Kern betraf dies Überlegungen zum weiteren Umgang mit dem im Rahmen von NSU-Untersuchungsausschüssen verhängten Löschmoratorium für Akten und Daten des Bayerischen Landesamts für Verfassungsschutz und der Bayerischen Polizei.

Aus meiner Sicht waren hierbei zwei unterschiedliche Kategorien von Daten und Akten zu beurteilen:

Die **erste Kategorie** bildeten solche Daten und Akten, die in einem **erkennbaren Kontext** mit dem Untersuchungsauftrag „NSU“ standen und daher auch den jeweiligen Untersuchungsausschüssen vorgelegt wurden. Auch wegen der herausragenden Bedeutung dieser Untersuchungsausschüsse, der daraus gewonnenen Erkenntnisse und ihrer nachwirkenden gesamtgesellschaftlichen Aufgabenstellung hatte ich aus datenschutzrechtlicher Sicht keine Bedenken, wenn diese Daten und Akten nicht gelöscht und vernichtet, sondern – wie vom Bayerischen Staatsministerium des Innern, für Sport und Integration vorgeschlagen – den zuständigen staatlichen Archiven angeboten werden.

Ein anderes Bild zeichnete sich jedoch bezüglich der **zweiten Kategorie**, also jenen Daten und Akten, die ebenfalls über die gesetzlich vorgesehenen Speicherfristen hinaus bevorratet wurden, jedoch in **keinem erkennbaren Bezug** zu dem Untersuchungsgegenstand „NSU“ standen. Nach Abschluss der Untersuchungsausschüsse des Bayerischen Landtags sowie des Bundestags existierte keine Rechtsgrundlage für eine weitere Aufbewahrung bzw. Speicherung. Im Ergebnis habe ich mich für eine zeitnahe Aufhebung des verfügten Löschmoratoriums betreffend die Daten und Akten der „zweiten Kategorie“ ausgesprochen.

Die endgültige Entscheidung über den weiteren Umgang mit dem im Rahmen von NSU-Untersuchungsausschüssen verhängten Löschmoratorium wurde letztlich zurückgestellt, als sich der Bayerische Landtag am 19. Mai 2022 für die Einsetzung eines Zweiten Untersuchungsausschusses des Landtags zur weiteren Aufklärung des NSU-Komplexes (Landtags-Drucksache 18/22844) entschied. Da der Untersuchungsgegenstand und der daraus resultierende Beweisbeschluss erneut Fragestellungen betraf, die auch im Kontext mit den bereits früher gesicherten Daten des ersten Untersuchungsausschusses standen, wurden bis auf Weiteres keine der betreffenden Daten und Akten der Löschung zugeführt.

Abschließend möchte ich zur komplexen Thematik „Untersuchungsausschüsse – Beweisbeschlüsse – Löschmoratorien“ noch auf folgende Entschließung der 103. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 23. März 2022 hinweisen:

Parlamentarische Untersuchungsausschüsse und Löschmoratorien:
Datenschutz durch klare Vorgaben und
Verarbeitungsbeschränkungen für Behörden

In den vergangenen Jahren gab es zahlreiche Parlamentarische Untersuchungsausschüsse im Bundestag und in den Landtagen, die das Handeln von Polizei- und Sicherheitsbehörden untersucht haben. Prominente Beispiele sind die Untersuchungsausschüsse zur „Terrorgruppe nationalsozialistischer Untergrund“ (sog. NSU).

Die Untersuchungsausschüsse möchten eine für die Aufklärung notwendige Datengrundlage sicherstellen. Deshalb fordern sie die Behörden regelmäßig auf, sämtliche personenbezogenen Daten weiterhin zu speichern, die in irgendeinem Bezug zum Untersuchungsgegenstand stehen können (etwa zum Thema „Rechtsextremismus“). Diese Daten sind dann für die Arbeit des Untersuchungsausschusses vorzuhalten. Dies soll auch solche Daten umfassen, die nach den gesetzlichen Regeln eigentlich zu löschen wären (so genanntes Löschmoratorium).

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hält das Interesse der Parlamentarischen Untersuchungsausschüsse an dem Erhalt personenbezogener Daten für nachvollziehbar und gewichtig, um den Untersuchungsauftrag umzusetzen. Es ist ihr insbesondere bewusst, dass dem parlamentarischen Informationsinteresse ein besonders hohes Gewicht zukommt, soweit es um die Aufdeckung möglicher Rechtsverstöße und vergleichbarer Missstände geht. Gleichzeitig gilt es allerdings zu berücksichtigen, dass dadurch erheblich in Grundrechte der betroffenen Personen eingegriffen wird, insbesondere dann, wenn diese Personen tatsächlich in keinerlei Bezug zum Untersuchungsgegenstand stehen bzw. gesetzliche Löschungsverpflichtungen suspendiert werden.

Um parlamentarischen Kontrollrechten und Grundrechten betroffener Personen gleichermaßen Geltung zu verschaffen, weist die Konferenz auf folgende Punkte hin:

- *Ohne die förmliche Einsetzung eines Untersuchungsausschusses und Anforderungen von Beweisunterlagen gibt es keine Rechtsgrundlage dafür, die gesetzlich vorgeschriebene Löschung personenbezogener Daten zu suspendieren.*

  Hierzu gehört, dass der Untersuchungsgegenstand klar definiert ist und die Beweisbeschlüsse hinreichend bestimmt formuliert sind (BVerfG, Beschluss vom 17.6.2009 – 2 BvE 3/07). Zudem müssen die Ausnahmen zeitlich auf die Arbeit des Untersuchungsausschusses begrenzt sein. Nur auf diese Weise können unnötige Datenspeicherungen und die damit verbundenen Risiken für die Rechte der betroffenen Personen vermieden werden.

- *„Löschreife" Daten, die die Behörden für Zwecke eines Untersuchungsausschusses zur Verfügung halten, dürfen sie im weiteren Verwaltungsvollzug nicht nutzen. Die DSK hält es daher für erforderlich, diese Daten in Anlehnung an § 58 Abs. 3 BDSG in ihrer Verarbeitung zu beschränken. Hierfür sollte der jeweilige Gesetzgeber Voraussetzungen und Grenzen präzise beschreiben. Einige Landesgesetzgeber haben dies bereits umgesetzt.*

Die DSK appelliert deshalb an die Gesetzgeber des Bundes und der Länder, den Sicherheitsbehörden klare gesetzliche Vorgaben zum Umgang mit zu löschenden Daten zu machen. Diese müssen den Untersuchungsausschüssen den Zugriff auf die Daten sichern. Gleichzeitig ist sicherzustellen, dass die Daten dem Verwaltungsvollzug der Behörden entzogen sind. So werden das Untersuchungsinteresse der Parlamentarischen Untersuchungsausschüsse und die Grundrechte der betroffenen Personen gewahrt.

3.6 Datenschutzrechtliche Prüfung beim Bayerischen Landesamt für Verfassungsschutz

Nicht nur bei der Polizei wird eine Vielzahl personenbezogener Daten verarbeitet, auch beim Bayerischen Landesamt für Verfassungsschutz ist dies der Fall. Die Behörde ist ein wichtiges Frühwarnsystem für Bestrebungen, die gegen die freiheitliche demokratische Grundordnung gerichtet sind.

Rechtsgrundlagen für Datenverarbeitungen des Landesamtes für Verfassungsschutz finden sich insbesondere in Art. 5 Abs. 1 BayVSG.

Art. 5 BayVSG
Allgemeine Befugnisse
(1) [1]Soweit nicht besondere Bestimmungen gelten, darf das Landesamt Informationen einschließlich personenbezogener Daten auch ohne Kenntnis der Betroffenen verarbeiten, soweit dies erforderlich ist

1. *zur Erfüllung seiner Aufgaben nach Art. 3,*
2. *zur Erforschung und Bewertung von Bestrebungen und Tätigkeiten sowie der hierfür erforderlichen Nachrichtenzugänge oder*
3. *zum Schutz seiner Mitarbeiter, Einrichtungen, Gegenstände und Nachrichtenzugänge gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten.*

[2]Voraussetzung für die Sammlung und Auswertung von Informationen ist, dass tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten nach Art. 3 vorliegen. [3]Informationen, die nach Satz 1 gespeicherte Angaben belegen, dürfen auch gespeichert werden, wenn darin weitere personenbezogene Daten Dritter enthalten sind; die Abfrage dieser Daten ist insoweit unzulässig. [4]Das Landesamt darf personenbezogene Daten auch für die Vorgangsverwaltung verarbeiten.
[…]

Da Speicherungen für die Betroffenen weitreichende Konsequenzen haben können, führe ich beim Landesamt für Verfassungsschutz regelmäßig datenschutzrechtliche Kontrollen durch.

Im Berichtszeitraum fand eine Vor-Ort-Prüfung statt, bei der speziell die Speicherung personenbezogener Daten von Personen, die das 14. Lebensjahr noch nicht vollendet hatten, im Fokus meiner Aufmerksamkeit stand. Grundsätzlich möglich sind solche Speicherungen, nachdem die bis 31. Juli 2016 geltende Altersgrenze von 14 Jahren (Art. 7 Abs. 2 Satz 1 BayVSG-alt) für die Speicherung von Daten Minderjähriger vom Gesetzgeber aufgehoben wurde.

Im Zuge meiner Prüfung konnte ich feststellen, dass das Landesamt für Verfassungsschutz maß- und verantwortungsvoll mit dieser gesetzlich eingeräumten Befugnis zur Speicherung personenbezogener Daten von Kindern umgeht.

Bereits wenige Tage vor meinem Besuch wurde ich darüber informiert, dass man im Zuge der fachlichen Vorbereitung des Termins selbständig auf einen Fall gestoßen sei, der nach aktueller Erkenntnislage keiner fortdauernden Speicherung mehr bedürfe.

Im Rahmen der Vor-Ort-Prüfung wurde unter anderem dieser Fall eingehend erörtert. Wenngleich die Speicherung personenbezogener Daten dieser Person datenschutzrechtlich ursprünglich vertretbar war, hatten sich seitdem keine weiteren Erkenntnisse ergeben, die für eine längerfristige Aufbewahrung des Datensatzes gesprochen hätten. Insofern sprach sich das Landesamt für Verfassungsschutz selbst für eine zeitnahe Löschung aus, was ich aus datenschutzrechtlicher Sicht nur begrüßen konnte. Zwei Tage nach meiner Prüfung erhielt ich bereits die schriftliche Bestätigung über den Vollzug der Löschung.

Trotz des durchweg positiven Prüfungsergebnisses habe ich die Behördenleitung des Landesamtes für Verfassungsschutz ersucht, mich aufgrund der besonderen Sensibilität derartiger Speicherungen von Kindern über die weiteren Entwicklungen auf dem Laufenden zu halten.

4 Justiz

4.1 Fehlerhafte Einholung von Bankauskünften im strafrechtlichen Ermittlungsverfahren

Für die Verfolgung von Straftaten im Bereich der Wirtschaftskriminalität ist die Einholung von Kontoauskünften bei Banken oftmals von entscheidender Bedeutung. Anhand von Kontoauszügen können die Ermittlungsbehörden verdächtige Buchungen näher analysieren. Die hierfür erforderliche Rechtsgrundlage findet sich in der sogenannten Ermittlungsgeneralklausel des § 161 Strafprozeßordnung (StPO).

§ 161 StPO
Allgemeine Ermittlungsbefugnis der Staatsanwaltschaft
(1) [1]Zu dem in § 160 Abs. 1 bis 3 bezeichneten Zweck ist die Staatsanwaltschaft befugt, von allen Behörden Auskunft zu verlangen und Ermittlungen jeder Art entweder selbst vorzunehmen oder durch die Behörden und Beamten des Polizeidienstes vornehmen zu lassen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln. [2]Die Behörden und Beamten des Polizeidienstes sind verpflichtet, dem Ersuchen oder Auftrag der Staatsanwaltschaft zu genügen, und in diesem Falle befugt, von allen Behörden Auskunft zu verlangen.
(2) Soweit in diesem Gesetz die Löschung personenbezogener Daten ausdrücklich angeordnet wird, ist § 58 Absatz 3 des Bundesdatenschutzgesetzes nicht anzuwenden.
(3) [1]Ist eine Maßnahme nach diesem Gesetz nur bei Verdacht bestimmter Straftaten zulässig, so dürfen die auf Grund einer entsprechenden Maßnahme nach anderen Gesetzen erlangten personenbezogenen Daten ohne Einwilligung der von der Maßnahme betroffenen Personen zu Beweiszwecken im Strafverfahren nur zur Aufklärung solcher Straftaten verwendet werden, zu deren Aufklärung eine solche Maßnahme nach diesem Gesetz hätte angeordnet werden dürfen. [2]§ 100e Absatz 6 Nummer 3 bleibt unberührt.
(4) In oder aus einer Wohnung erlangte personenbezogene Daten aus einem Einsatz technischer Mittel zur Eigensicherung im Zuge nicht offener Ermittlungen auf polizeirechtlicher Grundlage dürfen unter Beachtung des Grundsatzes der Verhältnismäßigkeit zu Beweiszwecken nur verwendet werden (Artikel 13 Abs. 5 des Grundgesetzes), wenn das Amtsgericht (§ 162 Abs. 1), in dessen Bezirk die anordnende Stelle ihren Sitz hat, die Rechtmäßigkeit der Maßnahme festgestellt hat; bei Gefahr im Verzug ist die richterliche Entscheidung unverzüglich nachzuholen.

Welche Konten bei welchen Banken für Abfragen in Betracht kommen, erfährt die Staatsanwaltschaft wiederum über entsprechende Anfragen bei der Bundesanstalt für Finanzdienstleistungsaufsicht. In diesem Zusammenhang kam eine Staatsanwaltschaft ihrer Meldepflicht gemäß § 500 StPO in Verbindung mit § 65 Bundesdatenschutzgesetz (BDSG) nach und schilderte mir folgenden Vorfall:

Im Rahmen eines strafrechtlichen Ermittlungsverfahrens forderte die Ermittlungsbehörde insgesamt sechs Bankauskünfte an. Hierfür nannte die Staatsanwaltschaft gegenüber den Banken jeweils sowohl den Namen als auch das Geburtsdatum des Beschuldigten. Die aufgrund dieser Angaben gegebenen Auskünfte betrafen jedoch eine dritte Person mit identischen Daten und teilweise deren Ehepartner. Demnach wurde den kontoführenden Bankinstituten ein unzutreffender Tatverdacht gegen

diese dritte Person bekanntgegeben, zugleich nahm der staatsanwaltschaftliche Sachbearbeiter unberechtigterweise Einsicht in Kontounterlagen.

Erfreulicherweise setzte die Staatsanwaltschaft nach Bekanntwerden des Vorfalls von sich aus unverzüglich die bei einem solchen Vorfall datenschutzrechtlich erforderlichen Maßnahmen um. So wurde die Vernichtung der Kontoauszüge veranlasst und gegenüber den Bankinstituten klargestellt, dass gegen die dritte Person kein Ermittlungsverfahren anhängig war. Des Weiteren wurden die dritte Person sowie ihr Ehepartner gemäß § 500 StPO in Verbindung mit § 66 BDSG über den Vorfall benachrichtigt. Zur Vermeidung künftiger Datenschutzverstöße in diesem Bereich hat die betroffene Behörde die Mitarbeitenden entsprechend sensibilisiert.

4.2 Unzulässige Datenübermittlung durch eine Staatsanwaltschaft an ein Jugendamt

Die Anordnung über Mitteilungen in Strafsachen (MiStra) regelt, in welchen Fällen Gerichte und Staatsanwaltschaften verpflichtet sind, personenbezogene Daten von Amts wegen an öffentliche Stellen zu übermitteln. Dass auch bei der Anwendung dieser Verwaltungsvorschrift, die gesetzliche Übermittlungsvorschriften konkretisiert, sorgfältig gearbeitet werden muss, zeigte im Berichtszeitraum der folgende Einzelfall:

Die Polizei nahm einen Verkehrsunfall auf, bei dem ein siebenjähriges Kind als Unfallverursacher festgestellt worden war. Im weiteren Verlauf erhielten die Eltern einen Bescheid der Staatsanwaltschaft, aus dem hervorging, dass von der Einleitung eines Ermittlungsverfahrens gegen das Kind abgesehen worden war und das zuständige Jugendamt eine Mitteilung über diese Entscheidung erhalten hatte. Daraufhin wandte sich der Vater an mich, um die Übermittlung der personenbezogenen Daten seines Sohnes von der Staatsanwaltschaft an das Jugendamt überprüfen zu lassen.

Nach Anforderung einer Stellungnahme bei der zuständigen Staatsanwaltschaft stellte sich heraus, dass mit der Einstellung des Verfahrens auch eine sog. „MiStra 32“, also eine Mitteilung an die Jugendgerichtshilfe in Strafsachen gegen Jugendliche und Heranwachsende nach Nr. 32 MiStra über den Verfahrensausgang veranlasst worden war. Der Staatsanwaltschaft zufolge gebe es solche Mitteilungen „grundsätzlich in allen Verfahren gegen straffällige Jugendliche“. Nachdem das unfallverursachende Kind zum Tatzeitpunkt jedoch noch nicht schuldfähig war, hätte die Mitteilung nicht angeordnet werden dürfen. Daher wurde durch die Staatsanwaltschaft die sofortige Löschung aller übermittelten Daten veranlasst.

Aufgrund der Eingabe des Vaters konnten nicht nur die Datenschutzrechte seines Sohnes gewahrt werden. Aufgrund meines Tätigwerdens überarbeitete die Staatsanwaltschaft zudem eigenverantwortlich die Handhabungsgrundsätze zur MiStra und sensibilisierte alle Mitarbeiterinnen und Mitarbeiter. Im Ergebnis leistete die Eingabe also einen wesentlichen Beitrag zur datenschutzkonformen Anwendung der MiStra.

4.3 Unzulässige Datenübermittlungen durch Staatsanwaltschaften an Ausländerbehörden

Nr. 42 Anordnung über Mitteilungen in Strafsachen (MiStra) sieht in Strafsachen gegen Ausländerinnen und Ausländer eine Information der örtlich zuständigen Auslän-

derbehörde vor. Im Berichtszeitraum habe ich in diesem Zusammenhang einige unzulässige Übermittlungen personenbezogener Daten durch Staatsanwaltschaften feststellen müssen.

Von entsprechenden Fällen erlangte ich unter anderem durch Beschwerden Kenntnis. So trugen zwei deutsche Staatsangehörige vor, die Staatsanwaltschaft habe aus sie betreffenden Strafsachen Mitteilungen nach Nr. 42 MiStra an die örtlich zuständige Ausländerbehörde gemacht. In einem weiteren Fall leitete eine Ausländerbehörde insgesamt 22 fälschlicherweise an sie übersandte Mitteilungen aus einem gesamten Jahr an die zuständige Staatsanwaltschaft zurück. Darüber setzte mich als Datenschutz-Aufsichtsbehörde die betreffende Staatsanwaltschaft im Rahmen einer Meldung von Verletzungen des Schutzes personenbezogener Daten in Kenntnis.

In allen Fällen waren die Datenübermittlungen unzulässig, da Nr. 42 MiStra nach ihrem eindeutigen Wortlaut auf Ausländerinnen und Ausländer gemäß § 2 Abs. 1 Aufenthaltsgesetz beschränkt ist. Meine datenschutzrechtliche Prüfung ergab, dass die zuständigen Beschäftigten der Staatsanwaltschaft in allen Einzelfällen irrtümlicherweise die Ausländereigenschaft angenommen hatten, ohne dies anhand der Akte nochmals zu überprüfen. Infolgedessen hatten sie jeweils fälschlicherweise eine Mitteilung an die jeweils zuständige Ausländerbehörde veranlasst.

Zur Aufarbeitung der zuvor genannten Datenschutzverstöße und zu präventiven Zwecken sensibilisierten die zuständigen Staatsanwaltschaften alle mit Mitteilungen nach Nr. 42 MiStra befassten Beschäftigten. Zum Teil wurde die Thematik auch im Rahmen der Abteilungsleiterbesprechung erörtert.

Um fehlerhafte Mitteilungen in Strafsachen an Ausländerbehörden künftig zu vermeiden, habe ich beim Bayerischen Staatsministerium der Justiz angeregt, die Problematik zusätzlich zentral zu thematisieren. Durch eine fallunabhängige und regelmäßige Sensibilisierung der Beschäftigten ließe sich nach meinem Dafürhalten der Datenschutz auch in diesem Bereich stärken. Darüber hinaus habe ich das Justizministerium um die Prüfung und gegebenenfalls Anpassung weitergehender qualitätssichernder Maßnahmen zur Verhinderung ähnlich gelagerter Datenschutzverstöße gebeten.

Das Justizministerium bedauerte die Unregelmäßigkeiten im Zusammenhang mit Mitteilungen nach Nr. 42 MiStra. Um bestmöglich zu vermeiden, dass sich solche und ähnlich gelagerte Vorgänge wiederholen, machte das Justizministerium die Generalstaatsanwälte in München, Nürnberg und Bamberg anhand eines Schreibens auf die fehlerhaften Mitteilungen aufmerksam und bat um regelmäßige Sensibilisierung für dieses Thema. Zusätzlich wurde auch die besondere Wichtigkeit der Datenpflege, insbesondere der korrekten Eintragung der Ausländereigenschaft, hervorgehoben. Ergänzend erzeugt das Sachbearbeitungsprogramm nach Abschluss wichtiger Verfahrensschritte standardmäßig einen Hinweis für die Sachbearbeitenden, die Personendaten – einschließlich der Staatsangehörigkeit – zu überprüfen.

4.4 Nennung personenbezogener Daten in einer Anklageschrift

Ich erhalte immer wieder Eingaben von Petentinnen und Petenten im Zusammenhang mit der Nennung personenbezogener Daten im Rahmen von Anklageschriften der Staatsanwaltschaften. Auch im Berichtszeitraum wandte sich eine Erziehungsberechtigte an mich, nachdem ihr minderjähriger Sohn zusammen mit weiteren Jugendlichen verschiedener Delikte angeklagt worden war. In datenschutzrechtlicher Hin-

sicht rügte sie die in der Anklageschrift erfolgte Nennung verschiedener personenbezogener Daten ihres Kindes, wie zum Beispiel die Angabe des Namens, Vornamens, Geburtsdatums, Familienstands und der Adresse sowie der Staatsangehörigkeit. Die betreffenden Angaben der gesetzlichen Vertreter seien ebenfalls in der Anklageschrift enthalten gewesen. Zudem habe die Anklageschrift die betreffenden Daten aller Angeschuldigten enthalten, die nun über die entsprechenden Daten zu ihren Mitangeschuldigten informiert seien.

§ 200 Strafprozessordnung (StPO) in Verbindung mit Nr. 110 Abs. 2 Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) bestimmen die Form und den erforderlichen Inhalt einer staatsanwaltschaftlichen Anklageschrift. Nach Nr. 110 Abs. 2 Buchst. a RiStBV sind in der Anklageschrift der Familienname und die Vornamen, Geburtsname, Beruf, Anschrift, Familienstand, Geburtstag und Geburtsort (Kreis, Bezirk) des Angeschuldigten und seine Staatsangehörigkeit, bei Minderjährigen Namen und Anschriften der gesetzlichen Vertreter anzugeben.

Weder die Erhebung noch die Verarbeitung der in Nr. 110 Abs. 2 RiStBV genannten Daten in der Anklageschrift war im vorliegenden Fall damit datenschutzrechtlich zu beanstanden. Hintergrund für die Erfassung der Erziehungsberechtigten und gesetzlichen Vertreter in der Anklageschrift ist, dass dem genannten Personenkreis weitreichende Mitwirkungsrechte am Prozess eingeräumt werden (beispielsweise das Ladungsrecht nach § 50 Abs. 2 Jugendgerichtsgesetz – JGG, Fragerechte nach § 67 JGG). Eine Einwilligung der betroffenen Personen ist für die Verarbeitung dieser Daten durch die Staatsanwaltschaft oder das Gericht nicht erforderlich.

Die Verarbeitung personenbezogener Daten mehrerer Mitangeschuldigter sowie ihrer gesetzlichen Vertreter im Rahmen einer einheitlichen Anklageschrift ist datenschutzrechtlich grundsätzlich nicht zu beanstanden. Denn gemäß §§ 2, 3 StPO in Verbindung mit Nr. 114 Satz 1 RiStBV sind zusammenhängende Strafsachen in einer Anklage zusammenzufassen. Nach § 3 StPO sind zusammenhängende Strafsachen gegeben, wenn eine Person mehrerer Straftaten beschuldigt wird oder wenn bei einer Tat mehrere Personen als Täter, Teilnehmer oder der Datenhehlerei, Begünstigung, Strafvereitelung oder Hehlerei beschuldigt werden. Soweit ein solcher Zusammenhang gegeben ist, ist die Staatsanwaltschaft verpflichtet, eine einheitliche Anklageschrift mit den oben genannten Angaben zu erstellen. Von einer nicht-einheitlichen Anklage kann nach Nr. 114 Satz 2 RiStBV lediglich abgesehen werden, wenn die Erhebung der öffentlichen Klage wegen einer Tat durch die Aufklärung der anderen Tat erheblich verzögert würde und wenn gewichtige Interessen der Allgemeinheit oder des Beschuldigten (an einer Beschleunigung mittels einheitlicher Anklage) nicht entgegenstehen.

Die Nennung von Geburtsdatum, Staatsangehörigkeit und Familienstand des gesetzlichen Vertreters in der Anklageschrift war nach Nr. 110 Abs. 2 Buchst. a RiStBV demgegenüber gerade nicht erforderlich und stellte einen datenschutzrechtlichen Verstoß dar.

Die betreffende Staatsanwaltschaft räumte den Fehler in Bezug auf die Nennung von Geburtsdatum, Staatsangehörigkeit und Familienstand des gesetzlichen Vertreters in der Anklageschrift unumwunden ein. Ursache hierfür war ein Versehen der zuständigen Sachbearbeitung, welche die betreffenden Angaben in der Anklageschrift guten Gewissen händisch ergänzt hatte, ohne auf die automatisierte (Nicht-)Vorbelegung hinreichend Rücksicht zu nehmen. Die Sachbearbeitung wie auch die Leitung der betreffenden Abteilung wurden auf die Regelung der Nr. 110 Abs. 2 Buchst. a RiStBV

hingewiesen und gebeten, künftig darüber hinausgehende Personalien gesetzlicher Vertreter nicht mehr in die Anklageschrift aufzunehmen.

4.5 Beanstandung eines Notars wegen unzulässiger Einsichtnahme in das Grundbuch

§ 12 Abs. 1 Grundbuchordnung (GBO) bestimmt, dass die Einsichtnahme in das Grundbuch jedem gestattet ist, der ein berechtigtes Interesse an der Einsichtnahme darzulegen vermag. Seit dem 1. September 2013 dürfen nach § 133a GBO auch Notare demjenigen, der ihnen ein berechtigtes Interesse im Sinne von § 12 GBO darlegt, den Inhalt des Grundbuchs mitteilen. Der Umfang der Einsichtnahme richtet sich hier danach, wie weit das berechtigte Interesse reicht und dargelegt wurde. Ein verständiges, durch die Sachlage gerechtfertigtes Interesse reicht grundsätzlich aus. Auch ein tatsächliches, wirtschaftliches oder öffentliches Interesse kann das Recht auf Einsichtnahme begründen. Es müssen lediglich sachliche Gründe vorgetragen werden, die die Verfolgung unbefugter Zwecke oder bloßer Neugier ausgeschlossen erscheinen lassen.

Bei der Einsichtnahme in das Grundbuch werden sensible personenbezogene Daten offenbart. Die Teilnahme am sogenannten automatisierten Grundbuchabrufverfahren ermöglicht nicht nur die Einsicht in ein bestimmtes Grundbuchblatt. Auch die Suche nach einem unbekannten Grundbuchblatt anhand von Angaben über Flurstück oder Eigentümer ist in technischer Hinsicht möglich. Neben der Prüfung des berechtigten Interesses ist durch Ergreifung technisch-organisatorischer Maßnahmen seitens des Abfragenden auch sicherzustellen, dass lediglich solche personenbezogenen Daten abgefragt werden, für die ein berechtigtes Interesse besteht.

Im vorliegenden Berichtszeitraum musste ich im Rahmen einer Petition einen Notar beanstanden, der diese notwendigen technisch-organisatorischen Maßnahmen bei einer Grundbucheinsicht nicht ergriffen hatte. Der Notar sollte im Auftrag eines Vollstreckungsgläubigers im automatisierten Abrufverfahren unbekannte Grundbuchblätter des Vollstreckungsschuldners recherchieren. Dies tat der Notar auch, verwendete aus zeitlichen Gründen bei der Suche allerdings lediglich Vor- und Nachnamen des Vollstreckungsschuldners als Suchparameter. Da der Petent sowohl den gleichen Vor- als auch Nachnamen wie der Vollstreckungsschuldner hatte, kam es zu einer Personenverwechslung, und dem Vollstreckungsgläubiger wurden durch den Notar die Grundbuchdaten des unbeteiligten Petenten übersandt. Dies führte schließlich zur Eintragung einer Zwangssicherungshypothek sowie eines Zwangsversteigerungsvermerks in das Grundstück des Petenten, der mit der zugrundeliegenden Angelegenheit nichts zu tun hatte.

Ich beanstandete den Notar wegen Nichteinhaltung der datenschutzrechtlichen Anforderungen bei Grundbuchabfragen. Denn im Rahmen der Suche anhand von Angaben zum Eigentümer kann im automatisierten Abrufverfahren neben Namen, Vornamen und gegebenenfalls. Geburtsnamen auch das Geburtsdatum als sucheingrenzendes Kriterium herangezogen werden. Soweit im Rahmen einer Suche nach unbekannten Grundbuchblättern nicht bereits der Name selbst hinreichende Gewähr dafür bietet, dass nicht fälschlicherweise Grundbuchinformationen Unbeteiligter als Suchergebnisse angezeigt werden, obliegt es dem Abfragenden durch die Verwendung aller zumutbarer Anstrengungen, insbesondere durch die Verwendung aller systemseitig vorhandenen Suchparameter, eine Personenverwechslung möglichst auszuschließen (so auch § 133 Abs. 2 Satz 2 Nr. 2 GBO in Verbindung mit Art. 5 Abs. 1

Buchst. c DSGVO). Dies macht es – vor allem bei gängigen Namen – regelmäßig notwendig, Recherchen zu unbekannten Grundbuchblättern nicht nur anhand des Vor- und Nachnamens durchzuführen, sondern insbesondere auch das Geburtsdatum als Suchkriterium zu verwenden.

5 Allgemeine Innere Verwaltung

5.1 Datennutzungssatzungen: nur Aufgabenkonkretisierung für unwesentliche Eingriffe zulässig

Im Rahmen meiner Prüftätigkeit habe ich erfahren, dass einige bayerische Kommunen mit dem Gedanken spielen, sogenannte Datennutzungssatzungen zu erlassen. In diesen Satzungen sollen nach den Vorstellungen der betroffenen Kommunen Datenverarbeitungsbefugnisse im Sinne von Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO für freiwillig von den Kommunen übernommene Aufgaben geschaffen werden. Begegnet ist mir etwa folgende Formulierung: „Im Rahmen der Ausübung ihrer Planungsaufträge dürfen nach Maßgabe dieser Satzung seitens der Sozial-, Jugendhilfe- und Bildungsplanung bei der Gemeinde X gesetzlich geschützte Daten aus unterschiedlichen Quellen für planerische Auswertungszwecke erhoben und verarbeitet werden". Aus datenschutzrechtlicher Sicht sind solche Satzungen zur Schaffung von Verarbeitungsbefugnissen jedoch sehr kritisch zu bewerten.

Allenfalls können die Kommunen in einem engen Rahmen und bei geringer Grundrechtsrelevanz durch Satzung Regelungen treffen, in denen **gesetzliche Datenverarbeitungsbefugnisse** (etwa aus Art. 4 Abs. 1 BayDSG oder § 37 Bundesmeldegesetz – BMG) gleichsam **„aktiviert"** werden. Dies beruht auf folgenden Erwägungen:

5.1.1 Erforderlichkeit einer Rechtsgrundlage für die Verarbeitung personenbezogener Daten

Öffentliche Stellen, wie sie etwa Kommunen bilden, benötigen für die Verarbeitung personenbezogener Daten eine Rechtsgrundlage (vgl. Art. 6 Abs. 1 DSGVO). Öffentliche Stellen sollen sich bei der Erfüllung ihrer öffentlichen Aufgaben primär auf die speziellen fachgesetzlichen Befugnisse zur Verarbeitung personenbezogener Daten bzw. auf die allgemeine Befugnisnorm des Art. 4 Abs. 1 BayDSG stützen (vgl. Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO).

Nach Art. 4 Abs. 1 BayDSG ist die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle unbeschadet sonstiger Bestimmungen zulässig, wenn sie zur Erfüllung einer ihr obliegenden Aufgabe erforderlich ist. Bei Berufung auf die allgemeine Befugnisnorm des Art. 4 Abs. 1 BayDSG hat die öffentliche Stelle grundsätzlich genau zu benennen, welche öffentliche – durch Gesetz auferlegte oder auf Grund gesetzlicher Zulassung ergriffene – Aufgabe sie mit der Datenverarbeitung erfüllt und inwiefern die Datenverarbeitung hierfür erforderlich ist.

Insoweit ist einzuräumen, dass die allgemeine Verarbeitungsbefugnis des Art. 4 Abs. 1 BayDSG nur wenige Tatbestandsmerkmale enthält. Die Vorschrift bezieht die Erforderlichkeit auf eine der betroffenen öffentlichen Stelle obliegende **Aufgabe**. Gleiches gilt hinsichtlich der allgemeinen Übermittlungsbefugnis in Art. 5 Abs. 1 Satz 1 Nr. 1 Var. 1 BayDSG sowie für melderechtlichen Übermittlungs- oder Weitergabebefugnisse nach § 34 Abs. 1 BMG bzw. § 37 Abs. 1 in Verbindung mit § 34 Abs. 1 BMG.

5.1.2 Erforderlichkeit einer parlamentsgesetzlichen Ermächtigung für Verarbeitungsbefugnisse in kommunalen Satzungen

Kommunen haben gesetzliche Pflichtaufgaben und freiwillige Aufgaben zu erfüllen (vgl. Art. 57 Abs. 1 und 2 Gemeindeordnung – GO, Art. 83 Abs. 1 Verfassung des Freistaates Bayern). Insbesondere können Kommunen im Rahmen ihres Selbstverwaltungsrechts (Art. 28 Abs. 2 Grundgesetz – GG) auch freiwillige öffentliche Aufgaben übernehmen.

Gleichwohl sind die Kommunen **nicht befugt, ohne parlamentsgesetzliche Ermächtigung durch Satzung Befugnisse zur Verarbeitung personenbezogener Daten zu schaffen.** Dies folgt weniger aus dem Unionsrecht als vielmehr aus dem **deutschen Verfassungsrecht**.[48] Der Rückgriff auf deutsche Grundrechte ist möglich, weil das Unionsrecht den Mitgliedstaaten im Bereich der datenschutzrechtlichen Normen zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, oder zur Ausübung öffentlicher Gewalt einen Regelungsspielraum gewährt (vgl. Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 UAbs. 1 Buchst. b DSGVO). Es handelt sich bei dem hier in Rede stehenden Bereich um unionsrechtlich nicht vollständig determiniertes innerstaatliches Recht, das an den deutschen Grundrechten zu messen ist.[49] Art. 6 Abs. 2, Abs. 3 UAbs. 1 Buchst. b DSGVO sieht für die Mitgliedstaaten eine Konkretisierungsbefugnis zur Schaffung nationaler Rechtsgrundlagen für die Datenverarbeitung zur Erfüllung öffentlicher Aufgaben vor (Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO). Bereits das unionsrechtliche Subsidiaritätsprinzip (Art. 4 Abs. 2, Art. 5 Vertrag über die Europäische Union) streitet dafür, den Mitgliedstaaten bei der Frage des „Wie" der Ausübung dieser Konkretisierungsbefugnis einen Gestaltungsspielraum zuzugestehen, zumal Art. 6 Abs. 2, Abs. 3 UAbs. 1 Buchst. b DSGVO in Bezug auf die Frage des Rangs der nationalen Konkretisierungsgesetze keine Vorgabe macht. Deutlich in diese Richtung auch Erwägungsgrund 41 DSGVO:

Erwägungsgrund 41 DSGVO
Rechtsgrundlagen und Gesetzgebungsmaßnahmen
[1]Wenn in dieser Verordnung auf eine Rechtsgrundlage oder eine Gesetzgebungsmaßnahme Bezug genommen wird, erfordert dies nicht notwendigerweise einen von einem Parlament angenommenen Gesetzgebungsakt; davon unberührt bleiben Anforderungen gemäß der Verfassungsordnung des betreffenden Mitgliedstaats. [2]Die entsprechende Rechtsgrundlage oder Gesetzgebungsmaßnahme sollte jedoch klar und präzise sein und ihre Anwendung sollte für die Rechtsunterworfenen gemäß der Rechtsprechung des Gerichtshofs der Europäischen Union (im Folgenden „Gerichtshof") und des Europäischen Gerichtshofs für Menschenrechte vorhersehbar sein.

So stellt die Verarbeitung von personenbezogenen Daten durch öffentliche Stellen einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) der hiervon betroffenen Personen dar. Auf Grund des verfassungsrechtlichen Vorbehalts des Gesetzes bedarf es hierfür einer gesetzlichen Grundlage.[50] Nach der sogenannten Wesentlichkeitstheorie ist „der Gesetzgeber verpflichtet […],– losgelöst vom Merkmal des ‚Eingriffs' – in grundlegenden nor-

48 Vgl. auch Albers/Veit, in: Wolff/Brink, Beck'scher Online-Kommentar Datenschutzrecht, Stand 11/2019, Art. 6 DSGVO Rn. 58.

49 Siehe Bundesverfassungsgericht, Beschluss vom 6. November 2019, 1 BvR 16/13, NJW 2020, 300 (302).

50 Siehe Bundesverfassungsgericht, Urteil vom 6. Juli 1999, 2 BvF 3/90, BVerfGE 101, 1 (34).

mativen Bereichen, zumal im Bereich der Grundrechtsausübung, soweit diese staatlicher Regelung zugänglich ist, alle wesentlichen Entscheidungen selbst zu treffen".[51] Das Bundesverfassungsgericht konkretisiert dabei die Wesentlichkeitstheorie insoweit, dass wesentlich (gerade) diejenigen Entscheidungen sind, die für die Verwirklichung von Grundrechten wesentlich sind.[52] Dies hat Auswirkungen auch auf die Frage, ob und wie mit Satzungsautonomie ausgestattete öffentliche Stellen durch eine Bestimmung in einer Satzung in Grundrechte eingreifen dürfen. Auch Kommunen benötigen daher für Grundrechtseingriffe im Rahmen ihres Satzungsrechts eine parlamentsgesetzliche Ermächtigung.[53] **Somit bedarf die Kommune einer gesetzlichen Ermächtigung, wenn sie mit einer Datennutzungssatzung in das Recht auf informationelle Selbstbestimmung eingreifen will.** Art. 23 Satz 1 GO stellt eine solche Ermächtigung jedoch **nicht** bereit, weil diese Vorschrift nur zu Regelungen ermächtigt, die nicht in Rechte Dritter eingreifen. Zwar enthält Art. 24 GO gesetzliche Ermächtigungen zum Erlass von Satzungen, die in Grundrechte Dritter eingreifen.[54] Für die Regelung von allgemeinen Datenverarbeitungsbefugnissen im Bereich freiwilliger Aufgaben lässt sich allerdings **aus Art. 24 GO keine besondere gesetzliche Ermächtigung ableiten**. Daher **können Kommunen in Satzungen** — auch im Bereich von freiwilligen kommunalen Aufgaben — **keine eigenständigen Datenverarbeitungsbefugnisse schaffen**.

5.1.3 Zulässig nur Aufgabenkonkretisierung bei unwesentlichen Eingriffen

Denkbar ist vor diesem Hintergrund nur, dass die Kommune in einer Satzung eine freiwillige öffentliche Aufgabe festlegt und sich dann bei der Datenverarbeitung auf daran knüpfende gesetzliche Verarbeitungsbefugnisse wie etwa in Art. 4 Abs. 1 oder Art. 5 Abs. 1 Nr. 1 Var. 1 BayDSG beruft. Auch dadurch wird es den Kommunen aber nicht möglich, quantitativ oder qualitativ in wesentlichem Ausmaß in das Grundrecht auf informationelle Selbstbestimmung einzugreifen. Vielmehr können insbesondere die allgemeinen Verarbeitungsbefugnisse aus dem Bayerischen Datenschutzgesetz auch auf Grund satzungsrechtlicher Aufgabenkonkretisierungen **nur unwesentliche Eingriffe legitimieren**. Denkbar sind insoweit insbesondere die in meinen Aktuellen Kurz-Informationen 5, 10 und 16 bereits eingehend erläuterten Konstellationen.[55]

51 Siehe Bundesverfassungsgericht, Beschluss vom 8. August 1978, 2 BvL 8/77, BVerfGE 49, 89 (126).

52 Siehe Bundesverfassungsgericht, Beschluss vom 6. Juni 1989,1 BvR 727/84, BVerfGE 80, 124 (132).

53 Siehe Bundesverfassungsgericht, Beschluss vom 13. Juli 2004, 1 BvR 1298/94, BVerfGE 111, 191, Rn. 147 ff.; Oberverwaltungsgericht Rheinland-Pfalz, Urteil vom 8. März 1994, 7 C 11302/93, juris, Rn. 22; Burghart in: Leibholz/Rinck, Grundgesetz, Stand 10/2019, Art. 20 GG Rn. 236; siehe auch speziell für Kommunen: Bayerischer Verwaltungsgerichtshof, Urteil vom 14. Juli 2011, 4 N 10.2660, juris, Rn. 29; Bayerischer Verwaltungsgerichtshof, Beschluss vom 27. Februar 2017, 4 N 16.461, ZD 2017, 487, Rn. 19 ff.

54 Siehe Bayerischer Verwaltungsgerichtshof, Beschluss vom 27. Februar 2017, 4 N 16.461, ZD 2017, 487, Rn. 19 f.

55 Bayerischer Landesbeauftragter für den Datenschutz, Melderegisterdaten und Gratulationen, Aktuelle Kurz-Information 5, Stand 1/2022, Einladungen zu Veranstaltungen durch bayerische Kommunen, Aktuelle Kurz-Information 10, Stand 10/2018, sowie Fotografien in der Öffentlichkeitsarbeit bayerischer Kommunen, Aktuelle Kurz-Information 16, Stand 12/2018, alle Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Aktuelle Kurz-Informationen".

5.2 E-Tickets im ÖPNV

5.2.1 Sachverhalt

Die Unternehmen des öffentlichen Personennahverkehrs bieten neben dem klassischen Papierfahrschein zunehmend auch sogenannte E-Tickets an. Hierbei handelt es sich um eine Form der Digitalisierung, mit der viele Bürgerinnen und Bürger tagtäglich bei der Fahrt mit den Verkehrsmitteln des ÖPNV in Berührung kommen. Erfahrungsgemäß verleiten solche elektronischen Angebote aufgrund ihrer systemimmanenten „Einfachheit“ dazu, mehr an Daten zu verarbeiten als zur Erreichung des verfolgten Zwecks erforderlich ist, was gegen den Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) verstößt. Daher habe ich mehrere Eingaben bei mir zum Anlass einer eingehenden Überprüfung der Datenverarbeitungen eines kommunalen Verkehrsunternehmens genommen, welches solche E-Tickets an seine Abonnentinnen und Abonnenten ausgab.

Konkret bestand das E-Ticket aus einer Chipkarte, wobei der Chip folgende Informationen speicherte: maskierter Vor- und Nachname (erster und letzter Buchstabe von Vor- und Nachnamen sowie die jeweilige Gesamtzahl der Zeichen), Geburtsdatum, Geschlecht, gewähltes Tarifprodukt (insbesondere Tarifzone, Preisstufe, zeitliche Gültigkeit, Ticketnummer) sowie die letzten 10 Transaktionen (etwa Kontrollen, Ticketkäufe oder Ticketänderungen). Aufgedruckt auf der Chipkarte waren Vor- und Nachname sowie ein Lichtbild, das von der Kundin oder dem Kunden im Rahmen des Bestellvorgangs zu übermitteln war und beim Unternehmen auch nach Aushändigung des E-Tickets weiterhin gespeichert blieb.

5.2.2 Zentrale Ergebnisse der Überprüfung

Vor der Darstellung der zentralen Prüfergebnisse skizziere ich zum besseren Verständnis kurz den rechtlichen Rahmen der Überprüfung.

Öffentliche Stellen, wie kommunale Verkehrsunternehmen, benötigen für die Verarbeitung von personenbezogenen Daten eine Rechtsgrundlage (vgl. Art. 6 Abs. 1 DSGVO). Die Erbringung von Verkehrsdienstleistungen im ÖPNV und die Direktwerbung für diese Dienstleistungen ist eine Teilnahme als Unternehmen am Wettbewerb gemäß Art. 1 Abs. 3 BayDSG. Daher gelten insoweit die Vorschriften für nicht öffentliche Stellen, das heißt die Datenschutz-Grundverordnung und nachrangig das Bundesdatenschutzgesetz(siehe dazu meine Ausführungen im 30. Tätigkeitsbericht 2020 unter Nr. 6.1.2). Mögliche Rechtsgrundlagen für die Verarbeitung personenbezogener Daten im Rahmen des E-Tickets sind daher neben der Einwilligung (Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO), die Vertragserfüllung (Art. 6 Abs. 1 UAbs. 1 Buchst. b), die Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 UAbs. 1 Buchst. c) und die Wahrnehmung berechtigter Interessen (Art. 6 Abs. 1 UAbs. 1 Buchst. f). Datenschutzverstöße können aufgrund der Wettbewerbsteilnahme zur Verhängung von Geldbußen führen (Art. 22 BayDSG, Art. 83 DSGVO).

5.2.2.1 Datenspeicherungen im Chip

Nichts einzuwenden hatte ich gegen die Speicherung des (maskierten) **Vor- und Nachnamens**, des **Geburtsdatums** und des **Tarifprodukts** im Chip. Die Verarbeitung dieser Daten war für das Verkehrsunternehmen erforderlich, um den mit der

Kundin oder dem Kunden geschlossenen Beförderungsvertrag, der auch die Kontrolle der Fahrtberechtigung einschließt, zu erfüllen. Dabei war zu beachten, dass es sich beim E-Ticket um ein personalisiertes Produkt handelt. Es wird nur eine bestimmte Person (Abonnentin oder Abonnent) durch das E-Ticket zur Fahrt im ÖPNV berechtigt und legitimiert. Somit konnte sich das Unternehmen auf Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO als Rechtsgrundlage berufen. Maskierter Vor- und Nachname sowie Geburtsdatum waren erforderlich, um eine Person eindeutig zu identifizieren.

Keine Rechtsgrundlage konnte ich dagegen für die Speicherung des **Geschlechts** erkennen. Zwar machte das Unternehmen geltend, dass es sich auch insoweit um ein Identifikationsmerkmal handle. Dem trat ich jedoch entgegen, da eine eindeutige Identifizierung bereits durch Vor- und Nachname sowie Geburtsdatum gelingt. Das Unternehmen verzichtet daher künftig auf die Speicherung des Geschlechts. Chipkarten von Bestandskundinnen und Bestandskunden sollen sukzessive aber zeitnah in einem rollierenden Verfahren bei Vertragsverlängerungen gegen die neuen, datensparsameren Chipkarten ausgetauscht werden.

Kritisch bewertete ich daneben die Speicherung der **Transaktionsdaten** im Chip, da hiervon auch Zeitpunkt, Ort, Fahrt und Linie umfasst sein können. Zwar speichert der Chip nur zehn Transaktionen, die elfte überschreibt also die erste Transaktion. Dennoch ist es theoretisch nicht ausgeschlossen, dass Bewegungsprofile gebildet werden können. Zu berücksichtigen war insoweit aber auch, dass die Möglichkeit einer solchen Profilbildung von der Dichte der Fahrscheinkontrollen abhängt. Bei nur zehn gespeicherten Transaktionen und einer lediglich gelegentlichen Kontrolle durch mobile Teams scheint diese Möglichkeit kaum zu bestehen. Wird jedoch das E-Ticket regelhaft beim Einstieg in Fahrzeuge des ÖPNV kontrolliert, so ist durchaus eine Profilbildung denkbar. Das geprüfte Unternehmen hatte zwar bei Fahrten mit Bussen solche Kontrollen vorgesehen, es versicherte mir jedoch, beim Betrieb des E-Tickets würden die kritischen Datenkategorien Ort, Fahrt und Linie mit Nullen oder anonymisierten Nummern gefüllt, was eine **Bewegungsprofilbildung verhindere**. Im Hinblick auf die Zusicherung, dass dies nicht geändert würde, stellte ich meine **Einwände zurück**. Gleichwohl wies ich das Unternehmen darauf hin, dass das rechtliche Fundament, auf dem die Speicherung der Transaktionsdaten zum Zeitpunkt meiner Prüfung beruhte, „brüchig“ war. Das Verkehrsunternehmen rechtfertigte die Speicherung des Transaktionslogbuchs vor allem mit dem Gesichtspunkt der Kundentransparenz. Allerdings war nach meiner Auffassung die Speicherung von zehn Transaktionsdaten zur Erfüllung des Beförderungsvertrags nicht erforderlich, da dieser keine solche Transparenzpflicht des Unternehmens vorsah. Daraufhin passte das Unternehmen den Vertragsinhalt an. Ich erläuterte dem Unternehmen jedoch auch, dass der Grundsatz der Transparenz (Art. 5 Abs. 1 Buchst. a DSGVO) nach der Systematik der Datenschutz-Grundverordnung im Wesentlichen durch Informationspflichten (Art. 13 f. DSGVO) und das Recht auf Auskunft (Art. 15 DSGVO) verwirklicht wird, nicht aber durch zusätzliche Datenspeicherungen. Daher begrüßte ich die Zusage des Unternehmens, in wenigen Jahren eine **neue Chipkartengeneration einzuführen, welche keine Transaktionsdaten mehr speichert.**

5.2.2.2 Chipkarte: Aufdruck von Lichtbild sowie Vor- und Nachname

Nach den Tarifbestimmungen des Verkehrsunternehmens diente das auf der Chipkarte aufgedruckte **Lichtbild** dem Zweck, sich bei Kontrollen als Abonnentin oder Abonnent auszuweisen. Ein Personalausweis musste dann während der Fahrt nicht zwecks Identifizierung mitgeführt werden. Dies war nur erforderlich, wenn Kundinnen oder Kunden im Bestellprozess kein Foto zur Verfügung gestellt hatten. Allerdings

kam ich bei der Prüfung der im Rahmen des Bestellprozesses übermittelten Informationen zu dem Ergebnis, dass über die genannten Umstände und Folgen nicht transparent aufgeklärt wurde. Im Gegenteil: Nach meiner Wahrnehmung wurde Kundinnen und Kunden vielmehr der Eindruck vermittelt, sie müssten stets ein Lichtbild zur Verfügung stellen. Mithin **fehlte** es an einer **wirksamen** – insbesondere informierten und freiwilligen – **Einwilligung** für die Datenverarbeitung. Auch eine **andere Rechtsgrundlage** für die Datenverarbeitung lag **nicht** vor. Für die Ticketkontrolle war das Foto nämlich nicht zwingend zur Vertragsabwicklung erforderlich. So war nach den Tarifbestimmungen eine Kontrolle auch durch Abgleich mit einem – dann verpflichtend mitzuführenden – Lichtbildausweis möglich. Daher war eine Verarbeitung des Fotos zu Kontrollzwecken nicht im datenschutzrechtlichen Sinne erforderlich. Zwar mag ein aufgedrucktes Foto dazu dienen, das eigene E-Ticket von denen anderer Fahrgäste oder Familienmitglieder schnell zu unterscheiden. Allerdings ist es für diesen Zweck **ausreichend und vorzugswürdig**, wenn die Chipkarte ein **unbeschriebenes Notizfeld** enthält, in welches freiwillig der Namen eingetragen werden kann.

