34. Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz

gemäß Art. 59 Datenschutz-Grundverordnung

Berichtszeitraum: 1. Januar 2024 bis 31. Dezember 2024

Impressum

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

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

Inhaltsverzeichnis

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), zuletzt geändert durch § 2 Gesetz vom 25. Juli 2025 (GVBl. S. 254)
DSGVO	Datenschutz-Grundverordnung; die vollständige Bezeichnung lautet: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. L 119 vom 4. Mai 2016, S. 1, berichtigt ABl. L 314 vom 22. November 2016, S. 72, ABl. L 127 vom 23. Mai 2018, S. 2, und ABl. L 74 vom 4. März 2021, S. 35)
RLDSJ	Datenschutz-Richtlinie für Polizei und Strafjustiz; die vollständige Bezeichnung lautet: Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4. Mai 2016, S. 89, berichtigt ABl. L 127 vom 23. Mai 2018, S. 9, und ABl. L 74 vom 4. März 2021, S. 36)

1 Überblick

1.1 Datenschutz und Entbürokratisierung: Welche Spielräume lässt die Datenschutz-Grundverordnung dem nationalen Gesetzgeber?

Bürokratieabbau und Deregulierung sind seit jeher Kernanliegen bayerischer Regierungspolitik. Sie sollen nicht nur die Attraktivität des Wirtschaftsstandorts Bayern stärken, sondern auch den Bürgerinnen und Bürgern ebenso wie den Unternehmen mehr Eigenverantwortung ermöglichen. Im Berichtszeitraum hat sich überdies eine Enquete-Kommission des Bayerischen Landtags mit der Frage befasst, wie die öffentliche Verwaltung bürokratieärmer und bürgerfreundlicher gestaltet werden könne.[1] Vor diesem Hintergrund bin ich verschiedentlich gefragt worden, welchen Beitrag das nationale Datenschutzrecht leisten könne, um diese Ziele zu unterstützen.

Bei entsprechenden Fragen klingt nicht selten das Vorverständnis an, Deutschland habe über die europäischen Datenschutzstandards hinaus zusätzliche Anforderungen aufgestellt, die sich negativ auf die Wettbewerbsfähigkeit deutscher Unternehmen und die Effektivität der öffentlichen Verwaltung auswirkten (Stichwort: „Goldplating").

Insofern ist zum einen zu bemerken, dass der Gestaltungsspielraum der nationalen Gesetzgeber – dazu zählen auch die deutschen Landesgesetzgeber – im Datenschutzrecht durchaus begrenzt ist. Das Datenschutzrecht ist in den Mitgliedstaaten zum einen maßgeblich von der Datenschutz-Grundverordnung geprägt. Der Unionsgesetzgeber hat einen übergreifenden Datenschutz-Rechtsrahmen geschaffen, der „unionsweit gleichmäßig und einheitlich" (EG 10 Satz 2 DSGVO) gelten soll. Das Unionsrecht versteht sich mithin gerade nicht als ein Mindeststandard, den die Mitgliedstaaten durch zusätzliche Anforderungen beliebig ausbauen könnten.

Sind den nationalen Gesetzgebern Spielräume eingeräumt, lassen sich diese zum andern nur in Einklang mit nationalem Verfassungsrecht ausfüllen. Dass hier in Deutschland eine in Jahrzehnten gewachsene verfassungsgerichtliche Rechtsprechung für einen Ausgleich der Interessen von Verantwortlichen auf der einen sowie von betroffenen Personen auf der anderen Seite sorgt, wird in der Diskussion gern übersehen.

Ich möchte daher insbesondere die Zusammenhänge von unionalem Datenschutzrecht und nationalem Verfassungsrecht wieder ins Gedächtnis rufen. Immerhin hat der Landesgesetzgeber mit dem 2018 in Kraft getretenen Bayerischen Datenschutzgesetz eine sehr schlanke Regelungslösung gefunden, die sich dieser Zusammenhänge in jeder Hinsicht bewusst ist und in ihrer Grundstruktur seitdem gut bewährt hat. Weder die Fortentwicklung des Datenschutzrechts im Allgemeinen noch der unionsgerichtlichen Rechtsprechung im Besonderen geben Anlass

[1] Beschluss des Bayerischen Landtags zur Einsetzung einer Enquete-Kommission im Bayerischen Landtag „Potenziale in Gesellschaft, Wirtschaft und Verwaltung entfesseln – Das Leben leichter machen, Bürokratie abbauen, den Staat neu denken", LT-Drs. 19/2909.

zu Änderungen an diesen Grundstrukturen. Die Notwendigkeit, neue Regelungsthemen – wie etwa nationale Aspekte der KI-Regulierung – legislativ zu bewältigen, erfordert kein Um-, sondern (nur) ein konsequentes Weiterdenken.

1.1.1 Eröffnet die Datenschutz-Grundverordnung den Mitgliedstaaten einen legislativen Gestaltungsspielraum?

Die Datenschutz-Grundverordnung ist ungeachtet ihrer Öffnungsklauseln eine EU-Verordnung, die nach Art. 288 Abs. 2 Vertrag über die Arbeitsweise der Europäischen Union in allen ihren Teilen verbindlich ist und unmittelbar in jedem Mitgliedstaat gilt. Dementsprechend bedürfen ihre Vorschriften grundsätzlich keiner Durchführungsmaßnahmen der Mitgliedstaaten.[2]

Als allgemeiner Datenschutz-Rechtsrahmen verzichtet die Datenschutz-Grundverordnung weitgehend auf sektorspezifische Regelungen der Verarbeitung personenbezogener Daten. Um solche speziellen Vorschriften zu ermöglichen, sieht sie zahlreiche Öffnungs- und Spezifizierungsklauseln für besonderes Unionsrecht oder nationales Datenverarbeitungsrecht vor.[3] Allerdings bleibt es dabei, dass die Datenschutz-Grundverordnung eine grundsätzliche Harmonisierung der nationalen Rechtsvorschriften zum Schutz personenbezogener Daten sicherstellen soll. Immerhin erkennt der Europäische Gerichtshof ausdrücklich an, dass die besagten Öffnungs- und Spezifizierungsklauseln den Mitgliedstaaten einen gewissen **Ermessensspielraum hinsichtlich der Art und Weise der Durchführung** dieser Bestimmungen lassen.[4] Auch Erwägungsgrund 10 DSGVO sieht vor, dass die Mitgliedstaaten nationale Bestimmungen, mit denen die Anwendung der Vorschriften der Datenschutz-Grundverordnung genauer festgelegt wird, einführen oder beibehalten können. Allerdings müssen sie von ihrem Ermessen unter den Voraussetzungen und innerhalb der Grenzen der Verordnung Gebrauch machen. Die nationalen Gesetzgeber dürfen mithin nur Rechtsvorschriften erlassen, die nicht gegen Inhalt und Ziele der Datenschutz-Grundverordnung verstoßen.[5]

Der konkrete Gestaltungsspielraum für die Mitgliedstaaten fällt dabei von Vorschrift zu Vorschrift durchaus unterschiedlich aus:

1.1.1.1 Ausnahmefall: Regelungsauftrag mit weitem Gestaltungsspielraum in Art. 85 DSGVO

Vereinzelt richtet die Datenschutz-Grundverordnung konkrete Regelungsaufträge an die Mitgliedstaaten. Namentlich Art. 85 DSGVO sieht vor, dass Mitgliedstaaten durch Rechtsvorschriften das Recht auf Datenschutz mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit in Einklang zu bringen haben. Der Wortlaut dieser Vorschrift ermöglicht den Mitgliedstaaten sehr weitgehende Einschränkungen des Datenschutzrechts.

[2] Ständige Rechtsprechung, vgl. Europäischer Gerichtshof, Urteil vom 15. Juni 2021, C-645/19, Rn. 109; Urteil vom 30. März 2023, C-34/21, Rn. 77.

[3] Vgl. Art. 4 Nr. 7 Halbsatz 2, Art. 4 Nr. 8, Art. 6 Abs. 3 Satz 1 Buchst. a und b, Art. 9 Abs. 2 Buchst. a, b, g, h, i, j, Abs. 3, Art. 10 Satz 1, Art. 14 Abs. 5 Buchst. d, Art. 17 Abs. 2 Buchst. e, Art. 28 Abs. 3 Satz 1, Abs. 4, Art. 29, Art. 35 Abs. 10, Art. 49 Abs. 5, Art. 80 Abs. 2, Art. 86, Art. 89 Abs. 2, Abs. 3 sowie Art. 90 DSGVO.

[4] Vgl. zum Beispiel Europäischer Gerichtshof, Urteil vom 28. April 2022, C-319/20, Rn. 57.

[5] Europäischer Gerichtshof, Urteil vom 3. April 2025, C-710/23, Rn. 40; Urteil vom 30. März 2023, C-34/21, Rn. 59; Urteil vom 28. April 2022, C-319/20, Rn. 60 ff.

Diesen Regelungsauftrag des Art. 85 DSGVO hat der Freistaat Bayern unter anderem mit Art. 38 Abs. 1 BayDSG erfüllt, der in Bezug auf die Verarbeitung personenbezogener Daten zu journalistischen, künstlerischen oder literarischen Zwecken die Anwendung des Datenschutzrechts im Wesentlichen auf technisch-organisatorische Fragen beschränkt.

1.1.1.2 Häufiger Regelfall: Öffnungsklauseln als gelenktes legislatives Ermessen

Wesentlich häufiger sieht die Datenschutz-Grundverordnung Öffnungsklauseln vor, die dem nationalen Gesetzgeber zwar Regelungsoptionen eröffnen, bei denen das Ziel eines einheitlichen Datenschutzniveaus aber regulativ relativ strikt abgesichert wird.

Der wohl wichtigste Anwendungsfall der Öffnungsklauseln ist Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 Satz 1 Buchst. b DSGVO. Danach wird die Rechtsgrundlage für den Bereich der Verarbeitung zur Erfüllung von Aufgaben im öffentlichen Interesse im nationalen Recht festgelegt.

Im Freistaat Bayern enthält Art. 4 BayDSG eine allgemeine Rechtsgrundlage für die behördliche Verarbeitung personenbezogener Daten. Sie wird durch Art. 5 BayDSG ergänzt, der Befugnisse speziell für Datenübermittlungen vorsieht. Allerdings können diese Befugnisnormen aus verfassungsrechtlichen Gründen lediglich eine Verarbeitung personenbezogener Daten rechtfertigen, die mit geringfügigen Grundrechtseingriffen verbunden ist.[6] Für weitergehende Verarbeitungen gibt es deshalb auch im bayerischen Recht zahlreiche spezifische Verarbeitungsbefugnisse.

1.1.1.3 Weiterer Regelfall: Spezifizierungsklauseln

Von den Öffnungsklauseln zu unterscheiden sind Spezifizierungsklauseln wie beispielsweise Art. 88 DSGVO. Diese Vorschrift ermöglicht es in Abs. 1 den Mitgliedstaaten, durch Rechtsvorschriften spezifischere Vorschriften zur Gewährleistung des Beschäftigtendatenschutzes vorzusehen. Zugleich legt Art. 88 Abs. 2 DSGVO die Grenzen der von der Datenschutz-Grundverordnung in Kauf genommenen Differenzierung fest.[7]

Der Europäische Gerichtshof hat klargestellt, dass die **Mitgliedstaaten** insoweit **keinen Gestaltungsspielraum** besitzen, von den allgemeinen Vorgaben der Datenschutz-Grundverordnung **inhaltlich abzuweichen**. Vielmehr dürfen sie lediglich Vorschriften erlassen, die einen zu dem geregelten Bereich passenden Regelungsgehalt haben.[8] Wenn die Mitgliedstaaten die Regelungsoption des Art. 88 DSGVO nutzen wollen, können sie sich zudem nicht darauf beschränken, die allgemeinen Bestimmungen der Datenschutz-Grundverordnung lediglich zu wiederholen. Vielmehr müssen sie dann konkretere Vorgaben zum Schutz der Beschäftigten treffen. Insoweit genügt beispielsweise § 26 Abs. 1 Satz 1 Bundesdatenschutzgesetz nicht den Anforderungen einer „spezifischeren“ Vorschrift im Sinne des Art. 88 Abs. 1 DSGVO, weil er den Verarbeitungsgrund des Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO letztlich nur paraphrasiert.

6 Bayerischer Verwaltungsgerichtshof, Beschluss vom 15. Februar 2024, 4 CE 23.2267, Rn. 19 f.
7 Europäischer Gerichtshof, Urteil vom 30. März 2023, C-34/21, Rn. 73.
8 Vgl. Europäischer Gerichtshof, Urteil vom 30. März 2023, C-34/21, Rn. 61.

Das bayerische Personalaktenrecht ist von dieser Rechtsprechung nicht unmittelbar betroffen, worauf ich bereits an anderer Stelle hingewiesen habe.[9]

1.1.2 Verfassungsrecht: Verarbeitung personenbezogener Daten setzt Verarbeitungsbefugnis voraus

Nutzen der Bundes- oder die Landesgesetzgeber Spielräume, die das Unionsrecht eröffnet, müssen sie auch Bindungen durch nationales Verfassungsrecht berücksichtigen. Dies gilt insbesondere für die Grundrechte des Grundgesetzes, wenn unter Gebrauch der Öffnungsklausel aus Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 Satz 1 Buchst. b DSGVO Rechtsgrundlagen für die Verarbeitung personenbezogener Daten geschaffen werden.

Im Mittelpunkt der Betrachtung steht dabei das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1, Art. 1 Abs. 1 Grundgesetz – GG) als nationales „Gegenstück" des unionalen Datenschutzgrundrechts (Art. 8 Abs. 1 Charta der Grundrechte der Europäischen Union). Eine Verarbeitung personenbezogener Daten durch öffentliche Stellen stellt danach in aller Regel einen Grundrechtseingriff dar, der rechtfertigungsbedürftig ist. **„Rechtfertigung" bedeutet** in diesem Zusammenhang, dass der Gesetzgeber eine **hinreichend bestimmte Befugnis** zur Verarbeitung personenbezogener Daten vorsieht und die Verantwortlichen diese Befugnis anwenden. Solche Befugnisse machen eine Verarbeitung davon abhängig, dass bestimmte Voraussetzungen vorliegen. Wie kurz der Gesetzgeber die Behörden dabei „an die Leine legen" kann oder muss, hängt maßgeblich davon ab, wie intensiv die legitimierten Grundrechtseingriffe ausfallen. Dabei sind stets auch Summeneffekte zu berücksichtigen.

So würde es beispielsweise nicht genügen, wenn der Bundesgesetzgeber für die Erfassung von personenbezogenen Meldedaten allein die Aufgaben der Meldebehörden festlegen würde, im Rahmen des Meldewesens ein Register zu führen – die entsprechende Regelung in § 2 Bundesmeldegesetz steht nur an der Spitze eines differenzierten Regelungsprogramms. Verfassungsrechtlich geboten sind hier auch hinreichend bestimmte Verarbeitungsbefugnisse, wie sie in den nachfolgenden Vorschriften des Bundesmeldegesetzes vorgesehen sind. Was die Meldebehörden dürfen und was nicht, ist auf diese Weise klar geregelt. Verarbeitungen von Meldedaten sind vorhersehbar, transparent und leicht zu überprüfen. Damit ist verfassungs- wie unionsrechtlichen Anforderungen gleichermaßen genügt.

Auf Grund der skizzierten verfassungsrechtlichen Vorgaben enthält das deutsche Datenschutzrecht des öffentlichen Sektors durchaus mehr Verarbeitungsregeln als in manchen anderen EU-Mitgliedstaaten. Die Verfassungsordnungen vieler anderer EU-Mitgliedstaaten lassen nämlich eine Aufgabenbeschreibung als Rechtsgrundlage für die Verarbeitung personenbezogener Daten genügen. Es gibt also EU-Mitgliedstaaten, die von Verfassung wegen mit relativ wenigen gesetzlichen Aufgabenbeschreibungen dem Grundsatz der Rechtmäßigkeit genügen und hierzu nicht – wie Deutschland – eine Fülle von Befugnissen schaffen müssen. Bei Gesprächen mit Vertreterinnen und Vertretern anderer EU-Mitgliedstaaten, etwa im Rahmen meiner Funktion als Ländervertreter im Europäischen

[9] Bayerischer Landesbeauftragter für den Datenschutz, Bayerisches Personalaktenrecht und unionales Datenschutzrecht, Aktuelle Kurz-Information 49, Stand 7/2023, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

Datenschutzausschuss (vgl. Abschnitt 10), erfahre ich, dass sie vor dem Hintergrund ihrer Regelungslage die deutsche Diskussion um bürokratische Hemmnisse durch das EU-Datenschutzrecht nur teilweise nachvollziehen können.

Die Datenschutz-Grundverordnung verhält sich zu den verfassungsrechtlichen Rahmenbedingungen der Verarbeitung personenbezogener Daten im öffentlichen Interesse neutral. Das Ermessen der nationalen Gesetzgeber wird insoweit lediglich durch die Vorgaben des Art. 6 Abs. 3 Satz 2 bis 4 DSGVO gelenkt.

Im Übrigen sind grundsätzlich alle übrigen Tatbestandsvoraussetzungen des Art. 6 Abs. 1 DSGVO EU-weit einheitlich auszulegen. Entsprechendes dürfte in aller Regel für die Anwendung der Datenschutzgrundsätze des Art. 5 Abs. 1 DSGVO gelten.[10] Jedenfalls gilt für die Begrifflichkeiten der Datenschutz-Grundverordnung, dass sie grundsätzlich in der gesamten Union eine autonome und einheitliche Auslegung erhalten, die insbesondere unter Berücksichtigung des Wortlauts der betreffenden Bestimmung, der mit ihr verfolgten Ziele und des Zusammenhangs, in den sie sich einfügt, zu ermitteln ist.[11]

1.1.3 Fazit

Im Ergebnis enthält die Datenschutz-Grundverordnung in der Auslegung des Europäischen Gerichtshofs durchaus Vorschriften, die den nationalen Gesetzgebern einen gewissen Gestaltungsspielraum belassen. Häufig geht es dabei allerdings nur um die Frage des „Ob“ einer Regelung. Hinsichtlich des „Wie“ einer Verarbeitung personenbezogener Daten unterliegen die Mitgliedstaaten nicht nur Grenzen aus dem Unionsrecht, sondern auch aus dem nationalen Verfassungsrecht. Vor diesem Hintergrund könnte es sich als „Selbstüberforderung“ erweisen, wenn ein effektiver Rückbau von Bürokratielasten gerade mit einem Instrument erreicht werden soll, das nur einen sehr punktuellen Zugriff auf die Regelungsmaterie erlaubt.

Reale Gestaltungsmöglichkeiten bestehen dagegen bei einer Weiterentwicklung des europäischen Datenschutzrechts. Einen ersten legislativen Vorschlag zur Änderung der Datenschutz-Grundverordnung hat die Europäische Kommission im Mai 2025 – also nach dem Ende des Berichtszeitraums – veröffentlicht, um die bürokratischen Lasten für kleine und mittlere Unternehmen zu reduzieren. Nach gegenwärtigem Stand werden bayerische öffentliche Stellen von diesen Vorschlägen voraussichtlich nicht unmittelbar profitieren.[12] Unbenommen bleibt den Lan-

[10] Hier nicht vertiefen kann ich die Frage, welche Spielräume Öffnungsklauseln ermöglichen, die wie etwa Art. 23 Abs. 1 DSGVO Beschränkungen oder wie Art. 9 Abs. 2 DSGVO Ausnahmen von Verarbeitungsverboten zulassen. Es sei nur angemerkt, dass sie als Ausnahme von der Regel eng auszulegen sind; vgl. exemplarisch in Bezug auf Art. 23 Abs. 1 DSGVO etwa Europäischer Gerichtshof, Urteil vom 26. Oktober 2023, C-307/22, Rn. 53 ff., und in Bezug auf Art. 9 Abs. 2 DSGVO Europäischer Gerichtshof, Urteil vom 4. Oktober 2024, C-446/21, Rn. 76, jeweils mit weiteren Nachweisen.

[11] Vgl. Europäischer Gerichtshof, Urteil vom 19. Dezember 2024, C-65/23, Rn. 37; Urteil vom 14. Dezember 2023, C-340/21, Rn. 23 mit weiteren Nachweisen.

[12] Vgl. Europäische Kommission, Vorschlag vom 21. Mai 2025 für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnungen (EU) 2016/679, (EU) 2016/1036, (EU) 2016/1037, (EU) 2017/1129, (EU) 2023/1542 und (EU) 2024/573 hin-

desgesetzgebern, ihre Rechte insbesondere aus Art. 23 GG zu nutzen, um „Straffungspotenziale“ im unionalen Datenschutzrecht deutlich zu machen und legislative Handlungsimpulse daraus zu generieren.

1.2 Über diesen Tätigkeitsbericht

Der Tätigkeitsbericht zieht eine Bilanz meiner **Arbeit aus dem Jahr 2024**. Was diese Arbeit ausmacht, hängt wesentlich davon ab, welche Gesetzgebungsvorhaben anstehen, welche Datenschutzfragen bei der Prüfung von Beschwerden und Beratungsanfragen aufkommen, welche Datenpannen sich ereignen, oder welche Entwicklungen der Informationstechnologie Datenschutzrelevanz erlangen. So zeigt auch dieser Tätigkeitsbericht wieder, wie Unionsrecht und nationales Recht in vielfältigen Verwaltungsmaterien Datenschutzüberlegungen veranlassen und wie Verantwortliche, behördliche Datenschutzbeauftragte und insbesondere meine Behörde auf Lösungen hinwirken, die pragmatischen Bedürfnissen, gleichermaßen aber den Bindungen aus der Datenschutz-Grundverordnung, dem Bayerischen Datenschutzgesetz und den bereichsspezifischen Regelungen gerecht werden.

Im Bereich der **Allgemeinen Inneren Verwaltung** konnte ich die Implementierung der vom Gesetzgeber neu eröffneten Gestaltungsmöglichkeiten beim Streaming von kommunalen Gremiensitzungen sowie von Bürgerversammlungen in einem Papier mit konkreten Hinweisen unterstützen (Beitrag Nr. 3.1). Namen von Personen zu veröffentlichen, die Gemeinden Geld zukommen lassen, kann die Korruptionsprävention nahelegen; manchmal möchte eine Spenderin oder ein Spender aber auch einfach ein gutes Werk tun, ohne dass irgendwer davon erfährt. Wie weit einem solchen Vertraulichkeitsinteresse entsprochen werden kann, habe ich anlässlich der Beratungsanfrage einer Gemeinde untersucht (Beitrag Nr. 3.2). Ferner war ich etwa mit der datenschutzkonformen Einrichtung eines digitalen „Mängelmelde-Tools“ befasst (Beitrag Nr. 3.3).

Einen Schwerpunkt bei der Beratung der **Polizei** bildete die Begleitung eines Gesetzgebungsverfahren, das die Voraussetzungen für den Einsatz einer verfahrensübergreifenden Recherche- und Analyseplattform betraf. Meine ausführliche, in Anbetracht meines gesetzlichen Auftrags zum Grundrechtsschutz unvermeidlich kritische Stellungnahme fand im Ergebnis leider wenig Gehör (Beitrag Nr. 2.1). Aus dem Polizeialltag beschäftigten mich auch im Berichtsjahr Speicherungen für Bürgerinnen und Bürger ungünstiger Informationen in den zahlreichen polizeilichen Dateien. Gleich drei Beiträge befassen sich mit Facetten dieses Themas (Beiträge Nr. 2.3 bis 2.5). Außerdem habe ich beispielsweise die Transparenz beim Einsatz von Polizeidrohnen sowie die Einhaltung datenschutzrechtlicher Vorgaben bei Observationen kontrolliert (Beiträge Nr. 2.2 und 2.8). Was die **Justiz** betrifft, möchte ich eine Beanstandung hervorheben, die ich gegenüber einer Staatsanwaltschaft ausgesprochen habe. Dabei ging es um eine ungesetzliche, für die betroffene Person zumindest potenziell folgenschwere Mitteilung aus einem dort geführten Verfahren (Beitrag Nr. 2.10).

Auch aus den vielfältigen Datenschutzproblemen im **Sozial- und Gesundheitsbereich** kann der Tätigkeitsbericht nur einige wenige aufgreifen. So gab mir eine

sichtlich der Ausweitung bestimmter für kleine und mittlere Unternehmen verfügbarer Abhilfemaßnahmen auf kleine Midcap-Unternehmen sowie hinsichtlich weiterer Vereinfachungsmaßnahmen, COM (2025) 501.

Beschwerde Anlass, die Wirkung datenschutzrechtlicher Vorgaben auf die behördliche Sachverhaltsermittlung näher zu analysieren. Insgesamt bin ich hier zu der Einschätzung gelangt, dass diese Vorgaben zwar einer gelegentlich zu beobachtenden „Überaufklärung" entgegenwirken, eine gründliche und kritische Sachverhaltsermittlung aber nicht hindern, wenn sie an den entscheidungserheblichen Normen orientiert bleibt (Beitrag Nr. 4.1). Einige Beratungsanfragen erreichten mich im Zusammenhang mit der Mitteilungsverordnung, in der es um Datentransfers von öffentlichen Stellen zu den Finanzämtern geht. Meine Erkenntnisse aus der Beschäftigung mit dieser recht spröden Materie habe ich in einem mehrteiligen Beitrag zusammengestellt (Beitrag Nr. 4.3). Ein unscheinbares, jedoch nicht ganz triviales Problem war die datenschutzrechtliche Verantwortlichkeit beim Wirken der ehrenamtlichen Pharmazieräte (Beitrag Nr. 4.7). Einrichtungen kritischer Infrastruktur sind mitunter darauf angewiesen, sicherheitssensible Bereiche mit Videotechnik zu überwachen. Die einschlägige gesetzliche Regelung lässt dies nur bei Nachweis einer Gefahrsituation zu. Dieser Nachweis kann am einfachsten mit einer Vorfallsdokumentation geführt werden. Einer bei mir anfragenden öffentliche Stelle konnte ich gleichwohl einen Weg aufzeigen, wie sie den Nachweis auch auf andere Art seriös führen kann (Beitrag Nr. 4.8).

Der **Personaldatenschutz** ist sehr detailliert und weithin landesrechtlich geregelt. Auf einem kontinuierlichen Strom von Beschwerden und Beratungsanfragen fließen mir hier immer wieder neue Datenschutzprobleme zu. So war ich gleich in zwei Fällen mit Datenerhebungen bei der Berufung von Professoren an bayerischen öffentlichen Hochschulen befasst. Einwände hatte ich gegen die Beschaffung von Informationen über eingestellte Straf- oder Disziplinarverfahren (Beitrag Nr. 5.1), während ich dem Verlangen einer Hochschule nach der frühzeitigen Vorlage einstellungsrelevanter Urkunden – auch auf Grund von Besonderheiten des Berufungsverfahrens – nicht entgegengetreten bin (Beitrag Nr. 5.2). Weniger speziell war die Frage, was bei einer Veröffentlichung von Beschäftigtendaten im Internet zu beachten ist. Die gesetzlichen Regelungen bieten hier eine Balance von Transparenz- und Vertraulichkeitsinteresse und sind gar nicht schwer anzuwenden (Beitrag Nr. 5.4).

Meine Datenschutzarbeit bei den bayerischen **öffentlichen Schulen** profitiert weiterhin von einer bereits über zwei Jahrzehnte aufgebauten Wissensbasis, die – in den Tätigkeitsberichten sowie ergänzenden Papieren dokumentiert – den Beteiligten ein hohes Maß an Handlungssicherheit vermittelt. Häufig sind daher Detailfragen zu klären, wie auch die aktuellen Beiträge in diesem Themenfeld zeigen. Hervorheben möchte ich eine Beschwerde, die den Umgang einer Schulleitung mit einem Auskunftsantrag betraf. Der Fall macht auf selten exemplarische Weise deutlich, wie einfallsreich öffentliche Stellen Auskunftsansprüche mitunter zu blockieren suchen und wie wenig tragfähig viele der vorgebrachten Hinderungsgründe bei näherer Betrachtung sind (Beitrag Nr. 6.2).

Im **technisch-organisatorischen Datenschutz** ist von massiven Hackerangriffen auf bayerische öffentliche Stellen zu berichten. Leider haben es IT-Verantwortliche den Hackern mitunter zu leicht gemacht, weil sie etwa ein wirksames Patch-Management versäumt haben. In diesem Kontext habe ich einige förmliche Beanstandungen ausgesprochen (Beitrag Nr. 8.6). Weiterhin erläutere ich – auch für Bürgerinnen und Bürger – Maßnahmen gegen Phishing-Angriffe sowie gegen eine unerwünschte Nutzung internetverfügbarer Fotos für das Training Künstlicher Intelligenz (Beiträge Nr. 8.3 und 8.1). In der analogen Welt waren etwa der Postversand von Datenträgern oder – wieder einmal – der Fehlversand von behördlichen Schreiben Gegenstände meiner Tätigkeit (Beitrag Nr. 8.5 und 8.2).

Soweit sich meine Kontrolltätigkeit schließlich auf den informationsfreiheitsrechtlichen **Zugangsanspruch aus Art. 39 BayDSG** bezieht, konnte ich einen größeren Fall abschließen, den ich bereits im letzten Tätigkeitsbericht geschildert habe. Ein Verein, der bei einer Vielzahl von Kommunen bestimmte Informationen angefragt hatte, gelangte mit meiner Unterstützung am Ende in der ganz überwiegenden Zahl der Fälle zum Ziel. In nicht wenigen Rathäusern wurde viel zu viel Zeit darin investiert, einen Anspruch nicht zu erfüllen, dessen Voraussetzungen recht offensichtlich gegeben waren (Beitrag Nr. 7.1). Einem Bürger, der Zugang zu einem „Abschleppkatalog" begehrte, konnte ich leider nicht weiterhelfen (Beitrag Nr. 7.3).

Einen besonderen **Dank** möchte ich in diesem Jahr den **Mitarbeiterinnen und Mitarbeitern meiner Geschäftsstelle** aussprechen. Von ihnen wird die Datenschutzarbeit geleistet, aus der dieser Tätigkeitsbericht eine Essenz zieht.

Neben dem Stammpersonal der Dienststelle, zu dem insbesondere die Referatsleitungen sowie die Servicekräfte zählen, sind hier die Referentinnen und Referenten zu nennen, meist junge Juristinnen und Juristen, die für eine gewisse Zeit aus den Staatsministerien, nachgeordneten Behörden oder der Justiz entsandt werden und bei mir vertiefte Datenschutzkompetenz erwerben. Sie erarbeiten die meisten Beratungsschreiben in Gesetzgebungsverfahren und bei konkreten Datenschutzproblemen bayerischer öffentlicher Stellen, Entscheidungen in Datenschutz-Beschwerdeverfahren samt dem nicht selten umfangreichen vorbereitenden Schriftverkehr, führen Vor-Ort-Prüfungen durch, halten Vorträge oder nehmen an Gremiensitzungen auf nationaler wie unionaler Ebene teil. All das sind fordernde, mitunter auch zeitlich gedrängt zu erledigende Aufgaben.

So werden die Voraussetzungen geschaffen, dass die Referentinnen und Referenten im Datenschutz handlungssicher zu ihren „Heimatbehörden" zurückkehren können. Sie dürfen dort im Idealfall ihre Expertise einbringen, Geschäftsprozesse von vornherein datenschutzgerecht zu steuern – damit Zeit, Geld oder Nerven kostende Probleme mit „dem Datenschutz" bereits gelöst werden, bevor sie entstehen können. Meine „Ehemaligen" können aber auch als Multiplikatoren wirken, die Funktion von behördlichen Datenschutzbeauftragten, von IT-Sicherheits- oder KI-Beauftragten übernehmen. Viele Ressorts der Bayerischen Staatsregierung haben diese Mehrwerte längst erkannt; mit einigen haben sich im Lauf der Zeit verlässliche „Entsende-Kooperationen" herausgebildet, von denen meine Behörde, das „Partnerministerium", aber auch sein nachgeordneter Bereich kontinuierlich profitieren. Gleichwohl böte eine Ausdehnung der engeren Zusammenarbeit auf weitere Teile der bayerischen Staatsverwaltung zusätzlichen Gewinn.

1.3 Neue Beiträge im digitalen Informationsangebot des Landesbeauftragten

Die Erläuterung des datenschutzrechtlichen Handlungsrahmens in einem breit gefächerten Informationsangebot für Verantwortliche des bayerischen öffentlichen Sektors ist mir seit jeher ein besonderes Anliegen. Daher freue ich mich sehr, dass im Jahr 2024 **zwei neue Orientierungshilfen** erscheinen konnten. Die beiden in der Erstellung aufwändigen Papiere dienen weniger einer „Grundsensibilisierung" oder dem ersten Überblick, sondern sollen bayerischen öffentlichen Stellen dabei helfen, auch schwierige Fragestellungen auf dem jeweiligen Themengebiet fachlich seriös in den Griff zu bekommen.

— Die Orientierungshilfe **„Gemeinsame Verantwortlichkeit“**[13] spiegelt die durch Digitalisierung und Globalisierung zunehmende Kooperation bei Datenumgängen wider. Sie soll durch die Vermittlung des nötigen Hintergrundwissens die Handlungssicherheit für bayerische öffentliche Stellen bei gemeinsam mit anderen Verantwortlichen durchgeführten Datenverarbeitungen erhöhen. Auf 71 Seiten behandelt die Orientierungshilfe nicht nur Voraussetzungen und Rechtsfolgen der gemeinsamen Verantwortlichkeit, sondern gibt auch ausführliche Hinweise zur Abgrenzung von anderen in der Datenschutz-Grundverordnung vorgesehenen Rollen sowie zur Gestaltung einschlägiger Vereinbarungen.

— Demgegenüber erläutert die Orientierungshilfe **„Daten-Governance-Rechtsakt“**[14] die seit Herbst 2023 vor dem Hintergrund einer beabsichtigten Erhöhung der Datenverfügbarkeit unionsweit geltenden Mechanismen für die Weiterverwendung bestimmter Kategorien geschützter Daten im Besitz öffentlicher Stellen. Sie befasst sich zudem mit den erstmals in dieser Form gesetzlich formulierten Rahmenbedingungen für Datenvermittlungsdienste und Datenaltruismus sowie mit Drittlandtransfers nicht personenbezogener Daten.

In der Reihe der **„Aktuellen Kurz-Informationen“** habe ich im Berichtsjahr die Nummern 53 bis 56 bereitgestellt. Hervorzuheben ist hier der Beitrag **„Widerspruchsrechte der Versicherten bei der elektronischen Patientenakte“**[15], der insbesondere Patientinnen und Patienten die vielfältigen Möglichkeiten des „Zugriffsmanagements“ beim eigenen Datenbestand nahebringen soll.

Von meinem zweisprachigen (deutsch/englisch) Newsletter **„Privacy in Bavaria“** konnte ich 2024 acht Ausgaben veröffentlichen. Für das kommende Jahr sind neue Publikationen, auch Überarbeitungen bereits vorhandener Papiere geplant. Verantwortliche des bayerischen öffentlichen Sektors, ihre behördlichen Datenschutzbeauftragten und alle anderen am Datenschutz Interessierten erfahren auf meinem **Mastodon-Kanal** https://social.bund.de/@BayLfD tagesaktuell, was es an Neuem gibt.

[13] Bayerischer Landesbeauftragter für den Datenschutz, Gemeinsame Verantwortlichkeit, Stand 6/2025, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek“.

[14] Bayerischer Landesbeauftragter für den Datenschutz, Daten-Governance-Rechtsakt. Auf dem Weg zu einem europäischen Binnenmarkt für Daten, Stand 5/2025, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek“.

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

2 Polizei, Justiz, Verfassungsschutz

2.1 Änderung des Polizeiaufgabengesetzes

Am 1. August 2024 trat das Gesetz zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften[16] in Kraft.

Bereits im November 2023 hatte mich das Bayerische Staatsministerium des Innern, für Sport und Integration über einen entsprechenden Gesetzentwurf unterrichtet.

Neben weiteren Änderungen sollte zum einen die Entscheidung des Bundesverfassungsgerichts vom 9. Dezember 2022, 1 BvR 1345/21, zum Gesetz über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern, welche indirekt auch Auswirkungen auf mehrere Vorschriften im Polizeiaufgabengesetz hatte, umgesetzt werden. Zum anderen sollte vor allem eine Rechtsgrundlage für die zukünftige Nutzung einer verfahrensübergreifenden Recherche- und Analyseplattform zum regelbasierten und formatübergreifenden Abgleich sowie zur Zusammenführung polizeiinterner Daten (VeRA) unter Berücksichtigung der Entscheidung des Bundesverfassungsgerichts vom 16. Februar 2023, 1 BvR 15/19 und 1 BvR 2634/20, geschaffen werden. Der geplanten Einführung einer Rechtsgrundlage für VeRA ging ein längerer Austausch zwischen dem Innenministerium und mir voraus, den ich ausführlich in meinem 32. Tätigkeitsbericht 2022 unter Nr. 3.1 dargestellt habe.

Im Rahmen des Gesetzgebungsverfahrens hatte ich Gelegenheit, mich zu den geplanten Änderungen des Polizeiaufgabengesetzes zu äußern. Meine ausführliche datenschutzrechtliche Bewertung des Gesetzesvorhabens habe ich veröffentlicht.[17] Daher gehe ich im Folgenden nur auf einige Aspekte ein, die mir als besonders wichtig erscheinen.

Eine meiner zentralen Forderungen im Gesetzgebungsverfahren betraf die Rechtsgrundlage für VeRA (Art. 61a PAG). Unter anderem wies ich diesbezüglich darauf hin, dass ich das spezifische Eingriffsgewicht der nach Art. 61a Abs. 1 PAG sowie vor allem auch in Art. 61a Abs. 2 PAG formulierten Befugnisse zur Datenanalyse oder -auswertung durch VeRA gemäß den vom Bundesverfassungsgericht in seiner Entscheidung vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, aufgestellten Grundsätzen für sehr hoch halte. Daher müssen diese Regelungen von Verfassungs wegen strengen Eingriffsvoraussetzungen genügen, insbesondere dem Schutz besonders gewichtiger Rechtsgüter dienen. Auch der Eingriffsanlass muss eng begrenzt sein. Aus diesem Grund habe ich die Streichung von Art. 61a Abs. 2 Satz 1 Nr. 1 PAG und die Anpassung von Art. 61a Abs. 2 Satz 1 Nr. 2 PAG gefordert. Soweit man an der Ausgestaltung von Art. 61a Abs. 2 PAG festhalte, genügten die Eingriffsschwellen nach meiner Auffassung nicht den

[16] Vom 23. Juli 2024 (GVBl. S. 247).

[17] Bayerischer Landesbeauftragter für den Datenschutz, Stellungnahme zum Fragenkatalog im Rahmen der Anhörung des Ausschusses für Kommunale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024, Internet: https://www.datenschutz-bayern.de, Rubrik „Themengebiete – Polizei".

verfassungsrechtlichen Anforderungen. Aus meiner Sicht ließe sich eine hinreichende Beschränkung des Eingriffsgewichts nur durch den normenklar festgeschriebenen Ausschluss von Systemen oder Dateien erreichen, die auf Art. 54 Abs. 1 PAG beruhen, also dem Zwecke der Aufgabenerfüllung, Dokumentation oder Vorgangsverwaltung dienen.

Aber auch im Weiteren enthielt der Gesetzentwurf aus meiner Sicht kritikwürdige Punkte:

So knüpft Art. 16 PAG die Meldeanordnung nun nicht mehr an die Bedrohung eines bedeutenden Rechtsgutes. Diese Herabsenkung der Anforderungen für eine Meldeanordnung hielt ich für nicht nachvollziehbar und ich machte im Gesetzgebungsverfahren unter anderem darauf aufmerksam, dass die Regelung trotz der Eingriffstiefe keine ausreichenden grundrechtssichernden Begleitmaßnahmen vorsehe.