Auch für den Aufdruck von **Vor- und Nachnamen** auf der Chipkarte lag **keine Rechtsgrundlage** vor. Im Hinblick auf die Individualisierung der eigenen Karte gilt das eben Gesagte entsprechend. Ein unbeschriebenes Notizfeld auf der Karte, in welches freiwillig der Name eingetragen werden kann, ist insoweit ausreichend und vorzugswürdig. In Bezug auf die Identifikationsmöglichkeit bei Fahrscheinkontrollen wies ich das Unternehmen darauf hin, dass Vor- und Nachname bereits im Chip des E-Tickets maskiert enthalten sind und bei Kontrollen ausgelesen werden können. Insoweit konnte mir nicht hinreichend begründet werden, welchen Sinn der Vergleich der aufgedruckten Namensdaten mit den im Chip enthaltenen maskierten Daten durch das Kontrollpersonal haben soll. Im Gegenteil führt doch der Aufdruck des Klarnamens auf der Chipkarte die Maskierung des Namens bei der Speicherung im Chip ad absurdum. Auch genügt der Abgleich des maskierten Namens mit einem mitgeführten amtlichen Ausweis für eine Identitätskontrolle. Daher **begrüßte** ich es, dass das Verkehrsunternehmen eine **neue Chipkarte** eingeführt hat, bei der keine Namen mehr aufgedruckt sind. Auch der Aufdruck des Fotos ist für die Kundinnen und Kunden jetzt im datenschutzrechtlichen Sinne freiwillig, da sie im Bestellprozess nun transparent aufgeklärt werden. Während Neukundinnen und Neukunden diese neue datensparsame Chipkarte sofort erhalten, wird diese an Bestandskundinnen und Bestandskunden wiederum in einem rollierenden Verfahren ausgegeben.

5.2.2.3 Speicherung des Fotos auch nach Aushändigung des E-Tickets

Das im Rahmen des Bestellprozesses von einer Kundin oder einem Kunden zur Verfügung gestellte Porträtfoto wurde von dem geprüften Unternehmen über die Erstellung des konkreten E-Tickets hinaus weiterhin gespeichert, um etwa im Falle einer Ersatzausstellung bereits ein Foto vorrätig zu haben. Auch für diese Datenverarbeitung lag **keine Rechtsgrundlage**, insbesondere keine wirksame Einwilligung, vor. Eine solche hatte das Unternehmen im Bestellvorgang nicht eingeholt, sondern nur auf die Löschmöglichkeit verwiesen. Allerdings ersetzt der Verweis auf das Recht auf Löschung (Art. 17 DSGVO) nicht die Einholung einer Einwilligung (Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 7 DSGVO). Das Unternehmen kündigte insoweit an, **zukünftig im Bestellprozess wirksame Einwilligungen** für die weitere Speicherung, etwa für die Ausstellung von Ersatzkarten oder neuer Karten, **einzuholen**. Bestandskundinnen und Bestandskunden würden angeschrieben und um Einwilligung zur weiteren Speicherung gebeten. Wird diese nicht erteilt, würden die bislang gespeicherten Fotos gelöscht.

5.2.2.4 Fazit

Bei der Digitalisierung im ÖPNV müssen kommunale Verkehrsunternehmen insbesondere den Grundsatz der Datenminimierung beachten, dürfen also bei der Verwendung von E-Tickets grundsätzlich nur solche Daten verarbeiten, die zur Erreichung des verfolgten Zwecks erforderlich sind. Soll die Datenverarbeitung auf eine Einwilligung gestützt werden, ist auf deren wirksame Einholung zu achten.

5.3 Erneut: Datenschutzkonformität von Förderungen

Im Berichtszeitraum war ich erneut mit der Datenschutzkonformität von Fördermaßnahmen befasst, wobei es diesmal nicht um staatliche Förderungen ging (siehe dazu meine Ausführungen im 29. Tätigkeitsbericht 2019 unter Nr. 5.4), sondern um eine kommunale Sportförderung.

Konkret war in einer kommunalen Sportförderrichtlinie insoweit Folgendes vorgesehen: Bei Anträgen auf Sportförderung hatten die antragstellenden Vereine von den bei ihnen tätigen Personen unter bestimmten Voraussetzungen die Vorlage eines erweiterten Führungszeugnisses nach § 30a Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz – BZRG) zu verlangen, dieses zu prüfen und die Prüfung für die Kommune nachprüfbar zu dokumentieren. Ziel der kommunalen Förderrichtlinie war es auszuschließen, dass in den geförderten Vereinen einschlägig vorbestrafte Personen im Kinder- und Jugendsport tätig sind.

§ 30 BZRG
Antrag
(1) [1]Jeder Person, die das 14. Lebensjahr vollendet hat, wird auf Antrag ein Zeugnis über den sie betreffenden Inhalt des Registers erteilt (Führungszeugnis). [2]Hat sie eine gesetzliche Vertretung, ist auch diese antragsberechtigt. [3]Ist die Person geschäftsunfähig, ist nur ihre gesetzliche Vertretung antragsberechtigt.
[…]

§ 30a BZRG
Antrag auf ein erweitertes Führungszeugnis
(1) Einer Person wird auf Antrag ein erweitertes Führungszeugnis erteilt,
1. wenn die Erteilung in gesetzlichen Bestimmungen unter Bezugnahme auf diese Vorschrift vorgesehen ist oder
2. wenn dieses Führungszeugnis benötigt wird für
d) eine berufliche oder ehrenamtliche Beaufsichtigung, Betreuung, Erziehung oder Ausbildung Minderjähriger oder
e) eine Tätigkeit, die in einer Buchstabe a vergleichbaren Weise geeignet ist, Kontakt zu Minderjährigen aufzunehmen.
(2) [1]Wer einen Antrag auf Erteilung eines erweiterten Führungszeugnisses stellt, hat eine schriftliche Aufforderung vorzulegen, in der die Person, die das erweiterte Führungszeugnis von der antragstellenden Person verlangt, bestätigt, dass die Voraussetzungen nach Absatz 1 vorliegen. [2]Im Übrigen gilt § 30 entsprechend.
(3) [1]Die Daten aus einem erweiterten Führungszeugnis dürfen von der entgegennehmenden Stelle nur verarbeitet werden, soweit dies zur Prüfung der Eignung der Person für eine Tätigkeit, die Anlass zu der Vorlage des Führungszeugnisses gewesen ist, erforderlich ist. [2]Die Daten sind vor dem Zugriff Unbefugter zu schützen. [3]Sie sind unverzüglich zu löschen, wenn die Person die Tätigkeit, die Anlass zu der Vorlage des Führungszeugnisses gewesen ist, nicht ausübt. [4]Die Daten sind spätestens sechs Monate nach der letztmaligen Ausübung der Tätigkeit zu löschen.

Das kommunale Sportförderreferat bot für die Umsetzung dieser Vorgaben den an der Sportförderung interessierten Vereinen seine Unterstützung an. Dieses „Serviceangebot" war unverbindlich.

Konkret konnten die Vereine von allen betroffenen Personen einen Antrag auf Ausstellung eines erweiterten Führungszeugnisses unterschreiben lassen und Ausweiskopien zur Vorlage beim kommunalen Sportförderreferat einbehalten. Weiter war vorgesehen, dass der Verein alle betroffenen Personen in einer Liste erfasst und diese mitsamt den jeweiligen Anträgen sowie den Ausweiskopien im kommunalen Sportförderreferat abgibt. Die auf den Anträgen befindlichen Unterschriften wurden sodann durch Beschäftigte des kommunalen Sportförderreferats gesichtet und mit den Unterschriften auf den übersandten Ausweiskopien abgeglichen. Insoweit wurde durch die Beschäftigten des kommunalen Sportförderreferats „bestätigt", dass die Unterschriften auf den Anträgen mit den Unterschriften auf den Ausweiskopien übereinstimmen und die Voraussetzungen des § 30 Abs. 1 BZRG vorliegen. Nach der Sichtung im kommunalen Sportförderreferat wurden die Ausweiskopien vernichtet und die gesammelten Anträge mitsamt den „Bestätigungen" weitergeleitet an die für die Bearbeitung von Anträgen auf Erteilung von Führungszeugnissen zuständige kommunale Meldebehörde. Diese reichte die Anträge auf Erteilung von Führungszeugnissen an das Bundesamt für Justiz weiter, welches die beantragten Führungszeugnisse erstellte und an die Antragstellenden verschickte. Die Liste mit den Anträgen auf erweiterte Führungszeugnisse verblieb beim kommunalen Sportförderreferat. Die Antragstellenden legten die Führungszeugnisse sodann bei ihren jeweiligen Vereinen vor, wo die Einsichtnahme dokumentiert wurde. Diese Dokumentation verblieb beim Verein und war dem kommunalen Sportförderreferat auf Anforderung vorzulegen.

Aus datenschutzrechtlicher Sicht bewertete ich diesen Sachverhalt wie folgt:

Die Kommune verarbeitete personenbezogene Daten gemäß Art. 4 Nr. 1 und 2 DSGVO, da sie durch ihr „Serviceangebot" in zurechenbarer Weise veranlasste, dass ihr die oben genannten Unterlagen mitsamt den darin enthaltenen personenbezogenen Daten zugänglich gemacht wurden und sie mit diesen wie beschrieben umging.

Öffentliche Stellen benötigen für die Verarbeitung personenbezogener Daten eine Rechtsgrundlage (vgl. Art. 6 Abs. 1 UAbs. 1 DSGVO). Zwar kann sich eine solche auch aus einer wirksamen Einwilligung ergeben (Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 4 Nr. 11, Art. 7 DSGVO). Öffentliche Stellen sollen sich jedoch grundsätzlich bei der Erfüllung ihrer öffentlichen Aufgaben vor allem auf die speziellen fachgesetzlichen Befugnisse zur Verarbeitung personenbezogener Daten bzw. auf die – auch im konkreten Fall mangels bereichsspezifischer Regelungen einschlägige – allgemeine Befugnisnorm des Art. 4 Abs. 1 BayDSG stützen. Danach ist die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle unbeschadet sonstiger Bestimmungen zulässig, wenn sie **zur Erfüllung einer ihr obliegenden Aufgabe erforderlich** ist. Entscheidende Bedeutung kommt insoweit dem Grundsatz der **informationellen Gewaltenteilung** zu. Dieser gebietet, dass nicht jeder Angehörige einer öffentlichen Stelle auf alle dort vorhandenen personenbezogenen Daten zugreifen können darf. Vielmehr gilt das Prinzip: **Jeder darf nur auf solche Daten zugreifen können, die er für seine Aufgaben benötigt.**

Insoweit **fehlte** es aber bereits an einer entsprechenden **Aufgabe des kommunalen Sportförderreferats** für die mit dem „Serviceangebot" zusammenhängenden Datenverarbeitungen hinsichtlich von Führungszeugnissen. So oblag dem Sportförder-

referat im konkreten Fall nur die Aufgabe der Sportförderung und der damit verbundenen Bearbeitung von Anträgen förderwilliger Vereine. Die **Umsetzung eines Tätigkeitsausschlusses einschlägig vorbestrafter Personen** in Verbindung mit Kindern und Jugendlichen gemäß § 72 a Achtes Buch Sozialgesetzbuch – Kinder- und Jugendhilfe – (SGB VIII), welche im Rahmen des dort spezialgesetzlich geregelten Verfahrens eine Datenverarbeitung hinsichtlich erweiterter Führungszeugnisse rechtfertigen kann (vgl. dazu meine Ausführungen im 25. Tätigkeitsbericht 2012 unter Nr. 8.8.), **obliegt** im öffentlichen Bereich kraft Gesetz der Kinder- und Jugendhilfe. Diese Aufgabe ist gemäß Art. 15 Satz 1, Art. 16 Abs. 1 Gesetz zur Ausführung der Sozialgesetze dem **kommunalen Jugendamt** als Träger der öffentlichen Jugendhilfe zugewiesen und eben nicht der Sportförderung. Auf diese Aufgabe konnte sich das Sportförderreferat für die Datenverarbeitungen daher nicht berufen.

§ 72 a SGB VIII
Tätigkeitsausschluss einschlägig vorbestrafter Personen
[…]
(2) Die Träger der öffentlichen Jugendhilfe sollen durch Vereinbarungen mit den Trägern der freien Jugendhilfe sowie mit Vereinen im Sinne des § 54 sicherstellen, dass diese keine Person, die wegen einer Straftat nach Absatz 1 Satz 1 rechtskräftig verurteilt worden ist, hauptamtlich beschäftigen.
[…]
(4) Die Träger der öffentlichen Jugendhilfe sollen durch Vereinbarungen mit den Trägern der freien Jugendhilfe sowie mit Vereinen im Sinne des § 54 sicherstellen, dass unter deren Verantwortung keine neben- oder ehrenamtlich tätige Person, die wegen einer Straftat nach Absatz 1 Satz 1 rechtskräftig verurteilt worden ist, in Wahrnehmung von Aufgaben der Kinder- und Jugendhilfe Kinder oder Jugendliche beaufsichtigt, betreut, erzieht oder ausbildet oder einen vergleichbaren Kontakt hat. Hierzu sollen die Träger der öffentlichen Jugendhilfe mit den Trägern der freien Jugendhilfe Vereinbarungen über die Tätigkeiten schließen, die von den in Satz 1 genannten Personen auf Grund von Art, Intensität und Dauer des Kontakts dieser Personen mit Kindern und Jugendlichen nur nach Einsichtnahme in das Führungszeugnis nach Absatz 1 Satz 2 wahrgenommen werden dürfen.
[…]

Die Kommune konnte dem Sportförderreferat eine entsprechende **Datenverarbeitungsbefugnis** auch **nicht** im Rahmen ihrer Selbstverwaltungsautonomie etwa mittels einer **Sportförderrichtlinie** verschaffen.[56]

Auch konnte sich das Sportförderreferat insbesondere hinsichtlich der Ausweiskopien **nicht** auf etwaige **Einwilligungen** der Betroffenen berufen. Wie ich bereits in meinem 29. Tätigkeitsbericht 2019 unter Nr. 5.6 ausgeführt habe, dürfen bayerische öffentliche Stellen eine fehlende Datenverarbeitungsbefugnis nicht durch die systematische Einholung von Einwilligungen – auch nicht im Rahmen eines freiwilligen Serviceangebots – ersetzen.

Daneben hinterfragte ich aber auch die Weiterleitung der Antragsunterlagen einschließlich der „Bestätigungen" betreffend die Übereinstimmung der Unterschriften – auf der Ausweiskopie und dem Antrag auf das erweiterte Führungszeugnis – durch das Sportförderreferat an die Meldebehörde in datenschutzrechtlicher Hinsicht. Zwar wird der Antrag auf Erteilung eines erweiterten Führungszeugnisses für die dortige

[56] Vgl. näher Bayerischer Landesbeauftragter für den Datenschutz, „Datennutzungssatzungen bei bayerischen Kommunen?", Aktuelle Kurz-Information 41, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Aktuelle Kurz-Informationen".

Sachbearbeitung bei der Meldebehörde grundsätzlich benötigt. Der Antrag muss jedoch gemäß §§ 30a Abs. 2 Satz 2, 30 Abs. 2 Satz 1 BZRG durch die Antragstellerinnen und Antragsteller persönlich oder, soweit der Antrag schriftlich gestellt werden soll, mit amtlich oder öffentlich beglaubigter Unterschrift bei der Meldebehörde eingereicht werden. Die im gewählten Verfahren angelegte regelhafte „Bestätigung" der Übereinstimmung der Unterschriften von Abwesenden durch das Sportförderreferat sollte wohl eine amtliche Beglaubigung im Sinne des Art. 34 Bayerisches Verwaltungsverfahrensgesetz darstellen. Dies war jedoch kaum mit dem Absatz 2 der Vorschrift vereinbar. Danach sollen Unterschriften nämlich nur beglaubigt werden, wenn sie in Gegenwart der beglaubigenden Bediensteten vollzogen werden.

Art. 34 BayVwVfG
Beglaubigung von Unterschriften
[…]
(2) Eine Unterschrift soll nur beglaubigt werden, wenn sie in Gegenwart des beglaubigenden Bediensteten vollzogen oder anerkannt wird.

Damit war aber auch das Vorliegen ordnungsgemäß gestellter Anträge auf Ausstellung von Führungszeugnissen fraglich, womit die Erforderlichkeit der diesbezüglichen Datenverarbeitungen im Sportreferat beziehungswiese der Weiterleitung der Unterlagen innerhalb der Kommune zur Meldebehörde ebenfalls zweifelhaft erschien.

Von einer förmlichen Beanstandung gemäß Art. 16 Abs. 4 BayDSG konnte ich absehen, da die betroffene Kommune im Rahmen meines Tätigwerdens bereits von sich aus eine datenschutzkonforme Überarbeitung des Verfahrens angekündigt hat.

6 E-Government und öffentliche Register

6.1 Erneut: Transparenz bei der Beauftragung staatlicher Rechenzentren

Über das Gesetzgebungsvorhaben zu einem Gesetz über die Digitalisierung im Freistaat Bayern (Bayerisches Digitalgesetz – BayDiG) habe ich in der Vergangenheit bereits mehrfach und ausführlich berichtet (siehe meine Ausführungen im 31. Tätigkeitsbericht 2021 unter Nr. 6.1 und im 30. Tätigkeitsbericht 2020 unter Nr. 7.1). Im aktuellen Berichtszeitraum wurde das Bayerische Digitalgesetz verkündet[57] und trat größtenteils auch in Kraft.

An dieser Stelle möchte ich speziell an meine Ausführungen im 30. Tätigkeitsbericht 2020 unter Nr. 7.1.3 zu der aus datenschutzrechtlicher Sicht notwendigen Transparenz bei der Beauftragung staatlicher Rechenzentren anknüpfen und über meine Beteiligung an der Erarbeitung des Entwurfs für eine Bekanntmachung der Staatsregierung über Allgemeine Nutzungsbedingungen zur datenschutzrechtlichen Auftragsverarbeitung durch staatliche Stellen für öffentliche Stellen (Allgemeine Nutzungsbedingungen Auftragsverarbeitungsverhältnis – ANB-AVV)[58] berichten.

Kurz rekapituliert geht es im Wesentlichen um Folgendes: Mit voranschreitender Digitalisierung der bayerischen Verwaltung wächst insbesondere das Interesse kleinerer Behörden und Kommunen, ihre IT-Verfahren zentral in einem staatlichen Rechenzentrum betreiben zu lassen. Derartige Sachverhalte stellen in datenschutzrechtlicher Hinsicht regelmäßig Auftragsverarbeitungen gemäß Art. 28 DSGVO dar. Zur Begründung eines wirksamen Auftragsverarbeitungsverhältnisses bestimmt Art. 28 Abs. 3 Satz 1 DSGVO:

„Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind.“

Auf diese Regelung nimmt Art. 38 BayDiG Bezug.

Art. 38 BayDiG
Auftragsverarbeitung durch staatliche Stellen
(1) [1]Unabhängig vom Anwendungsbereich dieses Gesetzes erfolgt die datenschutzrechtliche Auftragsverarbeitung durch staatliche Stellen für öffentliche Stellen auf Grundlage eines Vertrages im Sinne des Art. 28 Abs. 3 Satz 1 Alternative 1 DSGVO oder § 62 Abs. 5 Satz 1 Alternative 1 des Bundesdatenschutzgesetzes und mit dem Vertragsinhalt, wie er nach Maßgabe dieses Artikels bestimmt wird, wenn und soweit die Auftragsverarbeitung nicht anderweitig gesetzlich geregelt ist. [2]Zur Begründung

[57] Gesetz über die Digitalisierung im Freistaat Bayern (Bayerisches Digitalgesetz – BayDiG) vom 22. Juli 2022 (GVBl. S. 374).
[58] Zum Zeitpunkt der Erstellung dieses Berichts noch nicht veröffentlicht.

eines Auftragsverarbeitungsverhältnisses durch Vertrag teilt der Verantwortliche dem Auftragsverarbeiter in Textform mit:

1. Gegenstand und Dauer der Verarbeitung,
2. Art und Zweck der Verarbeitung,
3. die Art der personenbezogenen Daten und
4. die Kategorien betroffener Personen.

(2) [1]Bereits bestehende Auftragsverarbeitungsverhältnisse im Sinne des Abs. 1 Satz 1 werden zum Ablauf des dritten auf das Inkrafttreten des Gesetzes folgenden Kalenderjahres ungültig, soweit nicht rechtzeitig vor diesem Zeitpunkt der Verantwortliche oder der Auftragsverarbeiter ein bestehendes Auftragsverarbeitungsverhältnis in Textform bestätigt und der jeweils andere Vertragspartner zustimmt. [2]Die allgemeinen Nutzungsbedingungen zur datenschutzrechtlichen Auftragsverarbeitung werden in der jeweils geltenden Fassung, die durch Bekanntmachung der Staatsregierung im Bayerischen Ministerialblatt festgelegt werden, Bestandteil des Vertrages im Sinne des Abs. 1 Satz 1, soweit Verantwortlicher und Auftragsverarbeiter nicht eine abweichende individualvertragliche Vereinbarung treffen. [3]Die allgemeinen Nutzungsbedingungen zur datenschutzrechtlichen Auftragsverarbeitung können auch Regelungen zur Begründung von weiteren Auftragsverarbeitungsverhältnissen enthalten.

In § 38 Abs. 1 Satz 1 BayDiG wird klargestellt, dass die datenschutzrechtliche Auftragsverarbeitung durch staatliche Stellen für öffentliche Stellen grundsätzlich **auf vertraglicher Basis** erfolgt, während in § 38 Abs. 2 Satz 2 BayDiG der **Einbezug allgemeiner Nutzungsbedingungen** in dieses Vertragsverhältnis zugelassen wird.

Funktionsweise und Wirkung dieser allgemeinen Nutzungsbedingungen **entsprechen** nach meinem Verständnis den aus dem Privatrecht bekannten sogenannten **Allgemeinen Geschäftsbedingungen** und können wesentlich zur gewünschten Standardisierung und schnelleren Abwicklung derartiger Auftragsverarbeitungen beitragen. An der Ausarbeitung des Entwurfs der Allgemeinen Nutzungsbedingungen Auftragsverarbeitungsverhältnis beteiligte ich mich daher intensiv. Aus datenschutzrechtlicher Sicht waren mir im Rahmen meiner Beteiligung insbesondere folgende Punkte wichtig:

6.1.1 Wirksamer Vertrag über Auftragsverarbeitung erforderlich

Zur grundsätzlichen Einordnung der Allgemeinen Nutzungsbedingungen Auftragsverarbeitungsverhältnis verdeutlichte ich, dass das Auftragsverarbeitungsverhältnis gemäß Art. 38 Abs. 1 Satz 1 BayDiG – trotz eines mir gegenüber vorgebrachten dringenden Bedürfnisses nach möglichst weitgehender Standardisierung und Beschleunigung – durch einen von beiden Stellen abzuschließenden Vertrag zustande kommen soll. Damit sind zwei übereinstimmende Willenserklärungen in Gestalt von Angebot und Annahme erforderlich, welche die für die Vertragsart typischen wesentlichen Bestimmungen enthalten müssen. Zwar können insoweit auch vorformulierte Vertragsbedingungen zum Einsatz kommen, so dass nicht alles zum Gegenstand individualvertraglicher Regelungen gemacht werden muss. Jedoch sind die in **Art. 38 Abs. 1 Satz 2 BayDiG bezeichneten Inhalte**, welche wesentliche Bestandteile des Vertrages im Sinne von Art. 28 Abs. 3 Satz 1 DSGVO konkretisieren, nach meinem Verständnis **zwingender Gegenstand individualvertraglicher Regelungen**.

Konkret kann die in Art. 38 Abs. 1 Satz 2 BayDiG vorgesehene Mitteilung der Kernpunkte der vorgesehenen – möglichst standardisierten – Auftragsverarbeitung durch den Verantwortlichen nur das Angebot sein, entsprechende Leistungen in Anspruch

nehmen zu wollen. Dieses Angebot bedarf dann aber noch der rechtlich bindenden Annahme durch den Auftragsverarbeiter – insbesondere im Rahmen der vorhandenen Kapazitäten – etwa in Form einer Bestätigung, um dadurch einen Auftragsverarbeitungsvertrag zu begründen. Damit die –Allgemeinen Nutzungsbedingungen Auftragsverarbeitungsverhältnis Bestandteil des Auftragsverarbeitungsverhältnisses werden, müssen diese wirksam in den Vertrag einbezogen werden. **Deren Veröffentlichung im Amtsblatt soll zwar insoweit ihre Einbeziehung in das Vertragsverhältnis erleichtern, macht aber nicht die zum Abschluss eines wirksamen Auftragsverarbeitungsvertrages erforderliche Annahme eines vorherigen Angebots obsolet.** Hinzu kommt, dass die allgemeinen Nutzungsbedingungen nach Art. 38 Abs. 2 Satz 2 Halbsatz 2 BayDiG nur dann und insoweit gelten, als Verantwortlicher und Auftragsverarbeiter nicht eine abweichende individualvertragliche Vereinbarung treffen.

6.1.2 Beachtung der „Rollenverteilung“ nach der Datenschutz-Grundverordnung

Im Hinblick auf die „Machtverhältnisse“ der Vertragsparteien war mir wichtig, dass die in Art. 28 DSGVO ausdifferenziert festgelegte Rollenverteilung zwischen Verantwortlichen und Auftragsverarbeitern auch in den Allgemeinen Nutzungsbedingungen Auftragsverarbeitungsverhältnis abgebildet ist. Immer wieder habe ich daher im Rahmen meiner Beteiligung bei der Erarbeitung der Allgemeinen Nutzungsbedingungen Auftragsverarbeitungsverhältnis den Blick auf das mit mir abgestimmte vom Bayerischen Staatsministerium des Innern, für Sport und Integration veröffentlichte Muster einer Vereinbarung zur Auftragsverarbeitung[59] gelenkt. Beabsichtigte Abweichungen von diesem die Vorgaben des Art. 28 DSGVO datenschutzkonform und praxistauglich umsetzenden Muster habe ich mir detailliert erläutern lassen. Hierdurch ist es beispielsweise gelungen, die gegenseitigen Informationspflichten der Vertragsparteien auszutarieren und eine nach den ersten Entwürfen der Allgemeinen Nutzungsbedingungen Auftragsverarbeitungsverhältnis zunächst einseitig beim Verantwortlichen liegende Informationslast durch Aufnahme gleichwertiger Informationspflichten des Auftragsverarbeiters zu kompensieren. Beispielsweise sehen die Allgemeinen Nutzungsbedingungen Auftragsverarbeitungsverhältnis nun neben der Mitteilungspflicht des Verantwortlichen hinsichtlich der Kontaktdaten der Ansprechpartner auch eine Pflicht des Auftragsverarbeiters vor, dem Verantwortlichen nicht nur die oder den eigenen Datenschutzbeauftragten namhaft zu machen, sondern auch Ansprechpartner für im Rahmen der Auftragsverarbeitung etwa veranlasste Weisungen. Im Falle der Feststellung von Unregelmäßigkeiten im Rahmen der Auftragsverarbeitung sehen die Allgemeinen Nutzungsbedingungen Auftragsverarbeitungsverhältnis nun beide Vertragsparteien in der Pflicht, die jeweils andere Vertragspartei darüber zu informieren.

6.1.3 Bestimmtheit der Verarbeitungsdauer

Bei der Ausgestaltung von Auftragsverarbeitungsverhältnissen muss auch die Dauer der Verarbeitung zweifelsfrei festgelegt werden. Der Verantwortliche muss feststellen können, ob der Auftrag im vorgegebenen Zeitrahmen bleibt. Bei einem unbefristeten Auftragsverarbeitungsverhältnis ist insoweit ein ordentliches Kündigungsrecht vorzu-

[59] Bayerisches Staatsministerium des Innern, für Sport und Integration, Datenschutzreform-Arbeitshilfen, Stand 3/2022, Internet: https://www.stmi.bayern.de/sus/datensicherheit/datenschutz/reform_arbeitshilfen.

sehen. Bei schwerwiegenden Verstößen des Auftragsverarbeiters muss es dem Verantwortlichen aber auch möglich sein, sich vorzeitig vom Vertrag lösen zu können (außerordentliches Kündigungsrecht).

Bei der Erarbeitung der Allgemeinen Nutzungsbedingungen Auftragsverarbeitungsverhältnis waren insofern praxisgerechte und datenschutzkonforme Regelungen für die vielfältigen Möglichkeiten einer Auftragsverarbeitung durch staatliche Rechenzentren zu finden. Dabei war auch das Verhältnis zu dem Hauptvertrag in den Blick zu nehmen, welcher der – mittels der Auftragsverarbeitung geregelten – Datenverarbeitung regelmäßig zu Grunde liegen wird. Konkret ist insoweit beispielsweise vorgesehen, dass im Falle eines befristeten Dienstleistungsvertrags (Hauptvertrag) automatisch auch der Vertrag zur Auftragsverarbeitung entsprechend befristet ist, was einen grundsätzlichen zeitlichen Gleichlauf beider Verträge sicherstellt. Auch die Regelung des ordentlichen Kündigungsrechts orientiert sich an der Regelung des Hauptvertrages. Nur wenn der Hauptvertrag keine Regelung hierzu enthält, ist ein isoliertes ordentliches Kündigungsrecht für den Auftragsverarbeitungsvertrag vorgesehen. Geregelt ist daneben auch die Möglichkeit einer außerordentlichen Kündigung. Grenzen bei der Ausübung eines derartigen Kündigungsrechts können sich im Einzelfall aus der in Art. 3 Abs. 1 BayDSG niedergelegten datenschutzrechtlichen Sicherstellungspflicht – insbesondere von obersten staatlichen Dienststellen für ihren jeweiligen nachgeordneten Bereich – ergeben.

6.2 Melderegisterauskunft durch die Meldebehörde: zulässig nur aus dem örtlichem Melderegister

Zu Abfragen von Meldedaten im Bayerischen Behördeninformationssystem (BayBIS) habe ich mich bereits mehrfach geäußert (zu nicht dienstlich veranlassten Abfragen siehe zuletzt meinen 30. Tätigkeitsbericht 2020 unter Nr. 7.6 sowie meinen 28. Tätigkeitsbericht 2018 unter Nr. 7.1). Anlässlich einer an mich gerichteten Bürgereingabe war ich im Berichtszeitraum erneut mit derartigen Meldedatenabfragen, konkret mit einer **unzulässigerweise auf eine BayBIS-Abfrage gestützten Melderegisterauskunft** durch eine Meldebehörde befasst. Der an mich gerichteten Eingabe lag die Anfrage eines Rechtsanwalts bei einer Meldebehörde zu den Adressdaten eines namentlich benannten Bürgers zugrunde. Da die betreffende Person jedoch nie im Zuständigkeitsbereich der Meldebehörde gewohnt hatte, waren keine Daten im örtlichen Melderegister vorhanden. Daher holte die Meldebehörde die Adressdaten über eine BayBIS-Personenauskunft bei der Anstalt für kommunale Datenverarbeitung in Bayern (AKDB) ein und teilte sie dem Rechtsanwalt mit. Dagegen hat sich der von der Datenabfrage betroffene Bürger zu Recht bei mir beschwert.

6.2.1 Unterschied örtliches Melderegister und zentraler Meldedatenbestand

Die Gemeinden führen als **Meldebehörden** nach § 1 Bundesmeldegesetz (BMG) in Verbindung mit Art. 1 Abs. 1 Satz 1 Bayerisches Gesetz zur Ausführung des Bundesmeldegesetzes (BayAGBMG) ein **örtliches Melderegister** (§ 2 Abs. 2 BMG), in welchem der in § 3 BMG aufgelistete umfangreiche Datenkatalog wie etwa Name, Geschlecht, Staatsangehörigkeit, Anschrift, Familienstand oder die Seriennummern von Ausweisdokumenten der im Gebiet der jeweiligen Gemeinde meldepflichtigen Personen gespeichert werden.

§ 2 BMG
Aufgaben und Befugnisse der Meldebehörden
(1) Die Meldebehörden haben die in ihrem Zuständigkeitsbereich wohnhaften Personen (Einwohner) zu registrieren, um deren Identität und deren Wohnungen feststellen und nachweisen zu können.
(2) Die Meldebehörden führen zur Erfüllung ihrer Aufgaben Melderegister. Diese enthalten Daten, die bei der betroffenen Person erhoben, von öffentlichen Stellen übermittelt oder sonst amtlich bekannt werden.
[…]

Art. 1 BayAGBMG
Meldebehörden
(1) [1]Meldebehörden sind die Gemeinden. […]
(2) [1]Örtlich zuständig ist
1. im Fall des § 50 Abs. 1 des Bundesmeldegesetzes (BMG) die Meldebehörde des aktuellen Hauptwohnsitzes der betroffenen Person,
2. für Melderegisterauskünfte im Übrigen und für Datenübermittlungen an öffentliche Stellen aus dem Melderegister jede Meldebehörde, bei der der Betroffene gemeldet ist oder war,
3. im Übrigen die Meldebehörde, bei der ein meldepflichtiger Vorgang stattfindet.
[…]

Davon zu unterscheiden ist der bei der **AKDB** geschaffene **zentrale Meldedatenbestand** für die bayerischen Meldebehörden (Art. 7 Abs. 2 BayAGBMG), der aus dem täglich aktualisierten örtlichen Bestand gespeist wird (vgl. Art. 7 Abs. 1 BayAGBMG). Insoweit datenschutzrechtlich Verantwortlicher ist gemäß Art. 4 Nr. 7 DSGVO die AKDB. Auf diesem Datenbestand aufbauend betreibt die AKDB zum einen das Bayerische Behördeninformationssystem **(BayBIS)**, über welches öffentliche Stellen Meldedaten auf Grundlage des § 5 Abs. 1 Verordnung zur Übermittlung von Meldedaten (Meldedatenverordnung – MeldDV) abrufen können.

Art. 7 BayAGBMG
Zentraler Meldedatenbestand
(1) Die Meldebehörden übermitteln tagesaktuell die Daten ihrer Einwohner nach § 3 Abs. 1 BMG, bezüglich § 3 Abs. 1 Nr. 17 BMG ohne Sperrkennwort und Sperrsumme, und nach § 3 Abs. 2 Nr. 1 und 4 bis 11 BMG sowie Änderungen dieser Daten an die AKDB.
(2) [1]Die AKDB hat den nach Abs. 1 geschaffenen zentralen Meldedatenbestand zu speichern und darf ihn im Übrigen nur nach Maßgabe gesonderter Vorschriften verarbeiten. [2]Die AKDB ist hierbei Verantwortliche im Sinne des Kapitels IV der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung –DSGVO).
[…]

§ 5 MeldDV
Automatisierte Behördenauskunft
(1) Soweit es zur Erfüllung ihrer Aufgaben erforderlich ist, können öffentliche Stellen aus dem nach Art. 7 Abs. 1 BayAGBMG geschaffenen zentralen Meldedatenbestand
1. bei einer Personensuche vorbehaltlich abweichender Bestimmungen in dieser Verordnung die in § 5 Abs. 1 Satz 1 BMeldDAV und
2. bei einer freien Suche die in § 8 Abs. 1 Satz 1 BMeldDAV aufgezählten Daten automatisiert abrufen.
[…]

Zum anderen stellt die AKDB gemäß Art. 9 Abs. 1 Satz 1 BayAGBMG ein **Portal zur Verfügung**, über welches Auskunftssuchende aus dem zentralen Meldedatenbestand insbesondere einfache Melderegisterauskünfte (dazu näher sogleich) einholen können.[60]

Art. 9 BayAGBMG
Portal
(1) [1]Die AKDB kann aus dem nach Art. 7 geschaffenen Datenbestand ein Portal betreiben, aus dem automatisiert einfache Melderegisterauskünfte nach § 49 BMG und Datenbestätigungen nach § 49a BMG erteilt werden.
[…]

6.2.2 Unterschied einfache und erweiterte Melderegisterauskunft

§ 44 Abs. 1 BMG ermöglicht es einer Person, über eine andere Person Auskunft hinsichtlich der in dieser Norm enumerativ aufgezählten Grunddaten zu erhalten (**einfache Melderegisterauskunft**). Zu diesen Grunddaten zählen auch die derzeitigen Anschriften. Voraussetzung für die Auskunftserteilung ist insbesondere, dass gemäß § 44 Abs. 3 BMG die Identität der Person, deren Grunddaten begehrt werden, auf Grund der in der Anfrage mitgeteilten Angaben eindeutig festgestellt werden kann. Die Darlegung eines berechtigten Interesses ist für die Auskunft nicht erforderlich.

§ 44 BMG
Einfache Melderegisterauskunft
(1) [1]Wenn eine Person zu einer anderen Person oder wenn eine andere als die in § 34 Absatz 1 Satz 1 oder § 35 bezeichnete Stelle Auskunft verlangt, darf die Meldebehörde nur Auskunft über folgende Daten einzelner bestimmter Personen erteilen (einfache Melderegisterauskunft):
1. Familienname,
2. Vornamen unter Kennzeichnung des gebräuchlichen Vornamens,
3. Doktorgrad und
4. derzeitige Anschriften sowie,
5. sofern die Person verstorben ist, diese Tatsache.
[2]Sofern die Daten für gewerbliche Zwecke verwendet werden, sind diese anzugeben.
[…]
(3) Die Erteilung einer einfachen Melderegisterauskunft ist nur zulässig, wenn
1. die Identität der Person, über die eine Auskunft begehrt wird, eindeutig festgestellt werden kann auf Grund der in der Anfrage mitgeteilten Angaben über
a) den Familiennamen,
b) den früheren Namen,
c) die Vornamen,
d) das Geburtsdatum,
e) das Geschlecht oder
f) eine Anschrift und
2. die Daten nicht für Zwecke der Werbung oder des Adresshandels verwendet werden und die Auskunft verlangende Person oder Stelle dies erklärt.

Im Wege einer **erweiterten Melderegisterauskunft** nach **§ 45 Abs. 1 BMG** dürfen bei Vorliegen eines berechtigten Interesses zusätzliche Daten, wie beispielsweise

[60] Melderegisterauskunft mit BayernID – Bürgerauskunft (zentrales Portal), Internet: https://www.buergerserviceportal.de/bayern/service/bspx_bayern_buergerauskunft, dort auch nähere Informationen zur Kostenberechnung.

frühere Anschriften oder Name und Anschrift des Ehegatten oder Lebenspartners, beauskunftet werden.

§ 45 BMG
Erweiterte Melderegisterauskunft
(1) Soweit ein berechtigtes Interesse glaubhaft gemacht wird, darf zu den in § 44 Absatz 1 genannten Daten einzelner bestimmter Personen eine erweiterte Melderegisterauskunft erteilt werden über
1. frühere Namen,
2. Geburtsdatum und Geburtsort sowie bei Geburt im Ausland auch den Staat,
3. Familienstand, beschränkt auf die Angabe, ob verheiratet oder eine Lebenspartnerschaft führend oder nicht,
4. derzeitige Staatsangehörigkeiten,
5. frühere Anschriften,
6. Einzugsdatum und Auszugsdatum,
7. Familienname und Vornamen sowie Anschrift des gesetzlichen Vertreters,
8. Familienname und Vornamen sowie Anschrift des Ehegatten oder des Lebenspartners sowie
9. Sterbedatum und Sterbeort sowie bei Versterben im Ausland auch den Staat.
[…]

Für die **Erfüllung der Informationspflichten** nach Art. 14 DSGVO ist der Empfänger verantwortlich. Über Art. 14 Abs. 5 DSGVO hinaus sieht § 45 Abs. 2 BMG eine zusätzliche Beschränkung vor; die auf Art. 23 Abs. 1 Buchst. i und j DSGVO gestützte nationale Regelung gilt entsprechend auch für die einfache Melderegisterauskunft (§ 44 Abs. 5 BMG).

6.2.3 Auskunft über bei der Meldebehörde nie gemeldete Personen ist keine öffentliche Aufgabe

Wird ein Antrag auf Melderegisterauskunft bei einer Meldebehörde gestellt, bei der die Person, über die Auskunft begehrt wird, nie gemeldet war, kann und darf keine Auskunft erteilt werden. Vielmehr darf die Meldebehörde eine **Melderegisterauskunft nur aus dem örtlichen Melderegister erteilen**. In diesem liegen die begehrten Daten aber in einem solchen Fall nicht vor. Die Meldebehörde ist auch nicht befugt, sich die begehrten Daten im zentralen Meldedatenbestand der AKDB mittels einer BayBIS-Recherche oder durch Nachfrage bei einer anderen Meldebehörde zu beschaffen. Sowohl § 5 Abs. 1 MeldDV als auch § 34 Abs. 1 Satz 1, Abs. 2 Satz 1 Nr. 1 BMG in Verbindung mit § 34a Abs. 1 BMG sehen nämlich als Voraussetzung für einen Datenabruf durch eine Behörde vor, dass dieser **zur Erfüllung ihrer öffentlichen Aufgaben erforderlich** ist. Daran fehlt es jedoch, denn gemäß Art. 1 Abs. 2 Satz 1 Nr. 2 BayAGBMG ist für eine derartige Melderegisterauskunft **nur die Meldebehörde örtlich zuständig, bei welcher die oder der Betroffene gemeldet ist oder war.**

War die Person, über die Auskunft begehrt wird, nie in der angefragten Gemeinde gemeldet, gehört die Beauskunftung über diese Person folglich nicht zu den öffentlichen Aufgaben der Gemeinde und der Datenabruf über BayBIS ist daher nicht erforderlich. Selbst wenn die Person früher in der Gemeinde gewohnt hat, darf die Meldebehörde die neue Adresse ebenfalls nicht im zentralen Datenbestand recherchieren, da die **Erteilung der Melderegisterauskunft nur aus dem örtlichen Melderegister erfolgt** und darauf die öffentliche Aufgabe beschränkt ist.

6.3 Ausländerzentralregister: unzulässiger automatisierter Abruf durch Meldebehörde

Eine nach der Verlagerung einer Einrichtung des Zentrums für Ankunft, Entscheidung, Rückführung (AnkER-Einrichtung) melderechtlich für die dort untergebrachten Asylbewerbenden zuständige Gemeinde sah sich wegen häufiger Unklarheiten etwa bei Geburtsdaten oder Namensschreibweisen sowie dem Problem von Alias-Identitäten mit einem erheblichen Mehraufwand in der melderechtlichen Sachbearbeitung konfrontiert. Um die Bearbeitung zu vereinfachen, stellte die Gemeinde beim Bundesverwaltungsamt einen **Antrag** auf Zulassung zum **automatisierten Datenabruf aus dem Ausländerzentralregister**. Begründet wurde dieser Antrag mit dem Bestehen der AnkER-Einrichtung auf dem Gemeindegebiet sowie insbesondere der Aufgabe der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung, wobei die Gemeinde klarstellte, dass die Aufnahmeeinrichtung keine kommunale, sondern eine staatliche Einrichtung ist.

In der Folge wurde die Gemeinde zum automatisierten Datenabruf aus dem AZR zur alleinigen Nutzung durch das AnkER-Zentrum – im Sinne einer Dienststelle innerhalb der Gemeinde – zugelassen, obwohl die Gemeinde nicht zu dem Kreis der in § 22 Abs. 1 Gesetz über das Ausländerzentralregister (AZRG) genannten öffentlichen Stellten gehört, welche zum Abruf im automatisierten Verfahren zugelassen werden können. Die Zugriffsmöglichkeit wurde in der Folge durch die Gemeinde genutzt, um mangelhafte Meldedatensätze durch Auskünfte aus dem AZR zu korrigieren, wobei als Zugriffsgrund jeweils „ausländerrechtliche Aufgaben“ vermerkt wurde. Im Rahmen einer Überprüfung hat das Bundesverwaltungsamt den Fehler bemerkt und die Zulassung zum automatisierten Abruf zurückgenommen. Datenschutzrechtlich habe ich den Fall wie folgt bewertet:

6.3.1 Fehlende Befugnis zum automatisierten Datenabruf aus dem AZR

Mit dem Abruf der im AZR gespeicherten Informationen hat die Gemeinde personenbezogene Daten der hiervon Betroffenen verarbeitet (vgl. Art. 4 Nr. 1 und Nr. 2 DSGVO). Öffentliche Stellen benötigen für jede Verarbeitung personenbezogener Daten eine Rechtsgrundlage (vgl. Art. 6 Abs. 1 UAbs. 1 DSGVO). Dabei sollen sie sich bei der Erfüllung ihrer öffentlichen Aufgaben grundsätzlich auf die speziellen fachgesetzlichen Befugnisse zur Verarbeitung personenbezogener Daten bzw. auf die allgemeine Befugnisnorm des Art. 4 Abs. 1 BayDSG stützen (vgl. Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO).

Eine **bereichsspezifische Befugnisnorm**, welche der Gemeinde den **direkten Zugriff** auf die im AZR gespeicherten Datensätze erlauben würde, **enthalten weder das Gesetz über das Ausländerzentralregister noch das Bundesmeldegesetz.** Hierbei handelt es sich um eine **bewusste Entscheidung des Gesetzgebers** mit der Folge, dass sich die Gemeinde beim automatisierten Abruf auch **nicht** auf die **allgemeine Befugnisnorm Art. 4 Abs. 1 BayDSG** stützen konnte. § 22 Abs. 1 Satz 1 AZRG zählt vielmehr enumerativ und abschließend die Behörden und öffentlichen Stellen auf, welche zum Datenabruf im automatisierten Verfahren zugelassen werden können. Da eine Gemeinde nicht hierzu zählt, stellte formal betrachtet **jeder automatisierte Abruf einen Datenschutzverstoß** dar.

6.3.2 Datenverarbeitung als solche aber materiell-rechtlich zulässig

Bei der datenschutzrechtlichen Bewertung habe ich aber auch berücksichtigt, dass materiell-rechtlich eine Verarbeitung der abgefragten Daten durch die Gemeinde durchaus vorgenommen werden durfte. Letztlich war **nur** die **Art und Weise der Datenerlangung**, nämlich der Abruf im automatisierten Verfahren, **fehlerhaft.**

Aufgabe der Meldebehörde ist nach § 2 Bundesmeldegesetz (BMG) insbesondere die Registrierung der in ihrem Zuständigkeitsgebiet wohnhaften Personen, das Führen eines Melderegisters und die Mitwirkung bei der Durchführung von öffentlichen Aufgaben anderer öffentlicher Stellen. Bei Personen, die einen Asylantrag gestellt haben, ist sie als Daten an die Registerbehörde übermittelnde Stelle im Sinne einer Datenpflege berechtigt und verpflichtet, die von ihr übermittelten Daten auf Richtigkeit und Aktualität zu überprüfen, soweit dazu Anlass besteht (§ 8 Abs. 3 Satz 1 in Verbindung mit § 6 Abs. 1 Nr. 9 AZRG). Nach § 18e Abs. 1 Satz 1 AZRG werden in **Asylangelegenheiten** und Fällen unerlaubter Einreise oder Aufenthalten neben den **Grundpersonalien** die AZR-Nummer (zum Zweck der eindeutigen Zuordnung), die Anschrift im Bundesgebiet sowie Übermittlungssperren in einem automatisierten Verfahren **an die zuständige Meldebehörde** zur Erfüllung ihrer Aufgaben unverzüglich nach der Unterbringung in einer Aufnahmeeinrichtung **übermittelt**. Diese Grundpersonalien werden in § 3 Abs. 1 Nr. 4 AZRG definiert und setzen sich aus dem Familiennamen, dem Geburtsnamen, den Vornamen, der Schreibweise der Namen nach deutschem Recht, dem Geburtsdatum, Ort, Land und Bezirk der Geburt, dem Geschlecht sowie den Staatsangehörigkeiten zusammen. Außerdem werden Änderungen dieser Daten übermittelt, § 18e Abs. 1 Satz 2 AZRG. Melderechtlich kann nach § 23 Abs. 5 BMG die Anmeldung von Personen, die in eine Aufnahmeeinrichtung zugezogen sind, automatisiert durch Übernahme der Daten aus dem AZR nach § 18e AZRG erfolgen. **Über die Grundpersonalien hinausgehende Daten** – wie Angaben zum Zuzug oder Fortzug nach § 3 Abs. 1 Nr. 6 AZRG – **können der Meldebehörde** im Wege eines Übermittlungsersuchens **übermittelt werden**, soweit die Kenntnis dieser Daten zur Erfüllung ihrer Aufgaben erforderlich ist, § 10 Abs. 1 Satz 1 AZRG. § 10 Abs. 5 AZRG stellt daneben klar, dass zur Datenpflege im Sinne des § 8 Abs. 3 AZRG die zu überprüfenden Daten an die dazu berechtigte oder verpflichtete Stelle grundsätzlich übermittelt werden.

Gegenüber der Gemeinde sah ich mich zur **Feststellung eines Datenschutzverstoßes** veranlasst. Insoweit konnte sich die Gemeinde nicht auf einen entschuldigenden Vertrauenstatbestand in Gestalt der Zulassung zum automatisierten Datenabruf durch das Bundesverwaltungsamt berufen. Neben dem Umstand, dass es für die Feststellung eines Datenschutzverstoßes von vornherein nicht auf eine etwaige Bösgläubigkeit der öffentlichen Stelle ankommt, machte sie bei der jeweiligen Abfrage auch mit der Angabe von „ausländerrechtlichen Aufgaben“ als Auskunftszweck für ihre Aufgabenerfüllung aus dem Melderecht unrichtige Angaben und trug dazu bei, dass der unrechtmäßige Zustand, nämlich der Zugang zum automatisierten Verfahren zu melderechtlichen Zwecken, aufrechterhalten blieb.

6.4 Schengener Informationssystem, Visa-Informationssystem und Eurodac: datenschutzrechtliche Prüfung des Einsatzes

Die Bedeutung der Nutzung gerade auch von grenzüberschreitenden Informationssystemen nimmt stetig zu. Exemplarisch zu nennen sind hier der Einsatz des Schengener Informationssystems, des Visa-Informationssystems und des Eurodac. Kurz zusammengefasst geht es um Folgendes:

Das Schengener Informationssystem (SIS II) ist ein Großinformationssystem, das die Zusammenarbeit zwischen den nationalen Grenzschutz-, Zoll- und Polizeibehörden des Schengen-Raums vereinfacht. Das SIS II ermöglicht es den zuständigen Behörden der Schengener Mitgliedsstaaten, Ausschreibungen zu Personen oder Gegenständen vorzunehmen. Die Gründe für eine Ausschreibung umfassen etwa Einreiseverweigerungen von Personen, die den Schengen-Raum nicht betreten oder sich in diesem nicht aufhalten dürfen, Fahndungen nach Personen, die mittels Europäischem Haftbefehl gesucht werden, die Suche nach vermissten Personen oder die Fahndung nach verlorenen oder gestohlenen Gegenständen, wie etwa Reisepässe oder Autos.

Das Visa-Informationssystem (VIS) ist ein System für den Austausch von Visa-Daten zwischen den Schengen-Staaten.

Mit dem europäischen System Eurodac werden Fingerabdrücke von Asylbewerbern und Geflüchteten europaweit erhoben, zentral gespeichert (sog. Zentraleinheit) und abgeglichen.

Bereits in der Vergangenheit beschäftigte ich mich wiederholt und unter verschiedenen Blickwinkeln mit Datenverarbeitungen durch bayerische öffentliche Stellen im Schengener Informationssystem. Ich verweise hierzu insbesondere auf meine Ausführungen im 19. Tätigkeitsbericht 2000 unter Nr. 10.1, im 21. Tätigkeitsbericht 2004 unter Nr. 13.1 und im 25. Tätigkeitsbericht 2012 unter Nr. 12.2. In meiner datenschutzrechtlichen Praxis zu beurteilen war insoweit anhand konkreter Beschwerden insbesondere die Zulässigkeit einer Speicherung und Verlängerung von Ausschreibungen im Schengener Informationssystem durch bayerische Ausländerbehörden. Im Berichtszeitraum weitete ich jedoch angesichts der großen Tragweite der Datenverarbeitungen und der insoweit teilweise bestehenden Pflichten zur regelmäßigen Prüfung [61] den Fokus aus und überprüfte anlassunabhängig die Datenverarbeitung

[61] Hinsichtlich des SIS II nach Art. 44 Abs. 2 Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) (ABl. L 381 vom 28. Dezember 2006, S. 4) in Verbindung mit Art. 60 Abs. 1 Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) (ABl. L205 vom 7. August 2007, S. 63) bzw. nunmehr Art. 55 Abs. 2 Verordnung (EU) 2018/1861 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der Grenzkontrollen, zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen und zur Änderung und Aufhebung der Verordnung (EG) Nr. 1987/2006 bzw. Art. 69 Abs. 2 Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung und Aufhebung des Beschlusses 2007/533/JI des Rates und zur Aufhebung der Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates und des Beschlusses 2010/261/EU der Kommission bzw. Art. 19 Verordnung (EU) 2018/1860 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Nutzung des Schengener Informationssystems für die Rückkehr illegal aufhältiger Drittstaatsangehöriger und hinsichtlich des VIS nach Art. 41 Abs. 1 VO Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (ABl. L 218 vom 13. August 2008, S. 60) in Verbindung mit Art. 8 Abs. 5 und 6 Beschluss 2008/633/JI des Rates zur Reform des Visa-Informationssystems (ABl. L 248 vom 13. Juli 2021, S. 11) in Verbindung mit § 4 Abs. 1 Gesetz über den Zugang von Polizei- und Strafverfolgungsbehörden sowie Nachrichtendiensten zum Visa-Informationssystem.

einer zufällig ausgewählten bayerischen Kreisverwaltungsbehörde in Bezug auf die drei Informationssysteme generell.

Hierbei wandte ich mich an die betreffende Kreisverwaltungsbehörde und bat diese, mir die konkreten Rahmenbedingungen vor Ort zum Einsatz dieser Informationssysteme anhand eines von mir erstellten Fragebogens detailliert zu erläutern. Thema meiner Fragen war dabei unter anderem die konkrete technische Anbindung an die verschiedenen Systeme, die Vergabe von Zugriffsrechten, die Klärung von Anwendungsszenarien und die Schulung der zugriffsberechtigten Personen. Die Kreisverwaltungsbehörde hat legte mir daraufhin ausführlich dar, auf welche Art und Weise, in welchen Konstellationen und in welchem Umfang sie die entsprechenden Informationssysteme nutzt. Auf Grund der bayernweiten Bedeutung der Thematik und sich insbesondere auch durch die Erweiterung des Schengener Informationssystems (Einführung des SIS 3.0) ergebenden Neuerungen (wie beispielsweise den direkten schreibenden und lesenden Zugriff der Ausländerbehörden auf das Schengener Informationssystem) band ich auch das Bayerische Staatsministerium des Innern, für Sport und Integration ein. Insbesondere ließ ich mir die rechtlichen und technischen Rahmenbedingungen der Informationssysteme schildern und mir umfangreiche Unterlagen, vor allem zur Einführung des SIS 3.0, vorlegen. Diese enthielten unter anderem ausführliche Informationen zum Rechte- und Rollenkonzept des SIS 3.0.

Meine Prüfung ergab, dass bei der betreffenden Kreisverwaltungsbehörde im Umgang mit den oben genannten Informationssystemen keine grundlegenden Mängel festgestellt werden konnten. Ich forderte die Behörde jedoch auf, ein noch größeres Augenmerk als bisher auf – extern angebotene bzw. selbst durchzuführende – Schulungen, insbesondere zu den Themen Datensicherheit und Datenschutz bei der Nutzung der Informationssysteme, sowie auf die Eigenkontrolle zu legen. Ganz generell möchte ich die mit den genannten Informationssystemen arbeitenden Behörden dafür sensibilisieren, Maßnahmen zur Datensicherheit im Rahmen der Eigenkontrolle zu ergreifen. Auch sind die rechtlichen Vorgaben zur Belehrung über das Recht auf Information und das Recht auf Auskunft, Berichtigung unrichtiger Daten und Löschung unrechtmäßig gespeicherter Daten zu berücksichtigen. Schließlich muss auch darauf geachtet werden, die Zugriffsrechte der Mitarbeiterinnen und Mitarbeiter datenschutzkonform zu verteilen und diese entsprechend den tatsächlichen Aufgaben auf dem laufenden Stand zu halten.

Soweit veranlasst, werde ich in Zukunft erneut entsprechende Überprüfungen durchführen.

7 Soziales und Gesundheit

7.1 Nutzung von Gesundheits- und Patientendaten zu Forschungszwecken durch Universitätsklinika

Das novellierte Bayerische Universitätsklinikagesetz ist am 2. Januar 2023 in Kraft getreten. Hierzu hatte mich das Bayerische Staatsministerium für Wissenschaft und Kunst zwar im Vorfeld des Gesetzgebungsverfahrens einbezogen (siehe hierzu den Gesetzentwurf der Staatsregierung, mit Begründung, in der Landtags-Drucksache 18/24230). Umso irritierter war ich, dass meine deutliche Kritik an dem Gesetzentwurf im Wesentlichen keine Berücksichtigung fand.

7.1.1 Datenschutzrechtlicher Gegenstand des Gesetzes

Das zentrale datenschutzrechtliche Thema des Gesetzes ist die Einführung neuer Rechtsgrundlagen für die Verarbeitung von Patientendaten zu wissenschaftlichen Forschungszwecken durch die Universitätsklinika (Sekundärnutzung). Insbesondere wird im Hinblick auf die Übermittlung von Patientendaten an Dritte zu wissenschaftlichen Forschungszwecken (wie auch hinsichtlich der anschließenden Weiterverarbeitung) ein legislativer Sonderweg für die Universitätsklinika eingeschlagen. Bislang galt im Bereich der Sekundärnutzung von Patientendaten zu Forschungszwecken für alle Krankenhäuser gleichermaßen die Vorschrift des Art. 27 Bayerisches Krankenhausgesetz (BayKrG).

Für Krankenhäuser, die keine Universitätsklinika im Sinne des Bayerischen Universitätsklinikagesetzes sind, bleibt es derzeit unverändert bei der abschließenden Geltung des Art. 27 Abs. 5 BayKrG, der im Grundsatz (mangels anderweitiger erlaubender Rechtsvorschrift) die Einwilligung der betroffenen Person in die Übermittlung ihrer Patientendaten für wissenschaftliche Forschungszwecke an Dritte verlangt:

„(5) [1]Die Übermittlung von Patientendaten an Dritte ist insbesondere zulässig im Rahmen des Behandlungsverhältnisses oder dessen verwaltungsmäßiger Abwicklung oder wenn eine Rechtsvorschrift die Übermittlung erlaubt oder wenn die betroffenen Personen eingewilligt haben. [2]Eine Offenbarung von Patientendaten an Vor-, Mit- oder Nachbehandelnde ist zulässig, soweit das Einverständnis der Patienten anzunehmen ist.“

Für Universitätsklinika hingegen wurde erstmals eine gesetzliche Verarbeitungsbefugnis zu Forschungszwecken geschaffen, die – abweichend vom bisherigen Regelungsregime – unter gewissen Voraussetzungen einen Verzicht auf die Einwilligung der betroffenen Person zulässt.

7.1.2 Regulatorischer Rahmen im Einzelnen

Ausweislich der Gesetzesbegründung soll das Bayerische Universitätsklinikagesetz dem aktuellen Stand des bayerischen Hochschulrechts angepasst werden, insbesondere den Vorgaben des Bayerischen Hochschulinnovationsgesetzes, sowie verschiedenen politischen Herausforderungen für die Hochschulmedizin gerecht werden. Vor

diesem Hintergrund legt der Gesetzgeber ein besonderes Gewicht auf die Neufassung des Art. 12 Bayerisches Universitätsklinikagesetz (BayUniKlinG – „Zusammenarbeit mit der Universität"), indem er diese Rechtsnorm zu Beginn des Änderungsgesetzes herausgreift und gegenüber den übrigen Änderungen separat „vor die Klammer gezogen" thematisiert.

Diesbezüglich wies ich bereits im Rahmen meiner Beteiligung im Gesetzgebungsverfahren darauf hin, dass diese Vorschrift keine eigenständige Rechtsgrundlage im Sinne des Art. 6 Abs. 1 UAbs. 1 DSGVO enthält. Insbesondere sollte die Verarbeitung von Gesundheitsdaten, soweit sie im Rahmen der Zusammenarbeit des Universitätsklinikums mit der Universität erforderlich sein sollte, spezifisch in einer Rechtsverordnung des Wissenschaftsministeriums geregelt werden.

Darüber hinaus wurde geregelt, dass die Universitätsklinika „gemeinsame Einrichtungen, insbesondere Zentren für die Verarbeitung von Gesundheitsdaten und für die Übertragung von wissenschaftlichen Erkenntnissen in die Krankenversorgung" schaffen und mit ihnen kooperieren (Art. 13 Abs. 1 Satz 2 BayUniKlinG). Allerdings ist nicht eindeutig festgelegt, welche Aufgaben solche Zentren erfüllen sollen und wie die Kooperation der Universitätsklinika mit ihnen konkret auszusehen hat. Davon abgesehen begrüße ich es aber, dass zumindest in diesem Zusammenhang meine Anregung Berücksichtigung fand und in Art. 13 Abs. 2 Satz 1 BayUniKlinG eine Festlegung zur datenschutzrechtlichen Verantwortlichkeit der gemeinsamen Einrichtungen getroffen wurde.

Den datenschutzrechtlichen Schwerpunkt des Änderungsgesetzes bilden die neu gefassten Absätze 3 und 4 des Art. 16 BayUniKlinG. Sie lauten wie folgt:

„(3) [1]Personenbezogene Daten müssen im Rahmen eines Behandlungsverhältnisses bei dem oder der Behandelten von am Klinikum oder an der zugehörigen Universität tätigen Ärztinnen und Ärzten gemäß den Vorgaben des Bayerischen Krankenhausgesetzes verarbeitet werden. [2]Sie dürfen auch an andere Angehörige des wissenschaftlichen Personals des Klinikums oder der Universität, der das Klinikum im Sinne des Art. 19 Abs. 1 und des Art. 53 Abs. 1 BayHIG zugeordnet ist, übermittelt werden und von diesen auch zu eigenen Forschungszwecken verarbeitet werden, wenn

1. *die Daten ohne Personenbezug offengelegt werden und die identifizierenden Daten gesondert aufbewahrt und besonders geschützt werden,*
2. *im Falle, dass der Forschungszweck die Möglichkeit der Zuordnung erfordert, die betroffene Person eingewilligt hat oder*
3. *im Falle, dass weder auf die Zuordnungsmöglichkeit verzichtet noch die Einwilligung mit verhältnismäßigem Aufwand eingeholt werden kann, das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schützenswerten Interessen der betroffenen Person erheblich überwiegt und der Forschungszweck nicht auf andere Weise zu erreichen ist.*

[3]Die personenbezogenen Daten sind, soweit dies nach dem Forschungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert, zu anonymisieren oder, soweit eine Anonymisierung noch nicht möglich ist, zu pseudonymisieren. [4]Das Klinikum gewährleistet durch angemessene und spezifische Maßnahmen im Sinne des Art. 9 Abs. 2 Buchst. j DSGVO, dass die Daten auch, soweit sie noch nicht anonymisiert oder pseudonymisiert wurden, entsprechend der Datenschutz-Grundverordnung verarbeitet werden und dass dies auch nachträglich überprüfbar ist. [5]Die in den Art. 15, 16, 18 und 21 DSGVO vorgesehenen Rechte der Betroffenen sind insoweit beschränkt, als durch sie voraussichtlich die Verwirklichung der Forschungszwecke unmöglich gemacht oder ernsthaft beeinträchtigt

wird und die Beschränkung für die Forschungszwecke notwendig ist. 6 Art. 9 Abs. 3 DSGVO bleibt unberührt.
(4) [1]Für die Übermittlung von personenbezogenen Daten zu Zwecken der wissenschaftlichen Forschung zwischen verschiedenen Universitätsklinika und Universitäten sowie zwischen Universitätsklinika und sonstigen Dritten, die eine den Anforderungen der Datenschutz-Grundverordnung genügende Datenverarbeitung gewährleisten, gilt Abs. 3 entsprechend. [2]Eine Übermittlung personenbezogener Daten an private Dritte im Sinne des Satzes 1 in anderer als anonymisierter Form ist nur zulässig, wenn für das Forschungsvorhaben der oder des Dritten die Betroffenen in die Übermittlung eingewilligt haben und zuvor die oder der zuständige Datenschutzbeauftragte beteiligt wurde."

Darin sind für die Universitätsklinika als Verantwortliche neue Erlaubnistatbestände zur Verarbeitung von Patientendaten geschaffen worden. Aus Datenschutzsicht wird dabei ein grundlegender Paradigmenwechsel vollzogen: Während nach bisherigen Maßstäben (des für Universitätsklinika gemäß Art. 15 Abs. 2 BayUniKlinG entsprechend anwendbaren Art. 27 Abs. 5 BayKrG) die Übermittlung von personenbezogenen Gesundheitsdaten an Dritte zu wissenschaftlichen Forschungszwecken unterschiedslos die Einwilligung der betroffenen Person erforderte, erlaubt die Neufassung den Universitätsklinika als Verantwortlichen künftig eine Übermittlung an Dritte auch ohne vorherige Einwilligung der betroffenen Personen.

In Art. 16 Abs. 3 Satz 2 BayUniKlinG werden die drei Tatbestandsalternativen nach Nr. 1 bis Nr. 3 mit dem Wort „oder" verknüpft (siehe am Ende der Nr. 2). Daraus könnte gefolgert werden, dass neben den Voraussetzungen nach Nr. 1 keine weiteren Kriterien kumulativ hinzutreten müssen, also insbesondere nicht die Tatbestandsmerkmale gemäß Nr. 2 und Nr. 3 der Vorschrift. Im Ergebnis könnte dies bedeuten, dass allein die tatsächliche Pseudonymisierung – namentlich die Entfernung des Personenbezugs sowie die gesonderte Aufbewahrung verbunden mit einem besonderen Schutz der identifizierenden Daten – als Rechtsgrundlage für die Übermittlung und Weiterverarbeitung sensibler Patientendaten genügen soll. Dass lediglich die Pseudonymisierung von Daten ausreichen soll, um einen Erlaubnistatbestand hinsichtlich der Verarbeitung von sensiblen Gesundheitsdaten zu begründen, halte ich allerdings für problematisch. Denn die technisch-organisatorische Maßnahme der Pseudonymisierung reicht für sich genommen nicht aus, um die übergeordneten Vorgaben nach Art. 9 Abs. 2 Buchst. j DSGVO zu erfüllen. Da im Falle pseudonymisierter Daten eine Wiederherstellung des Personenbezugs möglich bleibt, sind vielmehr weitere angemessene und spezifische Maßnahmen gesetzlich festzuschreiben, damit diesen europarechtlichen Vorgaben genüge geleistet und somit die Wahrung der Grundrechte und der Interessen der betroffenen Person sichergestellt wird. Vor diesem Hintergrund sollte die Vorschrift **teleologisch dahingehend ausgelegt** werden, dass Nr. 1 nur in Verbindung mit den Rechtsgedanken nach Nr. 2 (Einwilligung) oder Nr. 3 (erhebliches Überwiegen des öffentlichen Interesses und Erreichen des Forschungszwecks nicht anders möglich) zum Tragen kommen kann.

Auch das Widerspruchsrecht der betroffenen Person nach Art. 21 DSGVO sowie weitere Betroffenenrechte erfahren mit der Gesetzesnovelle Beschränkungen. Denn es wird darauf abgestellt, ob „durch [die in Art. 15, 16, 18 und 21 DSGVO vorgesehenen Rechte] voraussichtlich die Verwirklichung der Forschungszwecke unmöglich gemacht oder ernsthaft beeinträchtigt wird und die Beschränkung für die Forschungszwecke notwendig ist". Diese Regelung im neuen Art. 16 Abs. 3 Satz 5 BayUniKlinG ist nach meiner Einschätzung zu unbestimmt. Sie beschränkt sich darauf, Art. 89 Abs. 2 DSGVO sinngemäß zu wiederholen. Der Gesetzgeber eröffnet damit den Uni-

versitätsklinika als Datenverarbeitern in sehr weitem Umfang die Möglichkeit, wesentliche Betroffenenrechte, insbesondere das Widerspruchsrecht der betroffenen Person, das nach meinem Dafürhalten voraussetzungslos gelten sollte, unter Berufung auf Forschungszwecke einzuschränken. Das halte ich gerade im Hinblick auf die hohe Sensibilität der hier in Rede stehenden Gesundheitsdaten und den weiten Adressatenkreis für eine sehr weitgehende Beschränkung der Betroffenenrechte.

Hinsichtlich der im neuen Art. 16 Abs. 4 BayUniKlinG vorgesehenen Übermittlung von personenbezogenen Daten zu Zwecken der wissenschaftlichen Forschung zwischen verschiedenen Universitätsklinika und Universitäten sowie zwischen Universitätsklinika und sonstigen Dritten, hätte ich mir gewünscht, dass die Vorschrift, abgesehen vom Verweis auf eine entsprechende Anwendung von Art. 16 Abs. 3, klarer ausgestaltet wird. Ich habe Zweifel geäußert, ob die rechtliche Möglichkeit zur Übermittlung an jede oder jeden Forschenden die schutzwürdigen Interessen der betroffenen Personen tatsächlich angemessen berücksichtigt. Die Gesetzesbegründung nimmt in diesem Zusammenhang zwar Bezug auf § 14 Abs. 2a Transplantationsgesetz. Die im Transplantationsgesetz geregelte Konstellation ist meines Erachtens jedoch nicht verallgemeinerbar, zumal sich die spezielle Situation im Kontext einer Transplantation von der allgemeinen Weitergabe von Gesundheitsdaten nach Art. 16 Abs. 3 und 4 BayUniKlinG deutlich unterscheidet. Diesen Hinweis hat der Gesetzgeber im Gesetzgebungsverfahren jedoch nicht berücksichtigt.

7.1.3 Fazit und Ausblick

Wenn sich Bürgerinnen und Bürger künftig zur Behandlung in ein Universitätsklinikum begeben, müssen sie nach Maßgabe der novellierten Regelungen des Bayerischen Universitätsklinikagesetzes damit rechnen, dass ihre im Rahmen der Behandlung erhobenen Patientendaten ohne vorherige ausdrückliche Einwilligung zu Forschungszwecken an Dritte übermittelt werden. Ein jegliches Fehlen von Partizipationsrechten der betroffenen Patientinnen und Patienten würde ich für grundrechtswidrig halten. Als Ausgleich dazu würde ich dabei den Universitätsklinika dringend empfehlen, in jedem Fall den betroffenen Patientinnen und Patienten ein Widerspruchsrecht einzuräumen, und sich nicht auf die Beschränkungsmöglichkeit zu berufen.

Insgesamt halte ich die Änderungen im Bayerischen Universitätsklinikagesetz angesichts des laufenden europäischen Gesetzgebungsverfahrens zu einem gemeinsamen europäischen Gesundheitsdatenraum für übereilt (siehe dazu Kapitel 1 zum EHDS).

7.2 Abfrage von Vorerkrankungen und Symptomen von mit dem Erreger SARS-CoV-2 infizierten Personen durch Gesundheitsämter

In den fortdauernden Zeiten der Corona-Pandemie erreichte mich im Zeitraum März bis Juni 2022 eine Reihe von Beschwerden gegen die Erhebung von Vorerkrankungs- und Symptomdaten mit dem Erreger SARS-CoV-2 infizierter Personen (sogenannter Indexpersonen) durch örtliche Gesundheitsämter.

7.2.1 Sachverhalt

Im Rahmen der behördlich angeordneten häuslichen Isolation (teilweise auch als „Quarantäne“ bezeichnet) forderten Gesundheitsämter aus unterschiedlichen Regionen in Bayern die betreffenden Indexpersonen standardmäßig mittels eines beigefügten Links zu einem digitalen Fragebogen – auch digitales Symptomtagebuch genannt – auf, für die Dauer der Isolation täglich ihre spezifischen Symptome anzugeben. Mancherorts fragten sie zugleich auch die jeweiligen Vorerkrankungen ab. In der Regel bezeichneten die Gesundheitsämter die Verwendung der digitalen Symptomtagebücher als freiwillige Option, die dazu beitragen sollte, den Arbeitsaufwand sowohl für Bürgerinnen und Bürger als auch für die Behörden zu minimieren. Bei Nichtverwendung des digitalen Fragebogens waren tägliche Anrufe bei der betroffenen Person vorgesehen, um die Daten auf diese Weise abzufragen.

Von den Datenkategorien im digitalen Fragebogen, der bei den verschiedenen Gesundheitsämtern inhaltlich unterschiedlich ausgestaltet war, waren manche Angaben als freiwillig gekennzeichnet. Sofern aber die Art der Symptome und die jeweiligen Vorerkrankungen verpflichtend erhoben werden sollten, stieß dies in den mir bekannt gewordenen Fällen auf weitgehendes Unverständnis der betroffenen Personen. Diese bezweifelten unter anderem die Erforderlichkeit der Datenkenntnis durch die Gesundheitsämter (insbesondere für Zwecke des Infektionsschutzes) und hinterfragten allgemein den Verarbeitungszweck. Vereinzelt wurde die Vermutung geäußert, das Sammeln von Gesundheitsdaten solle primär dazu dienen, die Durchführung von Forschungsprojekten zu ermöglichen. Nach den bei mir eingegangenen Beschwerden weigerten sich etliche Personen letztlich, ihre Vorerkrankungen oder Symptome dem Gesundheitsamt (wahrheitsgemäß) zu offenbaren, woraufhin ihnen mitunter die Verhängung von Zwangsmaßnahmen angedroht wurde.

7.2.2 Kommunikation mit den Gesundheitsbehörden

Veranlasst durch die ersten derartigen Beschwerden wandte ich mich zunächst an die betreffenden Gesundheitsämter und erbat die Mitteilung der Rechtsgrundlage für die Erhebung von Vorerkrankungen und Symptomdaten. Daraufhin erhielt ich überwiegend die Auskunft, dass die Verwendung der digitalen Fragebögen freiwillig sei und die Datenerhebung auf die §§ 25 ff., insbesondere auf § 25 Abs. 1, Abs. 2 Satz 1 in Verbindung mit § 16 Abs. 1 Infektionsschutzgesetz (IfSG), gestützt werde.

§ 25 IfSG
Ermittlungen
(1) [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. [2]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) [1]Für die Durchführung der Ermittlungen nach Absatz 1 gilt § 16 Absatz 1 Satz 2, Absatz 2, 3, 5 und 8 entsprechend. [2]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.
[…]

§ 16 IfSG
Allgemeine Maßnahmen zur Verhütung übertragbarer Krankheiten
(1) [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. [2]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.
[…]

Dieser Argumentation konnte ich mich nicht anschließen, da nach meiner Rechtsauffassung nicht alle Voraussetzungen der bezeichneten Rechtsnormen erfüllt sind. So sehe ich die Erhebung von Symptomen und Vorerkrankungen nicht als Ermittlung im Sinne des § 25 Abs. 1 IfSG („insbesondere über Art, Ursache, Ansteckungsquelle und Ausbreitung der Krankheit") an. Ferner müssen sich gesundheitsbehördliche Ermittlungen gemäß § 25 Abs. 1 IfSG stets am Maßstab der Erforderlichkeit messen lassen. Schließlich lässt sich auch § 16 Abs. 1 IfSG keine Rechtsgrundlage für die Erhebung der Symptomatik und der Vorerkrankungen entnehmen, da eine solche Erhebung nicht zur Gefahrenabwehr im Sinne der Vorschrift geeignet ist.

Vor diesem Hintergrund informierte ich das Bayerische Staatsministerium für Gesundheit und Pflege über meine grundlegenden Zweifel am Vorhandensein einer notwendigen Rechtsgrundlage für die Verarbeitung sowie an der Erforderlichkeit der Erhebung von Vorerkrankungs- und Symptomdaten von Indexpersonen. Ich wies darauf hin, dass ich ein undifferenziertes Sammeln von sensiblen Gesundheitsdaten für grundsätzlich nicht zulässig erachte.

Das Gesundheitsministerium nahm zu den aufgeworfenen Rechtsfragen ausführlich Stellung und führte im Wesentlichen aus, dass künftig keine Vorerkrankungen mehr erhoben werden würden und es lediglich bezüglich der Symptomatik von Indexpersonen – in Abhängigkeit von den Umständen des Einzelfalles – möglich bleiben müsse, die erforderlichen Gesundheitsdaten aus infektionsschutzrechtlichen Gründen zu erheben und zu verarbeiten, so zum Beispiel in Fällen gemäß § 29 IfSG.

§ 29 IfSG
Beobachtung
(1) Kranke, Krankheitsverdächtige, Ansteckungsverdächtige und Ausscheider können einer Beobachtung unterworfen werden.
(2) [1]Wer einer Beobachtung nach Absatz 1 unterworfen ist, hat die erforderlichen Untersuchungen durch die Beauftragten des Gesundheitsamtes zu dulden und den Anordnungen des Gesundheitsamtes Folge zu leisten. [2]§ 25 Absatz 3 gilt entsprechend. [3]Eine Person nach Satz 1 ist ferner verpflichtet, den Beauftragten des Gesundheitsamtes zum Zwecke der Befragung oder der Untersuchung den Zutritt zu seiner Wohnung zu gestatten, auf Verlangen ihnen über alle seinen Gesundheitszustand betreffenden Umstände Auskunft zu geben und im Falle des Wechsels der Hauptwohnung oder des gewöhnlichen Aufenthaltes unverzüglich dem bisher zuständigen Gesundheitsamt Anzeige zu erstatten. [4]Die Anzeigepflicht gilt auch bei Änderungen einer Tätigkeit im Lebensmittelbereich im Sinne von § 42 Abs. 1 Satz 1 oder in Einrichtungen im Sinne von § 23 Absatz 5 oder § 35 Absatz 1 Satz 1 sowie § 36 Absatz 1 sowie beim

Wechsel einer Gemeinschaftseinrichtung im Sinne von § 33. [5]§ 16 Abs. 2 Satz 4 gilt entsprechend. 6Die Grundrechte der körperlichen Unversehrtheit (Artikel 2 Abs. 2 Satz 1 Grundgesetz), der Freiheit der Person (Artikel 2 Abs. 2 Satz 2 Grundgesetz) und der Unverletzlichkeit der Wohnung (Artikel 13 Abs. 1 Grundgesetz) werden insoweit eingeschränkt.

In den bei mir anhängigen Beschwerdeverfahren war allerdings § 29 IfSG durchweg nicht einschlägig, da eine Beobachtungsunterwerfung in keinem der Fälle angeordnet worden war.

Ergänzend verwies das Gesundheitsministerium auf die Meldepflicht nach § 6 Abs. 1 Satz 1 Nr. 1 Buchst. t und § 7 Abs. 1 Nr. 44a IfSG sowie auf die Vorschrift des § 11 Abs. 1 Satz 1 Nr. 1 IfSG als Befugnisnorm für die Übermittlung der Daten an das Robert Koch-Institut.

§ 11 IfSG
Übermittlung an die zuständige Landesbehörde und an das Robert Koch-Institut
(1) [1]Die verarbeiteten Daten zu meldepflichtigen Krankheiten und Nachweisen von Krankheitserregern werden anhand der Falldefinitionen nach Absatz 2 bewertet und spätestens am folgenden Arbeitstag durch das nach Absatz 3 zuständige Gesundheitsamt vervollständigt, gegebenenfalls aus verschiedenen Meldungen zum selben Fall zusammengeführt und der zuständigen Landesbehörde sowie von dort spätestens am folgenden Arbeitstag dem Robert Koch-Institut mit folgenden Angaben übermittelt:

1. zur betroffenen Person:
   a) Geschlecht,
   b) Monat und Jahr der Geburt,
   c) Tag der Verdachtsmeldung, Angabe, wenn sich ein Verdacht nicht bestätigt hat, Tag der Erkrankung, Tag der Diagnose, gegebenenfalls Tag des Todes und wahrscheinlicher Zeitpunkt oder Zeitraum der Infektion,
   d) Untersuchungsbefund, einschließlich Typisierungsergebnissen,
   e) wahrscheinlicher Infektionsweg, einschließlich Umfeld, in dem die Übertragung wahrscheinlich stattgefunden hat; wahrscheinliches Infektionsrisiko, Impf- und Serostatus und erkennbare Zugehörigkeit zu einer Erkrankungshäufung,
   f) gegebenenfalls Informationen zur Art der Einrichtung bei Tätigkeit, Betreuung oder Unterbringung in Einrichtungen und Unternehmen nach § 23 Absatz 3 Satz 1, Absatz 5 Satz 1 oder § 35 Absatz 1 Satz 1 oder § 36 Absatz 1 oder Absatz 2,
   g) in Deutschland: Gemeinde mit zugehörigem amtlichem achtstelligem Gemeindeschlüssel, in der die Infektion wahrscheinlich erfolgt ist, ansonsten Staat, in dem die Infektion wahrscheinlich erfolgt ist,
   h) bei reiseassoziierter Legionellose: Name und Anschrift der Unterkunft,
   i) bei Tuberkulose, Hepatitis B und Hepatitis C: Geburtsstaat, Staatsangehörigkeit und gegebenenfalls Jahr der Einreise nach Deutschland,
   j) bei Coronavirus-Krankheit-2019 (COVID-19): durchgeführte Maßnahmen nach dem 5. Abschnitt; gegebenenfalls Behandlungsergebnis und Angaben zur Anzahl der Kontaktpersonen, und jeweils zu diesen Angaben zu Monat und Jahr der Geburt, Geschlecht, zuständigem Gesundheitsamt, Beginn und Ende der Absonderung und darüber, ob bei diesen eine Infektion nachgewiesen wurde,
   k) Überweisung, Aufnahme und Entlassung aus einer Einrichtung nach § 23 Absatz 5 Satz 1, gegebenenfalls intensivmedizinische Behandlung und deren Dauer,

l) Zugehörigkeit zu den in § 54a Absatz 1 Nummer 1 bis 5 genannten Personengruppen,
m) Gemeinde mit zugehörigem amtlichem achtstelligem Gemeindeschlüssel der Hauptwohnung oder des gewöhnlichen Aufenthaltsortes und, falls abweichend, des derzeitigen Aufenthaltsortes,
2. zuständige Gesundheitsämter oder zuständige Stellen nach § 54a und
3. Datum der Meldung.
[2]In den Fällen der Meldung nach § 6 Absatz 3 Satz 1 sind nur die Angaben nach Satz 1 Nummer 2 und 3 sowie zu den aufgetretenen nosokomialen Infektionen und den damit zusammenhängenden Kolonisationen jeweils nur die Angaben nach Satz 1 Nummer 1 Buchstabe a bis e erforderlich. [3]Für die Übermittlungen von den zuständigen Landesbehörden an das Robert Koch-Institut bestimmt das Robert Koch-Institut die technischen Übermittlungsstandards. [4]Frühere Übermittlungen sind gegebenenfalls zu berichtigen und zu ergänzen, insoweit gelten die Sätze 1 bis 3 entsprechend.
[...]

Richtigerweise lässt sich jedoch die konkrete Art der erhobenen Gesundheitsdaten unter keine der in § 11 Abs. 1 Satz 1 Nr. 1 IfSG bezeichneten Alternativen subsumieren. Insbesondere sind Vorerkrankungen sowie Symptome während einer Isolation weder als Angaben über den wahrscheinlichen Infektionsweg (im Sinne von Buchst. e) zu qualifizieren, noch als durchgeführte Maßnahme oder als Behandlungsergebnis (im Sinne von Buchst. j).

7.2.3 Datenschutzrechtliche Bewertung der Erhebung von Symptomdaten im Lichte der landesrechtlichen Vollzugsvorschriften zum Infektionsschutz

Das Hauptaugenmerk legte das Gesundheitsministerium auf die seinerzeit geltende Allgemeinverfügung „AV Isolation".[62]

AV Isolation
[...]
4. Beendigung der Isolation
4.1 Bei Personen, die mittels Antigentest durch eine medizinische Fachkraft oder eine vergleichbare, hierfür geschulte Person positiv getestet werden, endet die Isolation, falls der erste nach dem positiven Antigentest bei diesen Personen vorgenommene Nukleinsäuretest ein negatives Ergebnis aufweist, mit dem Vorliegen dieses negativen Testergebnisses. Ist das Testergebnis positiv, so richtet sich das Ende der Isolation nach Nr. 4.2, wobei hier als Erstnachweis des Erregers der positive Antigentest nach Satz 1 gilt. Im Übrigen endet die Isolation frühestens nach Ablauf von fünf Tagen nach dem positiven Antigentest und Symptomfreiheit seit mindestens 48 Stunden, spätestens jedoch nach Ablauf von zehn Tagen.
[...]

Demnach sei die Symptomatik der Indexpersonen relevant für die Dauer der Isolation. Die Symptomatik und deren Einordnung habe zudem Einfluss auf die Einschätzung der Infektiosität der betreffenden Person.

62 Allgemeinverfügung des Bayerischen Staatsministeriums für Gesundheit und Pflege „Vollzug des Infektionsschutzgesetzes (IfSG) – Isolation von positiv auf das Coronavirus SARS-CoV-2 getesteten Personen (AV Isolation)" vom 12. April 2022, BayMBL 2022, Nr. 225, geändert durch Bekanntmachung vom 29. Juni 2022, GCRASa-G8000-2022/44-317.

Im Ergebnis hielt auch diese Argumentation einer datenschutzrechtlichen Überprüfung nicht stand.

Bezüglich der Symptomatik einer Indexperson stellt der Normgeber in Unterabschnitt 4.1 AV Isolation begrifflich auf das Tatbestandsmerkmal der Symptomfreiheit (seit mindestens 48 Stunden und frühestens nach Ablauf von fünf Tagen nach dem positiven Antigentest) ab. Das Kriterium der **Symptomfreiheit** ist jedoch nicht gleichzusetzen mit den **unterschiedlichen Arten möglicher Symptome**. Aus dem Terminus der Symptomfreiheit lässt sich somit nicht ableiten, dass von der betroffenen Person Angaben über die spezifische Art ihrer Symptome systematisch erhoben werden dürfen, vor allem nicht bereits ab Beginn der Isolation und aufgeschlüsselt nach einzelnen Tagen. Hierzu ist in tatsächlicher Hinsicht anzumerken, dass die zuständigen Gesundheitsämter überhaupt nicht vorhatten, etwaige Angaben der betroffenen Personen zu Symptomen zu beurteilen oder zu hinterfragen. Die Daten sollten schlicht nur erhoben werden. Auf Nachfrage konnte nicht angegeben werden, welche Aufgaben mit den Informationen über die Art der Symptome erfüllt werden sollten. Auch das Gesundheitsministerium konnte bislang keine überzeugenden Argumente hierzu vorbringen. Vielmehr werde ein allgemeines Bedürfnis seitens der (ehemals in der Forschung tätig gewesenen) Kollegen gesehen, alle verfügbaren Daten zu erfassen. Eine solche Argumentation liefe freilich auf eine Vorratsspeicherung hinaus, die mit dem Grundsatz der Datenminimierung unvereinbar wäre.

Des Weiteren bestimmt die AV Isolation in Unterabschnitt 4.1, dass die Isolation einer Indexperson spätestens nach Ablauf von zehn Tagen endet. Dass die zuständigen Gesundheitsbehörden auf dieser Basis etwa gehalten wären, die Zeitspanne von maximal zehn Tagen auf die rechnerisch minimale Isolationsdauer abzukürzen – etwa von Amts wegen durch Erhebung der Symptomfreiheit im konkreten Einzelfall –, ist selbst bei extensiver Auslegung der Vorschriften nicht anzunehmen. Vielmehr dürfte gerade die nicht abgekürzte Isolationszeit dem Interesse eines effektiven Gesundheitsschutzes in einem höheren Maße dienen, das heißt das Risiko der Ansteckung weiterer Personen dürfte sich aufgrund der längeren Isolationsdauer mit höherer Wahrscheinlichkeit reduzieren. Da somit in Unterabschnitt 4.1 der AV Isolation letztlich eine Regelung getroffen wurde, welche die Ermittlung des Enddatums der Isolation hinreichend konkret und eindeutig ermöglicht, besteht weder eine erkennbare Notwendigkeit noch eine anderweitige rechtliche Legitimation dafür, betroffene Personen standardmäßig zu verpflichten, gegen ihren erklärten Willen Angaben zur Art ihrer Symptome zu machen.

Bei näherer Betrachtung erscheint es bereits nach dem Wortlaut der AV Isolation („Im Übrigen endet die Isolation frühestens nach Ablauf von fünf Tagen […] und Symptomfreiheit seit mindestens 48 Stunden, […]“) geboten, selbst im Falle einer seit 48 Stunden gegebenen Symptomfreiheit keine Offenlegung dieses Umstands gegenüber der zuständigen Gesundheitsbehörde zu fordern. Vielmehr deutet die Formulierung „endet“ auf ein automatisch eintretendes Ende der Isolation hin, das von der eigenen Feststellung der betreffenden Person über die bestehende Symptomfreiheit abhängig ist. Es ist auch aus der Begründung der AV Isolation nicht ersichtlich, dass das Ende der Isolation etwa eines weiteren Tätigwerdens der Gesundheitsbehörde, zum Beispiel in Form eines (wiederholenden) Verwaltungsakts bedürfen würde.

Zusammenfassend fehlt es grundlegend an der Erforderlichkeit der Symptomangaben zur Erfüllung einer (hoheitlichen) gesundheitsbehördlichen Aufgabe und damit an einem Erlaubnistatbestand für die Erhebung von Symptomdaten.

Im Übrigen kam ich bei meiner Überprüfung der Beschwerdefälle zu dem Ergebnis, dass die häufig in diesem Zusammenhang behauptete „Freiwilligkeit der Datenerhebung“ mittels digitaler Fragebögen aus rechtlicher Sicht nicht haltbar ist. Denn in der Praxis stellten die Gesundheitsämter den betroffenen Personen tägliche Anrufe in Aussicht, falls sie sich weigerten, die „freiwilligen“ Informationen preiszugeben. Von Freiwilligkeit kann in einem solchen Fall jedoch aus datenschutzrechtlicher Sicht nicht die Rede sein, weil durch die Ankündigung von Alternativmaßnahmen ein faktischer Zwang auf die Entscheidungsfreiheit der betroffenen Person ausgeübt wurde. Im Einzelfall drohte das Gesundheitsamt die Verhängung von Bußgeldern an. Durch die Ankündigung derartiger Konsequenzen wird ein psychischer Druck auf die betroffenen Personen ausgeübt, der einem subjektiv empfundenen Zwang zur Datenoffenlegung gleichkommt.

7.2.4 Fazit und Ausblick

Vor diesem Hintergrund plant das Gesundheitsministerium in enger Abstimmung mit meinem Haus ein Schreiben an die nachgeordneten Gesundheitsbehörden, damit für die Zukunft ein landesweit einheitlicher und datenschutzkonformer Vollzug der geltenden infektionsschutzrechtlichen Vorschriften gewährleistet werden kann. Der begonnene Abstimmungsprozess konnte im Berichtszeitraum noch nicht abgeschlossen werden.

Parallel bat ich die betreffenden Gesundheitsämter, ihre bisherige Praxis der Erhebung von personenbezogenen Vorerkrankungs- und Symptomdaten (sowohl von Indexpersonen als auch von etwaigen Kontaktpersonen) genau zu überprüfen und dabei meine datenschutzrechtliche Bewertung der Sach- und Rechtslage zu berücksichtigen. Gegenwärtig sind mir aus der Praxis keine Beispiele für besondere Einzelfallumstände bekannt, die bei stetig abebbender Pandemie und angesichts der geltenden normativen Vorgaben ausnahmsweise eine Erhebung von personenbezogenen Daten über Vorerkrankungen oder Symptome legitimieren könnten. Ein Gesundheitsamt teilte mir bereits ausdrücklich mit, dass es die Verwendung des bisherigen digitalen Fragebogens als Reaktion auf eine entsprechende Beschwerde eingestellt habe.

Auch das in der Folgezeit zu dieser Thematik eingeholte Meinungsbild der Datenschutzaufsichtsbehörden des Bundes und der Länder ergab keine Unterstützung für die Auffassung des Gesundheitsministeriums, dass das Infektionsschutzgesetz ausreichende Rechtsgrundlagen für die standardmäßige Abfrage der Symptomdaten biete. Vielmehr teilten einige der befassten Bundes- und Länderkolleginnen bzw. –kollegen explizit meine Zweifel an der Geeignetheit und Erforderlichkeit der Symptomdatenerhebung für infektionsschutzrechtliche Zwecke der Gesundheitsämter.

Ich werde die Entwicklungen in diesem Bereich weiterhin genau beobachten und habe angeboten, das Gesundheitsministerium bei der Abfassung wegweisender Vollzugsvorgaben mit meiner datenschutzrechtlichen Expertise beratend zu unterstützen.

7.3 Evaluierungsauftrag im Bayerischen Krebsregistergesetz

In den vergangenen Jahren befasste ich mich wiederholt mit dem Bayerischen Krebsregister. Insbesondere in meinem 27. Tätigkeitsbericht 2016 unter Nr. 7.3 beschäftigte ich mich eingehend mit der Neustrukturierung der Krebsregistrierung durch das

Bayerische Krebsregistergesetz und formulierte meinen Standpunkt zu wesentlichen datenschutzrechtlichen Fragestellungen.

7.3.1 Kritikpunkt „eingeschränktes Widerspruchsrecht“

Bereits im Rahmen meiner Beteiligung am Gesetzgebungsverfahren 2016/2017 äußerte ich grundlegende Zweifel an der Rechtmäßigkeit und Effektivität des vorgesehenen Widerspruchsrechts der betroffenen Patientinnen und Patienten. Auf meinen Vorschlag wurde daraufhin eine Evaluationsklausel in den Gesetzentwurf eingefügt mit dem Ziel, aus zwei Jahren Praxiserfahrung tragfähige Erkenntnisse über die Funktionsfähigkeit des Krebsregisters zu gewinnen und diese Erkenntnisse idealerweise im Rahmen einer weiteren Gesetzesnovelle zur Verbesserung des Datenschutzes umzusetzen.

Art. 5 Bayerisches Krebsregistergesetz (BayKRegG) bestimmt zum Widerspruchsrecht:

„(1) [1]Jeder kann der dauerhaften Speicherung der Identitätsdaten im Bayerischen Krebsregister widersprechen, soweit sie ihn selbst oder eine seiner Personensorge oder Betreuung unterstehende Person betreffen. [2]Diese Identitätsdaten sind unverzüglich zu löschen, sobald sie für Zwecke der verpflichtenden Qualitätssicherung, Abrechnung oder auf Grund anderer gesetzlicher Vorschriften nicht mehr benötigt werden. [3]Der Widerspruch ist schriftlich bei der Vertrauensstelle einzulegen. [4]Er kann auch über Personen, die gemäß Art. 4 Abs. 2 Satz 3 über das Widerspruchsrecht belehrt haben, bei der Vertrauensstelle eingelegt werden. [5]Der Widerspruch betrifft bereits erfasste sowie künftig eingehende Identitätsdaten. [6]Wurden Daten zu dieser Person von oder an ein anderes Landeskrebsregister gemeldet, ist dieses Landeskrebsregister über die Erhebung des Widerspruchs zu informieren.
(2) Für einen inhaltlich vergleichbaren Widerspruch, der in einem Land nach dessen Landesrecht eingelegt wurde, gilt Abs. 1 entsprechend, sobald er von den dortigen Behörden der zuständigen bayerischen Stelle zur Kenntnis gebracht wurde.
(3) Das für die Gesundheit zuständige Staatsministerium (Staatsministerium) überprüft zwei Jahre nach Inkrafttreten dieses Gesetzes die Regelungen der Abs. 1 und 2 unter den Gesichtspunkten eines wirksamen Datenschutzes und einer ausreichenden Qualitätssicherung für die Zwecke des Bayerischen Krebsregisters.“

Die Fassung des Absatzes 1 verdeutlicht, dass es sich hierbei – namentlich aufgrund der Begrenzung des Widerspruchs auf Identitätsdaten – um ein eingeschränktes Widerspruchsrecht handelt. Aktuell bewirkt ein Widerspruch im Sinne von Art. 5 Abs. 1 BayKRegG lediglich die Ersetzung der Identitätsdaten durch ein Pseudonym. Mithin führt dies zu keiner dem Willen der Widersprechenden vollends Rechnung tragenden kompletten Löschung ihrer Krebsregisterdaten. Demgegenüber würde ein uneingeschränktes Widerspruchsrecht nach meinem Verständnis verlangen, neben den Identitätsdaten auch sämtliche Daten zur Krankheitsgeschichte der betroffenen Person vollständig zu löschen.

Der maßgebliche Evaluationszeitraum gemäß Art. 5 Abs. 3 BayKRegG begann unmittelbar mit Inkrafttreten des Gesetzes am 1. April 2017 und dauerte zwei Jahre, also bis zum 31. März 2019. Im Anschluss an den Evaluationsbericht des Bayerischen Landesamtes für Gesundheit und Lebensmittelsicherheit verzögerten im Jahre 2020 vordringliche Aufgaben (zur Bewältigung der COVID-19-Pandemie) die notwendige Folgenbetrachtung durch das Bayerische Staatsministerium für Gesundheit und

Pflege und die datenschutzrechtliche Beratung durch mich, bis der gesamte Evaluationsprozesses im Sommer 2022 abgeschlossen werden konnte.

Dem mir im November 2019 zugeleiteten Evaluationsbericht zufolge war insgesamt nur eine geringe Anzahl von Widersprüchen gegen die dauerhafte Speicherung der Identitätsdaten der betroffenen Personen festzustellen. Dieser Befund verwies darauf, dass eine Löschung sämtlicher gespeicherten Krebsregisterdaten der widersprechenden Personen möglich erscheint, ohne die Funktionsfähigkeit des Bayerischen Krebsregisters zu beeinträchtigen. Allenfalls dürfte nach Angabe des Gesundheitsministeriums für die Zukunft mit einem gewissen Mehraufwand im Dokumentationssystem des Krebsregisters zu rechnen sein.

7.3.2 Komplette Löschung von Krebsregisterdaten im Widerspruchsfall

Zur Gewährleistung eines effektiven Schutzes von Patientendaten setzte ich mich vor diesem Hintergrund mit unverminderter Intensität für eine Abkehr von der bislang eingeschränkten Widerspruchslösung ein. Die bestehende Interessenlage bei der Verarbeitung hochsensibler Gesundheitsdaten, die sich in Ansätzen bereits in der Gesetzesbegründung aus dem Jahre 2017 widerspiegelt, erfordert nach meinem Dafürhalten, für die Zukunft gesetzlich zu verankern, dass ein wirksamer Widerspruch – über die Bestimmungen des gegenwärtigen Art. 5 BayKRegG hinaus – die vollständige Löschung sämtlicher Krebsregisterdaten der betroffenen Person zur Folge hat.

Erfreulicherweise griff das Gesundheitsministerium meine datenschutzrechtlichen Argumente nunmehr auf. Mitte August 2022 berichtete es mir von Planungen, so bald wie möglich einen Gesetzentwurf zur Änderung des Bayerischen Krebsregistergesetzes auf den Weg zu bringen, um hinsichtlich künftiger Widerspruchsfälle die rechtlichen Voraussetzungen für eine vollständige Löschung der gespeicherten Krebsregisterdaten zu schaffen. Auch in technisch-organisatorischer Hinsicht sei mit den im Vorfeld notwendigen Abstimmungen und Vorarbeiten bereits begonnen worden.

Ich werde den Gesetzgebungsprozess weiterhin aufmerksam verfolgen und mit meiner Expertise beratend begleiten. Ein erkennbar hohes Datenschutzniveau stärkt nach meiner Überzeugung das Vertrauen der Patientinnen und Patienten in die Funktionsweise von medizinischen Registern und ist zugleich ein wesentlicher Akzeptanzfaktor im Hinblick auf die künftige Forschung mit Gesundheitsdaten.

7.4 Corona-Impfstatusabfrage bei Besuch eines Krankenhauses

Im Berichtszeitraum erreichte mich die Beschwerde eines Bürgers, der anlässlich des Besuchs eines Patienten im Krankenhaus nach seinem Corona-Impfstatus gefragt wurde, obwohl er einen Testnachweis im Sinne des § 22a Abs. 3 Infektionsschutzgesetz (IfSG) vorlegen konnte.

Nach den zu diesem Zeitpunkt geltenden Bestimmungen der Sechzehnten Bayerischen Infektionsschutzmaßnahmenverordnung war der Zutritt von Besuchern zu einem Krankenhaus nur erlaubt, soweit diese geimpft, genesen **oder** getestet waren.

Die damals geltende COVID-19-Schutzmaßnahmen-Ausnahmeverordnung verwies für die Definition einer getesteten Person ausdrücklich auf den Testnachweis im Sinne von § 22a Abs. 3 IfSG.

Da die Tatbestandsalternativen mit einem „oder“ verknüpft waren, war die Frage nach dem Corona-Impfstatus bei einer nachweislich negativ getesteten Person datenschutzrechtlich unzulässig.

Nachdem ich das Krankenhaus hierauf hingewiesen hatte, wurde das Einlassverfahren umgestellt und auf die Abfrage des Corona-Impfstatus bei nachweislich negativ getesteten Personen verzichtet.