Eine weitere datenschutzrechtlich problematische Neuerung stellt die Regelung des Art. 33 Abs. 10 PAG dar. Diese Vorschrift erlaubt es der Polizei, auf Bildaufnahmen und Bildaufzeichnungen anderer Betreiber von Videoüberwachungsanlagen zuzugreifen. Ich habe in meinen Stellungnahmen unter anderem angemerkt, dass die in Art. 33 Abs. 10 PAG vorgesehenen weitreichenden Zugriffsmöglichkeiten eine massive Ausdehnung der polizeilichen Nutzung von Videoüberwachungsmaterial erwarten lassen. Unter Beachtung der Verhältnismäßigkeit und vor dem Hintergrund einer Überwachungsgesamtrechnung[18] habe ich diese Neuregelung daher aus datenschutzrechtlicher Sicht als bedenklich bewertet.

Insgesamt muss ich festhalten, dass in dem neuen Änderungsgesetz Befugnisse enthalten sind, die erwarten lassen, dass der Polizei noch mehr Datenmaterial zur Verfügung steht als bisher. Hinzukommt, dass aufgrund der fortschreitenden Digitalisierung Bürgerinnen und Bürger immer mehr Daten über die eigene Person generieren, auf welche die Polizei im Rahmen ihrer Aufgabenerfüllung dann zugreifen kann. Durch die geplante Einführung einer datenbank- und formatübergreifenden Recherche innerhalb der polizeiinternen Datenbestände zur Unterstützung der Analyse und Auswertung erhalten solche Daten einen anderen „Wert“ und das Eingriffsgewicht der bloßen Speicherung erhöht sich weiter.

Vor diesem Hintergrund hielt ich eine isolierte Einführung von VeRA ohne gleichzeitige Anpassung der polizeilichen Datenverarbeitungsregelungen in Art. 54 PAG aus Sicht des Datenschutzes grundsätzlich für problematisch.

Ich habe daher im Gesetzgebungsverfahren insbesondere empfohlen, die Mitziehklausel (Art. 54 Abs. 2 Satz 6 PAG, siehe dazu insbesondere meinen 30. Tätigkeitsbericht 2020 unter Nr. 5.5) ersatzlos zu streichen, sowie in Art. 54 Abs. 1 PAG eine regelmäßige Höchstspeicherfrist von zwei Jahren sowie die Verpflichtung aufzunehmen, den Zweck der Speicherung (Aufgabenerfüllung, Vorgangsverwaltung oder Dokumentation) eindeutig und verbindlich festzuhalten.

Durch derartige gesetzgeberische Maßnahmen könnte der in der Rechtsprechung des Bundesverfassungsgerichts wesentlichen Überwachungsgesamtrechnung, aber auch allgemeinen Verhältnismäßigkeitserwägungen ein Stück weit

[18] Vgl. Bundesverfassungsgericht, Urteil vom 2. März 2010, 1 BvR 256/08, 1 BvR 263/08 und 1 BvR 586/08, BeckRS 2010, 46771, Rn. 218.

Rechnung getragen werden. Leider ist der Gesetzgeber meinen Anregungen nicht gefolgt.

2.2 Einsatz von Unbemannten Luftfahrtsystemen (ULS) im Rahmen von Fußballspielen

Unbemannte Luftfahrtsysteme (ULS), umgangssprachlich auch als Drohnen bekannt, kommen bei polizeilich relevanten Anlässen immer häufiger zum Einsatz. Ausgestattet mit Video- und Wärmebildkameras wird die Technik beispielsweise bei der Suche nach vermissten Personen im unwegsamen Gelände, zur Fertigung von Übersichtsaufnahmen nach größeren Unfällen oder im Rahmen von Veranstaltungen wie etwa Fußballspielen genutzt.

Art. 47 Abs. 1 Nr. 1 PAG in Verbindung mit Art. 33 Abs. 1 bis 3 PAG gestattet der Polizei offene Bild- und Tonaufzeichnungen mittels Drohne. So können unter den Voraussetzungen des Art. 33 PAG auch während öffentlichen Veranstaltungen personenbezogene Daten offen erhoben oder Übersichtsaufzeichnungen gefertigt werden. Die Polizei treffen hier Transparenzpflichten (vgl. Art. 47 Abs. 2 PAG, siehe bereits meinen 29. Tätigkeitsbericht 2019 unter Nr. 3.5).

Aufgrund bei mir eingegangener Beschwerden habe ich den Einsatz von ULS im Rahmen von Fußballspielen bei zwei Polizeipräsidien datenschutzrechtlich überprüft. Insbesondere die Wahrung der Offenheit einer solchen Maßnahme stand dabei im Vordergrund.

Bei einem Präsidium waren Drohneneinsätze bei zwei Fußballspielen insgesamt nicht zu beanstanden. Transparenzmaßnahmen wie eine gezielte Fananspräche durch sogenannte Kommunikationsbeamte, wiederkehrende Lautsprecherdurchsagen sowie ein Informationsschreiben an die Fanbeauftragten flankierten die Polizeieinsätze und führten so zu einer ausreichenden Wahrnehmbarkeit der Videoaufnahmen durch Drohnen.

Auch die Überwachungsmaßnahmen des anderen Polizeipräsidiums bewegten sich grundsätzlich im Rahmen der oben angeführten Rechtsgrundlagen. Die Offenheit der Maßnahme sollte hier allerdings allein durch den Schriftzug „POLIZEI“ auf dem ULS gewährleistet werden. Aufgrund der zum Teil großen Distanzen von ULS zur überwachten Menschenmenge oder auch bei schlechten Sichtverhältnissen durch Nebel oder Dämmerung bewerte ich die Aufschrift „POLIZEI“ auf der Drohne oder auch eine angepasste, polizeitypische Farbgebung (blau-gelb) jedoch als allein nicht ausreichendes Mittel, um die Offenheit der polizeilichen Videoüberwachung sicherzustellen. Zudem befinden sich ein ULS fliegende Polizeikräfte nicht unbedingt in Sichtweite der Drohne, so dass der Hinweispflicht auch mit einer gekennzeichneten Einsatzkleidung nicht in jedem Fall Genüge getan wird. Geeignete zusätzliche Maßnahmen wären daher etwa die Anbringung von gut sicht- und lesbaren Hinweisschildern mit einem Verweis auf die Videoaufzeichnungen (zum Beispiel mit Piktogrammen), oder bei Bedarf auch Lautsprecherdurchsagen. Da das Polizeipräsidium in diesem Fall die Drohne nicht konspirativ eingesetzt hatte, hielt ich weitere aufsichtsrechtliche Maßnahmen nicht für geboten und beließ es bei einem Hinweis darauf, meine Ausführungen zur Kenntlichmachung eines ULS-Einsatzes künftig zu beachten.

Unabhängig davon bin ich vor dem Hintergrund der wachsenden Bedeutung des Einsatzmittels „Drohne“ weiterhin im Austausch mit der Bayerischen Polizei.

2.3 Prüfung der Speicherung jugendlicher Intensivtäter

Als jugendliche Intensivtäter gelten junge Menschen im Alter von zehn bis 20 Jahren, die durch wiederholtes delinquentes Verhalten in Erscheinung treten. Nachdem diese relativ kleine Gruppe häufig für einen Großteil der Straftaten in diesem Altersspektrum verantwortlich gemacht wird, stellt sie eine besondere Herausforderung für die Polizei dar. In vielen Bundesländern werden daher spezielle Jugendintensivtäter-Programme mit entsprechenden Dateien geführt, um die jungen Menschen vor einer lebenslangen Karriere als Kriminelle abzuhalten. So werden auch bei bayerischen Polizeipräsidien in solchen Dateien polizeilich relevante Ereignisse gesammelt, ausgewertet und zusammengeführt. Dadurch sollen polizeiliche Präventivmaßnahmen zur unmittelbaren Straftatenverhinderung, jedoch auch eine Umsetzung längerfristiger behördenübergreifender Präventionsansätze ermöglicht werden.

Nachdem von den Speicherungen vornehmlich Kinder und Jugendliche betroffen sind, habe ich die entsprechende Datei eines Polizeipräsidiums im Berichtszeitraum einer datenschutzrechtlichen Prüfung unterzogen. Von den als Intensivtäter geführten Personen habe ich die Speicherungen der drei Jüngsten – ein Kind im Alter von 13 Jahren und zwei 14-jährige Jugendliche – überprüft.

Rechtsgrundlage für derartige Speicherungen ist regelmäßig Art. 54 Abs. 2 Polizeiaufgabengesetz (PAG). Nach dieser Vorschrift kann die Polizei zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten, Daten von Kindern in der Regel für zwei und von Jugendlichen in der Regel für fünf Jahre speichern.

Allein die Tatsache, dass lediglich ein Kind, welches im Zeitraum der Prüfung schon das 14. Lebensjahr erreicht hatte, gespeichert wurde, spricht für eine datenschutzfreundliche und verhältnismäßige Umsetzung der Speichermöglichkeiten durch die Polizei. Ebenfalls positiv kann ich die umfassende und zielorientierte Dokumentation der Prognoseentscheidung hervorheben, die zu jeder gespeicherten Person aufgrund des jeweiligen Tatverhaltens sowie individueller Schutz- und Risikofaktoren erstellt wurde. Schließlich ist diese auch die Bewertungsgrundlage für die Erforderlichkeit zur Fortführung der polizeilichen Präventionsmaßnahmen und damit für die Speicherdauer.

Einträge sind bei diesen jungen Delinquenten jedoch nicht ausschließlich in der genannten Datei, sondern auch in INPOL und IGVP vorhanden.[19] Hier musste ich feststellen, dass die rechtlichen Vorgaben aus Art. 54 PAG in Bezug auf die Festlegung von Aussonderungsprüffristen nicht immer eingehalten wurden. In einem Fall führte beispielsweise die Klarstellung der Ermittlungszuständigkeit in INPOL zur Speicherverlängerung. Diese fehlerhaften Fristsetzungen wurden nach meiner Anregung vollumfänglich korrigiert.

Im Ergebnis kann ich jedoch festhalten, dass die Speicherungen in der oben erwähnten Datei dem präventiven Ziel dienen, die drohende „Kriminalitätsspirale“ bei diesen jungen Menschen nachhaltig zu durchbrechen, und datenschutzrechtlich nicht zu beanstanden waren.

[19] Zu diesen Dateien siehe die Erläuterungen auf https://www.datenschutz-bayern.de unter „Themengebiete – Polizei – Speicherung personenbezogener Daten durch die Polizei“.

2.4 Prüfung der Vergabe des personengebundenen Hinweises „Psychische und Verhaltensstörung (PSYV)“

INPOL (das Informationssystem der Polizei) ist ein elektronischer Datenverbund für die Polizeibehörden des Bundes und der Länder. Betrieben wird INPOL vom Bundeskriminalamt; Daten speichern und abrufen können dort alle teilnehmenden Polizeibehörden. Das System stellt auch einen Katalog mit sog. personengebundenen Hinweisen (PHW) zur Verfügung. Die dort festgelegten Kriterien wie etwa „gewalttätig“, „bewaffnet“, „Ausbrecher“ usw. sollen dem Bundeskriminalamt zufolge „dem Schutz des Betroffenen und der Eigensicherung von Polizeibediensteten“ dienen.

Ist zu einer Person ein PHW vergeben, wird dieses bei einem Datenabruf aus INPOL, beispielsweise im Rahmen einer Personenkotrolle, bei der Ausgabe auffällig angezeigt, damit die kontrollierenden Beamtinnen und Beamten ohne weitere aufwändige Auswertungen von Einzelspeicherungen mit wesentlichen Hinweisen zur überprüften Person versorgt werden. Eine maßgelbliche gesetzliche Regelung zu PHW findet sich in § 29 Abs. 4 Satz 2 in Verbindung mit § 16 Abs. 6 Nr. 1 Bundeskriminalamtgesetz. Danach kann das Bundeskriminalamt in den Fällen, in denen bereits Daten zu einer Person vorhanden sind, zu dieser Person auch personengebundene Hinweise, die zum Schutz dieser Person oder zur Eigensicherung von Beamten erforderlich sind, weiterverarbeiten.

Die fallbezogene Zuweisung eines PHW unterliegt bundesweit einheitlich festgelegten Vergabekriterien. Diese Kriterien müssen bundesweit einheitlich angewendet werden, damit die Datenqualität auch hinsichtlich der PHW verlässlich gesichert ist. Nimmt es eine Polizeidienststelle mit den festgelegten Vergabekriterien nicht so genau, kann sie dadurch den polizeilichen Zweck verfehlen, aber auch die Datenschutzrechte der betroffenen Person verletzen.

Aus diesem Grund habe ich im Berichtszeitraum bei der Bayerischen Polizei die Vergabe des besonders sensiblen PHW „Psychische und Verhaltensstörung (PSYV)“ geprüft.

Eine erste Bestandsaufnahme beim Bayerischen Landeskriminalamt ergab, dass der PHW „PSYV“ von der Bayerischen Polizei im Zeitraum von drei Jahren insgesamt 1.301-mal vergeben wurde.

Diese hohe Anzahl hatte mich überrascht, da die bundesweit einheitlich festgelegten Vergabekriterien des PHW „PSYV“ durchaus anspruchsvoll sind. Demnach darf dieser PHW nur vergeben werden, wenn **ärztlich** festgestellt ist, dass der Betroffene an einer psychischen Erkrankung leidet und daraus Gefahren für ihn selbst oder andere, insbesondere für Polizeibedienstete, resultieren können. Darüber hinaus muss die Information über das Vorliegen einer solchen Erkrankung schriftlich dokumentiert sein (etwa durch ein Attest oder Gutachten).

Führt man sich vor Augen, dass nach Angaben des Bundesministeriums für Gesundheit fast jeder dritte Mensch im Laufe seines Lebens an einer behandlungsbedürftigen psychischen Erkrankung leidet, so sind die oben beschriebenen Eingrenzungen in Form der Vergabekriterien hin auf eine polizeiliche Relevanz dringend notwendig.

Aufgrund der überraschend hohen Zahl der von der Bayerischen Polizei vergebenen PHW konnte ich mich bei meiner Prüfung des PHW „PSYV“ letztlich nur auf Stichprobenfälle innerhalb von drei ausgewählten Polizeipräsidien beschränken.

Meine Prüfungserkenntnisse zur Vergabe des PHW „PSYV“ durch die Bayerische Polizei ließen deutliche Mängel erkennen und zeigten dringenden Handlungsbedarf bei den Polizeipräsidien und auch dem Bayerischen Staatsministerium des Innern, für Sport und Integration als Führungsstelle der Bayerischen Polizei. Drei Viertel der von mir überprüften PHW „PSYV“ entsprachen nicht den oben genannten Vergabekriterien und mussten daher gelöscht werden.

Dabei hatte ich für die Stichprobe von vornherein keine Altfälle, sondern PHW-Vergaben ausgewählt, die in den Zeitraum vom 1. Januar 2020 bis 31. Dezember 2022 fielen. Zu dieser Zeit war das seit Mai 2018 geltende neue Datenschutzrecht etabliert; ein entsprechendes Grundverständnis sowie eine zeitgemäße Sensibilität im Umgang mit Gesundheitsdaten konnten daher vorausgesetzt werden.

Nach meiner Prüfung habe ich das Innenministerium ersucht, im Hinblick auf die von mir bei den Polizeipräsidien festgestellten Problemfelder, insbesondere was die Einhaltung der verbindlichen Vergabekriterien und Maßnahmen zur zeitgerechten Aussonderung angeht, wirksame Überlegungen anzustellen und umzusetzen. Ich erwarte Maßnahmen, die sowohl künftig als auch rückwirkend zur dringend notwendigen Qualitätssicherung und Wahrung der Datenschutzrechte von betroffenen Personen bei der polizeilichen Vergabe des PHW „PSYV“ – und zugleich auch bei allen anderen PHW – beitragen.

Einer ersten Rückmeldung ist zu entnehmen, dass sich das Innenministerium des Themas angenommen und insbesondere zeitnah alle Polizeipräsidien auf die Problematik hingewiesen hat.

Ich werde dem Thema auch künftig meine Aufmerksamkeit schenken und die weitere Entwicklung genau verfolgen.

2.5 Speicherungen im Kriminalaktennachweis trotz unbekannter Verfahrensausgänge

Zu Speicherungen im Kriminalaktennachweis (KAN) erreichen mich kontinuierlich Anfragen und Beschwerden. Die Speicherungen sind daher regelmäßig Gegenstand meiner Prüfungs- und Beratungstätigkeit. Maßgeblich ist insofern Art. 54 Abs. 2 Polizeiaufgabengesetz:

„[1]Die Polizei kann insbesondere personenbezogene Daten, die sie im Rahmen strafrechtlicher Ermittlungsverfahren oder von Personen gewonnen hat, die verdächtig sind, eine Straftat begangen zu haben, speichern und anderweitig verarbeiten, soweit dies zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. [2]Entfällt der der Speicherung zugrunde liegende Verdacht, sind die Daten unverzüglich zu löschen. [3]Die nach Art. 53 Abs. 5 festzulegenden Prüfungstermine oder Aufbewahrungsfristen betragen in der Regel bei Erwachsenen zehn Jahre, bei Jugendlichen fünf Jahre und bei Kindern zwei Jahre. [4]In Fällen von geringerer Bedeutung sind kürzere Fristen festzusetzen. [5]Die Frist beginnt regelmäßig mit dem Ende des Jahres, in dem das letzte Ereignis erfaßt worden ist, das zur Speicherung der Daten geführt hat, jedoch nicht vor Entlassung des Betroffenen aus einer Justizvollzugsanstalt oder der Beendigung einer

mit Freiheitsentziehung verbundenen Maßregel der Besserung und Sicherung. [6]Werden innerhalb der Frist der Sätze 3 bis 5 weitere personenbezogene Daten über dieselbe Person gespeichert, so gilt für alle Speicherungen gemeinsam der Prüfungstermin, der als letzter eintritt, oder die Aufbewahrungsfrist, die als letzte endet."

Eine wesentliche Voraussetzung für eine Speicherung im KAN ist, dass gegen die betroffene Person ein sogenannter polizeilicher Restverdacht besteht (siehe hierzu auch mein 27. Tätigkeitsbericht 2016 unter Nr. 3.6.5). Auch wenn der strafprozessuale Tatnachweis hinsichtlich einer Straftat nicht geführt werden konnte, können Zeugenaussagen oder sonstige Anhaltspunkte dafür sprechen, dass ein Restverdacht fortbesteht; eine Speicherung für präventiv polizeiliche Zwecke bleibt dann möglich.[20]

Im Berichtszeitraum stach in diesem Zusammenhang ein Fall besonders hervor: Ein Beschwerdeführer hatte bei einem Polizeipräsidium um Auskunft und zugleich Löschung seiner personenbezogenen Daten ersucht. Die Bearbeitungsstelle der Polizei hatte der Person daraufhin umfassend Auskunft erteilt und eine Speicherung gelöscht. Im Hinblick auf die weiteren Eintragungen zu dieser Person erklärte die Polizei, diese ebenfalls geprüft, aber für zulässig befunden zu haben. Daher komme eine Löschung nicht in Betracht. Gleichwohl fiel mir in dem Bescheid der Polizei der Satz auf, dass die jeweiligen Verfahrensausgänge zu den gespeicherten Ermittlungsergebnissen im KAN nicht bekannt seien.

Solche „Verfahrensausgänge" geben Auskunft darüber, welches Ergebnis die Justiz aus den polizeilichen Ermittlungen gewonnen hat, ob es etwa zu einer Verurteilung, einer Verfahrenseinstellung wegen Geringfügigkeit oder wegen eines nicht zu führenden Tatnachweises gekommen ist, oder aber zu einem Freispruch wegen erwiesener Unschuld.

Dies macht deutlich, wie wichtig die Kenntnis der Verfahrensausgänge ist und, dass ohne diese Kenntnis die Frage, ob ein polizeilicher Restverdacht – als Grundlage einer Speicherung im KAN – vorliegt, nicht abschließend beantwortet werden kann.

Aus diesem Grund findet sich auch im in meinem 33. Tätigkeitsbericht 2023 unter Nr. 3.2 erwähnten Konzept der Bayerischen Polizei zur Bearbeitung von Auskunfts- und Löschungsersuchen die Vorgabe, dass die Verfahrensausgänge für die Sachverhaltswürdigung eines Löschungsantrags benötigt werden und daher – falls noch nicht vorhanden – bei der zuständigen Staatsanwaltschaft anzufordern sind.

In dem betreffenden Fall habe ich dem zuständigen Polizeipräsidium daher mitgeteilt, dass ich dessen Bewertung zur Zulässigkeit der Speicherungen gegenüber der antragstellenden Person für nicht vertretbar erachte. Des Weiteren sah ich mich veranlasst, das Polizeipräsidium um Einholung aller erforderlichen Verfahrensausgänge zu ersuchen, um auf dieser Grundlage erneut die Speicherungsvoraussetzungen zu prüfen und zu dokumentieren. Das Polizeipräsidium kam meiner Aufforderung nach und versicherte mir, die Hinweise künftig zu beachten.

[20] Vgl. Bundesverfassungsgericht, Beschluss vom 16. Mai 2002, 1 BvR 2257/01, BeckRS 2002, 30260253, sowie Beschluss vom 1. Juni 2006, 1 BvR 2293/03, BeckRS 2009, 35816.

2.6 Beanstandung wegen unzulässiger polizeilicher Beobachtung

Die polizeiliche Beobachtung ist eine eingriffsintensive präventive Maßnahme der Polizei. Sie ist in Art. 40 Abs. 1 Polizeiaufgabengesetz (PAG) geregelt. Dort heißt es:

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

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

Die polizeiliche Beobachtung dient dem Zweck, polizeiliche Zufallserkenntnisse über das Antreffen einer bestimmten ausgeschriebenen Person zusammenzuführen. Die ausschreibende Dienststelle gewinnt diese Erkenntnisse, um insbesondere punktuell die Reisewege der Person sowie andere Zusammenhänge und Querverbindungen nachvollziehen zu können.

Im Falle von verdeckten polizeilichen Eingriffsmaßnahmen hat grundsätzlich jede betroffene Person einen Anspruch auf eine nachträgliche Benachrichtigung. Aufgrund der Mitteilungspflicht aus Art. 50 PAG hatte ein Bürger erfahren, dass er insgesamt fast acht Jahre zur polizeilichen Beobachtung ausgeschrieben war.

Der Bürger sah für seine langjährige „Überwachung" keine Rechtsgrundlage und wandte sich mit der Bitte um Überprüfung an mich. Dem bin ich nachgekommen und habe mir von der Polizei die entsprechenden Anordnungen (Erstanordnung sowie Anordnungen der jeweils einjährigen Verlängerungen) vorlegen lassen.

Hierbei musste ich feststellen, dass diese nicht den gesetzlichen Vorgaben des Art. 40 PAG (beziehungsweise der Vorgängerregelung des Art. 36 PAG in der bis zum 24. Mai 2018 geltenden Fassung) entsprachen:

Dem Wortlaut nach wurden die Erstanordnung sowie die ersten drei Verlängerungen auf Art. 36 Abs. 1 Nr. 1 PAG in der bis zum 24. Mai 2018 geltenden Fassung gestützt. Hiernach musste „die Gesamtwürdigung der Person und ihrer bisher begangenen Straftaten erwarten lassen, daß sie auch künftig Straftaten von erheblicher Bedeutung begehen wird".

Dass der Beschwerdeführer bereits mehrfach, beispielsweise durch versuchte Nötigung, Hausfriedensbruch und Körperverletzung, strafrechtlich in Erscheinung getreten war, genügte für eine polizeiliche Beobachtung nicht, weil es sich dabei nicht um Straftaten von **erheblicher Bedeutung** handelte. Außerdem fehlte es in den Anordnungen an einer fundierten Prognose zur Begehung künftiger Straftaten von erheblicher Bedeutung.

Ähnliches galt für die ab dem Jahr 2019 auf Art. 40 Abs. 1 PAG gestützten Anordnungen. Nach dieser Vorschrift muss die Gesamtwürdigung erwarten lassen, dass

von der Person auch künftig eine Gefahr für bedeutende Rechtsgüter im Sinne des Art. 11 Abs. 3 Satz 2 PAG ausgeht.

Insofern fehlten in den Anordnungen ebenfalls eine Gefahrenprognose und eine ausreichende Begründung. Bisher begangene Straftaten sind nach dem Willen des Gesetzgebers von besonderer Bedeutung und in die Gefahrenprognose mit einzubeziehen. In den geprüften Unterlagen zur Anordnung stellte die Polizei jedoch ausdrücklich fest, dass im zurückliegenden Beobachtungszeitraum gar keine Straftaten bekannt geworden waren. Bei den aufgelisteten Aktivitäten, auf welche sich die Anordnung stützen sollte, handelte es sich zwar um auffällige, jedoch nicht illegale Tätigkeiten im Zusammenhang mit einer vom Verfassungsschutz beobachteten Kleinpartei.

Darüber hinaus hätte vor dem Hintergrund der langen Maßnahmedauer mit jeder Verlängerung eine stets noch kritischere Prüfung der Verhältnismäßigkeit stattfinden müssen. Dies ist bedauerlicherweise unterblieben. Insbesondere mit Blick auf die hohe Dauer der verdeckten Maßnahme habe ich eine Beanstandung gemäß Art. 16 Abs. 4 BayDSG ausgesprochen. Das betreffende Polizeipräsidium räumt die Datenschutzverletzung ein und hat sofort Maßnahmen getroffen, damit vergleichbare Verstöße nicht mehr vorkommen.

2.7 Beanstandung wegen der nicht fristgerechten Löschung von Akkreditierungsdaten

Im Rahmen von Zuverlässigkeitsüberprüfungen nach Art. 60a Bayerisches Polizeiaufgabengesetz (PAG) fallen regelmäßig Akkreditierungsdaten, welche im Vorgangsbearbeitungssystem „Integrationsverfahren Polizei“ (IGVP) gespeichert werden, an (zum Thema „Zuverlässigkeitsüberprüfungen“ siehe auch meinen 31. Tätigkeitsbericht 2021 unter Nr. 3.2 und meinen 33. Tätigkeitsbericht 2023 unter Nr. 3.7).

Derartige Akkreditierungsdaten dürfen von der Polizei nur solange gespeichert werden, wie dies für die Durchführung des Zuverlässigkeitsüberprüfungsverfahrens erforderlich ist.

Durch zwei Datenpannen-Meldungen des zuständigen Polizeiverbands gemäß Art. 33 DSGVO in Verbindung mit Art. 28 Abs. 1 Satz 1 Nr. 1, Abs. 2 Satz 2, Art. 33 BayDSG, die im Abstand von zehn Monaten bei mir eingingen, wurde mir bekannt, dass es wiederholt Fehler bei der fristgerechten Löschung von Akkreditierungsdaten aus dem Vorgangsbearbeitungssystem IGVP gegeben hatte und diese Daten somit zu lange gespeichert wurden.

Dabei hatte ich schon nach der ersten Datenpannen-Meldung, die mir übersandt worden waren, sehr kritisch die Umstände hinterfragt, wie es dazu kommen konnte, dass eine zunächst unbestimmte Anzahl von Personendaten nicht rechtzeitig gelöscht worden war. Vor allem fand ich die in der Meldung vorhandene Einschätzung nicht schlüssig, dass eine Wiederholung des Vorfalls nicht zu befürchten sei, obwohl die tatsächlichen Ursachen des Vorfalls zu diesem Zeitpunkt offensichtlich noch nicht aufgeklärt waren. Ich hatte daher den zuständigen Polizeiverband nachdrücklich um eine Aufklärung der Ursachen ersucht und gebeten, mich darüber und in Bezug auf eine mögliche Wiederholungsgefahr auf dem Laufenden zu halten.

Nachdem ich keine Rückmeldung erhalten hatte, habe ich mit mehreren Erinnerungsschreiben nachgefasst.

Anstatt einer erwarteten detaillierten Aufklärung der näheren Umstände der nicht fristgerechten Aussonderung von Akkreditierungsdaten erreichte mich schließlich rund zehn Monate nach der ersten Datenpannen-Meldung eine zweite Mitteilung, wonach bei einer erneuten Prüfung festgestellt worden sei, dass trotz zweier Löschläufe weiterhin vereinzelt Daten im Vorgangsbearbeitungssystem IGVP vorhanden seien, obwohl diese bereits seit Monaten der Löschung unterlagen.

Auch wenn fortan ernsthafte und sehr aufwändige Bemühungen zur Klärung der wesentlichen Ursachen und deren Beseitigung sowie umfangreiche Abstimmungen insbesondere mit anderen Polizeiverbänden stattfanden, so musste ich, den Gesamtverlauf betrachtend, gleichwohl feststellen, dass dies insbesondere anfänglich nicht der Fall war. Trotz meiner wiederholt ergangenen kritischen Hinweise waren letztendlich zehn Monate verstrichen, in denen durch den zuständigen Polizeiverband keine für mich akzeptable Aufarbeitung erfolgte, das heißt keine genügende Ermittlung der Ursache und keine effektive Verhinderung der Wiederholung beziehungsweise keine hinreichende Beseitigung der kausalen Mängel.

In Anbetracht des für mich zunächst nicht erkennbaren ausreichenden Aufklärungsinteresses, der mangelhaften Transparenz mir gegenüber und der Anzahl der betroffenen Datensätze im unteren vierstelligen Bereich war für mich eine aufsichtliche Maßnahme unumgänglich.

Aus diesem Grund habe ich die nicht fristgerechte Löschung der Akkreditierungsdaten wegen der Verletzung der polizeilichen Löschpflichten nach Art 62 Abs. 2 Satz 1 Nr. 2 und 3 PAG in Verbindung mit Art. 53 Abs. 5 Sätze 1, 2 und 5 PAG sowie wegen des Verstoßes gegen die gemäß Art. 28 Abs. 1 Satz 1 Nr. 1, Abs. 2 Satz 1 Nr. 2 in Verbindung mit Art. 66 Satz 1 PAG anwendbaren Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 DSGVO, namentlich gegen die Grundsätze der Speicherbegrenzung (Buchst. e) sowie der Vertraulichkeit und Integrität (Buchst. f), beanstandet.

2.8 Datenschutzrechtliche Prüfung polizeilicher Observationen

Im Rahmen meiner gesetzlichen Verpflichtung nach Art. 51 Abs. 2 Satz 1 Polizeiaufgabengesetz (PAG), Art. 15 BayDSG habe ich im Berichtszeitraum bei einem Polizeipräsidium die Befugnis zur polizeilichen Observation nach Art. 36 Abs. 1, Abs. 2 PAG geprüft.

Hierfür habe ich das Polizeipräsidium zunächst um eine Auflistung aller längerfristigen Observationen in einem bestimmten Zeitraum gebeten. Das Polizeipräsidium meldete insgesamt vier Fälle. Im Rahmen eines Vor-Ort-Termins habe ich sodann Einsicht in die betreffenden Unterlagen genommen. Dies gab mir die Gelegenheit, unmittelbar Nachfragen zu stellen, die das Polizeipräsidium auch beantworten konnte. Dabei waren einige Mängel festzustellen, was die Erfüllung der Dokumentationspflicht sowie der Pflicht zur Benachrichtigung der betroffenen Person betraf:

Nach Art. 51 Abs. 1 PAG muss die längerfristige Observation protokolliert werden. Das von der Polizei dafür eingesetzte Tool „ProMa“ (Protokollierung polizeilicher

Maßnahmen) erscheint mir als grundsätzlich gut geeignet. Insbesondere waren die vorgelegten Ausdrucke übersichtlich gestaltet. Die vom Bundesverfassungsgericht in seinem BKAG-Urteil aufgestellten Anforderung, dass die Protokolle der kontrollierenden Stelle in praktikabel auswertbarer Weise zur Verfügung stehen sollen,[21] war in Bezug auf die nach Art. 51 Abs. 1 Satz 2 PAG erforderlichen Daten grundsätzlich erfüllt.

Nicht umfassend einverstanden war ich hingegen mit der konkreten „Befüllung" der Eingabemasken: So genügten beispielsweise die Angaben zum Zweck der Observation, zur Art ihrer Ausführung, zur Weiterverarbeitung der erhobenen Daten oder zum wesentlichen Ergebnis der Maßnahme nicht durchgehend den gesetzlichen Vorgaben aus Art. 51 Abs. 1 Satz 2 Nr. 3 ff. PAG.

Nach Art. 50 Abs. 1 Satz 1 Nr. 3 PAG hat unverzüglich eine Benachrichtigung der betroffenen Person zu erfolgen, sobald dies ohne Gefährdung des Zwecks der Maßnahme, der eingesetzten Polizeibeamten beziehungsweise Vertrauenspersonen oder der in der jeweiligen Befugnisnorm genannten Rechtsgüter geschehen kann.

In einem der geprüften Fälle musste ich feststellen, dass die Benachrichtigung fehlte. Die Polizei sah die Benachrichtigung im konkreten Fall als entbehrlich an, da die betroffene Person anderweitig von den Maßnahmen erfahren habe, etwa im Rahmen der Akteneinsicht oder der mündlichen Verhandlung, in welcher die Maßnahmen umfangreich erörtert worden seien.

Ich habe die Polizei darauf hingewiesen, dass diese Vorgehensweise den klaren gesetzlichen Vorgaben nicht gerecht wird – umso mehr, als mir die Polizei nicht nachweisen konnte, dass die betroffene Person auch tatsächlich Kenntnis vom Mindestinhalt der Benachrichtigung nach Art. 50 Abs. 2 in Verbindung mit Art. 31 Abs. 4 Satz 5 und Satz 6 PAG erlangt hatte.

Unter bestimmten Voraussetzungen kann eine Benachrichtigung zwar zunächst zurückgestellt werden, jedoch sind gemäß Art. 50 Abs. 5 PAG die Gründe hierfür zu dokumentieren. Dies dient vor allem auch einer effektiven datenschutzrechtlichen Kontrolle. Leider musste ich auch hier feststellen, dass das von der Polizei verwendete Tool „ProMa" zwar die entsprechenden Angaben vorgesehen hätte, jedoch nicht immer ausreichend befüllt worden war.

Ich habe das betreffende Polizeipräsidium über die festgestellten Mängel informiert und um zukünftige Beachtung der gesetzlichen Vorgaben gebeten.

2.9 Eurodac

Das europäische Fingerabdruck-Identifizierungssystem (Eurodac) dient dazu, Fingerabdrücke von Asylbewerbern und Geflüchteten europaweit zu erheben und zentral zu speichern. Dadurch soll verhindert werden, dass Personen in mehreren EU-Mitgliedstaaten Asyl beantragen. Auch die Polizei kann im Rahmen der festgelegten gesetzlichen und sicherheitstechnischen Vorgaben die gespeicherten

[21] Vgl. Bundesverfassungsgericht, Beschluss vom 20. April 2016, 1 BvR 966/09 und 1 BvR 1140/09, BeckRS 2016, 44821, Rn 141.

Daten verarbeiten, um terroristische oder sonstige schwere Straftaten zu verhüten, aufzudecken und zu untersuchen.

Um gemäß meiner Verpflichtung nach Art. 33 Abs. 2 Eurodac-VO zu überprüfen, ob die Bayerische Polizei den Zugriff auf die Eurodac-Daten rechtskonform umsetzt, habe ich im Prüfungszeitraum Abfragen, die nicht im Zusammenhang mit der sogenannten Altfallsachbearbeitung („cold cases“) stehen, stichprobenartig kontrolliert. Hierzu habe ich mir die diesbezüglichen Anträge für Eurodac-Abfragen aus einem Jahr vorlegen lassen. Der Schwerpunkt meiner Prüfung lag hierbei auf den formalen und inhaltlichen Voraussetzungskriterien des Artikels 20 Abs. 1 Eurodac-VO:

Demnach ist der Abgleich formal nur zulässig, sofern nicht bereits eine Abfrage in nationalen Fingerabdruck-Datenbanken, in nationalen daktyloskopischen Identifizierungssystemen aller anderen Mitgliedsstaaten (sog. PRÜM-Recherche) oder im Visa-Informationssystem zur Feststellung der Identität der betreffenden Person geführt hat („Abfrage-Kaskade“). Inhaltliches Ziel muss zudem die Verhütung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten sein – also ein öffentliches Sicherheitsinteresse bestehen –, der Abgleich muss im Einzelfall erforderlich sein und es müssen hinreichende Gründe zur Annahme vorliegen, dass der Abgleich wesentlich zur Verhütung, Aufdeckung oder Ermittlung einer der fraglichen Straftaten beitragen wird.

Anhand vorgelegter ausgefüllter Antragsformulare zu Eurodac-Anfragen konnte ich jeweils sowohl die durchgeführte Abfrage-Kaskade als auch die inhaltlichen Voraussetzungen, wie Straftatbestand, Darlegung der Erforderlichkeit und die Verdachtsbegründung weitgehend nachvollziehen. Dennoch war es in einem Fall notwendig, weitere Stellungnahmen von der sachbearbeitenden Dienststelle anzufordern, da aus den Anträgen nicht klar hervorging, weshalb in diesem konkreten Fall der begründete Verdacht bestand, dass der unbekannte Täter in der Vergangenheit einen Asylantrag im Dublin-Vertragsgebiet gestellt beziehungsweise eine EU-Außengrenze illegal übertreten haben sollte.

Um die Nachvollziehbarkeit für eine effektive datenschutzrechtliche Kontrolle zukünftig zu verbessern, habe ich angeregt, die Dokumentation in den Antragsformularen insbesondere bei unklarer Sachlage zu intensivieren. Dies kommt vor allem zum Tragen, wenn sich ein begründeter Verdacht oder die Wahrung des Verhältnismäßigkeitsgrundsatzes nicht offensichtlich ergibt. Letztendlich muss die Schwelle für die Abfrage in Eurodac signifikant höher sein als die Schwelle für eine Abfrage strafrechtlicher Datenbanken.

Im Ergebnis waren die geprüften Zugriffe der Bayerischen Polizei auf das europäische Fingerabdruck-Identifizierungssystem jedoch nicht zu beanstanden. Alle formalen und inhaltlichen Voraussetzungen waren in den geprüften Fällen eingehalten.

In einem nächsten Schritt habe ich begonnen, mich mit Eurodac-Anträgen im Zusammenhang mit Altfällen zu beschäftigen und stehe hierzu im Austausch mit der Polizei.

2.10 Beanstandung einer Staatsanwaltschaft wegen unzulässiger Datenübermittlung

Immer wieder wenden sich Bürgerinnen und Bürger an mich, die sich durch die Mitteilung von Informationen aus Strafsachen durch Staatsanwaltschaften an andere öffentliche Stellen in ihren subjektiven Datenschutzrechten verletzt sehen.

Grundsätzlich sind Staatsanwaltschaften in Strafsachen zwar nach Maßgabe von §§ 12 ff. Einführungsgesetz zum Gerichtsverfassungsgesetz (EGGVG) zur Mitteilung personenbezogener Daten an andere öffentliche Stellen auch für verfahrensfremde Zwecke befugt. Verpflichtet sind sie zu entsprechenden Mitteilungen allerdings nur, wenn dies im Rahmen der Anordnung über Mitteilungen in Strafsachen (MiStra) angeordnet oder in besonderen Vorschriften bestimmt ist (siehe Nr. 1 Abs. 1 Satz 2 MiStra).

Nach Nr. 39 Abs. 1 MiStra sind in Strafsachen gegen Inhaberinnen und Inhaber von Berechtigungen und gegen Gewerbetreibende rechtskräftige Entscheidungen mitzuteilen, wenn Grund zu der Annahme besteht, dass Tatsachen, die den Gegenstand des Verfahrens betreffen und auf eine Verletzung von Pflichten schließen lassen, die bei der Ausübung des Berufs oder des Gewerbes zu beachten oder in anderer Weise geeignet sind, Zweifel an der Eignung, Zuverlässigkeit oder Befähigung hervorzurufen, den Widerruf, die Rücknahme oder die Einschränkung einer behördlichen Erlaubnis, Genehmigung oder Zulassung zur Ausübung eines Gewerbes oder eines Berufs, zum Führen einer Berufsbezeichnung, die Untersagung der gewerblichen Tätigkeit oder der Einstellung, Beschäftigung oder Beaufsichtigung von Kindern und Jugendlichen zur Folge haben können. Die Mitteilungen sind nach Nr. 39 Abs. 5 MiStra an die Behörde zu richten, die die Berechtigung erteilt hat oder für die Untersagung der Berufs- oder Gewerbeausübung zuständig ist.