7.5 Datenschutzrechtliche Verantwortlichkeit in den Bereitschaftspraxen der Kassenärztlichen Vereinigung Bayerns

Die Verpflichtungen nach der Datenschutz-Grundverordnung treffen in erster Linie den Verantwortlichen, der in Art. 4 Nr. 7 DSGVO definiert wird:

Art. 4 DSGVO
Begriffsbestimmungen
Im Sinne dieser Verordnung bezeichnet der Ausdruck:
[…]
7. „Verantwortlicher“ 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; […]

Doch nicht immer lässt sich ohne weiteres bestimmen, wer bei einer Datenverarbeitung der Verantwortliche ist, was sich im Berichtszeitraum am Beispiel der Bereitschaftspraxen der Kassenärztlichen Vereinigung Bayerns (KVB) zeigte.

Aus der Ärzteschaft erhielt ich davon Kenntnis, dass von der KVB zur Verfügung gestellte Praxisräume nicht über geeignete Wartezimmer verfügten. Patientinnen und Patienten müssten in unmittelbarer Nähe des Anmeldetresens warten und könnten so Kenntnis von Gesundheitsdaten Dritter erhalten.

Zunächst vertrat die KVB die Auffassung, dass die diensthabende Ärztin oder der diensthabende Arzt hinsichtlich aller Datenverarbeitungen im Rahmen der Bereitschaftspraxis allein verantwortlich sei. Aufgrund meiner Prüfung kam ich hingegen zu der Einschätzung, dass sich die KVB nicht von der Verantwortlichkeit freizeichnen kann. Vielmehr ist die KVB grundsätzlich die für die Organisation des Bereitschaftsdienstes verantwortliche Stelle, soweit sie beispielsweise Räume, Software, Hardware und angestelltes Personal zur Verfügung stellt. Für die medizinische Behandlung von Patientinnen und Patienten sind nach meiner Auffassung dagegen allein die behandelnden Ärztinnen und Ärzte datenschutzrechtlich verantwortlich.

Für die Einordnung der Verantwortlichkeit nach Art. 4 Nr. 7 DSGVO ist entscheidend, wer die wesentliche Entscheidungsbefugnis hinsichtlich der Zwecke einer Datenverarbeitung, und Mittel innehat. Ein bestimmender Einfluss erfordert jedoch nicht, dass jeder der Beteiligten die umfassende Kontrolle über alle Umstände und Phasen der Verarbeitung besitzt. Auch ist keine vollständig gleichrangige Kontrolle durch alle Beteiligten erforderlich.

Die Zuordnung der Verantwortlichkeit muss sich vorliegend an der gesetzlichen Aufgabenverteilung orientieren.

So kommt der KVB gemäß § 75 Abs. 1b Satz 1 Fünftes Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (SGB V) der sogenannte Sicherstellungsauftrag zu.

Sie hat dafür zu sorgen, dass auch zu den üblicherweise sprechstundenfreien Zeiten eine vertragsärztliche Versorgung vorhanden ist (Notdienst). Die KVB hat eine Struktur zu schaffen, die unter quantitativen wie qualitativen Gesichtspunkten in der Lage ist, die vertragsärztliche Versorgung der Versicherten zu gewährleisten. Wie sie diesem Sicherstellungsauftrag nachkommt, steht weitgehend in ihrem gestalterischen Ermessen.

Zur Erfüllung des Sicherstellungsauftrages bedient sich die KVB der an der vertragsärztlichen Versorgung teilnehmenden Ärztinnen und Ärzte. Diese sind zur Beteiligung am vertragsärztlichen Notdienst verpflichtet. Sie stehen weder in einem abhängigen Beschäftigungsverhältnis zur KVB, noch unterliegen sie deren Weisungsrecht. Sie erfüllen ihre Aufgaben als Vertragsärztin oder Vertragsarzt auf der Grundlage ihrer statusbezogenen Zulassung zur vertragsärztlichen Versorgung im Rahmen ihres freien ärztlichen Berufes. Gleichzeitig schafft § 75 Abs. 2 Satz 2 SGB V grundsätzlich eine Befugnis für die Kassenärztlichen Vereinigungen, die Erfüllung der den Vertragsärztinnen und Vertragsärzten obliegenden Pflichten zu überwachen.

Tatsächlich ergab meine Prüfung, dass die KVB den Bereitschaftspraxen Hard- und Software zur Verfügung stellt. Sie mietet zum Teil auch die Räumlichkeiten an und stellt das Praxispersonal ein. Insofern steht den beteiligten Ärztinnen und Ärzten keine Auswahl- oder Einflussmöglichkeit zu.

Des Weiteren verhält sich die KVB zum Teil bereits faktisch wie ein Verantwortlicher. Zum Beispiel sollen Meldungen von Datenpannen durch die KVB erfolgen. Auch werden das Blanko-Formular des Anamnesebogens sowie die Datenschutzinformationen der Bereitschaftspraxen von der KVB vorgegeben.

Gleichzeitig verarbeiten die an der vertragsärztlichen Versorgung teilnehmenden Ärztinnen und Ärzte im Rahmen ihres Dienstes in den Bereitschaftspraxen Daten der zu behandelnden Personen, ohne dass die KVB Einfluss auf den Umfang der Datenverarbeitung hat.

Aus meiner Sicht kann daher den tatsächlichen und rechtlichen Gegebenheiten nur Rechnung getragen werden, wenn die KVB als Verantwortliche hinsichtlich der Organisation des Bereitschaftsdienstes sowie die jeweils diensthabenden Ärztinnen oder Ärzte als Verantwortliche für die medizinische Behandlung betrachtet werden. Auch aus Patientensicht erscheint dieses Ergebnis als sachgerecht. Dem hat sich im Zuge des beratenden Austausches zwischenzeitlich auch die KVB angeschlossen.

7.6 Beanstandung nach Datenpanne bei Krankenkasse

Eine Bürgerin wandte sich im Berichtszeitraum mit einer Beschwerde wegen einer Datenpanne bei einer Krankenkasse an mich.

Die Petentin hatte eine Mitgliedsbescheinigung der Krankenkasse benötigt. Die Krankenkasse übersandte die Bescheinigung wie vorher vereinbart mittels verschlüsselter E-Mail, zusätzlich entgegen der Absprache jedoch auch noch per Brief. Dieser Brief wurde aufgrund eines Versehens der Krankenkasse nicht an die Petentin adressiert, sondern an ihren von ihr getrennt lebenden Ehemann (und früheren Bevollmächtigten). Aufgrund des Versehens erlangte der Ehemann Kenntnis von der neuen Adresse der Petentin.

Die rechtliche Bewertung des Falles war unkompliziert: Die unbefugte Offenbarung von Adressdaten der Petentin durch fälschliche Versendung einer Mitgliedsbescheinigung an deren Ehemann stellte einen Verstoß gegen das Sozialgeheimnis nach § 35 Abs. 1 Satz 1 Erstes Buch Sozialgesetzbuch – Allgemeiner Teil – (SGB I) dar. Nach dieser Vorschrift hat jeder Anspruch darauf, dass die ihn betreffenden Sozialdaten von den Leistungsträgern nicht unbefugt verarbeitet werden.

Ich habe gegenüber der Krankenkasse eine Beanstandung ausgesprochen. Die Krankenkasse ließ nicht nur fahrlässig personenbezogene Daten an einen Außenstehenden gelangen; sie missachtete bei dem Fehlversand auch eine Auskunftssperre, die auf Wunsch der Petentin im EDV-System der Krankenkasse hinterlegt worden war und Datenübermittlungen an Dritte hätte verhindern sollen. Dem Datenschutzverstoß kam besonderes Gewicht zu, weil die Petentin ihre Adressdaten vor ihrem früheren Ehemann geheim halten wollte und der Krankenkasse dies ausweislich der Auskunftssperre auch bekannt war; auch die Folgen für die Petentin waren einschneidend. Der unberechtigte Empfänger konnte die Petentin kontaktieren. Die Petentin hielt vor diesem Hintergrund letztlich einen weiteren Umzug für erforderlich.

Bedauerlich war zudem, dass die Krankenkasse mir den Fehlversand erst Wochen nach dem Bekanntwerden anlässlich meiner Bitte um Stellungnahme meldete. Die Meldung einer solchen Datenpanne ist nach Art. 33 Abs. 1 Satz 1 DSGVO unverzüglich, mithin ohne schuldhaftes Zögern, zu erstatten. Im Verlauf der Prüfung wurden noch weitere vergleichbare Vorfälle bekannt, bei denen die Krankenkasse unter Missachtung einer Auskunftssperre unbefugt personenbezogene Daten offenbart hatte.

7.7 Auftragsverarbeitung bei bayerischen öffentlichen Krankenhäusern

Bayerische öffentliche Krankenhäuser durften sich bislang zur Verarbeitung von Patientendaten, die nicht zur verwaltungsmäßigen Abwicklung der Behandlung der Patientinnen und Patienten erforderlich sind, nur anderer Krankenhäuser bedienen. Diese nicht mehr ganz zeitgemäße Vorgabe aus Art. 27 Abs. 4 Satz 6 Bayerisches Krankenhausgesetz (BayKrG) in der bis zum 31. Mai 2022 geltenden Fassung hat der bayerische Gesetzgeber durch die am 1. Juni 2022 in Kraft getretene Novelle des Gesundheitsdienstgesetzes (GDG)[63] aufgehoben. Das hat zur Folge, dass Auftragsverarbeitungsverhältnisse insoweit nun auch mit anderen Auftragsverarbeitern als Krankenhäusern begründet werden dürfen. Der in Art. 27 Abs. 4 BayKrG verbleibende Regelungsbestand wird weiterhin durch die allgemeinen Regelungen der Datenschutz-Grundverordnung zur Auftragsverarbeitung ergänzt; ein regelungsloser Zustand tritt nicht ein.

Was die Rechtsänderung betrifft, möchte ich bayerische öffentliche Krankenhäuser auf folgende Gesichtspunkte aufmerksam machen:

7.7.1 Gestaltungsimpulse bei Auftragsverarbeitung im Krankenhaus

Die Gesetzesänderung macht bewusst, dass bayerische öffentliche Krankenhäuser Patientendaten betreffende Auftragsverarbeitungsverhältnisse mit externen IT-

[63] Vom 10. Mai 2022 (GVBl. S. 182). – Die Aufhebung von Art. 27 Abs. 4 Satz 6 BayKrG ist in Art. 32c Nr. 2 Buchst. a GDG geregelt, das Inkrafttreten in Art. 33 Abs. 1 Satz 1 GDG.

Dienstleistern nun noch mehr als bislang aktiv gestalten müssen. Das ist keine „banale“ Aufgabe:

— In Krankenhäusern werden große Mengen an Daten verarbeitet, welche die Gesundheit der Patientinnen und Patienten und damit deren intimsten Lebensbereich betreffen.

— Durch die Beteiligung externer Stellen wird der Kreis derer, die mit sensiblen medizinischen Patientendaten in Berührung kommen, größer. Gleichzeitig sinken die direkten Einflussmöglichkeiten der Krankenhäuser auf den Umgang mit den Daten ihrer Patientinnen und Patienten.

— Krankenhäuser sind nicht selten Opfer von Cybercrime-Attacken mit teilweise schwerwiegenden Folgen für die Patientinnen und Patienten. Eine Konzentration der Patientendatenverarbeitung auf wenige IT-Dienstleister erhöht die Attraktivität und damit die Eintrittswahrscheinlichkeit von Cybercrime-Angriffen in diesem Bereich.

— Für die Verarbeitung setzen nicht wenige IT-Dienstleister Betriebsmittel ein, bei denen die Zulässigkeit einer (möglichen) Datenübermittlung in ein Drittland oder an eine internationale Organisation gewährleistet sein muss. Übermittlungen dieser Art sind seit Geltungsbeginn der Datenschutz-Grundverordnung allerdings strikt reglementiert, wie das Urteil des Europäischen Gerichtshofs in der Rechtssache Schrems II[64] zeigt. Dabei ist zu beachten, dass auch ein Fernzugriff, den eine Stelle in einem Drittland auf die im Europäischen Wirtschaftsraum befindlichen Patientendaten hat, eine Übermittlung begründen kann.

— Im Krankenhausbereich sind mit zunehmender Digitalisierung sehr viele neue, innovative Formen der Verarbeitung von Patientendaten – oft unter Beteiligung mehrerer Stellen – zu beobachten. In diesem Zusammenhang ist es empfehlenswert, frühzeitig die jeweilige datenschutzrechtliche Rolle einer an der Verarbeitung beteiligten Stelle (wie etwa eigenständiger oder gemeinsamer Verantwortlicher, Auftragsverarbeiter, Datenexporteur, Datenimporteur) mit ihren datenschutzrechtlichen Pflichten und Befugnissen zu identifizieren und die damit erforderlichen Nachweise und sonstigen Unterlagen zu erarbeiten (wie beispielsweise eine Auftragsverarbeitungsvereinbarung, eine Datenschutz-Folgenabschätzung oder eine allgemeine Risikoanalyse).

— Die fortschreitende Digitalisierung und die wachsende Komplexität aktueller IT-Systeme führen regelmäßig dazu, dass IT-Dienstleister als Auftragsverarbeiter zur Erbringung ihrer Leistungen weitere Unterauftragsnehmer nutzen, deren Verarbeitung ebenfalls die Anforderungen der Datenschutz-Grundverordnung erfüllen müssen (vgl. Art. 28 Abs. 4 DSGVO).

64 Europäischer Gerichtshof, Urteil vom 16. Juli 2020, C-311/18.

7.7.2 Regelungsrahmen

Bayerische öffentliche Krankenhäuser müssen bei der Begründung von Auftragsverarbeitungsverhältnissen weiterhin die Regelungen beachten, welche die Datenschutz-Grundverordnung dafür bereithält. Dies betont auch der neu gefasste Art. 27 Abs. 6 BayKrG. Darin heißt es seit dem 1. Juni 2022:

„Im Anwendungsbereich der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO), insbesondere Art. 28 DSGVO (Auftragsverarbeiter) und Art. 32 DSGVO (Sicherheit der Verarbeitung), sind besondere Schutzmaßnahmen technischer und organisatorischer Art zu treffen, dass Patientendaten nicht unberechtigt verwendet oder übermittelt werden können."

Bayerische öffentliche Krankenhäuser können bei der Erfüllung dieser Aufgabe auf vielfältige Informationsmaterialien zurückgreifen. Zu nennen sind insbesondere:

— meine Orientierungshilfe „Auftragsverarbeitung";[65]

— mein „Leitfaden zum Outsourcing kommunaler IT";[66]

— meine Aktuelle Kurz-Information 39 „Office-Anwendungen aus Drittstaaten bei bayerischen öffentlichen Stellen";[67]

— meine Materialien zur Risikoanalyse;[68]

— das Vertragsmuster zur Auftragsverarbeitung des Bayerischen Staatsministeriums des Innern, für Sport und Integration;[69]

— die „Leitlinien 07/2020 zu den Begriffen ‚Verantwortlicher' und ‚Auftragsverarbeiter' in der DSGVO" des Europäischen Datenschutzausschusses[70] sowie

— die „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten" des Europäischen Datenschutzausschusses.[71]

Dass bei der Erfüllung dieser Aufgabe ein Synergiepotenzial für die bayerischen Krankenhäuser besteht, spricht die Gesetzesbegründung zum neuen Gesundheitsdienstgesetz ausdrücklich an:[72]

65 Stand 4/2019, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Auftragsverarbeitung".

66 Stand 3/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Auftragsverarbeitung".

67 Stand 12/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Aktuelle Kurz-Informationen".

68 Überblick im Internet: https://www.datenschutz-bayern.de, Rubrik „DSFA".

69 Internet: https://www.innenministerium.bayern.de, Rubrik „Schutz und Sicherheit – Datenschutz und Cybersicherheit – Schutz persönlicher Daten – Datenschutzreform-Arbeitshilfen".

70 Internet: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_de.

71 Internet: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de.

72 Landtags-Drucksache 18/19685, S. 30.

„Durch die Aufhebung von Art. 27 Abs. 4 Satz 6 BayKrG gehen bewährte Schutzelemente für die Verarbeitung von Patientendaten zunächst ersatzlos verloren. Diese Lücke sollte für die verantwortlichen Krankenhäuser bedarfsgerecht und idealerweise auf Selbstverpflichtungsbasis zum Beispiel durch ein einvernehmlich geschaffenes Regelwerk geschlossen werden, welches nach Maßgabe der Datenschutz-Grundverordnung die unabdingbaren technischen und organisatorischen Maßnahmen präzisiert und damit den Weg ebnet für eine möglichst einheitliche Anwendungspraxis bei gleichbleibend hohem Schutzniveau für die Patientendaten. Ein derartiges Regelwerk zur Präzisierung der technischen und organisatorischen Maßnahmen könnte beispielsweise seitens der Interessensvertretung der bayerischen Krankenhausträger und deren Spitzenverbände ins Leben gerufen werden."

Um ein einheitlich hohes Sicherheits- und Datenschutzniveau sicherzustellen, empfehle ich den beteiligten Verkehrskreisen nachdrücklich, möglichst zeitnah mit der Erarbeitung eines solchen Regelwerks zu beginnen.

8 Steuer- und Finanzverwaltung

8.1 Neuregelung der Datenschutzaufsicht im Bereich der Grundsteuer

Das Bundesverfassungsgericht hat im Jahr 2018 die Ermittlung der Grundsteuer auf Basis veralteter Einheitswerte für unvereinbar mit dem Grundgesetz für die Bundesrepublik Deutschland (GG) erklärt und den Gesetzgeber zu einer Neuregelung aufgefordert.[73]

Daraufhin hat der Bund in Art. 105 Abs. 2 Satz 1 GG zum einen die Gesetzgebungszuständigkeit des Bundes für die Grundsteuer klargestellt und zum anderen den Ländern in Art. 72 Abs. 3 Satz 1 Nr. 7 GG erlaubt, von den Regelungen des Bundes durch Gesetz abzuweichen. Im Rahmen der sogenannten Abweichungsgesetzgebung dürfen die Länder ein eigenes Grundsteuermodell einführen und ab 2025 (vgl. Art. 125b Abs. 3 GG) die „neue" Grundsteuer erheben. Auf dieser Grundlage beruht das bereits zum 1. Januar 2022 in Kraft getretene Bayerische Grundsteuergesetz (BayGrStG).

Neben Fragen der Bemessung der Grundsteuer regelt das Gesetz auch das von Finanzamt und Gemeinden zu beachtende Verfahren sowie die Datenschutzaufsicht. Gemäß Art. 10 Abs. 2 Satz 2 BayGrStG überwache ich die staatlichen Finanzbehörden und die Gemeinden bei der Verwaltung der bayerischen Grundsteuer. Die Vorschrift lautet:

„[2]§ 32h AO gilt mit der Maßgabe, dass der Landesbeauftragte für den Datenschutz zuständig und das Bayerische Datenschutzgesetz einschlägig ist."

8.1.1 Bisher: Aufsichtszuständigkeit nach § 32h Abs. 1 Satz 1 Abgabenordnung

Übergangsweise bis einschließlich 2024 wird die Grundsteuer weiterhin nach den bisherigen bundesgesetzlichen Regelungen erhoben (vgl. Art. 10 Abs. 1 Satz 2 BayGrStG). Insoweit ist für die Datenschutzaufsicht gemäß § 32h Abs. 1 Satz 1 AO weiterhin der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständig. Dabei macht es keinen Unterschied, ob die staatlichen Finanzbehörden (Feststellung des Grundsteuer-Messbetrags) oder die Gemeinden (Erlass des Grundsteuerbescheids) handeln.

Für die Finanzämter folgt die Zuständigkeit des Bundesbeauftragten unmittelbar aus § 32h Abs. 1 Satz 1 AO. Demnach überwacht der Bundesbeauftragte die Finanzbehörden von Bund und Ländern im Anwendungsbereich der Abgabenordnung. Das ist gemäß § 1 Abs. 1 AO bei der Verwaltung europa- oder bundesgesetzlich geregelter Steuern, mithin auch beim Vollzug des vorübergehend noch anzuwendenden Grundsteuergesetzes des Bundes der Fall.

Was die Gemeinden betrifft, folgt die Zuständigkeit des Bundesbeauftragten aus § 1 Abs. 2 Nr. 1 AO. Da die Grundsteuer eine Realsteuer ist (vgl. § 3 Abs. 2 AO), gilt nach § 1 Abs. 2 Nr. 1 AO die in § 32h AO geregelte Datenschutzaufsicht durch den Bun-

[73] Bundesverfassungsgericht, Urteil vom 10. April 2018, 1 BvL 11/14 u. a., BeckRS 2018, 4904.

desbeauftragten „sinngemäß“; § 32h AO kann nur „sinngemäß“ gelten, weil die Gemeinden nicht, wie § 32h Abs. 1 Satz 1 AO eigentlich voraussetzt, Finanzbehörden im Sinne der Abgabenordnung sind (vgl. § 6 AO). Gemäß § 1 Abs. 2 AO sind sie aber wie Finanzbehörden zu behandeln.

Hätte der Bundesgesetzgeber die partielle Datenschutzaufsicht des Bundesbeauftragten über die Gemeinden ausschließen wollen, hätte er die Regelung zur Datenschutzaufsicht nicht in den Katalog der für die Gemeinden geltenden Vorschriften der Abgabenordnung aufnehmen dürfen. Dann wäre es selbstverständlich, dass die Gemeinden bei der Verwaltung der Grundsteuer datenschutzrechtlich – wie üblich – als öffentliche Stellen der Länder behandelt werden und der Datenschutzaufsicht auf Landesebene unterliegen.

8.1.2 Neuregelung nach dem Bayerischen Grundsteuergesetz

Auch wenn die Grundsteuer nach dem Bayerischen Grundsteuergesetz erst ab 2025 erhoben wird, hat die staatliche Finanzverwaltung mit der Ermittlung der Besteuerungsgrundlagen nach dem neuen Recht bereits begonnen. Schon jetzt stellen sich daher auch praktische Fragen bei der Aufsichtszuständigkeit.

Ich begrüße es, dass mit Art. 10 Abs. 2 Satz 2 BayGrStG die Aufsichtszuständigkeit entgegen § 32h AO zu mir zurückkehren soll. Allerdings bezweifle ich, dass der bayerische Gesetzgeber aufgrund der Befugnis, gemäß Art. 72 Abs. 3 Satz 1 Nr. 7 GG vom Grundsteuermodell des Bundes abzuweichen, auch die Aufsichtszuständigkeit gänzlich eigenständig regeln konnte.

Nach meiner Einschätzung trägt die Befugnis zur Abweichung von den Grundsteuervorschriften des Bundes, auf die ausweislich der Gesetzesbegründung das gesamte Bayerische Grundsteuergesetz gestützt ist,[74] die in Art. 10 Abs. 2 Satz 2 BayGrStG enthaltene Zuständigkeitszuweisung nicht. Gleichwohl sehe ich mich zumindest teilweise für die Datenschutzaufsicht bei der Verwaltung der bayerischen Grundsteuer als zuständig an. Nach meiner Auffassung sind hier drei Konstellationen zu unterscheiden. Bevor ich näher darauf eingehe, möchte ich aber bemerken, dass die nachfolgenden Ausführungen unter dem Vorbehalt der verfassungsgerichtlichen Klärung einiger grundlegender Fragen der noch vergleichsweise jungen Abweichungsgesetzgebung nach Art. 72 Abs. 3 GG stehen.

8.1.2.1 Verwaltung der Grundsteuer B durch die Finanzämter

Für die Grundsteuer B („baulich“, betrifft Grundvermögen und Grundstücke, im Gegensatz zur Grundsteuer A, „agrarisch“, betrifft Land- und Forstwirtschaft) enthält das Bayerische Grundsteuergesetz in Art. 1 bis 5 BayGrStG detaillierte Regelungen, die sich vom Bundesmodell erheblich unterscheiden. Die bayerische Grundsteuer B wird flächenabhängig berechnet. Anders als im Bundesmodell fließt der Grundstückswert nicht in die Berechnung ein.

Ist die Grundsteuer B folglich als landesrechtliche Steuer anzusehen, ist die Abgabenordnung nicht unmittelbar anwendbar, da sie für die staatlichen Finanzbehörden gemäß § 1 Abs. 1 Satz 1 AO nur gilt, „soweit“ sie bundes- oder europarechtliche Steuern verwalten. Das wiederum hätte zu Folge, dass auch § 32h Abs. 1 AO, der die Auf-

74 Vgl. Landtags-Drucksache 18/15755, S. 1.

sichtszuständigkeit des Bundesbeauftragten vorsieht, nicht anzuwenden wäre. Stattdessen müsste meine Zuständigkeit aus der allgemeinen Vorschrift des Art. 15 Abs. 1 Satz 1 BayDSG folgen. Danach überwache ich die Einhaltung des Datenschutzrechts bei bayerischen öffentlichen Stellen.

Daran ändert auch die in Art. 10 Abs. 2 Satz 1 BayGrStG angeordnete entsprechende Geltung der Abgabenordnung – als Landesrecht – nichts. Landesrechtlich kann die in § 32h Abs. 1 AO vorgesehene Zuständigkeit des Bundesbeauftragten nicht begründen werden, weil ein Landesgesetz dem Bund nur unter besonderen Voraussetzungen Aufgaben übertragen kann; diese Voraussetzungen (insbesondere eine Übernahme der Verwaltungskosten des Bundesbeauftragten durch den Freistaat) sind hier aber nicht gegeben (vgl. § 32h Abs. 3 AO).

Vor diesem Hintergrund halte ich Art. 10 Abs. 2 Satz 2 BayGrStG hinsichtlich der Verwaltung der Grundsteuer B durch die staatlichen Finanzbehörden jedenfalls für überflüssig, soweit er abweichend von Art. 15 Abs. 1 Satz 1 BayDSG meine Zuständigkeit im Wege einer entsprechenden Anwendung von § 32h AO bestimmt, der zudem nur modifiziert gelten soll. An die Stelle der in § 32h Abs. 1 Satz 2 AO angesprochenen §§ 13 bis 16 Bundesdatenschutzgesetz (BDSG) sollen die entsprechenden Vorschriften des Bayerischen Datenschutzgesetzes treten, das sich mit den in §§ 13 bis 16 BDSG geregelten Fragen allerdings allenfalls am Rande befasst. Einen Vorteil dieser umständlichen Konstruktion gegenüber einer Zuständigkeit nach Art. 15 Abs. 1 Satz 1 BayDSG kann ich daher nicht erkennen.

Nicht verschweigen will ich in diesem Zusammenhang, dass die Einordnung der Grundsteuer als landesgesetzliche Steuer auch anders gesehen werden kann. Insbesondere wird vertreten, dass nur eine landesrechtliche Vollregelung den Charakter der Grundsteuer als Landesgesetz begründen könne. Immer dann, wenn die vollständige Steuerregelung aus Bundes- und Landesrecht zusammengesetzt ist, soll die Abgabenordnung gemäß § 1 Abs. 1 AO anzuwenden sein, da die Finanzbehörden – zumindest auch – Bundesrecht anwenden.[75]

Eine Vollregelung in diesem Sinne enthält das Bayerische Grundsteuergesetz nicht; gemäß Art. 10 Abs. 1 Satz 1 BayGrStG sind bundesrechtliche Bestimmungen des Grundsteuergesetzes und des Bewertungsgesetzes ergänzend anzuwenden. Mit dem bayerischen Gesetzgeber nehme ich derzeit aber an, dass jedenfalls die Grundsteuer B nach dem Bayerischen Grundsteuergesetz als landesgesetzliche Steuer zu behandeln ist. Immerhin regelt das Bayerische Grundsteuergesetz die wesentlichen Aspekte der Grundsteuer B umfassend.

8.1.2.2 Verwaltung der Grundsteuer A durch die Finanzämter

Gemäß Art. 10 Abs. 2 Satz 2 BayGrStG bin ich auch für die Aufsicht über die Finanzbehörden bei der Verwaltung der die Land- und Forstwirtschaft betreffenden Grundsteuer A zuständig. Im Gegensatz zur Grundsteuer B soll die Grundsteuer A weiterhin im Wesentlichen nach den bundesgesetzlichen Vorgaben ermittelt werden. Art. 9 BayGrStG ergänzt diese um Details. Ob auf dieser Grundlage von einer eigenen bayerischen Grundsteuer A gesprochen werden kann, kann bezweifelt werden.

[75] Vgl. Krumm, in: Tipke/Kruse, Abgabenordnung/Finanzgerichtsordnung, Kommentar, Stand: 10/2022, § 1 AO Rn. 17a.

Dennoch vertrete ich derzeit die Auffassung, dass bei der bayerischen Grundsteuer insgesamt eine landesgesetzlich geregelte Steuer vorliegt. Dafür spricht eine Gesamtbetrachtung der Grundsteuer. Die Summe aus einer eigenständigen Regelung der Grundsteuer B und Abweichungen bei der Grundsteuer A verleiht der Grundsteuer insgesamt einen bayerischen Charakter.

Dann wenden die Finanzämter auch mit der Grundsteuer A kein Bundesrecht an, so dass – wie bei der Verwaltung der Grundsteuer B durch die Finanzämter – mangels Anwendbarkeit der Abgabenordnung eine Bundesaufsicht gemäß § 32h Abs. 1 AO ausscheidet. Auch hinsichtlich der Verwaltung der Grundsteuer A durch die Finanzämter sehe ich mich deshalb auf der Grundlage von Art. 10 Abs. 2 Satz 2 BayGrStG für die Datenschutzaufsicht als zuständig an. Noch mehr als bei der Grundsteuer B halte ich allerdings eine andere Betrachtungsweise, nämlich die Grundsteuer A weiterhin als im Sinne von § 1 Abs. 1 AO bundesgesetzlich geregelt anzusehen, für ebenso gut vertretbar.

8.1.2.3 Verwaltung der Grundsteuer durch die Gemeinden

Schwierigkeiten bereitet mir die in Art. 10 Abs. 2 Satz 2 BayGrStG vorgesehene Zuständigkeit für die Datenschutzaufsicht über die Gemeinden. Bei den Gemeinden kommt es für die Geltung der Abgabenordnung einschließlich § 32h AO nur darauf an, ob sie Realsteuern (Grund- oder Gewerbesteuer, vgl. § 3 Abs. 2 AO) verwalten oder nicht, vgl. § 1 Abs. 2 AO. Anders als bei den Finanzbehörden ist es nicht entscheidend, ob es um eine europa- und bundesgesetzlich geregelte Steuer geht. Die Abgabenordnung kann – unmittelbar, nicht als Landesrecht – auch gelten, wenn die Gemeinden ein Landessteuergesetz anwenden.

Vor diesem Hintergrund halte ich die Abgabenordnung in dem in § 1 Abs. 2 AO genannten Umfang grundsätzlich für anwendbar. Das schließt § 32h AO ein, auch wenn hinterfragt werden kann, ob diese Vorschrift als solche den verfassungsrechtlichen Anforderungen entspricht (siehe hierzu meine Ausführungen im 28. Tätigkeitsbericht 2018 unter Nr. 10.1.6). Solange die Vorschrift in der Abgabenordnung enthalten ist, ist sie als gültig anzusehen.

Demnach wäre auch bei der bayerischen Grundsteuer der Bundesbeauftragte für die Datenschutzaufsicht bei den Gemeinden zuständig, da sich Bundesrecht (§ 32h AO) gegen Landesrecht (Art. 10 Abs. 2 Satz 2 BayGrStG) grundsätzlich durchsetzt (vgl. Art. 31 GG). Anderes könnte nur gelten, wenn der Landesgesetzgeber auch von den Vorschriften der Abgabenordnung abweichen dürfte.

Insofern ist zu beachten, dass das Grundgesetz dem Bund die Regelung des Verfahrens der Gemeinden bei der Grundsteuer auch für den Fall gestattet, dass es um die Anwendung eines Landesgesetzes geht (vgl. Art. 108 Abs. 5 Satz 2 GG).[76] Die Gesetzgebungskompetenzen für steuerliche und sonstige Vorschriften können daher auseinanderfallen. Eine steuerliche Regelung liegt vor, soweit sich ein Gesetz mit Fragen von Steuersubjekt, Steuerobjekt, Bemessungsgrundlage, Bewertung und Tarif befasst. Dagegen zählen zum Verfahren die Art und Weise der Ausführung von Gesetzen, die Prüfung von Entscheidungen sowie verwaltungsinterne Mitwirkungs- und Kontrollvorgänge.

[76] Vgl. zum Beispiel Schwarz, in: Dürig/Herzog/Scholz, Grundgesetz-Kommentar, Stand 3/2022, Art. 108 Rn. 59 ff.; Kube, in: Beck'scher Online-Kommentar Grundgesetz, Stand 11/2022, Art. 108 Rn. 23.

Nach meiner Auffassung gestattet Art. 72 Abs. 3 Satz 1 Nr. 7 GG den Ländern nur Abweichungen von den grundsteuerlichen Regelungen des Bundes. Soweit der Bund von seiner entsprechenden Gesetzgebungskompetenz (Art. 105 Abs. 2 Satz 1 GG) Gebrauch gemacht hat, können die Länder durch eigene Regeln davon abweichen. Das betrifft in erster Linie das Grundsteuergesetz und das Bewertungsgesetz und die Entscheidung für ein bestimmtes Grundsteuermodell. Von anderen Vorschriften des Bundes kann nach meiner Einschätzung im Wege der Abweichungsgesetzgebung nur abgewichen werden, soweit es zur Durchsetzung des eigenen Grundsteuermodells erforderlich ist.

§ 32h AO beruht weder auf einem Gesetz des Bundes zur Regelung der Grundsteuer, noch betrifft die Regelung der Datenschutzaufsicht eine grundsteuerspezifische Frage. Die Bestimmung der zuständigen Datenschutzaufsichtsbehörde ist für die Einführung eines eigenen bayerischen Grundsteuermodells aus meiner Sicht nicht relevant. Auch der Bund könnte § 32h AO nicht auf seine Kompetenz zur Regelung der Grundsteuer (Art. 105 Abs. 2 Satz 1 GG) stützen. Damit scheidet diese Vorschrift als Gegenstand einer grundsteuerlichen Abweichungsgesetzgebung durch die Länder wohl aus.

Dann fehlt es aber an einer Rechtsgrundlage, die dem bayerischen Gesetzgeber eine Abweichung von § 32h AO gestatten würde. Die Gesetzgebungskompetenz für § 32h AO wird teilweise in Art. 108 Abs. 5 GG gesehen, der dem Bund die Regelung des Verfahrens erlaubt, teilweise in Art. 87 Abs. 3 GG, der die Errichtung von obersten Bundesbehörden wie den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit betrifft. Beide Vorschriften kennen keine Abweichungsbefugnis für die Länder. Somit bleibt es aus meiner Sicht beim Vorrang des Bundesrechts (§ 1 Abs. 2 Nr. 1 in Verbindung mit § 32h Abs. 1 Satz 1 AO) vor entgegenstehendem Landesrecht (Art. 10 Abs. 2 Satz 2 BayGrStG) – und somit bei der Zuständigkeit des Bundesbeauftragten für die Datenschutzaufsicht bei den Gemeinden, wenn es um Verarbeitungen personenbezogener Daten bei der Verwaltung der Grundsteuer geht.

8.1.3 Vorläufige Bewertung und Ausblick

Den im Jahr 2018 in Kraft getretenen § 32h AO betrachte ich seit jeher - und auch weiterhin unverändert - sehr kritisch (vgl. dazu meinen 28. Tätigkeitsbericht 2018 unter Nr. 10.1). Ich bin der Auffassung, dass auch die bayerischen Finanzbehörden und Gemeinden von einer ungeteilten Datenschutzaufsicht profitieren sollten. Dennoch habe ich mich im Gesetzgebungsverfahren zum Bayerischen Grundsteuergesetz ausdrücklich gegen die Vorschrift des Art. 10 Abs. 2 Satz 2 BayGrStG ausgesprochen. Aus den oben dargelegten Gründen halte ich diese Regelung für sachlich entbehrlich, rechtlich problematisch und – mit Blick auf die Verweisung in das Bayerische Datenschutzgesetz – für teilweise unverständlich.

Soweit die Abgabenordnung nicht anwendbar ist, wäre ich gemäß Art. 15 Abs. 1 Satz 1 BayDSG auch unabhängig von Art. 10 Abs. 2 Satz 2 BayGrStG zuständig. Und soweit die Abgabenordnung – nach meiner Auffassung jedenfalls für die Gemeinden – gemäß § 1 Abs. 2 AO als Bundesrecht anwendbar ist, kann sich der bayerische Gesetzgeber darüber nicht im Wege der grundsteuerlichen Abweichungsgesetzgebung hinwegsetzen und die entsprechende Anwendung der Abgabenordnung als Landesrecht mit einem modifizierten § 32h AO anordnen. Entsprechendes würde hinsichtlich der Finanzämter gelten, falls die Grundsteuer aufgrund der Anwendung von grundsteuerlichen Regeln des Bundes neben dem Bayerischen Grundsteuergesetz in den Anwendungsbereich von § 1 Abs. 1 AO fiele.

Da ich mich an die Vorgaben des bayerischen Gesetzgebers gleichwohl gebunden fühle und die Einschätzung des bayerischen Gesetzgebers, die Grundsteuer sei eine Landessteuer, für gut vertretbar halte (siehe oben Nr. 8.1.2), habe ich mit Blick auf Art. 10 Abs. 2 Satz 2 BayGrStG begonnen, die Datenschutzaufsicht über die Verwaltung der bayerischen Grundsteuer durch die Finanzbehörden auszuüben.

Ab dem Jahr 2025, wenn die bayerische Grundsteuer erstmals erhoben wird, werden auch die Gemeinden durch den Erlass von Grundsteuerbescheiden aktiv. Dann könnte sich die oben angesprochene Frage nach der Verfassungsmäßigkeit des § 32h AO – soweit er über § 1 Abs. 2 Nr. 1 AO für die Gemeinden gilt – für die bayerische Grundsteuer konkret stellen. Möglicherweise ist aber auch Art. 10 Abs. 2 Satz 2 BayGrStG einschränkend dahingehend auszulegen, dass er nur die Aufsicht über die Finanzbehörden bei der Verwaltung der Grundsteuer betrifft. Bis zum Jahr 2025 ist noch genügend Zeit, bestehende Unklarheiten auszuräumen.

Wenn der bayerische Gesetzgeber meine Aufsichtsbefugnisse im Steuerbereich tatsächlich stärken möchte, wäre aus meiner Sicht eine Initiative zur Änderung der Abgabenordnung die vorrangig zu ergreifende Maßnahme. Auch wenn eine Änderung des verfassungsrechtlich höchst bedenklichen § 32h AO wohl mangels bundesweiten Interesses an einer Rückübertragung der Aufsichtsbefugnisse über die Finanzbehörden auf die Landesbeauftragten wohl kaum durchzusetzen ist, wäre für den Bereich der Grundsteuer schon viel gewonnen, wenn die „Datenschutzaufsicht“ aus § 1 Abs. 2 Nr. 1 AO gestrichen würde. Dann wäre § 32h AO, der ausdrücklich auf Finanzbehörden im Sinne von § 6 AO abstellt, für die Gemeinden von vornherein nicht anwendbar, und ich wäre bei der Verwaltung der bayerischen Grundsteuer ohne jeden Zweifel für die Gemeinden zuständig. Aktuell wird das letztlich durch die missglückte Vorschrift des § 32h AO bewirkte datenschutzrechtliche „Zuständigkeitschaos“ jedoch in der Tendenz noch weiter vergrößert.

8.2 Erste praktische Erfahrungen mit dem Bayerischen Grundsteuergesetz

Zum 1. Januar 2022 ist das Bayerische Grundsteuergesetz (BayGrStG) in Kraft getreten (vgl. dazu allgemein den Beitrag unter Nr. 8.1). Auch wenn die Grundsteuer nach diesem Gesetz erst ab dem Jahr 2025 erhoben wird, hat die Finanzverwaltung mit den Vorbereitungen zur Erhebung der bayerischen Grundsteuer bereits begonnen. Mehrere Millionen bayerische Grundeigentümerinnen und Grundeigentümer wurden aufgefordert, eine Grundsteuererklärung abzugeben.

8.2.1 Drei Fallgruppen von Datenschutzbeschwerden

Da Steuererklärungen personenbezogene Daten enthalten, sind sie naturgemäß datenschutzrelevant. Verglichen mit der schieren Masse an Grundsteuerfällen war die Anzahl der bei mir eingegangenen Datenschutzbeschwerden im Zusammenhang mit der bayerischen Grundsteuer bislang allerdings gering. Die Beschwerden können ganz überwiegend in drei Gruppen eingeteilt werden.

8.2.1.1 Namensverwechslungen

Eine erste Gruppe von Datenschutzbeschwerden betraf Namensverwechslungen. Aufgrund eines Programmierungsfehlers der Steuerverwaltung kam es in einigen Fällen vor, dass bei vollständiger oder teilweiser Namensgleichheit von Steuerpflichtigen (regelmäßig Vater und Sohn) die Aufforderung zur Abgabe der Steuererklärung

nicht an die Eigentümerin oder den Eigentümer des Grundstücks, sondern an die andere Namensträgerin oder den anderen Namensträger gerichtet war. Mitunter wurden auch Sohn und Mutter als Eigentümer und Eigentümerin ausgewiesen, obwohl das Grundstück dem Sohn und seiner Ehefrau gehörte.

In derartigen Konstellationen konnte der unzutreffende Eindruck entstehen, dass der – falsche – Empfänger der Aufforderung Eigentümerin oder Eigentümer eines Grundstücks war. In einem Fall befand sich der falsche Empfänger in einem Insolvenzverfahren und befürchtete, er könne verdächtigt werden, im Insolvenzverfahren einen erheblichen Vermögensbestandteil verschwiegen zu haben (Insolvenzstraftat nach § 283 Abs. 1 Nr. 1 Strafgesetzbuch).

Auf meine Intervention hin haben die Finanzämter die fehlerhaften Schreiben rasch korrigiert und den Sachverhalt den betroffenen Personen gegenüber klargestellt. Ich habe im Übrigen keine Kenntnis davon, dass eine solche Namensverwechslung in der Folge zu einem greifbaren Nachteil geführt hätte.

8.2.1.2 Angaben zu Wohnungseigentümergemeinschaften

Mehrere Beschwerden von Wohnungseigentümerinnen und Wohnungseigentümern betrafen die Aufforderung, Angaben zu den Mitgliedern einer Wohnungseigentümergemeinschaft zu machen. Die Beschwerdeführerinnen und Beschwerdeführer machten vor allem geltend, dass sie über Angaben zu diesen ihnen regelmäßig fremden Personen nicht verfügten, überdies nicht wüssten, wie sie diese Informationen beschaffen sollten, und das im Übrigen auch nicht einsähen.

Hier lag allerdings ein Missverständnis vor. Die Pflicht zur Angabe der Mitglieder der Wohnungseigentümergemeinschaft bezieht sich allein auf die Wohnung, für welche die Steuererklärung abzugeben ist. Nur für diese Wohneinheit schulden Miteigentümerinnen und Miteigentümer gemeinsam die Grundsteuer (vgl. § 10 Abs. 2 Grundsteuergesetz in Verbindung mit Art. 10 Abs. 1 Satz 1 BayGrStG). Angaben zu Eigentümerinnen und Eigentümern fremder Wohnungen, für die ausschließlich andere Personen grundsteuerpflichtig sind, verlangt die Finanzverwaltung dagegen nicht. Die Missverständnisse konnte ich rasch aufklären.

8.2.1.3 Angabe der Wohnfläche

Eine dritte Gruppe von Beschwerden betraf schließlich die Verpflichtung zur Angabe der Wohnfläche. Die Steuerpflichtigen machten geltend, das Finanzamt habe keine Befugnis, die Größe der einzelnen Räume einer Wohnung zu erfragen. Dem stimme ich allerdings nur mit Einschränkung zu. Da sich die Grundsteuer nach der Gebäudefläche richtet und bei Wohnnutzung die nach der Wohnflächenverordnung berechnete Wohnfläche maßgeblich ist, ist in der Steuererklärung zwar nicht die Größe der einzelnen Räume, regelmäßig aber die gesamte Wohnfläche anzugeben (vgl. Art. 2 Abs. 1 BayGrStG).

Dieser Vorgabe entsprachen allerdings auch die Hinweise der Finanzverwaltung zum Ausfüllen der Steuererklärung. Nur wenn das Finanzamt berechtigte Zweifel hat, ob die Angabe der Wohnfläche zutrifft, kann sie nach allgemeinen steuerverfahrensrechtlichen Regeln den Sachverhalt näher erforschen, wozu auch eine genaue Ermittlung der Wohnfläche zählen kann. Das ist aber kein spezifisch grundsteuerliches Datenschutzproblem, sondern betrifft die allgemeine Verpflichtung des Finanzamts zur rechtmäßigen Steuerfestsetzung nach den Regeln der Abgabenordnung.

8.2.2 Vorläufige Bewertung

Von der Fallgruppe der Namensverwechslungen abgesehen, beruhten die Datenschutzbeschwerden ganz überwiegend auf Missverständnissen hinsichtlich der in der Steuererklärung geforderten Angaben. Zur relativ geringen Anzahl der Beschwerden haben sicherlich die aus meiner Sicht durchaus gelungenen Ausfüllhinweise der bayerischen Finanzverwaltung im Internet beigetragen. Insoweit beurteile ich den Beginn der praktischen Einführung der bayerischen Grundsteuer aus Datenschutzsicht bislang im Grundsatz positiv.

Ich hoffe aber, dass bis zur tatsächlichen Erhebung der Grundsteuer nach dem Bayerischen Grundsteuergesetz und der damit verbundenen Einbindung der Gemeinden, die den Grundsteuerbescheid erlassen, meine unter Nr. 8.1 geäußerten Bedenken hinsichtlich meiner Aufsichtszuständigkeit beseitigt sind. Noch könnten diese Zweifel durch den Bundesgesetzgeber recht unkompliziert ausgeräumt werden.

8.3 Weitergabe von persönlichen Daten durch die Staatliche Lotterie- und Spielbankverwaltung

Ein leicht kurioser Beschwerdesachverhalt betraf im Berichtszeitraum mit der Staatlichen Lotterie- und Spielbankverwaltung einen Seitenzweig der staatlichen Finanzverwaltung.

Der Beschwerdeführer war Inhaber eines Kontos bei einer privaten Geschäftsbank. Ein Konto mit derselben Kontonummer wurde bei dieser Bank zuvor für einen Dritten geführt. Dieser Dritte war Kunde der Staatlichen Lotterie- und Spielbankverwaltung. Für sein dortiges Kundenkonto hatte er der Lotterie- und Spielbankverwaltung eine Lastschrifteinzugsermächtigung auf sein früheres Bankkonto erteilt.

Offenbar hatte aber der Dritte vergessen, der Lotterie- und Spielbankverwaltung anzuzeigen, dass er nicht mehr Inhaber des Bankkontos war. Da auch der Bank bei einem Lastschrifteinzug der zwischenzeitliche Wechsel des Kontoinhabers nicht aufgefallen war, wurde die monatliche Zahlung im Ergebnis von dem Beschwerdeführer für den Glücksspieler geleistet.

Nachdem der Beschwerdeführer der Lotterie- und Spielbankverwaltung das Versehen angezeigt hatte, wollte einer ihrer Beschäftigten für einen „unbürokratischen“ Zahlungsausgleich sorgen. Er informierte den Kunden und früheren Kontoinhaber über den Sachverhalt und leitete ihm Namen und Adresse des Beschwerdeführers mit der Bitte weiter, diesem den eingezogenen Betrag unter der allseits bekannten Kontonummer zu erstatten. Der Beschwerdeführer war mit der Weitergabe seiner Daten an den früheren Kontoinhaber allerdings nicht einverstanden und beschwerte sich deswegen bei mir.

Die Weitergabe personenbezogener Daten ist eine Datenverarbeitung im Sinne von Art. 4 Nr. 2 DSGVO. Jede Datenverarbeitung in diesem Sinne erfordert eine Rechtsgrundlage (vgl. Art. 6 DSGVO). Ohne wirksames Einverständnis der betroffenen Person dürfen bayerische öffentliche Stellen personenbezogene Daten an eine nicht öffentliche Stelle, wozu auch Privatpersonen zählen, nur übermitteln, wenn diese Stelle ein berechtigtes Interesse an der Kenntnis dieser Daten glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat (vgl. Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG). Diese Voraussetzungen waren hinsichtlich der Weitergabe der Daten des jetzigen an den früheren Kontoinhaber erkennbar

nicht erfüllt. Daher habe ich nach Art. 16 Abs. 4 Satz 1 BayDSG gegenüber der Staatlichen Lotterie- und Spielbankverwaltung eine förmliche datenschutzrechtliche Beanstandung ausgesprochen. Die Lotterie- und Spielbankverwaltung hat den Rechts- und Datenschutzverstoß im Rahmen der vorherigen Anhörung sofort eingeräumt und das Vorkommnis bedauert.

Aus welchen Gründen die Lotterie-und Spielbankverwaltung nach Aufklärung des Sachverhalts den eingezogenen Betrag nicht dem Beschwerdeführer erstattet und diese Summe bei ihrem Kunden nachgefordert hat, hat sich mir nicht erschlossen.

9 Personalverwaltung

9.1 Verarbeitung von COVID-19-Immunitätsnachweisen im Rahmen der einrichtungsbezogenen Impfpflicht

Fragen zur Verarbeitung von Beschäftigtendaten durch bayerische Dienstherren und öffentliche Arbeitgeber im Zusammenhang mit der COVID-19-Pandemie haben mich auch in diesem Berichtszeitraum wieder in erheblichem Umfang beschäftigt (vgl. zuletzt Nr. 8.1 meines 31. Tätigkeitsberichts 2021). Anlass für eine förmliche Flut an Beschwerden bildete dabei die **einrichtungsbezogene Impfpflicht** für bestimmte Berufsgruppen. Diese ist mit dem Gesetz zur Stärkung der Impfprävention gegen COVID-19 und zur Änderung weiterer Vorschriften im Zusammenhang mit der COVID-19-Pandemie[77] im Infektionsschutzgesetz (§ 20a IfSG a. F.) verankert worden. Einrichtungen und Unternehmen, die von dem Anwendungsbereich dieser Vorschrift erfasst sind, mussten Angaben zu einem Immunitätsschutz ihrer Beschäftigten gegen COVID-19 verarbeiten. Mit Ablauf des 31. Dezember 2022 ist die einrichtungsbezogene Impfpflicht nach § 20a IfSG a. F. wieder **außer Kraft** getreten.

9.1.1 Die einrichtungsbezogene Impfpflicht im Überblick

Nach § 20a Abs. 2 Satz 1 IfSG a. F. waren Personen, die in bestimmten Einrichtungen oder Unternehmen des Gesundheits- und Pflegebereichs (unter anderem in Krankenhäusern) tätig sind, verpflichtet, der Einrichtungs- oder Unternehmensleitung bis zum 15. März 2022 einen **Immunitätsnachweis gegen COVID-19** vorzulegen. Die gleiche Verpflichtung galt für Personen, die ab dem 16. März 2022 in diesen Einrichtungen tätig werden sollten (§ 20a Abs. 3 Satz 1 IfSG a. F.).

Als **Nachweise** kamen gemäß § 20a Abs. 2 Satz 1 IfSG a. F. in Betracht:

- ein Impfnachweis nach § 22a Abs. 1 IfSG (§ 20a Abs. 2 Satz 1 Nr. 1 IfSG a. F.),
- ein Genesenennachweis nach § 22a Abs. 2 IfSG (§ 20a Abs. 2 Satz 1 Nr. 2 IfSG a. F.),
- ein ärztliches Zeugnis über das Vorliegen einer Schwangerschaft im ersten Drittel (§ 20a Abs. 2 Satz 1 Nr. 3 IfSG a. F.) sowie
- ein ärztliches Zeugnis darüber, dass die betreffende Person auf Grund einer medizinischen Kontraindikation nicht gegen SARS-CoV-2 geimpft werden kann (§ 20a Abs. 2 Satz 1 Nr. 4 IfSG a. F.).

Wurde ein bereits vorgelegter Nachweis aufgrund Zeitablaufs **ungültig**, mussten betroffene Personen binnen Monatsfrist einen **neuen Nachweis** vorlegen (§ 20a Abs. 4 Satz 1 IfSG a. F.).

Für Einrichtungs- und Unternehmensleitungen bestanden in diesem Zusammenhang verschiedene **Benachrichtigungs- und Übermittlungspflichten** gegenüber

[77] Vom 10. Dezember 2021 (BGBl. I S. 5162).

dem jeweils zuständigen Gesundheitsamt. Diese Pflichten griffen etwa dann, wenn Nachweise nicht oder nicht rechtzeitig vorgelegt wurden (§ 20a Abs. 2 Satz 2 Var. 1, Abs. 4 Satz 2 Var. 1 IfSG a. F.) oder wenn Zweifel an der Echtheit oder inhaltlichen Richtigkeit der vorgelegten Nachweise bestanden (§ 20a Abs. 2 Satz 2 Var. 2, Abs. 3 Satz 2, Abs. 4 Satz 2 Var. 2 IfSG a. F.). Das Gesundheitsamt konnte dann nach § 20a Abs. 5 IfSG a. F. etwa eine ärztliche Untersuchung der betroffenen Person anordnen (§ 20a Abs. 5 Satz 2 IfSG a. F.) oder dieser gegebenenfalls ein Betretungs- oder Tätigkeitsverbot auferlegen (§ 20a Abs. 5 Satz 3 IfSG a. F.)

Zur Erfüllung der dargestellten Benachrichtigungs- und Übermittlungspflichten mussten Einrichtungs- und Unternehmensleitungen personenbezogene Daten der vorlagepflichtigen Personen verarbeiten. Das war zum einen der Fall bei der **Datenübermittlung** an die gesetzlich vorgesehenen Stellen, zum anderen im Rahmen der **Dokumentation**, dass ein Nachweis vorgelegt worden war. Die im Rahmen der Benachrichtigung des Gesundheitsamts erforderlichen Datenverarbeitungen waren grundsätzlich von Art. 6 Abs. 1 UAbs. 1 Buchst. c, Art. 9 Abs. 2 Buchst. i DSGVO in Verbindung mit – je nach Konstellation – § 20a Abs. 2 Satz 2, Abs. 3 Satz 2 oder Abs. 4 Satz 2 IfSG a. F. gedeckt. Die Dokumentation der Nachweisvorlage konnte im bayerischen öffentlichen Dienst – im Rahmen des Erforderlichen – grundsätzlich auf Art. 103 Bayerisches Beamtengesetz (BayBG) gestützt werden, der gemäß Art. 145 Abs. 2 BayBG im Grundsatz entsprechend auch für vertraglich Beschäftigte gilt.

9.1.2 Beschwerden und Anfragen zur einrichtungsbezogenen Impfpflicht

Die bei mir eingegangenen Beschwerden richteten sich ganz überwiegend gegen die einrichtungsbezogene **Impfpflicht als solche**. Insoweit wurde schon angezweifelt, ob eine Vorlage von Immunitätsnachweisen gegenüber bayerischen Dienstherren und öffentlichen Arbeitgebern zum Zwecke des Infektionsschutzes überhaupt erforderlich ist. Dies habe ich jeweils zum Anlass genommen, Beschwerdeführerinnen und Beschwerdeführern die Rechtslage in datenschutzrechtlicher Hinsicht ausführlich zu erläutern.

Eine ganze Reihe von Eingaben und Beratungsanfragen betraf die konkrete **Umsetzung** der einrichtungsbezogenen Impfpflicht in den jeweiligen Einrichtungen und Unternehmen des Gesundheits- und Pflegebereichs. Nähere datenschutzrechtliche Vorgaben hierzu enthielt § 20a IfSG a. F. allerdings nicht. Die oben genannten Verarbeitungsbefugnisse setzten zunächst voraus, dass die Verarbeitung personenbezogener Beschäftigtendaten durch den Dienstherrn oder öffentlichen Arbeitgeber zur Erreichung der gesetzlich vorgesehenen Zwecke **erforderlich** war. Aus dem allgemeinen Datenschutzrecht waren zudem insbesondere die **Grundsätze** der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO), der Speicherbegrenzung (Art. 5 Abs. 1 Buchst. e DSGVO) sowie der Integrität und Vertraulichkeit personenbezogener Daten (Art. 5 Abs. 1 Buchst. f DSGVO) zu beachten. Sind Daten im Sinne von Art. 9 DSGVO betroffen, verlangt Art. 8 Abs. 2 Satz 1 BayDSG ferner angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Personen. Im Rahmen der gesetzlichen Vorgaben verblieb Dienstherren und öffentlichen Arbeitgebern somit ein gewisser Umsetzungsspielraum.

In datenschutzrechtlicher Hinsicht wesentlich war dabei zunächst, dass betroffene Beschäftigte gesetzlich nur zur Vorlage, nicht hingegen zu einer Hinterlegung von Nachweisen verpflichtet waren. Die Aufbewahrung von **Kopien** der vorgelegten Nachweise – etwa in der Personalakte – war daher regelmäßig nicht erforderlich und damit **unzulässig**.

Ausreichend war vielmehr eine **Sichtprüfung** der Nachweise. In diesem Rahmen war festzustellen, ob die vorgelegten Nachweise den gesetzlichen Vorgaben (vgl. § 20a Abs. 2 Satz 1 IfSG a. F.) entsprachen. Ein zur Vorlage bei einem Dienstherrn oder öffentlichen Arbeitgeber bestimmtes **ärztliches Zeugnis** nach § 20a Abs. 2 Satz 1 Nr. 4 IfSG a. F. brauchte dabei sowohl nach dem Gesetzeswortlaut als auch nach der Gesetzesbegründung[78] keine konkreten Angaben – insbesondere keine Diagnosen – zum Grund der medizinischen Kontraindikation enthalten.

Dokumentiert werden durfte im Rahmen der Nachweisprüfung jedenfalls, dass und wann ein Nachweis vorgelegt worden war, sowie eine etwaige Gültigkeitsdauer des Nachweises; nach Ablauf der Gültigkeit war ein neuer Nachweis vorzulegen (§ 20a Abs. 4 Satz 1 IfSG a. F.).

Die Nachweise waren gegenüber der Leitung der jeweiligen Einrichtung oder des jeweiligen Unternehmens zu erbringen (vgl. § 20a Abs. 2 Satz 1, Abs. 3 Satz 1 IfSG a. F.). Die Einrichtungs- oder Unternehmensleitung konnte die mit der einrichtungsbezogenen Impfpflicht zusammenhängenden Aufgaben allerdings an geeignete Beschäftigte oder Dritte **delegieren** (vgl. auch § 2 Nr. 15a Buchst. a IfSG). Dabei war zu beachten, dass die Nachweis- und Vorlagepflicht nach § 20a IfSG a. F. letztlich eine „gesetzliche Tätigkeitsvoraussetzung" darstellte. Angaben zum Immunitätsschutz Beschäftigter waren in diesem Zusammenhang demnach grundsätzlich den Personalaktendaten im Sinne von § 50 Satz 2 Beamtenstatusgesetz (BeamtStG), Art. 103 ff. BayBG zuzuordnen. Daher war der mit der Überprüfung der Nachweise befasste **Personenkreis möglichst klein** zu halten. Da Personalaktendaten ferner nur durch Beschäftigte verarbeitet werden dürfen, die mit der Bearbeitung von Personalangelegenheiten betraut sind (Art. 103 Satz 2 BayBG), bot es sich insbesondere an, ausgewählte Beschäftigte der Personalstelle mit dieser Aufgabe zu beauftragen. Eine Delegation auf **unmittelbare Fachvorgesetzte** sollte hingegen **unterbleiben**, weil dadurch der mit der Überprüfung der Nachweise befasste Personenkreis regelmäßig (teils erheblich) erweitert worden wäre. Etwas anderes konnte allenfalls in Betracht kommen, wenn die öffentliche Stelle die Umsetzung ihrer gesetzlichen Pflichten im Rahmen der einrichtungsbezogenen Impfpflicht insbesondere aufgrund ihrer Größe oder Struktur nicht anderweitig gewährleisten konnte. Dies hatte der jeweilige Verantwortliche eigenständig zu prüfen.

Im Falle einer gesetzlich vorgesehenen **Benachrichtigungspflicht** (etwa nach § 20a Abs. 2 Satz 2 IfSG a. F.) durften Einrichtungs- oder Unternehmensleitungen neben dem Übermittlungsanlass (Nichtvorlage oder Zweifel an der Echtheit oder Richtigkeit des Nachweises) personenbezogene Daten höchstens im Umfang des § 2 Nr. 16 IfSG[79] (insbesondere Vor- und Zuname, Kontaktdaten) an das Gesundheitsamt übermitteln.

Bei der Umsetzung der einrichtungsbezogenen Impfpflicht hatten Verantwortliche die Anforderungen an die Datensicherheit – vor allem im Hinblick auf die Umsetzung geeigneter technischer und organisatorischer Maßnahmen – zu beachten (vgl. Art. 32 DSGVO, Art. 8 Abs. 2 Satz 1 BayDSG).

Nach Außerkrafttreten der einrichtungsbezogenen Impfpflicht mussten – und müssen auch weiterhin – Verantwortliche schließlich sicherstellen, dass in diesem Rahmen – etwa bei der Dokumentation der Nachweisprüfung – gespeicherte Beschäftigtendaten **gelöscht** werden, sobald eine weitere Aufbewahrung dieser Daten zu den

78 Vgl. Bundestags-Drucksache 20/188, S. 40.
79 Vgl. Bundestags-Drucksache 20/188, S. 40.

gesetzlich vorgesehenen Zwecken (einschließlich etwaiger Dokumentationspflichten) nicht mehr erforderlich ist.

9.1.3 Fazit

Im Zuge der einrichtungsbezogenen Impfpflicht mussten bayerische Dienstherren und öffentliche Arbeitgeber Angaben zum Immunitätsschutz ihrer Beschäftigten gegen COVID-19 in den betroffenen Einrichtungen verarbeiten. Bei diesen Angaben handelte es sich (auch) um Daten, die nach Art. 9 DSGVO besonders geschützt sind. Mit einer Verarbeitung dieser Daten durch Dienstherren und öffentliche Arbeitgeber gehen spezifische Risiken für Beschäftigte einher. Verantwortliche sahen sich demnach mit der Herausforderung konfrontiert, die einrichtungsbezogene Impfpflicht auch in datenschutzrechtlicher Hinsicht ordnungsgemäß umzusetzen.

Im Berichtszeitraum habe ich sowohl Verantwortliche als auch betroffene Beschäftigte intensiv zu dieser Thematik beraten. Dabei konnte ich – teils angestoßen durch Beschwerden von Beschäftigten – immer wieder datenschutzrechtliche Verbesserungen erreichen. Um Verantwortlichen und betroffenen Beschäftigten im Berichtszeitraum einen Leitfaden an die Hand zu geben, habe ich mich der einrichtungsbezogenen Impfpflicht auch umfassend in meinem **Arbeitspapier „Verarbeitung des COVID-19-Impfstatus im bayerischen öffentlichen Dienst“** gewidmet. Die jeweils maßgebliche Fassung dieses Arbeitspapiers war – und ist auch weiterhin – auf meiner Internetseite https://www.datenschutz-bayern.de in der Rubrik „Corona-Pandemie“ abrufbar.

9.2 Einwilligung im Beschäftigungsverhältnis

In einer eher ungewöhnlichen Konstellation stellte sich mir im Berichtszeitraum die Frage, unter welchen Voraussetzungen eine Anstalt des öffentlichen Rechts Dritten Auskunft über das Gehalt ihrer Beschäftigten erteilen darf.

Die Anstalt stellt bestimmten öffentlichen Amtsträgern Personal zur Verfügung. Diese öffentlichen Amtsträger beschäftigen auf privatrechtlicher Grundlage auch eigene Hilfskräfte, deren Verdienst regelmäßig das Gehalt übersteigt, das die Anstalt ihren Beschäftigten zahlen kann. Manche Amtsträger wollen nun das Gehalt des ihnen gestellten Personals der Anstalt aufstocken, um zwischen den eigenen und den überlassenen Beschäftigten Lohngleichheit herzustellen.

Zu diesem Zweck müssen die Amtsträger jedoch Kenntnis von der Vergütung erlangen, die bereits durch die Anstalt sichergestellt ist. Aus Sicht der Anstalt sprach nichts dagegen, die Gehaltsinformationen – ohne vorherige Einbindung oder auch nur Kenntnis ihrer eigenen Beschäftigten – an die jeweiligen Amtsträger zu übermitteln, da die Beschäftigen im Ergebnis nur begünstigt werden sollten. Die Übermittlung der individuellen Gehaltsinformationen sei zu Zwecken der Personalorganisation oder Personalverwaltung erforderlich und somit nach Art. 103 Satz 1 Bayerisches Beamtengesetz (BayBG) zulässig.

Dieser Einschätzung habe ich widersprochen. Ohne Einwilligung der betroffenen Beschäftigten ist die Übermittlung der individuellen Gehälter datenschutzrechtlich unzulässig. Das ergibt sich aus den Vorschriften des Personalaktenrechts:

Informationen über das Gehalt stehen mit dem Beschäftigungsverhältnis in einem unmittelbaren inneren Zusammenhang. Als Personalaktendaten im Sinne von § 50 Satz 2 Beamtenstatusgesetz unterliegen diese Informationen einem besonderen Schutz. Dieser Schutz ist in den Art. 104 ff. BayBG näher ausgestaltet und gilt nicht nur für Beamtinnen und Beamte, sondern auch für vertraglich Beschäftigte von juristischen Personen des öffentlichen Rechts, insbesondere von öffentlich-rechtlichen Anstalten (vgl. Art. 145 Abs. 2, Art. 1 Abs. 1 BayBG).

Das Datenschutzrecht verhindert die Aufstockung des Gehalts der Beschäftigten der Anstalt natürlich nicht. Allerdings dürfen Auskünfte aus der Personalakte an Dritte, zu denen auch die „aufstockungswilligen" Amtsträger gehören, eben nur mit Einwilligung der Beschäftigten erteilt werden, vgl. Art. 108 Abs. 4 Satz 1 BayBG.

Art. 108 BayBG
Übermittlung von Personalakten und Auskunft an nicht betroffene Personen
(1) Eine Übermittlung oder eine Auskunft aus der Personalakte an Behörden eines anderen Dienstherrn ist für die in Art. 103 Satz 1 genannten Zwecke nur mit Einwilligung des Beamten oder der Beamtin zulässig.
(2) Ohne Einwilligung des Beamten oder der Beamtin darf die Personalakte den zuständigen Behörden oder anderen Stellen übermittelt werden, soweit dies erforderlich ist
1. zur Erstellung ärztlicher Gutachten im Auftrag der personalverwaltenden Behörde oder der Pensionsbehörde,
2. für die Festsetzung, Berechnung und Rückforderung der Besoldung, der Versorgung oder für die Prüfung der Kindergeldberechtigung,
3. für die Prüfung und Durchführung der Buchung von Einzahlungen von den Betroffenen oder von Auszahlungen an die Betroffenen oder
4. für die Durchführung von Auswertungen für anonymisierte Statistik- und Berichtszwecke und deren Abruf.
(3) […]
(4) [1]Auskünfte an Dritte dürfen nur mit Einwilligung des Beamten oder der Beamtin erteilt werden, es sei denn, dass die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz berechtigter, höherrangiger Interessen des Dritten die Auskunftserteilung zwingend erfordert. [2]Inhalt und Empfänger der Auskunft sind dem Beamten oder der Beamtin schriftlich mitzuteilen.
(5) [1]Ohne Einwilligung des Beamten oder der Beamtin können den zuständigen Behörden Auskünfte aus der Personalakte erteilt werden, soweit dies im Einzelfall
1. zu den in Abs. 2 genannten Zwecken,
2. zur Entscheidung über die Verleihung von staatlichen Orden, Ehrenzeichen oder sonstigen staatlichen Ehrungen oder
3. im Rahmen der Art. 8a bis 8e BayVwVfG zwingend
erforderlich ist. [2]Soweit eine Auskunft für die in Abs. 2 genannten Zwecke ausreichend ist, unterbleibt eine Übermittlung.
(6) […]
(7) [1]Übermittlung und Auskunft sind auf den jeweils erforderlichen Umfang zu beschränken. [2]Ein automatisierter Datenabruf durch andere Behörden ist unzulässig, soweit durch besondere Rechtsvorschrift nichts anderes bestimmt ist.

Eine datenschutzrechtliche Einwilligung muss gewisse, in Art. 4 Nr. 11 und Art. 7 DSGVO aufgestellte Voraussetzungen erfüllen, insbesondere freiwillig erklärt werden, vgl. Art. 7 Abs. 4 DSGVO. Wegen des typischen Machtungleichgewichts im Beschäftigungsverhältnis sind hier an die Beurteilung der Freiwilligkeit der Einwilligung grundsätzlich strenge Anforderungen zu stellen (vgl. Erwägungsgrund 43 DSGVO).

Einwilligungen im Beschäftigungsverhältnis werden oft erteilt, weil die Beschäftigten andernfalls berufliche Nachteile befürchten. Typische Beispiele betreffen Einwilligungen in die Veröffentlichung von Beschäftigtenfotos (siehe hierzu meinen 27. Tätigkeitsbericht 2016 unter Nr. 11.5), in den Einsatz von Ortungsdiensten in Dienstfahrzeugen (siehe dort Nr. 11.4) oder in die Teilnahme an Evaluierungsmaßnahmen (siehe bereits meinen 20. Tätigkeitsbericht 2002 unter Nr. 20.2.1).

Auch wenn die Freiwilligkeit einer Einwilligung häufig nur schwer nachweisbar ist, besteht im vorliegenden Fall die Besonderheit, dass die Übermittlung der Gehaltsdaten für die betroffenen Beschäftigten ganz eindeutig vorteilhaft ist. Sie sollen einen Zuschlag auf ihr Gehalt bekommen, ohne eine weitere Gegenleistung erbringen zu müssen. Das typische Machtungleichgewicht des Beschäftigungsverhältnisses wirkt sich hier also nicht zulasten der Beschäftigten aus, so dass eine wirksame Einwilligung in die Übermittlung der Gehaltsdaten möglich ist.

Ergänzend habe ich die Anstalt darauf hingewiesen, dass sie, wenn sie auf dieser Grundlage das Gehalt mitteilt, die betroffenen Beschäftigten schriftlich über Inhalt und Empfänger der Auskunft zu informieren hat (vgl. Art. 108 Abs. 4 Satz 2 BayBG); auch muss die Anstalt einen Abdruck dieser Mitteilung zur Personalakte nehmen.

9.3 Verdeckte Tonaufzeichnung einer Videokonferenz

Als Folge der Corona-Pandemie ist der Einsatz von Videokonferenzsystemen auch bei bayerischen öffentlichen Stellen zunehmend verbreitet. Dadurch werden allerdings auch neue datenschutzrechtliche Problemkonstellationen hervorgerufen. So erreichte mich beispielsweise im Berichtszeitraum eine Beschwerde, die eine verdeckte Tonaufzeichnung einer Videokonferenz von Beschäftigten einer bayerischen öffentlichen Stelle betraf. Im Zuge der Sachverhaltsermittlung und -bewertung musste ich gravierende Datenschutzverstöße feststellen:

9.3.1 Sachverhalt

Die Beschwerdeführerin hatte einen kritischen Beitrag auf einer allen Beschäftigten zugänglichen internen Kommunikationsplattform ihres Arbeitgebers verfasst. Daraufhin wurde sie zu einer Führungskräftebesprechung geladen, die als Videokonferenz durchgeführt wurde. Da die Protokollführerin im Verlauf der Besprechung den Raum verlassen musste, startete sie vor Verlassen des Raums mit dem Diensthandy eine **Tonaufzeichnung der Videokonferenz, allerdings ohne die Teilnehmenden davor darauf hinzuweisen**. Stattdessen erhielt die Beschwerdeführerin von der Tonaufzeichnung Kenntnis, als sie in dem ihr übersandten Protokoll im Verlauf den Hinweis „Ab jetzt Wortprotokoll“ und zudem eine Korrekturanmerkung ihres Vorgesetzten entdeckte, mit der die Protokollführerin zum „Nachhören“ aufgefordert wurde. Nach der Fertigstellung des Protokolls **löschte die Protokollführerin die Aufzeichnung**, ohne sie davor weiteren Personen zugänglich gemacht zu haben.

In der Folge wandte sich die Beschwerdeführerin an mich. Daraufhin ersuchte ich die öffentliche Stelle um eine Stellungnahme. Dabei wollte ich insbesondere wissen, auf welche Rechtsgrundlage die Aufzeichnung der Videokonferenz auf einen Tonträger und das wiederholte Abhören gestützt und weshalb eine solche Aufzeichnung überhaupt für erforderlich gehalten wurde.

9.3.2 Rechtliche Würdigung

Die öffentliche Stelle führte mir gegenüber aus, die Protokollierung einer Führungskräftebesprechung **sei für ihre Aufgabenerfüllung wesentlich** und daher nach Art. 4 Abs. 1 BayDSG zulässig. Daneben komme als Grundlage für Protokollaufzeichnungen die **Einwilligung** nach Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO sowie ein **berechtigtes Interesse** nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO in Betracht, wobei die öffentliche Stelle zugleich einräumte, dass eine Zustimmung zur Aufzeichnung des Gesprächs von allen Gesprächsteilnehmenden nicht eingeholt worden sei.

Diesen Ausführungen konnte ich mich nicht anschließen:

Die öffentliche Stelle verarbeitete im Rahmen der Aufzeichnung der Besprechung personenbezogene Daten der Beschwerdeführerin. Eine solche Datenverarbeitung bedarf einer **Rechtsgrundlage** im Sinne des Art. 6 Abs. 1 DSGVO.

Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO erlaubt die Datenverarbeitung für den Fall, dass diese **zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich** ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Allerdings ist in diesem Zusammenhang die **Einschränkung** des Art. 6 Abs. 1 UAbs. 2 DSGVO zu beachten, wonach die Rechtsgrundlage des Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO nicht herangezogen werden kann, wenn **Behörden die Daten in Erfüllung ihrer Aufgaben verarbeiten**. Dies war, wie die öffentliche Stelle selbst ausführte, hier der Fall. Ein Rückgriff auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO schied demnach aus.

Art. 6 DSGVO
Rechtmäßigkeit der Verarbeitung
(1) [1]Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
[…]
f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.
[…]
[2]Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.
[…]

Nach Art. 4 Abs. 1 BayDSG kann eine Verarbeitung personenbezogener Daten durch bayerische öffentliche Stellen zulässig sein, wenn und soweit die Verarbeitung **zur Aufgabenerfüllung der öffentlichen Stelle erforderlich** ist.

Art. 4 BayDSG
Rechtmäßigkeit der Verarbeitung
(zu Art. 6 Abs. 1 bis 3 DSGVO)
(1) Die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle ist unbeschadet sonstiger Bestimmungen zulässig, wenn sie zur Erfüllung einer ihr obliegenden Aufgabe erforderlich ist.
[…]

Dabei ist stets auch der **Grundsatz der Datenminimierung** (vgl. Art. 5 Abs. 1 Buchst. c DSGVO) zu beachten; die Datenverarbeitung ist auf das absolut notwendige Maß zu beschränken. Dies bedeutet insbesondere, dass die Menge an zu verarbeitenden Daten in der Weise zu begrenzen ist, dass (zusätzliche) Daten nicht verarbeitet werden dürfen, wenn der Verarbeitungszweck auch ohne sie erreicht werden kann.

In diesem Zusammenhang ist zu berücksichtigen, dass bei einer **Aufzeichnung** der Besprechung mittels Diensthandy personenbezogene Daten von Gesprächsbeteiligten **in einem erheblich größeren Umfang** verarbeitet werden, als dies bei einer – gegebenenfalls auch detaillierten – Niederschrift des Inhalts von Redebeiträgen durch eine anwesende Person der Fall ist. Dies folgt schon daraus, dass bei einer Tonaufzeichnung Äußerungen nicht nur ihrem Inhalt nach, sondern auch so, wie sie getätigt worden sind – einschließlich des genauen Wortlauts, der Stimmen sowie eines etwaigen Zögerns der jeweiligen Gesprächsbeteiligten –, festgehalten werden. Noch weitere, zusätzliche Daten werden darüber hinaus freilich verarbeitet, wenn eine Videokonferenz auch im Hinblick auf die visuelle Komponente aufgezeichnet wird – für Letzteres lagen mir allerdings keine Anhaltspunkte vor.

Hiernach kann zwar die Protokollierung einer Führungskräftebesprechung grundsätzlich auf Art. 4 Abs. 1 BayDSG gestützt werden. An der **Erforderlichkeit** einer Gesprächsaufzeichnung mittels Diensthandy **fehlt** es in diesem Zusammenhang jedoch: Wie aus dem Protokoll hervorgeht, fertigte die Protokollführerin zunächst ein **detailliertes Verlaufsprotokoll** an. Erst als ihr eine weitere Protokollierung nicht mehr möglich war, begann die Protokollführerin mit der Aufzeichnung der Besprechung mittels Diensthandy, was zu einem **Wortprotokoll** führte. Dies belegt bereits, dass insgesamt ein detailliertes Verlaufsprotokoll zur Aufgabenerfüllung der öffentlichen Stelle genügt hätte. Während der Abwesenheit der Protokollführerin hätte daher entweder die Besprechung unterbrochen oder die Protokollführung auf eine andere Person übertragen werden müssen.

Da es an der Erforderlichkeit der Aufzeichnung fehlte, konnte die öffentliche Stelle die Verarbeitung personenbezogener Daten der Beschwerdeführerin nicht auf Art. 4 Abs. 1 BayDSG stützen. Ohnehin ist fraglich, ob der allgemeine datenschutzrechtliche Auffangverarbeitungstatbestand des Art. 4 Abs. 1 BayDSG überhaupt derart weitreichende Eingriffe in die Rechte der Beteiligten, wie sie mit der Aufzeichnung von Besprechungen einhergehen, zu legitimieren vermag. Aus dem gleichen Grund kam auch eine Rechtfertigung durch Art. 103 Satz 1 in Verbindung mit Art. 145 Abs. 2 Bayerisches Beamtengesetz nicht in Betracht.

Die von der öffentlichen Stelle als mögliche Rechtsgrundlage genannte **Einwilligung** ist zwar nach Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO eine mögliche Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Sie muss aber, um wirksam zu sein, **freiwillig** erklärt werden (vgl. Art. 4 Nr. 11, Art. 7 Abs. 4 DSGVO). Dazu hätte eine echte Wahlmöglichkeit hinsichtlich der Aufzeichnung bestehen müssen (vgl. Erwägungsgrund 42 DSGVO). Im **Beschäftigungsverhältnis** sind an die Freiwilligkeit strenge Anforderungen zu stellen. Das typische **Machtungleichgewicht** (vgl. Erwägungsgrund 43 DSGVO) zwischen öffentlichen Arbeitgebern und Beschäftigten schließt eine wirksame Einwilligung in der Regel aus (zu einem seltenen Ausnahmefalle siehe Nr. 9.2). Im vorliegenden Fall fehlte nicht nur eine Nachfrage seitens des Arbeitgebers, sodass bereits die Möglichkeit, einzuwilligen, nicht eröffnet war; vielmehr wurde die Aufzeichnung sogar verdeckt herbeigeführt.

Im Übrigen müssen personenbezogene Daten gemäß Art. 5 Abs. 1 Buchst. a DSGVO in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden

(**Grundsatz der Transparenz**). Zur Verwirklichung dieses Transparenzgrundsatzes dienen insbesondere die **Informationspflichten** gemäß Art. 13 und 14 DSGVO, wonach die betroffene Person unter anderem über Existenz und Zwecke eines Verarbeitungsvorgangs unterrichtet werden muss (vgl. Erwägungsgrund 60 Satz 1 DSGVO).

Der Verwirklichung des Transparenzgedankens dient auch der **Direkterhebungsgrundsatz** nach Art. 4 Abs. 2 Satz 1 BayDSG: Hiernach sind personenbezogene Daten grundsätzlich bei der betroffenen Person und **mit ihrer Kenntnis** zu erheben. Für das Vorliegen eines Ausnahmefalls von diesem Grundsatz nach Art. 4 Abs. 2 Satz 4 in Verbindung mit Abs. 2 Satz 2 Nr. 1 und 2 BayDSG waren keine Anhaltspunkte ersichtlich. Indem die öffentliche Stelle die Beschwerdeführerin nicht über die Aufzeichnung der Besprechung mittels Diensthandy in Kenntnis setzte, verstieß sie somit auch gegen die Grundsätze der Transparenz gemäß Art. 5 Abs. 1 Buchst. a DSGVO und der Direkterhebung gemäß Art. 4 Abs. 2 Satz 1 BayDSG und ließ die Informationspflichten nach Art. 13 Abs. 1 und 2 DSGVO unerfüllt.

Da es sich gleich um mehrere Datenschutzverstöße von erheblichem Gewicht handelte, habe ich in der Folge das geschilderte Vorgehen der öffentlichen Stelle nach Art. 16 Abs. 4 Sätze 1 und 2 BayDSG förmlich datenschutzrechtlich **beanstandet**.

9.4 Einsatz von Ortungssystemen in Dienstfahrzeugen zur Dienstaufsicht

Im Berichtszeitraum erhielt ich davon Kenntnis, dass eine bayerische Kommune in Dienstfahrzeugen satellitengestützte GPS-Ortungssysteme verwendete und somit personenbezogene Beschäftigtendaten verarbeitete. Allgemein habe ich mich zur Zulässigkeit der Ausstattung von Dienstfahrzeugen mit Ortungssystemen bereits in meinem 27. Tätigkeitsberichts 2016 unter Nr. 11.4 geäußert; an diesen Ausführungen halte ich auch nach Geltungsbeginn der Datenschutz-Grundverordnung im Wesentlichen fest. Der vorliegende Fall erforderte jedoch eine intensive Auseinandersetzung mit den Grenzen der Zulässigkeit der Verarbeitung von Ortungsdaten bei behaupteten Dienst- bzw. Arbeitspflichtverletzungen von Beschäftigten; der Beitrag konkretisiert die einschlägigen Grundsätze somit weiter.

9.4.1 Sachverhalt

Die Kommune setzte bei Außendiensten von Beschäftigten elektronische GPS-Aufzeichnungssysteme ein, um Positionsdaten, Datum und Uhrzeit zu erfassen. Die Datenerhebung fand während der Außendienste durchgehend statt; ein Datenzugriff sei jedoch nur stichprobenartig oder anlassbezogen vorgesehen gewesen. Die Beschäftigten seien über die Maßnahmen zuvor schriftlich informiert worden.

Nach Darstellung der Kommune sei die GPS-Überwachung aufgrund vielfachen Missbrauchs von Außendiensten für private Zwecke (u. a. Lebensmitteleinkäufe, Essensbestellungen, private Nebentätigkeiten) durch Beschäftigte der betroffenen Organisationseinheit erforderlich gewesen. Dienstvergehen und arbeitsvertragliche Pflichtverletzungen seien konkret und unabhängig voneinander durch verschiedene Augenzeuginnen und Augenzeugen innerhalb und außerhalb der Organisationseinheit beschrieben und belegt worden. Belastbare Nachweise seien aber nicht zu führen, da Augenzeuginnen und Augenzeugen nur unter Wahrung ihrer Anonymität zur Sachverhaltsaufklärung beigetragen hätten. Disziplinarverfahren und arbeitsrechtliche Konsequenzen gegen einzelne Beschäftigte seien daher nicht in Betracht gekommen.

Angeordnet wurde die Überwachungsmaßnahme für alle Beschäftigten der Organisationseinheit bei Außendiensten. Ein Teil der Beschäftigten der Organisationseinheit führte regelmäßig Außendienste mit GPS-Ortungsgerät durch. Bei einigen dieser Beschäftigten gab es jedoch keine Verdachtsmomente bezüglich dienst- oder arbeitsrechtlicher Pflichtverletzungen.

Eine Interessenabwägung seitens der Kommune habe ergeben, dass kein milderes, gleich geeignetes Mittel als die GPS-Überwachung der Beschäftigten zur Verfügung stand, um dem Ziel einer ordnungsgemäßen Pflichterfüllung der Beschäftigten näher zu kommen. Die Teilnahme zusätzlicher Führungskräfte an Außendiensten sei nicht möglich. Personalgespräche oder allgemeine Hinweise zur Pflichterfüllung, die Verwendung von Mobiltelefonen und das Führen von Fahrtenbüchern oder Tätigkeitsprotokollen seien nicht ausreichend gewesen. Der erforderliche hinreichende, tatsachengestützte Verdacht auf eine dienst- oder arbeitsrechtliche Pflichtverletzung sei gegeben. Die Interessen des Dienstherrn bzw. Arbeitgebers an der ordnungsgemäßen Pflichterfüllung seiner Beschäftigten hätten daher das informationelle Selbstbestimmungsrecht der Beschäftigten überwogen. Nicht eine Leistungskontrolle der Beschäftigten, sondern die Unterbindung des Außendienstmissbrauchs sei Ziel der Maßnahme gewesen.

9.4.2 Verarbeitung personenbezogener Ortungsdaten

Die rechtliche Würdigung ergab, dass die verarbeiteten Ortungsdaten einen Personenbezug im Sinne von Art. 4 Nr. 1 DSGVO aufwiesen. Die Personenidentifizierbarkeit mittels Standortdaten war möglich, da die jeweilige Person über die Zuordnung zu einem zugeteilten GPS-Überwachungsgerät identifizierbar war.

Die Verarbeitung der Positionsdaten von Beschäftigten zum Zwecke der Ausübung der Dienstaufsicht war grundsätzlich an Art. 103 Satz 1 Bayerisches Beamtengesetz (BayBG) zu messen. 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. Diese Vorschrift ist grundsätzlich auch auf die nichtverbeamteten Beschäftigten des bayerischen öffentlichen Dienstes gemäß Art. 145 Abs. 2 BayBG entsprechend anzuwenden.

Anders als in den Fallkonstellationen des Beitrags Nr. 11.4 meines 27. Tätigkeitsberichts 2016 diente die Erfassung der Bewegungsdaten vorliegend nicht etwa der Organisation des Betriebsablaufs, sondern ausschließlich personalverwaltenden Zwecken. Die Daten waren also kein „Beifang“ einer betriebsorganisatorischen Maßnahme, sondern Hauptzweck einer Personalmaßnahme, sodass Rechtsgrundlagen des bereichsspezifischen Personalaktendatenschutzes in Betracht kamen. Die Zwecksetzung für die Verarbeitung der erfassten Daten führte somit zu einem unmittelbaren inneren Zusammenhang mit dem jeweiligen Dienst- oder Arbeitsverhältnis im Sinne von § 50 Satz 2 Beamtenstatusgesetz (BeamtStG). Zweck der Überwachungsmaßnahme war es nicht, Pflichtverletzungen oder Straftaten aufzuklären, um daran etwaige dienst-, disziplinar-, arbeits- oder strafrechtliche Folgen zu knüpfen. Die Überwachungsmaßnahme sollte vielmehr dazu dienen, Missbrauch zu verhindern und Beschäftigte zu rechtmäßigem Verhalten zu motivieren. Unter Personalverwaltung im Sinne von Art. 103 Satz 1 Nr. 1 BayBG ist die gesamte Betreuung des konkreten Dienstverhältnisses durch den Dienstherrn zu verstehen (einschließlich seiner

Begründung, Durchführung und Beendigung), so dass die Maßnahme als Gegenstand der Personalverwaltung angesehen werden konnte.

9.4.3 Rechtmäßigkeit der Überwachung

Die Überwachungsmaßnahme konnte insgesamt allerdings nicht auf Art. 103 Satz 1 Nr. 1 BayBG gestützt werden und war im Übrigen auch nicht erforderlich; sie war damit rechtswidrig:

9.4.3.1 Fehlende Rechtsgrundlage

Zweifelhaft war bereits, ob Art. 103 BayBG für die vorliegende Überwachung als verhaltenslenkende Maßnahme zum Zwecke der Abwehr rechtswidriger Verhaltensweisen eine hinreichend bestimmte Rechtsgrundlage darstellen konnte. Entsprechend dem Grundsatz der Normenbestimmtheit und Normenklarheit erfordern erhebliche Grundrechtseingriffe eine Ermächtigungsgrundlage, die Anlass, Zweck und Grenzen des Eingriffs bereichsspezifisch, präzise und normenklar festlegt.[80] Diese Vorgaben kann Art. 103 BayBG nur für vereinzelte, geringfügige Überwachungseingriffe erfüllen. Dauerhafte, eingriffsintensive Überwachungsmaßnahmen können auf Art. 103 BayBG nicht gestützt werden, weil es insoweit an eindeutigen Festlegungen zu Inhalt und Umfang von Überwachungsmaßnahmen fehlt. Eine mit der Videoüberwachung gemäß Art. 24 BayDSG vergleichbare spezifische Rechtsgrundlage für GPS-Überwachungen als Dauermaßnahme existiert nicht.

Die vorliegende Überwachungsmaßnahme konnte daher nicht auf Art. 103 BayBG als Rechtsgrundlage gestützt werden und war bereits mangels hinreichend konkreter Rechtsgrundlage rechtswidrig.

9.4.3.2 Erforderlichkeit

Im Übrigen hat sich die Überwachung als nicht erforderlich im Sinne von Art. 103 Satz 1 Nr. 1 BayBG herausgestellt. Maßnahmen in der Personalverwaltung gemäß Art. 103 Satz 1 BayBG müssen zur Erreichung des festgelegten Zwecks erforderlich und somit verhältnismäßig sein. Zweck der Maßnahme war es nicht, Aufklärungsarbeit zu leisten, um eine Tatsachengrundlage für die Verfolgung etwaiger Pflichtverletzungen oder Straftaten zu schaffen. Vielmehr sollten verdächtige Beschäftigte mittels der ihnen bekannten GPS-Überwachung zu einem rechtmäßigen Verhalten motiviert werden. Die Maßnahme diente somit der präventiven Verhaltenssteuerung.

Zu beachten war zunächst, dass die Überwachungsmaßnahme für alle Beschäftigten der Organisationseinheit ohne Unterscheidung galt. Die Überwachungsmaßnahme erfolgte somit auch gegenüber Beschäftigten, die keinen Anlass für eine Überwachung gegeben hatten, weil bei ihnen keine Anhaltspunkte eines pflichtwidrigen Verhaltens vorlagen. Diese Überwachung war schon nicht erforderlich und somit rechtswidrig. Soweit Ortungsdaten zu Zwecken der Dienstaufsicht verwendet werden sollen, ist zumindest ein hinreichender, tatsachengestützter Verdacht auf eine dienst- oder arbeitsrechtliche Pflichtverletzung oder ein durch konkrete Tatsachen begründeter Verdacht auf eine Straftat oder Ordnungswidrigkeit vorausgesetzt. Bezüglich dieses Personenkreises lag ein solcher Verdacht schon gar nicht vor. Die Zweckbe-

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

stimmung, Beschäftigte zu einem ordnungsgemäßen Verhalten anzuleiten, lief jedenfalls bei denjenigen Beschäftigten ins Leere, die sich ohnehin bereitwillig ordnungsgemäß verhielten.

Aber auch im Hinblick auf die Überwachung der anderen Beschäftigten der betroffenen Organisationseinheit stellte sich die Überwachungsmaßnahme als nicht erforderlich im Sinne von Art. 103 Satz 1 BayBG dar.

Nicht von vornherein und in jedem Falle unzulässig ist zwar eine Verwendung von Ortungsdaten zu Zwecken der Dienstaufsicht (vgl. mein 27. Tätigkeitsbericht 2016 unter Nr. 11.4.3). Im Ausnahmefall kann es statthaft sein, einen tatsachengestützten Verdacht einer dienst- oder arbeitsrechtlichen Pflichtverletzung bei bestimmten Personen durch eine offene GPS-Überwachung zu konkretisieren, um daran anknüpfend weitere Maßnahmen arbeits- oder dienstrechtlicher Natur folgen zu lassen. In einem solchen Fall müsste die Überwachung aber das einzige Mittel sein, um eine Tatsachengrundlage für weitere Maßnahmen zu schaffen (vgl. die ähnliche Ausgangslage in § 26 Abs. 1 Satz 2 Bundesdatenschutzgesetz). So lag der gegenständliche Fall jedoch nicht. Die Überwachung sollte vorliegend einem Missbrauch von Außendiensten allgemein entgegenwirken, nachdem die Tatsachenlage weitgehend aufgeklärt war, jedoch keine arbeits- oder dienstrechtlichen Maßnahmen ergriffen wurden.

Einem Verdacht auf pflichtwidriges Verhalten von Beschäftigten ist allerdings primär dienst- bzw. arbeitsrechtlich zu begegnen. Um den Beschäftigten ihr Fehlverhalten aufzuzeigen und eine Warnung auszusprechen und um sie dadurch zu einem rechtmäßigen Verhalten anzuhalten und künftigen Missbrauch zu unterbinden, kommen hier zunächst insbesondere Missbilligung bzw. Abmahnung Betracht. Derartige Maßnahmen wurden nicht ergriffen und sollten auch nicht ergriffen werden. Die Prüfung derartiger Maßnahmen und eine entsprechende sachliche Auseinandersetzung wären der öffentlichen Stelle durchaus zumutbar gewesen.

Soweit dienst- bzw. arbeitsrechtliche Maßnahmen unterblieben, weil Augenzeuginnen und Augenzeugen nur unter Wahrung ihrer Anonymität zur Sachverhaltsaufklärung beigetragen hatten, war diese Vorgehensweise in Zweifel zu ziehen. Die Kommune hätte zumindest eingehend prüfen müssen, ob eine Verfahrensdurchführung und die Erhebung von Zeugenaussagen rechtlich ausgeschlossen waren. Einem Fehlverhalten adäquate, von der Rechtsordnung vorgesehene formelle Reaktionen können nicht durch ungesetzliche Einflussnahmen ersetzt werden, weil Befindlichkeiten Dritter entgegenstehen. In formalisierten Verfahren ist die Gewährleistung der Anonymität von Zeugen eine Frage des Verfahrensrechts, ebenso wie die Pflicht zu einer wahrheitsgemäßen Aussage. Hinsichtlich verbeamteter Beschäftigter steht die Einleitung eines Disziplinarverfahrens nicht im Ermessen der Behörde, sondern hat gemäß Art. 19 Abs. 1 Satz 1 Bayerisches Disziplinargesetz (BayDG) von Amts wegen zu erfolgen. Die Beweiserhebung ist ebenso wie die Regelungen zur Erhebung und Verwertung von Zeugenaussagen streng formalisiert. Dies gilt gleichfalls für gerichtliche Verfahren. Demgemäß sind Zeugen zur Aussage verpflichtet, sofern kein Zeugnis- oder Auskunftsverweigerungsrecht besteht. Ob und inwiefern in arbeitsrechtlicher (vgl. § 46 Abs. 2 Satz 1 Arbeitsgerichtsgesetz in Verbindung mit § 495, §§ 383 ff. Zivilprozessordnung) oder in dienstrechtlicher (vgl. Art. 27 Abs. 1 Satz 2 BayDG im Verbindung mit §§ 52 ff. Strafprozeßordnung – StPO) Hinsicht Zeugenaussagen aus rechtlichen Gründen nicht zur Sachverhaltsaufklärung herangezogen werden durften, wurde von Seiten der öffentlichen Stelle nicht vorgetragen. Einer etwaigen besonderen Schutzbedürftigkeit von Zeugen hätte gegebenenfalls mit spezifischen verfahrensrechtlichen Schutzmaßnahmen begegnet werden können (vgl. etwa Art. 27 Abs. 1 Satz 2 BayDG in Verbindung mit § 48a, § 68 Abs. 3, § 168e StPO). Selbst wenn

die zugesicherte Anonymität der Zeugen dazu geführt haben sollte, dass keine ausreichende Tatsachenfeststellung zur Einleitung und Durchsetzung dienst- oder arbeitsrechtlicher Maßnahmen bestanden hat, so hätten weitere Ermittlungsquellen zunächst ausgeschöpft werden müssen, um die Problematik einer dienst- oder arbeitsrechtlichen Lösung zuzuführen.

Als nicht erforderlich im Sinne von Art. 103 Satz 1 Nr. 1 BayBG hat sich die GPS-Überwachung auch mit Blick auf die Angemessenheit des Verhältnisses von Zweck und Mittel der Maßnahme dargestellt. Soweit GPS-Maßnahmen im Rahmen der Dienstaufsicht verwendet werden, sind die Zwecksetzung und die Erreichung des legitimen Zwecks durch verhältnismäßige Mittel entscheidend für die Rechtmäßigkeit der Maßnahme. Zweifelhaft ist bereits, ob eine allgemeine Verhaltensbesserung der Beschäftigten als legitimer Zweck eines erheblichen Grundrechtseingriffs angesehen werden kann. Dies wiegt umso schwerer, wenn der Grundrechtseingriff mittels einer dauerhaften Überwachungsmaßnahme erfolgt, die einen permanenten Kontroll- und Rechtfertigungsdruck erzeugt. Der Zweck der Maßnahme, die Beschäftigten zu einem rechtmäßigen Verhalten anzuleiten, liegt dem beamten- und arbeitsrechtlichen Pflichtengefüge ohnehin zu Grunde. Die Maßnahme diente dazu, ein Verhalten sicherzustellen, zu dem die Beschäftigten ohnehin verpflichtet waren. Die Fürsorgepflicht des Dienstherrn bzw. Arbeitgebers reicht nicht soweit, dass er einem bestimmten Verhalten seiner Beschäftigten „um jeden Preis“ – insbesondere nicht um den Preis erheblicher Rechtseingriffe – nachzusorgen hat. Vielmehr nimmt der Gesetzgeber – wie die vorhandenen dienst- und arbeitsrechtlichen Instrumente zeigen – an, dass die Beschäftigten ihre Pflichten eigenverantwortlich erfüllen, insbesondere wenn sie auf ihr Fehlverhalten aufmerksam gemacht wurden.

9.4.4 Fazit

Die rechtswidrige Verarbeitung personenbezogener Daten im Rahmen der GPS-Überwachung habe ich gegenüber der Kommune nach Art. 16 Abs. 4 Sätze 1 und 2 BayDSG förmlich datenschutzrechtlich beanstandet. Zudem habe ich die Kommune zur Löschung der unrechtmäßig gespeicherten personenbezogenen Daten gemäß Art. 17 Abs. 1 Buchst. d DSGVO aufgefordert; dem ist die Kommune in der Folge nachgekommen.

9.5 Zugriff auf den dienstlichen E-Mail-Account eines verstorbenen Professors

Eine staatliche Hochschule wandte sich an mich mit der Frage, ob sie einem Testamentsvollstrecker Zugriff auf das dienstliche E-Mail-Konto eines verstorbenen, ehemaligen Professors gestatten dürfe. Der Professor befand sich vor seinem Ableben im Ruhestand; eine Weiternutzung des dienstlichen E-Mail-Kontos auch zu privaten Zwecken war von der Hochschule erlaubt worden.

9.5.1 Verarbeitung personenbezogener Daten

Aus datenschutzrechtlicher Sicht kommt es bei der Gewährung des Zugriffs auf E-Mails zu einer Verarbeitung personenbezogener Daten gemäß Art. 4 Nr. 1 DSGVO. Keine personenbezogenen Daten in diesem Sinne waren allerdings in E-Mails enthaltene Informationen, die sich auf die Person des verstorbenen Professors bezogen. Die Datenschutz-Grundverordnung gilt gemäß Erwägungsgrund 27 DSGVO nicht für

die personenbezogenen Daten Verstorbener. In E-Mails sind jedoch regelmäßig personenbezogene Daten von Kommunikationspartnern enthalten. So weisen E-Mail-Adressen jedenfalls dann einen Personenbezug auf, wenn sich aus ihnen Identifizierungsmerkmale (etwa Namen) ableiten lassen. Auch im Übrigen war anzunehmen, dass der dienstliche und nicht dienstliche E-Mail-Verkehr eine Vielzahl personenbezogener Daten von Kommunikationspartnern des Erblassers enthielt.

Die beabsichtigte Bereitstellung der Zugriffsmöglichkeit auf die E-Mails des Erblassers wäre als Verarbeitung personenbezogener Daten durch die Hochschule gemäß Art. 4 Nr. 2 DSGVO in Form einer Offenlegung zu werten. Sobald es zum Abruf der bereitgestellten Daten käme, erfolgt eine Datenübermittlung.

9.5.2 Rechtsgrundlage der Verarbeitung

Rechtmäßig wäre eine solche Verarbeitung nur dann, wenn sie auf eine Rechtsgrundlage gemäß Art. 6 Abs. 1 DSGVO gestützt werden könnte. Rechtsgrundlagen für Verarbeitungen gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO werden gemäß Art. 6 Abs. 3 Satz 1 Buchst. b DSGVO insbesondere durch mitgliedstaatliches Recht festgelegt.

Die Übermittlung wäre nicht auf Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG zu stützen, weil sie nicht zur Erfüllung einer Aufgabe der Hochschule erforderlich wäre. Der Testamentsvollstrecker als Datenempfänger war keine öffentliche Stelle im Sinne von Art. 1 Abs. 1, 2 oder 4 BayDSG. Er übernimmt zwar ein „Amt“, vgl. § 2202 Abs. 1 Bürgerliches Gesetzbuch (BGB), mit der Aufgabe, die letztwilligen Verfügungen des Erblassers zur Ausführung zu bringen (§ 2203 BGB). Zum Testamentsvollstrecker ernannt werden üblicherweise natürliche Personen oder juristische Personen des Privatrechts. Vor diesem Hintergrund hätten datenschutzrechtliche Vorschriften für öffentliche Stellen auf Testamentsvollstrecker allenfalls gemäß Art. 1 Abs. 4 BayDSG angewendet werden können, sofern sie als nicht öffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen. Testamentsvollstrecker haben jedoch ein privates Amt inne und sind keine Beliehenen.[81]

Demgegenüber käme eine Datenübermittlung auf Grund von Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG in Betracht, da der Testamentsvollstrecker als nicht öffentliche Stelle anzusehen ist. Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG setzt voraus, dass der Datenempfänger ein berechtigtes Interesse an der Kenntnis der personenbezogenen Daten glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

9.5.2.1 Berechtigtes Interesse

Das berechtigte Interesse des Testamentsvollstreckers könnte sich aus dessen Verwaltungsbefugnis gemäß § 2205 BGB ergeben. Zum Verwaltungsrecht des Testamentsvollstreckers gehören alle Maßnahmen zur Feststellung, Sicherung, Erhaltung und Nutzbarmachung des Nachlasses.[82] Dies setzte aber voraus, dass die E-Mails mitsamt dem E-Mail-Konto des Erblassers entweder zum Nachlass gehörten (1) oder

81 Vgl. Papier/Shirvani, in: Münchener Kommentar zum Bürgerlichen Gesetzbuch, 8. Aufl. 2020, § 839 BGB Rn. 186.

82 Vgl. Zimmermann, in: Münchener Kommentar zum Bürgerlichen Gesetzbuch, 8. Aufl. 2020, § 2205 BGB Rn. 11.

zumindest Informationen enthielten, die für die Erfüllung der Verwaltungsaufgabe des Testamentsvollstreckers von Bedeutung wären (2).