Vor diesem Hintergrund stand eine Beschwerde, die ein betroffener Gewerbetreibender bei mir erhob. Der Beschwerdeführer war Inhaber von Erlaubnissen nach § 34c Gewerbeordnung (GewO). Gegen ihn hatte die Staatsanwaltschaft beim Amtsgericht einen Strafbefehl wegen Urkundenfälschung beantragt. Dem lag die Mitwirkung des Beschwerdeführers an der Beschaffung eines falschen Impfnachweises zugrunde. Mit dem Strafbefehlsantrag verfügte die Staatsanwaltschaft auch eine Mitteilung nach Nr. 39 MiStra an das Landratsamt. Das Landratsamt reichte die Mitteilung an die Industrie- und Handelskammer als die für Erlaubnisse nach § 34c GewO zuständige Stelle weiter. Diese wandte sich daraufhin an den Beschwerdeführer und forderte diesen auf, auf die ihm erteilten gewerberechtlichen Erlaubnisse zu verzichten. Da der Beschwerdeführer dem nicht nachkam und seine betreffende Verurteilung bestritt, wandte sich die Industrie- und Handelskammer telefonisch an die Staatsanwaltschaft und erhielt von dort die unzutreffende Auskunft, gegen den Beschwerdeführer sei eine Geldstrafe wegen Urkundenfälschung festgesetzt worden, obwohl zuvor auf gerichtlichen Hinweis hin der Strafbefehlsantrag durch die Staatsanwaltschaft zurückgenommen und das Verfahren schließlich nach § 170 Abs. 2 Strafprozeßordnung eingestellt worden war.

Die Datenschutzrechte des Beschwerdeführers wurden vorliegend gleich mehrfach verletzt, insbesondere da seine Daten unzulässigerweise übermittelt wurden: So war die initiale Mitteilung durch die Staatsanwaltschaft bereits mit dem Strafbefehlsantrag und nicht – wie in Nr. 39 Abs. 1 MiStra vorgesehen – nach Vorliegen

einer rechtskräftigen Entscheidung gegen den Beschwerdeführer verfügt worden.

Zudem ging die Mitteilung an das sachlich unzuständige Landratsamt und nicht an die nach Nr. 39 Abs. 5 MiStra in Verbindung mit § 34c GewO und § 37 Abs. 7 Satz 1 Nr. 2 Zuständigkeitsverordnung zuständige Industrie- und Handelskammer.

Die Staatsanwaltschaft bedauerte den Vorgang und ergriff Sensibilisierungsmaßnahmen. Gleichwohl habe ich die Datenschutzverstöße nach Art. 16 Abs. 4 BayDSG förmlich beanstandet.

2.11 Dauer der Speicherung von Kontaktdaten beim Landesjustizprüfungsamt

Im Rahmen meiner Bearbeitung von Beschwerden wurde ich darauf aufmerksam, dass das Landesjustizprüfungsamt die Kontaktdaten von (ehemaligen) Prüfungsteilnehmerinnen und Prüfungsteilnehmern für 20 Jahre nach Abschluss des jeweiligen Prüfungsverfahrens speicherte. Dies galt auch für die E-Mail-Adressen.

Auf meine Anfrage teilte das Landesjustizprüfungsamt mit, dass erfahrungsgemäß auch noch viele Jahre nach Abschluss des Prüfungsverfahrens von Prüflingen Anfragen und Anträge – zum Beispiel auf Ausstellung von Zeugniszweitschriften – gestellt würden, zu deren Bearbeitung man die Kontaktdaten noch benötige. Nach 20 Jahren würden sie dann aber gelöscht und nur noch sogenannte Restdaten (insbesondere der Namen der Prüflinge sowie Prüfungsdaten) gespeichert. Diese Restdaten würden dauerhaft aufbewahrt, da dies für die Erledigung der dem Landesjustizprüfungsamt als zeugnisausstellender Behörde obliegenden Aufgaben notwendig sei. Denn auch nach Ablauf von 20 Jahren bestehe noch das Bedürfnis, etwa beim Verdacht einer Zeugnisfälschung, feststellen zu können, ob und in welchem Termin Prüflinge vor dem Landesjustizprüfungsamt eine Prüfung abgelegt und welches Ergebnis sie dabei erzielt hätten.

In meiner Prüfung kam ich zu dem Ergebnis, dass die Speicherung der genannten Daten durch das Landesjustizprüfungsamt im Grundsatz nach Art. 4 Abs. 1 BayDSG zulässig ist, da sie zur Erfüllung der Aufgaben des Landesjustizprüfungsamtes erforderlich ist.

Für eine Speicherung von Kontaktdaten nach Abschluss des Prüfungsverfahrens über den langen Zeitraum von 20 Jahren sah ich jedoch keine Erforderlichkeit., insbesondere da zu erwarten sei, dass Kontaktdaten viele Jahre nach dem Prüfungsverfahren nicht mehr mit den beim Landesjustizprüfungsamt gespeicherten Daten übereinstimmen.

Das Landesjustizprüfungsamt antwortete mir, dass eine Löschung der Kontaktdaten unmittelbar nach Abschluss des jeweiligen Prüfungsverfahrens nicht sachgerecht sei, da sich unter anderem bei einem erheblichen Teil der Prüflinge eine weitere Prüfung anschließe, etwa zum Zweck der Notenverbesserung. Würden die Kontaktdaten bereits unmittelbar nach dem ersten Prüfungsversuch gelöscht, müssten sie dann erneut erhoben und in die EDV eingepflegt werden. Allerdings beabsichtige man, die Kontaktdaten künftig einheitlich bereits fünf Jahre nach der (letzten) Prüfungsteilnahme zu löschen.

Ich teilte dem Landesjustizprüfungsamtes daraufhin mit, dass ich die Verkürzung der Speicherfristen für Kontaktdaten begrüße und eine fünfjährige Aufbewahrung dieser für vertretbar halte.

2.12 Kommunikation mittels nicht ausreichend verschlüsselter E-Mail

Aufgrund einer Beschwerde wurde ich darauf aufmerksam, dass eine Gerichtsverwaltung mit einem Rechtsanwalt mittels nicht ausreichend verschlüsselter E-Mail kommuniziert hatte. In diesem Zusammenhang waren personenbezogene Daten des Rechtsanwalts in der E-Mail selbst sowie in den dort beigefügten Anhängen enthalten. Im Rahmen meiner datenschutzrechtlichen Prüfung stellte sich zusätzlich heraus, dass die Anhänge inhaltlich für die Kommunikation nicht zwingend erforderlich waren.

Ich musste daher Verstöße gegen den Grundsatz der Integrität und Vertraulichkeit der Datenverarbeitung gemäß Art. 5 Abs. 1 Buchst. f DSGVO einerseits sowie gegen den Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 Buchst. c DSGVO andererseits feststellen.

Des Weiteren wies ich die betroffene Gerichtsverwaltung darauf hin, künftig die ressorteigenen Vorgaben zur Kommunikation mittels E-Mail zu beachten und die Mitarbeiter entsprechend zu sensibilisieren. Gerade bei der Kommunikation mit Rechtsanwälten existieren mit dem Besonderen elektronischen Behördenpostfach (BeBPo, vgl. § 6 Abs. 1, 2 Elektronischer-Rechtsverkehr-Verordnung – ERVV) und dem Elektronischen Gerichts- und Verwaltungsportal (EGVP, vgl. § 6 Abs. 3 ERVV) einerseits sowie dem Besonderen elektronischen Anwaltspostfach andererseits (BeA, vgl. § 31a BRAO) technische und organisatorische Maßnahmen, die gemäß Art. 32 Abs. 1 DSGVO unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignet sind, ein angemessenes Schutzniveau bei der Kommunikation zu gewährleisten.

2.13 Prüfung der Info- und Hinweistelefone beim Bayerischen Landesamt für Verfassungsschutz

Das Bayerische Landesamt für Verfassungsschutz bietet vor dem Hintergrund seiner gesetzlichen Aufgabenstellung mehrere Info- und Hinweistelefone an, darunter ein Aussteigertelefon Rechtsextremismus, ein Hinweistelefon Scientology, ein Hinweistelefon für Verdachtsfälle und Salafismus-Prävention, ein Hinweis- und Beratungstelefon Wirtschaftsschutz und Cyber-Allianz-Zentrum sowie das Bürgertelefon Bayerische Informationsstelle gegen Extremismus.

Im Berichtszeitraum habe ich den Betrieb dieser Info- und Hinweistelefone überprüft. Dafür habe ich vom Landesamt Informationen unter anderem zum jeweiligen Hinweisaufkommen erbeten sowie erfragt, ob die Info-/Hinweistelefone in entsprechende Konzeptionen eingebettet sind, ob eine Rufnummernanzeige auch bei unterdrückter Anruferkennung erfolgt, schließlich, welche Datenverarbeitungen sich im Nachgang zu einem Anruf ergeben können.

Da die entsprechenden Antworten des Landesamts als Verschlusssache eingestuft, mithin geheim sind, kann ich nur berichten, dass ich eine transparente und schlüssige Rückmeldung erhalten habe, die meine Fragen beantwortete.

Insgesamt kam ich zu dem Ergebnis, dass mögliche Datenverarbeitungen im Rahmen des Betriebs der Info- und Hinweistelefone in einem datenschutzrechtlich vertretbaren Rahmen liegen, weshalb von mir nichts weiter zu veranlassen war.

3 Allgemeine Innere Verwaltung

3.1 Kommunale Willensbildung in Livestream und Mediathek

Die mit der Kommunalrechtsnovelle 2023 (dazu bereits mein 33. Tätigkeitsbericht 2023) neu eingeführten Vorschriften sind mittlerweile in der Praxis „angekommen". Um den Kommunen konkrete Hilfestellungen für eine datenschutzgerechte Anwendung zu geben habe ich eine Aktuelle Kurz-Information[22] veröffentlicht, die sich mit den neuen Gestaltungsmöglichkeiten bei der Übertragung von Gemeinderatssitzungen und Bürgerversammlungen sowie dem Vorhalten einer Mediathek befasst. Das Papier zeigt in Frage und Antwort zum einen die datenschutzrechtlichen Rahmenbedingungen auf, geht zum anderen aber auch auf Fehlerquellen und Maßnahmen zu deren Vermeidung ein.

3.1.1 Bürgerversammlung: Livestream

Mit dem neuen Art. 18 Abs. 4 Gemeindeordnung (GO) ist den Gemeinden zum einen die Möglichkeit eröffnet, Bürgerversammlungen live im Internet zu übertragen (Sätze 2 bis 5); zum anderen können sie Bürgerversammlungen für eine Teilnahme über das Internet öffnen, mithin in einer hybriden Form abhalten (Sätze 6 bis 7).

Bevor eine Bürgerversammlung gestreamt werden darf, muss die Gemeinde die Live-Übertragung durch Satzung oder durch Beschluss des Gemeinderats zulassen (Art. 18 Abs. 4 Satz 2 GO). Auch dann darf ein Redebeitrag aber nur gestreamt werden, wenn die sprechende Person dafür eine **Einwilligung** erteilt hat (Art. 18 Abs. 4 Satz 3 GO); die Versammlungsleitung ist davon ausgenommen. Kameras dürfen nur die Versammlungsleitung und – falls sie eingewilligt haben – die sprechenden Personen erfassen (Art. 18 Abs. 4 Satz 4 GO). Übersichtsaufnahmen sind nicht zulässig; das bedeutet praktisch, dass der Saal bis auf das Rednerpult und den Platz der Versammlungsleitung grundsätzlich „kamerafrei" bleiben muss. Über die geplante Live-Übertragung muss frühzeitig informiert werden, und zwar mit der Einladung zur Bürgerversammlung sowie (nochmals) vor ihrem Beginn (Art. 18 Abs. 4 Satz 5 GO). Speziell für die sich in der Praxis oftmals stellende Frage, ob und gegebenenfalls wie die danach notwendigen **Einwilligungen auch schlüssig erteilt oder verweigert werden können** und wie damit umzugehen ist, wenn die oder der Sprechende Daten „loslässt", die unter das Verarbeitungsverbot des Art. 9 DSGVO fallen, habe ich den Kommunen detaillierte Hinweise gegeben. So habe ich etwa darauf hingewiesen, dass eine örtliche Regelung zulässig ist, die eine Möglichkeit schlüssiger Einwilligung in eine Echtzeitübertragung durch Nutzung des Rednerpultes eröffnet.

[22] Bayerischer Landesbeauftragter für den Datenschutz, Kommunale Willensbildung in Livestream und Mediathek, Aktuelle Kurz-Information 54, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

Aufmerksam gemacht habe ich auch darauf, dass die Übertragung von Abstimmungen, das „Auflockern" des Livestreams durch Übersichtsaufnahmen vom Veranstaltungsort und die Speicherung der Aufnahmen in einer Mediathek unzulässig sind.

3.1.2 Selbstverwaltungsgremien: Livestream und Mediathek

Neu geschaffen hat der Gesetzgeber zudem die Möglichkeit, öffentliche Gremiensitzungen live im Internet zu übertragen und die Aufzeichnung für eine bestimmte Zeit in einer Mediathek zu speichern. Die Vorgaben zu Livestream und Mediathek hat der bayerische Gesetzgeber für den Gemeinderat in Art. 52 Abs. 4 GO, für den Kreistag in Art. 46 Abs. 4 Landkreisordnung (LKrO) und für den Bezirkstag in Art. 43 Abs. 4 Bezirksordnung (BezO) vergleichbar geregelt. Davon zu unterscheiden ist die Teilnahme von Gremienmitgliedern in Bild und Ton; diese Option der hybriden Sitzung gibt es bereits seit 2021 (vgl. Art. 47a GO, Art. 41a LKrO und Art. 38a BezO sowie – für die Verbandsversammlungen von Zweckverbänden – Art. 33a Gesetz über die kommunale Zusammenarbeit).

Will eine Kommune von den neu geschaffenen Möglichkeiten Gebrauch machen, ist vorab ein **Beschluss des zuständigen Gremiums** erforderlich. So muss etwa in Gemeinden der Gemeinderat entscheiden, wobei ein qualifiziertes Mehrheitserfordernis zu beachten ist (Art. 52 Abs. 4 Satz 5 GO). Aber auch dann dürfen an den Gremiensitzungen teilnehmende Personen – mit Ausnahme der oder des Vorsitzenden – grundsätzlich nur dann von einer Aufzeichnung und Speicherung erfasst werden, wenn sie **eingewilligt** haben (Art. 52 Abs. 4 Satz 6 GO). Unbeteiligte – insbesondere Bürgerinnen und Bürger im Auditorium – dürfen allenfalls im Rahmen von Übersichts- oder Hintergrundaufnahmen „festgehalten" werden, wobei solche Aufnahmen dann keine Identifizierung ermöglichen dürfen. Daher muss die Gemeinde, bevor es „losgehen kann", von den an einer Sitzung regelmäßig aktiv teilnehmenden Personen (insbesondere Gemeinderatsmitgliedern, Ortssprechern, Sitzungsdienst leistenden Beschäftigten der Gemeinde) generelle oder – bei nur vereinzelter Teilnahme – sitzungsbezogene Einwilligungen einholen. Da die Einwilligung freiwillig ist, muss die Gemeinde in der Lage sein, auf verweigerte aber auch auf widerrufene Einwilligungen durch Unterbrechung des Livestreams oder dessen Nachbearbeitung zu reagieren. Auch bei Einhaltung dieser Voraussetzungen ist die Übertragung von Abstimmungen nicht zulässig.

Im Hinblick auf die Speicherung in einer Mediathek ist die zulässige Speicherdauer (sechs Wochen, oder falls die nächste Sitzung nicht innerhalb von sechs Wochen stattfindet, bis zum Ende der nächsten Sitzung) zu beachten.

3.2 Bekanntgabe von Spenden in öffentlicher Gemeinderatssitzung: Datenschutzrechtliche Abwägung im Einzelfall erforderlich

Manche Bürgerinnen und Bürger möchten die Verbundenheit mit ihrer Gemeinde auch durch finanzielle Zuwendungen zum Ausdruck bringen. Ein solches Engagement dient dem Gemeinwohl – wenn kein „Entgegenkommen" bei eigenen Anliegen erwartet wird. Um an dieser Stelle gar nicht erst einen „falschen Eindruck" entstehen zu lassen, möchten Gemeinden nachvollziehbarerweise auf Transparenz setzen – mit einer Bekanntgabe von Spenden in öffentlicher Gemeinderatssitzung.

Mitunter haben Spenderinnen und Spender aber gerade daran kein Interesse, aus Bescheidenheit oder weil sie ihre Finanzkraft nicht öffentlich machen wollen. Einer Kommune, die sich mit der Bitte um Beratung an mich gewandt hat, habe ich in Abstimmung mit dem Bayerischen Staatsministerium des Innern, für Sport und Integration folgende Hinweise gegeben:

3.2.1 Verarbeitung personenbezogener Daten

Die Spendernamen sowie Art und Höhe der jeweiligen Spende sind bei natürlichen Personen von Art. 4 Nr. 1 DSGVO erfasste Daten. Die Offenlegung stellt eine Verarbeitung dar, die einer Rechtsgrundlage bedarf (Art. 6 Abs. 1 UAbs. 1 DSGVO). In Betracht kommt eine Befugnis im Sinne von Art. 6 Abs. 1 UAbs. 1 Buchst. e, UAbs. 3 Buchst. b DSGVO, in Verbindung mit Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG. Maßgeblich ist insoweit die Frage, ob die Datenverarbeitung zur Erfüllung gemeindlicher Aufgaben erforderlich ist.

3.2.2 Entgegennahme von Spenden: Aufgabe gerade auch des Gemeinderats

Spenden zur eigenen (steuerbegünstigten) Verwendung wird die Gemeinde grundsätzlich annehmen, wenn der Spenderzweck mit der gemeindlichen Planung in Einklang steht und keine unwirtschaftlichen Entscheidungen ausgelöst werden,[23] so dass im Außenverhältnis (gerade auch zur spendenden Person) eine gemeindliche Aufgabe grundsätzlich vorliegt.

Gemeindeintern ist die Entgegennahme von Spenden grundsätzlich eine laufende Angelegenheit im Sinne von Art. 37 Abs. 1 Nr. 1 Gemeindeordnung (GO), für die als Organ die oder der Erste Bürgermeisterin oder Erste Bürgermeister zuständig ist.[24] Auch eine Übertragung auf weitere Bürgermeisterinnen und Bürgermeister, sowie auf Gemeinderatsmitglieder beziehungsweise Gemeindebedienstete ist im Rahmen des Art. 39 Abs. 2 GO grundsätzlich möglich.[25]

Neben der gerade erläuterten, primär kommunal- und steuerrechtlich motivierten korrekten „Verbuchung“ der Spende, ist jedoch auch zu bedenken, dass die Kontrolle der Verwaltung wiederum die Aufgabe des Gemeinderats, also der Vertretungskörperschaft (vgl. Art. 30 Abs. 3 GO) ist. Um diesen möglichst frühzeitig in den Prozess der Spendenannahme einzubinden, wird gerade auch aus Gründen der Transparenz in einer gemeinsamen Handlungsempfehlung des Bayerischen Staatsministerium des Innern, für Sport und Integration, des Bayerischen Staatsministeriums der Justiz und der kommunalen Spitzenverbände[26] nahe gelegt, dass Zuwendungen nicht (sofort) durch den ersten Bürgermeister selbst, sondern erst nach einer entsprechenden Entscheidung des Gemeinderats oder eines Ausschusses an- und entgegengenommen werden.

[23] Vgl. Nr. 6 Bekanntmachung des Bayerischen Staatsministeriums des Innern über die Entgegennahme und Verwendung von Spenden und sonstigen Zuwendungen durch Kommunen vom 2. August 2000 (AIIMBl. S. 571), zuletzt geändert durch Bekanntmachung vom 14. Mai 2009 (AIIMBl. S. 175).

[24] Vgl. Wernsmann/Kriegl in: Dietlein/Suerbaum, Beck'scher Online-Kommentar Kommunalrecht Bayern, Stand 2/2024, Art. 37 GO Rn. 8.

[25] Vgl. Nr. 3.3.3 Bekanntmachung (Fn. 23).

[26] Dokumentiert in BayGT 2009, S. 39 (40), Internet: https://www.bay-gemeindetag.de, Rubrik „Verbandszeitschrift“.

3.2.3 Bekanntgabe in öffentlicher Gemeinderatssitzung erfordert Abwägung zwischen öffentlichem Transparenzinteresse und den berechtigten Interessen Einzelner

Mit der Einbindung des Gemeinderats in den Prozess der Spendenannahme ist jedoch noch nicht die Frage beantwortet, ob und inwieweit die Gemeindeöffentlichkeit – insbesondere in öffentlicher Gemeinderatssitzung – etwa den Namen der Spenderin oder des Spenders erfährt.

Die mich um Beratung ersuchende Gemeinde hatte sich unter Heranziehung der Handlungsempfehlung insoweit entschieden, bei der Beratung in öffentlicher Sitzung generell die personenbezogenen Daten der Spender zu schwärzen und diese auch nicht in sonstiger Weise der Öffentlichkeit bekanntzugeben. Diese Praxis wurde aber von einem Gemeindebürger als intransparent gerügt und darauf hingewiesen, dass in anderen Bundesländern die dortigen Datenschutz-Aufsichtsbehörden gegen eine generelle Bekanntgabe insbesondere von Namen und Wohnort der Spender sowie Spendenhöhe, aber auch von sonstigen Begleitumständen in öffentlicher Gemeinderatssitzung regelmäßig keine Einwände erheben.[27]

In Abstimmung mit dem Innenministerium habe ich der Gemeinde folgende Hinweise gegeben:

Die sachgerechte Erfüllung der gemeindlichen Aufgabe – Entgegennahme der Spende – kann im Einzelfall auch eine personenbezogene Information über die Spenderin oder den Spender in öffentlicher Gemeinderatssitzung erforderlich machen.

Grund hierfür ist nicht nur die allgemein mit einer Behandlung in öffentlicher Gemeinderatssitzung gemäß Art. 52 Abs. 2 Satz 1 GO verbundene Kontrollfunktion. Vielmehr lässt die speziell im Bereich der Annahme von Zuwendungen für den staatlichen Bereich in Nr. 8.1 Satz 1 Sponsoringrichtlinie geregelte öffentliche Berichtspflicht erkennen, dass die Herstellung von Transparenz bereits Bestandteil der eigentlichen Aufgabenwahrnehmung sein kann, wenn Zuwendungen entgegengenommen werden, auf die kein Rechtsanspruch besteht. Dieser Rechtsgedanke trifft auch auf den Bereich der Kommunen zu, wenngleich die Sponsoringrichtlinie dort nicht verbindlich ist.

Da sich die bayerischen Kommunen jedoch vielfältig hinsichtlich Größe und Leistungsfähigkeit – und damit auch hinsichtlich der realistischen Möglichkeit einer unzulässigen Beeinflussung durch Spenden – unterscheiden, empfehle ich auch keine schematische Orientierung an der in der Sponsoringrichtlinie enthaltenen Wertgrenze. Vielmehr ist im Rahmen des Art. 52 Abs. 2 Satz 1 GO eine **einzelfallbezogene Abwägung zwischen dem Transparenzinteresse der Öffentlichkeit und den berechtigten Interessen Einzelner** unter Berücksichtigung der konkreten Umstände und Verhältnisse der jeweiligen Gemeinde erforderlich.

„Die Sitzungen sind öffentlich, soweit nicht Rücksichten auf das Wohl der Allgemeinheit oder auf berechtigte Ansprüche einzelner entgegenstehen."

[27] Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, 31. Tätigkeitsbericht 2022, Nr. 11.1.2.

Bei Gewichtung des öffentlichen Transparenzinteresses wird man neben der bereits genannten **Größe und Leistungsfähigkeit der Gemeinde** in Relation zu **Art und Höhe der Spende** auch deren eventuelle **Zweckgebundenheit** berücksichtigen müssen. Berechtigte Interessen Einzelner sind dagegen rechtlich geschützte oder sonstige schutzwürdige (private) Interessen natürlicher oder juristischer Personen. Sie erfordern den Ausschluss der Öffentlichkeit in der Gemeinderatssitzung, wenn im Verlauf einer öffentlichen Sitzung **persönliche oder wirtschaftliche Verhältnisse** zur Sprache kommen könnten, **an deren Kenntnis schlechthin kein berechtigtes Interesse der Allgemeinheit bestehen kann und deren Bekanntgabe dem Einzelnen nachteilig sein könnte.** Je nach Art und Höhe der Spende können durchaus Rückschlüsse auf die wirtschaftlichen und finanziellen Verhältnisse von Spendern möglich sein. Bei gleichwohl überwiegendem Transparenzinteresse können dennoch im Einzelfall die gesetzlichen Voraussetzungen für eine Behandlung in öffentlicher Sitzung vorliegen.

Soll die **Niederschrift zusätzlich im Internet**, etwa auf der Homepage der Kommune, veröffentlicht werden, ist zu berücksichtigen, dass die Informationen im Internet weltweit und oftmals dauerhaft abgerufen und ausgewertet werden können. Vor diesem Hintergrund halte ich in Übereinstimmung mit dem Innenministerium eine Veröffentlichung von Sitzungsniederschriften mit personenbezogenen Daten, die über den Mindestinhalt des Art. 54 Abs. 1 Satz 2 und Satz 3 GO hinausgehen, auf der Homepage der Kommune für datenschutzrechtlich unzulässig. Daher sind aus datenschutzrechtlicher Sicht jedenfalls bei einer Internetveröffentlichung grundsätzlich die **Namen der Spender wegzulassen oder zu anonymisieren.**

3.3 Datenschutzkonformes Management von Bürgeranliegen: Mängelmelder bei bayerischen Kommunen

Kommunale Mängelmelder sind eine Form des sogenannten Anliegen-Managements. Gemeinden bieten etwa im Rahmen der eigenen Internetpräsenz Online-Formulare, mit denen Bürgerinnen und Bürger insbesondere Defizite im Bereich der öffentlichen Infrastruktur (etwa Straßenschäden, defekte Laternen oder illegale Müllablagerungen) melden können. Solche Mängelmelder sind ein niedrigschwelliges Angebot für eine Kontaktaufnahme mit der Kommune, die dann „Schwachstellen“ effektiv beheben kann. Mittlerweile verfügen rund zehn Prozent der bayerischen Kommunen über solche Angebote. Mängelmelder sind grundsätzlich datenschutzkonform betreibbar, wenn einige Punkte Beachtung finden.

3.3.1 Personenbezogene Daten in veröffentlichten Mängelmeldungen

Werden die Mängelmeldungen auf der Internetpräsenz der Gemeinde bereitgestellt, können im Einzelfall personenbezogene Daten offengelegt werden. Das gilt insbesondere dann, wenn die Möglichkeit besteht, mit der Mängelmeldung auch Fotos hochzuladen. Zwar kann die Meldung einer schadhaften Gehwegplatte – auch bei fotografischer Dokumentation – ohne personenbezogene Daten auskommen. Geht es um einen „Dauerfalschparker“ ist bei Erkennbarkeit des Kennzeichens die Grenze ins Datenschutzrecht aber bereits überschritten. Gleiches gilt bei Missständen an einem konkreten Privatgrundstück und erst recht, wenn eine Mitbürgerin oder ein Mitbürger als Störerin oder Störer namhaft gemacht wird. Dann braucht die Gemeinde für die „Präsentation“ auf der Homepage eine Rechtsgrundlage.

Daran fehlt es aber in aller Regel. Zwar kommen für die Kommunen grundsätzlich die allgemeinen Verarbeitungsbefugnisse nach Art. 4 und 5 BayDSG in Betracht. Auch stellt die Bereitstellung eines Mängelmelders im Grundsatz wohl eine öffentliche Aufgabe der Kommune dar. Für die Bearbeitung der Mängel oder auch die Mitteilung des Bearbeitungsstatus an die meldenden Bürgerinnen und Bürger ist es jedoch grundsätzlich nicht erforderlich, dass die Kommune die Mängelmeldung – und mit ihr personenbezogene Daten – weltweit veröffentlicht. Ein Mängelmelder darf sich nicht faktisch als „digitaler Pranger" darstellen.

3.3.2 Datenschutzkonforme Ausgestaltung eines Mängelmelders

Der datenschutzkonforme Betrieb von Mängelmeldern ist gleichwohl möglich. Ich habe dazu insbesondere folgende Hinweise gegeben, die das Bayerische Staatsministerium des Innern, für Sport und Integration erfreulicherweise allen Kommunen zur Kenntnis gebracht hat:

Die Gemeinden müssen durch technische und organisatorische Maßnahmen **sicherstellen, dass keine personenbezogenen Daten veröffentlicht** werden. Hier sind unterschiedliche Lösungen denkbar. In Betracht kommt eine Einschränkung der Arten „meldbarer" Mängel, (etwa ein Ausschluss von individuell vorwerfbaren Missständen wie Ordnungswidrigkeiten), ferner ein Hinweis, dass die Meldung möglichst keine personenbezogenen Daten enthalten soll. Sollen die Meldungen veröffentlicht werden, ist weiterhin sicherzustellen, dass auch tatsächlich keine personenbezogenen Daten erfasst sind. Mängelmeldungen sollten deshalb nicht automatisiert veröffentlicht, sondern vorab durch Beschäftigte der Kommune daraufhin überprüft werden, ob sie personenbezogene Daten enthalten. Diese Daten sind dann vor der Veröffentlichung zu löschen oder unkenntlich zu machen.

Betreibt die **Kommune** den Mängelmelder selbst, ist sie in datenschutzrechtlicher Hinsicht für die Zulässigkeit der Verarbeitung personenbezogener Daten **verantwortlich**. Daran ändert sich aber auch dann nichts, wenn die Kommune hierfür einen Dienstleister einschaltet. Der Dienstleister wird dann regelmäßig als Auftragsverarbeiter tätig, sodass ein schriftlicher Auftragsverarbeitungsvertrag zu schließen ist. Hilfestellungen dazu bietet meine einschlägige Orientierungshilfe.[28]

Auch wenn die Meldungen nicht veröffentlicht werden, gelten für die Mängelmelder bei der Verarbeitung personenbezogener Daten die einschlägigen datenschutzrechtlichen Bestimmungen. Dies bedeutet unter auch, dass die meldenden Personen in einer **Datenschutzerklärung** (Art. 13, 14 DSGVO) insbesondere darüber in Kenntnis gesetzt werden müssen, ob und welche Daten von ihnen gegebenenfalls verarbeitet werden sowie welche Rechte ihnen zustehen. Ausführliche Informationen zu diesem Thema finden sich in meiner Orientierungshilfe zu diesem Thema.[29] Ferner ist als Maßnahme nach Art. 32 DSGVO ein **Löschkon-**

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

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

zept zu erarbeiten, welches festlegt, wann die Daten wieder zu löschen sind. Zudem muss durch technische und organisatorische Maßnahmen die angemessene **Sicherheit** der personenbezogenen Daten sichergestellt sein.

3.4 Aufgepasst bei schnellen Auskünften am Telefon: besser Rückruf anbieten

Bereits in meinem 25. Tätigkeitsbericht 2012 unter Nr. 9.7 habe ich auf die Problematik telefonischer Auskünfte – speziell in steuerlichen Angelegenheiten – aufmerksam gemacht und generell zur Zurückhaltung geraten. Auch in einem abfallrechtlichen Sachverhalt kann sich dieses Problem stellen, wie beispielhaft die Beschwerde eines betroffenen Bürgers zeigte. Diesmal hatte ein Mitarbeiter eines Landratsamtes am Telefon etwas vorschnell gegenüber einer – zwar in einem Verwandtschaftsverhältnis zu den übrigen datenschutzrechtlich Betroffenen stehenden, aber dennoch – dritten Person die geänderten Eigentumsverhältnisse bezüglich eines Hausgrundstücks offengelegt.

Konkret hatte eine Tante des Beschwerdeführers wegen einer Frage zur Müllentsorgung vom Hausgrundstück ihrer Eltern – den Großeltern des Beschwerdeführers – beim Landratsamt angerufen. In dem Telefonat machte sie der Behördenmitarbeiter darauf aufmerksam, dass die Grundstückseigentümer die Immobilie kürzlich an den Beschwerdeführer übereignet hätten. Dieses Geschäft war der Anruferin allerdings nicht bekannt und sollte vor ihr wohl auch erst einmal geheim gehalten werden. Die telefonische Auskunftserteilung machte den „Deal“ nun verwandtschaftsöffentlich, was zu einem erheblichen Konflikt führte und die bei mir eingereichte Beschwerde des neuen Hauseigentümers veranlasst hat.

3.4.1 Unbefugte Datenverarbeitung durch das Landratsamt

Die Kenntnis über die geänderten Eigentumsverhältnisse am Hausgrundstück ist ein personenbezogenes Datum. Dieses wurde durch die seitens eines Mitarbeiters des Landratsamtes im Zusammenhang mit dessen (abfallrechtlicher) Amtsführung erfolgte Offenlegung auch amtlicherseits verarbeitet, konkret: an die Tante des Beschwerdeführers übermittelt. Eine Rechtsgrundlage für diese Verarbeitung war jedoch weder speziell im Abfallrecht noch im allgemeinen Datenschutzrecht vorhanden. Es war schlichtweg nicht zur abfallrechtlichen Aufgabenerfüllung erforderlich, die Tante des Beschwerdeführers von der erfolgten Eigentumsübertragung in Kenntnis zu setzen. Die hierdurch gewonnene Kenntnis hätte die „Begünstigte der Datenübermittlung“ auch nicht etwa aus dem Liegenschaftskataster gewinnen können, da es hierfür des (nicht ersichtlichen) Vortrags eines berechtigten Interesses an der Kenntnis des personenbezogenen Datums gemäß Art. 11 Abs. 1 Satz 3 Vermessungs- und Katastergesetz bedurft hätte (ebenso die grundbuchrechtliche Wertung; vgl. dazu näher sogleich). Das Verhalten des Behördenmitarbeiters wird dem Landratsamt auch zugerechnet. Öffentliche Stellen müssen sich auch ein vorwerfbares (fahrlässiges) Verhalten ihrer Mitarbeiter/Amtsträger nämlich grundsätzlich zurechnen lassen. Auch sind datenschutzwidrig handelnde Mitarbeiter/Amtsträger öffentlicher Stellen trotz deren Adressierung in Art. 11 Satz 1 BayDSG keine eigenständigen öffentlichen Stellen, sondern nur unselbständiger Teil der sie beschäftigenden öffentlichen Stelle selbst. Die Zurechnung zur öffentlichen Stelle erfolgt insbesondere, dann wenn – wie vorliegend – bei der in Rede stehenden Datenverarbeitung offensichtlich ein räumlicher, zeitlicher oder funktionaler Zusammenhang zur Tätigkeit als Beschäftigter beziehungsweise als Amtsträger besteht.

3.4.2 Beanstandung des Datenschutzverstoßes

Die Entscheidung, ob ich einen Datenschutzverstoß formell beanstande, treffe ich im Rahmen pflichtgemäßen Ermessens (Art. 16 Abs. 4 Satz 1 BayDSG). Zwar war dem Behördenmitarbeiter im Moment des Telefonats wohl gar nicht bewusst, dass gerade unberechtigt Daten offenlegt werden. Auch konnte die familiäre Gesamtkonstellation auf Seiten der Anruferin in diesem Moment wohl kaum (vollständig) überblickt werden. Gleichwohl hätte der Behördenmitarbeiter leicht erkennen können, dass eine weibliche Anruferin nicht der neue (männliche) Eigentümer des Grundstücks sein kann. Zu berücksichtigen waren auch die erheblichen negativen Auswirkungen auf die Familie des Beschwerdeführers. Die Tante hätte die geänderten Eigentumsverhältnisse auf dem dafür gesetzlich vorgesehenen Weg wohl nicht in Erfahrung bringen können. Die dafür primär in Betracht kommende Einsicht in das beim Grundbuchamt geführte Grundbuch erfordert nach § 12 Abs. 1 Satz 1 Grundbuchordnung nämlich die Darlegung eines berechtigten Interesses. Zukünftige Ansprüche, Sicherungsbedürfnisse, Erwartungen und Entwicklungen können ein solches jedoch gerade nicht begründen, da sie im hypothetischen Bereich liegen und völlig ungewiss sind.[30] Die Tante ging vorliegend (gegebenenfalls) davon aus, dass sie im Rahmen der gesetzlichen Erbfolge hinsichtlich der Hausgrundstücks ihrer Eltern bei deren Todesfall als Erbin berechtigt sein würde. Diese Erwartung hätte eine Einsicht in das Grundbuch jedoch nicht ermöglicht. Ich habe daher eine Beanstandung ausgesprochen.

3.4.3 Fazit

Mitarbeiterinnen und Mitarbeiter bayerischer öffentlicher Stellen sollten sich stets bewusst sein, dass (vor)schnelle Auskünfte am Telefon im Einzelfall gravierende Auswirkungen für die Betroffenen haben können. Auch „mittelbare“ Auskünfte, wie zum Beispiel „Die Abfallgebühren tragen ja nicht mehr …, sondern diese trägt seit dem 1. Mai …“ ermöglichen dem Gesprächspartner gegebenenfalls **Rückschlüsse auf sensible Informationen**, wie zum Beispiel geänderte Eigentumsverhältnisse. Im Zweifel daher besser bei Unklarheit über die Berechtigung des Auskunftbegehrenden einen Rückruf anbieten und den Vorgang vor der Auskunft nochmals daraufhin reflektieren, ob und welche Auskünfte datenschutzrechtlich erforderlich sind und daher auch datenschutzgerecht erteilt werden dürfen!

3.5 Unzulässige Auskunft aus Melderegister an politische Parteien vor Wahlen: Widerspruch aufgrund fehlerhafter Technikgestaltung missachtet

Vor Wahlen erreichen mich stets vermehrt Anfragen von Bürgerinnen und Bürgern, die Auskünfte aus dem Melderegister an politische Parteien betreffen. Daher habe ich bereits in einer Aktuellen Kurz-Information[31] vertiefte Hinweise zu diesem Thema gegeben. Kurz gesagt ist eine Auskunft aus dem Melderegister an politische Parteien zum Zweck der Wahlwerbung nach Maßgabe der einschlägigen fachgesetzlichen Befugnis des § 50 Abs. 5 Bundesmeldegesetz (BMG) im Grund-

[30] Wilsch in: Hügel, Beck'scher Online-Kommentar Grundbuchordnung, Stand 3/2024, § 12 Rn. 91.

[31] Bayerischer Landesbeauftragte für den Datenschutz, Auskunft aus dem Melderegister an politische Parteien vor Wahlen, Stand 1/2025, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek“.

satz zulässig. Bürgerinnen und Bürger haben es aber in der Hand, durch vorherigen Widerspruch bei der Meldebehörde eine Auskunft aus dem Melderegister zu verhindern.

In einer bayerischen Gemeinde wurden jedoch auf Grund eines Versehens in Kombination mit einer „datenschutzunfreundlichen" technischen Voreinstellung der eingesetzten IT-Anwendung bereits erhobene Widersprüche nicht beachtet. Dies hat dazu geführt, dass mehrere hundert Datensätze unzulässigerweise trotz solcher Widersprüche an eine politische Partei übermittelt wurden. Den so bewirkten Datenschutzverstoß habe ich beanstandet. Ich nehme den Vorgang zum Anlass, nochmals auf Folgendes hinzuweisen:

3.5.1 Melderegisterauskunft zu Zwecken der Wahlwerbung grundsätzlich zulässig

Nach § 50 Abs. 1 Satz 1 BMG darf die Meldebehörde Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit Wahlen und Abstimmungen auf staatlicher und kommunaler Ebene in den sechs der Wahl oder Abstimmung vorangehenden Monaten Auskunft aus dem Melderegister über die in § 44 Abs. 1 Satz 1 BMG bezeichneten Daten von Gruppen von Wahlberechtigten erteilen, soweit für deren Zusammensetzung das Lebensalter bestimmend ist. Bei den in § 44 Abs. 1 Satz 1 BMG genannten Daten handelt es sich um den Familiennamen, den/die Vornamen, den Doktorgrad und die derzeitigen Anschriften sowie, sofern die Person verstorben ist, diese Tatsache.

Mit dieser Norm möchte der Gesetzgeber Parteien, Wählergruppen und Trägern von Wahlvorschlägen eine altersspezifische Wahlwerbung ermöglichen und damit die Teilnahme an Wahlen fördern. Die genannten Auskunftsberechtigten sollen Angehörige der von ihnen ausgewählten Gruppen von Wahlberechtigten individuell ansprechen können. Der Empfänger der Daten darf die erhaltenen Daten gemäß § 50 Abs. 1 Satz 3 BMG nur für die Wahlwerbung verwenden und hat sie spätestens einen Monat nach der Wahl zu löschen. Die Sicherstellung der Einhaltung dieser Löschpflicht obliegt dem Empfänger, insbesondere also der Partei, selbst.

3.5.2 Aber: Widerspruchsmöglichkeit

Da es allerdings auch Bürgerinnen und Bürger gibt, die eine Weitergabe ihrer Meldedaten an nichtstaatliche Stellen ablehnen und von Wahlwerbung verschont bleiben wollen, hat der Gesetzgeber in § 50 Abs. 5 Satz 1 BMG eine **Widerspruchsmöglichkeit** vorgesehen. Der Widerspruch kann schriftlich oder mündlich bei der Meldebehörde eingelegt werden. Er ist nicht von Voraussetzungen abhängig und muss nicht begründet werden. Gemäß § 50 Abs. 5 Satz 1 Halbsatz 2 BMG muss auf das Widerspruchsrecht bei der Anmeldung nach § 17 Abs. 1 BMG sowie einmal jährlich durch ortsübliche Bekanntmachung hingewiesen werden.

Ein solcher Widerspruch löst eine **Übermittlungssperre** aus, die gem. § 50 Abs. 5 Satz 2, § 36 Abs. 2 Satz 2 BMG unentgeltlich im Melderegister einzurichten sowie solange zu speichern und zu beachten ist, bis der Einwohner ausdrücklich durch Erklärung gegenüber der Meldebehörde die Aufhebung beantragt. Die Übermittlungssperre gilt damit unbefristet, bis die betroffene Person den Widerspruch zurücknimmt.

3.5.3 Datenschutz durch Technikgestaltung muss Beachtung des Widerspruchs unterstützen

In dem von mir beurteilten Fall versäumte die Meldebehörde ein „Häkchen“ in einem entsprechenden Menü des Fachverfahrens zu setzen. Mit diesem Häkchen wären Personen, die nach § 50 Abs. 5 Satz 1 BMG widersprochen haben, von der Datenübermittlung an die betreffende Partei ausgeschlossen worden. Diese Unachtsamkeit wurde ganz wesentlich dadurch erleichtert, dass die Gemeinde bereits zuvor gegen den in Art. 25 Abs. 2 DSGVO enthaltenen Grundsatz des Datenschutzes durch datenschutzfreundliche Voreinstellung verstoßen hatte. Dort heißt es:

„Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.“

Das eingesetzte Fachverfahren hätte generell – entweder bereits herstellerseitig oder spätestens bei der Inbetriebnahme durch die Gemeinde – so konfiguriert werden müssen, dass Personen mit eingetragener Übermittlungssperre automatisch von Melderegisterauskünften zum Zweck der Wahlwerbung ausgenommen sind.

Zum Zeitpunkt der fehlerhaften Datenübermittlung war also eine Software im Einsatz, die nicht dem Grundsatz von Privacy by Design and Default entsprach. Die Verpflichtung zum Einsatz datenschutzfreundlicher Technologien und speziell auch zu datenschutzfreundlichen Voreinstellungen trifft den Verantwortlichen schon bei der Beschaffung und Implementierung der Verarbeitungsmittel. Beachtet der Verantwortliche diese Verpflichtung, reduziert er auch das Risiko, dass es später aus Unachtsamkeit zu unnötigen Datenschutzverstößen kommt.

4 Soziales und Gesundheit

4.1 Zulässiger Umfang der Datenerhebung im Sozialverwaltungsverfahren zur Sachverhaltsermittlung

Eine betroffene Person beschwerte sich bei mir über das Anliegen eines Jobcenters, eine Vielzahl personenbezogener Daten bei ihr erheben zu wollen. Ihr Antrag auf Bürgergeld wurde zunächst abgelehnt. Im Rahmen des darauffolgenden Widerspruchsverfahrens forderte das Jobcenter verschiedene Unterlagen von der betroffenen Person an, die aus ihrer Sicht für die Bearbeitung des Widerspruchs nicht erforderlich waren. Diese Unterlagen enthielten eine Vielzahl personenbezogener Daten. So sollten etwa Miet- und Untermietverträge, Bescheide sowie Auszüge verschiedener Konten vorgelegt werden. Die betroffene Person wertete das Verhalten des Jobcenters als schikanös, da aus ihrer Sicht bereits ausreichende Belege vorlagen wie etwa eine Bescheinigung des Vermieters. Andere Unterlagen seien bereits im Ausgangsverfahren eingeführt worden oder für die Ermittlung des relevanten Sachverhalts nicht erforderlich gewesen. Die betroffene Person bat mich um eine datenschutzaufsichtliche Überprüfung des Sachverhalts.

4.1.1 Grundsatz der Datenminimierung

Bei der rechtlichen Bewertung des Sachverhalts stand der Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) im Vordergrund.

Dieser Grundsatz besagt, dass personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen. Er ist dem allgemeinen Verhältnismäßigkeitsgedanken verwandt, wonach Rechtseingriffe zur Zweckerreichung geeignet („erheblich"), erforderlich („auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt") und verhältnismäßig im engeren Sinne („dem Zweck angemessen") sein müssen.

Der Grundsatz der Datenminimierung bezieht sich auf die Zwecke der Verarbeitung und ist mit dem Grundsatz der Zweckbindung gemäß Art. 5 Abs. 1 Buchst. b DSGVO verzahnt, der dem datenschutzrechtlich Verantwortlichen aufgibt, den Verarbeitungszweck eindeutig festzulegen und grundsätzlich beizubehalten. Die Beziehung der Datenminimierung auf den Verarbeitungszweck bedeutet aber auch, dass es keine absolute Einschränkung des Umfangs der Datenverarbeitung gibt; vielmehr folgt diese relativ der jeweiligen Verarbeitungssituation in Bezug auf den festgelegten Verarbeitungszweck. Der Verarbeitungszweck kann auch weit bestimmt werden, was die verantwortliche öffentliche Stelle gleichwohl nicht von der Beachtung (fach-)gesetzlich vorgegebener Zweckrichtungen befreit.

4.1.2 Kriterium der Erforderlichkeit

Das Kriterium der Erforderlichkeit ist – als Ausdruck des Grundsatzes der Datenminimierung[32] – typischerweise in (fach-)gesetzlichen Verarbeitungsbefugnissen enthalten und beschränkt den Umfang der Verarbeitung auf das zur Zweckerreichung erforderliche Maß. Er sorgt insbesondere auf fachgesetzlicher Ebene zur Umsetzung des Grundsatzes der Datenminimierung.

Der Erforderlichkeitsgrundsatz war vorliegend im Rahmen der Verarbeitungsbefugnis aus § 67a Abs. 1 Satz 1 Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X) zu beachten. Demnach ist die Erhebung von Sozialdaten durch die betreffenden Stellen zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe nach diesem Gesetzbuch erforderlich ist. Die Erforderlichkeit wird insoweit durch den Zweck der behördlichen Aufgabenerfüllung definiert und beschränkt.

Die Aufgabe des Jobcenters bestand vorliegend darin, über das Bestehen oder Nichtbestehen eines Bürgergeldanspruchs im Widerspruchsverfahren zu entscheiden. Die Erhebung der betreffenden Sozialdaten musste der Bedarfsermittlung und somit der Berechnung eines etwaigen Bürgergeldanspruchs im Sinne des Zweiten Buchs Sozialgesetzbuch – Bürgergeld, Grundsicherung für Arbeitsuchende – (SGB II) dienen und zur Erfüllung dieser Aufgabe erforderlich sein.

Auf Seiten des Leistungsberechtigten korrespondiert damit eine Mitwirkungspflicht gemäß § 60 Erstes Buch Sozialgesetzbuch – Allgemeiner Teil – (SGB I). Wer Sozialleistungen beantragt oder erhält, hat gemäß § 60 Abs. 1 Satz 1 Nr. 1 SGB I alle Tatsachen anzugeben, die für die Leistung erheblich sind, und auf Verlangen des zuständigen Leistungsträgers der Erteilung der erforderlichen Auskünfte durch Dritte zuzustimmen.

4.1.3 Der Umfang der Erforderlichkeit bei der Sachverhaltsermittlung

Meine datenschutzrechtliche Bewertung nahm in den Blick, welche Tatsachen zur Aufgabenerfüllung des Jobcenters für die Leistungsgewährung erheblich (vgl. § 60 Abs. 1 Satz 1 Nr. 1 SGB I) und daher erforderlich sind. Im Sozialrecht sind dafür die jeweiligen leistungsrechtlichen Anspruchsvoraussetzungen maßgeblich, deren Vorliegen zu ermitteln ist. Das Jobcenter als Leistungsträger muss in die Lage versetzt werden, über das „Ob“ und „Wie“ der Leistung – einschließlich der Bezugsdauer – zu entscheiden.[33] Dabei muss es ihm möglich sein, etwaige Sachverhaltslücken oder bestehende Unstimmigkeiten aufzuklären, um eine eindeutige Aussage über das Bestehen oder Nichtbestehen der Anspruchsvoraussetzungen treffen zu können.

Ein gewisser Informationsüberschuss des Leistungsträgers bei der Sachverhaltsaufklärung ist hinzunehmen, insbesondere dann, wenn andere in Betracht kommende Beweismittel sich nicht als gleichermaßen ergiebig für die Sachverhaltsfeststellung erweisen. Zu beachten ist, dass im Rahmen des Amtsermittlungsgrundsatzes (§ 20 Abs. 1 SGB X) dem Leistungsträger bei der Bestimmung von Art und Umfang der Ermittlungen ein Einschätzungsspielraum zukommt. Ihm muss es möglich sein, sich jedenfalls ein so umfassendes Bild machen zu können,

[32] Vgl. Stief, in: Schröder, Bayerisches Datenschutzgesetz, 2021, Art. 4 Rn. 41.
[33] Vgl. Spellbrink, in: Kasseler Kommentar, Stand 8/2019, § 60 SGB I Rn. 12.

dass er den für die Entscheidung relevanten Sachverhalt zuverlässig einschätzen kann. Dazu hat der Leistungsträger gemäß § 20 Abs. 2 SGB X alle für den Einzelfall bedeutsamen, auch die für die Beteiligten günstigen Umstände zu berücksichtigen.

4.1.4 Konkrete Prüfung

Das Jobcenter konnte mir im konkreten Fall für jede fragliche Unterlage plausibel Gründe darlegen, die eine Anforderung im Widerspruchsverfahren erforderlich gemacht haben und somit erheblich im Sinne von § 60 Abs. 1 Satz 1 Nr. 1 SGB I waren. Das Jobcenter konnte insbesondere konkret begründen, für welche Anspruchsvoraussetzungen welche Unterlagen relevant und weshalb bereits vorgelegte Unterlagen noch nicht ausreichend waren, um den Sachverhalt hinreichend klar feststellen zu können. Von Schikane bei der Anforderung der Unterlagen konnte daher nicht die Rede sein.

Im Ergebnis war kein Verstoß gegen Datenschutzrecht, insbesondere kein Verstoß gegen den Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) festzustellen. Die Erhebung der betreffenden Sozialdaten durch das Jobcenter war zur Bedarfsermittlung und somit zur Berechnung eines etwaigen Bürgergeldanspruchs im Sinne von § 67a Abs. 1 Satz 1 SGB X erforderlich.

4.1.5 Fazit

Bei Sachverhaltsermittlungen in Verwaltungsverfahren hat die Behörde im Rahmen des Amtsermittlungsgrundsatzes einen gewissen Spielraum beim Umfang der Datenerhebung.

Geht es um eine Leistungsgewährung, legen die fachgesetzlichen Voraussetzungen, unter denen die betreffende Leistung gewährt wird, auch fest, über welche Informationen sich die Behörde „Gedanken machen darf“. Klärt die Behörde die tatsächlichen Umstände auf, mit denen die fachgesetzlichen Voraussetzungen belegt werden, steht dem das Datenschutzrecht grundsätzlich nicht entgegen. Es respektiert auch, dass die Behörde Unsicherheiten bei einzelnen Umständen durch Gewinnung einer breiteren Informationsbasis begegnet. Die Behörde muss sich beispielsweise nicht auf Unterlagen eines Antragstellers verlassen, die auf bestimmte Umstände hindeuten, wenn diese Unterlagen nicht die nötige Sicherheit vermitteln.

Grenzen zöge das Datenschutzrecht insbesondere dann, wenn eine Behörde anlässlich eines Verwaltungsverfahrens personenbezogene Daten erheben würde, die aus fachrechtlicher Sicht nicht relevant werden können, im Fall einer Leistungsgewährung also insbesondere bei Informationen, die für die Voraussetzungen der betreffenden Leistung keinen Aussagewert haben können.

4.2 Übermittlung von Sozialdaten eines Jobcenters an eine kommunale Ausländerbehörde

Mit einer Beratungsanfrage zur Datenübermittlung von Sozialdaten wandte sich eine bayerische Kommune an mich. Konkret ging es um die Frage, welche Daten eine Ausländerbehörde im Rahmen ihrer Aufgabenerfüllung bei einem Jobcenter

erheben darf, beziehungsweise welche Daten das Jobcenter im Rahmen von § 71 Abs. 2 Satz 1 Nr. 1 Buchst. a Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X) an die kommunale Ausländerbehörde übermitteln darf.

Hintergrund der Frage war, dass Sozialleistungsbezüge durch Ausländerinnen und Ausländer aufenthaltsrechtlich relevant sein können. Das Jobcenter vertrat die Auffassung, dass generell keine Daten zur Höhe und zur Dauer des Leistungsbezugs übermittelt werden dürfen, sondern lediglich die Tatsache, ob Leistungen gewährt werden oder nicht. Dieser Ansicht ist die Kommune entgegengetreten. Aus ihrer Sicht sind auch Daten über die Art der Leistungen und zur Höhe und Dauer des Leistungsbezugs im Einzelfall – soweit erforderlich – zu übermitteln. Zwischen der Kommune und dem Jobcenter bestand somit eine Meinungsverschiedenheit über den Umfang der zu übermittelnden Daten.

4.2.1 Ausgangspunkt: Doppeltürmodell

Die Einschätzung der Kommune bezog sich vor allem auf § 71 Abs. 2 Satz 1 Nr. 1 Buchst. a SGB X und § 87 Abs. 1 Aufenthaltsgesetz (AufenthG). Dabei handelt es sich datenschutzrechtlich um Übermittlungstatbestände. § 71 Abs. 2 Satz 1 Nr. 1 SGB X schränkt die Mitteilungspflichten des § 87 Abs. 1 AufenthG ein.[34]

Bei der Regelung eines Datentransfers zur Wahrnehmung öffentlicher Aufgaben ist nach der verfassungsgerichtlichen Rechtsprechung mit dem sogenannten Doppeltürmodell zwischen der Datenübermittlung von der auskunfterteilenden Stelle und dem Datenabruf durch die auskunftersuchenden Stelle zu unterscheiden. Der Datentransfer vollzieht sich in den einander korrespondierenden Eingriffen von Abfrage und Übermittlung, die jeweils einer eigenen Rechtsgrundlage bedürfen.[35]

Als Befugnis zur Erhebung personenbezogener Daten durch die Ausländerbehörde kommt § 86 AufenthG in Betracht. Gemäß § 86 Satz 1 AufenthG dürfen die mit der Ausführung dieses Gesetzes betrauten Behörden zum Zweck der Ausführung dieses Gesetzes und ausländerrechtlicher Bestimmungen in anderen Gesetzen personenbezogene Daten erheben, soweit dies zur Erfüllung ihrer Aufgaben nach diesem Gesetz und nach ausländerrechtlichen Bestimmungen in anderen Gesetzen erforderlich ist.

Die kommunale Ausländerbehörde argumentierte mit Blick auf Art. 14 Abs. 3 sowie Erwägungsgrund 16 Richtlinie 2004/38/EG (sog. Freizügigkeits-Richtlinie), dass es nicht ausreichend sei, lediglich über das „Ob" der Gewährung von Sozialleistungen an die betroffene Person informiert zu werden, nicht dagegen über das „Wie". Müsse die Verweigerung des Aufenthaltsrechts oder eine Ausweisung geprüft werden, sei eine umfassende Würdigung des Einzelfalls durch die Ausländerbehörde geboten. Dabei seien auch etwa die Modalitäten der Inanspruchnahme von Sozialhilfeleistungen zu berücksichtigen.

[34] Vgl. Martin, in: Kasseler Kommentar, Stand 5/2024, § 71 SGB X Rn. 51.

[35] Vgl. Bundesverfassungsgericht, Beschluss vom 24. Januar 2012, 1 BvR 1299/05, BeckRS 2012, 47556, Rn. 123.

Aus datenschutzrechtlicher Sicht hatte ich aufgrund der gesetzlichen Einschränkung durch das Erforderlichkeitskriterium in § 86 Satz 1 AufenthG keine grundsätzlichen Bedenken im Hinblick auf das von der kommunalen Ausländerbehörde fachrechtlich favorisierte Verständnis.

4.2.2 Verantwortlichkeit für die Datenübermittlung

Allerdings war zu beachten, dass die Verantwortlichkeit für die Datenübermittlung gemäß § 67d Abs. 1 Satz 1 SGB X grundsätzlich bei der übermittelnden Stelle liegt. Da die Datenschutzaufsicht über das betreffende Jobcenter als übermittelnde Stelle nicht bei mir, sondern bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit liegt, war es mir nicht möglich, die Rechtmäßigkeit der erwogenen Datenübermittlung abschließend zu prüfen, da sich diese meiner Aufsichtszuständigkeit entzog. Dies betraf insbesondere die Rechtsfrage, wie die Worte „Daten über die Gewährung oder Nichtgewährung von Leistungen" in § 71 Abs. 2 Satz 1 Nr. 1 Buchst. a SGB X genau zu verstehen sind.

Zur Lösung dieses Problems ist die Abgrenzung der datenschutzrechtlichen Verantwortlichkeit von besonderer Bedeutung. Dabei war auch die Allgemeine Verwaltungsvorschrift zum Aufenthaltsgesetz (AufenthGAVwV)[36] zu beachten. Diese enthält in Nr. 87.1.1.5 AufenthGAVwV nicht nur einen Hinweis zum Verhältnis von § 87 Abs. 1 AufenthG zu § 71 Abs. 2 Satz 1 Nr. 1 Buchst. a SGB X, sondern in Nr. 87.1.4.2 AufenthGAVwV auch eine Verfahrensvorschrift bei einem Dissens der Ansichten von ersuchender und ersuchter Stelle:

„Ist zwischen der Ausländerbehörde und der übermittelnden Stelle streitig, ob die Übermittlung rechtmäßig ist, so ist die Auffassung jeder Seite insoweit maßgebend, als sie die Verantwortung für die Rechtmäßigkeit der Übermittlung trägt (vgl. Nummer 87.1.4.1). Im Zweifel ist die Entscheidung der gemeinsamen Aufsichtsbehörde herbeizuführen. Fehlt eine derartige gemeinsame Aufsichtsbehörde, hat die Ausländerbehörde die Entscheidung der obersten Landesbehörde herbeizuführen."

Demnach kommt es bei einem Meinungsstreit in erster Linie auf die Verantwortung für die Rechtmäßigkeit an. Gemäß § 67d Abs. 1 Satz 1 SGB X liegt die Verantwortlichkeit für die Datenübermittlung grundsätzlich bei der übermittelnden Stelle. Bei diesem Grundsatz bleibt es auch, wenn die Übermittlung auf Ersuchen eines Dritten erfolgt. Der Dritte trägt nach § 67d Abs. 1 Satz 2 SGB X allein die Verantwortlichkeit für die Richtigkeit seiner Angaben. Im Ergebnis kommt es bei einem Konflikt über die Zulässigkeit einer Übermittlung somit nicht auf die Auffassung der ersuchenden Stelle an.[37]

Eine gemeinsame Aufsichtsbehörde zwischen dem betreffenden Jobcenter, das als gemeinsame Einrichtung im Sinne von § 44b Abs. 1 Satz 1 Zweites Buch Sozialgesetzbuch – Bürgergeld, Grundsicherung für Arbeitsuchende – (SGB II) als öffentliche Stelle des Bundes anzusehen war, und der kommunalen Ausländerbehörde bestand nicht. Nr. 87.1.4.2 AufenthGAVwV letzter Satz sieht in diesem Fall vor, dass die Ausländerbehörde die Entscheidung der obersten Landesbehörde herbeizuführen hat. Ich habe daher der anfragenden Kommune anheimgestellt,

[36] Vom 26. Oktober 2009 (GMBl S. 878).

[37] Vgl. Eichenhofer, in: Huber/Mantel, Aufenthaltsgesetz/Asylgesetz, 3. Aufl. 2021, § 87 AufenthG Rn. 25.

sich zur abschließenden Klärung an das Bayerische Staatsministerium des Innern, für Sport und Integration als oberste Ausländerbehörde (oberste Landesbehörde) im Sinne von § 1 Nr. 5 Zuständigkeitsverordnung Ausländerrecht zu wenden. Ebenfalls habe ich – mit Blick auf die Auslegung sozialrechtlicher Tatbestände – vorgeschlagen, das Bayerische Staatsministerium für Familie, Arbeit und Soziales, das zusammen mit dem Bundesministerium für Arbeit und Soziales gemeinsam die Aufsicht über die gemeinsamen Einrichtungen im Sinne von § 44b Abs. 1 Satz 1 SGB II führt, einzubeziehen.

4.2.3 Ergebnis

Bei Datenübermittlungen zwischen zwei Verantwortlichen ist das sogenannte Doppeltürmodell zu beachten und genau zu prüfen, auf welche Erhebungsbefugnis die ersuchende Stelle die Datenerhebung und auf welche Übermittlungsbefugnis die ersuchte Stelle die Datenübermittlung stützt. Bei der Übermittlung von Sozialdaten sind besondere Übermittlungsgrundsätze, insbesondere gemäß § 67d SGB X zu beachten. Bei einem Dissens zwischen ersuchender und ersuchter Stelle spielt die Abgrenzung der datenschutzrechtlichen Verantwortlichkeit und die daraus folgende Entscheidungskompetenz eine wichtige Rolle.

4.3 Vollzug der Mitteilungsverordnung

Der Staat ist für die Besteuerung auf Informationen angewiesen. Das Gesetz sieht insofern auch Mitteilungspflichten vor, die Zahlungen leistende Stellen treffen. Grundsätzlich geregelt ist das in § 93a Abgabenordnung, wobei die Details in einer Rechtsverordnung, der „Verordnung über Mitteilungen an die Finanzbehörden durch andere Behörden und öffentlich-rechtliche Rundfunkanstalten“, kurz: Mitteilungsverordnung, festgelegt sind. Ob im Einzelfall eine Mitteilungspflicht besteht, ist nicht immer zweifelsfrei. Das Problem stellt sich mitunter auch für Sozialleistungsträger, wie die folgenden vier Beratungsanfragen zeigen.

4.3.1 Zahlungen an Pflegeeltern

Die Datenschutzbeauftragte einer bayerischen Sozialbehörde hat mich um Beratung zu der Frage gebeten, ob die vom Jugendamt an Pflegeeltern geleisteten Zahlungen des Pflegegeldes dem Finanzamt mitzuteilen sind. Sie hat sich in diesem Zusammenhang auf die allgemeine Mitteilungspflicht an Finanzbehörden berufen.

Nach § 2 Abs. 1 Satz 1 Mitteilungsverordnung (MV) erstreckt sich die Mitteilungspflicht grundsätzlich auf alle Zahlungen von Behörden und anderen öffentlichen Stellen an Dritte. Diese Pflicht gilt jedoch nur, sofern keine Ausnahme geregelt ist. Gemäß § 1 Abs. 2 MV sind personenbezogene Daten, die dem Sozialgeheimnis unterliegen, nicht mitzuteilen.

Dem Schreiben des Bundesministeriums der Finanzen betreffend die Anwendung der Mitteilungsverordnung vom 26. September 2023[38] kann unter Textziffer 3.5 entnommen werden, dass personenbezogenen Daten nicht mitzuteilen sind, soweit sie durch § 35 Erstes Buch Sozialgesetzbuch – Allgemeiner Teil –

[38] BStBl. I S. 1663; geändert durch BMF vom 12. April 2024, BStBl. I S. 696.

(SGB I) geschützt sind. Nicht mitteilungspflichtig sind danach personenbezogene Daten (Art. 4 Nr. 1 DSGVO), die von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach dem Sozialgesetzbuch verarbeitet werden. Nicht unter den Sozialdatenschutz fallen andere personenbezogene Daten, welche die in § 35 SGB I genannte Stelle beispielsweise als Dienstherr oder öffentlicher Arbeitgeber oder im Rahmen der Fiskalverwaltung verarbeitet (zum Beispiel für Honorarzahlungen, die von Sozialbehörden an Leistungserbringer erbracht werden, und für Zahlungen an ehrenamtlich Tätige).

Bei der Betreuung von Pflegefamilien handelt es sich um eine Aufgabe im Rahmen der Hilfe zur Erziehung in Vollzeitpflege gemäß § 33 Achtes Buch Sozialgesetzbuch – Kinder- und Jugendhilfe – (SGB VIII). Diese Aufgabe umfasst auch die Gewährung wirtschaftlicher Jugendhilfe in Gestalt des so genannten Pflegegelds gemäß § 39 Abs. 1 Satz 1 SGB VIII. Da somit ein Sozialleistungsträger, also eine in § 35 SGB I genannte Stelle, eine Aufgabe nach dem Sozialgesetzbuch erfüllt, stellen die in diesem Zusammenhang verarbeiteten Daten – auch die Daten der Pflegeeltern – Sozialdaten dar, die nach § 67 Abs. 2 Satz 1 Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X) verarbeitet werden. Für diese gilt das Sozialgeheimnis gemäß § 35 Abs. 1 Satz 1 SGB I, weshalb eine Mitteilung gemäß § 1 Abs. 2 MV zu unterbleiben hat.

Dies würde nur dann nicht gelten, sofern eine (Rück-)Ausnahme die „Durchbrechung" des Sozialgeheimnisses ermöglicht. Eine solche Rückausnahme wäre systematisch im Sozialgesetzbuch zu suchen, da dieses im Hinblick auf die Verarbeitung von Sozialdaten grundsätzlich als abschließend zu betrachten ist (siehe § 35 Abs. 2 SGB I).

Für die beschriebene Fallgestaltung lässt sich jedoch weder im Achten noch im Zehnten Buch Sozialgesetzbuch eine (spezielle) Datenübermittlungsbefugnis finden. Es gibt zwar eine Regelung im Sozialgesetzbuch, die die Mitteilung zu abgabenrechtlichen Zwecken ausdrücklich gestattet, allerdings nur in Bezug auf Daten ausländischer Unternehmen, die auf Grund bilateraler Regierungsvereinbarungen über die Beschäftigung von Arbeitnehmern zur Ausführung von Werkverträgen tätig werden, nach § 93a Abgabenordnung (siehe § 71 Abs. 1 Satz 1 Nr. 3 SGB X). Auf diese Datenübermittlungsbefugnis stützt sich wiederum die auch in der Mitteilungsverordnung geregelte Ausnahme zur Weitergabe von Daten, die dem Sozialgeheimnis unterliegen, in § 6 Abs. 2 MV.[39]

Vor diesem Hintergrund bleibt es bei dem oben bereits festgestellten Ergebnis, dass die an Pflegeeltern geleisteten Zahlungen des Pflegegeldes dem Finanzamt nicht mitgeteilt werden dürfen.

4.3.2 Leistungen für Heizung und Unterkunft

In einem anderen Fall wurde ich von der Datenschutzbeauftragten eines bayerischen Landratsamtes um Klärung gebeten, inwiefern bestimmte Leistungen für Heizung und Unterkunft nach § 1 Abs. 2 MV von der Mitteilungspflicht ausgenommen sind.

Den sozialrechtlichen Hintergrund der Frage bilden § 22 Abs. 7 Satz 1 Zweites Buch Sozialgesetzbuch – Bürgergeld, Grundsicherung für Arbeitsuchende –

[39] Vgl. BMF vom 26. September 2023, BStBl. I S. 1663, Tz. 4.1.5.2.

(SGB II) und § 35a Abs. 3 Satz 1 Zwölftes Buch Sozialgesetzbuch – Sozialhilfe – (SGB XII). Hiernach können Sozialleistungsträger die jeweiligen Bedarfe für Unterkunft und Heizung auf Antrag des Leistungsberechtigten durch Direktzahlung an dessen Vermieter gewähren.

Die Direktzahlung an den Vermieter gemäß § 22 Abs. 7 SGB II beziehungsweise § 35a Abs. 3 SGB XII stellt ein Sozialdatum dar, weil insofern ein Leistungsträger im Sinne des § 35 Abs. 1 Satz 1 SGB I personenbezogene Daten zur Erfüllung einer Aufgabe nach dem Sozialgesetzbuch verarbeitet.

Es ist unerheblich, dass der Vermieter nicht selbst leistungsberechtigt nach dem Sozialgesetzbuch ist. Maßgebend sind die schuldrechtlichen Leistungsbeziehungen. Werden die Leistungen für Unterkunft und Heizung aufgrund § 22 Abs. 7 SGB II beziehungsweise § 35a Abs. 3 SGB XII direkt an den Vermieter gezahlt, wirkt dies rechtlich als Anspruchserfüllung gegenüber dem Leistungsberechtigten. Im Verhältnis von Leistungsberechtigtem und Vermieter wirkt die Zahlung des Leistungsträgers als Erfüllung des mietvertraglichen Anspruchs des Vermieters durch den Leistungsberechtigten. Es werden durch die direkte Mietzahlung durch den Leistungsträger aber keine rechtlichen Verpflichtungen des Leistungsträgers gegenüber dem Vermieter erfüllt, denn solche bestehen hier nicht.

Eine Mitteilung der Direktzahlung an die Finanzbehörden scheidet somit nach § 1 Abs. 2 MV aus.

4.3.3 Mietzahlungen im Zusammenhang mit der Unterbringung von Leistungsberechtigten nach dem Asylbewerberleistungsgesetz

Eine vergleichbare Frage, jedoch mit anderem Ergebnis, stellte man mir auch für Zahlungen im Zusammenhang mit dem Asylbewerberleistungsgesetz (AsylbLG).

Im Vollzug des Asylbewerberleistungsgesetzes sowie der ergänzenden Landesgesetze und Verordnungen mietete das anfragende Landratsamt (teils auch von privaten Vermietern) geeignete Unterkünfte für die Unterbringung der Leistungsberechtigten.

Im Hinblick auf § 1 Abs. 2 MV fehlt es bei diesen Mietzahlungen – anders als in den oben untersuchten Fällen – an einer den Sozialdatenschutz begründenden Aufgabe nach dem Sozialgesetzbuch. Das Asylbewerberleistungsgesetz gilt nicht als besonderer Teil des Sozialgesetzbuches (vgl. § 68 SGB I). Zwar verweist das Asylbewerberleistungsgesetz vereinzelt auf Vorschriften des Sozialgesetzbuches (vgl. insbesondere § 9 AsylbLG), der Verweis erstreckt sich aber nicht auf sozialdatenschutzrechtliche Bestimmungen, insbesondere nicht auf das Sozialgeheimnis nach § 35 Abs. 1 Satz 1 SGB I.

Hinzu kommt, dass die Mietzahlungen selbst auch keine unmittelbaren Leistungen nach dem Asylbewerberleistungsgesetz sind. Geschuldet ist hiernach grundsätzlich die Unterbringung als solche. Die Mietzahlung an den Vermieter findet ihre Grundlage hingegen im privatrechtlichen Mietvertrag. Sie ist der Fiskalverwaltung zuzurechnen.

Einer Mitteilung der Mietzahlungen gemäß § 2 Abs. 1 Satz 1 MV steht § 1 Abs. 2 MV somit nicht entgegen.

4.3.4 Zahlungen an Dolmetscher

Außerdem trat ein bayerischer Bezirk mit der Frage an mich heran, ob der Finanzbehörde Zahlungen an Dolmetscher zu melden sind, die innerhalb eines Sozialverwaltungsverfahrens nach § 19 Abs. 2 Satz 4 SGB X für die Behörde tätig geworden sind oder – so die Ansicht des Bezirks – ob sie wegen § 1 Abs. 2 MV von der Mitteilungspflicht ausgenommen sind.

Ich vertrete die Ansicht, dass die für Zahlungen an einen Dolmetscher verarbeiteten personenbezogenen Daten – und nur um diese geht es – keine Sozialdaten darstellen.

Zwar werden die personenbezogenen Daten des Dolmetschers von einer in § 35 SGB I genannten Stelle verarbeitet. Die Verarbeitung für Zwecke der Honorarzahlung erfolgt aber nicht wie von § 67 Abs. 2 SGB X verlangt „im Hinblick auf ihre Aufgaben nach dem Sozialgesetzbuch". Erforderlich wäre hierfür, dass der Sozialleistungsträger die fraglichen personenbezogenen Daten unmittelbar zur Erfüllung einer Aufgabe nach dem Sozialgesetzbuch verarbeitet. Es genügt nicht, dass zwischen der gesetzlichen Aufgabe und der Datenverarbeitung eine bloße Korrelations- oder Kausalitätsbeziehung besteht. Die Leistung an den Dolmetscher mag – je nach Rechtsgrund der Zahlung – der Erfüllung einer vertraglichen oder sonstigen Rechtspflicht des Leistungsträgers dienen, nicht aber – worauf es ankommt – der Erfüllung einer Aufgabe nach dem Sozialgesetzbuch.

Mit Blick auf § 8 Abs. 1 MV (Inhalt der Mitteilung) wäre aber im Einzelfall zu prüfen, inwiefern eine Meldung (teilweise) zu unterbleiben hat. Soweit die Meldung Daten beinhaltet, die einen Rückschluss auf ein konkretes Sozialverwaltungsverfahren, und somit auf Sozialdaten, zulassen, wären diese von der Mitteilung auszunehmen (beispielsweise das Aktenzeichen des betreffenden Sozialverwaltungsverfahrens).

Im Ergebnis steht daher § 1 Abs. 2 MV einer Mitteilung von Zahlungen an Dolmetscher an die Finanzbehörde nicht generell entgegen.

4.4 Meldepflichten nach § 47 SGB VIII

Einrichtungen, in denen ganztägig oder für einen Teil des Tages Kinder oder Jugendliche betreut werden, benötigen für ihren Betrieb grundsätzlich eine Erlaubnis gemäß § 45 Abs. 1 Satz 1 Achtes Buch Sozialgesetzbuch – Kinder- und Jugendhilfe – (SGB VIII). Eine Legaldefinition des Einrichtungsbegriffs findet sich in § 45a SGB VIII. Hiervon umfasst sind etwa Heime, heilpädagogische Tagesstätten und Kindertageseinrichtungen. Welche Behörde für die Erteilung der Betriebserlaubnis zuständig ist, richtet sich nach Art. 45 Abs. 1 Satz 1 Gesetz zur Ausführung der Sozialgesetze.

Ist eine Betriebserlaubnis erteilt, muss die Einrichtung der Erlaubnisbehörde zunächst die Betriebsaufnahme anzeigen, sodann treffen sie weitere Anzeige-, Melde- und Dokumentationspflichten, etwa zu nachträglichen Entwicklungen, einer Schließung der Einrichtung, Konzeption und Belegungszahlen (siehe im Einzelnen § 47 SGB VIII).

Im Berichtszeitraum habe ich mich mit dem Umfang dieser Meldepflichten befasst. Im Zentrum stand dabei die Frage, ob vor Erfüllung der Anzeigepflicht wegen

einer möglichen Kindeswohlgefährdung (§ 47 Abs. 1 Nr. 2 SGB VIII) das Einverständnis der betroffenen Kinder oder Jugendlichen und/oder ihrer Personensorgeberechtigten einzuholen ist.

Nach § 47 Abs. 1 Nr. 2 SGB VIII sind Ereignisse und Entwicklungen anzuzeigen, die geeignet sind, das Wohl der Kinder und Jugendlichen zu beeinträchtigen. Hierbei handelt es sich zunächst um eine unbestimmte Vorgabe, welche einen nicht unerheblichen Interpretationsspielraum eröffnet.[40] Bislang fehlt es an einer hinreichenden Konkretisierung des meldepflichtigen Ereignisses durch Rechtsprechung und Literatur.[41]

Zur Orientierung werden in der Praxis unter anderem die „Handlungsleitlinien zur Umsetzung des Bundeskinderschutzgesetzes im Arbeitsfeld der betriebserlaubnispflichtigen Einrichtungen nach § 45 SGB VIII“ der Bundesarbeitsgemeinschaft Landesjugendämter[42] herangezogen. Diese Leitlinien definieren die Ereignisse und Entwicklungen, die geeignet sind, das Wohl der Kinder und Jugendlichen zu beeinträchtigen, als nicht alltägliche, akute Ereignisse oder über einen gewissen Zeitraum anhaltende Entwicklungen in einer Einrichtung, die sich in erheblichem Maße auf das Wohl von Kindern und Jugendlichen auswirken oder zumindest auswirken können.[43]

Konkret werden als solche Ereignisse unter anderem benannt: Gefährdungen, Schädigungen durch zu betreuende Kinder und/oder Jugendliche und delinquentes Verhalten von zu betreuenden Kindern und/oder Jugendlichen (hierunter sind insbesondere zu verstehen: gravierende selbstgefährdende Handlungen, auf eine Selbsttötung zielende Handlungen, sexuelle Gewalt, Körperverletzungen und sonstige erhebliche oder wiederholte Straftaten).

Wie sich aus der in § 47 Satz 1 Nr. 2 SGB VIII verwendeten Formulierung der Eignung des Ereignisses oder der Entwicklung zur „Beeinträchtigung“ des Kindeswohls ergibt, muss immer eine gewisse Erheblichkeitsschwelle überschritten werden, um eine Meldepflicht auszulösen.[44]

Sofern dies der Fall ist, müssen die Ereignisse oder Entwicklungen angezeigt werden; § 47 Abs. 1 SGB VIII eröffnet der Einrichtung keinen Entscheidungsspielraum. Die Meldepflicht besteht dabei auch ohne ausdrückliche Aufforderung durch die Behörde; der Träger der Einrichtung muss ihr von sich aus nachkommen.[45]

Inwieweit die Meldung personenbezogene Angaben von Kindern, Jugendlichen oder deren Personensorgeberechtigten enthalten muss, ist zwar eine Frage des Einzelfalls.[46] Bei der Meldung ist auch der Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) zu beachten. Das bedeutet, dass der Inhalt der Meldung

40 Siehe Mörsberger, in: Wiesner/Wapler, SGB VIII, 6. Aufl. 2022, § 47 Rn. 7c.

41 Kepert/Dexheimer, in: Lehr- und Praxiskommentar Sozialgesetzbuch VIII, 8. Aufl. 2022, § 47 Rn. 6.

42 2. aktualisierte Fassung 2013, Internet beispielsweise: https://mbjs.brandenburg.de/sixcms/media.php/140/handlungsleitlinien_umsetzung_bkischg_betriebserlaub.pdf.

43 Siehe Handlungsleitlinien (Fn. 42), S. 9.

44 Kepert/Dexheimer, in: Lehr- und Praxiskommentar Sozialgesetzbuch VIII, 8. Aufl. 2022, § 47 Rn. 6.

45 Janda, in: Kasseler Kommentar, Stand 11/2023, § 47 SGB VIII Rn. 11.

46 Siehe zum Beispiel Verwaltungsgericht Frankfurt (Oder), Beschluss vom 20. August 2021, VG 6 L 289/21, BeckRS 2021, 23003.

nicht mehr über konkrete Personen offenlegen darf als für die Zweckerreichung geboten. Wohl regelmäßig wird eine Meldung nach § 47 Satz 1 Nr. 2 SGB VIII aber nicht ohne personenbezogene Daten auskommen. Die Vorschrift regelt also (auch) eine Pflicht zur Datenübermittlung.