(1) Ob E-Mails als „digitaler Nachlass“ vererbbar sind, richtet sich nach § 1922 Abs. 1 BGB. Demnach geht mit dem Tode einer Person (Erbfall) deren Vermögen (Erbschaft) als Ganzes auf eine oder mehrere andere Personen (Erben) über. Konkret vererbbar sind Rechte des Erblassers; auch die Verbindlichkeiten gehen auf den Erben über, vgl. § 1967 BGB. Erbschaft ist somit die Gesamtheit der vererbbaren Rechtsverhältnisse jeweils mit Einschluss der Verbindlichkeiten.[83]

— Der „digitale Nachlass“ war Gegenstand einer Entscheidung des Bundesgerichtshofs,[84] die sich auf den Rechtsübergang des vom Erblasser abgeschlossenen Nutzungsvertrags mit dem Betreiber eines sozialen Netzwerks auf die Erben bezog. Die Erben nahmen im Rahmen der Gesamtrechtsnachfolge auch die Stellung des Nutzers im Rechtsverhältnis mit dem Betreiber ein und gelangten so an einen Anspruch auf Zugang zu dem Nutzerkonto. Diese rechtliche Beurteilung ließe sich grundsätzlich auch auf andere digitale Konten – etwa E-Mail-Konten – übertragen.[85]

— Der vorliegende Fall war jedoch anders zu beurteilen, weil die Hochschule die Weiternutzung des (ehemals) dienstlichen E-Mail-Kontos nicht aufgrund einer schuldrechtlichen Vertragsbeziehung gestattet hatte, die vererbbar gewesen wäre. Vielmehr gründete die Gestattung im Beamtenverhältnis des Erblassers, das mit dem Tod des Beamten endete.

  Aus dem Beamtenrecht ergab sich keine Rechtsposition in Bezug auf die E-Mails, die vererbbar gewesen wäre und somit ein berechtigtes Interesse des Testamentsvollstreckers hätte begründen können. Das dienstliche E-Mail-Konto diente in erster Linie als Arbeitsmittel, vgl. § 10 Abs. 4 Allgemeine Geschäftsordnung für die Behörden des Freistaates Bayern (AGO). Daran vermochte auch die Gestattung der privaten Nutzung in geringfügigem Umfang nichts zu ändern. Mit Eintritt in den Ruhestand standen dem Professor gemäß Art. 60 Abs. 6 Bayerisches Hochschulinnovationsgesetz (BayHIG) weiter die mit der Lehrbefugnis verbundenen Rechte zur Abhaltung von Lehrveranstaltungen und zur Beteiligung an Prüfungsverfahren zu. Die Belassung des E-Mail-Kontos als grundlegendes Kommunikationsmittel war vor diesem Hintergrund zu würdigen. Ein schuldrechtliches Rechtsverhältnis wurde zwischen der Hochschule und dem verstorbenen Professor auch nach dessen Eintritt in den Ruhestand nicht begründet.

Aus dem der E-Mail-Nutzung zugrundeliegenden Rechtsverhältnis ergab sich keine vererbbare Rechtsposition, die ein Zugriffsrecht der Erben oder des Testamentsvollstreckers auf das dienstliche E-Mail-Konto des Erblassers vermit-

83 Vgl. Leipold, in: Münchener Kommentar zum Bürgerlichen Gesetzbuch, 8. Aufl. 2020, § 1922 BGB Rn. 17.

84 Bundesgerichtshof, Urteil vom 12. Juli 2018, III ZR 183/17, BeckRS 2018, 16463.

85 Vgl. Leipold, in: Münchener Kommentar zum Bürgerlichen Gesetzbuch, 8. Aufl. 2020, § 1922 BGB Rn. 46.

telte. Insoweit fehlte es am berechtigten Interesse des Testamentsvollstreckers gemäß Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG an der Kenntnis der personenbezogenen Daten.

(2) Dies bedeutete gleichwohl nicht, dass dem Testamentsvollstrecker oder den Erben jegliches berechtigte Interesse im Sinne von Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG an der Kenntnis bestimmter – in E-Mails enthaltener – Informationen abzusprechen wäre. Der Begriff des berechtigten Interesses ist grundsätzlich weit auszulegen und umfasst jedes im Einklang mit der Rechtsordnung stehende rechtliche, ideelle oder wirtschaftliche Interesse.[86]

— Auch wenn das Nutzungsverhältnis in Bezug auf das E-Mail-Konto vorliegend nicht vererbbar war, könnten bestimmte in E-Mails enthaltene Informationen für den Nachlass relevant sein.

  Grundsätzlich begründen Informationen per se keine Rechtspositionen. An Informationen als immateriellen Gütern können jedoch etwa Immaterialgüterrechte mit absoluter Schutzwirkung und subjektiver Rechtsposition bestehen. So ist es denkbar, dass in E-Mails enthaltene Informationen urheberrechtlich geschützte Werke gemäß § 2 Abs. 1 Urheberrechtsgesetz (UrhG) darstellen. Zum urheberrechtlichen Werk hat der Urheber oder der Erbe als sein Rechtsnachfolger (vgl. § 28 Abs. 1, § 30 UrhG) gemäß § 25 Abs. 1 UrhG einen Zugangsanspruch.

  Informationen können auch dem allgemeinen persönlichkeitsrechtlichen Schutz unterliegen. Jedenfalls hinsichtlich der vermögensrechtlichen Bestandteile des allgemeinen Persönlichkeitsrechts ist die Vererbbarkeit anerkannt. Etwa Details aus dem Privat- oder Intimleben von bedeutenden Persönlichkeiten können gegebenenfalls einen kommerziellen Wert aufweisen.

— Auch können in E-Mails enthaltene Erklärungen Rechtswirkungen entfalten, die für den Nachlass von Relevanz sind. So ist es denkbar, dass der Erblasser per E-Mails Willenserklärungen abgegeben oder empfangen und somit Rechtsgeschäfte, etwa Verträge, abgeschlossen hat. Zu beachten ist dabei auch, dass es gemäß § 130 Abs. 2 BGB auf die Wirksamkeit der Willenserklärung ohne Einfluss ist, wenn der Erklärende nach der Abgabe stirbt oder geschäftsunfähig wird.

— Rein faktische Informationsübermittlungen, die keine Rechtspositionen enthalten oder begründen, können für den Nachlass ebenfalls von Bedeutung sein. So können Mitteilungen auf Geschäftsbeziehungen oder Vermögenswerte hindeuten und einen Verwaltungsaufwand zur Vermögenswahrung erforderlich machen (etwa wenn in geschäftlichen E-Mails auf den Ablauf von Fristen o. ä. hingewiesen wird).

Vor diesem Hintergrund könnten in E-Mails enthaltene Informationen für den Nachlass von Bedeutung sein und ein berechtigtes Interesse des Testamentsvollstreckers im Sinne von Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG jedenfalls insofern begründen, als die Kenntnis der Informationen für die Nachlassverwaltung erforderlich ist.

86 Vgl. Stief, in: Schröder, Bayerisches Datenschutzgesetz, 2021, Art. 5 BayDSG Rn. 60.

9.5.2.2 Glaubhafte Darlegung des berechtigten Interesses

Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG erfordert eine „glaubhafte Darlegung" dieses berechtigten Interesses. Dabei wäre zu beachten, dass der Inhalt der E-Mails dem auskunftsbegehrenden Testamentsvollstrecker noch nicht bekannt war. Dieses unverschuldete Substantiierungsdefizit durfte nicht allein zu einem Ausschluss der „glaubhaften Darlegung" führen. An die „glaubhafte Darlegung" waren daher keine unrealistisch hohen Anforderungen – etwa in Bezug auf das Interesse an der Kenntnis spezifischer E-Mail-Inhalte – zu stellen. Notwendig, aber auch ausreichend wäre, dass der Testamentsvollstrecker sich entsprechend zu erkennen gibt und gegebenenfalls unter Vorlage von Legitimationsdokumenten angibt, die Kenntnis der Informationen zur Nachlassverwaltung zu benötigen.

9.5.2.3 Kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung

Im Übrigen dürften an dem Ausschluss der Datenübermittlung keine schutzwürdigen Interessen betroffener Personen bestehen. Insoweit kämen Datenschutzinteressen der Kommunikationspartner des Erblassers am Ausschluss der Datenübermittlung an den Testamentsvollstrecker in Betracht. Bei der insofern gebotenen Interessenabwägung wäre entsprechend der Argumentation des Bundesgerichtshofs[87] zu beachten, dass die Kommunikationspartner die relevanten Daten freiwillig und bewusst an den Erblasser übermittelt haben. Ein Kommunikationspartner kann nach dem Versenden einer E-Mail nicht mehr kontrollieren, wer nach der Übermittlung letztlich von deren Inhalt Kenntnis nimmt. Er hat grundsätzlich keine Möglichkeit, die übermittelte E-Mail bzw. deren Inhalt zurückzufordern. Auch können Kommunikationspartner vernünftigerweise absehen, dass im Erbfall unter Umständen Hinterbliebene oder der Testamentsvollstrecker des E-Mail-Empfängers Zugriff nehmen möchten.

Aus datenschutzrechtlicher Sicht könnte eine Datenübermittlung an den Testamentsvollstrecker daher grundsätzlich auf Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG gestützt werden.

9.5.3 Fazit

Zusammengefasst kam eine Datenübermittlung der staatlichen Hochschule gestützt auf Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG an den Testamentsvollstrecker hinsichtlich derjenigen E-Mails des Erblassers in Betracht, deren Inhalt für die Nachlassverwaltung relevant war.

9.6 Polizeiärztliche Untersuchung anlässlich einer Versetzung

Fragen zu dienstlich veranlassten amtsärztlichen Untersuchungen haben mich im Berichtszeitraum erneut beschäftigt (vgl. zuletzt Nr. 8.5 meines 31. Tätigkeitsberichts 2021). Einer Beschwerde lag dabei der folgende Sachverhalt zugrunde:

Der Beschwerdeführer war als Beamter auf Lebenszeit bei einer bayerischen Behörde beschäftigt. Auf seinen eigenen Wunsch hin war die **Versetzung** des Beschwerdeführers an eine bayerische Polizeidienststelle vorgesehen. Dort sollte er ebenfalls im Verwaltungsbereich eingesetzt werden.

[87] Vgl. Bundesgerichtshof, Urteil vom 12. Juli 2018, III ZR 183/17, BeckRS 2018, 16463, Rn. 88 ff.

Anlässlich der geplanten Versetzung wurde der Beschwerdeführer von der Polizeidienststelle aufgefordert, sich einer **polizeiärztlichen Untersuchung** bei dem Ärztlichen Dienst der Bayerischen Polizei (im Folgenden: polizeiärztlicher Dienst) zu unterziehen. Im Rahmen dieser Untersuchung sollte **geklärt** werden, ob bei dem Beschwerdeführer schwerwiegende Erkrankungen vorliegen, welche zu erhöhten Krankheitszeiten oder eventuell zu einer vorzeitigen Ruhestandsversetzung führen könnten. Die Polizeidienststelle wies den Beschwerdeführer in diesem Zusammenhang darauf hin, dass die geplante Versetzung noch unter dem **Vorbehalt** stehe, dass das Ergebnis der polizeiärztlichen Untersuchung „dem nicht entgegensteht". Unter dem Eindruck, die polizeiärztliche Untersuchung sei notwendige Voraussetzung für seine Versetzung und damit **„obligatorisch"**, unterzog sich der Beschwerdeführer schließlich dieser Untersuchung.

Im Nachgang kamen dem Beschwerdeführer allerdings – berechtigte – Zweifel, ob das Vorgehen der Polizeidienststelle rechtmäßig war. Diese hatte ihm auf seine Nachfrage hin im Wesentlichen lediglich mitgeteilt, bei der polizeiärztlichen Untersuchung handle es sich um ein „übliches Verfahren". In der Folge wandte sich der Beschwerdeführer an mich.

Ich bat die Polizeidienststelle daraufhin um eine Stellungnahme. Dabei wollte ich insbesondere wissen, auf welcher Rechtsgrundlage die polizeiärztliche Untersuchung des Beschwerdeführers veranlasst und weshalb eine solche Untersuchung überhaupt für erforderlich gehalten wurde.

Die Polizeidienststelle führte mir gegenüber aus, die polizeiärztliche Untersuchung des Beschwerdeführers auf Art. 33 Abs. 2 Grundgesetz für die Bundesrepublik Deutschland und auf § 9 Beamtenstatusgesetz (BeamtStG) gestützt zu haben. Der Dienstherr sei danach berechtigt, Bewerberinnen und Bewerber vor Einstellung durch einen Amtsarzt auf **gesundheitliche Eignung** zu überprüfen, wenn mit der Versetzung eine **mögliche Ernennung** verbunden sei. Dies diene dazu, die geeignetste Person für die jeweils ausgeschriebene Stelle zu gewinnen. Die polizeiärztliche Untersuchung sei daher obligatorisch gewesen.

Überzeugen konnte mich diese Begründung allerdings nicht:

Die Polizeidienststelle hat im Rahmen der Prüfung der gesundheitlichen Eignung des Beschwerdeführers dessen personenbezogene Daten verarbeitet. Hierfür war eine **Rechtsgrundlage** im Sinne des Art. 6 Abs. 1 UAbs. 1 DSGVO erforderlich. Soweit eine Verarbeitung auch **besondere Kategorien** personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO – wie vorliegend Gesundheitsdaten – umfasst, muss ergänzend ein Zulässigkeitstatbestand nach Art. 9 Abs. 2 DSGVO erfüllt sein.

Im vorliegenden Zusammenhang kommt als Rechtsgrundlage Art. 103 Satz 1 Bayerisches Beamtengesetz (BayBG) in Betracht. Danach darf der Dienstherr personenbezogene Daten über Bewerber und Bewerberinnen verarbeiten, soweit dies zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere zu Zwecken der Personalverwaltung oder Personalwirtschaft erforderlich ist (Art. 103 Satz 1 Nr. 1 BayBG). „Personalverwaltung" umfasst dabei insbesondere Personalangelegenheiten einschließlich Einstellungen und Versetzungen. In diesem Zusammenhang kann auch die Verarbeitung von Gesundheitsdaten zulässig sein, vgl. Art. 103 Satz 1 Nr. 2 BayBG in Verbindung mit Art. 8 Abs. 1 Satz 1 Nr. 2 und 3 BayDSG. Zulässig ist eine Datenverarbeitung nach den genannten Vorschriften allerdings nur, wenn und soweit sie im Sinne von Art. 103 Satz 1 BayBG, Art. 8 Abs. 1 Satz 1 Nr. 2 und 3 BayDSG **erforderlich** ist.

Art. 103 BayBG
Verarbeitung personenbezogener Daten
[1]Der Dienstherr darf personenbezogene Daten über Bewerber und Bewerberinnen sowie aktive und ehemalige Beamte und Beamtinnen verarbeiten, soweit dies

1. *zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere zu Zwecken der Personalverwaltung oder Personalwirtschaft erforderlich ist,*
2. *zusätzlich bei der Verarbeitung besonderer Kategorien personenbezogener Daten Art. 8 Abs. 1 Nr. 2, 3 und 5 sowie Abs. 2 des Bayerischen Datenschutzgesetzes (BayDSG) erlaubt*

und nachfolgend nichts anderes bestimmt ist. [2][…]

Art. 8 BayDSG
Verarbeitung besonderer Kategorien personenbezogener Daten
(zu Art. 9 DSGVO)
(1) [1]Die Verarbeitung von Daten im Sinne des Art. 9 Abs. 1 DSGVO ist auch zulässig, soweit sie erforderlich ist
[…]

2. *zur Wahrnehmung von Rechten und Pflichten der öffentlichen Stellen auf dem Gebiet des Dienst- und Arbeitsrechts,*
3. *zum Zweck der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit von beschäftigten Personen, […].*

An der **Erforderlichkeit** hat es vorliegend **gefehlt**: Entsprechend den Ausführungen der Polizeidienststelle kann sich bei Versetzungen eine Berechtigung des Dienstherrn, Bewerberinnen und Bewerber auf ihre gesundheitliche Eignung zu überprüfen, (nur) ergeben, wenn **mit der Versetzung eine mögliche Ernennung** des konkreten Bewerbers oder der konkreten Bewerberin verbunden ist. Zu dem Zeitpunkt, als die Polizeidienststelle die polizeiärztliche Untersuchung des Beschwerdeführers beantragt hatte, war dieser allerdings bereits auf Lebenszeit verbeamtet. Es war daher davon auszugehen, dass im Vorfeld seiner beamtenrechtlichen Ernennung auch die **gesundheitliche Eignung** des Beschwerdeführers im Sinne von Art. 33 Abs. 2 GG, § 9 BeamtStG **überprüft und bejaht** worden war. Die gesundheitliche Eignung ist dabei im Hinblick auf die laufbahntypischen Anforderungen zu beurteilen.[88] In der Regel genügt hierfür **eine** Einstellungsuntersuchung, die sich auf die Feststellung des allgemeinen Gesundheitszustandes beschränkt. Etwas anderes kann gelten, wenn „wegen der besonderen Art der mit einer Laufbahn verbundenen Aufgaben erhöhte Anforderungen an die gesundheitliche Eignung zu stellen sind".[89] Für Letzteres war im vorliegenden Fall allerdings nichts erkennbar. Insbesondere ging die im Rahmen der polizeiärztlichen Begutachtung zu beurteilende Fragestellung nicht über eine Überprüfung des allgemeinen Gesundheitszustands des Beschwerdeführers hinaus, wie sie bereits regelmäßig im Rahmen der Einstellungsuntersuchung vor der beamtenrechtlichen Ernennung durchgeführt wird. Denn schließlich sollte der Beschwerdeführer ja nicht im Polizeivollzugsdienst, sondern ausschließlich im Verwaltungsbereich eingesetzt werden.

Da die Verarbeitung personenbezogener Daten des Beschwerdeführers im vorliegenden Zusammenhang nicht erforderlich war, schied Art. 103 Satz 1 BayBG, Art. 8

88 Bundesverwaltungsgericht, Urteil vom 21. Juni 2007, 2 A 6/06, BeckRS 2007, 25462, Rn. 22.
89 Baßlsperger, in: Weiß/Niedermaier/Summer/Zängl, Beamtenrecht in Bayern, Stand: 3/2020, § 9 BeamtStG Rn. 25.

Abs. 1 Satz 1 Nr. 2 und 3 BayDSG als Rechtsgrundlage aus. Eine andere Rechtsgrundlage, auf welche die erneute Überprüfung der gesundheitlichen Eignung des Beschwerdeführers hätte gestützt werden können, war nicht ersichtlich.

Das Vorgehen der Polizeidienststelle habe ich daher nach Art. 16 Abs. 4 Sätze 1 und 2 BayDSG förmlich datenschutzrechtlich **beanstandet**.

10 Schulen, Hochschulen, Kultur

10.1 Beratung bei der Änderung schulrechtlicher Vorschriften

Auch in diesem Berichtszeitraum beriet ich das Bayerische Staatsministerium für Unterricht und Kultus intensiv zu Änderungen schulrechtlicher Vorschriften. Datenschutzrechtlich relevante Änderungen betrafen das Bayerische Gesetz über das Erziehungs- und Unterrichtswesen sowie die Bayerische Schulordnung. Zudem veröffentlichte das Kultusministerium zwei neue Bekanntmachungen im Bereich des Schuldatenschutzes.

10.1.1 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen

Im Bayerischen Gesetz über das Erziehungs- und Unterrichtswesen ist vor allem die Einfügung von Bestimmungen zum Distanzunterricht hervorzuheben.

Mit der Einfügung des **neuen Art. 30 Abs. 2 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG)** kam der Gesetzgeber meiner früh zu Beginn der COVID-19-Pandemie erhobenen Forderung (siehe hierzu Beitrag Nr. 10.1.2 in meinem 30. Tätigkeitsbericht 2020) nach, den bislang in § 19 Abs. 4 Bayerische Schulordnung (BaySchO) nur auf Ebene einer Rechtsverordnung geregelten **Distanzunterricht** dem Wesentlichkeitsgedanken des Bundesverfassungsgerichts entsprechend **in einem formellen Gesetz zu verankern**. Die nun erfolgte Umsetzung begrüße ich, weil damit der unmittelbar demokratisch legitimierte Gesetzgeber die wegen der Eingriffsintensität vor allem auch unter dem Blickwinkel des Datenschutzes bedeutsame Entscheidung zum Distanzunterricht ausdrücklich getroffen hat.

Zudem bewerte ich die Klarstellung in Art. 30 Abs. 2 Satz 1 BayEUG positiv, dass der **Präsenzunterricht der Regelfall** ist (und bleibt). Die Beschränkung des Distanzunterrichts auf den Ausnahmefall, wie es die derzeitige Regelung des § 19 Abs. 4 Satz 1 BaySchO vorsieht, halte ich für geboten, weil beim Distanzunterricht verschiedene Grundrechte betroffen sein können (Recht auf informationelle Selbstbestimmung, Gleichheitsgebot, unter Umständen auch Unverletzlichkeit der Wohnung). Nach meiner derzeitigen Einschätzung birgt der Distanzunterricht wegen der Natur der Sache stets gewisse Risiken für die Rechte der betroffenen Personen, insbesondere für das Recht auf informationelle Selbstbestimmung.

Für den Fall des Distanzunterrichts hat der Gesetzgeber sowohl für die Lehrkräfte als auch für die Schülerinnen und Schüler die **Pflicht** zu einer **Bild-und-Ton-Übertragung geregelt**. Die entsprechenden Normen lauten:

Art. 56 BayEUG
Rechte und Pflichten
[…]
(4) […] [4]Erfolgt die Teilnahme am Distanzunterricht im Wege einer Videoübertragung, sind die teilnehmenden Schülerinnen und Schüler zur Übertragung des eigenen Bildes und Tones verpflichtet, soweit die Aufsicht führende Lehrkraft dies aus pädagogischen Gründen fordert und die technischen Voraussetzungen vorliegen. […]

Art. 59 BayEUG
Lehrkräfte
[…]
(2) […] [2]Erteilen Lehrkräfte Distanzunterricht im Wege einer Videoübertragung und liegen die technischen Voraussetzungen vor, sind sie in der Regel zur Übertragung des eigenen Bildes und Tones verpflichtet. […]

Zuvor war nach der bis dahin allein relevanten Regelung des § 46 Abs. 1 BaySchO in Verbindung mit Anlage 2 Abschnitt 7 Nr. 3.2 BaySchO die Freigabe des Videobilds oder der Bildschirmanzeige freiwillig.

Die Notwendigkeit dieser aus Sicht der betroffenen Person strengeren Regelung durch Art. 56 Abs. 4 Satz 4 BayEUG und Art. 59 Abs. 2 Satz 2 BayEUG ließ ich mir vom Kultusministerium ausführlich erläutern. Es legte mir daraufhin nachvollziehbar dar, die bestehenden Erfahrungen hätten gezeigt, dass die Videobildübertragung von Schülerinnen und Schülern sowie Lehrkräften regelmäßig von essenzieller Bedeutung für einen funktionierenden Distanzunterricht sei. Denn auch der Distanzunterricht würde sich durch schulisches Miteinander und synchrone soziale Interaktion auszeichnen. Gegen diese aus schulfachlicher Sicht gut begründete Auffassung zur Erforderlichkeit der Neuregelung hatte ich daher aus datenschutzrechtlicher Sicht keine Einwände.

10.1.2 Bayerische Schulordnung

Im Berichtszeitraum wurden in der **Anlage 2 der Bayerischen Schulordnung** zum einen punktuelle Änderungen im Abschnitt 7 „Digitale Kommunikations- und Kollaborationswerkzeuge“ vorgenommen. Zum anderen wurde ein **neuer Abschnitt 8** „Zentrale vom Freistaat Bayern über das Staatsministerium bereitgestellte Nutzerverwaltung und Anmeldeinfrastruktur“ aufgenommen. Dieser neue Abschnitt 8 ist im Zusammenhang mit dem Projekt des Kultusministeriums „BayernCloud Schule (ByCS)“ zu sehen. Die **BayernCloud Schule** wird vom Kultusministerium als Plattform für Unterricht, Kommunikation, Zusammenarbeit, Fortbildung, Organisation und Verwaltung entwickelt. Der neue Abschnitt 8 schafft in Verbindung mit § 46 BaySchO die normative Grundlage für ein **Identitäts-Management-System** (IDM), welches eine zentrale Nutzerverwaltung und Anmeldestruktur innerhalb des Programms BayernCloud Schule gewährleistet. Wie mir das Kultusministerium darlegte, sei die zentrale Bevorratung der Daten im IDM aus technischer Sicht zwingend notwendig. Eine gemeinsame Datenbasis für alle an das IDM angeschlossenen Anwendungen (etwa ein Videokonferenztool) sichere die Integrität der Daten durch die Minimierung von Redundanzen. Vor diesem Hintergrund trat ich der neuen Regelung nicht entgegen.

Allerdings konnte ich **durch meine Hinweise deutliche Verbesserungen des Datenschutzes** erreichen, die ich hier auswahlweise vorstelle:

— In Abschnitt 7 von Anlage 2 der Bayerischen Schulordnung, der die Datenverarbeitung durch digitale Kommunikations- und Kollaborationswerkzeuge umfasst, wurde der Umfang der nach Nr. 3.1.4 zulässig zu verarbeitenden Inhaltsdaten um die Information „– auf den Einzelfall bezogene und im Einzelfall auf Veranlassung der betroffenen Person erzeugte Standortdaten“ erweitert. In der Begründung wurde erläutert, dass damit vor allem im **Notfall** ein Schüler seinen **Standort per Messenger** für andere Schüler oder Lehrkräfte freigeben oder übermitteln könne. Ich ließ mir vom Kultusministerium bestätigen,

dass diese neue Regelung nur Datenverarbeitungen auf Initiative der betroffenen Person, also **auf freiwilliger Basis**, erfasst. Zudem wurde dieser Aspekt der Freiwilligkeit durch die Nachbemerkung „(freiwillig)“ deutlicher im Normtext hervorgehoben.

— Auf mein Anraten hin begrenzte das Kultusministerium Abschnitt 8 von Anlage 2 der Bayerischen Schulordnung zum IDM normtextlich und damit tatbestandlich auf „Zentrale vom Freistaat Bayern über das Staatsministerium bereitgestellte Nutzerverwaltung und Anmeldeinfrastruktur“. Denn hierdurch wird klargestellt, dass von Abschnitt 8 **nur das vom Kultusministerium geprüfte und freigegebene IDM** erfasst wird und die Schulen aus datenschutzrechtlicher Sicht nur dieses IDM verwenden dürfen, weil (nur) insoweit eine Verarbeitungsbefugnis nach § 46 BaySchO in Verbindung mit Anlage 2 Abschnitt 8 BaySchO besteht.

— In Abschnitt 8 von Anlage 2 der Bayerischen Schulordnung zum IDM wird **als neues Datum auch ein sogenanntes „Ordnungsmerkmal“ für Schülerinnen und Schüler sowie Lehrkräfte eingeführt** (Nrn. 3.2.1 und 3.3.1). Ich ließ mir vom Kultusministerium ausführlich erläutern, dass es sich bei diesem Ordnungsmerkmal nicht um eine Art Schüler-Identifikationsnummer oder Schüler-ID handelt (siehe dazu auch Beitrag Nr. 10.1. in meinem 24. Tätigkeitsbericht 2010 sowie die Entschließung „Keine Schülerstatistik ohne Datenschutz“ der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 2006 in Naumburg), sondern nur um ein technisches Ordnungsmerkmal. Damit dieses – rein technische – Ordnungsmerkmal nicht zu einer eindeutigen und für die gesamte Schullaufbahn gültigen Personenkennziffer wird, drängte ich auf eine geeignete Klarstellung. Erfreulicherweise konnte ich die ausdrückliche Aufnahme in den Normtext erreichen, dass dieses Ordnungsmerkmal **weder für die Schulen noch für die internen und externen Empfänger einsehbar** ist, sondern **nur eine rein technische Speicherung bzw. Verarbeitung** umfasst.

10.1.3 Bekanntmachungen

Schließlich beriet ich das Kultusministerium intensiv zu seiner neuen **Bekanntmachung** über den **Vollzug des Datenschutzrechts an staatlichen Schulen**[90] sowie zu seiner neuen Bekanntmachung über **Hinweise zur Nutzung der IT-Infrastruktur und des Internetzugangs an Schulen**.[91] Diese neuen Bekanntmachungen lösen die Bekanntmachung über erläuternde Hinweise zum Vollzug der datenschutzrechtlichen Bestimmungen für die Schulen sowie die Bekanntmachung über rechtliche Hinweise zur Nutzung der EDV-Einrichtung und des Internets an Schulen ab. Bei den Bekanntmachungen handelt es sich um Verwaltungsvorschriften, die zumindest für staatliche Schulen bindend sind und wichtige Vorgaben für die Schulen zur Umsetzung des Datenschutzes vor Ort enthalten.

Die Bekanntmachung zum Vollzug des Datenschutzes an staatlichen Schulen enthält in Nr. 4.2 Vorgaben zu **Foto-, Ton- und Videoaufnahmen**. Wie mir meine Beratungspraxis immer wieder vor Augen führt, ist dies ein Thema, das Schulen gerade unter dem Blickwinkel des Datenschutzes sehr beschäftigt. Meine Erfahrung zeigt

90 Vom 14. Juli 2022 (BayMBl. Nr. 435).
91 Vom 14. Juli 2022 (BayMBl. Nr. 436).

auch, dass die Schulen ganz überwiegend bemüht sind, die Vorgaben des Datenschutzrechts einzuhalten. Gleichwohl bestehen an Schulen noch Unsicherheiten, wie die Gestaltung eines lebendigen Schulalltags und Schulunterrichts im Einzelfall auch unter Einsatz von Foto- oder Videoaufnahmen rechtskonform mit dem Datenschutz in Einklang zu bringen ist.

Vor diesem Hintergrund begrüße ich, dass die Bekanntmachung diese wichtige Thematik behandelt. Bei meiner Beratung zu dieser Bestimmung achtete ich darauf, dass meine Auffassung dort abgebildet wird. Dabei nutzte ich die Gelegenheit, meine Auffassung zum Datenschutz bei Fotoaufnahmen sowie bei Videoaufnahmen in der Schule zu konsolidieren.

10.2 Datenverarbeitung bei der elektronischen Fernprüfung an Hochschulen (Videoaufsicht)

Über eine Prüfung der Datenverarbeitung einer Hochschule bei einer elektronischen Fernprüfung berichtete ich bereits (siehe Beitrag Nr. 9.2. in meinem 31. Tätigkeitsbericht 2021). Die Hochschule teilte mir **zwischenzeitlich** mit, dass sie nach Erhalt meiner Bewertungen **Sofortmaßnahmen ergriffen** und noch im laufenden Prüfungsbetrieb des Wintersemesters 2021/2022 auf die aufgezeigten Datenschutzverstöße reagiert habe. So habe die Hochschule etwa umgehend die Informationen für Studierende ergänzt, die Organisation von Leih-Laptops aufgebaut und bestimmte Software-Funktionen bei Fernklausuren teilweise, bei Präsenzklausuren grundsätzlich komplett abgeschaltet.

Ich konnte nachvollziehen, dass sich im laufenden Prüfungsbetrieb Fernprüfungen mit der eingesetzten Software nicht sofort durch ein anderes Prüfungsformat ersetzen ließen. Die ergriffenen Sofortmaßnahmen begrüßte ich ebenso wie die Entscheidung der Hochschule, die **zuvor verwendete Prüfungssoftware seit dem Sommersemester 2022 nicht mehr einzusetzen**. Die Hochschule wollte ihre Erfahrungen bewerten und daraus eine **neue Strategie für digital unterstützte Präsenz- und Fernprüfungen entwickeln**. Dazu bot ich der Hochschule meine Beratung an.

Während ich in meinem letzten Bericht vor allem auf die Datenverarbeitung bei der zur Fernprüfung als Alternative angebotenen Präsenzprüfung einging, steht die Prüfung von Datenverarbeitungen bei der elektronischen Fernprüfung in Form der (menschlichen) Videoaufsicht im Zentrum dieses Beitrags.

Bei dieser Prüfungsform findet die Prüfung auf dem eigenen Computer des Prüflings mit menschlicher (Video-)Aufsicht statt. Die Prüflinge wählen dabei den Raum selbst aus, in dem sie die Fernprüfung ableisten. Meist wird dies ein privater Wohnraum sein. Die Videoaufsicht findet über eine Webcam (eine etwa im Smartphone oder im Laptop integrierte Kamera) statt. Nachfolgend beschränke ich mich auf einige Punkte meiner umfangreichen Prüfung.

10.2.1 Videoaufsicht bei der elektronischen Fernprüfung

10.2.1.1 Rechtsgrundlage

Die von mir geprüfte Hochschule konnte sich im Hinblick auf die Datenverarbeitung bei der Videoaufsicht grundsätzlich auf § 4 Abs. 1 in Verbindung mit § 6 Abs. 1, Abs. 2 **Bayerische Fernprüfungserprobungsverordnung** (BayFEV) berufen (siehe dazu

auch Beitrag Nr. 10.1.4 in meinem 30. Tätigkeitsbericht 2020). Die Bayerische Fernprüfungserprobungsverordnung trat gemäß § 13 Abs. 1 BayFEV rückwirkend zum 20. April 2020 in Kraft. Des Weiteren hatte sich die Hochschule zusätzlich auf eine datenschutzrechtliche Einwilligung (Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 7 DSGVO) der Prüflinge gestützt, da sie mit der Durchführung elektronischer Fernprüfungen noch vor Erlass der Bayerischen Fernprüfungserprobungsverordnung begonnen hatte.

10.2.1.2 § 1 Abs. 2 Satz 2 BayFEV

Nach § 1 Abs. 2 Satz 2 BayFEV kann die **elektronische Fernprüfung** auch **als Alternative zu einer Präsenzprüfung** angeboten werden, **wenn und soweit** diese als Folge von Einschränkungen und Hindernissen aufgrund einer Pandemie, Epidemie oder eines anderen erheblichen Infektionsgeschehens nicht oder nicht für alle Studierenden durchgeführt werden kann. In ihrer Stellungnahme trug die Hochschule vor, dass die Hochschulleitung nach ausführlicher Prüfung aller Möglichkeiten, insbesondere der Anmietung von Zelten, Messe- oder Sporthallen, zu dem Ergebnis gekommen sei, dass selbst unter Ausschöpfung aller räumlichen und personellen Ressourcen eine Durchführung der Prüfung in Präsenzform gemäß den infektionsschutzrechtlichen Rahmenbedingungen nicht bewältigt werden hätte können. Die Hochschule hätte eine fünfstellige Zahl an Prüflingen und das gesamte Aufsichtspersonal im Stadtgebiet konzentrieren müssen. Ausweichmöglichkeiten hätten der Hochschule nicht zur Verfügung gestanden.

Die elektronische Fernprüfung ist nach § 1 Abs. 2 Satz 2 BayFEV – jedenfalls nach datenschutzrechtlichen Maßstäben – eine **rechtfertigungsbedürftige Ausnahme vom Regelfall**. Nach Art. 5 Abs. 2 DSGVO liegt es in der datenschutzrechtlichen Verantwortung der Hochschule, die Einhaltung der zentralen datenschutzrechtlichen Grundsätze, unter anderem der Rechtmäßigkeit, der Datenminimierung, der Speicherbegrenzung sowie der Integrität und Vertraulichkeit aus Art. 5 Abs. 1 Buchst. a, c, e und f DSGVO zu gewährleisten.

Die Hochschulen haben also nach Art. 5 Abs. 1 Buchst. c DSGVO unter anderem zu prüfen, inwiefern eine elektronische Verarbeitung personenbezogener Daten von Prüflingen in Gestalt einer elektronischen Fernprüfung tatsächlich erforderlich ist. Diese Verpflichtung besteht nach Art. 25 Abs. 1 DSGVO nicht nur bei Festlegung des Verarbeitungsmittels, sondern auch zum Zeitpunkt der eigentlichen Verarbeitung.

Auch nach **§ 8 Abs. 2 Satz 1 BayFEV** haben die Hochschulen festzustellen, ob und für wie viele Studierende eine Präsenzprüfung unter Beachtung der jeweils geltenden infektionsschutzrechtlichen Vorgaben und Empfehlungen angeboten werden kann.

Dem genügte der pauschale Vortrag der Hochschule nicht. Vielmehr wäre nötig gewesen, dass die Hochschule für jede konkrete Prüfung, die sie als elektronische Fernprüfung durchführen wollte, eine individuelle Kalkulation erstellt hätte, wonach unter den jeweils geltenden infektionsschutzrechtlichen Vorgaben eine Präsenzprüfung auch unter Einsatz erhöhter personeller und sachlicher Mittel für die Prüflinge nicht bzw. nicht für alle Prüflinge durchführbar gewesen wäre (vgl. auch § 8 Abs. 2 Satz 1 BayFEV).

Gleichwohl war nicht zu verkennen, dass die Hochschule bei der Planung und Durchführung der hier in Rede stehenden elektronischen Fernprüfung zu Beginn der Pandemie und noch vor Erlass der Bayerischen Fernprüfungserprobungsverordnung mit ganz erheblichen rechtlichen und praktischen Schwierigkeiten konfrontiert war. Vor diesem Hintergrund nahm ich für die damalige Ausnahmesituation den doch recht

pauschalen Vortrag zur Kenntnis und wies die Hochschule darauf hin, dass sie diese **Vorgaben bei eventuellen zukünftigen elektronischen Fernprüfungen zu beachten** hat.

10.2.1.3 § 4 Abs. 1 Satz 1, § 6 Abs. 1 BayFEV

§ 4 Abs. 1 Satz 1 BayFEV erlaubt, dass die Hochschulen im Rahmen elektronischer Fernprüfungen **personenbezogene Daten verarbeiten, soweit** dies **zur ordnungsgemäßen Durchführung der Prüfung zwingend erforderlich** ist. Dies gilt nach § 4 Abs. 1 Satz 2 BayFEV insbesondere für Zwecke der Authentifizierung nach § 5 BayFEV und der Videoaufsicht nach § 6 BayFEV.

§ 6 Abs. 1 BayFEV sieht Folgendes vor:

§ 6 BayFEV
Videoaufsicht bei Fernklausuren
(1) [1]Zur Unterbindung von Täuschungshandlungen während einer Fernklausur sind die Studierenden verpflichtet, die Kamera- und Mikrofonfunktion der zur Prüfung eingesetzten Kommunikationseinrichtungen zu aktivieren (Videoaufsicht). [2]Eine darüberhinausgehende Raumüberwachung findet nicht statt. [3]Die Videoaufsicht ist im Übrigen so einzurichten, dass der Persönlichkeitsschutz und die Privatsphäre der Betroffenen nicht mehr als zu den berechtigten Kontrollzwecken erforderlich eingeschränkt werden.

Die Begründung zur Vorschrift führt Folgendes aus:

„Abs. 1 Satz 1 regelt die Verpflichtung der Studierenden, während der Prüfung die Kamera- und Mikrofonfunktion der zur Prüfung eingesetzten Kommunikationseinrichtungen zu aktivieren, und beinhaltet insoweit eine Legaldefinition des Begriffes der Videoaufsicht. Dies wird im Regelfall die in modernen Computern eingebaute Kamera („Webcam“) und das interne Mikrofon, kann aber auch die Kamera und/oder das Mikrofon eines Smartphones sein, das zu Kontrollzwecken genutzt wird. Letzteres gilt insbesondere in den Fällen, in denen kein Computer mit Kamerafunktion vorhanden ist oder die interne Kamera (wie bei einem Tabletcomputer) bei bestimmungsgemäßem Gebrauch zur Videoaufsicht ungeeignet ist.“

Die Videoaufsicht erfolgt durch Aufsichtspersonal der Hochschulen (§ 6 Abs. 2 Satz 1 BayFEV). Somit sieht das Gesetz das sogenannte **live-proctoring als Normallfall** vor. Die **automatisierte Videoaufsicht nach § 6 Abs. 4 BayFEV ist dagegen die Ausnahme** „im Sinne einer ultima ratio-Maßnahme“ (vgl. Begründung zur Bayerischen Fernprüfungserprobungsverordnung). Dies entspricht der verfassungsrechtlichen Lage und dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO). Die von mir geprüfte Hochschule hatte – was ich aus datenschutzrechtlicher Sicht sehr begrüßte – von einer automatisierten Videoaufsicht Abstand genommen.

Vor diesem Hintergrund waren die **Videoaufnahmen** des Prüflings und die **Audioaufnahme** des Prüfungsraumes (Nachweis von Gesprächen) von § 4 Abs. 1, § 6 Abs. 1 und Abs. 2 BayFEV **gedeckt**.

10.2.1.4 Freiwilligkeit

Zentrales Kriterium für die gesetzliche Befugnis in § 4 Abs. 1 in Verbindung mit § 6 BayFEV ist die **Freiwilligkeit** der elektronischen Fernprüfung. In der Bayerischen Fernprüfungserprobungsverordnung findet sich das Kriterium in § 8 BayFEV. Aber

auch für die datenschutzrechtliche Einwilligung als Rechtsgrundlage (Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 7 DSGVO) ist die Freiwilligkeit eine maßgebliche Bedingung. § 8 BayFEV regelt hierzu Folgendes:

„(1) [1]Die Teilnahme an elektronischen Fernprüfungen erfolgt auf freiwilliger Basis. [2]Die Freiwilligkeit der Teilnahme ist grundsätzlich auch dadurch sicherzustellen, dass eine termingleiche Präsenzprüfung als Alternative angeboten wird. [3]Termingleich sind Prüfungen, die innerhalb desselben Prüfungszeitraums unter strenger Beachtung der Grundsätze der Chancengleichheit stattfinden.
(2) […][2]Kann eine Präsenzprüfung nicht durchgeführt werden oder melden sich zu viele Studierende für die Alternative der Präsenzprüfung an, können die Hochschulen Studierende auf den voraussichtlich nächstmöglichen Präsenzprüfungstermin verweisen. [3]Prüfungsrechtliche Nachteile dürfen dadurch nicht entstehen. […]“

10.2.2 Übermittlung des Bildes an Mitprüflinge

Die von mir geprüfte Hochschule hatte zur Durchführung der Videoaufsicht bei der Fernprüfung unter anderem eine Software eingesetzt, welche die Problematik einer Datenübermittlung in die USA aufwarf, die ich in diesem Beitrag nicht weiter vertiefe. Bei Einsatz dieser Software wurde zudem jedenfalls das **Bild des** Prüflings durch die Webcam nicht nur an die Aufsicht übermittelt, sondern auch an alle anderen Mitprüflinge.

Dies stellt eine Datenübermittlung des Bildes durch die Hochschule an die Mitprüflinge dar, für welche die Hochschule eine Rechtsgrundlage benötigte (vgl. Art. 6 Abs. 1 UAbs. 1DSGVO).

10.2.2.1 Aufnahmen durch Mitprüflinge möglich

Damit im Zusammenhang steht auch das Problem, dass Prüflinge von den anderen Mitprüflingen (unbefugt) Aufnahmen machen oder speichern konnten. Zwar hatte die Hochschule versucht, dieses Risiko durch technisch-organisatorische Maßnahmen zu verringern. Zum einen hatte sie in der Musteranleitung darauf hingewiesen, dass die Prüfungen weder von der Aufsicht noch von den Prüflingen aufgezeichnet werden dürfen. Auch hatte die Hochschule mitgeteilt, dass technisch mittels zentraler Vorgabe die Aufnahmefunktion deaktiviert worden sei. Gleichwohl ist damit nicht ausgeschlossen, dass Prüflinge mit einer (Foto-/Handy-)Kamera die auf dem Bildschirm angezeigten Mitprüflinge fotografieren oder filmen.

10.2.2.2 Keine gesetzliche Befugnis

Auf die gesetzliche Befugnis zur Datenverarbeitung nach § 4 Abs. 1, § 6 Abs. 1 BayFEV konnte sich die Hochschule nicht stützen. Denn die Übermittlung des Bildes an die Mitprüflinge war weder für die Kontrollzwecke der Aufsicht noch für die Durchführung der Klausur erforderlich. Im Gegenteil: § 6 Abs. 1, Abs. 2 BayFEV sieht bei der Videoaufsicht nur eine Übermittlung an das Aufsichtspersonal der Hochschule vor. Zudem ist die Videoaufsicht so einzurichten, dass der Persönlichkeitsschutz und die Privatsphäre der Betroffenen nicht mehr als zu den berechtigten Kontrollzwecken erforderlich eingeschränkt werden (Art. 6 Abs. 1 Satz 3 BayFEV). Dem widerspricht die Übermittlung des Bildes an die Mitprüflinge.

Auch den in der Sache wenig substantiierten Vortrag der Hochschule, wonach diese Software erforderlich gewesen sei, da die Kapazitätsgrenze der On-Premise-Systeme ohne Einbindung weiterer Alternativen einen regulären Prüfungsbetrieb bei weitem nicht zugelassen hätte, konnte ich aus Datenschutzsicht nicht gelten lassen. Denn auch nach der Rechtsprechung des Bundesverfassungsgerichts gilt: „Die Anforderungen an die technische Datenverarbeitung haben insoweit den Anforderungen des Grundrechts auf informationelle Selbstbestimmung zu genügen und nicht umgekehrt."[92]

10.2.2.3 Keine wirksame Einwilligung

Die Hochschule hatte für die hier in Rede stehende Datenverarbeitung auch eine Einwilligung der Prüflinge unter anderem zur Übermittlung des Bildes an die Mitprüflinge eingeholt. Diese Einwilligung war nach meiner Auffassung jedoch unwirksam.

Denn mit der Einwilligung darf eine öffentliche Stelle nicht die Bindungen der gesetzlichen Verarbeitungsbefugnisse unterlaufen.[93] Vorliegend sieht – wie vorstehend erläutert – die gesetzliche Konzeption gerade nicht vor, dass das Bild an die Mitprüflinge übermittelt wird. Dies ist im Übrigen auch ein Gebot des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO).

Überdies fehlte es bei den Einwilligungen wohl auch an der notwendigen Freiwilligkeit. Denn eine gleichwertige Alternative zu dieser Datenverarbeitung (etwa die Nutzung eines Videokonferenztools, bei dem das Bild nicht an die Mitprüflinge übermittelt wird) wurde nicht angeboten. Insoweit genügte der Verweis auf eine alternative Präsenzprüfung nicht, da er einen anderen Bezugspunkt hat, nämlich nicht die hier in Rede stehende Datenübermittlung an die Mitprüflinge, sondern die insgesamt mit der elektronischen Fernprüfung verbundene Datenverarbeitung.

Da somit keine Rechtsgrundlage für die Übermittlung des Bildes an die Mitprüflinge vorlag, rügte ich gegenüber der Hochschule einen Datenschutzverstoß.

10.3 Öffentliche Theater und Museen: Online-Ticketkauf mit Kundenkonto

Bereits im Beitrag Nr. 11.4 meines 28. Tätigkeitsberichts 2018 äußerte ich mich zum Datenschutz beim Online-Ticketkauf. Die zentralen Aussagen dieses Beitrags lauten zusammengefasst:

— Ein Kundenkonto ist für die Abwicklung des Online-Ticketverkaufs nicht erforderlich. Das heißt, das Theater kann sich – für die Speicherung eines Kontos über den Verkauf hinaus – insoweit nicht auf die gesetzliche Befugnis nach Art. 4 Abs. 1 BayDSG bzw., wenn dem Online-Kartenverkauf ein Vertrag zwischen dem Kunden und einem Theater zugrunde liegt, nicht auf Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO stützen.

— Ein Kundenkonto muss nach der Abwicklung des Ticketverkaufs gelöscht werden.

92 Bundesverfassungsgericht, Beschluss vom 13. Mai 2015, 1 BvR 99/11, BeckRS 2015, 52585.

93 Bayerischer Landesbeauftragter für den Datenschutz, Die Einwilligung nach der Datenschutz-Grundverordnung, Stand 09/2021, Rn. 19 ff., Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Einwilligung".

— Eine Beibehaltung des Kontos aus Servicegründen – etwa um zukünftige Käufe zu erleichtern – ist nur aufgrund einer wirksamen Einwilligung denkbar.

Diese Aussagen lassen sich auch auf den Online-Ticketverkauf von – staatlichen oder kommunalen – Museen übertragen.

Im Ergebnis bedeutet dies, dass ein öffentliches Theater oder Museum für den Online-Ticketverkauf zwingend ein Gastkonto oder einen Gastzugang anbieten muss. Der Kauf im Webshop muss ohne die dauerhafte Anlegung eines Kundenkontos durchzuführen sein, das typischerweise die E-Mail-Adresse und ein Passwort sowie weitere personenbezogene Daten enthält (wie etwa Name, Anrede, Adresse, Telefonnummer, Kaufhistorie).

Seit dem oben erwähnten Beitrag gingen weitere Beschwerden von Bürgerinnen und Bürgern gegen bayerische staatliche Theater und Museen ein, die insbesondere rügten, dass die betreffenden öffentlichen Einrichtungen beim Online-Ticketkauf keinen Erwerb über ein Gastkonto erlauben. Bei der Durchsetzung der Rechte betroffener Bürgerinnen und Bürger musste ich feststellen, dass sich einzelne öffentliche Theater und Museen mit verschiedenen Argumenten gegen ein Gastkonto „sträuben". Daher verdeutliche ich im Folgenden nochmals meine Auffassung:

— Eine zwingende Erstellung eines Kundenkontos kann nicht etwa mit der Berufung auf die mitunter langen Zeiträume zwischen Kauf und Erfüllung, Unwägbarkeiten bezüglich der Leistungserfüllung, möglichen Leistungsstörungen oder Problemen bei der Zahlungsabwicklung gerechtfertigt werden. Gleiches gilt für die Geltendmachung von Anfechtungs-, Widerrufs- oder Widerspruchsrechten bezüglich der gewählten Zahlungsart.