Dies hat im Datenschutzrecht zwei Konsequenzen:

— Zum einen schafft § 47 Satz 1 Nr. 2 SGB VIII im Zusammenspiel mit Art. 6 Abs. 1 UAbs. 1 Buchst. c, Abs. 3 UAbs. 1 Buchst. b DSGVO – soweit Gesundheitsdaten betroffen sein sollten zusätzlich in Verbindung mit Art. 9 Abs. 2 Buchst. h, Abs. 3 DSGVO – eine Rechtsgrundlage für die Übermittlung der erforderlichen personenbezogenen Daten von der Einrichtung an die Erlaubnisbehörde.

— Zum anderen steht damit auch fest, dass das Einverständnis der betroffenen Kinder oder Jugendlichen und/oder ihrer Personensorgeberechtigten nicht benötigt wird; Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO fordert eine solche Mitwirkung (gerade) nicht. Dieses Ergebnis ist auch sachgerecht, weil die Norm dem Schutz der Rechtsgüter und Interessen der Kinder und Jugendlichen verpflichtet ist. Sofern die Anzeigepflicht von einem Einverständnis abhängig gemacht werden würde, würde dieser Zweck konterkariert werden.

4.5 Anforderung von erweiterten Führungszeugnissen

Weiterhin war ich mit der Frage befasst, ob die Erlaubnisbehörde erweiterte Führungszeugnisse des (zukünftig) beschäftigten Personals einschließlich der Leitung der Einrichtung anfordern darf.

Nach § 62 Abs. 1 SGB VIII darf die Erlaubnisbehörde Sozialdaten nur erheben, soweit ihre Kenntnis zur Erfüllung der Aufgabe, über eine Erlaubnis nach § 45 Abs. 1 Satz 1 SGB VIII zu entscheiden, erforderlich ist.

Vor Erteilung einer Betriebserlaubnis ist nach meiner Auffassung lediglich die Erhebung eines Nachweises angezeigt, dass Führungszeugnisse nach § 30 Abs. 1 Satz 1 und § 30a Abs. 1 Bundeszentralregistergesetz vorgelegt und geprüft werden. Eine Vorlage der Führungszeugnisse bei der Erlaubnisbehörde ist dagegen grundsätzlich nicht notwendig.

§ 45 Abs. 3 Nr. 2 SGB VIII spricht im Hinblick auf die Eignung des Personals nur von einem Nachweis der Sicherstellung durch den Träger der Einrichtung. Diese Vorschrift enthält keine Befugnis für die Erlaubnisbehörde, selbst Führungszeugnisse zu verlangen.[47] Sie regelt zugleich, wer die Führungszeugnisse zu prüfen und wer darüber wem gegenüber Rechenschaft abzulegen hat. Das Regelungskonzept setzt also auf ein dezentrales Modell: Der Träger der Einrichtung lässt sich die Führungszeugnisse vorlegen und prüft diese; gegenüber der Erlaubnisbehörde führt er den Nachweis eines entsprechenden „Zeugnismanagements“. Eine „Doppelprüfung“ ist daher grundsätzlich nicht angezeigt.

[47] So Janda, in: Kasseler Kommentar, Stand 11/2023, § 45 SGB VIII Rn. 76.

Diese Grundsätze dürften auch nach Betriebsaufnahme und Wechsel im Personalbestand gelten.

Lediglich in Ausnahmefällen kann – gestützt auf § 62 Abs. 1 SGB VIII – die Vorlage eines konkreten Führungszeugnisses bei der Erlaubnisbehörde erforderlich sein. Dies ist dann der Fall, wenn konkrete Anhaltspunkte für eine bestehende oder drohende Kindeswohlgefährdung bestehen.

So sind beispielsweise andere öffentliche Stellen, die von Gefährdungen in einer Einrichtung für Kinder und Jugendliche erfahren, gehalten, im Rahmen ihrer Aufgaben und Befugnisse die nach §§ 45 ff. SGB VIII zuständige Aufsichtsbehörde zu informieren.[48] Anschließend hat diese zu prüfen, ob die hiervon betroffene Leitung der Einrichtung oder dort beschäftigte Personen die für ihre Tätigkeit erforderliche Eignung (noch) besitzen.[49] Die Anforderungen an die persönliche Eignung des Personals richten sich dabei nach der Zweckbestimmung der Einrichtung und den jeweils auszuübenden Funktionen. Wesentlich ist dabei, dass die eingesetzten Kräfte den Anforderungen der jeweiligen Einrichtung gewachsen sind und das Kindeswohl gewährleistet ist.[50]

Unabhängig davon besteht zwar auch noch die Möglichkeit, das Anforderungsprofil des § 45 SGB VIII zu konkretisieren und zu ergänzen; § 49 SGB VIII begründet insoweit ausdrücklich einen entsprechenden Gestaltungsspielraum. Das bedeutet, auf Landesebene könnte grundsätzlich geregelt werden, dass der Erlaubnisbehörde auch erweiterte Führungszeugnisse des Personals sowie der Leitung der Einrichtung etwa vor Betriebsaufnahme vorgelegt werden müssen.

Aufgrund der objektiv berufsregelnden Tendenz einer derartigen Vorgabe bedarf es insoweit jedoch einer gesetzlichen Grundlage in Form eines Parlamentsgesetzes oder einer Rechtsverordnung. Bloße Verwaltungsvorschriften genügen nicht. Bayern hat von der durch § 49 SGB VIII eingeräumten Möglichkeit, soweit ersichtlich jedoch bisher keinen Gebrauch gemacht, obwohl Art. 44 Gesetz zur Ausführung der Sozialgesetze (AGSG) die Staatsregierung auf Landesebene ermächtigt, (zumindest) durch Rechtsverordnung Mindestvoraussetzungen festzulegen, die erfüllt sein müssen, damit das Wohl von Kindern und Jugendlichen in nach § 45 SGB VIII erlaubnispflichtigen Einrichtungen gewährleistet ist. Eine solche Rechtsverordnung ist jedenfalls auf der Grundlage von Art. 44 AGSG nicht ergangen; der geltenden Bekanntmachung des Bayerischen Staatsministeriums für Familie, Arbeit und Soziales über die Richtlinien für Heilpädagogische Tagesstätten, Heime und sonstige Einrichtungen für Kinder und Jugendliche und junge Volljährige mit Behinderung[51] fehlt es gerade am geforderten Verordnungscharakter.[52]

Datenschutzrechtlich bedeutet dies im Ergebnis, dass eine Erlaubnisbehörde dem Grunde nach keine erweiterten Führungszeugnisse anfordern, also erheben, darf.

48 Siehe Wiesner, in: ders./Wapler, SGB VIII, 6. Aufl. 2022, § 45 Rn. 107.

49 Im Ergebnis verneint: Oberverwaltungsgericht des Saarlandes, Beschluss vom 8. April 2020, 2 D 65/20, BeckRS 2020, 5882.

50 So Bayerischer Verwaltungsgerichtshof, Beschluss vom 2. Februar 2017, 12 CE 17.71, BeckRS 2017, 101762, Rn. 31 ff.

51 Vom 28. Oktober 2022 (BayMBl. Nr. 655).

52 Siehe Bayerischer Verwaltungsgerichtshof, Beschluss vom 2. Februar 2017, 12 CE 17.71, BeckRS 2017, 101762, Rn. 39, 43.

4.6 Vollzug des Masernschutzgesetzes – Anforderung von Impfnachweisen

Im Zusammenhang mit dem zum 1. März 2020 in Kraft getretenen Masernschutzgesetz erreichen mich weiterhin zahlreiche Anfragen von Bürgerinnen und Bürgern (vgl. bereits den 30. Tätigkeitsbericht 2020 unter Nr. 10.2.1, den 31. Tätigkeitsbericht 2021 unter Nr. 7.1 und den 33. Tätigkeitsbericht 2023 unter Nr. 6.5). Aktuell habe ich die Praxis eines Gesundheitsamtes überprüft, bei den Kindertageseinrichtungen in seinem Zuständigkeitsbereich stichprobenweise durch das Infektionsschutzgesetz (IfSG) geforderte Nachweise im Zusammenhang mit dem Masernschutz anzufordern. Die Kindertageseinrichtungen hatten zuvor keine Zweifel an der Echtheit oder inhaltlichen Richtigkeit der vorgelegten Nachweise mitgeteilt. Zudem war das Gesundheitsamt überhaupt erst nach einer gewissen Zeit tätig geworden (wohl ein bis drei Jahre nach Vorlage der Nachweise bei den betreuenden Kindertageseinrichtungen), was für Verwunderung bei den betroffenen Personen sorgte.

Nach § 20 Abs. 9 Satz 1 IfSG müssen Nachweise über das Vorliegen eines ausreichenden Impfschutzes oder Immunität gegen Masern oder das Vorliegen einer entsprechenden medizinischen Kontraindikation zunächst gegenüber der Leitung der Kindertageseinrichtung erbracht werden. Allerdings enthält § 20 Abs. 12 Satz 1 Nr. 1 IfSG (zusätzlich) die Befugnis des Gesundheitsamtes, sich ebenfalls die entsprechenden Nachweise von Personen vorlegen zu lassen, die in Gemeinschaftseinrichtungen nach § 33 Nr. 1 bis 3 IfSG (dazu gehören auch Kindertageseinrichtungen) betreut werden.

Die genannte Regelung hat dabei nicht nur die Fälle im Blick, in denen dem Gesundheitsamt „Impfverweigerer“ gemeldet werden. Ebenso fallen Konstellationen in den Anwendungsbereich der Norm, in denen das Gesundheitsamt von einer Einrichtung geprüfte (und gegebenenfalls sogar akzeptierte) Nachweise selbst überprüfen will oder es von Amts wegen die Einhaltung der Vorschrift des § 20 IfSG durch bestimmte Einrichtungen kontrollieren möchte.[53] Die Vorschrift soll das Gesundheitsamt auch in die Lage versetzen, die Einhaltung der Pflichten aus § 20 Abs. 8 bis 11 IfSG zu kontrollieren und auf dieser Grundlage über das Ergreifen von (eigenen) Maßnahmen entscheiden zu können.[54]

Was das Zeitmoment betrifft, mögen betroffene Personen darauf vertrauen, dass es mit der Vorlage der Nachweise bei der Einrichtung sein Bewenden hat. Die im Gesetz ausdrücklich geregelte Befugnis des Gesundheitsamtes zur eigenständigen Kontrolle (siehe oben) wird dadurch aber nicht beschränkt. § 20 Abs. 12 Satz 1 IfSG ist auch keine zeitliche Vorgabe zu entnehmen, dass das Gesundheitsamt stichprobenartige Kontrollen im engen zeitlichen Zusammenhang mit der Aufnahme in die Einrichtung durchführen muss.

Da die Nachweispflichten aus § 20 Abs. 8 ff. IfSG nicht nur bei Betreuung in einer Kindertageseinrichtung, sondern anschließend in der Schule (weiter) gelten, erscheint auch eine spätere Kontrolle der Nachweise durch die Gesundheitsämter noch zweckmäßig, um der oben beschriebenen Regelung gerecht zu werden.

[53] Siehe hierzu Bundestags-Drucksache 19/13452, S. 30: „stichprobenartige Kontrollen in solchen Einrichtungen“; Niedersächsisches Oberverwaltungsgericht, Beschluss vom 22. Juni 2022, 14 ME 258/22, BeckRS 2022, 14159, Rn. 19.

[54] Gerhardt, in: ders., Infektionsschutzgesetz, 6. Aufl. 2022, § 20 IfSG, Rn. 112.

Vor diesem Hintergrund konnte ich die beschriebenen stichprobenartigen Kontrollen datenschutzrechtlich nicht missbilligen.

4.7 Tätigkeit einer Pharmazierätin oder eines Pharmazierates – Wer ist datenschutzrechtlich Verantwortlicher?

Die Überwachung von Apotheken gehört in Bayern zu den Aufgaben der Kreisverwaltungsbehörden. Da diese Behörden regelmäßig kein pharmazeutisches Personal beschäftigen, setzt der Landesgesetzgeber auf die Fachkunde ausgewählter niedergelassener Apothekerinnen und Apotheker, welche die Kreisverwaltungsbehörden als Sachverständige unterstützen.

Diese Apothekerinnen und Apotheker werden von der zuständigen Regierung im Einvernehmen mit der Landesapothekerkammer bestellt; sie führen die Bezeichnung „Pharmazierätin“ oder „Pharmazierat“ und stehen in einem Ehrenbeamtenverhältnis zum Freistaat (vgl. Art. 2 Abs. 3 Gesundheitsdienstgesetz – GDG, Nr. 3 Bekanntmachung des Bayerischen Staatsministeriums für Gesundheit und Pflege über den Vollzug arzneimittel- und apothekenrechtlicher Vorschriften bei öffentlichen Apotheken[55]).

Im Rahmen meiner Kontrolltätigkeit hat sich die Frage ergeben, welche Stelle als datenschutzrechtlich **Verantwortlicher** im Sinne von Art. 4 Nr. 7 DSGVO anzusehen ist, wenn eine Pharmazierätin oder ein Pharmazierat im Rahmen der Überprüfung einer Apotheke tätig wird. Nach der Definition der Datenschutz-Grundverordnung ist 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**, als Verantwortlicher anzusehen. Bei der vorliegenden Fallkonstellation war die Zuordnung, wer datenschutzrechtlich Verantwortlicher ist, nicht von vornherein eindeutig:

Eine Pharmazierätin oder ein Pharmazierat wird – wie bereits oben beschrieben – gemäß Art. 2 Abs. 3 Satz 1 GDG als Sachverständige oder Sachverständiger tätig und ist in diesem Zusammenhang für die Überwachung hinsichtlich der Sicherstellung der ordnungsgemäßen Arzneimittelversorgung der Bevölkerung zuständig. Einer sachverständigen Person ist grundsätzlich immanent, dass sie auf einem bestimmten Fachgebiet eine besondere Fachkunde besitzt.

Aus diesem Umstand kann grundsätzlich auch auf eine gewisse eigenverantwortliche Erledigung der übertragenen Aufgabe geschlossen werden. Zudem ist wohl anzunehmen, dass es sich bei der einer Pharmazierätin oder einem Pharmazierat übertragenen Tätigkeit um eine solche hoheitlicher Art handeln dürfte. Dies spräche dafür, dass Art. 1 Abs. 4 BayDSG zur Anwendung kommt und die **Pharmazierätin oder der Pharmazierat** im Rahmen der hoheitlichen Aufgabenwahrnehmung als eigene verantwortliche (öffentliche) Stelle angesehen werden könnte. Auch die **Regierung** als bestellende Behörde gemäß Art. 2 Abs. 3 Satz 1 GDG könnte als datenschutzrechtlich Verantwortlicher grundsätzlich in Betracht kommen.

Allerdings wird eine Pharmazierätin oder ein Pharmazierat bei der Überwachung der Apotheken im Auftrag der zuständigen **Kreisverwaltungsbehörde** tätig. Der

[55] Vom 7. Januar 2016 (AllMBl. S. 7).

Wortlaut von § 2 Abs. 2 Satz 2 sowie § 3 Abs. 1 Satz 2 Arzneimittelüberwachungszuständigkeitsverordnung sowie Nr. 4.1 Satz 1 der oben erwähnten Bekanntmachung, der jeweils von „bedienen“ spricht, lässt den Schluss zu, dass die Kreisverwaltungsbehörde als Verantwortlicher und die Pharmazierätin oder der Pharmazierat als in die Aufgabenerfüllung der Kreisverwaltungsbehörde eingebunden anzusehen ist, da sie oder er eine mit der Rolle von bei der Kreisverwaltungsbehörde beschäftigten Personen in hohem Maße vergleichbare Stellung innehat.

Vor diesem Hintergrund ist die beauftragende Kreisverwaltungsbehörde als (alleiniger) datenschutzrechtlich Verantwortlicher zu betrachten. Auch die in der genannten Bekanntmachung vorgesehene „Eingliederung“ der Pharmazierätin oder des Pharmazierates in das entsprechende Prüfverfahren einer Apotheke durch die Kreisverwaltungsbehörde (zum Beispiel Vorgaben hinsichtlich Prüfungsumfang sowie unverzügliche Zuleitung einer Niederschrift über die stattgefundene Besichtigung) spricht für diese Einordnung.

Die beiden Regierungen, die in Bayern für die Bestellung einer Pharmazierätin oder eines Pharmazierates zuständig sind (siehe Art. 2 Abs. 3 Satz 2 GDG), haben meine Einschätzung geteilt.

4.8 Videoüberwachung bei kritischen Infrastruktureinrichtungen

Eine Einrichtung der kritischen Infrastruktur im Sinne der BSI-Kritisverordnung (BSI-KritisV) fragte bei mir an, welche Regelungen für die Videoüberwachung gelten würden und ob sich rechtliche Besonderheiten für die Videoüberwachung aus dieser Eigenschaft ergäben. Insbesondere bezog sich die Anfrage auf die Rechtsgrundlage der Videoüberwachung, die Prüfung der Gefahrensituation und die Verhältnismäßigkeit der Maßnahme. Die Einrichtung plante, einen Serverraum mit Videotechnik zu überwachen.

4.8.1 Gesetzliche Rechtsgrundlage

Videoüberwachungen bayerischer öffentlicher Stellen müssen – soweit personenbezogene Daten verarbeitet werden – auf eine Rechtsgrundlage im Sinne von Art. 6 Abs. 1 DSGVO gestützt werden – unabhängig davon, ob es sich um eine kritische Infrastruktureinrichtung handelt oder nicht. Gemäß Art. 6 Abs. 3 Satz 1 Buchst. b DSGVO werden Rechtsgrundlagen für die Verarbeitungen gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. c und e DSGVO mitgliedstaatliches Recht festgelegt. Die Zulässigkeit einer Videoüberwachung zum Zweck der Eigensicherung durch eine bayerische öffentliche Stelle richtet sich nach Art. 24 BayDSG. Anders als von der anfragenden Einrichtung kritischer Infrastruktur erwogen, können das IT-Grundschutz-Kompendiums und dazu veröffentlichter Checklisten des Bundesamts für Sicherheit in der Informationstechnik nicht die Rolle einer Rechtsgrundlage übernehmen. Diese Dokumente enthalten zwar hilfreiche technische und organisatorische Vorgaben, die auch bei der Planung und dem Betrieb einer Videoüberwachungsanlage von Nutzen sind. Sie haben aber nicht die Qualität mitgliedstaatlichen Rechts, die Art. 6 Abs. 3 Satz 1 Buchst. b DSGVO grundsätzlich voraussetzt.

4.8.2 Anforderungen an die Gefahrensituation

Videoüberwachungen im Rahmen von Art. 24 BayDSG dienen der Gefahrenabwehr und verfolgen in erster Linie präventive Zwecke. Deshalb setzen sie das Vorliegen einer Gefahrensituation voraus. In meiner einschlägigen Orientierungshilfe[56] habe ich dazu ausgeführt, dass eine Gefahrensituation im Einzelfall anhand einer Prognose festzustellen ist.

4.8.2.1 Vorfallsdokumentation als Regelfall

Zur Abgabe einer Gefahrenprognose ist die Erstellung einer Vorfallsdokumentation der Regelfall. Insoweit hat sich der Bayerische Verwaltungsgerichtshof meiner Ansicht angeschlossen.[57] Hierfür werden in einer strukturierten Sammlung aus tatsächlichen Anhaltspunkten einzelne Begebenheiten und ihre Auswirkungen im Hinblick auf die gesetzlichen Schutzziele in einem bestimmten räumlichen Kontext aufgeführt, gegebenenfalls ergänzt um Nachweise wie Anzeigen, Beschwerden, Schadensmeldungen oder polizeiliche Ermittlungsberichte.

Videoüberwachungen gemäß Art. 24 BayDSG können aber ausnahmsweise auch zulässig sein, wenn es in der Vergangenheit noch nicht zu einem Vorfall oder einer Schädigung kam. In derartigen Fällen muss die Gefahrensituation auf andere Weise dargelegt werden, soweit es sich nicht um einen Ort handelt, an dem Gefahren für die Rechtsgüter immanent sind.[58]

4.8.2.2 Gefahrimmanente Orte

Soweit Gefahrensituationen bestimmten Orten immanent sein können, handelt es sich dabei um Orte mit einer atypischen „Schadensneigung". Zu denken ist hier insbesondere an eine ortsgebundene sächliche Gefahrenquelle im Bereich einer öffentlichen Einrichtung, beispielsweise ein schlecht einsehbarer Abschnitt im Beckenbereich eines öffentlichen Schwimmbads. Eine solche Situation liegt an oder in einem Serverraum allerdings typischerweise nicht vor.

4.8.2.3 Konkrete Bedrohungs- oder Gefährdungslage

Eine Gefahrensituation kann auch auf andere Weise dargelegt werden, insbesondere bei einer atypischen Bedrohungs- oder Gefährdungslage im Einzelfall. Dies gilt namentlich dann, wenn ein außergewöhnlich gravierender Schaden zu besorgen ist, der sich nicht oder nur mit einem sehr großen Aufwand beheben lässt. Dann muss eine Schädigung nicht erst abgewartet werden, um einen Vorfall dokumentieren zu können. Ein Beispiel ist das Risiko, dass Personen mit Gewalt auf die Außenmauer einer Justizvollzugsanstalt einwirken, um einem Gefangenen die Möglichkeit zum Verlassen der Einrichtung zu eröffnen.

[56] Vgl. Bayerischer Landesbeauftragter für den Datenschutz, Videoüberwachung durch bayerische öffentliche Stellen, Orientierungshilfe, Stand 2/2020, Rn. 46, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

[57] Vgl. Bayerischer Verwaltungsgerichtshof, Urteil vom 30. Mai 2023, 5 BV 20.2104, BeckRS 2023, 12517, Rn. 45.

[58] Vgl. Bayerischer Verwaltungsgerichtshof, Urteil vom 30. Mai 2023, 5 BV 20.2104, BeckRS 2023, 12517, Rn. 46.

Eine Analyse und Bewertung der Gefahrensituation insbesondere in räumlicher und zeitlicher Hinsicht ist allerdings auch in solchen Fällen zwingend. Der Verantwortliche muss seine Rechenschaftspflicht für die Rechtmäßigkeit der Verarbeitung gemäß Art. 5 Abs. 2, Abs. 1 Buchst. a DSGVO erfüllen können. Die bloße Behauptung einer Gefahr oder eines allgemeinen Unsicherheitsgefühls reichen nicht aus. Die Eigenschaft einer öffentlichen Einrichtung als kritische Infrastruktur kann die Prüfung der Gefahrensituation zwar nicht ersetzen, aber bei deren Einschätzung als „Begründungshilfe" herangezogen werden.

Um eine Gefahrenlage auch ohne Vorfallsdokumentation zu beschreiben, muss sie in vergleichbarer Art und Weise wie mit einer (ausreichenden) Vorfallsdokumentation eingegrenzt werden können. Das bedeutet, dass die Gefahr und die Modalitäten der gegenwärtigen und der erwarteten Situation (auch ohne vergangene Vorfälle) möglichst genau umrissen werden müssen. Gelingt dies nicht und wird nur ein diffuses Gefahrenszenario ohne tatsächliche Anhaltspunkte „ins Blaue" behauptet („es könnte irgendwas, irgendwann, irgendwo passieren"), ist dies ein starkes Indiz dafür, dass eine für eine Videoüberwachung gemäß Art. 24 Abs. 1 BayDSG erforderliche Gefahrensituation nicht vorliegt.

Zu beschreiben sind die derzeitige Situation und die Hintergründe, die zur Entwicklung der Gefahr geführt haben. Zu beschreiben ist insbesondere der prognostizierte Geschehensablauf nach Art der Angriffshandlung (etwa erwartete Körperverletzung, Einbruch und Diebstahl, Verschaffen eines unbemerkten Zugriffs usw.), der erwartete Verletzungserfolg bezüglich der Schutzziele gemäß Art. 24 Abs. 1 Nr. 1 und Nr. 2 BayDSG, die erwartete Dauer und eine mögliche zeitliche Begrenzung der Gefahr (Tages- und/oder Nachtzeit, nur zu bestimmten Ereignissen oder Jahreszeiten), der Ort der Gefahr (möglichst genaue räumliche Eingrenzung), die Schwere (insbesondere Behebbarkeit) möglicher Folgen unter Berücksichtigung von Fernwirkungen, ferner ihre Dauer (einmalig, wiederkehrend, gegebenenfalls dauerhaft). Einzuschätzen ist zudem die Eintrittswahrscheinlichkeit dieser Folgen.

Zur Beschreibung der Gefahrensituation können auch vergleichbare Bezugsfälle herangezogen werden. Dazu müssen aber die Gefahrensituationen tatsächlich vergleichbar und übertragbar sein. So wird etwa die Gefahr einer Gefangenenbefreiung vergleichbar in verschiedenen anderen Justizvollzugsanstalten bestehen, weil bereits der Aufenthalt von Strafgefangenen risikoerhöhend wirkt. Ein Einbruch in eine andere öffentliche Stelle kann aber nicht ohne weiteres deshalb angenommen werden, weil es in einem beliebigen anderen Gebäude schon einmal zu einem Einbruch gekommen ist. Die bloße Behauptung einer Gefährdungslage ersetzt nicht ihr tatsächliches Vorliegen. Vielmehr sind weitere Gefahrermittlungen erforderlich. Soll eine Gefährdung mit vergleichbaren Vorfällen bei anderen Stellen begründet werden, bedarf es auch hierzu regelmäßig einer Dokumentation der Fremdvorfälle und einer Prüfung, welche die Vergleichbarkeit der Risiken in den Blick nimmt.

Bei der Bestimmung und Eingrenzung der Gefahrensituation ist entsprechend meiner Orientierungshilfe[59] zu beachten, dass das gefährdete Rechtsgut und das Ausmaß des drohenden Schadens mit dem zu fordernden Wahrscheinlichkeitsgrad in Beziehung stehen.

[59] Vgl. Bayerischer Landesbeauftragter für den Datenschutz, Videoüberwachung durch bayerische öffentliche Stellen (Fn. 56), Rn. 48.

Bei der Beurteilung der Gefahrensituation kann es eine Rolle spielen, dass der zu überwachende Bereich zu einer Einrichtung gehört, die kritische Dienstleistungen im Sinne der BSI-Kritisverordnung erbringt. Bei kritischen Dienstleistungen ist gemäß § 1 Abs. 1 Nr. 3 BSI-KritisV zu beachten, dass deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde. Der Gesetzgeber betont die Bedeutung von kritischer Infrastruktur für das Funktionieren des Gemeinwesens und erkennt ein besonderes Gefährdungspotential.

Soweit sich die Videoüberwachung im konkreten Fall auf Serverräume der Einrichtung kritischer Infrastruktur bezog, müsste der datenschutzrechtlich Verantwortliche im Einzelfall die oben dargestellten Aspekte prüfen. Das Risiko eines Hackerangriffs über das Internet könnte beispielsweise nicht mittels Videoüberwachung gemindert werden, so dass sich die Frage nach einer alternativen Angriffsart stellt. Die Gefahrensituation ist dabei mit Blick auf den Verarbeitungszweck der Videoüberwachung als verhaltenslenkende, risikomindernde, präventive Maßnahme zu prüfen.

Im Hinblick auf die Schadensfolgen können bei kritischen Infrastruktureinrichtungen Besonderheiten zu berücksichtigen sein, wobei das Ausmaß des potentiellen Schadens im Falle einer Schädigung ebenfalls möglichst genau beschrieben werden muss. Könnte ein gezielter Angriff auf Server der Einrichtung etwa zu einem dauerhaften Systemausfall führen, hätte dies mitunter erhebliche Schadensfolgen für Dritte, die über den örtlichen Schaden bei der Einrichtung selbst hinausgingen. Überdies könnten im Schadensfall auch andere Rechtsgüter als die öffentliche Einrichtung selbst betroffen sein. Erhebliche Schadensfolgen und die gefährdeten, sensiblen Datensätze als Teil der öffentlichen Einrichtung im Sinne von Art. 24 Abs. 1 Nr. 2 BayDSG könnten gegebenenfalls eine geringe Eintrittswahrscheinlichkeit ausgleichen. Vor diesem Hintergrund wäre zu prüfen, ob auch bei niedriger Eintrittswahrscheinlichkeit von einer Gefahrensituation ausgegangen werden kann, die eine Videoüberwachung gemäß Art. 24 Abs. 1 BayDSG legitimiert.

4.8.3 Verhältnismäßigkeit der Videoüberwachung

Soweit eine Gefahrenlage nach eingehender Prüfung unter Beachtung der Besonderheiten der kritischen Infrastruktureinrichtung und das Vorliegen der übrigen Tatbestandsvoraussetzungen von Art. 24 Abs. 1 BayDSG angenommen werden kann, wird auf der Rechtsfolgenseite nur ein verhältnismäßiger Rechtseingriff in Bezug auf die konkrete Ausgestaltung der Videoüberwachungsanlage legitimiert. Bei der Verhältnismäßigkeitsprüfung ergeben sich grundsätzlich keine Besonderheiten aus der Tatsache, dass es sich bei der öffentlichen Stelle um eine kritische Infrastruktureinrichtung handelt. Eine flächendeckende Videoüberwachung in allen Räumlichkeiten der Einrichtung wäre etwa nicht erforderlich, wenn sich die Gefahr allein auf einen Serverraum bezieht.

Es bietet sich an, die Videoüberwachung und die vorzunehmende Prüfung der Verhältnismäßigkeit als Teil eines Sicherheitskonzepts zu begreifen. Ob es neben sonstigen Sicherheitsmaßnahmen wie Alarmanlagen, Zugangsschutz mit Schließ- und Berechtigungskonzept, technischem Schutz von Computersystemen usw. noch einer zusätzlichen Videoüberwachung bedarf, ergibt eine Prüfung unter Einbeziehung aller relevanten Faktoren vor Ort. Dabei sind auch mögliche Gefährdungslagen in den Blick zu nehmen und zu untersuchen, ob eine Videoüberwachung überhaupt eine abschreckende Wirkung entfalten kann.

4.8.4 Fazit

Die Videoüberwachung von kritischen Infrastruktureinrichtungen unterfällt grundsätzlich denselben rechtlichen Vorgaben nach Art. 24 BayDSG, wie sie auch für andere bayerische öffentliche Stellen gelten. Bei der Prüfung der Gefahrensituation können sich aus der Tatsache der kritischen Infrastruktur relevante Besonderheiten im Einzelfall ergeben. Dies entbindet die öffentliche Stelle aber nicht von ihrer Rechenschaftspflicht und der genauen Prüfung, bevor mit der Videoüberwachung begonnen wird. Bei der Feststellung einer Gefahrenlage ohne Vorfallsdokumentation muss die Gefahr in vergleichbarer Art und Weise wie bei einer (ausreichenden) Vorfallsdokumentation eingegrenzt werden können. Die bloße Behauptung einer Gefahrenlage reicht für eine Videoüberwachung gemäß Art. 24 BayDSG nicht aus.

5 Personalverwaltung

5.1 Erklärung zu Vorstrafen und Disziplinarverfahren in Berufungsverfahren auf Professuren

Bei Stellenbesetzungsverfahren im öffentlichen Dienst gilt der Grundsatz der „Bestenauslese". Diese im Grundgesetz (GG) verankerte Vorgabe (vgl. Art. 33 Abs. 2 GG) besagt im Wesentlichen, dass öffentliche Ämter allein nach Eignung, Befähigung und fachlicher Leistung zu besetzen sind. Um eine fundierte Auswahlentscheidung treffen zu können, muss sich ein Dienstherr oder öffentlicher Arbeitgeber im Vorfeld daher aussagekräftige Informationen über die Bewerberinnen und Bewerber verschaffen. Diese müssen also teils sensible Informationen über sich offenlegen, um ihre Chancen im Wettbewerb um ein öffentliches Amt zu wahren.

Auch in Stellenbesetzungsverfahren ist das Datenschutzrecht zu beachten. Dies bedeutet insbesondere, dass ein Dienstherr oder öffentlicher Arbeitgeber nur solche Angaben bei Bewerberinnen und Bewerbern „abfragen" darf, die er für seine spätere Auswahlentscheidung benötigt. Bei der Verwendung von Formularen, in denen sich Bewerberinnen und Bewerber zum (Nicht-)Vorliegen bestimmter Sachverhalte erklären sollen, müssen Dienstherren und öffentliche Arbeitgeber daher besonders darauf achten, dass nicht zu viele und damit nicht erforderliche Daten erhoben werden. Dies gilt auch, wenn sich Bewerberinnen und Bewerber in einem entsprechenden Formular zu etwaigen Vorstrafen und Disziplinarverfahren erklären sollen.

5.1.1 Sachverhalt

Eine betroffene Person beschwerte sich bei mir über die Verarbeitung ihrer personenbezogenen Daten in Berufungsverfahren auf Professuren an mehreren bayerischen Hochschulen für angewandte Wissenschaften. Konkret ging es um die Verwendung von formularmäßigen Erklärungen zu möglichen Vorstrafen und (beamtenrechtlichen) Disziplinarverfahren. Der Beschwerdeführer wandte sich dabei nicht gegen die Erhebung der personenbezogenen Daten an sich, sondern gegen den konkreten Inhalt der von den Hochschulen vorgelegten und von den Bewerberinnen und Bewerbern auszufüllenden Vordrucke. Der Beschwerdeführer sollte etwa die folgende Erklärung unterschreiben:

„Ich erkläre hiermit, dass ich nicht vorbestraft bin, keine gerichtlichen Verfahren gegen mich anhängig sind, keine staatsanwaltschaftlichen Ermittlungsverfahren gegen mich laufen und – falls im öffentlichen Dienst – keine Disziplinarverfahren gegen mich durchgeführt wurden oder anhängig sind."

Der Beschwerdeführer kritisierte die unterschiedliche „Behandlung" von Vorstrafen und Disziplinarverfahren in dieser Erklärung. Während sich der Passus zu abgeschlossenen Strafverfahren ausschließlich auf solche bezog, die mit einer „Verurteilung" abgeschlossen waren, wurden Disziplinarverfahren in ihrer Gesamtheit betrachtet. Strafverfahren, die etwa bereits im Ermittlungsverfahren eingestellt wurden oder vor Gericht mit einem Freispruch endeten, hätten nicht angegeben

werden müssen. Dagegen wären auch erfolglos durchgeführte Disziplinarverfahren anzugeben gewesen, und darunter sogar solche, die auf widerlegten Vorwürfen beruhten. Die Erklärung hätte sich damit nicht auf Disziplinarverfahren beschränkt, die tatsächlich auch zu einer Disziplinarmaßnahme geführt haben.

Da mehrere Hochschulen entsprechende Erklärungsformulare verwendet hatten und daher ein hochschulübergreifendes Interesse anzunehmen war, habe ich mich im Rahmen meiner datenschutzrechtlichen Prüfung mit dem Bayerischen Staatsministerium für Wissenschaft und Kunst abgestimmt.

5.1.2 Erstes Problem: Inkonsistenz zwischen Vorstrafen und Disziplinarverfahren

In rechtlicher Hinsicht dienen die abzugebenden Erklärungen im Stellenbesetzungsverfahren dazu, die persönliche Eignung von Bewerberinnen und Bewerbern einzuschätzen (vgl. § 9 Beamtenstatusgesetz – BeamtStG, Art. 33 Abs. 2 GG). Als Rechtsgrundlage für die Datenerhebung kommt Art. 103 Satz 1 Nr. 1 Bayerisches Beamtengesetz (BayBG) in Betracht, wonach der Dienstherr personenbezogene Daten über Bewerber und Bewerberinnen verarbeiten darf, soweit dies insbesondere zu Zwecken der Personalverwaltung oder Personalwirtschaft erforderlich ist. Maßgebend war in der vorliegenden Konstellation somit vor allem die Frage, ob die in den Erklärungsformularen verwendete Formulierung das Kriterium der Erforderlichkeit hinreichend beachtet hatte. Nicht erforderliche Verarbeitungen sind von der gesetzlichen Verarbeitungsbefugnis nicht gedeckt.

Ich konnte bei meiner Prüfung nicht nachvollziehen, aus welchem Grund ohne Disziplinarmaßnahme abgeschlossene Disziplinarverfahren angegeben werden sollen, ohne Verurteilung abgeschlossene Strafverfahren jedoch nicht angegeben werden mussten. Nach meiner Einschätzung waren die Angaben in beiden Fällen nicht für Zwecke der Personalverwaltung erforderlich (Art. 103 Satz 1 Nr. 1 BayBG). Informationen über Disziplinarverfahren, die ohne eine Disziplinarmaßnahme abgeschlossen worden sind, wird mit Blick auf die Eignung einer Bewerberin oder eines Bewerbers im Regelfall keine Aussagekraft zukommen.

5.1.3 Zweites Problem: Verwertungsverbote

Ein weiteres datenschutzrechtliches Problem ergab sich bei den Erklärungsvordrucken aus der Tatsache, dass bei etwaigen Vorstrafen und Disziplinarverfahren nicht danach differenziert wird, ob diese einem Verwertungsverbot unterfallen oder nicht.

Nach § 51 Abs. 1 Bundeszentralregistergesetz (BZRG) dürfen eine Tat und die Verurteilung dem Betroffenen im Rechtsverkehr grundsätzlich nicht mehr vorgehalten und nicht zu seinem Nachteil verwertet werden, wenn die Eintragung über eine Verurteilung im Register getilgt worden oder zu tilgen ist. Die Tilgung ist von einer Tilgungsfrist (§§ 45, 46 BZRG) abhängig. § 53 BZRG beschränkt die Offenbarungspflicht der betroffenen Personen über Verurteilungen. Gemäß § 53 Abs. 1 BZRG dürfen sich Verurteilte als unbestraft bezeichnen und brauchen den Sachverhalt, welcher der Verurteilung zugrunde liegt, nicht zu offenbaren, wenn die Verurteilung nicht in das Führungszeugnis oder nur in ein Führungszeugnis nach § 32 Abs. 3, 4 BZRG aufzunehmen oder zu tilgen ist.

Da die Erklärungsvordrucke nicht in Bezug auf die Verwertbarkeit der Vorstrafen differenzierten, war nicht auszuschließen, dass die betreffenden Hochschulen personenbezogene Daten, die Verwertungsverboten unterfielen, unrechtmäßig erheben und weiterverarbeiten könnten. Um diese Problematik zu entschärfen, schlug ich dem Wissenschaftsministerium vor, folgenden Hinweis bei der Frage nach etwaigen Vorstrafen aufzunehmen:

„Unter den in § 53 BZRG genannten Voraussetzungen besteht keine Offenbarungspflicht."

Ein vergleichbares Problem stellte sich bei der Frage nach Disziplinarverfahren, da Disziplinarvorgänge nach Zeitablauf ebenfalls weitgehend einem Verwertungsverbot unterfallen, vgl. Art. 17 Abs. 1 und 4 Bayerisches Disziplinargesetz (BayDG). Das Verwertungsverbot nach Art. 17 Abs. 1 Satz 1 BayDG gilt nicht nur für weitere Disziplinarmaßnahmen, sondern erstreckt sich auch auf sonstige Personalmaßnahmen.[60] Zu beachten ist dabei, dass das Verwertungsverbot nicht nur für verhängte Disziplinarmaßnahmen gilt, sondern entsprechend auch für Disziplinarvorgänge, die nicht zu einer Disziplinarmaßnahme oder zu einer Feststellung nach Art. 33 Abs. 2 Satz 2 BayDG geführt haben (Art. 17 Abs. 4 Satz 1 BayDG).

Vor diesem Hintergrund schlug ich dem Wissenschaftsministerium die Aufnahme eines Hinweises auf den Vordrucken vor, der klarstellt, dass Disziplinarvorgänge, die einem Verwertungsverbot unterfallen, nicht zu offenbaren sind.

5.1.4 Fazit

Die Kenntnis einer Hochschule von erfolglos eingestellten Straf- oder Disziplinarverfahren eines Bewerbers oder einer Bewerberin ist in Berufungsverfahren auf Professuren grundsätzlich nicht für Zwecke der Personalverwaltung erforderlich. Soweit Vorstrafen oder Disziplinarmaßnahmen abgefragt werden, ist zumindest auf in Betracht kommende Verwertungsverbote hinzuweisen. Das Wissenschaftsministerium hat sich meiner Rechtsauffassung angeschlossen, die Hochschulen informiert und zur Verwendung neuer Musterformulierungen angehalten.

5.2 Anforderung von Unterlagen in Berufungsverfahren auf Professuren

Ein weiteres Mal hat mich die Frage beschäftigt, in welchem Umfang bayerische Hochschulen in Stellenbesetzungsverfahren personenbezogene Daten von Bewerberinnen und Bewerbern erheben dürfen. Dieses Mal ging es nicht um die Frage nach Vorstrafen und Disziplinarverfahren (siehe Nr. 5.1), sondern um die Anforderung bestimmter Unterlagen im Rahmen eines Berufungsverfahrens auf eine Professur.

Eine Person, die sich auf eine solche Professur beworben hatte, war der Ansicht, dass die betreffende Hochschule für angewandte Wissenschaften in diesem Zusammenhang zu vielfältig personenbezogene Daten von ihr erhob. Die Hochschule forderte unter anderem eine Geburtsurkunde, eine Heiratsurkunde, Geburtsurkunden der Kinder, Arbeitsverträge sowie diverse Zeugnisse und weitere Urkunden an. Die betroffene Person hatte Bedenken insbesondere in Bezug auf

[60] Vgl. Bayerischer Verwaltungsgerichtshof, Beschluss vom 10. März 2009, 7 CE 08.3022, BeckRS 2010, 45074, Rn. 24.

die Wahrung des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO).

5.2.1 Allgemeine Einstellungsvoraussetzungen und Personalaktenbezug

Ich hatte zu überprüfen, ob die Hochschule die Erhebung der jeweiligen Bewerberdaten auf eine Rechtsgrundlage stützen konnte (Grundsatz der Rechtmäßigkeit gemäß Art. 5 Abs. 1 Buchst. a, Art. 6 Abs. 1 DSGVO) und den Grundsatz der Datenminimierung gewahrt hatte.

Als Rechtsgrundlage kam die Verarbeitungsbefugnis aus Art. 103 Satz 1 Nr. 1 Bayerisches Beamtengesetz (BayBG) in Betracht. Danach darf der Dienstherr personenbezogene Daten auch über Bewerber und Bewerberinnen verarbeiten, soweit dies zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere zu Zwecken der Personalverwaltung oder Personalwirtschaft erforderlich ist. Das Kriterium der Erforderlichkeit steht in engem Zusammenhang mit dem Grundsatz der Datenminimierung. Dieser Grundsatz verlangt, dass personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen.[61] Bei diesen Kriterien kann auch das Zeitmoment eine Rolle spielen: Je nach Konstellation ist die Vorlage bestimmter Unterlagen gegebenenfalls erst in einem fortgeschrittenen Stadium eines Stellenbesetzungsverfahrens erforderlich im vorgenannten Sinne (vgl. etwa für die Anforderung und Vorlage des Personalakts anlässlich einer Bewerbung meinen 23. Tätigkeitsbericht 2008 unter Nr. 21.3; an diesen Ausführungen halte ich auch nach Geltungsbeginn der Datenschutz-Grundverordnung fest).

Die Erforderlichkeit der Verarbeitung war im Hinblick auf die einzelnen angeforderten Unterlagen zu beurteilen. Hier kam es maßgeblich auf beamten- und hochschulrechtliche Vorgaben für die Einstellung von Professorinnen und Professoren an, die an bayerischen Hochschulen gemäß Art. 58 Abs. 1 Satz 1 Bayerisches Hochschulinnovationsgesetz (BayHIG) in der Regel zu Beamtinnen und Beamten auf Lebenszeit ernannt werden. Die Einstellungsvoraussetzungen für Professorinnen und Professoren an Hochschulen für angewandte Wissenschaften sind in Art. 57 Abs. 3 BayHIG geregelt. Soweit Art. 57 Abs. 3 Satz 1 BayHIG auf die „allgemeinen dienstrechtlichen Voraussetzungen“ verweist, sind damit grundsätzlich die beamtenrechtlichen Vorgaben gemeint, die für eine Verbeamtung zwingend zu erfüllen sind, etwa die allgemeinen Voraussetzungen für die Begründung eines Beamtenverhältnisses aus § 7 Beamtenstatusgesetz (BeamtStG) oder die Ernennungskriterien gemäß § 9 BeamtStG, die für die Begründung des Beamtenverhältnisses gemäß § 8 Abs. 1 Nr. 1 BeamtStG relevant sind.

Zu beachten ist auch, dass bei der Begründung eines Beamtenverhältnisses für jede Beamtin und jeden Beamten eine Personalakte angelegt wird. Die Verarbeitung von Personalaktendaten richtet sich nach Art. 103 ff. BayBG, § 50 BeamtStG. Nach dem materiellen Personalaktenbegriff gehören zur Personalakte alle Unterlagen, die die Beamtin oder den Beamten betreffen, soweit sie mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (§ 50 Satz 2 Be-

[61] Vgl. nur Europäischer Gerichtshof, Urteil vom 9. Januar 2015, C-394/23, Rn. 49, wonach „die Voraussetzung der Erforderlichkeit der Datenverarbeitung gemeinsam mit dem Grundsatz der Datenminimierung zu prüfen ist“.

amtStG). Diese Unterlagen sind grundsätzlich zwingend in die formelle Personalakte aufzunehmen. Zweck der Personalakte ist es, ein möglichst vollständiges Bild von der Persönlichkeit des Beamten zu geben und vor allem ein lückenloses Bild der Entstehung und Entwicklung des Dienstverhältnisses in einem historischen Geschehensablauf zu vermitteln.[62]

Vor diesem Hintergrund sind Unterlagen im Berufungsverfahren nicht nur für die Prüfung der beamten- und hochschulpersonalrechtlichen Einstellungsvoraussetzungen relevant; nach Einstellung können sie auch für die spätere Aufnahme in die Personalakte erforderlich werden.

5.2.2 Geburtsurkunde

Nach dem Willen des Gesetzgebers sind Personenstandsurkunden und Unterlagen über die Staatsangehörigkeit als Personalaktendaten in den Personalakt aufzunehmen.[63] Unter die Personenstandsurkunden fallen unter anderem gemäß § 55 Abs. 1 Satz 1 Nr. 3, § 59 Personenstandsgesetz (PStG) Geburtsurkunden. Die Geburtsurkunde enthält gemäß § 59 Abs. 1 PStG zumindest die Vornamen und den Geburtsnamen sowie Ort, Tag, Stunde und Minute der Geburt. Sie wird als eine Unterlage, die Aussagen zur Persönlichkeit der Beamtin oder des Beamten enthält, und somit als Personalaktendatum angesehen.[64]

5.2.3 Heiratsurkunde und Geburtsurkunden der Kinder

Unter Personenstandsurkunden können auch Heiratsurkunden (das Gesetz spricht nunmehr in § 55 Abs. 1 Satz 1 Nr. 1, § 57 PStG von Eheurkunden) und Geburtsurkunden der Kinder fallen. Diese Urkunden enthalten nicht nur Angaben über die Persönlichkeit der Beamtin oder des Beamten, sondern können auch für die zutreffende Festsetzung der Besoldung – etwa zur Festsetzung von Familienzuschlägen gemäß Art. 43 in Verbindung mit Art. 35 Bayerisches Besoldungsgesetz (BayBesG) – relevant sein. Sie stellen daher Personalaktendaten dar.

5.2.4 Arbeitsverträge und Arbeitszeugnisse

Die Vorlage von Arbeitsverträgen im Berufungsverfahren soll insbesondere der Überprüfung der besonderen hochschulpersonalrechtlichen Einstellungsvoraussetzungen dienen. Einstellungsvoraussetzungen für Professoren und Professorinnen an Hochschulen für angewandte Wissenschaften sind gemäß Art. 57 Abs. 3 Satz 1 Nr. 3 BayHIG etwa besondere Leistungen bei der Anwendung oder Entwicklung wissenschaftlicher Erkenntnisse und Methoden in einer mindestens fünfjährigen beruflichen Praxis. Diese Praxis muss nach Abschluss des Hochschulstudiums erworben und mindestens drei Jahre außerhalb des Hochschulbereichs ausgeübt worden sein. Ob diese Voraussetzungen vorliegen und die notwendige Zeitspanne erfüllt wurde, lässt sich im Rahmen des Erforderlichen grundsätzlich anhand von Unterlagen wie Arbeitsverträgen und Arbeitszeugnissen ermitteln.

62 Vgl. Bundesverwaltungsgericht, Urteil vom 26. Januar 1978, 2 C 66/73, BeckRS 1978, 108552.
63 Vgl. Landtags-Drucksache 12/13988, S. 19.
64 Vgl. Reich, in: Reich, Beamtenstatusgesetz, 4. Aufl. 2025, § 50 Rn. 3.

5.2.5 Prüfungszeugnisse und Urkunden

Nachweise über Vor-, Aus- und Fortbildungen sowie Prüfungszeugnisse und anderweitige Befähigungsnachweise sind ebenso wie Wehr- oder Zivildienstbescheinigungen (soweit vorhanden) den Personalaktendaten zuzuordnen.[65] Ein abgeschlossenes Hochschulstudium ist ebenso wie die pädagogische Eignung Einstellungsvoraussetzung gemäß Art. 57 Abs. 3 Satz 1 Nr. 1, Abs. 1 Satz 1 Nr. 1, Nr. 2 BayHIG. Die Erhebung entsprechender Zeugnisse, Urkunden und Nachweise im Berufungsverfahren konnte die Hochschule demnach auf Art. 103 Satz 1 Nr. 1 BayBG stützen.

5.2.6 Fazit

Im Ergebnis war bei der Anforderung der oben genannten Unterlagen durch die Hochschule im Berufungsverfahren nicht von einem Verstoß gegen datenschutzrechtliche Vorgaben auszugehen. Ob bei einer Verarbeitung der Grundsatz der Datenminimierung beachtet und die Erforderlichkeit gewahrt ist, muss immer vor dem Hintergrund des jeweiligen Verarbeitungszwecks beurteilt werden. Eine Personalakte soll ein umfassendes Bild über die Beamtin oder den Beamten abgeben. Angesichts dessen können auch umfassendere Datenerhebungen zulässig sein, soweit der zuvor festgelegte Verarbeitungszweck nicht verlassen und die Anforderungen des Grundsatzes der Datenminimierung beachtet werden. Zu berücksichtigen war im konkreten Fall auch, dass die Hochschule der betroffenen Person die Möglichkeit eröffnet hatte, einzelne Dokumente erst im späteren Verlauf des Berufungsverfahrens – und damit gegebenenfalls zum Zeitpunkt einer etwaig gesteigerten „Berufungserwartung“ – nachzureichen.

5.3 Vorstellung neuer Beschäftigter in einer Informationsbroschüre

Organisatorische Erwägungen können es erfordern, bestimmte Beschäftigtendaten – insbesondere Kontaktdaten – intern offenzulegen, insbesondere um eine effiziente Zusammenarbeit verschiedener Organisationseinheiten zu gewährleisten. Zu denken ist etwa an interne Telefon- oder Organisationsverzeichnisse, wie sie vielfach in einem behördeneigenen Intranet bereitgestellt werden. Das Datenschutzrecht steht einer solchen internen Verwendung von Beschäftigtendaten grundsätzlich nicht entgegen, sofern der Dienstherr oder öffentliche Arbeitgeber nachvollziehbar begründen kann, weshalb sie für organisatorische Zwecke erforderlich ist.

Hin und wieder erwarten Dienstherren oder öffentliche Arbeitgeber aber auch, dass Beschäftigte weitere Daten – etwa Fotos – von sich intern preisgeben. Begründet wird dies mit dem Gedanken, dass sich Beschäftigte auf diese Weise besser kennenlernen und untereinander vernetzen können. Nicht zuletzt könnten hierdurch auch neue Beschäftigte zügiger integriert werden. So nachvollziehbar dieser Gedanke dem Grunde nach auch ist, dürfen bei seiner Umsetzung allerdings die Persönlichkeitsrechte der Beschäftigten nicht außer Acht gelassen und müssen datenschutzrechtliche Anforderungen eingehalten werden. So dürfen

[65] Vgl. Landtags-Drucksache 12/13988, S. 19.

etwa Fotos von Beschäftigten grundsätzlich nur mit deren Einwilligung in ein behördeneigenes Intranet eingestellt werden (vgl. hierzu bereits meinen 27. Tätigkeitsbericht 2016 unter Nr. 11.5; an diesen Ausführungen halte ich weiterhin fest).

Anlässlich einer Beschwerde hatte ich mich nun mit der Veröffentlichung personenbezogener Beschäftigtendaten in einer Informationsbroschüre zu befassen, die an verschiedene, fachlich verbundene Behörden adressiert war.

5.3.1 Sachverhalt

Ein Staatsministerium gibt regelmäßig eine Informationsbroschüre insbesondere für Beschäftigte eines bestimmten Verwaltungszweigs im eigenen Haus sowie im nachgeordneten Bereich heraus. In dieser Broschüre wurden auch neue Kolleginnen und Kollegen in Textbeiträgen und Fotos vorgestellt.

Hintergrund war – wie ich im Laufe des Beschwerdeverfahrens vom Staatsministerium erfahren habe – insbesondere die komplexe, behördenübergreifende Organisationsstruktur des betreffenden Verwaltungszweigs. Die Broschüre solle als Informations- und Vernetzungsmedium einen regelmäßigen Austausch gewährleisten. In diesem Rahmen sollte neuen Beschäftigten die Möglichkeit gegeben werden, sich mit eigens verfassten Beiträgen in der Broschüre vorzustellen.

Der Beschwerdeführer war in dem fraglichen Verwaltungszweig beschäftigt. Seine Beschäftigungsbehörde gab sowohl ein Foto von ihm als auch einen Text mit Angaben aus dem Lebenslauf an das Staatsministerium weiter. Foto und Textbeitrag wurden in einer späteren Ausgabe der Informationsbroschüre abgedruckt. Daraufhin wandte sich der Beschwerdeführer an mich. Er habe zu keinem Zeitpunkt in die Weitergabe und spätere Veröffentlichung seiner Daten eingewilligt.

Ich bat sowohl die Beschäftigungsbehörde als auch das Staatsministerium um eine Stellungnahme. Dabei wollte ich insbesondere wissen, auf welcher Rechtsgrundlage das Foto des Beschwerdeführers und der ihn betreffende Text an das Staatsministerium übermittelt und sodann im Rahmen der Broschüre veröffentlicht wurden.

Die angeschriebenen Stellen informierten mich unter anderem, dass das Einreichen der „Vorstellungsbeiträge“ für die Beschäftigten freiwillig sei und ohne Gruppendruck erfolge. Beschäftigten, die keine Beiträge einreichten, drohten keine Nachteile. Auch sei es nicht ungewöhnlich, dass sich neue Mitarbeiterinnen und Mitarbeiter in diesem Rahmen nicht vorstellten. Die Beschäftigungsbehörde trug weiter vor, dass der Beschwerdeführer auf eine Nachricht nicht reagiert habe, wonach sich Betroffene melden mögen, wenn sie mit der Veröffentlichung ihres Bildes nicht einverstanden seien.

Die Beschäftigungsbehörde und das Staatsministerium nahmen bei der jeweiligen Datenverarbeitung zunächst an, dass Einwilligungen nach Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 4 Nr. 11, Art. 7 DSGVO vorgelegen hätten. Insbesondere habe die Beschäftigungsbehörde das Schweigen des Beschwerdeführers auf die oben genannte Nachricht anfänglich als Zustimmung gewertet. Zudem seien die Beiträge entsprechend der bisherigen Praxis von den betroffenen Beschäftigten selbst verfasst worden. Beide Behörden führten allerdings weiter aus, im Nach-

gang zu der Ansicht gekommen zu sein, dass der Beschwerdeführer in die Verarbeitung seiner personenbezogenen Daten bei Erstellung und Veröffentlichung der Broschüre nicht wirksam eingewilligt hatte.

5.3.2 Fehlender Nachweis wirksamer Einwilligungen

Sowohl mit der Übermittlung des Fotos und des Vorstellungsbeitrags des Beschwerdeführers durch die Beschäftigungsbehörde an das Staatsministerium als auch mit der späteren Veröffentlichung dieser Daten in einer Ausgabe der Informationsbroschüre sind personenbezogene Daten des Beschwerdeführers verarbeitet worden. Dabei war im vorliegenden Fall für die Übermittlung dieser Daten die Beschäftigungsbehörde, für deren spätere Veröffentlichung das Staatsministerium datenschutzrechtlich Verantwortlicher.

Jede Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage. Als solche kam vorliegend nur eine Einwilligung der betroffenen Person in Betracht. Insbesondere war nicht ersichtlich – und wurde von den betreffenden Stellen auch nicht vorgetragen –, dass die Verarbeitung der Daten des Beschwerdeführers zur Aufgabenerfüllung der jeweiligen Stellen (vgl. Art. 4 Abs. 1 und Art. 5 Abs. 1 BayDSG) oder zu einem der in Art. 103 Satz 1 Nr. 1 Bayerisches Beamtengesetz (BayBG) genannten Zwecke (insbesondere zur Personalverwaltung oder Personalwirtschaft) im datenschutzrechtlichen Sinn erforderlich gewesen wäre. Soweit man in den geschilderten Vorgängen eine Übermittlung (in Form der Offenlegung) von Personalaktendaten an Dritte erblickt, setzt auch Art. 108 Abs. 4 Satz 1 BayBG grundsätzlich die Einwilligung der betroffenen Beschäftigten voraus.

Eine wirksame, insbesondere informiert und freiwillig erteilte (vgl. Art. 4 Nr. 11 DSGVO) Einwilligung muss der datenschutzrechtlich Verantwortliche aber auch nachweisen können.[66] Dies ergibt sich bereits aus seiner allgemeinen Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) und wird speziell für Verarbeitungen auf Grundlage einer Einwilligung durch Art. 7 Abs. 1 DSGVO noch einmal spezifiziert:

„Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat."

Ein besonderes Formerfordernis für Einwilligungen enthält die Datenschutz-Grundverordnung grundsätzlich nicht. Art. 4 Nr. 11 DSGVO verlangt jedoch eine „unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung"; diese Willensbekundung muss unter anderem „in informierter Weise" erfolgt sein. Mit anderen Worten muss der betroffenen Person hinreichend klar sein, worin sie einwilligt. Übertragen auf den vorliegenden Fall hätten die beiden Behörden damit nachvollziehbar darlegen müssen, dass der Beschwerdeführer mit der Verarbeitung seiner Daten gerade auch im Hinblick auf die Erstellung und spätere Veröffentlichung der Broschüre einverstanden gewesen war – genau dies hatte der Beschwerdeführer ja bestritten.

[66] Vgl. zum Folgenden auch Bayerischer Landesbeauftragter für den Datenschutz, Die Einwilligung nach der Datenschutz-Grundverordnung, Orientierungshilfe, Stand 9/2021, insbesondere Rn. 48 ff., 91 ff. und 117 ff., Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

Ein solcher Nachweis gelang den beiden Behörden vorliegend schon nach eigener Darstellung nicht. Angesichts der klaren gesetzlichen Vorgaben ist eine wirksame Einwilligung insbesondere nicht allein deshalb anzunehmen, weil eine betroffene Person einer Verarbeitung nicht aktiv „widerspricht". Damit sind die öffentlichen Stellen ihrer Rechenschaftspflicht im Hinblick auf die Rechtmäßigkeit der Verarbeitung jeweils nicht nachgekommen.

5.3.3 Ergriffene Maßnahmen

Aufgrund der Nachrichten des Beschwerdeführers an die Beschäftigungsbehörde, dass er weder einer Weitergabe noch einer Veröffentlichung seiner Daten zugestimmt habe, hat das Staatsministerium eine neue Fassung der Broschüre ohne die personenbezogenen Daten des Beschwerdeführers erstellt. Das Staatsministerium hat im Nachgang ferner allen Empfängern die Löschung der ursprünglichen Fassung der Broschüre mitgeteilt. Darüber war der Beschwerdeführer auch informiert worden. Angesichts des Gewichts der Datenschutzverstöße habe ich gegenüber beiden Behörden gleichwohl eine förmliche datenschutzrechtliche Beanstandung ausgesprochen.

Im Laufe des Verfahrens habe ich zudem ausführliche Hinweise dazu erteilt, wie die bislang praktizierte Erstellung und Veröffentlichung der Informationsbroschüre datenschutzkonform ausgestaltet werden kann. Insbesondere habe ich erläutert, wie die Einholung wirksamer – insbesondere freiwilliger und informierter – Einwilligungen im vorliegenden Zusammenhang gewährleistet werden könnte. Die beteiligten Stellen teilten allerdings mit, zukünftig keine personenbezogenen Beschäftigtendaten mehr in der Broschüre veröffentlichen zu wollen. Die Informationsbroschüre werde sich vielmehr auf Fachbeiträge beschränken. Insofern würden den Beschäftigungsbehörden des Fachbereichs auch keine Vorstellungsbeiträge neuer Mitarbeiterinnen und Mitarbeiter mehr an das Staatsministerium übermitteln. Obgleich diese Maßnahme aus datenschutzrechtlicher Perspektive nicht zwingend erforderlich erschien, konnte ich hiergegen natürlich keine Einwände vorbringen.

5.4 Beschäftigtendaten in der (auch weltweiten) Öffentlichkeit

Ob und in welchem Umfang Beschäftigtendaten einer breiteren Öffentlichkeit zugänglich gemacht werden dürfen, ist im Beschäftigtendatenschutz eine vieldiskutierte Frage (vgl. zuletzt in meinem 33. Tätigkeitsbericht 2023 unter Nr. 7.5 und Nr. 7.6). Häufig stellt sich heraus, dass eine Offenlegung nicht oder jedenfalls nicht vollständig von einer Rechtsgrundlage gedeckt ist – so auch in einem weiteren Fall, in dem eine bayerische Gemeinde personenbezogene Daten ihrer Beschäftigten gleich dreifach öffentlich gemacht hat.

5.4.1 Sachverhalt

— Die Gemeinde stellte unter anderem Kontaktdaten von Ansprechpersonen im Rathaus – konkret: Namen, Funktionen, dienstliche Telefonnummern und dienstliche E-Mail-Adressen – auf ihre **Internetseite**. Bei drei längerfristig erkrankten Beschäftigten fand sich ein Hinweis, dass diese derzeit nicht im Haus seien und bei Bedarf die Organisationseinheit kontaktiert

werden könne. Später wurden die Kontaktdaten der betroffenen Beschäftigten entfernt; der Name und ein Vertretungshinweis verblieben aber auf der Internetpräsenz.

— Nachfolgend äußerte sich der erste Bürgermeister auf einer **Bürgerversammlung** zum mehrmonatigen „Ausfall“ von drei Beschäftigten der Gemeinde. Zwar wurden die Beschäftigten dabei nicht namentlich erwähnt, jedoch deren Anzahl und deren „Gesamt“-Arbeitsausfall in Arbeitsstunden pro Monat.

— Danach wurde der Bürgermeister in einem **Zeitungsartikel** zu einem Krankheitsfall in der Gemeindeverwaltung und einem damit einhergehenden Ausfall personeller Ressourcen zitiert. Der Bürgermeister nahm dabei auf das konkret betroffene Amt und dessen Neubesetzung innerhalb der Gemeinde Bezug, ohne allerdings Beschäftigtennamen zu nennen.

Die betroffenen Beschäftigten wandten sich später mit datenschutzrechtlichen Beschwerden an mich. Bei der Bearbeitung hatte ich insbesondere zu prüfen, inwieweit die Gemeinde bei den geschilderten Vorgängen jeweils personenbezogene Daten ihrer Beschäftigten offengelegt hat und ob dafür Rechtsgrundlagen vorhanden waren.

5.4.2 Abwesenheitsvermerk auf der Internetseite der Gemeinde

Veröffentlichen bayerische öffentliche Stellen personenbezogene Daten von Beschäftigten, um eine Kontaktaufnahme zu erleichtern, verarbeiten sie diese Daten grundsätzlich zu organisatorischen Zwecken. Die Veröffentlichung von personenbezogenen Sachaktendaten Beschäftigter – insbesondere von Namen, Kontaktdaten, Funktion und Amtsbezeichnung – kann auf Art. 5 Abs. 1 Satz 1 Nr. 1 Var. 1 BayDSG gestützt werden, wenn sie zur Erfüllung einer Aufgabe erforderlich ist, die der übermittelnden öffentlichen Stelle obliegt. Zu den Aufgaben einer bayerischen öffentlichen Stelle gehört es auch, Bürgerinnen und Bürger darüber zu informieren, welche Beschäftigten die richtigen Ansprechpersonen für ihre Anliegen sind (siehe meine Ausführungen im 33. Tätigkeitsbericht 2023 unter Nr. 7.5.1). Daher müssen Beschäftigte, die eine Funktion mit Außenwirkung wahrnehmen, eine Veröffentlichung etwa ihres Namens, ihrer dienstlichen Kontaktdaten wie Telefonnummer und E-Mail-Adresse und ihres Zuständigkeitsbereichs hinnehmen.

Abwesenheitshinweise auf der Internetseite sind aber zur Aufgabenerfüllung regelmäßig nicht erforderlich. Zwar mögen derartige Hinweise nützlich sein, damit Bürgerinnen und Bürger den direkten Kontakt nur mit tatsächlich anwesenden Beschäftigten suchen. Die bloße Nützlichkeit oder Förderlichkeit allein ist aber nicht ausreichend, um eine für die Aufgabenerfüllung erforderliche Verarbeitung personenbezogener Daten anzunehmen.[67] Ist absehbar, dass Beschäftigte für einen längeren Zeitraum abwesend sind, erscheint die Einrichtung von E-Mail-Abwesenheitsnotizen und Telefonumleitungen als ein effektiveres Mittel, das die Datenschutzgrundrechte der betroffenen Beschäftigten weniger beeinträchtigt. Auch die ersatzlose Löschung der personenbezogenen Daten von der Webseite

[67] Vgl. Bayerisches Oberstes Landesgericht, Beschluss vom 6. August 2020, 1 VA 33/20, BeckRS 2020, 18859, Rn. 60.

kann ein Mittel sein, um Bürgerinnen und Bürger vor erfolglosen Kontaktversuchen zu bewahren, ohne zugleich die Abwesenheit der betroffenen Beschäftigten hervorzuheben.

Vor diesem Hintergrund bin ich zu der Auffassung gelangt, dass die ins Internet gestellten Abwesenheits- und Vertretungshinweise für die Aufgabenerfüllung der Gemeinde nicht erforderlich waren. Die Gemeinde konnte diese Hinweise daher nicht auf Art. 5 Abs. 1 Satz 1 Nr. 1 Var. 1 BayDSG stützen.

5.4.3 Äußerungen zum mehrmonatigen Ausfall von Beschäftigten auf der Bürgerversammlung

Die öffentliche Äußerung des Bürgermeisters der Gemeinde auf der Bürgerversammlung bezüglich des mehrmonatigen Ausfalls von drei Beschäftigten stellt jedenfalls in Kombination mit den unter Nr. 5.4.2 zuvor nach außen getragenen Abwesenheitshinweisen eine Verarbeitung personenbezogener Daten in Form einer Offenlegung dar.

Personenbezogen sind Daten gemäß Art. 4 Nr. 1 DSGVO bereits dann, wenn sich Informationen auf eine (lediglich) identifizierbare natürliche Person beziehen, wobei auch eine indirekte Zuordnung ausreicht. Laut Erwägungsgrund 26 Satz 3 DSGVO sind bei der Feststellung der Identifizierbarkeit einer natürlichen Person alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind (Erwägungsgrund 26 Satz 4 DSGVO).

Für das Vorliegen personenbezogener Daten ist es daher ausreichend, wenn Informationen, die an sich noch keinen Schluss auf eine bestimmte Person zulassen, erst in Verbindung mit anderen Informationen – insbesondere in Form von „Zusatzwissen“ – die Identifizierung ermöglichen. Dabei darf der Aufwand, der für die Identifizierung erforderlich ist, nicht unverhältnismäßig hoch sein. Zwar hat der Bürgermeister eine geschlechtsneutrale Formulierung gewählt, um Identitäten der monatelang ausfallenden Beschäftigten nicht preiszugeben. Für Außenstehende war jedoch mithilfe der noch auf der Internetseite der Gemeinde angebrachten Abwesenheitsnotizen bei den Kontaktdaten der betroffenen Personen ersichtlich, wer konkret gemeint war.

Freilich ist im Einzelnen noch nicht abschließend geklärt, inwieweit das Wissen und die Möglichkeiten anderer Personen zur Identifizierung betroffener Personen Berücksichtigung finden.[68] Dies wirkt sich vorliegend aber nicht aus, weil die betroffenen Personen für die Gemeinde als dem datenschutzrechtlich Verantwortlichen ohnehin feststanden, während Bürgerinnen und Bürgern eine Identifizierung mit dem verhältnismäßig geringen Aufwand einer Internetrecherche möglich war. Der

[68] Vgl. zu Einzelheiten, Bayerischer Landesbeauftragter für den Datenschutz, Wann ist eine natürliche Person identifizierbar?, Aktuelle Kurz-Information 53, Stand 1/2024, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek“.

Bürgermeister hat mit seiner Äußerung also auch ohne Namensnennung personenbezogene Daten der betroffenen Beschäftigten offengelegt. Zu den Gründen des Ausfalls hat er sich zwar nicht näher geäußert; da längere Ausfallzeiten aber oftmals auf gesundheitliche Ursachen zurückzuführen sind, wäre es nicht fernliegend gewesen, in der Äußerung zugleich eine Offenlegung von Gesundheitsdaten und gegebenenfalls auch Personalaktendaten zu erblicken, die eine qualifizierte Rechtsgrundlage benötigt.

Die Gemeinde konnte mir nicht darlegen, dass die Kommunikation der personenbezogenen Daten zur Erfüllung ihrer Aufgaben erforderlich gewesen wäre. Eine Bürgerversammlung dient zwar der Erörterung gemeindlicher Angelegenheiten (Art. 18 Abs. 1 Satz 1 Gemeindeordnung). Vor diesem Hintergrund bestünden keine datenschutzrechtlichen Bedenken gegen die Erörterung der allgemeinen Personalsituation ohne Personenbezug. Die Zweckbestimmung der Bürgerversammlung legitimiert aber nicht die vorliegende Offenlegung personenbezogener Beschäftigtendaten.

5.4.4 Äußerungen zu einem Krankheitsfall in der Gemeindeverwaltung im Rahmen der Pressearbeit

Soweit der Bürgermeister im Rahmen der Pressearbeit auf einen Krankheitsfall im Rathaus und die Neubesetzung des konkret genannten Amts innerhalb der Gemeinde Bezug nahm, war eine Identifizierung der betroffenen Person mit Hilfe der Internetpräsenz oder auf Grund von „Rathauswissen“ kommunalpolitisch interessierter Bürgerinnen und Bürger möglich. Der Bürgermeister hat also auch in diesem Kontext ohne Namensnennung personenbezogene Daten offengelegt.

Krankheitsbedingte Fehlzeiten sind Personalaktendaten, deren Verarbeitung den personaldatenschutzrechtlichen Vorgaben gemäß § 50 Beamtenstatusgesetz, Art. 103 ff. Bayerisches Beamtengesetz (BayBG) entsprechen muss. Die Vorschriften finden gemäß Art. 145 Abs. 2 BayBG auch auf vertraglich Beschäftigte im öffentlichen Dienst grundsätzlich entsprechende Anwendung. Die Tatsache der Erkrankung selbst ist ein Gesundheitsdatum im Sinne von Art. 4 Nr. 15 DSGVO, das zu den besonderen Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO gehört und dessen Verarbeitung nur unter zusätzlichen Voraussetzungen gemäß Art. 9 Abs. 2 DSGVO, Art. 8 BayDSG zulässig ist.

Eine Auskunft an die Presse zur Erkrankung der betroffenen Person hätte vorliegend gemäß Art. 108 Abs. 4 BayBG, Art. 9 Abs. 2 Buchst. a DSGVO grundsätzlich nur mit ihrer ausdrücklichen Einwilligung erteilt werden dürfen; für einen Ausnahmetatbestand nach Art. 108 Abs. 4 Satz 1 Halbsatz 2 BayBG war im konkreten Fall nichts ersichtlich (siehe zu Art. 108 Abs. 4 BayBG meine Ausführungen im 33. Tätigkeitsbericht 2023 unter Nr. 7.6). Eine – im Beschäftigungsverhältnis ohnehin nur selten freiwillig und damit wirksam (vgl. Art. 4 Nr. 11 DSGVO) erteilte – Einwilligung wurde nicht eingeholt. Ein Rückgriff auf Art. 5 Abs. 1 Satz 1 Nr. 1 Var. 1 BayDSG ist durch die abschließende fachgesetzliche Regelung versperrt (vgl. Art. 1 Abs. 5 BayDSG). Die Erkrankung der betroffenen Person wurde daher ohne Rechtsgrundlage offengelegt.

5.4.5 Ergebnis

Die Gemeinde hat damit in drei Fällen die Anforderung missachtet, personenbezogene Daten nur mit Rechtsgrundlage offenzulegen. Der Abwesenheitsvermerk auf der gemeindlichen Internetseite zu den betroffenen Beschäftigten war ebenso wenig zur Aufgabenerfüllung erforderlich wie die der Gemeinde zurechenbare Äußerung des Bürgermeisters auf einer Bürgerversammlung zum Ausfall dreier Beschäftigter. Die auf ein konkretes Amt und dessen Neubesetzung bezogene Äußerung des Bürgermeisters zu einem Krankheitsfall in einem Zeitungsartikel war nicht von der erforderlichen fachgesetzlichen Rechtsgrundlage gedeckt.

Im Ergebnis habe ich aufgrund der festgestellten unrechtmäßigen Verarbeitungen personenbezogener Daten gegenüber der Gemeinde eine förmliche datenschutzrechtliche Beanstandung ausgesprochen (Art. 16 Abs. 4 Satz 1 BayDSG).

5.5 Veröffentlichung privater Kontaktdaten von Bereichslehrkräften

Veröffentlicht eine bayerische öffentliche Stelle auf ihrer Internetseite Namen und dienstliche Kontaktdaten von bestimmten Beschäftigten, verfolgt sie damit regelmäßig den Zweck, Bürgerinnen und Bürger über behördliche Ansprechpersonen zu informieren und ihnen die Kontaktaufnahme zu erleichtern. Ein solche Veröffentlichung ist datenschutzrechtlich in gewissem Umfang zulässig; mit den Voraussetzungen und Grenzen der dabei einschlägigen Rechtsgrundlagen habe ich mich zuletzt in meinem 33. Tätigkeitsbericht 2023 unter Nr. 7.5 ausführlich befasst.

Die Veröffentlichung privater Kontaktdaten von Beschäftigten ist für bayerische Dienstherren und öffentliche Arbeitgeber allerdings tabu, wie auch der nachfolgende Fall anschaulich zeigt:

5.5.1 Sachverhalt

Bereichslehrkräfte sind mit der Unterstützung und Förderung der Kinder beruflich Reisender (Schaustellerfamilien, Zirkusangehörige, fahrende Personen) in ihrem Einsatzgebiet beauftragt. Hierzu veröffentlicht das Bayerische Staatsministerium für Unterricht und Kultus auf seiner Internetseite eine Liste mit Namen, Zuständigkeitsbereichen und dienstlichen Kontaktdaten der bayerischen Bereichslehrkräfte, um insbesondere für die Eltern eine einfache Erreichbarkeit zu gewährleisten.

Bei rein dienstlichen Kontaktdaten ist es dabei allerdings nicht geblieben: Gleich mehrere bayerische Bereichslehrkräfte wandten sich an mich und beschwerten sich darüber, dass das Kultusministerium auf seiner Homepage eine Liste im PDF-Format mit zum Teil privaten Kontaktdaten (darunter private Telefonnummern und E-Mail-Adressen) von mobilen Bereichslehrkräften veröffentlicht habe. Einwilligungen seien dazu nicht erteilt worden; mitunter seien die Beschwerdeführenden als Folge der Veröffentlichung privat von Dritten (telefonisch) kontaktiert worden. Nahezu zeitgleich meldete mir das Kultusministerium den bekannt gewordenen Sachverhalt als „Datenpanne“ im Rahmen seiner Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DSGVO.

Wie mir das Kultusministerium in seiner darauffolgenden Stellungnahme mitteilte, entstammten die privaten Kontaktdaten offenbar einer Liste, die zum Zweck der Datenaktualisierung von nachgeordneten Behörden zugeleitet worden war. Die privaten Kontaktdaten seien dabei nicht zur Veröffentlichung bestimmt gewesen; eine entsprechende Überprüfung habe vor Veröffentlichung jedoch nicht stattgefunden. Aufgrund eines Hinweises einer Bereichslehrkraft sei die Liste allerdings von der Homepage des Kultusministeriums genommen worden.

Dennoch war die Liste „aus technischen Gründen" zunächst noch abrufbar, bevor sie auf mein Hinwirken von der Webseite entfernt wurde. Zudem musste ich das Kultusministerium darauf hinweisen, dass die privaten Kommunikationsdaten der Lehrkräfte auch danach über das Vorschaufenster von Internetsuchmaschinen zunächst noch auffindbar waren. Erst auf meinen diesbezüglichen Hinweis hin konnte auch insofern eine Löschung erreicht werden.

5.5.2 Unrechtmäßige Veröffentlichung der privaten Kontaktdaten

Private Telefon- und Faxnummern sowie E-Mail-Adressen von Beschäftigten im bayerischen öffentlichen Dienst sind Personalaktendaten, deren Verarbeitung den Vorgaben gemäß § 50 Beamtenstatusgesetz, Art. 103 ff. Bayerisches Beamtengesetz (BayBG) unterfällt. Diese Vorschriften sind gemäß Art. 145 Abs. 2 BayBG auch auf die nichtverbeamteten Beschäftigten des bayerischen öffentlichen Dienstes im Grundsatz entsprechend anzuwenden. Eine Weitergabe dieser Personalaktendaten an Dritte – hier an die Internetöffentlichkeit – wäre allenfalls auf Grund von Art. 108 Abs. 4 BayBG in Betracht gekommen. Auskünfte aus der Personalakte sind danach grundsätzlich nur mit Einwilligung der betroffenen Person zulässig, es sei denn, dass die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz berechtigter, höherrangiger Interessen des Dritten die Auskunftserteilung zwingend erfordert (Art. 108 Abs. 4 Satz 1 BayBG). Einwilligungen der Bereichslehrkräfte zur Veröffentlichung ihrer privaten Kontaktdaten lagen nicht vor. Im Übrigen sind Einwilligungen im Beschäftigungsverhältnis ohnehin nur selten freiwillig und damit wirksam (vgl. Art. 4 Nr. 11 DSGVO), weshalb ich von deren Einholung grundsätzlich abrate. Für das Vorliegen des erwähnten Ausnahmefalls war ebenfalls nichts ersichtlich.

Die privaten Kontaktdaten der Bereichslehrkräfte wurden deshalb ohne Rechtsgrundlage veröffentlicht.

5.5.3 Entfernung der Datensätze aus Vorschauanzeigen von Internetsuchmaschinen

Soweit private Kontaktdaten der Bereichslehrkräfte trotz Entfernung des Datensatzes von der Homepage des Kultusministeriums noch in Vorschauanzeigen von Internetsuchmaschinen auftauchten, hat das Kultusministerium auf meine Intervention hin auf deren Entfernung bei den Suchmaschinenbetreibern hingewirkt.

Hier kam das „Recht auf Vergessenwerden" zum Zuge: Gemäß Art. 17 Abs. 2 DSGVO hat ein zur Löschung verpflichteter Verantwortlicher, der personenbezogene Daten öffentlich gemacht hat (hier: das Kultusministerium), angemessene Maßnahmen zu treffen, um andere Verantwortliche (hier: die Betreiber der betreffenden Internetsuchmaschinen) darüber zu informieren, dass eine betroffene

Person die Löschung verlangt hat. Diese Informationspflicht bedeutet im Ergebnis, dass dem Kultusministerium selbst kein eigener Anspruch auf Löschung gegenüber den Suchmaschinenbetreibern zustand, es aber auf eine Löschung hinwirken musste.