  Eine Kontaktierung der Kundinnen und Kunden kann in diesen Fällen auch mittels eines Gastzugangs erfolgen. Auch bei einem Gastzugang muss ein Kunde personenbezogene Daten angeben, die für die Abwicklung des Onlinekaufs erforderlich sind. Diese Daten werden bei einem Gastzugang vom Theater oder Museum in einem Kundendatensatz gespeichert. Für diese Datenverarbeitungen gibt es grundsätzlich gesetzliche Befugnisse (Art. 4 Abs. 1 BayDSG bzw. Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO). Mit einer in diesem Zusammenhang erhobenen E-Mail-Adresse können die Kundinnen und Kunden – ohne die Anlage eines dauerhaften Kundenkontos – kontaktiert werden.

— Die Berufung auf eine „unternehmerische Entscheidung", keinen Gastzugang anzubieten, trägt nicht. Die unternehmerischen Entscheidungen müssen sich selbstverständlich im Rahmen der geltenden Datenschutzgesetze bewegen. Gleiches gilt in Bezug auf das zuweilen vorgebrachte Argument, ein Kundenkonto sei für die Marketingstrategie des Betriebs nötig.

— In Bezug auf ein Kundenkonto genügt es auch nicht, wenn der Webshop vorsieht, dass Neukunden in die Anlage eines Kundenkontos einwilligen, und er dabei einen Hinweis auf die anonyme Kaufmöglichkeit an der Tages- oder Abendkasse gibt.

  - Ein vorliegender Hinweis im Online-Ticketshop auf die anonyme Bezahlmöglichkeit an der Tages- und Abendkasse ist zwar zu begrüßen und notwendig. Dies alleine genügt aber nicht, um die Anlage eines Kundenkontos auf eine Einwilligung stützen zu können.

- Denn die **Wirksamkeit** der **Einwilligung** setzt insbesondere voraus, dass sie **freiwillig** ist. Die Freiwilligkeit bedingt vor allem, dass der Einwilligende eine echte oder freie Wahl haben muss und somit in der Lage sein muss, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden (Erwägungsgrund 42 DSGVO). Auch das sogenannte Koppelungsverbot ist von Bedeutung. Dieses wird in der Datenschutz-Grundverordnung wie folgt erläutert: Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind (Art. 7 Abs. 4 DSGVO). **Die Einwilligung gilt nicht als freiwillig erteilt,** wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, **oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist** (Erwägungsgrund 43 DSGVO).

  Wie eben dargelegt, ist ein Kundenkonto im Grundsatz für den Verkauf von Online-Tickets für Theateraufführungen oder Museumsbesuche nicht erforderlich.

  Eine **echte, freie Wahl** beim Kauf eines Online-Tickets hat ein Kunde **nur, wenn ein Online-Kauf auch über einen Gastzugang oder ein Gastkonto möglich ist.**

  Der Verweis auf eine Kaufmöglichkeit an der Tages- oder Abendkasse ist dagegen keine gleichwertige Alternative zum Angebot eines Gastzugangs oder Gastkontos. Denn um diese Möglichkeit zu nutzen, muss der Kunde die Verkaufsstellen zu den (eingeschränkten) Öffnungszeiten persönlich aufsuchen, während im Online-Ticketshop ein Kauf „rund um die Uhr" möglich ist. Ein Kauf an der Abendkasse ist regelmäßig auf ein geringeres Angebot (Restposten) reduziert.

- Um Missverständnissen vorzubeugen: Das Erfordernis eines Gastzugangs zur Sicherstellung der Freiwilligkeit eines Kundenkontos beim Online-Ticketverkauf bedeutet nicht, dass auf das Angebot einer anonymen Kaufmöglichkeit an der Tages- oder Abendkasse verzichtet werden kann. Diese anonyme Bezahlmöglichkeit ist unabhängig von der Frage eines Kundenkontos notwendig, um überhaupt eine anonyme Kaufmöglichkeit von Theater- oder Museumstickets und damit eine anonyme Besuchsmöglichkeit von Theatern oder Museen zu erhalten. Denn bei einem Online-Ticketkauf werden – unabhängig davon, ob mit Kundenkonto oder Gastzugang – stets personenbezogene Daten verarbeitet. Mit anderen Worten: Die Tages- oder Abendkasse sichert somit im Sinne des Datenschutzes die Einhaltung des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) beim Ticketverkauf.

- Zahlreiche Online-Webshops sehen mittlerweile die Möglichkeit des Kaufs mittels Gastkonto oder Gastzugang vor. Dies belegt, dass ein Online-Ticketvertrieb auch mittels Gastkonto faktisch realisierbar ist.

- Öffentliche Stellen, wie die staatlichen oder kommunalen Theater und Museen, sind – anders als private Organisationen (wie etwa ein privat betriebenes Kino) – unmittelbar grundrechtsgebunden, also auch in Bezug auf das Recht auf informationelle Selbstbestimmung. Mit diesem Befund kommt öffentlichen Stellen im Umgang mit personenbezogenen Daten eine besondere Verantwortung zu. Auch sollten öffentliche Stellen in Bezug auf den Datenschutz eine Vorbildfunktion ausüben und somit allein schon aus diesem Grund den Online-Kauf als Gast ermöglichen.

Die zentrale datenschutzrechtliche Botschaft lautet somit kurz gefasst: **Die Einräumung der Möglichkeit eines Kaufs über einen Gastzugang ist notwendige Bedingung, damit eine Einwilligung in die Datenverarbeitung zur Anlage eines Kundenkontos aus Datenschutzsicht freiwillig ist und damit für das Anlegen eines Kundenkontos eine datenschutzrechtliche Befugnis vorliegt.**

Diese **Auffassung** wird **auch** von den anderen Datenschutzaufsichtsbehörden vertreten. So hat die **Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 24. März 2022 Hinweise zum datenschutzkonformen Online-Handel mittels Gastzugang beschlossen.**[94]

Mir ist freilich bewusst, dass die öffentlichen Theater und Museen für eine Implementierung eines Gastkontos auf die Kooperation des Softwareanbieters angewiesen sind oder den Anbieter wechseln müssen. Allerdings erinnere ich in diesem Zusammenhang wiederholt an den – im Rechtsstaat selbstverständlichen – Grundsatz, dass die Anforderungen an die technische Datenverarbeitung dem Datenschutzrecht zu folgen haben und nicht umgekehrt. **Gegen Ende des Berichtszeitraums** teilten mir **erfreulicherweise mehrere öffentliche Stellen mit, dass sie mit ihren Dienstleistern nach technischen Lösungen suchen, um Gastzugänge anzubieten. Ich werde weiterhin darauf drängen, dass die bayerischen öffentlichen Theater und Museen beim Online-Ticketkauf zeitnah einen Gastzugang anbieten.**

94 Internet: https://www.datenschutzkonferenz-online.de, Rubrik „Infothek - Beschlüsse".

11 Zensus

11.1 Zensus 2022

11.1.1 Hintergrund und Vorbereitungen

Im Berichtszeitraum fanden zum Stichtag 15. Mai 2022 die Erhebungen zum Zensus 2022 statt. Im Gesamtzusammenhang des Zensus 2022 habe ich Gesetzgebungsverfahren, die Vorbereitungen und die Durchführung aus datenschutzrechtlicher Sicht kritisch begleitet.

Die **Verordnung (EG) Nr. 763/2008**[95] verpflichtet die Mitgliedstaaten der Europäischen Union zur Erfassung von Bevölkerungsdaten. Unter anderem zur Erfüllung dieser Verpflichtung wurde am 3. März 2017 das **Zensusvorbereitungsgesetz 2021** verabschiedet. Es regelt alle notwendigen Schritte zum Aufbau der für den registergestützten Zensus erforderlichen Infrastruktur sowie zum Aufbau und zur Pflege des Steuerungsregisters. Es folgte sodann am 26. November 2019 das **Zensusgesetz 2021**, welches die konkrete Durchführung regelt. Es legt unter anderem die einzelnen Merkmale fest, die erhoben werden sollen. Auch die Auskunftspflicht, Maßnahmen zur Gewährleistung des Datenschutzes und die Kostenaufteilung zwischen Bund und Ländern sind darin geregelt. Der ursprünglich für das Jahr 2021 geplante Zensus wurde aufgrund der Corona-Pandemie mit dem „Gesetz zur Verschiebung des Zensus in das Jahr 2022 und zur Änderung des Aufenthaltsgesetzes“ vom 3. Dezember 2020 um ein Jahr verschoben. Das Zensusgesetz 2021 wurde in **Zensusgesetz 2022** umbenannt. Auch das Bayerische Statistikgesetz wurde in einem neuen Abschnitt IVa um die länderspezifischen Regelungen für Bayern ergänzt. So bestimmt etwa Art. 25a Bayerisches Statistikgesetz (BayStatG), dass für den Vollzug des Zensusgesetzes 2022 in Bayern grundsätzlich das Bayerische Landesamt für Statistik (im Folgenden: Landesamt) zuständig ist.

Im Rahmen des Gesetzgebungsverfahrens nahm ich mehrfach gegenüber dem Bayerischen Staatsministerium des Innern, für Sport und Integration Stellung. So trug ich dadurch zum Beispiel maßgeblich dazu bei, dass eine vergleichbare Regelung wie in § 11 Abs. 3 Sätze 3 und 4 Zensusgesetz 2011 (ZensG 2011) – Erhebungsbeauftragte dürfen nicht in der unmittelbaren Nähe ihrer Wohnung eingesetzt werden – auch in das Zensusgesetz 2022 aufgenommen wurde. Zudem wies ich darauf hin, dass aus Gründen der Datensparsamkeit auf Fragen verzichtet werden sollte, die über die Vorgaben der Europäischen Union hinausgehen.

Im Vorfeld der Erhebungen wurde ich mehrfach vom Landesamt zur Beratung der Abläufe hinzugezogen. Hierbei drängte ich beispielweise auf eine genaue Abgrenzung der datenschutzrechtlichen Verantwortlichkeiten zwischen dem Landesamt und dem Statistischen Bundesamt. Dies ist insbesondere auch für die Informationspflich-

95 Verordnung (EG) Nr. 763/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über Volks- und Wohnungszählungen (ABl. L 218 vom 13. August 2008, S. 14).

ten und die Geltendmachung der Betroffenenrechte nach der Datenschutz-Grundverordnung relevant. Letztlich wurde auch eine **Vereinbarung nach Art. 26 DSGVO** zwischen den Ämtern geschlossen.

Ich machte im Rahmen der Vorbereitungen außerdem geltend, dass die Hinweise in den **ländereinheitlichen Informationsblättern** noch verbessert werden können, und forderte eine bayernspezifische Information insbesondere zur Verantwortlichkeit des Landesamts für die Ausübung der Betroffenenrechte. Dem folgte das Landesamt durch ein zusätzliches Hinweisblatt.

Nach den Erfahrungen aus der Beratungspraxis im Zusammenhang mit der Vorbefragung zur Gebäude- und Wohnungszählung hatte der Umstand, dass die Informationsblätter vorrangig die Möglichkeit einer elektronischen Auskunftserteilung aufzeigten, bei einem Teil der betroffenen Personen zu erheblichen Verunsicherungen geführt. Gemäß § 23 Zensusgesetz 2022 (ZensG 2022) erfolgt die Auskunftserteilung **grundsätzlich elektronisch. Eine schriftliche Auskunftserteilung ist jedoch möglich.** Die Beschwerden aufgreifend erreichte ich beim Landesamt, dass bei der Hauptbefragung ausdrücklich auf diese Alternative hingewiesen wurde (vgl. auch Art. 13 Abs. 2 Buchst. e DSGVO).

Die kreisfreien Gemeinden und Landkreise richteten zur Durchführung des Zensus vielfach gemäß § 19 ZensG 2022 in Verbindung mit Art. 25b BayStatG sogenannte **örtliche Erhebungsstellen** ein. Ich wies im Vorfeld darauf hin, dass die datenschutzrechtliche Verantwortlichkeit der Erhebungsstellen klarer herausgearbeitet werden sollte. Dies ist wohl leider nicht in der erforderlichen Deutlichkeit gelungen. Jedenfalls erhielt ich hierzu wiederholt Anfragen von betroffenen Personen , denen ich dann die genauen Verantwortlichkeiten erläuterte.

11.1.2 Durchführung des Zensus 2022

Die Durchführung des Zensus 2022 verfolgte ich kritisch. Verschiedentlich holte ich dazu Stellungnahmen beim Landesamt ein. Die Nachfragen waren insbesondere durch die bei mir eingegangenen Beschwerden veranlasst. Im Folgenden stelle ich ausgewählte Fallgruppen und meine Bewertungen dazu dar:

— **Beschwerden gegen den Zensus 2022 als solchen oder die konkrete Erhebungsmethode**

Seit dem Beginn der Haupterhebungen im Mai 2022 gingen einige Beschwerden bei mir ein, die entweder die Datenerhebung anlässlich des Zensus 2022 im Allgemeinen oder auch die konkrete Erhebungsmethode kritisierten. Den Anfragenden erläuterte ich insbesondere mit den folgenden Hinweisen die Rechtslage:

Mit dem Zensus 2022 folgt Deutschland auch seiner Verpflichtung aus der Verordnung (EG) Nr. 763/2008, alle zehn Jahre den Bevölkerungsstand festzustellen und bestimmte Strukturmerkmale sowie den Wohnungsbestand zu ermitteln.

Zwar war das Volkszählungsgesetz 1983 vom Bundesverfassungsgericht in Teilen für verfassungswidrig erklärt und die Zählung damit gestoppt worden. Auch gilt die damalige Entscheidung bis heute als wegweisend für den Datenschutz, zumal darin das **„Recht auf informationelle Selbstbestimmung“** als

Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz – GG) konturiert wurde.

Anders als bei der Volkszählung 1983 handelte es sich beim Zensus 2022 jedoch nicht um eine Vollerhebung, sondern um eine registergestützte Erhebung. Schon für den Zensus 2011 wurde in großem Umfang auf bestehende Datenbestände aus Verwaltungsregistern als Basis zurückgegriffen. Dieses Grundprinzip wurde auch für den Zensus 2022 beibehalten. **Die Verfassungskonformität dieser Erhebungsmethode wurde vom Bundesverfassungsgericht zum Zensusgesetz 2011 bestätigt.**[96]

Zentraler Erlaubnistatbestand für die Verarbeitung personenbezogener Daten im Rahmen des Zensus 2022 ist dabei Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO in Verbindung mit den Regelungen des Zensusgesetzes 2022.

— **Beschwerden über einzelne Fragestellungen**

Außerdem wandten sich Bürgerinnen und Bürger mit der Sorge an mich, dass einzelne im Rahmen des Zensus 2022 gestellte Fragen nicht erforderlich und daher unzulässig seien.

Entscheidend für die Zulässigkeit der einzelnen Fragen ist, dass der Bundesgesetzgeber in §§ 10, 13 und 15 ZensG 2022 ausdrücklich festgelegt hat, welche Daten als Erhebungsmerkmale und Hilfsmerkmale erhoben werden dürfen. Aus seiner Sicht sind mit den getroffenen Regelungen die Zwecke des Zensus 2022 mit dem Grundsatz der Datensparsamkeit und dem informationellen Selbstbestimmungsrecht der Betroffenen am besten in Einklang zu bringen.

Die in den konkreten Beschwerden gerügten Fragestellungen überprüfte ich im Einzelnen. Dabei konnte ich nicht feststellen, dass über die gesetzlichen Vorgaben hinausgehende Fragen gestellt worden wären. So standen im Mittelpunkt der Eingaben beispielsweise die Fragen nach den Bewohnern einer vermieteten Immobilie oder nach Straße, Hausnummer und Anschriftenzusatz, die nach § 10 Abs. 2 Nrn. 3 und 5 ZensG 2022 erhoben werden dürfen.

Gegen die **Erhebung gesetzlich festgelegter Daten habe ich datenschutzrechtlich nichts zu erinnern**. Ich erläuterte den anfragenden Personen jeweils die geltenden Bestimmungen und versuchte dabei auch, ihnen die gesetzgeberischen Entscheidungen, etwa durch einschlägige Zitate aus der Gesetzesbegründung, nachvollziehbar zu machen.

— **Beschwerden über die Auswahl der Auskunftspflichtigen**

Bei manchen betroffenen Personen schien der Eindruck entstanden zu sein, dass immer dieselben Auskunftspflichtigen zu statistischen Befragungen herangezogen werden. Im Rahmen mehrerer Beschwerden wurde eine zufällige Auswahl zum Zensus 2022 bezweifelt. Auch in diesen Fällen konnte ich den Bürgerinnen und Bürgern durch Erläuterungen des gesetzlich festgelegten Auswahlverfahrens weiterhelfen:

96 Bundesverfassungsgericht, Urteil vom 19. September 2018, 2 BvF 1/15, 2 BvF 2/15, BeckRS 2018, 22100.

Beim Zensus 2022 findet zum einen gemäß § 11 ZensG 2022 die **Haushaltebefragung** auf Basis einer Stichprobe von Anschriften statt. Weiter werden alle Personen, die in Wohnheimen und Gemeinschaftsunterkünften leben, befragt. Gemäß § 22 ZensG 2022 sind hierbei auch Wiederholungsbefragungen zur Qualitätssicherung möglich.

Außerdem werden **Eigentümerinnen und Eigentümer** im Rahmen der **Gebäude- und Wohnungszählung** (im Folgenden: GWZ) angeschrieben und um Auskunft gebeten. Ziel der GWZ ist die flächendeckende und vollzählige Erfassung aller am Erhebungsstichtag bestehenden Gebäude mit Wohnraum, bewohnten Unterkünften sowie der darin befindlichen Wohnungen. Auskunftspflicht besteht für alle Eigentümerinnen und Eigentümer, Verwalterinnen und Verwalter sowie sonstige Verfügungs- und Nutzungsberechtigte von Gebäuden oder Wohnungen (§ 24 Abs. 1 ZensG 2022). Im Gegensatz zur Haushaltebefragung erfolgt die GWZ damit nicht aufgrund einer Stichprobe und damit einer zufälligen Auswahl, sondern einer flächendeckenden Gesamterfassung. Rechtsgrundlage hierfür bildet § 9 ZensG 2022.

Im Herbst 2021 erfolgte gemäß § 6 Abs. 1 Bundestatistikgesetz (BStatG) außerdem die **Vorbefragung zur GWZ**. Dabei wurde ein Teil aller Eigentümerinnen und Eigentümer sowie der Verwalterinnen und Verwalter befragt. Hierdurch wurde ermittelt, ob die vorliegenden Verwaltungsdaten aktuell und von guter Qualität sind.

Darüber hinaus findet unabhängig vom Zensus 2022 der **Mikrozensus** (siehe dazu auch meinen Beitrag Nr. 11.2) als sogenannte „kleine Bevölkerungszählung" statt. Hierbei werden gemäß dem Gesetz zur Durchführung einer Repräsentativstatistik über die Bevölkerung und die Arbeitsmarktbeteiligung sowie die Wohnsituation der Haushalte (Mikrozensusgesetz) circa ein Prozent der Bevölkerung zu ihren Arbeits- und Lebensbedingungen befragt.

Die Regelungen des Mikrozensusgesetzes, des Bundesstatistikgesetzes und Zensusgesetzes 2022 können also dazu führen, dass dieselbe Person im Lauf der Zeit **mehrfach zur Auskunft herangezogen wird**, ohne dass daraus eine besondere Auffälligkeit im Hinblick auf die Verarbeitung der personenbezogenen Daten dieser Person zu folgern wäre. Anhaltspunkte für unzulässige Datenverarbeitungen in diesem Zusammenhang haben sich nicht ergeben.

– **Beschwerden im Zusammenhang mit der Einbindung eines US-amerikanischen IT-Dienstleisters**

Zum Einsatz eines US-amerikanischen IT-Dienstleisters bei der Zensus 2022-Webseite erreichten mich zahlreiche Anfragen. Den Anfragenden teilte ich mit, dass die betroffene Zensus 2022-Webseite nach deren Datenschutzerklärung vom Statistischen Bundesamt betrieben wird. Dessen **Datenschutz-Aufsichtsbehörde ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit**. Der Bundesbeauftragte stellte in seiner ersten Überprüfung fest, dass keine Gefahr für die auf der Zensus-Webseite eingegebenen Daten bestanden habe. Die Prüfung der Webseite durch den Bundesbeauftragten war im Berichtszeitraum aber noch nicht abgeschlossen.

– **Beschwerden im Zusammenhang mit der Tätigkeit von Erhebungsbeauftragten**

Ich erhielt diverse Anrufe und Zuschriften durch Betroffene, die im Rahmen des Zensus 2022 von Erhebungsbeauftragten kontaktiert wurden.

Dazu ist zunächst festzuhalten, dass die Möglichkeit, für die Erhebung einer Bundesstatistik amtlich betraute Personen einzusetzen (sogenannte „**Erhebungsbeauftragte“), in § 14 BStatG und für den Zensus 2022 zusätzlich ausdrücklich in § 20 ZensG 2022 sowie in Art. 25d BayStatG normiert wird.**

Einige Bürgerinnen und Bürger hatten konkret die Befürchtung, dass die Personen, welche sie in Sachen Zensus 2022 kontaktierten, keine „echten“ Erhebungsbeauftragten gewesen wären. Hier konnte ich im Wege der Beratung unter anderem durch folgende Hinweise Unterstützung leisten:

Um einen Nachweis für die Legitimation als Erhebungsbeauftragter zu erbringen und damit auch Missbrauch vorzubeugen, ist von den Statistischen Ämtern des Bundes und der Länder vorgesehen, dass sich die Erhebungsbeauftragten mittels eines **speziellen Ausweises für Erhebungsbeauftragte** in Kombination mit einem amtlichen Lichtbildausweis entsprechend ausweisen. Das Landesamt wies auch in einer Pressmitteilung darauf hin, wonach bei Zweifeln an der Legitimität des Erhebungsbeauftragten oder der Echtheit eines vorgelegten Ausweises die zuständige Erhebungsstelle, Polizeidienststelle oder das Landesamt kontaktiert werden soll.

Die meisten der Beschwerdeführerinnen und Beschwerdeführer sorgten sich allerdings um die Sicherheit ihrer Daten vor dem Hintergrund eventueller Weitergaben an Dritte, insbesondere auch im Zusammenhang mit den eingesetzten Tablets.

Bisher konnte ich jedoch bei keinem der mir vorgetragenen Fälle feststellen, dass Erhebungsbeauftragte personenbezogene Daten an Dritte weitergegeben hatten. Der Bundesgesetzgeber traf hierzu auch Vorsorge. So bestimmt beispielsweise § 14 Abs. 2 BStatG, dass die **Erhebungsbeauftragten die aus ihrer Tätigkeit gewonnenen Erkenntnisse nicht in anderen Verfahren oder für andere Zwecke verwenden dürfen** und auf die Wahrung des Statistikgeheimnisses nach § 16 BStatG und zur Geheimhaltung auch solcher Erkenntnisse schriftlich zu verpflichten sind, die gelegentlich ihrer Tätigkeit gewonnen werden. Diese Verpflichtung gilt auch nach Beendigung ihrer Tätigkeit.

Vom Landesamt wurden für den Zensus 2022 und speziell auch für die dortige Verwendung der mobilen Endgeräte diverse Schutzmaßnahmen in organisatorischer und technischer Hinsicht getroffen und mir nachgewiesen. So werden beispielsweise die erfassten Daten nach Abschluss der Befragung von den mobilen Endgeräten an eine zentrale Speicherlösung übertragen. Sobald die Daten erfolgreich übertragen wurden, werden sie auf dem mobilen Endgerät gelöscht und stehen auch den Erhebungsbeauftragten nicht mehr zur Verfügung.

— **Beschwerden zur Einbeziehung von Auftragsverarbeitern**

Weitere Bürgerinnen und Bürger wandten sich wegen Datenweitergaben an externe Unternehmen im Zusammenhang mit dem Zensus 2022 an mich.

Nach entsprechender Befassung konnte ich den anfragenden Personen mitteilen, dass die Weitergabe der Daten datenschutzrechtlich grundsätzlich nicht zu bemängeln ist.

Art. 28 DSGVO sieht die Möglichkeit einer Auftragsverarbeitung ausdrücklich vor. Auftragsverarbeitung im Sinne des Datenschutzrechts bedeutet die Verarbeitung personenbezogener Daten durch einen Auftragsverarbeiter (regelmäßig einen entsprechenden Dienstleister) im Auftrag des Verantwortlichen. Dabei wird dem Auftragsverarbeiter nicht die eigentliche (Verwaltungs-) Aufgabe übertragen, sondern nur eine Hilfstätigkeit. Vorliegend war dies der Druck und Versand der Anschreiben zum Zensus 2022.

Durch einen entsprechenden Vertrag kann zwischen dem Verantwortlichen und dem Auftragsverarbeiter eine rechtlich ausreichende Basis für die Weitergabe der Daten an einen Dienstleister geschaffen werden. In datenschutzrechtlicher Hinsicht gilt bei der Auftragsverarbeitung insoweit nichts anderes als beim Einsatz von eigenem Personal des Verantwortlichen; der Auftragsverarbeiter ist datenschutzrechtlich zwar Empfänger der Daten gemäß Art. 4 Nr. 9 DSGVO, jedoch kein „Dritter“ (vgl. Art. 4 Nr. 10 DSGVO).

Da das Fachrecht die Begründung eines Auftragsverarbeitungsverhältnisses für die fraglichen Dienstleistungen nicht ausschloss, war gegen den Einsatz von Dienstleistern für Druck und Versand der Anschreiben aus Datenschutzsicht grundsätzlich nichts zu erinnern.

11.2 Mikrozensus

Auch im Zusammenhang mit dem Mikrozensus wandten sich Betroffene an mich und **zweifelten** dabei insbesondere eine **zufällige Auswahl** ihrer Person **an**.

Nach § 4 Abs. 1 Mikrozensusgesetz (MZG) werden die Erhebungseinheiten auf der Grundlage von Flächen oder vergleichbaren Bezugsgrößen (Auswahlbezirke) ausgewählt. Die Erhebungseinheiten werden durch mathematisch-statistische Verfahren bestimmt. Ausgangspunkt der Auswahl sind also nicht die zu befragenden Personen als solche, sondern Zählbezirke, in denen dann alle dort wohnenden Haushalte bzw. Personen einbezogen und befragt werden. Das Mikrozensusgesetz regelt in § 5 Abs. 1 MZG zudem die sogenannte Periodizität. Dies bedeutet, dass ein einmal ausgewählter Zählbezirk und damit dann die darin enthaltenen Haushalte bzw. Personen innerhalb von fünf aufeinanderfolgenden Kalenderjahren bis zu viermal (eine Erstbefragung und drei Folgebefragungen in den nächsten Jahren) befragt werden können. Diese Folgebefragungen beruhen in diesem Rahmen dann jedoch nicht auf einer nochmaligen zufälligen Auswahl im Sinne des § 4 Abs. 1 MZG, sondern auf der bereits erfolgten Auswahl zur Erstbefragung.

Im Falle einer späteren erneuten Auswahl nach § 4 Abs. 1 MZG, die dann **auf einer erneuten zufälligen Auswahl eines Zählbezirks und nicht der Auswahl einer Einzelperson** beruhen würde, kann es in Kombination mit Folgebefragungen nach § 5 Abs. 1 MZG je nach konkreter Konstellation in der Summe zu einer erheblichen Anzahl von Befragungen kommen. Die Regelungen des Mikrozensusgesetzes können also dazu führen, dass dieselbe Person im Lauf der Zeit über einen im jeweiligen Zählbezirk gelegenen Wohnsitz in einer erheblichen Anzahl von Jahren zur Auskunft herangezogen wird, ohne dass daraus eine besondere Auffälligkeit im Hinblick auf die Verarbeitung der personenbezogenen Daten dieser Person zu folgern wäre.

Konkrete Anhaltspunkte, dass das Landesamt in diesem Zusammenhang personenbezogene Daten unzulässig verarbeitet hatte, konnte ich nicht erkennen.

12 Technik und Organisation

12.1 Datenschutzrechtliche Anforderungen für Penetrationstests

Täglich neue Meldungen und Hinweise aus dem Bereich der Sicherheit der Verarbeitung und der IT-Sicherheit zeigen, dass auch bayerische öffentliche Stellen in den Fokus der Cyberkriminalität geraten können. Bei digitalisierten Verarbeitungen sind Verantwortliche aufgerufen, Angriffsmöglichkeiten Dritter frühzeitig zu entdecken und durch technisch-organisatorische Maßnahmen wirksam zu verhindern. Sogenannte Penetrationstests sind eine erprobte und geeignete Maßnahme, um das Angriffspotenzial bei digitalisierten Verarbeitungen festzustellen. Bei einem solchen Test werden die Erfolgsaussichten eines vorsätzlichen Angriffs in Form einer Momentaufnahme eingeschätzt und daraus notwendige ergänzende Schutzmaßnahmen abgeleitet bzw. die Wirksamkeit von bereits umgesetzten Schutzmaßnahmen überprüft.[97]

Im Rahmen eines Penetrationstests kann regelmäßig nicht ausgeschlossen werden, dass zumindest die Durchführenden Zugriff auf personenbezogene Daten erhalten und diese verarbeiten. In diesem Fall stellt der Test selbst eine Verarbeitung dar, welche die einschlägigen datenschutzrechtlichen Anforderungen erfüllen muss.

Auch einige Datenpannenmeldungen von bayerischen öffentlichen Stellen bestätigen eindrucksvoll, dass bei einem Penetrationstest datenschutzrechtliche Aspekte vorab zu beachten und Risiken zu reduzieren sind, um auch bei solchen Tests ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Der Verantwortliche kann Penetrationstests entweder selbst vornehmen oder sie durch andere Stellen als Dienstleister durchführen lassen. In beiden Fällen ist insbesondere auf die folgenden Punkte zu achten:

– **Klassifizierung eines Penetrationstests:**

  Üblicherweise werden technische Penetrationstests in Blackbox- und Whitebox-Tests unterteilt, wobei Kombinationen aus diesen beiden Tests als Greybox-Test bezeichnet werden. Bei einem Blackbox-Test stehen den durchführenden Personen lediglich die Adressinformationen des Zielsystems zur Verfügung. Mittels der Vorgehensweise „Blackbox-Test“ soll der Angriff eines typischen Außentäters simuliert werden, bei dem nur unvollständige und öffentlich zugängliche Kenntnisse über das Zielsystem vorliegen. Dagegen haben die durchführenden Personen bei einem Whitebox-Test umfangreiche Informationen über die zu testenden Systeme. Dazu gehören beispielsweise Informationen über IP-Adressen des internen Netzes und die eingesetzte Soft- und Hardware. Diese Angaben werden den durchführenden Personen zuvor vom Verantwortlichen mitgeteilt.

  Zudem können Penetrationstests in unterschiedlicher Tiefe durchgeführt werden. Zu vermeiden sind dabei destruktive Tests, das heißt Tests, bei denen die

97 Der „Praxis-Leitfaden für IS-Penetrationstests“ des BSI ist im Internet veröffentlicht unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.html.

Zielsysteme, auf denen personenbezogene Daten verarbeitet werden, zu Schaden kommen können.

— **Zweckfestlegung:**

Die Zweckbestimmung für einen Penetrationstest, bei dem zumindest möglicherweise personenbezogene Daten verarbeitet werden, muss datenschutzrechtlich hinreichend bestimmt und tragfähig sein. Vorab sollte der Verantwortliche den behördlichen Datenschutzbeauftragten und gegebenenfalls auch die Personalvertretung einbinden.

— **Durchführende Stellen und Personen:**

Dem Verantwortlichen sollte bewusst sein, dass die Stellen und Personen, die den Penetrationstest durchführen, gewöhnlich Zugriff auf personenbezogene Daten und die diese schützende Technik erhalten. Je nach Prüfungskontext können mit dieser Offenlegung hohe datenschutzrechtliche Risiken verbunden sein. Neben der Besonderheit, dass sich aus bereichsspezifischen Sonderregelungen zur Auftragsverarbeitung schon ausdrücklich besondere Anforderungen an die Durchführenden ergeben können,[98] ist stets auf eine geeignete technische sowie sonstige fachliche und persönliche Qualifikation der Durchführenden zu achten.

Beispielsweise darf eine Schule ihre Schülerinnen und Schüler nicht während entsprechender Projektarbeiten veranlassen, relativ selbständig Penetrationstests an produktiven schulischen IT-Systemen durchzuführen. Hier wäre das Risiko viel zu hoch, dass schulische personenbezogene Daten insbesondere auf den für den Penetrationstest genutzten Privatgeräten rechtswidrig verarbeitet werden. Aber auch ohne schulische Veranlassung besteht die Gefahr, dass Schülerinnen und Schüler neu erworbene IT-Kenntnisse anhand schulischer IT-Systeme ausprobieren möchten. Da in diesem Kontext auch eine strafrechtliche Relevanz nicht ausgeschlossen werden kann, sollten Schulen dieses Risiko mit geeigneten Schutzmaßnahmen (zum Beispiel Sensibilisierung der Lehrkräfte, Schülerinnen und Schüler) reduzieren.

— **Speicherbegrenzung:**

Da in der Regel nicht ausgeschlossen werden kann, dass die Durchführenden während des Penetrationstests personenbezogene Daten verarbeiten und diese zur Erstellung bzw. zur Rechtfertigung des Prüfberichts erforderlich sind, muss vorab festgelegt werden, welche Daten in welcher Form (zum Beispiel verschlüsselt und/oder pseudonymisiert) und auf welchen Datenträgern verarbeitet werden. Zudem muss festgelegt sein, nach welcher Zeit die erhobenen Daten gelöscht werden müssen und welche Nachweise für die Löschung zu erbringen sind.

98 Vgl. zu einzelnen Regelungen Bayerischer Landesbeauftragter für den Datenschutz, Leitfaden zum Outsourcing kommunaler IT, Stand 3/2021, S. 6 ff., Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Auftragsverarbeitung“.

— **Rechenschaftspflicht:**

Wenn ein Penetrationstest mit einer Verarbeitung personenbezogener Daten verbunden ist, muss der Verantwortliche insofern auch seine Rechenschaftspflicht erfüllen (Art. 5 Abs. 2 DSGVO). Im Falle einer Hochrisikoverarbeitung geschieht dies in Form einer Datenschutz-Folgenabschätzung. In anderen Konstellationen kann im Rahmen dieses Nachweises auch auf eine allgemeine datenschutzrechtliche Risikoanalyse zurückgegriffen werden.[99]

— **Weiterführende Literatur:**

Es gibt zahlreiche weitere Anforderungen, Empfehlungen und Hinweise für die Durchführung von Penetrationstests, so etwa den „Praxis-Leitfaden für IS-Penetrationstests" des Bundesamtes für Sicherheit in der Informationstechnik. Darin werden auch Anforderungen, die aus datenschutzrechtlicher Sicht zu beachten sind, dargelegt (zum Beispiel Vier-Augen-Prinzip bei der Durchführung, Dokumentation, Durchführung von Wiederholungsprüfungen, gegebenenfalls Einverständnis von Betreibern der zu testenden IT-Systeme).

Beauftragt der Verantwortliche eine andere Stelle mit der Durchführung von Penetrationstests, müssen regelmäßig die Voraussetzungen der Auftragsverarbeitung gemäß Art. 4 Nr. 8, Art. 28 DSGVO eingehalten werden.[100] Insbesondere muss grundsätzlich ein Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter geschlossen werden, der den Anforderungen von Art. 28 Abs. 3 DSGVO genügt. Dort kann auch als vertragliche Leistungsposition vereinbart werden, dass der beauftragte Dienstleister dem Verantwortlichen bei der Erstellung von datenschutzrechtlichen Nachweisen wie beispielswiese einer Risikoanalyse zuarbeiten muss.

12.2 Datenschutz-Folgenabschätzung (DSFA) und Risikoanalyse in der Praxis

Der Umgang mit Risiken ist nicht immer einfach. Das ist auch im Datenschutzrecht so. Damit bayerische öffentliche Stellen Risiken bei der Verarbeitung personenbezogener Daten noch leichter aufspüren und angemessen reduzieren können, habe ich mein Informationsangebot rund um die Datenschutz-Folgenabschätzung weiter ausgebaut.

Die neue, über 80 Seiten starke Orientierungshilfe „Risikoanalyse und Datenschutz-Folgenabschätzung – Systematik, Anforderungen, Beispiele" bildet nun das Kernstück des umfangreichen Informationspakets. Sie entwickelt für die Datenschutz-Folgenabschätzung und die in Datenschutzliteratur und Datenschutzpraxis weniger im Fokus stehende allgemeine Risikoanalyse einen gemeinsamen methodischen Ansatz. Erweitert wurde das zu diesem Informationspaket gehörende Set von Formularen, welche die Durchführung von Datenschutz-Folgenabschätzungen und allgemeinen Risikoanalysen anleiten und eine ordnungsgemäße Dokumentation unterstützen

99 Bayerischer Landesbeauftragter für den Datenschutz, Risikoanalyse und Datenschutz-Folgenabschätzung, Stand 5/2022, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Datenschutz-Folgenabschätzung".

100 Vgl. ausführlich zu den allgemeinen Anforderungen zur Zulässigkeit von Auftragsverarbeitungen Bayerischer Landesbeauftragter für den Datenschutz, Auftragsverarbeitung, Stand 4/2019, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Auftragsverarbeitung".

sollen. Der konkrete Einsatz dieser Formulare wird durch mehrere, in sechs Modulen strukturierte Beispiele veranschaulicht.

Alle diese Hilfen legen besonderen Wert auf die Durchführung in der Praxis und versetzen auch kleinere Staatsbehörden und Kommunen in die Lage, mit Datenschutzrisiken adäquat umzugehen. In diesem Zusammenhang erwähnenswert ist etwa der Gedanke der Skalierung: Risikoanalysen müssen nicht in jedem Fall aufwändig sein; je nach Anlass sind verschiedene „Ausbaustufen" möglich. Das wird anhand mehrerer konkreter Anwendungsfälle beispielhaft dargestellt.

Zudem kann eine zweigeteilte Datenschutz-Folgenabschätzung oder eine zweigeteilte allgemeine Risikoanalyse den Aufwand verantwortlicher Stellen deutlich reduzieren. Wirken bei einer Verarbeitungstätigkeit mehrere Stellen zusammen, kann im Einzelfall die formale Aufteilung nach Wissens- und Zuständigkeitssphären sowie aus Effizienz-, Konsistenz- und Aktualitätsgründen sinnvoll sein. Ein solches Zusammenwirken kann insbesondere im Verhältnis zwischen einem Verantwortlichen und dem Hersteller eines Betriebsmittels oder einem Auftragsverarbeiter, ebenso in Fällen gemeinsamer Verantwortlichkeit sinnvoll sein. Die jeweiligen Teile einer Datenschutz-Folgenabschätzung oder einer allgemeinen Risikoanalyse können in solchen Konstellationen in einer vorab geplanten Verweisstruktur synergetisch miteinander verbunden werden.

In meiner Beratungspraxis konnten noch weitere typische Optimierungspotenziale bei der Durchführung von Datenschutz-Folgenabschätzungen und allgemeinen Risikoanalysen identifiziert werden, die in den Arbeitshilfen neben den bereits genannten Aspekten aufgezeigt werden.

12.3 Arbeitsgruppe zu Ethik und Datenschutz bei Künstlicher Intelligenz

Künstliche Intelligenz (KI) verbreitet sich rasant in Wirtschaft und Gesellschaft und hält in immer mehr Lebensbereichen Einzug. Bisher noch auf Spezialanwendungen beschränkte künstliche Intelligenzen sind selbst in Smartphone-Apps keine Seltenheit mehr, bei denen diese im Hintergrund auf dem Server des Anbieters oder als vortrainierte Machine-Learning-Modelle sogar lokal auf dem Gerät des Anwenders oder im Browser laufen. Die Auseinandersetzung mit den verschiedenen Spielarten dieser Technologie und den damit jeweils einhergehenden Risiken für die Rechte und Freiheiten der Nutzer und der Gesellschaft wird auf absehbare Zeit wachsende Bedeutung gewinnen.

Die Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre (International Conference of Data Protection & Privacy Commissioners – ICDPPC) benannte sich zum Jahr 2020 in „Internationale Datenschutzkonferenz" (Global Privacy Assembly – GPA) um. Dieses Gremium bildete per Beschluss eine ständige Arbeitsgruppe, die sich mit ethischen Fragen und speziell dem Thema Datenschutz im Bereich künstlicher Intelligenz befasst („Working Group on Ethics and Data protection in Artificial Intelligence").

Anfang 2021 einigte sich die Arbeitsgruppe auf ihre Jahresziele und organisierte sich für die Umsetzung ihrer Arbeitspakete in Teams von Berichterstattern und Mitberichterstattern. Ich beteiligte mich in der Rolle eines Beobachters an dieser Gruppe und kann von folgenden Arbeitsergebnissen der Arbeitsgruppe berichten:

- Es wurde eine gemeinsame Sammlung von KI-bezogenen Dokumenten geschaffen, auf die alle GPA-Mitglieder und Beobachter zugreifen können.

- Bei der Entwicklung künstlicher Intelligenzen gilt es, Bias (Voreingenommenheit) und Diskriminierung auszuschließen. Dazu kann es aber aus statistischen Gründen nötig sein, die damit zusammenhängenden Eigenschaften zu sammeln. So entsteht aber durch dafür nötige zusätzliche Datenerhebungen möglicherweise ein neues Datenschutzrisiko. Zu diesem Aspekt wurden Risikoanalysen durchgeführt, die relevante und insbesondere gesamtgesellschaftliche Risiken aufdecken und grundlegende Hinweise für den Umgang mit diesen Risiken in Bezug auf die verschiedenen beteiligten Interessengruppen geben sollen.

- Es wurde eine Umfrage zu Kapazitäten und der Expertise der Behörden im Umgang mit Ethik- und Datenschutzfragen in KI-Systemanwendungen durchgeführt. Diese Umfrage stellte einen ersten Schritt dar, um die Arbeit der Arbeitsgruppe in Zukunft hinsichtlich Kapazitäten und Expertise im Bereich KI festzustellen. Die Ergebnisse sollen für eine Gap-Analyse genutzt und es sollen entsprechende Empfehlungen gegeben werden, um den Wissensaustausch und den Kapazitätsaufbau im Bereich KI innerhalb der GPA zu verbessern.

- Die Arbeitsgruppe erstellt einen Bericht zum Thema Datenschutz im Beschäftigungskontext im Allgemeinen und zur Arbeitgeberüberwachung im Besonderen. Auch hierzu wurde eine Umfrage durchgeführt.

- Aufgrund der besonderen datenschutzrechtlichen Brisanz und gesamtgesellschaftlichen Auswirkung gründete die Arbeitsgruppe eine eigene Untergruppe zum Thema Gesichtserkennung (Face Recognition Technologies – FRT) und beauftragte diese mit der Erarbeitung von Grundsätzen und Anforderungen bei der Verwendung personenbezogener Daten in diesem Bereich. Die diesbezügliche „Entschließung über Grundsätze und Erwartungen für die angemessene Nutzung personenbezogener Daten in der Gesichtserkennungstechnologie“ wurde auf der 44. Sitzung der GPA verabschiedet.[101]

- Weitere Informationen über die Arbeit und Ergebnisse der Gruppe werden im offiziellen Bericht ausführlicher dargestellt. Im Allgemeinen scheinen die ursprünglich identifizierten Prioritäten aber weiterhin Gültigkeit zu besitzen. Die nächste Arbeitsphase der Gruppe wird einerseits durch die Überwachung konkreter Gesetzesinitiativen einiger nationaler, regionaler und internationaler Stellen gekennzeichnet sein und andererseits durch die Notwendigkeit, langfristige Herausforderungen für die Menschenrechte zu berücksichtigen, wie etwa Umweltentwicklungen und globale Ungleichheit.

12.4 Unzulässige Veröffentlichung von personenbezogenen Daten im Internet

Immer wieder musste ich im Berichtszeitraum feststellen, dass öffentliche Stellen auf Grund von Fehlern ihrer Beschäftigten unzulässig auf ihren Webseiten personenbezogene Daten veröffentlichten. Regelmäßig gibt es hierfür drei mögliche Ursachen:

[101] Internet: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/GPA/2022_44GPA_facial-recognition.html.

— Veröffentlichung auf Grund von Unwissenheit oder mangelnder Sensibilität, dass ein personenbezogenes Datum nicht veröffentlicht werden darf: Im Berichtszeitraum wurde beispielsweise ein Gemeinderatsprotokoll auf die Webseiten einer Gemeinde eingestellt, in dem Gesundheitsdaten einer Person enthalten waren, die durch die genannte Amtsbezeichnung identifizierbar war.

— Veröffentlichung auf Grund von Unachtsamkeit: Im Berichtszeitraum wurden beispielsweise nicht für die Öffentlichkeit bestimmte Dokumente aus einer Gemeinderatssitzung versehentlich auf den Webseiten der Gemeinde veröffentlicht, die zugleich personenbezogene Daten von Bürgerinnen und Bürgern enthielten.

— Veröffentlichung auf Grund der falschen Konfiguration eines Webservers: Auch beispielsweise zu weit reichende Berechtigungen für interne Verzeichnisse zum Datenaustausch können zur unzulässigen Veröffentlichung führen.

Unabhängig von den möglichen Ursache ist die verantwortliche Stelle verpflichtet zu prüfen, ob es sich um einen meldepflichtigen Vorfall gemäß Art. 33 DSGVO handelt und ob die betroffenen Personen gemäß Art. 34 DSGVO benachrichtigt werden müssen. Hierfür verweise ich auf meine Orientierungshilfe „Meldepflicht und Benachrichtigungspflicht des Verantwortlichen“.[102]

Wie ich in meiner Orientierungshilfe „Das Recht auf Löschung nach der Datenschutz-Grundverordnung“[103] ausgeführt habe, können Betroffene vom Verantwortlichen verlangen, den für die Datenverarbeitung Verantwortlichen, die diese personenbezogenen Daten verarbeiten (also beispielsweise Suchmaschinen), mitzuteilen, alle Links zu diesen personenbezogenen Daten oder Kopien oder Replikationen der personenbezogenen Daten zu löschen.

Nachdem im Folgenden zunächst die Weiterverarbeitung von im Internet veröffentlichten Daten durch Suchmaschinenbetreiber und Webarchive dargestellt wird, werden sodann Wege aufgezeigt, wie dort aus praktischer Sicht eine Löschung veranlasst werden kann.

12.4.1 Suchmaschinen und Webarchiv

Suchmaschinen indexieren laufend das World Wide Web. Hierfür durchsuchen sie die öffentlich erreichbaren Webseiten nach bestimmten Kriterien („Crawling“). Diese Kriterien unterscheiden sich von Suchmaschine zu Suchmaschine und sind wohlgehütete Geschäftsgeheimnisse der jeweiligen Suchmaschinenbetreiber. Durch das Crawling können Suchmaschinen ihre **Suchindizes** – das verschlagwortete Verzeichnis der Webseiten – aktuell halten. Hierbei werden neue Webseiten oder veränderte Inhalte im Suchindex berücksichtigt; ebenso wird erkannt, wenn Inhalte auf Websei-

[102] Bayerischer Landesbeauftragter für den Datenschutz, Meldepflicht und Benachrichtigungspflicht des Verantwortlichen, Stand 06/2019, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Melde- und Benachrichtigungspflicht“.

[103] Bayerischer Landesbeauftragter für den Datenschutz, Das Recht auf Löschung nach der Datenschutz-Grundverordnung, Stand 06/2022, Rn. 65, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Recht auf Löschung“.

ten nicht mehr verfügbar sind. Die Aktualisierung der Suchindizes erfolgt laufend, allerdings kann es unter Umständen mehrere Monate dauern, bis sich Änderungen an Webseiten im Suchindex auswirken.

Eine Suchmaschine gibt auf Grund der Anfrage eines Nutzenden und des darauf erfolgten Nachschlagens im Suchindex eine **Suchergebnisliste** an den Nutzenden zurück. Die Suchergebnisliste enthält üblicherweise nicht nur Links mit möglichen passenden Webseiten, sondern auch Auszüge aus den Inhalten der Webseiten. Bereits in den Suchergebnissen können somit die unzulässig veröffentlichten Daten sichtbar sein. Da Suchergebnisse durch die laufende, aber verzögerte Aktualisierung nicht immer den aktuellen Veröffentlichungsstand der Webseite widerspiegeln, werden diese Daten hier in der Regel auch nach der Löschung von der eigenen Webseite weiterhin für einige Zeit angezeigt.

Neben der Bereitstellung der Suchergebnisse gibt es Suchmaschinen, die Webseiten in ihren **Cache** aufnehmen, das heißt die Seiten in Gänze kopieren und den Nutzenden zur Verfügung stellen. Somit kann beispielsweise bei Ausfall eines Webservers ein Inhalt dennoch abgerufen werden oder gegebenenfalls auch eine Vorversion des aktuellen Inhalts betrachtet werden. Letzteres ist in erweiterter Form Strategie der WayBack-Maschine,[104] die sich als eine digitale Bibliothek für Webseiten versteht und dafür unterschiedliche Versionsstände aller zugänglichen Webseiten im World Wide Web („Snapshots“) speichert und frei zugänglich zur Verfügung stellt. Während Suchmaschinen Suchergebnisse und auch Cache-Versionen nach einiger Zeit entfernen, wenn die Ursprungsquelle nicht mehr vorhanden ist, ist eine automatische Löschung bei der WayBack-Maschine nicht vorgesehen. Während sich also Suchmaschinen mit der Zeit selbst bereinigen, ist dies bei der WayBack-Maschine nicht der Fall. Sollen Daten aus ihr entfernt werden, muss explizit eine Löschung beantragt werden.

Google ist in Deutschland derzeit die marktführende Suchmaschine, gefolgt von Bing (Microsoft). Sowohl Google wie auch Bing legen eigene Suchindizes an, die auch von anderen Suchmaschinen genutzt werden. Ebenso erstellen diese beiden Suchmaschinen Cache-Kopien der Webseiten. Daher erscheint es sinnvoll, zumindest diese beiden Anbieter über ein Löschbegehren zu informieren. Sind die Suchmaschinenbetreiber tätig geworden und haben die Suchindizes aktualisiert, werden weder über die Suchergebnisse noch über den Cache die entsprechenden Daten preisgegeben.

12.4.2 Praktisches Vorgehen

Will eine verantwortliche Stelle Daten bei einer Suchmaschine löschen lassen, besteht der erste Schritt darin zu prüfen, ob Suchmaschinen die betreffenden Seiten bereits gecrawlt haben, die fraglichen personenbezogenen Daten bereits in den Suchindizes gelistet sind und gegebenenfalls in den Suchmaschinencache kopiert wurden.

Hierzu kann in den meisten Suchmaschinen mit dem Operator „site:“ gesucht werden, der die Suchergebnisse auf die nach ihm eingegebene Webseite einschränkt. Mit dieser Suche ist auch die korrekte URL (Uniform Resource Locator) ermittelbar, die möglicherweise aus dem Suchindex gelöscht werden muss.

[104] Internet: https://archive.org/web.

Um – wie im Folgenden beschrieben – tätig werden zu können, ist jeweils ein sogenannter Webmaster-Account und der administrative Zugriff auf die betreffende Webseite Voraussetzung.