5.5.4 Ergebnis

Ich habe gegenüber dem Kultusministerium aufgrund der unrechtmäßigen Veröffentlichung privater Kontaktdaten bei Würdigung der geschilderten Begebenheiten eine datenschutzrechtliche Verwarnung (Art. 58 Abs. 2 Buchst. b DSGVO) ausgesprochen. Da der Datenschutzverstoß zwischenzeitlich behoben worden ist, konnte ich von weiteren aufsichtlichen Maßnahmen absehen.

5.6 Unverschlüsselte Übermittlung eines amtsärztlichen Gutachtens an eine private E-Mail-Adresse

Der Fall ist schnell zusammengefasst: Ein Beamter wird durch die Medizinische Untersuchungsstelle (MUS) einer bayerischen Regierung im Hinblick auf seine Dienstfähigkeit amtsärztlich begutachtet. Die MUS übermittelt ihr Gutachten an den Dienstvorgesetzten des Beamten. Dieser prüft auf Grundlage des Gutachtens, ob und wie der Beamte dienstlich weiter eingesetzt werden kann. Das Ergebnis seiner Prüfung übermittelt der Dienstvorgesetzte per unverschlüsselter und mit dem Betreff „Anhörung“ versehener E-Mail unter anderem an die private E-Mail-Adresse des betroffenen Beamten. Das Gutachten der MUS hat er dieser E-Mail als Anlage beigefügt. Der Beamte ist der Ansicht, dass sein Dienstvorgesetzter hierdurch gegen datenschutzrechtliche Vorgaben verstoßen hat, und wendet sich mit einer Beschwerde an mich.

Bevor ich mich der eigentlichen „Fallfrage“ widme, möchte ich kurz wesentliche Aspekte des zugrunde liegenden Begutachtungsverfahrens darstellen:

— Dienstunfähige Beamtinnen und Beamte sind unter den Voraussetzungen des § 26 Beamtenstatusgesetz, Art. 65 Abs. 2 Bayerisches Beamtengesetz (BayBG) in den Ruhestand zu versetzen. Bei Zweifeln an ihrer Dienstunfähigkeit kann der Dienstherr betroffene Beamtinnen und Beamte anweisen, sich (amts-)ärztlich untersuchen zu lassen. Grundlage hierfür ist Art. 65 Abs. 2 Satz 1 BayBG:

  „[1]Bestehen Zweifel über die Dienstunfähigkeit, so ist der Beamte oder die Beamtin verpflichtet, sich nach Weisung des oder der Dienstvorgesetzten ärztlich untersuchen und, falls ein Amtsarzt oder eine Amtsärztin dies für erforderlich hält, beobachten zu lassen. [2]Auf Verlangen des Amtsarztes oder der Amtsärztin hat sich der Beamte oder die Beamtin zudem einer fachärztlichen Zusatzbegutachtung zu unterziehen. [3]Wer sich trotz wiederholter schriftlicher Aufforderung ohne hinreichenden Grund der Verpflichtung, sich nach Weisung des oder der Dienstvorgesetzten untersuchen oder beobachten zu lassen, entzieht, kann so behandelt werden, wie wenn die Dienstunfähigkeit amtsärztlich festgestellt worden wäre.“

— Nähere Einzelheiten zu diesem Verfahren finden sich insbesondere in Art. 67 BayBG sowie in Abschnitt 8 der Verwaltungsvorschriften zum Beamtenrecht (VV-BeamtR). Das amtsärztliche Gutachten gibt die oder der

jeweilige Dienstvorgesetzte in Auftrag. Der Gutachtensauftrag enthält neben einer umfassenden Schilderung des Sachverhalts, der Anlass für den Auftrag gegeben hat, insbesondere auch konkrete Fragen an die Begutachtungsärztin oder den Begutachtungsarzt. Die betroffene Beamtin oder der betroffene Beamte erhält eine Kopie des Gutachtensauftrags (Abschnitt 8 Nr. 1.3.2 VV-BeamtR).

– Zuständig für Dienstfähigkeitsbegutachtungen sind grundsätzlich die Regierungen, Art. 5 Satz 1 Gesundheitsdienstgesetz (GDG). Diese verfügen dazu jeweils über eine MUS. Die Entscheidung, ob eine begutachtete Beamtin oder ein begutachteter Beamter tatsächlich dienstunfähig ist, treffen nicht die Amtsärztinnen oder Amtsärzte, sondern die jeweiligen Dienstvorgesetzten (vgl. Abschnitt 8 Nr. 1.8 Satz 1 VV-BeamtR). Das amtsärztliche (Gesundheits-)Zeugnis soll als „Ergebnis" der Begutachtung den Dienstvorgesetzten eine umfassende Entscheidungsgrundlage an die Hand geben (Abschnitt 8 Nr. 1.4.1 Satz 1 VV-BeamtR). Die Weitergabe amtsärztlicher Erkenntnisse an Dienstvorgesetzte bedarf, soweit sie zur Erfüllung des Gutachtenauftrags erforderlich ist, keiner (ausdrücklichen) Einwilligung der betroffenen Person – Art. 67 Abs. 1 BayBG normiert insoweit nämlich eine ausdrückliche gesetzliche Übermittlungsbefugnis für die Gesundheitsbehörde (vgl. auch Art. 27 Abs. 2 Satz 1 Nr. 1 GDG). In diesem Rahmen tritt auch die ärztliche Schweigepflicht nach § 203 Strafgesetzbuch von Amtsärztinnen und Amtsärzten zurück.

– Es liegt auf der Hand, dass amtsärztliche Gesundheitszeugnisse über Dienstfähigkeitsuntersuchungen hochsensible Daten der begutachteten Beamtinnen und Beamten enthalten. Sie sind daher in besonderem Maße gegen eine unbefugte Einsichtnahme zu schützen. Für den Übermittlungsweg von den begutachtenden amtsärztlichen Stellen an die Dienstvorgesetzten sieht Art. 67 Abs. 2 BayBG daher vor, dass die amtsärztliche Mitteilung in einem gesonderten, verschlossenen und versiegelten Umschlag zu übersenden ist.

Im vorliegenden Fall gab es keine Anhaltspunkte dafür, dass die MUS hinter diesen Vorgaben zurückgeblieben wäre. Auf welche Weise Dienstvorgesetzte amtsärztliche Zeugnisse gegebenenfalls an betroffene Beamtinnen und Beamte übermitteln dürfen, ist hingegen in den Art. 65 ff. BayBG nicht spezifisch geregelt. Hier kommen neben personalaktenrechtlichen Aspekten insbesondere technische und organisatorische Vorgaben der Datenschutz-Grundverordnung ins Spiel:

Für die Übermittlung des Gutachtens an den betroffenen Beamten war vorliegend die personalverwaltende Stelle datenschutzrechtlich verantwortlich im Sinne von Art. 4 Nr. 7 DSGVO. Nach dem datenschutzrechtlichen Grundsatz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 Buchst. f DSGVO) haben Verantwortliche bei der Verarbeitung personenbezogener Daten durch technische und organisatorische Maßnahmen eine angemessene Sicherheit dieser Daten zu gewährleisten. Dies schließt den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung mit ein. Spezifizierend hierzu verpflichtet Art. 32 Abs. 1 DSGVO Verantwortliche, geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein dem Risiko der Verarbeitung angemessenes Schutzniveau zu gewährleisten. Die letztgenannte Vorschrift zeigt verschiedene Kriterien auf, die der Verantwortliche bei der Maßnahmenauswahl zu berücksichtigen hat, darunter die Eintrittswahrscheinlichkeit und Schwere des mit der jeweiligen Verarbeitung einhergehenden Risikos für die Rechte und Freiheiten natürlicher Personen (vgl. auch Art. 32 Abs. 2 DSGVO).

In die danach durchzuführende Risikoanalyse[69] war insbesondere einzustellen, dass es sich bei dem übermittelten amtsärztlichen Gutachten für den Dienstherrn um Personalaktendaten im Sinne von § 50 Satz 2 Beamtenstatusgesetz, Art. 103 ff. BayBG handelt, die ihrer Natur nach besonders sensibel sind; zugleich umfasst (jedenfalls) das übermittelte Gutachten inhaltlich Gesundheitsdaten des Beschwerdeführers und damit auch besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO. Solche unterliegen einem besonderen Schutz. Bei ihrer Verarbeitung hat der Dienstherr angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen (Art. 103 Satz 1 Nr. 2 BayBG in Verbindung mit Art. 8 Abs. 2 Satz 1 BayDSG). Als technische und organisatorische Maßnahme im Sinne dieser Vorschriften kommt insbesondere die Verschlüsselung personenbezogener Daten in Betracht (vgl. Art. 32 Abs. 1 Buchst. a DSGVO sowie die Gesetzesbegründung zu Art. 8 BayDSG[70]).

Die personalverwaltende Stelle hatte insoweit vorgetragen, betroffene Beschäftigte in vergleichbaren Konstellationen grundsätzlich schriftlich per Brief anzuhören. In diesem Rahmen werde auch das jeweilige Gutachten übersandt. Da der betroffene Beamte auf seiner damaligen Position dienstunfähig gewesen sei und so schnell wie möglich habe umgesetzt werden müssen, sei dieser im vorliegenden Fall ausnahmsweise aus Zeitgründen per einfacher E-Mail angehört worden. Die personalverwaltende Stelle räumte allerdings selbst ein, dass der Versand des Gutachtens an die private E-Mail-Adresse des betroffenen Beamten per einfacher, ungeschützter E-Mail nicht den datenschutzrechtlichen Anforderungen genügt hatte.

Bei meiner Bewertung des Sachverhalts habe ich berücksichtigt, dass es sich bei dem vorliegenden E-Mail-Versand nach Darstellung der personalverwaltenden Stelle um einen Einzelfall handelte. Anhaltspunkte für systematisch-organisatorische Mängel waren für mich nicht erkennbar. Die personalverwaltende Stelle hat den festgestellten Datenschutzverstoß eingeräumt, betont, dass sich dieser nicht wiederholen werde, und entsprechende interne Sensibilisierungsmaßnahmen ergriffen.

In Anbetracht der Sensibilität der übermittelten Daten, die sowohl Personalaktendaten als auch besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO umfassten, habe ich wegen des festgestellten Verstoßes gegen Art. 32 Abs. 1 DSGVO sowie Art. 103 Satz 1 Nr. 2 BayBG in Verbindung mit Art. 8 Abs. 2 Satz 1 BayDSG gleichwohl eine datenschutzrechtliche Verwarnung (Art. 58 Abs. 2 Buchst. b DSGVO) ausgesprochen.

5.7 Betriebsärztliche Gutachten im Betrieblichen Eingliederungsmanagement und im Präventionsverfahren: Weitergabe an die Schwerbehindertenvertretung?

Anlässlich einer Beratungsanfrage habe ich mich erneut mit datenschutzrechtlichen Aspekten des Betrieblichen Eingliederungsmanagements (BEM) und des

[69] Vgl. hierzu eingehend Bayerischer Landesbeauftragter für den Datenschutz, Risikoanalyse und Datenschutz-Folgenabschätzung – Systematik, Anforderungen, Beispiele, Stand 5/2022, Internet: https://www.datenschutz-bayern.de, Rubrik „DSFA".

[70] Landtags-Drucksache 17/19628, S. 36.

Präventionsverfahrens beschäftigt. Diesmal ging es um die Frage, ob betriebsärztliche Gutachten im Rahmen dieser Verfahren durch den Arbeitgeber an die Schwerbehindertenvertretung weitergegeben werden dürfen.

5.7.1 Hintergrund

Nach § 178 Abs. 2 Satz 1 Neuntes Buch Sozialgesetzbuch – Rehabilitation und Teilhabe von Menschen mit Behinderungen – (SGB IX) hat der Arbeitgeber die Schwerbehindertenvertretung in allen Angelegenheiten, die einen einzelnen oder die schwerbehinderten Menschen als Gruppe berühren, unverzüglich und umfassend zu unterrichten und vor einer Entscheidung anzuhören. Ein eigenständiges, einwilligungsunabhängiges Recht auf Einsicht in die Personalakte von schwerbehinderten Beschäftigten steht der Schwerbehindertenvertretung dagegen nicht zu (vgl. § 178 Abs. 3 Satz 1 SGB IX).[71] Vor diesem Hintergrund habe ich eine Anfrage erhalten, ob die Pflicht zur Unterrichtung der Schwerbehindertenvertretung möglicherweise auch die Weitergabe betriebsärztlicher Gutachten durch den Arbeitgeber an die Schwerbehindertenvertretung im BEM und bei Präventionsverfahren umfasst. Eine grundsätzliche Einbeziehung der Schwerbehindertenvertretung hat der Gesetzgeber bei beiden Verfahrensarten schließlich ausdrücklich vorgesehen.

Gemäß § 167 Abs. 2 Satz 1 SGB IX ist der Arbeitgeber verpflichtet, allen Beschäftigten, die innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig sind, ein **BEM** anzubieten. Ein BEM bezweckt nach dieser Vorschrift, die Arbeitsunfähigkeit zu überwinden, erneuter Arbeitsunfähigkeit vorzubeugen und den Arbeitsplatz zu erhalten beziehungsweise eine Arbeitsunfähigkeit zu vermeiden. Das BEM umfasst also alle Aktivitäten, Maßnahmen und Leistungen, die im Einzelfall zur Wiedereingliederung nach längerer Arbeitsunfähigkeit erforderlich sind. Was hierfür konkret zu tun ist, hat der Arbeitgeber bei schwerbehinderten Menschen unter Beteiligung der Schwerbehindertenvertretung zu klären – dies allerdings unter der Voraussetzung, dass der oder die betroffene Beschäftigte dieser Beteiligung – wie auch dem BEM insgesamt – zugestimmt hat (§ 167 Abs. 2 Satz 1 SGB IX).

In einem vom BEM zu unterscheidenden **Präventionsverfahren** nach § 167 Abs. 1 SGB IX schaltet der Arbeitgeber frühzeitig unter anderem die Schwerbehindertenvertretung ein, wenn personen-, verhaltens- oder betriebsbedingte Schwierigkeiten eintreten, die das Beschäftigungsverhältnis mit einem schwerbehinderten oder ihm gleichgestellten Menschen gefährden könnten. Ziel dieses Verfahrens ist es, eine vorzeitige Beendigung des Beschäftigungsverhältnisses (insbesondere durch Kündigung) aufgrund dieser Schwierigkeiten möglichst zu vermeiden. Im Präventionsverfahren soll umfassend erörtert werden, wie die bestehenden Schwierigkeiten im Beschäftigungsverhältnis beseitigt werden können. Es dient damit vorrangig der Konfliktprävention. Das Präventionsverfahren bedarf im Vergleich zum BEM keiner Zustimmung der oder des betroffenen Beschäftigten.

Die Verpflichtungen aus § 167 Abs. 1 SGB IX und § 167 Abs. 2 Satz 1 SGB IX gelten auch für öffentliche Arbeitgeber. Im Zuge eines BEM wie auch eines Präventi-

[71] Vgl. Pahlen, in: Neumann/Pahlen/Greiner/Winkler/Westphal/Krohne, Sozialgesetzbuch IX, 15. Aufl. 2024, § 178 Rn. 13.

onsverfahrens werden Beschäftigtendaten verarbeitet. Jedenfalls im Rahmen eines BEM, das den Fokus auf die Gesundheit legt, sind auch sensible Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DSGVO betroffen. Die datenschutzrechtlichen Anforderungen, die für das BEM zu beachten sind, habe ich bereits in meinem 25. Tätigkeitsbericht 2012 unter Nr. 11.2 ausführlich erläutert. Sowohl die Schwerbehindertenvertretung als auch die örtliche Personalvertretung haben nach § 167 Abs. 2 Satz 8 SGB IX darüber zu wachen, dass Arbeitgeber ihre Verpflichtungen zur Anbietung und – bei Annahme des Angebots – auch zur ordnungsgemäßen Durchführung eines BEM erfüllen. Zur Reichweite ihres diesbezüglichen Informationsanspruchs habe ich in meinem 26. Tätigkeitsbericht 2014 unter Nr. 11.3 sowie in meinem 27. Tätigkeitsbericht 2016 unter Nr. 11.3 Stellung genommen. Die Beiträge beziehen sich zwar auf die Vorgängervorschrift des heutigen § 167 Abs. 2 Satz 1 SGB IX und auf Berichtszeiträume vor Inkrafttreten der Datenschutz-Grundverordnung; ich halte an diesen Ausführungen aber weiterhin fest.

Nicht ausdrücklich befasst hatte ich mich bislang mit der Frage, inwieweit die Schwerbehindertenvertretung im Rahmen der genannten Verfahren in etwaige betriebsärztliche Gutachten von betroffenen Beschäftigten Einsicht nehmen darf.

5.7.2 Einsichtnahme in betriebsärztliche Gutachten durch die Schwerbehindertenvertretung

Bei der Schwerbehindertenvertretung handelt es sich nicht um einen eigenständigen Verantwortlichen im Sinne von Art. 4 Nr. 7 DSGVO. Vielmehr ist sie – ebenso wie etwa der Personalrat[72] – als Teil der jeweiligen öffentlichen Stelle anzusehen. Die öffentliche Stelle ist damit auch für die Verarbeitung personenbezogener Daten durch die Schwerbehindertenvertretung datenschutzrechtlich verantwortlich.

Auch die interne Weitergabe oder Offenlegung personenbezogener Daten innerhalb einer verantwortlichen Stelle – beispielsweise durch Aushändigung von betriebsärztlichen Gutachten durch die Dienststelle an die Schwerbehindertenvertretung – stellt eine Verarbeitung personenbezogener Daten dar, die einer Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO bedarf. Als Rechtsgrundlagen kämen vorliegend grundsätzlich Art. 103 Satz 1 Bayerisches Beamtengesetz (BayBG) und § 178 Abs. 2 Satz 1 SGB IX in Betracht: Die Weitergabe der Gutachten müsste also zur Personalverwaltung oder zur Erfüllung der sozialgesetzlichen Unterrichtungspflicht erforderlich sein. Im Übrigen käme als Rechtsgrundlage die Einwilligung der betroffenen Beschäftigten nach Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 4 Nr. 11, Art. 7 DSGVO in Frage. Da betriebsärztliche Gutachten Gesundheitsdaten enthalten, ist auch Art. 9 DSGVO zu beachten.

5.7.2.1 BEM

Arbeitgeber haben die Schwerbehindertenvertretung zwar auch ohne Einwilligung der jeweils betroffenen Person zu informieren, welchen schwerbehinderten Beschäftigten ein BEM angeboten worden ist (vgl. hierzu meinen 26. Tätigkeitsbericht 2014 unter Nr. 11.3.2). Nach meiner Einschätzung dürfen Arbeitgeber im Rahmen der eigentlichen BEM-Durchführung jedoch betriebsärztliche Gutachten

[72] Vgl. hierzu ausführlich Bayerischer Landesbeauftragter für den Datenschutz, Der Personalrat – Verantwortlicher im Sinne des Datenschutzrechts?, Aktuelle Kurz-Information 23, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek“

nicht ohne wirksame ausdrückliche **Einwilligung der betroffenen Person** im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 9 Abs. 2 Buchst. a DSGVO an die Schwerbehindertenvertretung weitergeben (vgl. hierzu grundlegend meinen 25. Tätigkeitsbericht 2012 unter Nr. 11.2). Eine solche Einwilligung muss sich ausdrücklich auch auf Gesundheitsdaten beziehen; überdies ist darauf zu achten, dass sie insbesondere informiert und freiwillig erteilt werden muss (vgl. Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 4 Nr. 11, Art. 7, Art. 9 Abs. 1, Abs. 2 Buchst. a DSGVO).

Dieses Einwilligungserfordernis ergibt sich für das BEM in der vorliegenden Konstellation aus folgenden Erwägungen: Zunächst setzt bereits die Durchführung eines BEM gemäß § 167 Abs. 2 Satz 1 SGB IX die Zustimmung der betroffenen Person voraus. Da die oder der Beschäftigte insoweit auch über die Beteiligung der Schwerbehindertenvertretung und gegebenenfalls die Einbeziehung einer Betriebsärztin oder eines Betriebsarztes frei entscheiden kann, kommt ein „Einsichtsrecht" der Schwerbehindertenvertretung in betriebsärztliche Gutachten ohnehin nur in Betracht, wenn sich die betroffene Person für eine Teilnahme der Schwerbehindertenvertretung entschieden hat.

Zur Durchführung des BEM hat das Bayerische Staatsministerium der Finanzen und für Heimat einen Leitfaden „Betriebliches Eingliederungsmanagement" herausgegeben.[73] Hiernach soll im BEM-Gespräch zwischen den Beteiligten die derzeitige Situation des oder der betroffenen Beschäftigten umfassend analysiert werden; hierauf aufbauend sollen mögliche Maßnahmen vereinbart werden, um die Arbeitsunfähigkeit möglichst dauerhaft zu überwinden. Personenbezogene medizinische Daten dürfen dabei nur „in Textform" erfasst werden, wenn die betroffene Person dem zugestimmt hat (Leitfaden, S. 10 f.). Vor diesem Hintergrund und in Anbetracht der in einem medizinischen Gutachten regelmäßig enthaltenen spezifischen Angaben zum Gesundheitszustand Beschäftigter darf die Schwerbehindertenvertretung in betriebsärztliche Gutachten nur Einsicht nehmen, soweit eine entsprechende wirksame ausdrückliche Einwilligung der betroffenen Person vorliegt. Da das betriebsärztliche Gutachten regelmäßig Teil des jeweiligen Personalakts sein wird, stünde ohnehin § 178 Abs. 3 Satz 1 SGB IX einer einwilligungsunabhängigen Einsicht durch die Schwerbehindertenvertretung entgegen.

5.7.2.2 Präventionsverfahren

Bei Präventionsverfahren ist zwar zu berücksichtigen, dass eine Erörterung von Möglichkeiten und Hilfen, um bestehende Schwierigkeiten zu beseitigen und das Beschäftigungsverhältnis möglichst dauerhaft fortzusetzen (vgl. § 167 Abs. 1 SGB IX), eine Weitergabe personenbezogener Daten der betroffenen Person bedingt und das Gesetz – anders als beim BEM – für dieses Verfahren grundsätzlich auch keine Zustimmung der betroffenen Beschäftigten vorsieht. Unabhängig von der Frage, inwieweit im Falle krankheitsbedingter Fehlzeiten das Verfahren des BEM dem Präventionsverfahren als spezielleres Verfahren ohnehin vorgeht,[74] ist für mich aus der Beratungsanfrage nicht ersichtlich geworden, inwieweit die Kenntnis der Schwerbehindertenvertretung vom Inhalt etwaiger betriebsärztlicher Gutachten angesichts der Zielsetzung des Präventionsverfahrens (siehe bereits oben) für diese Erörterung erforderlich wäre. Da betriebsärztliche Gutachten regelmäßig Teil des jeweiligen Personalakts sein werden, stünde ferner § 178 Abs. 3

[73] Der Leitfaden ist im Bayerischen Behördennetz von der Seite des Bayerischen Staatsministeriums der Finanzen und für Heimat abrufbar.

[74] Vgl. Karb, in: Conze/Karb/Reidel/Hahn/Krellig, Personalbuch Arbeits- und Tarifrecht öffentlicher Dienst, 8. Aufl. 2024, Präventionsverfahren Rn. 3.

Satz 1 SGB IX einer Einsicht der Schwerbehindertenvertretung ohne Zustimmung der betroffenen Person entgegen. Insofern gehe ich davon aus, dass für die Einsicht der Schwerbehindertenvertretung in betriebsärztliche Gutachten auch im Rahmen eines Präventionsverfahrens in aller Regel eine wirksame ausdrückliche Einwilligung der betroffenen Person erforderlich ist.

5.7.2.3 Ergebnis

Im Ergebnis verbleibt die Entscheidung über die Weitergabe betriebsärztlicher Gutachten im Rahmen des BEM oder des Präventionsverfahrens durch den Arbeitgeber an die Schwerbehindertenvertretung in aller Regel bei der betroffenen Person. Verantwortliche haben das Vorliegen etwaiger wirksamer ausdrücklicher Einwilligungen im Rahmen ihrer Rechenschaftspflicht nachzuweisen (vgl. Art. 5 Abs. 2, Art. 7 Abs. 1 DSGVO).

6 Schulen

6.1 Beratung bei der Änderung schulrechtlicher Vorschriften

Im Jahr 2024 wurden unter anderem das Bayerische Gesetz über das Erziehungs- und Unterrichtswesen, die Bayerische Schulordnung und die Grundschulordnung geändert. Betroffen waren dabei auch datenschutzrelevante Vorschriften. Ich habe das Bayerische Staatsministerium für Unterricht und Kultus jeweils eingehend beraten.

Herausgreifen möchte ich Änderungen an Vorschriften, durch welche die Bayerische Staatsregierung verbindliche Sprachstandserhebungen und Sprachfördermaßnahmen vor der Einschulung sicherstellen will. Gemäß dem Gesetzentwurf[75] schafft eine fundierte Sprachstandserhebung die notwendige Grundlage, um die Zeit bis zur Einschulung bedarfsgerecht für geeignete Fördermaßnahmen nutzen zu können und rechtzeitig sicherzustellen, dass vor der Einschulung erforderliche Förderangebote wahrgenommen werden.

Durch meine Stellungnahmen konnte ich erfreulicherweise datenschutzrechtliche Verbesserungen erreichen:

Der parlamentarische Gesetzgeber hat das Kultusministerium in Art. 89 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG) im dort genannten Rahmen ermächtigt, Näheres durch eine Rechtsverordnung zu regeln. Auf dieser Grundlage wollte das Kultusministerium in der Grundschulordnung einzelne Regelungen zur Sprachstandserhebung vor der Einschulung treffen. Meiner Bitte, die **Verordnungsermächtigung** durch die **Einfügung** der Wörter „und die vorausgehende Sprachstandserhebung und -förderung“ in Art. 89 Abs. 1 Satz 3 Nr. 2 BayEUG klarzustellen, wurde nachgekommen. Zudem enthält die Begründung des Gesetzentwurfs nun folgenden Satz: „Die Verordnungsermächtigung wird hinsichtlich der Sprachstandserhebung und -förderung ergänzt.“ Die **dadurch erlangte Rechtsklarheit** unterstützt die Umsetzung der Regelungen **auch in datenschutzrechtlicher Hinsicht**.

Soweit bei Kindern vor der Einschulung gemäß Art. 37 Abs. 3 Satz 2, 3 BayEUG eine Sprachstandserhebung an der jeweils zuständigen Sprengelschule durchgeführt werden soll, war im Regelungsentwurf die Option vorgesehen, dass eine Tonaufnahme angefertigt und bis zur Auswertung an der Grundschule gespeichert werden kann.

Angesichts des Grundsatzes der Datenminimierung (vgl. Art. 5 Abs. 1 Buchst. c DSGVO) war allerdings insbesondere zu ergänzen, dass Tonaufnahmen lediglich dann angefertigt werden sollten, soweit andere ebenso geeignete Verfahren zur Sprachstandserhebung nicht zur Verfügung stehen. Dies gilt umso mehr, als es sich bei Tonaufnahmen von Kindern auch dann um sensible Datenverarbeitungen handelt, wenn sie nur vorübergehend gespeichert werden sollten.

[75] Landtags-Drucksache 19/3248.

Offenbar konnte meine Argumentation überzeugen. Denn der am 17. Dezember 2024 in Kraft getretene **§ 2 Abs. 1 Satz 5 Grundschulordnung** lautet wie folgt:

„Zur Erhebung des Sprachstandes kann erforderlichenfalls eine Tonaufnahme angefertigt und bis zur zeitnahen Auswertung an der Grundschule gespeichert werden."

Die **Begründung** des Gesetzentwurfs[76] wurde wie folgt gefasst:

„Zur Erhebung des Sprachstandes kann je nach eingesetztem Diagnoseverfahren eine Tonaufnahme – soweit erforderlich – angefertigt werden; diese wird bis zur zeitnahen Auswertung an der Grundschule gespeichert und danach gelöscht. Ein Diagnoseverfahren darf nur dann mit Tonaufnahmen eingesetzt werden, wenn kein geeignetes Verfahren ohne Tonaufnahme zur Verfügung steht. […]"

Das im März 2025 erstmalig zur Anwendung kommende Verfahren der bayernweiten Sprachstandserhebungen sieht erfreulicherweise keine Tonaufnahmen vor. Ob dies mittelfristig so bleiben soll, wird insbesondere die Evaluierung der derzeitigen Verfahrensweise zeigen.

6.2 Auskunft nach Art. 15 DSGVO

Im Berichtszeitraum beschwerten sich die Eltern eines Schülers bei mir, weil die Schule seinen Anspruch auf Kopie (vgl. Art. 15 Abs. 3 DSGVO), insbesondere von den Prüfungsarbeiten, nicht erfüllt hätte.

Nachdem ich der Schule datenschutzrechtliche Hinweise gegeben und sie zur Stellungnahme aufgefordert hatte, teilte mir die Schule mit, sie habe die erbetenen Unterlagen nun an die Eltern gesandt.

Im Schriftverkehr mit der Schule zeigte sich manche **Fehleinschätzung, die ich korrigieren konnte.** Dies betraf – vereinfacht und zusammengefasst – insbesondere folgende Aspekte:

Nach Auffassung der Schule war das Auskunftsersuchen gemäß Art. 12 Abs. 5 DSGVO **„offensichtlich unbegründet"**. Die Schule habe das Anliegen an den behördlichen Datenschutzbeauftragten sowie dann anonymisiert an eine vorgesetzte Stelle weitergegeben. Dort würde der Sachverhalt diesbezüglich geprüft. Wann die vorgesetzte Stelle ihre Prüfung abgeschlossen haben werde, liege allerdings nicht in den Händen der Schule. Es stehe im Raum, dass das Auskunftsersuchen **rechtsmissbräuchlich** sei.

6.2.1 Schule als Verantwortlicher

Verantwortlicher für die Einhaltung der datenschutzrechtlichen Vorschriften (vgl. Art. 4 Nr. 7 DSGVO, Art. 3 Abs. 2, Art. 1 Abs. 1 Satz 1 BayDSG) bleibt die Schule auch dann, wenn sie eine Beratungsanfrage an eine vorgesetzte Stelle richtet. Dies gilt gleichermaßen für die Einhaltung der vorgeschriebenen Fristen.

[76] Landtags-Drucksache 19/3248, S. 17.

6.2.2 Anspruch auf Auskunft nach Art. 15 DSGVO

Nach Art. 15 Abs. 3 DSGVO besteht ein Recht auf Kopie. Dieses Recht erfasst grundsätzlich auch die eigenen Prüfungsarbeiten (siehe hierzu bereits meinen 33. Tätigkeitsbericht 2023 unter Nr. 8.4).

Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – **exzessiven Anträgen** hätte die Schule zwar nach Maßgabe von **Art. 12 Abs. 5 Satz 2 DSGVO** entweder ein angemessenes Entgelt verlangen oder sich weigern können, aufgrund des Antrags tätig zu werden. Die Schule hätte aber den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags erbringen müssen (Art. 12 Abs. 5 Satz 3 DSGVO).

Art. 12 Abs. 5 Satz 2 DSGVO ist als Ausnahmevorschrift und mit Blick auf die Bedeutung des Auskunftsanspruchs nach Art. 15 DSGVO eng auszulegen.

Ein Auskunftsantrag ist gemäß den einschlägigen Leitlinien des Europäischen Datenschutzausschusses **offenkundig unbegründet**,[77] wenn die Voraussetzungen nach Art. 15 DSGVO unter objektiven Gesichtspunkten eindeutig und offensichtlich nicht erfüllt sind. Dabei ist zu beachten, dass die Inanspruchnahme des Auskunftsrechts an nur sehr wenige Voraussetzungen geknüpft ist.

Exzessiv im Sinne des Art. 12 Abs. 5 Satz 2 DSGVO kann ein Antrag auch dann sein, wenn es sich nicht um einen Fall häufiger Wiederholung handelt, auch wenn die häufige Wiederholung den Hauptanwendungsfall darstellt. In den erwähnten Leitlinien werden hierzu Beispiele genannt,[78] etwa, dass ein Auskunftsantrag gestellt, gleichzeitig aber angeboten wird, ihn zurückzuziehen, wenn im Gegenzug ein irgendwie gearteter Vorteil durch den Verantwortlichen gewährt wird. Als weiteres Beispiel wird ein Antrag in böswilliger Absicht angeführt, also um zu schikanieren, ohne dass ein anderer Zweck verfolgt wird. Dies sei etwa daran zu erkennen, dass die antragstellende Person ausdrücklich erklärt, dass ihr allein daran liegt, Störungen zu verursachen oder im Rahmen einer Kampagne systematisch, zum Beispiel einmal pro Woche, verschiedene Anträge an den Verantwortlichen mit der Absicht sendet, Störungen zu verursachen. Ein Antrag sei hingegen nicht als exzessiv anzusehen, wenn keine Gründe für den Auskunftsantrag angegeben werden oder der Verantwortliche den Antrag als sinnlos betrachtet.

Die Schule konnte im Ergebnis allerdings keinen gesetzlich vorgesehenen Grund darlegen, nach dem die Kopien hätten verweigert werden können. Insbesondere konnte ein Nachweis zu einer der Fallgruppen offensichtlich unbegründeter oder exzessiver Anträge nicht geführt werden.

[77] Europäischer Datenschutzausschuss, Leitlinien 01/22 zu den Rechten der betroffenen Person – Auskunftsrecht; Stand 5/2024, Rn. 177, Internet: https://www.edpb.europa.eu/system/files/2024-04/edpb_guidelines_202201_data_subject_rights_access_v2_de.pdf.

[78] Leitlinien 01/22 (Fn. 77), Rn. 184.

— **Keine Erkennbarkeit, dass die Unterlagen benötigt werden, um Kenntnis über Datenschutzverstöße zu erhalten**

Die Argumentation, der Antrag habe keinen für die Schule erkennbaren Bezug zum Datenschutz und es sei kein Vorteil durch die Herausgabe der Kopien ersichtlich, ist nicht geeignet, einen Exzess zu begründen oder sonst eine Ablehnung des Antrags zu rechtfertigen.

Der Europäische Gerichthof[79] hat unter Hinweis auf den von Wortlaut des Art. 12 Abs. 5 und Art. 15 Abs. 3 DSGVO entschieden, dass Auskunftsersuchende ihren Antrag nicht begründen müssen und die Verpflichtung aus Art. 15 Abs. 1, Abs. 3 DSGVO auch dann gilt, wenn der Antrag mit einem anderen Zweck als einem in Erwägungsgrund 63 Satz 1 DSGVO genannten („um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können") begründet wird.

Aus meiner Sicht wäre im Übrigen im konkreten Fall ein Motiv mit datenschutzrechtlichem Bezug durchaus denkbar gewesen.

— **„Schikane"**

Die für „Schikane" angeführten Begründungen waren ebenfalls nicht geeignet, einen Exzess abzuleiten.

Aus Spannungen zwischen Erziehungsberechtigten und Schule oder einer Antragstellung „erst am Schuljahresende" kann nicht auf ein „schikanöses" Vorgehen geschlossen werden. Dies gilt auch für das von der Schule vorgebrachte Argument, der Auskunftsantrag sei auf bestimmte Unterlagen beschränkt worden. Wer schikanieren will, wird bestehende Rechte gerade möglichst umfassend nutzen wollen.

Auch die geäußerte Vermutung, dass sich die Eltern mit dem Antrag für ein nicht zufriedenstellendes Prüfungsergebnis revanchieren wollten, belegte die Schule nicht. Vielmehr stellte sie sogleich selbst fest, dass dies vermutlich zunächst keine Auswirkung auf das Auskunftsbegehren habe. Es gehe hier aber um die grundsätzliche **Abwägung**, was die Schule im konkreten Fall leisten müsse. Einen gesetzlichen Anknüpfungspunkt für diese eigenständige „Rechtsfortbildung" nannte die Schule nicht. Zu Letzterem hielt ich nachdrücklich fest, dass bei einem Antrag nach Art. 15 DSGVO die gesetzlichen Voraussetzungen zu prüfen sind und – sind sie erfüllt – die Auskunft zu erteilen ist.

— **Bereits bestehende Kenntnis von Unterlagen, § 10 Abs. 4 Satz 2 Grundschulordnung (GrSO)**

Unabhängig davon, dass den Eltern nach Angaben der Schule „nahezu" alle beantragten Unterlagen bereits bekannt waren: Kenntnisnahmen nach § 10 Abs. 4 Satz 2 GrSO sind nicht geeignet, einen Auskunftsanspruch zu einem späteren Zeitpunkt (insbesondere gegen Ende des Schuljahres) auszuschließen.

[79] Urteil vom 26. Oktober 2023, C-307/22.

§ 10 GrSO
Leistungsnachweise
(4) […] [2]Sie sind den Schülerinnen und Schülern zur Kenntnisnahme durch die Erziehungsberechtigten mit nach Hause zu geben; in begründeten Einzelfällen kann von dieser Regelung abgewichen werden. [3]Sie sind der Schule binnen einer Woche zurückzugeben.

Diese Vorschrift steht mit Art. 15 DSGVO in keinem Zusammenhang; sie will weder nach ihrem Wortlaut noch nach ihrem Sinn und Zweck Auskunftsansprüche einschränken. Auch die Anforderungen nach Art. 23 DSGVO für Vorschriften, welche die Betroffenenrechte einschränken, dürften nicht erfüllt sein. Darüber hinaus ist Sinn des Auskunftsanspruchs nach Art. 15 DSGVO unter anderem, sich ein Bild von der aktuellen Speicherung personenbezogener Daten und deren Umfang machen zu können. Dadurch kann beispielweise nachvollzogen werden, ob Unterlagen zwischenzeitlich annotiert, ergänzt oder sonst verändert worden sind. Des Weiteren können sich zwischenzeitlich Umstände ergeben haben, die Antragstellende erst nach einer Kenntnisnahme gemäß § 10 Abs. 4 Satz 2 GrSO zu einer genaueren Prüfung Anlass geben.

– **Möglichkeit der Einsichtnahme in die Schülerunterlagen, § 41 Bayerische Schulordnung (BaySchO)**

Unabhängig von weiteren Aspekten kann die Möglichkeit der Einsichtnahme nach § 41 BaySchO offensichtlich einer Auskunft nach Art. 15 DSGVO schon deshalb nicht entgegenstehen, da in § 41 Abs. 3 BaySchO ausdrücklich geregelt ist, dass andere ein Recht auf Einsicht oder Auskunft gewährende Vorschriften unberührt bleiben. Dies bezieht sich im Besonderen auf Art. 15 DSGVO.

– **Erheblicher Mehraufwand, keinen Präzedenzfall schaffen**

Die Argumentation „eine Auskunftserteilung auf Grundlage der Datenschutz-Grundverordnung würde für die betroffene Schule darüber hinaus einen erheblichen Mehraufwand bedeuten“ findet als Ablehnungsgrund keinen Niederschlag im Gesetz (vgl. hierzu im Übrigen auch die zitierten Leitlinien[80]).

Auch die Auswirkungen einer in den Raum gestellten fiktiven Information einer fiktiven Person auf einem fiktiven Portal ist nicht geeignet, an der bestehenden Auskunftspflicht etwas zu ändern: Man stelle sich vor, jemand würde auf einem Portal darüber informieren, man solle keinen Präzedenzfall schaffen.

Unabhängig von der fehlenden rechtlichen Relevanz des angeführten Begriffs „Präzedenzfall“ im Rahmen des Art. 15 DSGVO handelt es sich hierbei nicht um einen „Präzedenzfall“ bezogen auf Prüfungsarbeiten (vgl. hierzu etwa meinen 33. Tätigkeitsbericht 2023 unter Nr. 8.4).

[80] Leitlinien 01/22 (Fn. 77), Rn. 188.

6.3 Masernschutz – Vorlage von Nachweisen an weiterführenden Schulen

Zur Weitergabe ärztlicher Atteste über Kontraindikationen gegen eine Masernimpfung von Schulen an Gesundheitsämter habe ich mich bereits in meinem 33. Tätigkeitsbericht 2023 unter Nr. 8.2 geäußert.