Bei beiden Suchmaschinenbetreibern erscheint es derzeit als das schnellste Vorgehen, zunächst die entsprechende (genaue) URL aus den Suchergebnissen temporär entfernen zu lassen (Google: „Tool zum Entfernen und für SafeSearch-Meldungen“;[105] Bing: „Block URLs“[106]). Google zeigt diese URL für etwa sechs Monate nicht mehr an, Bing für 90 Tage. Nach diesem Zeitraum können die Seiten wieder angezeigt werden, wenn sie noch auf dem ursprünglichen Webauftritt verfügbar sind. Beide Suchmaschinenbetreiber erklären allerdings, die entsprechenden Seiten neu zu indexieren. Sind also die betreffenden Daten von der jeweiligen Seite entfernt, wird der neue Seiteninhalt indexiert; ist die Seite mit korrektem HTTP-Status (404 oder 401) komplett entfernt, wird sie nicht wieder in den Suchindex aufgenommen. Über den Webmaster-Account wird laut Suchmaschinenanbieter Rückmeldung über den Stand der Antragsbearbeitung gegeben.

Google gibt an, dass die Bearbeitung eines Antrags auf temporäres Entfernen einer Seite aus dem Suchindex einen Tag dauern könne und die Gefahr bestehe, dass der Antrag abgelehnt würde. Alternativ könne auch die komplette Neuindexierung der Webseite beantragt werden. Das Crawling könne jedoch einige Tage oder auch mehrere Wochen dauern.

Auch das Internetarchiv WayBack-Maschine sollte daraufhin überprüft werden, ob die unzulässig veröffentlichten Daten bereits ihren Weg dorthin gefunden haben, insbesondere, da die WayBack-Maschine nicht vorsieht, die Daten von selbst zu löschen. Auch bei der WayBack-Maschine können Löschanträge gestellt werden.

Prinzipiell können Vorkehrungen getroffen werden, so dass die WayBack-Maschine gar nicht erst Snapshots erstellt. Da eine Webseiten-Kopie bei WayBack im Vergleich zu einer Auflistung von Suchergebnissen bei Suchmaschinen für öffentliche Stellen keinen deutlichen Mehrwert bietet, stellt dies durchaus eine in Betracht zu ziehende Möglichkeit dar. Anleitungen hierfür finden sich bei der WayBack-Maschine selbst oder über eine entsprechende Websuche.

12.4.3 Portale zur Überprüfung auf Schadsoftware

Neben den drei oben beschriebenen Arten der unzulässigen Veröffentlichung auf der Webseite des Verantwortlichen gibt es noch eine weitere, auf die ich hier kurz eingehen möchte.

Verschiedene Portale bieten eine kostenlose Überprüfung von Dateien auf Schadsoftware an. Im Berichtszeitraum wurde mir gemeldet, dass mehrere Dokumente offenbar eines Landratsamts auf einem derartigen Portal veröffentlicht waren. Anscheinend hatte mindestens eine nutzende Person Dokumente des Landratsamts zur Prüfung auf Schadcode hochgeladen. Häufig veröffentlichen entsprechende Portale - zumindest in der kostenlosen Nutzungsvariante – die Dokumente zusammen mit dem Prüfergebnis, so dass dort eine Vielzahl von Dokumenten auffindbar ist, die sensible Inhalte preisgeben.

105 Internet: https://support.google.com/webmasters/answer/9689846?hl=de.
106 Internet: https://www.bing.com/webmasters/help/block-urls-264e560b.

Derartige Portale warnen im Normalfall ausdrücklich davor, sensible Inhalte hochzuladen, und weisen darauf hin, dass die Dateien anderen Nutzenden zur Verfügung gestellt werden. Leider scheinen diese Hinweise häufig nicht zu fruchten. Je nach Portal und gebuchtem Service können die hochgeladenen Dokumente von allen Nutzenden oder von einer eingeschränkten Nutzergruppe eingesehen werden. Auch wenn diese Dokumente nicht gänzlich frei zugänglich zur Verfügung stehen, stellt die Übermittlung von personenbezogenen Daten an derartige Portale eine unrechtmäßige Offenlegung dar.

Die Löschung hochgeladener Dokumente ist laut Angaben auf den Webseiten entweder nicht möglich oder dem Nutzenden vorbehalten, der die Dokumente hochgeladen hat. Derartige Portale erläutern häufig nicht, wie Löschanträge gestellt werden können. Sofern diese Portale von Anbietern außerhalb des Geltungsbereichs der Datenschutz-Grundverordnung betrieben werden, gestaltet sich die Durchsetzung von Betroffenenrechten gegebenenfalls schwierig. Dennoch sollte eine Kontaktaufnahme über die bekanntgemachten Kontaktwege erfolgen. Im Übrigen müsste bei der Nutzung derartiger Portale gegebenenfalls auch die Datenübermittlung ins Nicht-EU-Ausland den rechtlichen Vorgaben von Art. 44 ff. DSGVO genügen.

Auf Grund einer möglichen Verletzung von Rechten betroffener Personen, die möglicherweise nicht behoben werden kann, rate ich öffentlichen Stellen, derartige Dienste nicht zu nutzen und gegebenenfalls die Nutzung zu sperren, um nicht Gefahr zu laufen, sensible Dokumente zu veröffentlichen. Die Möglichkeit der Prüfung von Dokumenten auf Schadsoftware sollte stattdessen von der eigenen IT-Abteilung deutlich kommuniziert werden. Sollen derartige Dienste dennoch genutzt werden, so sollte ein dediziertes Portal ausgewählt und dessen Bedingungen insbesondere in Bezug auf einen datenschutzkonformen Einsatz ausführlich überprüft werden.

12.5 Sachstandserhebung zur elektronischen Datenverarbeitung im Zusammenhang mit der COVID-19-Pandemie in den Gesundheitsämtern

Wie bereits in meinem 31. Tätigkeitsbericht unter Nr. 10.2 ausgeführt, waren seit Beginn der Pandemie in den bayerischen Gesundheitsämtern nicht nur neue Aufgaben des Infektionsschutzes zu bewältigen und dafür weitere Kräfte zu integrieren; die bayerische Gesundheitsverwaltung hat auch flächendeckend und teils ohne größere Vorbereitungszeit neue IT-Verfahren eingeführt. Dabei entstanden spezifische datenschutzrechtliche Risiken, die durch geeignete Schutzmaßnahmen auf ein angemessenes Niveau reduziert werden mussten. Das gilt insbesondere für die Verarbeitung von Gesundheitsdaten im Sinne von Art. 4 Nr. 15 DSGVO.

Vor diesem Hintergrund wandte ich mich im Frühjahr 2022 mit einer Online-Befragung an die bayerischen Gesundheitsämter, um eine Bestandsaufnahme hinsichtlich der personellen und technischen Ausstattung und der damit verbundenen datenschutzrechtlichen Erfordernisse zu gewinnen. Diese Erhebung wurde per Online-Formular auf freiwilliger Basis durchgeführt, um im direkten Kontakt mit den Gesundheitsämtern eventuell datenschutzbezogene Handlungsbedarfe zu identifizieren.

Die Umfrage umfasste die Themenbereiche:

— personelle Ausstattung, mit Angaben zur Anzahl der internen und externen Personen, die im Zusammenhang mit der Pandemie im Einsatz sind, sowie zu datenschutzrelevanten Vereinbarungen, die externes Personal betreffen;

- Einsatz von Privatgeräten, mit Fragestellungen zur Nutzung von Privatgeräten und zu Regelungen oder spezifischen technisch-organisatorischen Maßnahmen zur Absicherung der Nutzung von Privatgeräten;

- Eingesetzte Software, die im Zusammenhang mit der Pandemie operativ genutzt wird. Hier wurde sowohl nach Software, die speziell zur Pandemiebewältigung zur Verfügung stand, wie auch nach Standardsoftware gefragt;

- Kontaktnachverfolgung, mit Angaben zur Häufigkeit der Anforderung von Kontaktlisten und der dabei eingesetzten IT-Systeme;

- Elektronische Kommunikation mit Bürgerinnen und Bürgern, mit Fragen zum Einsatz von Fax, verschlüsselter und unverschlüsselter E-Mail und weiteren Kommunikationsmitteln;

- Datenschutzmanagement, ein Frageblock zu Dokumentation im Verarbeitungsverzeichnis, Risikoanalyse, Datenschutz-Folgenabschätzung und Datenpannen;

- Herausforderungen, Handlungsbedarfe und bestehende Good Practice-Umsetzungen.

Zu allen Themenbereichen gab es die Möglichkeit, zusätzliche Kommentare und Erläuterungen mitzuteilen.

An der Umfrage beteiligten sich 37 der 76 bayerischen Gesundheitsämter. Die hohe Beteiligung von fast 50 % begrüße ich sehr, auch wenn ich es bedauere, dass die restlichen Gesundheitsämter nicht die Gelegenheit genutzt haben, an der Erhebung teilzunehmen.

Nachfolgend möchte ich die Ergebnisse der Umfrage kurz zusammenfassen.

12.5.1 Personelle Ausstattung

In diesem Themenabschnitt sollte ein Gesamteindruck zur personellen Ausstattung in Bezug auf die Anzahl der Beschäftigten, die im Rahmen der Bewältigung der Pandemie zum Einsatz kamen und kommen, und die Unterstützung durch Externe sowie die datenschutzrechtlichen Rahmenbedingungen vor Ort für die externe Unterstützung entstehen.

Sieben Gesundheitsämter gaben an, zum Zeitpunkt der Umfragebeantwortung noch Unterstützung durch Externe erhalten zu haben. Da ein Teil der externen Unterstützung durch Beschäftigte anderer öffentlicher Stellen geleistet wurde, für die die Verschwiegenheit zu den Dienstpflichten zählt, wurden nur wenige datenschutzrelevante Vereinbarungen getroffen (zwölf Verschwiegenheitsvereinbarungen, ein Auftragsverarbeitungsvertrag, sechs Regelungen zu Weisungsbefugnissen), zusätzlich gab es Belehrungen über die Dienstpflichten nach der Datenschutz-Grundverordnung und dem Bayerischen Datenschutzgesetz.

Im Rahmen von Meldungen nach Art. 33 DSGVO und Beschwerden hat sich jedoch gezeigt, dass externe Mitarbeitende in Einzelfällen durchaus mangelnde Sensibilität in Sachen Datenschutz gezeigt haben. So wurden beispielsweise die im Zusammen-

hang mit der Kontaktverfolgung erhobenen Kontaktdaten genutzt, um junge, an COVID-19 erkrankte Frauen auch privat zu kontaktieren. Dies zeigt, wie wichtig auch hier regelmäßige Sensibilisierungsmaßnahmen oder Konsequenzen für die externen Beschäftigten nach Eintreten eines Verstoßes sind.

12.5.2 Einsatz von Privatgeräten

Da insbesondere in Gesundheitsämtern durch die Verarbeitung von sensiblen Gesundheitsdaten ein hohes Sicherheitsniveau bei der Verarbeitung notwendig ist, stellt der Einsatz von Privatgeräten und deren Absicherung am Heimarbeitsplatz ein besonderes Problem dar.

In zehn Gesundheitsämtern kamen der Umfrage nach Privatgeräte wie Tablet, Laptop, Rechner, Smartphone oder Drucker zum Einsatz. In sieben der Stellen gab es eine Dienstvereinbarung zum Einsatz der Privatgeräte, nur ein Gesundheitsamt teilte mit, weder eine Dienstvereinbarung abgeschlossen, noch technisch-organisatorische Maßnahmen für den Einsatz von Privatgeräten gemacht zu haben. Als absichernde Maßnahmen wurden VPN-Tunnel mit Authentifizierung durch Token, die Nutzung einer gekapselten Umgebung und das Verbot zur Speicherung von Daten auf den Privatrechnern genannt.

Auch wenn ich gerade zu Beginn der Pandemie bei der Frage der der Nutzung von Privatgeräten auch bestehenden Gerätemangel und organisatorische Zwänge (rasches Aufwachsen von Personalkörpern in den Gesundheitsämtern) berücksichtigt habe, mache ich nochmals auf die nach wie vor bestehenden besonderen Risiken und die Ausführungen in meinem 25. Tätigkeitsbericht unter Nrn. 2.1.3 und 7.3 aufmerksam.

Eine Meldung nach Art. 33 DSGVO zeigte zudem, dass eine regelmäßige Sensibilisierung der Beschäftigten zum korrekten Umgang mit privater IT notwendig ist. Demnach schickte sich eine Beschäftigte per E-Mail Dokumente an ihre private E-Mail-Adresse, um diese am privaten Drucker ausdrucken zu können. Hierunter waren auch E-Mails mit personenbezogenen Daten von Geflüchteten. Erst im Nachgang wurde der Beschäftigten klar, dass dies einen Datenschutzverstoß darstellte, und sie informierte ihre Vorgesetzte.

12.5.3 Eingesetzte Software

Neben der eingesetzten Hardware war auch die konkret eingesetzte Software von besonderem Interesse, gerade da diese häufig sehr kurzfristig eingeführt werden musste.

Die bayerischen Gesundheitsämter verwenden hier eine weite Bandbreite an Softwareprodukten. Hierunter fallen die Produkte, die speziell zum Infektionsschutz oder zur Pandemie-Bekämpfung entwickelt wurden, wie BaySIM, SORMAS, R23, CISS – digitaler Kollege und Äskulab, sowie die SORMAS-Schnittstellen SurvNet, DEMIS, Climedo, SORMAS2SORMAS und Luca.

Zudem sind neben den üblichen Office-Produkten selbsterstellte Formulare sowie Cloudlösungen für die Kommunikation und den Datenaustausch im Einsatz.

12.5.4 Kontaktnachverfolgung

Von besonderem Interesse waren aus meiner Sicht auch die Ergebnisse zur Nutzung von Luca und der in Papierform angeforderten Listen zur Kontaktnachverfolgung, die in Restaurants, bei Veranstaltungen etc. geführt werden mussten.

Seit Juni 2021 wurden von 16 der an der Umfrage teilnehmenden Gesundheitsämter insgesamt 140 Listen angefordert. Einige Gesundheitsämter gaben an, dass gar keine Listen angefordert werden mussten, da Kontaktpersonen entweder über die Indexperson ermittelt wurden oder das Infektionsrisiko bei Veranstaltungen, die in fraglichen Zeitraum stattfinden durften, vernachlässigbar war. Lediglich sechs Gesundheitsämter gaben an, zehn oder mehr Listen angefordert zu haben, überwiegend scheinen die Listen auf Papier oder Excel eingegangen zu sein, wobei sie gegebenenfalls eingescannt und elektronisch übermittelt wurden. Sieben Gesundheitsämter gaben an, Listen über Luca angefordert zu haben, wobei auf ein Gesundheitsamt insgesamt zwölf Anforderungen entfielen, die anderen Gesundheitsämter forderten zwischen ein und dreimal Listen an, jedoch lag der Fokus eher darauf, die Software zu testen.

Die geringe Nutzung von Luca in der Praxis bestätigt exemplarisch, dass häufig von der Politik kurzfristig getroffene Entscheidungen für den Einsatz eines bestimmten Produkts im konkreten Einsatz nicht zu dem gedachten Nutzen führen, wenn die Einsatzszenarien und auch die Einbindung in die konkrete Systemlandschaft nicht vorab mit den Nutzern abgestimmt und konzipiert werden. Die Ergebnisse der Umfrage bestätigen daher meine schon im 31. Tätigkeitsbericht unter Nr. 10.2.4 geäußerte Kritik.

12.5.5 Elektronische Kommunikation mit den Bürgerinnen und Bürgern

Auf Grund der Sensibilität der Daten und der Eilbedürftigkeit war und ist die Kommunikation mit den Bürgerinnen und Bürgern eine besondere Herausforderung. Dieser Themenblock des Fragebogens sollte die Möglichkeiten der Gesundheitsämter zur elektronischen Kommunikation mit Bürgerinnen und Bürgern beleuchten.

Als elektronische Kommunikationsmittel zum Kontakt mit Bürgerinnen und Bürgern wurde 13-mal das Fax genannt, 31-mal die E-Mail, davon sechsmal mit der Möglichkeit einer Ende-zu-Ende-Verschlüsselung, fünfmal mit Transportverschlüsselung, sechzehnmal mit der Möglichkeit, verschlüsselte Anhänge bereitzustellen, und 15-mal ohne Verschlüsselung. Fünf Gesundheitsämter gaben an, die E-Mail als Kommunikationsweg nicht zu verwenden.

Bei zwei Gesundheitsämtern besteht die Möglichkeit, De-Mail einzusetzen, allerdings teilte uns ein Gesundheitsamt mit, dass diese Möglichkeit unter den Bürgern nicht weit verbreitet sei. An zwei Gesundheitsämtern kommt das Bayernportal zum Einsatz. Zudem gibt es die folgenden weiteren Kommunikationsmöglichkeiten: Selbstgehostete Formulare, Up- und Download über eine selbstgehostete Cloud, Kommsafe, BePo und BayernBox, Verschlüsselter Versand von E-Mails über Cryptshare, sowie Versand über Hybrid-Brief, Postbrief und SMS.

Eine besondere Herausforderung für die Gesundheitsämter war und ist teilweise immer noch die Bereitstellung einer Kommunikationsinfrastruktur, die auch in Zeiten von Hochlasten für die Beschäftigten ohne großen Zusatzaufwand benutzbar ist und trotzdem den Anforderungen des Datenschutzes entspricht. Derzeit gibt es keine

bayernweit eingeführte Möglichkeit, Bürger elektronisch und vertraulich zu kontaktieren.

Aus diesem Grund begrüße ich es sehr, dass das Bayerische Staatsministerium für Gesundheit und Pflege angekündigt hat, im Laufe des Jahres 2023 eine zentrale Kommunikationsmöglichkeit für die Gesundheitsämter zur Verfügung zu stellen. Auch wenn dieses Projekt meines Erachtens etwas verspätet gestartet wurde, werden die Gesundheitsämter auch in Zukunft sichere Kommunikationsmöglichkeiten benötigen.

Meine Anregung für dieses Projekt ist die Verknüpfung mit dem Digitalen Bürgerkonto/BayernID, sodass Bürgerinnen und Bürger sich in Bayern nicht mehrmals an unterschiedlichen Portalen registrieren müssen, sondern sämtliche Kommunikation mit Behörden über das Digitale Bürgerkonto/BayernID abgewickelt werden kann.

12.5.6 Datenschutzmanagement

Insbesondere in Zeiten mit hohem Arbeitsaufkommen und der Notwendigkeit einer hohen Flexibilität zeigt sich, ob das etablierte Datenschutzmanagement ausgereift ist. Das Datenschutzmanagement ist dabei eine bewährte Methode, um systematisch alle datenschutzrechtlichen Anforderungen in einem Gesundheitsamt zu planen, zu organisieren, zu steuern sowie die dauerhafte Wirksamkeit der relevanten Prozesse und Schutzmaßnahmen zu kontrollieren. Denn jedes Gesundheitsamt ist muss den Nachweis erbringen können, dass die Vorgaben für die Verarbeitung personenbezogener Daten eingehalten werden. Da die jeweilige „Verarbeitungslandkarte“ der bayerischen Gesundheitsämter einen hohen Übereinstimmungsgrad aufweist, bietet sich mit Blick auch auf das Datenschutzmanagement an, bestehende Synergiepotenziale zu realisieren.

21 der Gesundheitsämter gaben an, dass die Verarbeitungstätigkeiten im Zusammenhang mit der Aufgabe der Pandemiebekämpfung beschrieben und im Verzeichnis der Verarbeitungstätigkeiten erfasst seien, 16 gaben an, die dazugehörigen Risikoanalysen ganz oder teilweise durchgeführt, und 13, eine Datenschutz-Folgenabschätzung ganz oder teilweise erstellt zu haben.

Nicht meldepflichtige Datenpannen wurden in sieben Gesundheitsämtern erfasst. Bei drei Gesundheitsämtern wurden seit Juni 2021 in größerem Umfang (in mehr als fünf Fällen) Betroffenenrechte nach Art. 12 bis 23 DSGVO geltend gemacht.

12.5.7 Herausforderungen, Handlungsbedarfe und bestehende Good Practice-Umsetzungen

Die datenschutzrechtlichen und technisch-organisatorischen Herausforderungen im Zusammenhang mit der Bekämpfung der COVID-19-Pandemie wurden überwiegend als hoch oder sehr hoch eingeschätzt.

Als besondere Herausforderung wurde die extrem hohe Belastung über einen langen Zeitraum empfunden mit stark wechselnden Teambesetzungen und suboptimalen Softwarelösungen. Hinzu kam die Notwendigkeit einer großen Flexibilität bezüglich den andauernd notwendigen Anpassungen der Prozesse. Die Möglichkeiten, aber auch Notwendigkeiten, die Prozesse und eingesetzte Software selbst festzulegen, wurde teilweise als Belastung empfunden, ebenso wie die Verpflichtung, SORMAS

einzusetzen – unabhängig davon, ob möglicherweise bereits gut funktionierende Softwarelösungen im konkreten Einsatz waren.

Da auch die Umsetzung der Belange des Datenschutzes vor Herausforderungen stellte, wurde insbesondere der Wunsch nach einem zentralen Portal zum datenschutzkonformen Austausch mit Bürgerinnen und Bürgern geäußert. Außerdem wurde zusätzliche personelle Unterstützung im Bereich des Datenschutzes und der IT zur besseren Unterstützung der Gesundheitsämter als sinnvoll erachtet.

Es konnten daher nur wenige Beispiele für Good Practice gefunden werden. So wurde von einem Gesundheitsamt die Möglichkeit für Bürger zur datenschutzkonformen Kontaktaufnahme mit Eingabe der Kontaktdaten sowie die Möglichkeit zum Hochladen des Testergebnisses über die Internetseite des Gesundheitsamts genannt. Die Daten werden anschließend so weiter verarbeitetet, dass das Gesundheitsamt diese direkt in SORMAS einspielen kann.

12.6 Elektronische Kommunikation im Rahmen des COVID-19-Pandemiemanagements

Bereits in meinem 30. Tätigkeitsbericht 2020 unter Nr. 3.5 und im 31. Tätigkeitsbericht 2021 unter Nr. 10.3 befasste ich mich mit der elektronischen Kommunikation in Bezug auf die Bekämpfung der COVID-19-Pandemie. In diesen beiden Beiträgen gab ich viele Hinweise zur elektronischen Kommunikation mit sensiblen Inhalten wie beispielsweise mit Gesundheitsdaten.

Die elektronische Kommunikation von Gesundheitsdaten ist weiterhin ein zentrales Thema meiner Prüfungs- und Beratungspraxis.

Bürgerinnen und Bürger wie auch Behörden nehmen den Versand von E-Mails als schnelle und unkomplizierte Kommunikationsmöglichkeit wahr. Gerade bei der Übermittlung von Gesundheitsdaten müssen aber einige Anforderungen an diese Kommunikationsform gestellt werden, um die Vertraulichkeit der sensiblen Daten zu gewährleisten.

Zum besseren Verständnis erläutere ich zunächst die **Transportverschlüsselung** und die **Ende-zu-Ende-Verschlüsselung** (auch E2E- Verschlüsselung).

Eine Übersicht der möglichen Angriffspunkte im Anschluss zeigt die Risiken beim Versand einer E-Mail in unverschlüsselter, transportverschlüsselter und E2E-verschlüsselter Form. Wie sich aus meiner Prüfpraxis ergab, zeigen mögliche Erweiterungen des Prozesses der E-Mail-Kommunikation Lösungsansätze auf.

Transportverschlüsselung:

Die Transportverschlüsselung sichert die Kommunikation auf den Wegen zwischen Empfänger und Sender ab, allerdings nicht durchgängig. Überall dort, wo die E-Mail (zwischen-)gespeichert wird, liegt sie unverschlüsselt vor. Dies ist regelmäßig in E-Mail-Programmen und auf den E-Mail-Servern von Sender und Empfänger der Fall. Auf dem Transportweg selbst kann bei einer korrekt eingerichteten Transportverschlüsselung ein Angreifer den Inhalt einer E-Mail nicht mitlesen.

Betreiber eines E-Mail-Servers müssen darauf achten, dass die Transportverschlüsselung korrekt konfiguriert wird, eine alleinige Aktivierung der Transportverschlüsselung mit der Übernahme von Voreinstellungen kann zu einer unsicheren Konfiguration führen. Im Rahmen des Kommunikationsaufbaus handeln die E-Mail-Server eine konkrete Protokoll-Version mit konkretem kryptografischen Algorithmus für die Transportverschlüsselung aus. Welche Protokoll-Versionen und Algorithmen jeweils zur Verfügung stehen, entscheidet der Administrator bei der Einrichtung des eigenen Servers. Um auch mit älteren E-Mail-Servern, die gegebenenfalls nicht aktuell gehalten werden, kommunizieren zu können, werden häufig ältere Protokoll-Versionen und veraltete Algorithmen auch auf neueren E-Mail-Servern unterstützt. Alte Protokoll-Versionen und veraltete Algorithmen weisen allerdings bekannte Schwachstellen auf, die es einem Angreifer ermöglichen, die verschlüsselte Kommunikation zu entschlüsseln und somit Inhalte mitzulesen und möglicherweise sogar zu verändern. Beim Versenden einer E-Mail ist es für den Absender grundsätzlich nicht erkennbar, welche Protokoll-Version und welchen Algorithmus die E-Mail-Server aushandeln oder ob überhaupt eine Transportverschlüsselung erfolgt. Dies bedeutet, dass – selbst wenn bekannt sein sollte, dass eine Transportverschlüsselung eingerichtet ist – unklar ist, ob ein Angreifer gegebenenfalls durch Manipulation des Aushandelns einer „unsicheren" Verschlüsselung oder gar einer unverschlüsselten Kommunikation (sog. Downgrade-Attacke) dafür sorgen kann, dass er Kenntnis vom Kommunikationsinhalt erhält.

In der Praxis wägen Administratoren aber oft technische Sicherheit gegen die Möglichkeit ab, dass E-Mails mit einem unsicher eingerichteten E-Mail-Server nicht ausgetauscht werden können, und öffnen so eventuell ein Tor für Downgrade-Attacken, um einen zuverlässigen Empfang und die Zustellung von E-Mails nicht zu gefährden.

Hinweise für Technikerinnen und Techniker:

Zur sicheren Implementierung der Transportverschlüsselung kann die Orientierung an den Richtlinien des Bundesamts für Sicherheit in der Informationstechnik BSI TR-02102-2 „Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)"[107] und „BSI TR-03108 Sicherer E-Mail-Transport"[108] hilfreich sein. Es sollten nur solche TLS-Versionen auf dem Webserver angeboten werden, die vom BSI als ausreichend sicher angesehen werden.

Die Transportverschlüsselung wird heute als eine **allgemein anerkannte Regel der Technik betrachtet**. Eine allgemein anerkannte Regel der Technik ist der niedrigste Technikstandard in einer dreistufigen Abstufung und spiegelt die überwiegende Auffassung unter technischen Praktikern wieder. Hiervon grenzt sich der **Stand der Technik** ab, der unterhalb des **Stands der Wissenschaft und Technik** anzusiedeln ist. Allgemein anerkannte Regeln der Technik nicht umzusetzen bedeutet in der Regel, fahrlässig zu handeln.

Auf Grund der Einordnung der Transportverschlüsselung als eine allgemein anerkannte Regel der Technik kann und muss heutzutage auch von öffentlichen Stellen eine Transportverschlüsselung bei Versand und Empfang von E-Mails per entspre-

107 Internet: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.html.

108 Internet: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03108/tr-03108.html.

chender Konfiguration technisch erzwungen werden, so dass der Versuch von Angreifern, dennoch einen unverschlüsselten oder „unsicher“ verschlüsselten Versand durch Downgrade-Attacken zu erreichen, unterbunden werden kann.

Weder E-Mail-Server von öffentlichen Stellen noch E-Mail-Provider sollten für Privatpersonen auf Transportverschlüsselung verzichten. Die Umsetzung der Transportverschlüsselung ist dabei die Aufgabe der Administratoren der E-Mail-Server, ein Anwender hat hierauf im Allgemeinen keinen Einfluss. Zudem kann er nicht ohne weiteres erkennen, ob eine E-Mail transportverschlüsselt versandt wurde oder nicht.

Da E-Mails, die ausschließlich transportverschlüsselt übertragen werden, auf E-Mail-Servern im Klartext vorliegen, können diese beispielsweise im Supportfall von Beschäftigten des E-Mail-Providers zur Kenntnis genommen werden. Es machen aber auch immer wieder E-Mail-Provider auf sich aufmerksam, die private Daten ihrer Kunden automatisiert scannen, um strafbare Inhalte zu finden oder kontextbezogene, an Nutzerinteressen angepasste Werbung einzublenden. Auch wenn laut Angaben der Anbieter ausschließlich automatisierte Scans ohne Kenntnisnahme der Inhalte durch Menschen erfolgen, zeigt dies, dass eine Kenntnisnahme von sensiblen Inhalten durch den Diensteanbieter nicht ausgeschlossen ist und eine Verarbeitung von personenbezogenen Inhaltsdaten erfolgen kann.

Zudem hat der Sender nicht immer Wissen darüber, welche Personen tatsächlich Zugriff auf einen E-Mail-Account haben. Während bei personalisierten behördlichen E-Mail-Adressen anzunehmen ist, dass diese im Regelfall nur von empfangsberechtigten Personen gelesen werden können, ist dies bei Privatpersonen nicht der Fall. Häufig werden E-Mail-Adressen als Familienadressen verwendet oder haben im Haushalt lebende Personen unbeschränkten Zugriff auf Rechner, Tablet oder auch Smartphone. Somit kann ein Zugriff einer nicht empfangsberechtigten Person im Allgemeinen nicht ausgeschlossen werden. Dies kann beispielsweise der Fall sein, wenn für die Tätigkeit im Gemeinderat private E-Mail-Adressen verwendet werden.

Ende-zu-Ende-Verschlüsselung:

Die E2E-Verschlüsselung sichert die Kommunikation durchgängig auf dem kompletten Weg von der Person des Senders zur Person des Empfängers ab. Lediglich in den E-Mail-Clients ist der Klartext der E-Mail einsehbar. Vor dem Zugriff auf eine verschlüsselte E-Mail im E-Mail-Client findet eine Authentifizierung beispielsweise durch Eingabe eines Passworts statt. Eine E2E-Verschlüsselung für E-Mails wird heute als Stand der Technik betrachtet. Es gibt praxisnahe Lösungen, die Verbreitung ist allerdings immer noch nicht weit genug fortgeschritten. Die fehlende Nutzer-Akzeptanz und die zahlreichen, mit der E2E-Verschlüsselung einhergehenden Alltagsprobleme sorgen dafür, dass sie kaum zur Sicherung der alltäglichen Kommunikation eingesetzt wird.

Mit einer E2E-Verschlüsselung ist es sehr unwahrscheinlich, dass unberechtigte Dritte vom E-Mail-Inhalt Kenntnis nehmen können. Natürlich ist nicht auszuschließen, dass ein Empfänger sein Endgerät mit anderen Personen teilt und den Zugriff auf verschlüsselte E-Mails so eingerichtet hat, dass keine weitere Authentifizierung erfolgen muss. Meiner Auffassung nach widerspricht eine derartige Einrichtung allerdings dem Ziel einer E2E-Verschlüsselung und ist mit geringer Wahrscheinlichkeit anzunehmen. Das Risiko ist bei einer Abwägung daher nicht dem Sender, sondern dem Empfänger zuzurechnen.

Hinweise für Technikerinnen und Techniker:

Für die Übermittlung einer E2E-verschlüsselten E-Mail müssen sowohl der Sender als auch der Empfänger über die Möglichkeit der Ver- und Entschlüsselung verfügen, zudem müssen beide den gleichen Standard für die Verschlüsselung beherrschen. Hier gibt es zwei unterschiedliche, nicht kompatible Produkte / Standards (PGP und S/MIME). Üblicherweise muss der Sender beim Versenden der E-Mail aktiv werden, also auswählen, dass die E-Mail verschlüsselt werden soll. Außerdem muss der Sender den öffentlichen Schlüssel des Empfängers kennen.

Idealerweise wird in der öffentlichen Stelle die Möglichkeit der E2E-Verschlüsselung so eingerichtet, dass die Anwender in der öffentlichen Stelle möglichst wenig Aufwand betreiben müssen, um E2E-verschlüsselte E-Mails verschicken zu können (zum Beispiel Integration in Outlook, Zugriff auf Adressbücher, gegebenenfalls ein passendes Add-In, dass die Aufgabe der Verschlüsselung übernimmt).

In der folgenden Tabelle findet sich ein Vergleich der beiden Verschlüsselungsmöglichkeiten.

Gegenüberstellung:

	Transportverschlüsselung	**E2E-Verschlüsselung**
Absicherung	Verschlüsselte Transportwege, unverschlüsselt mindestens in den E-Mail-Clients und auf den E-Mail-Servern	Komplettverschlüsselung von der Person des Senders zur Person des Empfängers
Technikstandard	Stand der allgemein anerkannten Regeln der Technik	Stand der Technik
Zuständigkeit für die Einrichtung der Verschlüsselung	Für E-Mail-Server verantwortliche Stellen	**In der öffentlichen Stelle:** – verantwortliche Stelle: für die Bereitstellung der Infrastruktur – Absender: Verschlüsseln der einzelnen E-Mails **Privatperson:** in der Regel selbst für Einrichtung und verschlüsselten Versand verantwortlich.
Einflussmöglichkeit des Anwenders	In der Regel keine	**Beschäftigte der öffentlichen Stelle:** Auswahl der Verschlüsselung bei Versand einer E-Mail insbesondere mit sensiblen Inhalten **Privatperson:** Gegebenenfalls Einrichtung, Bekanntgabe des öffentlichen Schlüssels, Auswahl der Verschlüsselung bei Versand einer E-Mail mit sensiblen Inhalten

Zum besseren Verständnis zeigt die nachfolgende Tabelle zusammenfassend die möglichen Ansatzpunkte für einen Angriff oder einen möglichen Zugriff durch Dritte:

Angriffspunkte:

	Unverschlüsselter Versand	Versand ausschließlich mit Transportverschlüsselung	Versand mit E2E-Verschlüsselung
Zugriff auf dem Transportweg	Ja	In der Regel nein, gegebenenfalls über Downgrade-Attacken	Nein
Möglicher Zugriff auf den E-Mail-Servern	Ja	Ja	Nein
Zugriff auf den E-Mail-Client durch Dritte	Ja	Ja	In der Regel nein

Bei den Angriffspunkten zeigt sich, dass ein Risiko für eine unrechtmäßige Kenntnisnahme in der Regel nur beim Versand von E-Mails mit E2E-Verschlüsselung ausgeschlossen werden kann. Für E-Mails mit sensiblen Inhalten wie Gesundheitsdaten sollte daher eine E2E-Verschlüsselung umgesetzt werden. Soll oder muss auf den Einsatz einer E2E-Verschlüsselung verzichtet werden, müssen bei sensiblen Daten zusätzliche Sicherheitsmaßnahmen ergriffen werden, die den Angriffspunkten bei der Transportverschlüsselung oder einem komplett unverschlüsselten Versands entgegengestellt werden.

Gerade in der Kommunikation mit Bürgerinnen und Bürgern fehlt häufig die Möglichkeit der E2E-verschlüsselten Kommunikation per E-Mail sowohl auf Seiten der öffentlichen Stellen als auch bei den Empfängern.

Aus diesem Grund sind – wie ich durch die Umfrage unter den Gesundheitsämtern (siehe Nr. 12.5) sowie meine Prüfungs- und Beratungspraxis weiß – entweder zusätzliche Sicherheitsmaßnahmen, wie der Versand einer unverschlüsselten E-Mail mit verschlüsselten Anhang, oder die Bereitstellung eines Dokuments zum Download über einen sicheren Clouddienst als Alternativen im Einsatz. Zu diesen Einsatzszenarien gab ich bereits in meinem 31. Tätigkeitsbericht 2021 unter Nr. 10.3.1 Hinweise.

Zudem etablierten einige Gesundheitsämter die Möglichkeit zur Kontaktaufnahme durch Bürger über ein sicheres Formular – gegebenenfalls mit der Möglichkeit zum Upload von Dokumenten.

Ein Landratsamt bat mich um Einschätzung, ob im Zuge einer derartigen Kontaktaufnahme durch den Bürger die Übermittlung eines Passworts zur Verschlüsselung zukünftiger Kommunikation über das Formular möglich wäre. Konkret wurde hier erwogen, einen Captcha-Mechanismus zur Passwortgenerierung zu verwenden und dem Bürger mitzuteilen, dass er sich dieses Captcha als Passwort für zukünftig übermittelte verschlüsselte Anhänge notieren solle.

Aus meiner Sicht stellt die Übermittlung eines Passworts bei der Kontaktaufnahme über ein (mittels SSL/„https“ gesichertes) Online-Formular einen sicheren Kommunikationsweg dar, der sich vom Kommunikationsweg mittels unverschlüsselter E-Mail unterscheidet und einen höheren Schutz bietet. Somit könnten in diesem Zuge Passwörter übermittelt werden, die in der Folge zum Beispiel für die Verschlüsselung von E-Mail-Anhängen zum Einsatz kommen könnten. Ob dieses Passwort per Captcha-Mechanismus generiert wird, erscheint in diesem Fall als nachranging. Wichtig ist,

dass die übermittelten Passwörter ausreichend sicher sein sollten, beispielsweise gemäß den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik.[109] Allerdings rege ich auf Grund der Sensibilität der Daten eine Mindestlänge von zehn Zeichen an.

12.7 Software für das Kontaktpersonen- und Fallmanagement

12.7.1 SORMAS

Bereits in meinem 31. Tätigkeitsbericht 2021 berichtete ich unter Nr. 10.2.1 über das Verfahren SORMAS-ÖGD (Surveillance Outbreak Response Management Analysis System im Öffentlichen Gesundheitsdienst), das die Gesundheitsämter bei ihrer Aufgabe des Falldaten- und des Kontaktpersonenmanagements unterstützen soll.

In Abstimmung mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und den Datenschutz-Aufsichtsbehörden der Länder stimmte ich nach Erörterung der eingereichten Unterlagen im Januar 2021 dem Betrieb von SORMAS in den Gesundheitsämtern unter Vorbehalt zu.

Um eine Ablösung des Papier- und Telefaxversands zu erreichen und zu einer effizienten und datenschutzkonformen digitalen Kontaktnachverfolgung in den Gesundheitsämtern zu gelangen, war eine intensive Begleitung des Projektes in Abstimmung mit den anderen Datenschutz-Aufsichtsbehörden auch in diesem Berichtszeitraum erforderlich. Für folgende Aspekte ergab sich nach wie vor Klärungsbedarf:

- Das Kryptographiekonzept blieb größtenteils unvollständig.
- Das Löschkonzept war noch lückenhaft.
- Bei einigen Merkmalen und Datenfeldern strittig, ob sie dem Grundsatz der Datenminimierung bzw. der Datensparsamkeit gemäß Art. 5 Buchst. c DSGVO entsprechen würden.
- Die Datenschutz-Folgenabschätzung lag lediglich als Entwurf vor.

Dies zeigt wiederum, wie wichtig es ist, nicht nur die Einführung einer bestimmten Software politisch zu beschließen, sondern diesen Prozess von Seiten der zuständigen Ministerien auch inhaltlich zu unterstützen, beispielsweise im Hinblick auf die von allen Stellen zu nutzenden Datenfelder.

12.7.2 Climedo

Neben der eigentlichen Kontaktnachverfolgung ist eine wesentliche Aufgabe der Gesundheitsämter und zentrale Säule in der Pandemiebekämpfung auch die Betreuung

[109] Internet: beispielsweise unter https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und Verbraucher/Informationen-undEmpfehlungen/CyberSicherheitsempfehlungen/ Accountschutz/Sichere-Passwoertererstellen/sicherepasswoerter-erstellen_node.html.

und Verwaltung der betroffenen, positiv getesteten Personen durch die tägliche Abfrage ihres Gesundheitszustandes.[110]

Um eine Entlastung bei der telefonischen bzw. postalischen Nachfrage zu erreichen, bietet SORMAS die Interoperabilität mit weiteren Software-Modulen externer Anbieter zur elektronischen Kontaktaufnahme und Bescheiderstellung bzw. zur Anbindung eines sogenannten elektronischen Symptomtagebuchs für Indexfälle.

Hierbei kommt zunehmend die Software-Lösung Climedo zum Einsatz, die in Abstimmung mit dem Bundesministerium für Gesundheit, dem Robert-Koch-Institut und der Entwicklerfirma Climedo unter Einbeziehung des Bundesamtes für Sicherheit in der Informationstechnik, des Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und der Akademie für öffentliches Gesundheitswesen entstand.

Die Einführung der Software Climedo verlief jedoch in vielen Gesundheitsämtern nicht reibungsfrei, wie ich durch den vermehrten Eingang von Beschwerden beobachten konnte:

In einigen Fällen wurden betroffene Personen von einem E-Mail-Server der Firma Climedo, an den im Vorfeld Daten von SORMAS übermittelt wurden, mittels E-Mail oder SMS darüber informiert, dass sie COVID-19-positiv seien, ohne dass von Seiten des Gesundheitsamts entsprechende Datenschutzhinweise vorgeschaltet waren. Ein solches Verfahren ist für die betroffenen Personen völlig intransparent. Dementsprechend erhielt ich eine Vielzahl von Beschwerden, wonach in den entsprechenden Gesundheitsämtern besonders sensible Gesundheitsdaten an externe Dritte weitergegeben würden.

Auch in diesem Fall zeigte sich, dass die Prozessstruktur bei SORMAS-ÖGD noch lückenhaft ist, insbesondere die Anbindung von weiteren Software-Modulen und Schnittstellen zu anderen Softwarelösungen. Es genügt nicht, die Schnittstellen nur technisch einzurichten, sondern es müssen auch entsprechende vertragliche Regelungen und Datenschutzinformationen bereitgestellt werden. Auch hier bietet es sich an, dass diese nicht – wie derzeit üblich – jeweils eigenständig von den Gesundheitsämtern erarbeitet werden müssen, sondern dass diese zentral bereitgestellt werden.

Ich werde das Projekt SORMAS auch weiterhin aufmerksam begleiten. Insbesondere werde ich weiterhin kritisch prüfen, ob bei der Entwicklung der Software dem Datenschutz durch Technikgestaltung gemäß Art. 25 Abs. 2 DSGVO entsprochen wird.

12.8 Meldungen von Verletzungen des Schutzes personenbezogener Daten

Ein Einblick in die bei mir eingegangenen Meldungen ist seit Inkrafttreten der Datenschutz-Grundverordnung zu einer festen Größe geworden und erhält auch in diesem Tätigkeitsbericht wieder ihren Platz.

Das im Vergleich zum Jahr 2021 beinahe gleichgebliebene Meldeaufkommen zeigt auch im aktuellen Berichtszeitraum, dass es den meisten bayerischen öffentlichen Stellen gelungen ist, ein gut funktionierendes Meldewesen zu etablieren und die nach

[110] Internet: https://www.bundesgesundheitsministerium.de/service/begriffe-von-a-z/o/oeffentlicher-gesundheitsheitsdienst-pakt/digitale-unterstuetzung-gesundheitsaemter.html.

Art. 33 DSGVO erforderlichen Meldungen an die Datenschutz-Aufsichtsbehörde erfolgreich in ihre Geschäftsprozesse zu integrieren.

Auf die spezifischen Arten der Verletzungen ging ich bereits in meinen früheren Tätigkeitsberichten ein. Insbesondere in meinem 31. Tätigkeitsbericht 2021 unter Nr. 10.9 befasste ich mich eingehend mit dem Thema.

Ein besonderes Augenmerk lag in diesem Jahr auf den Meldungen aus dem Gesundheitsbereich, da auch 2021 von der COVID-19-Pandemie geprägt war. Hierbei wurde vorrangig der Schutz der Vertraulichkeit von personenbezogenen Daten verletzt, insbesondere bei der Übermittlung von medizinischen Informationen wie Quarantänebescheide und Testergebnissen, aber auch bei sogenannten Neugierzugriffen, bei denen sich außerhalb eines Behandlungsverhältnisses Klinikpersonal Kenntnis vom Inhalt einer Patientenakte verschafft, etwa, um unberechtigt festzustellen, ob eine COVID-19-Erkrankung vorliegt. Die Thematik der Neugierzugriffe beleuchtete ich bereits eingehend in meinem 30. Tätigkeitsbericht 2020 unter Nr. 12.10.

Meldungen erreichten mich jedoch gleichermaßen aus anderen Teilen des bayerischen öffentlichen Sektors. Auch die Themen Hackerangriffe und Schadsoftware haben nach wie vor hohe Relevanz und bedeuten eine große Gefahr für die Sicherheit bei der Verarbeitung personenbezogener Daten. Zunehmend häuft sich hier das Problem, dass größere, überregionale Dienstleister angegriffen werden und somit eine Vielzahl von öffentlichen Stellen von Sicherheitsvorfällen bis hin zu längeren Ausfällen von IT-Systemen betroffen ist. Dies macht noch einmal deutlich, wie wichtig neben eigenen Sicherheitsmaßnahmen (siehe in meinem 29. Tätigkeitbericht 2019 unter Nr. 12.3) auch die sorgfältige Auswahl von Dienstleistern ist. Insbesondere muss festgelegt werden, wie ein Dienstleister die Verletzung des Schutzes personenbezogener Daten seiner Kunden zeitnah und zuverlässig an seinen Auftraggeber meldet, so dass dieser innerhalb der vorgegebenen Zeitspanne seinerseits eine Meldung bei mir abgeben kann.

Bezüglich der Cybersicherheit relevante und wesentliche Meldungen fließen im Rahmen der Cyberabwehr Bayern – grundsätzlich ohne Nennung der betroffenen öffentlichen Stellen – in ein bayernweites Lagebild ein, so dass eine Meldung bei mir auch anderen öffentlichen und nicht-öffentlichen Stellen helfen kann. Nur durch ein möglichst umfangreiches Lagebild können alle Behörden mit Cybersicherheitsaufgaben die richtigen Entscheidungen treffen und Maßnahmen ergreifen, so dass sich zukünftige Schadensereignisse reduzieren lassen. Auch wenn dies hohe personelle Ressourcen meiner Dienststelle bindet, kann ich damit dazu beitragen, die Cybersicherheit in Bayern proaktiv zu erhöhen.

13 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:

Leitende Ministerialrätin Christina Rölz, Datenschutzbeauftragte des Bayerischen Staatsministeriums des Innern, für Sport und Integration

Stellvertretendes Mitglied:

Leitende Ministerialrätin Ilka Bürger, Datenschutzbeauftragte des Bayerischen Staatsministeriums für Wirtschaft, Landesentwicklung und Energie

Auf Vorschlag der kommunalen Spitzenverbände in Bayern:

Mitglied:

Rudolf Schleyer, Vorstandsvorsitzender der Anstalt für Kommunale Datenverarbeitung in Bayern

Stellvertretendes Mitglied:

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 Geschäftsführer der Deutschen Rentenversicherung Nordbayern

Stellvertretendes Mitglied:

Dr. Irmgard Stippler, Vorsitzende des Vorstandes der AOK Bayern – Die Gesundheitskasse

Auf Vorschlag des Verbands Freier Berufe in Bayern e.V.:

Mitglied:

Dr. Till Schemmann, Notar

Stellvertretendes Mitglied:

Dr. Thomas Kuhn, Rechtsanwalt

Herr Peter Tomaschko, MdL, führte den Vorsitz in der Datenschutzkommission; stellvertretender Vorsitzender war Herr Benjamin Adjei, MdL.

Die Datenschutzkommission beim Bayerischen Landtag tagte im Berichtszeitraum drei Mal.

14 Ländervertreter im EDSA

Der Europäische Datenschutzausschuss (EDSA) hat im Jahr 2022 regelmäßig getagt, überwiegend in der Form von Videokonferenzen (zu diesem Ausschuss und zu meiner Aufgabe als Ländervertreter siehe ausführlich meinen 31. Tätigkeitsbericht 2021 unter Nr. 12).

Insbesondere hat der EDSA im Berichtszeitraum zahlreiche Leitlinien zur Vereinheitlichung des Datenschutzes im Europäischen Wirtschaftsraum sowie mehrere Stellungnahmen zu aktuellen Rechtsfragen beraten und verabschiedet, Meinungsverschiedenheiten zwischen einzelnen Aufsichtsbehörden im sogenannten Streitbeilegungsverfahren geklärt und ganz allgemein die Zusammenarbeit der europäischen Datenschutzbehörden verbessert.

Hervorheben möchte ich folgende Leitlinien:

- Leitlinien 01/2022 zu den Rechten betroffener Personen (Guidelines 01/2022 on data subjects rights – Right of access) zu Einzelfragen des Auskunftsrechts nach Art. 15 DSGVO;

- Leitlinien 03/2022 zu manipulativen Benutzeroberflächen von Social-Media-Plattformen (Guidelines 03/2022 on dark patterns in social media platform interfaces: how to recognise and avoid them);

- Leitlinien 05/2022 für den Einsatz von Gesichtserkennungstechnologien im Strafverfolgungsbereich (Guidelinies 05/2022 on the use of facial recognition technology in the area of law enforcement).

In bedeutenden europäischen Gesetzgebungsverfahren hat sich der EDSA gemeinsam mit dem Europäischen Datenschutzbeauftragten (EDSB) geäußert:

- Gemeinsame Stellungnahme 01/2022 zur Verlängerung der Covid-19-Bescheinigung Verordnung;

- Gemeinsame Stellungnahme 03/2022 zu dem Vorschlag für eine Verordnung über den Europäischen Gesundheitsdatenraum;

- Gemeinsame Stellungnahme 04/2022 zu dem Vorschlag für eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern.

Die genannten Leitlinien und Stellungnahmen sowie umfangreiche weitere den EDSA betreffende Informationen können unter https://edpb.europa.eu/edpb_de abgerufen werden, teilweise allerdings nur in englischer Sprache.

Abkürzungsverzeichnis

ABl.	Amtsblatt der Europäischen Union
Abs.	Absatz
a. F.	alte Fassung
AfD	Alternative für Deutschland
Art.	Artikel
Aufl.	Auflage
BayDSG	Bayerisches Datenschutzgesetz
BeckRS	Beck-Rechtsprechung (Datenbank)
BDSG	Bundesdatenschutzgesetz
BGBl.	Bundesgesetzblatt
Buchst.	Buchstabe
bzw.	beziehungsweise
CSU	Christlich-Soziale Union in Bayern
DSFA	Datenschutzfolgenabschätzung
DSGVO	Datenschutz-Grundverordnung
EDV	Elektronische Datenverarbeitung
FDP	Freie Demokratische Partei
ff.	(nach)folgende
GVBl.	Bayerisches Gesetz- und Verordnungsblatt
https	Hyper Text Transfer Protocol Secure
IP	Internet Protocol
IT	Informationstechnik
MdL	Mitglied des Landtages
Nr.	Nummer
PC	Personalcomputer
RLDSJ	Datenschutz-Richtlinie für Polizei und Strafjustiz
Rn.	Randnummer
sog.	sogenannt
SPD	Sozialdemokratische Partei Deutschlands
SSL	Secure Socket Layer
u. a.	unter anderem/und andere
UAbs.	Unterabsatz
vgl.	vergleiche
www	World Wide Web

Stichwortverzeichnis