Im Berichtszeitraum wandte sich eine Mutter an mich, da eine weiterführende Schule bei der Schuleinschreibung die Vorlage eines Nachweises über die erfolgte Impfung gegen Masern verlangte. Den **Nachweis hatte die Mutter bereits der zuvor besuchten Grundschule** vorgelegt (vgl. § 20 Abs. 9 Satz 1 Nr. 1 Infektionsschutzgesetz – IfSG). Die Mutter hinterfragte deshalb, ob es tatsächlich notwendig sei, dass sie die erfolgte Impfung auch gegenüber der weiterführenden Schule nachweist. Ähnliche Gedanken hatten sich auch die Gesetzgeber gemacht. Daher genügt auch eine Bestätigung der zuvor besuchten Grundschule, dass ein Nachweis bereits vorgelegen hat (vgl. § 20 Abs. 9 Satz 1 Nr. 3 IfSG). Diese **Bestätigung erfolgt im Regelfall durch die Weitergabe des Masern-Dokumentationsbogens** auf Grundlage von § 39 Abs. 1 Satz 4 Bayerische Schulordnung.

Die Schule teilte mir zwar mit, es habe auch Fallgestaltungen gegeben, in denen eine Bestätigung durch die zuvor besuchte Schule nicht möglich gewesen sei, beispielsweise bei einem Zuzug aus dem Ausland. Sie musste jedoch einräumen, dass einzelne Ausnahmen nicht dazu führen können, von allen Schülerinnen und Schülern (erneut) einen Nachweis zu verlangen, also auch von denjenigen, bei denen eine Schülerin oder ein Schüler zwischen öffentlichen Schulen wechselt und eine Bestätigung mittels der Weitergabe des Dokumentationsbogens durch die vorhergehende Schule erfolgt.

Die Schule änderte daraufhin die (beabsichtigte) Verfahrensweise. Das Kultusministerium hatte die Rechtslage übrigens bereits zuvor auf seiner Website erläutert. Der aufmerksamen Mutter ist es zu verdanken, dass sich auch diese Schule künftig daran halten wird und Eltern Nachweise nicht unnötig mehrfach vorlegen müssen. In dieser Konstellation wird **beispielhaft** deutlich, dass **Datenschutz keine zusätzliche Bürokratie verursacht, sondern zu effektivem Verwaltungshandeln beiträgt.**

6.4 Unzulässige Datenübermittlung durch Klassenelternsprecher über Eltern-Messenger-Gruppe

Hat jemand die Trinkflasche meiner Tochter gesehen? Wer beteiligt sich am Geschenk für den Klassenlehrer? Kann jemand beim Adventsfrühstück helfen? Zur schnellen Klärung dieser oder ähnlicher Fragen gründen die Eltern von Kindern derselben Schulklasse oft eine gemeinsame Messenger-Gruppe. Dass diese einen einfachen Weg bietet, alle Eltern schnell zu erreichen, haben mittlerweile auch einige Schulen erkannt. Manchmal werden deshalb – sozusagen durch die Hintertür – die Klassenelternsprecher gebeten, schulrelevante Informationen schnell über die Messenger-Gruppe an die anderen Eltern weiterzugeben. Vielen ist hierbei jedoch nicht bewusst, dass Klassenelternsprecher (Art. 64 Abs. 2 Satz 1 Bayerisches Erziehungs- und Unterrichtsgesetz – BayEUG) – wie auch Elternbeiräte – als Organe der Schule einzuordnen sind. Das Handeln der Klassenelternsprecher **in dieser Funktion wird datenschutzrechtlich der Schule zugerechnet.** Aufgrund des fehlenden Bewusstseins hierfür werden die Elternsprecher meistens auch nicht datenschutzrechtlich geschult.

Die daraus resultierende Unwissenheit war mutmaßlich Ursache dafür, dass in einem Beschwerdefall die Klassenelternsprecher in der gemeinsamen Messenger-Gruppe darüber informierten, dass aufgrund eines „rechtlichen Streites zwischen einer Familie der Klasse und der Schule“ die vorweihnachtliche Feier abgesagt werden musste. Die betroffene Familie fühlte sich durch diese Informationsweitergabe an den Pranger gestellt und wandte sich diesbezüglich an mich. Im Rahmen der bei der Schule eingeholten Stellungnahme wurde klar, dass sich die Schule für das Handeln der Klassenelternsprecher zunächst nicht verantwortlich fühlte. Außerdem war man der Ansicht, keine personenbezogenen Daten im Sinne des Art. 4 Nr. 1 DSGVO weitergegeben zu haben. Angesichts der Gesamtumstände des konkreten Falles war jedoch von einer **Personenbeziehbarkeit** und damit Einordnung als personenbezogene Daten auszugehen.

Unabhängig von weiteren Aspekten erfolgte die Übermittlung der personenbezogenen Daten jedenfalls ohne die erforderliche Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 DSGVO, weshalb ich gegenüber der Schule einen Datenschutzverstoß festgestellt habe. Die Schule sicherte mir zu, die datenschutzrechtlichen Vorgaben zukünftig strikt zu beachten und auch die Klassenelternsprecher dementsprechend zu sensibilisieren.

6.5 Überwachungsdruck in der Schule durch deaktivierte Kameras oder fehlende Hinweise

Mit Blick auf das Recht auf informationelle Selbstbestimmung sind **Videoüberwachungen an Schulen nur in engen Grenzen zulässig.** Dazu habe ich mich in meinen Tätigkeitsberichten bereits mehrfach geäußert (siehe den 29. Tätigkeitsbericht 2019 unter Nr. 10.2, den 27. Tätigkeitsbericht 2016 unter Nr. 10.5, den 26. Tätigkeitsbericht 2014 unter Nr. 10.9.1, den 25. Tätigkeitsbericht 2012 unter Nr. 10.5 sowie den 23. Tätigkeitsbericht 2008 unter Nr. 12.2.2).

Möchte eine Schule eine Videoüberwachungsanlage installieren, hat sie zuerst anhand des Art. 24 BayDSG und der Anlage 2 Abschnitt 6 zu § 46 Bayerische Schulordnung (BaySchO) die rechtlichen Vorgaben zu prüfen. Auch Nr. 3.2.3 Bekanntmachung des Bayerischen Staatsministeriums für Unterricht und Kultus über den Vollzug des Datenschutzrechts an staatlichen Schulen (VollzBek DS – Schulen)[81] enthält Ausführungen hierzu.

Nachdem mir in einem Beschwerdefall die betreffende Schule die Zulässigkeit für einen Teil der installierten Kameras – unter anderem aufgrund einer fehlenden Vorfallsdokumentation – nicht nachweisen konnte, mussten diese Kameras wieder abgeschaltet werden.

Entgegen der Zusage der Schule wurden die deaktivierten Kameras jedoch nicht abgedeckt oder die Außerbetriebnahme anderweitig kenntlich gemacht. Ich musste deshalb erneut an die Schule herantreten und sie darauf hinweisen, dass auch der Anschein einer Videoüberwachung dazu führen kann, dass sich betroffene Personen – in der fälschlichen Annahme des Betriebes – beobachtet oder beeinträchtigt fühlen und ihr Verhalten bewusst oder unbewusst der vermeintlichen Beobachtungssituation entsprechend anpassen. Da von **deaktivierten Videokameras** in der Sache – gleichermaßen wie bei funktionsfähigen Videokame-

[81] Vom 14. Juli 2022 (BayMBl. Nr. 435).

ras – ein sogenannter **Überwachungsdruck** für die betroffenen Personen entsteht, stellt ihre Vorhaltung einen Eingriff in das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 und Art. 1 Abs. 1 Grundgesetz dar. Auf meinen Hinweis sind die deaktivierten Kameras von der Schule nunmehr vollständig abgebaut worden.

Bei den (zulässigen) **aktiven Kameras** musste ich wiederum feststellen, dass der Überwachungszeitraum (22 bis 6 Uhr) nicht kenntlich gemacht war. Hierdurch entsteht letztlich ein ähnlicher Überwachungsdruck wie soeben beschrieben. Außerdem ist bei einer zeitlichen Begrenzung der Videoüberwachung bereits aufgrund des Transparenzgebotes gemäß Art. 24 Abs. 2 BayDSG **das konkrete Zeitintervall des Betriebes auf den Hinweisen anzugeben.** Auch darauf habe ich die Schule aufmerksam gemacht.

7 Informationsfreiheit

7.1 Ignorieren von Auskunftsanträgen – Ende gut alles gut?

In meinem 33. Tätigkeitsbericht 2023 hatte ich unter Nr. 10.2 darüber berichtet, dass es keine gute Option ist, Auskunftsanträge nach Art. 39 BayDSG zu ignorieren. Von 68 Kommunen, die ich unter Fristsetzung zur Beantwortung des Auskunftsantrags eines Vereins aufgefordert hatte, verblieben nach Darstellung des Vereins **19 Kommunen**, die ihm bis zum Fristablauf nicht geantwortet hatten. Daraufhin bat ich diese Kommunen unter erneuter Fristsetzung im Hinblick auf eine mögliche förmliche Beanstandung um Stellungnahme. Den Fortgang im Jahr 2024 stelle ich nachfolgend dar.

Acht Kommunen antworteten mir nicht innerhalb der gesetzten Frist. Nach Art. 16 Abs. 1 Satz 1 BayDSG müssen mich die Kommunen in der Erfüllung meiner Aufgaben unterstützen. Insbesondere haben sie mir nach Art. 16 Abs. 1 Satz 2 Var. 1 BayDSG alle zur Erfüllung meiner Aufgaben notwendigen Auskünfte zu geben. Daher beanstandete ich nach Art. 16 Abs. 4 BayDSG Verstöße gegen Art. 16 Abs. 1 Satz 1 und Satz 2 Var. 1 BayDSG. Dies hatte ich bereits in meinen vorangegangenen Schreiben in Aussicht gestellt.

Diese Beanstandungen verband ich mit einer erneuten Fristsetzung und der Ankündigung, nach Art. 16 Abs. 4 Satz 3 BayDSG von der jeweiligen Rechtsaufsichtsbehörde geeignete Maßnahmen zur Abhilfe zu fordern, sollte mir innerhalb der gesetzten Frist weiterhin keine Stellungnahme zugehen. Die Rechtsaufsichtsbehörden erhielten zugleich Abdrucke meiner Schreiben an die Kommunen.

Daraufhin erhielt ich die angeforderten Stellungnahmen. Gegenüber sechs dieser Kommunen sprach ich jeweils eine weitere Beanstandung aus, nun wegen Verstoßes gegen Art. 39 BayDSG. Im Rahmen der Stellungnahmen hatte sich zwar herausgestellt, dass die Kommunen dem Verein auf seinen Antrag mittlerweile geantwortet hatten. Allerdings geschah dies deutlich nach Ablauf eines angemessenen Zeitraums (vgl. auch hierzu meinen 33. Tätigkeitsbericht 2023 unter Nr. 10.2).

Sechs andere Kommunen nahmen mir gegenüber zwar sogleich fristgerecht Stellung. Auch bei ihnen ergab sich, dass sie dem Verein nunmehr auf seinen Antrag geantwortet hatten. Sie hatten jedoch ebenfalls einen angemessenen Zeitraum weit überschritten, sodass ich auch hier Verstöße gegen Art. 39 BayDSG beanstandete.

Auf Beanstandungen verzichtet habe ich bei lediglich zwei „zögerlichen“ Kommunen. Sie konnten die verspätete Reaktion gegenüber dem Verein nachvollziehbar erläutern und waren um die Einhaltung der rechtlichen Vorschriften ersichtlich bemüht, was etwa dadurch deutlich wurde, dass sie Maßnahmen ergriffen, um zukünftig eine angemessene Beantwortungszeit sicherzustellen.

Die übrigen Beschwerden erledigten sich im weiteren Verlauf auf andere Weise auch im Austausch mit dem Verein, wenn etwa der Eingang eines Antrags nicht feststellbar oder eine Antwort doch schon früher erfolgt war.

Im Ergebnis erhielt der Verein in allen aufrechterhaltenen Beschwerdefällen Antworten von den Kommunen und ich erhielt die angeforderten Stellungnahmen. **Also: Ende gut alles gut? Noch nicht wirklich.** Denn tatsächlich gut wäre es, wenn alle **bayerischen Behörden Auskunftsanträge zeitnah beantworten und dadurch ein unnötiger Einsatz von Zeit und Ressourcen bei allen Beteiligten möglichst vermieden wird.**

7.2 Berechtigtes Interesse

Der Auskunftsanspruch nach Art. 39 BayDSG setzt voraus, dass die antragstellende Person ein berechtigtes Interesse glaubhaft darlegt. Im 33. Tätigkeitsbericht 2023 unter Nr. 10.3 habe ich dazu ausgeführt, dass noch immer nicht allen Behörden klar zu sein scheint, dass ein berechtigtes Interesse grundsätzlich jedes rechtliche, wirtschaftliche oder ideelle Interesse sein kann.

Anhand eines Vorgangs aus dem Berichtszeitraum möchte ich nochmals beispielhaft verdeutlichen, dass eine zutreffende Einordnung weiterhin nicht immer gelingt.

In der Nachbarschaft eines Antragstellers befand sich ein Betrieb, aus dem unter anderem Lärm und erheblicher Anlieferverkehr resultierten. Der Antragsteller hatte vorgetragen, dass er durch den – aus seiner Sicht in dieser Form unzulässigen – Betrieb sowie den Lieferverkehr beeinträchtigt werde. Er benötigte die beantragten Auskünfte daher zur Wahrung seiner Rechte auf Gesundheit und Eigentum, insbesondere wollte er eine Beeinträchtigung seiner Lebensqualität und Nachtruhe verhindern sowie einer Wertminderung seiner Immobilie entgegenwirken.

Die zuständige Behörde lehnte den Auskunftsantrag ab, da ein berechtigtes Interesse nicht glaubhaft dargelegt worden sei. Sie führte aus, dass die zulässigen Lärmrichtwerte an seinem Haus eingehalten würden und es keinen Anspruch auf völlig immissionsfreies Wohnen gebe. Mit einer gewissen Lärmbelästigung sei zu rechnen, diese sei auch hinzunehmen, sodass eine Beeinträchtigung der Lebensqualität nicht ersichtlich sei. Inwieweit die Gesundheit beeinträchtigt sein solle, sei nicht schlüssig dargelegt und nicht nachvollziehbar. Die Wertminderung seiner Immobilie sei in keiner Weise substantiiert belegt und im Übrigen in einem verwaltungsrechtlichen Verfahren ohne jede Relevanz.

Die Behörde hat hier die Anforderungen an die glaubhafte Darlegung eines berechtigten Interesses überdehnt. Der Betrieb und der Lieferverkehr hatten nach den Darlegungen des Antragstellers Auswirkungen auf seine Lebens- und Wohnsituation. Ich habe der Behörde mitgeteilt, dass der Antragsteller seine unmittelbare Betroffenheit durch den Betrieb sowie den zugehörigen Lieferverkehr und damit auch ein berechtigtes Interesse glaubhaft dargelegt hat. Nur beispielhaft möchte ich darauf hinweisen, dass es **an dieser Stelle** nicht darauf ankommt, ob die Behörde den Betrieb und seine Lärmemissionen immissionsschutzrechtlich als zulässig erachtet. Maßgeblich ist vielmehr, ob ein berechtigtes Interesse an Auskünften aus den Akten und Dateien hierzu besteht. Vorliegend waren die Darlegungen des Antragstellers ausreichend, weitere Ausführungen oder gar Nachweise durch Atteste oder Gutachten zu verlangen, würde die Anforderungen weit überspannen.

Im geschilderten Fall kam es übrigens letztlich gar nicht auf ein berechtigtes Interesse an. Denn die begehrten Daten waren als Umweltinformationen einzuordnen, sodass der allgemeine Auskunftsanspruch nach Art. 39 Abs. 2 BayDSG hinter den Zugangsanspruch nach Art. 3 Abs. 1 Satz 1 Bayerisches Umweltinformationsgesetz zurücktrat, der die glaubhafte Darlegung eines berechtigten Interesses nicht verlangt.

7.3 Auskunftsbegehren gegenüber einer Kommune zum „Abschleppkatalog“

Ein Bürger hatte in der Zeitung von einem „Abschleppkatalog“ gelesen, der vorher definierte Standardsituationen und das Vorgehen zum Abschleppen beschreiben solle. Daraufhin stellte er unter Hinweis auf den Zeitungsartikel einen Antrag auf Auskunft bei der Kommune, wie die genauen Regelungstatbestände lauteten.

Die Kommune lehnte den Antrag ab, da kein berechtigtes Interesse glaubhaft dargelegt worden sei. Daraufhin bat mich der Antragsteller um Unterstützung, denn er habe als Bürger selbstverständlich einen Anspruch auf Transparenz.

Ein berechtigtes Interesse kann grundsätzlich jedes rechtliche, wirtschaftliche oder ideelle Interesse sein (vgl. Nr. 7.2). Für die Bejahung eines berechtigten Interesses sind keine hohen Anforderungen zu stellen.

Nicht ausreichend ist allerdings das bloße Bestehen eines berechtigten Interesses oder die Mitteilung eines berechtigten Interesses an mich. Das berechtigte Interesse **muss** – so die gesetzliche Regelung – **der Stelle, von der die Auskunft begehrt wird, „glaubhaft dargelegt“ werden.** Denn diese Stelle hat in der Folge zu prüfen, ob die (weiteren) Voraussetzungen für einen Zugangsanspruch vorliegen.

Da der Antrag keine Ausführungen über das bloße Begehren der Auskunft hinaus enthielt, empfahl ich dem Antragsteller, der Kommune sein Interesse an der Auskunft darzulegen.

Nachdem er dies nachgeholt hatte, blieb eine Reaktion der Kommune erst einmal aus. Daher forderte ich die Kommune zur Stellungnahme auf. Sie machte mir gegenüber dann mehrere Ablehnungsgründe geltend: Unter anderem handele es sich beim „Abschleppkatalog“ um einen Datei- und Aktenbestandteil der Polizei, der sich (auch) in den Dateien und Akten der Kommune befinde. **Eine Auskunft aus Datei- und Aktenbestandteilen der Polizei** sei **nach Art. 39 Abs. 4 Satz 1 Nr. 4 in Verbindung mit Abs. 4 Satz 2 BayDSG** jedoch **ausgeschlossen.**

Um mir ein vollständiges Bild zu machen, forderte ich den „Abschleppkatalog“ an und bat um eine ergänzende Stellungnahme.

Letztendlich war gegen die Einordnung des „Abschleppkatalogs“ als Datei- und Aktenbestandteil der Polizei im Sinne von Art. 39 Abs. 4 Satz 1 Nr. 4 in Verbindung mit Abs. 4 Satz 2 BayDSG **nichts einzuwenden**. Zusammengefasst definiert der „Abschleppkatalog“ Örtlichkeiten in der Kommune, an denen verbotswidrig parkende Kraftfahrzeuge auf Initiative der kommunalen Verkehrsüberwachung abgeschleppt werden können. Abschleppungen verbotswidrig abgestellter Fahrzeuge sind hoheitliche Maßnahmen der Polizei. Soweit eine Örtlichkeit des „Abschleppkatalogs“ betroffen ist, wird die Kommune mit der unmittelbaren Ausführung der Maßnahme beauftragt.

Der „Abschleppkatalog“ an sich werde von der Polizei als Excel-Datei geführt und ist mit dem Namen der zuständigen Polizeidienststelle und dem Aktenzeichen überschrieben. Die Polizei übe die „Hoheit“ über den „Abschleppkatalog“ aus. Soweit die Kommune eine Anpassung des „Abschleppkatalog“ wünsche, wende sie sich an die Polizei, die dann entsprechende Änderungen vornehmen könne. Es komme auch vor, dass die Polizei den „Abschleppkatalog“ von sich aus ändere und die Kommune darüber informiere.

Art. 39 Abs. 4 Satz 2 BayDSG regelt die Beschränkung der informationellen Verfügungsbefugnis. Ein wichtiger Anhaltspunkt für die Feststellung einer fehlenden Verfügungsbefugnis ist die Urheberschaft der Information, mit anderen Worten, es ist die Stelle verfügungsbefugt, welche die Information im Rahmen ihrer Aufgabenerfüllung erhoben oder „kreiert“ hat.[82] Vorliegend wird der „Abschleppkatalog“ von der Polizei geführt. Sie ist mithin Urheber der darin enthaltenen Informationen. Mit der Dispositionsmacht bezüglich des Inhalts verbleibt die Verfügungsberechtigung hinsichtlich des Mediums bei der die Dispositionsmacht innehabenden Stelle.[83] Auch die Dispositionsmacht über den Inhalt des „Abschleppkatalogs“ liegt vorliegend bei der Polizei. Ausschließlich die Polizei nimmt Änderungen an der Datei vor.

Ich teilte der Kommune und dem Antragsteller mit, dass ein Auskunftsanspruch nach Art. 39 BayDSG aus den genannten Gründen nicht besteht, die Kommune lehnte den Auskunftsantrag gegenüber dem Antragsteller ab.

7.4 Kosten für die beantragte Auskunft gemäß Art. 39 Abs. 5 BayDSG

Ein Bürger staunte kürzlich nicht schlecht, als eine Stadt die voraussichtlich anfallenden Kosten für die von ihm beantragte Auskunft nach Art. 39 Abs. 1 BayDSG mit etwa 450,– Euro bezifferte. Er wandte sich daraufhin an mich und bat um Überprüfung, da er die Kostenforderung der Stadt für – so der Beschwerdeführer – ein „monetäres Schutzschild“ hielt, um den beantragten städtebaulichen Vertrag nicht der Öffentlichkeit zugänglich machen zu müssen.

Nach Art. 15 Abs. 1 Satz 1 BayDSG überwache ich die Einhaltung des Bayerischen Datenschutzgesetzes – folglich auch des Art. 39 BayDSG – und anderer Vorschriften **über den Datenschutz** bei den bayerischen öffentlichen Stellen. Gemäß Art. 39 Abs. 5 BayDSG kann eine öffentliche Stelle für die Auskunft Kosten nach Maßgabe des Kostengesetzes erheben. Insofern ist gegen eine Kostenforderung an sich datenschutzrechtlich grundsätzlich nichts einzuwenden.

Die konkrete **Kostenentscheidung** selbst ist jedoch keine datenschutzrechtliche Frage und **unterliegt daher nicht meiner Aufsichtszuständigkeit.** Selbst wenn man die Ansicht vertreten würde, dass es mir im Rahmen meiner Zuständigkeit möglich wäre, eine Vereitelung der effektiven Ausübung des Anspruchs nach Art. 39 BayDSG durch eine **offensichtlich unverhältnismäßige** Kostenforderung (ähnlich dem Verbot der prohibitiven Wirkung in § 10 Abs. 2 Informationsfreiheitsgesetz [des Bundes]) zu prüfen, konnte ich eine solche im betreffenden Fall nicht erkennen: Die veranschlagten Kosten bewegten sich im zulässigen Rahmen.

[82] v. Lewinski, in: Schröder, Bayerisches Datenschutzgesetz, 2021, Art. 39 Rn. 109 f.

[83] Engelbrecht, in: Wilde/Ehmann/Niese/ Knoblauch, Datenschutz in Bayern, Stand 4/2023, Art. 39 BayDSG Rn. 31.

Außerdem hatte die Stadt dargestellt, dass es sich um ein umfangreiches Vertragswerk handeln würde, welches intensiv auf möglicherweise zu schwärzende Stellen durchgesehen werden müsse.

8 Technik und Organisation

8.1 Fotos veröffentlichen = KI trainieren?

Entwickler von Systemen Künstlicher Intelligenz (KI) sind auf eine Nutzung umfangreicher Datenbestände angewiesen, wenn sie auf statistische Verfahren gestützte Modelle effektiv trainieren möchten. Allgemein gilt der Grundsatz: Die Qualität der Ergebnisse steigt mit der Quantität der Trainingsdaten. Was liegt da näher, als den „Datenhunger" der KI mit öffentlich verfügbaren Informationen zu stillen?

Das Internet bietet hier reichlich Nahrung: Die Bilddokumentation des eigenen Lebens unter Einschluss zahlreicher anderer Personen in Sozialen Medien ist längst keine Seltenheit mehr. Dabei sind in Fotos oft mehr Informationen gespeichert, als es den Beteiligten lieb ist: Kontexte, Bildbeschreibungen, auch die gern übersehenen, oftmals automatisiert angelegten Metadaten „plaudern" darüber, wer wo wie abgebildet ist. Eine KI, die aus solchen Daten lernt, wird dann auch damit arbeiten.

Der vorliegende Beitrag ordnet die skizzierten Risiken ein und gibt Bürgerinnen und Bürgern wie auch bayerischen öffentlichen Stellen Empfehlungen für präventive Maßnahmen.

8.1.1 Um welche Risiken geht es?

Viele Nutzerinnen und Nutzer von internetbasierten Anwendungen, insbesondere Sozialen Medien, haben keine genauen Vorstellungen darüber, wie detailreich ihr digitales Abbild ausfällt – und welche „Schönheitsfehler" es im Einzelnen (schon) zeigt. Manche vor Jahren geschriebenen Posts und hochgeladenen Fotos sind immer noch öffentlich, selbst wenn die Kennung und das Passwort für die betreffende Plattform längst vergessen sind und die Nutzerin oder der Nutzer auf andere Plattformen weitergezogen ist. Vielen Nutzenden war bei alldem auch nie so recht bewusst, dass moderne Smartphones gespeicherte Fotos häufig „von sich aus" mit Metadaten wie dem Namen oder Geokoordinaten anreichern. **Nutzende können deshalb durchaus weit mehr von sich öffentlich preisgegeben haben, als ihnen aktuell bewusst und/oder erwünscht ist.**

Was einmal an zuordnungsfähigen Informationen, insbesondere an Fotos, öffentlich ist, kann grundsätzlich jedermann zu Gesicht bekommen – auch derzeitige (oder zukünftige) Vorgesetzte, Geschäftspartnerinnen, die Gegenpartei in einem Rechtsstreit, Mitschüler, (Ex-)Partner oder Verwandte. Ganz unscheinbar und zunächst einmal unbemerkt gesellt sich eine wachsende Anzahl von KI-Systemen hinzu, die öffentlich abrufbare Informationen zu unterschiedlichen, teils unbekannten oder sogar unerwünschten Zwecken sammeln („crawlen") und nutzen.

Initiativen wie das Large-scale Artificial Intelligence Open Network (LAION) kommen den KI-Entwicklern noch weiter entgegen: Nach ihren an sich positiv klingenden Grundsätzen von Transparenz und Offenheit bietet diese Non-Profit-Organisation eigenen Angaben zufolge Trainings-Datensätze, Werkzeuge und Modelle zum Experimentieren mit Machine Learning zur freien Verfügung an. Auf dieser

Grundlage sollen KI-Anwendungen ohne hohe Investitionskosten für den Aufbau umfangreicher Datenbestände entwickelt werden können, damit – so das Ziel dieser Organisation – nicht ausschließlich finanzstarke Großunternehmen den Markt- und Forschungsbereich „KI" unter sich aufteilen. Wie ein bekannt gewordener Fall zeigt, können solche Trainingsdatensätze jedoch auch (ungewollt) sogar sensible personenbezogene Daten enthalten: Bei der Analyse des Trainingsdatensatzes für die KI-Bildgenerierung „LAION-5B"[84] haben Datenjournalistinnen des Bayerischen Rundfunks eine Vielzahl an Informationen entdeckt, mit denen Personen identifiziert werden könnten: Neben Gesichtern und Namen fanden sie Geokoordinaten, E-Mails und sogar Kontonummern.[85]

Das Beispiel zeigt: Angesichts des „Datenhungers" von KI und der bereits heute umfangreichen Verarbeitung öffentlich abrufbarer Informationen ist immer wieder zu überdenken, welche potenziellen Risiken mit einer Veröffentlichung personenbezogener Informationen einhergehen können. Unbeabsichtigt preisgegebene, zusätzliche Informationen in Form von Metadaten verschärfen das Problem zusätzlich.

Insbesondere trägt der internationale Datenhandel dazu bei, dass „das Internet" einmal veröffentlichte Daten oft nicht „vergisst" – selbst wenn personenbezogene Daten auf Löschungsanträge hin aus einzelnen Trainingsdatensätzen vielleicht eliminiert werden können. Sind die Daten einmal in ein KI-System eingeflossen, gestaltet sich die Situation noch komplizierter: Einzelne Daten können grundsätzlich nicht wieder „heraustrainiert" werden. Vielmehr müsste das jeweilige Modell mit einem aktualisierten Trainingsdatensatz „fortgebildet" werden (was mit erheblichen Kosten verbunden wäre). Zudem lässt sich an einem trainierten Modell in der Regel nicht nachweisen, dass bestimmte Daten Teil der Trainingsdaten waren.

Die Risiken für die Rechte und Freiheiten der Bürgerinnen und Bürger wachsen also. Werden etwa Personenfotos zum Training KI-gestützter Gesichtserkennung genutzt und wird dieses Instrument etwa in einem Urlaubsland für Fahndungszwecke eingesetzt, können sich bei einer „ahnungslosen" Einreise leicht nachteilige Konsequenzen ergeben – zumal im Fall falsch-positiver Treffer.

8.1.2 Fotos: mehr als die Summe ihrer Pixel

Beim Speichern eines Fotos können der eigentlichen Aufnahme zusätzliche Informationen (sog. Metadaten) – meist automatisiert – hinzugefügt werden. Dabei fungiert etwa das „Exchangeable Image File Format" (kurz: „Exif") als Standard für solche Metadaten und definiert eine ganze Reihe an Datenfeldern (sog. „Exif-Tags") mit technischen Informationen,[86] wie etwa Kameramodell, Zeitpunkt der Aufnahme oder Kameraeinstellungen. Die Liste an Informationen wirkt auf den ersten Blick unauffällig, doch können gleich in mehreren Datenfeldern personenbezogene Daten hinterlegt werden. Besonders erwähnenswert sind hier die Felder „Autor/Fotograf" sowie der Copyright-Vermerk, die ganz bewusst einen Personenbezug vorsehen, aber auch die geografische Position, die von Geräten mit integriertem GPS-Sensor hinzugefügt wird (fast jedes moderne Smartphone verfügt über einen solchen). Viele sind sich der Existenz dieser Datenfelder ebenso wenig bewusst wie der schädlichen Verwendungsmöglichkeiten für deren Inhalte.

84 Internet: https://laion.ai/blog/laion-5b.
85 Internet: https://interaktiv.br.de/ki-trainingsdaten.
86 Ausführliche Liste unter: https://exiftool.org/TagNames/EXIF.html.

Werden Fotodateien mit Exif-Tags im Internet veröffentlicht, kann die Privatsphäre beispielsweise folgendermaßen beeinträchtigt werden:

— **Ortungsverfolgung:** Eine Person veröffentlicht ein Urlaubsfoto an einem Strand. Das Foto weist keine besonderen Landschaftsmerkmale auf, und die Person ist deshalb der Überzeugung, dass ihr konkreter Aufenthaltsort bei einer Veröffentlichung dieses Fotos unbekannt bleibt. Das für die Aufnahme genutzte Smartphone speichert jedoch im Hintergrund die Geokoordinaten mit ab. Wird diese Bilddatei auf ein Soziales Netzwerk hochgeladen, können die Metadaten ausgelesen werden, um den Standort des Benutzers zu erfahren. Dass es sich hierbei um kein rein theoretisches Szenario handelt, zeigt ein Fall, über den die Presse bereits im Jahr 2012 berichtete.[87]

— **Veröffentlichung privater Momente:** Angenommen, eine Person lädt ein Bild mit sensiblen Inhalten – wie zum Beispiel ein freizügiges Foto oder eine private Versammlung – in der Annahme hoch, dass sie selbst auf dem Foto nicht ohne weiteres identifizierbar ist (Gesicht nicht ausreichend gut erkennbar). Da die Metadaten aber den Namen des Benutzers enthalten können, ist mit diesen unbewusst mitgespeicherten Informationen unter Umständen doch eine Identifizierung möglich. Dies war zwar bereits vor der Existenz aktueller KI möglich, neueste Entwicklungen in der Bilderkennung und im gesamten Verarbeitungsprozess verschärfen das Problem aber deutlich. Fotos können automatisiert in sehr großer Zahl und sehr hoher Geschwindigkeit verarbeitet, verglichen und ganz allgemein mit anderen Fotos und Informationen zusammengeführt werden. Das ist betroffenen Personen beim Hochladen oder dem Festlegen der Privatsphäreeinstellungen oftmals kaum bewusst. Fotos, auf denen Gesichter zu erkennen sind, können schnell zur Quelle einer Rufschädigung werden.

  In diesem Zusammenhang sorgte die US-amerikanische „Gesichtersuchmaschine" Clearview AI bereits mehrfach für Aufsehen. Diese kostenpflichtige Software erlangte 2020 Bekanntheit, als die New York Times mit einer Recherche die eindrucksvolle Datensammlung des Unternehmens aufdeckte.[88] In der Suchmaschine kann neben dem Namen auch ein Foto als Suchkriterium genutzt werden.[89] Seine Datensammlung hatte das Unternehmen mutmaßlich aus Online-Quellen wie Sozialen Medien oder Nachrichten zusammengestellt. Da es sich bei Clearview AI um eine Software handelt, die auch von Strafverfolgungsbehörden (in den USA) eingesetzt wird, können die Folgen betroffenen Personen insbesondere in Fällen von Fehlzuordnungen, über die in den Medien bereits berichtet wurde,[90] nachhaltig schaden.

87 Internet: https://www.golem.de/news/vice-john-mcafee-mit-iphone-geolocation-geortet-1212-96131.html.

88 Internet: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

89 Internet: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

90 Internet: https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html.

Social Media Plattformen entfernen Metadaten beim Upload von Fotos nicht immer automatisch von selbst. Dies mag zum einen an einem möglichen Eigeninteresse der Betreiber an diesen Daten liegen. Es können aber auch urheberrechtliche Gründe gegen die Entfernung sprechen.[91]

8.1.3 Zwischenfazit

Zusammenfassend lässt sich festhalten, dass die Fortschritte im Bereich KI die Risiken für die Rechte und Freiheiten von Bürgerinnen und Bürgern zunehmend anwachsen lassen. Die Abhängigkeit der KI-Systeme von großen Datensätzen und das daraus folgende Heranziehen öffentlich zugänglicher Informationen für das KI-Training bringen für die Internetveröffentlichung personenbezogener Daten neue, unter Umständen schwer kalkulierbare Risiken mit sich.

Angesichts der vielfältigen Möglichkeiten der Veröffentlichung personenbezogener Informationen insbesondere über Soziale Medien ist es daher Aufgabe einer und eines jeden Einzelnen, die eigenen Gewohnheiten insofern grundlegend zu überdenken.

8.1.4 Empfehlungen für Bürgerinnen und Bürger

Um persönliche Informationen zu schützen und potenzielle Risiken zu mindern, sollten Bürgerinnen und Bürger folgende Maßnahmen in Betracht ziehen:

Bewusster Verzicht: Überlegen Sie, ob Sie wirklich personenbezogene Daten – insbesondere Fotos oder Kurzvideos – veröffentlichen möchten. Nur weil es einfach und schnell geht, sind „ein paar Likes" schwer kalkulierbare Risiken nicht wert. Verzichten Sie im Zweifel zu Ihrem eigenen Schutz auf eine Veröffentlichung.

Entfernen von Bild-Metadaten: Bevor Sie Bilder online teilen, können Sie Metadaten entfernen (oder modifizieren). Dafür gibt es zahlreiche (auch kostenlose) Tools und Anwendungen, die dabei helfen, Ihre Privatsphäre zu schützen. Auch der Windows Explorer kann nach einem „Rechtsklick" auf ein Bild im „Details"-Reiter unten „Eigenschaften entfernen", die Personenbezüge haben können.

Datenschutzeinstellungen und Bewusstsein: Machen Sie sich mit den Datenschutzeinstellungen der von Ihnen genutzten Sozialen Medien vertraut. Dazu gehört insbesondere die Einstellung, wer welchen Beitrag, welches Foto oder Kurzvideo sehen darf – hier ist insbesondere die Einstellung „öffentlich" problematisch.

Zu dieser „Öffentlichkeit" haben sich nämlich nun möglicherweise KI-Firmen „hinzugesellt", die zum Training ihrer Machine Learning-Modelle diese „frei verfügbaren Daten und Informationen" auch auf Social Media-Plattformen sammeln. Die damit verbundenen Risiken lassen sich aktuell noch nicht absehen. Selbst auferlegte wie auch gesetzliche Regelungen können mit den rasant wachsenden Fähigkeiten von KI nicht immer mithalten.

[91] Dazu näher Oberlandesgericht Köln, Urteil vom 20. Januar 2017, 6 U 105/16, BeckRS 2017, 102365, Rn. 27 und Urteil vom 2. Juni 2023, 6 U 17/23, GRUR-RS 2023, 12243, Rn. 14 ff.

Auf den Medientagen Ende Oktober 2023 in München tauschten sich rund 5.000 Besucher drei Tage lang über die wichtigsten KI-Trends aus und sprachen insbesondere über Chancen und Risiken.[92] Neben bewusster Desinformation und unbewusster Falsch- und Fantasieinformation wurde hier die Sorge geäußert, „dass am Vorabend der Wahl irgendwelche Deepfakes auftauchen". Bei Deepfakes handelt es sich um von KI generierte, täuschend echt aussehende Fotos oder sogar bewegte Videos mit Ton, in denen die betroffene Person Dinge tut oder sagt, die sie so eventuell nie wirklich getan oder gesagt hat. Moderne KI kann schon mit nur wenig Trainingsmaterial solche Deepfakes erstellen – **je mehr Fotos, Videos und Sprachaufnahmen einer Person** öffentlich verfügbar sind, desto authentischer gelingt dies. Bekannt geworden sind etwa täuschend echte „Fotos", die eine Verhaftung von Donald Trump zeigen oder Papst Franziskus im neuen Designer-Daunenmantel,[93] ebenso ein gefaketes Statement des Bundeskanzlers zu einem Parteiverbot.[94]

Passen Sie also die Einstellungen zur Sichtbarkeit Ihrer Daten und Beiträge entsprechend Ihren Präferenzen an. Bleiben Sie wachsam und informiert. Üben Sie auch Selbstkritik: Sie wissen selbst am besten, was Sie schon alles öffentlich gepostet haben. Haben Sie schon einmal eine Veröffentlichung bereut? Gibt es von Ihnen Bilder, die heute nicht mehr zu Ihnen passen? Würden Sie die auf Social Media-Plattformen hochgeladenen Bilder auch mit Ihren aktuellen Kontakten teilen wollen? Was sagt die in Ihrem digitalen Leben bisher entstandene Sammlung von Texten, Bildern und Videoclips über Sie aus? Vermittelt sie das Bild, das andere von Ihnen haben sollen? Wenn Fragen dieser Art Ihnen ein „ungutes" Gefühl bereiten: Werden Sie aktiv!

Überprüfen und Löschen: Überprüfen Sie am besten regelmäßig persönliche Informationen, die Sie eventuell auch schon vor längerer Zeit geteilt haben, auf ihre „Sichtbarkeit", indem Sie die Beiträge betrachten, nachdem Sie sich aus dem jeweiligen Dienst abgemeldet haben. Löschen Sie sie im Bedarfsfall. Beachten Sie zudem, dass Sie auch auf Fotos erkennbar sein könnten, die andere gemacht oder hochgeladen haben. Bitten Sie hier um Löschung; Sie haben grundsätzlich ein Recht darauf (Art. 17 DSGVO).

Um etwa bestimmte Informationen bei Facebook zu löschen, können Sie nach der Anmeldung zu den entsprechenden Abschnitten in den Einstellungen gehen. Beispielsweise können Sie unter „Profil und Tagging" Ihre einzelnen Beiträge prüfen und löschen. Es ist jedoch wichtig zu beachten, dass selbst in diesem Fall möglicherweise Kopien der Daten auf den Servern von Facebook oder in den Konten anderer Personen vorhanden sind, wenn Sie Inhalte geteilt haben.

Ungenutzte Accounts löschen: Sie nutzen bestimmte Soziale Medien tatsächlich nicht mehr und konnten sich bisher nur nicht durchringen, Ihren Account zu löschen? Dann nehmen Sie die aktuellen Entwicklungen im Bereich von KI zum Anlass, vielleicht doch den einen oder anderen Zugang aufzulösen oder zumindest

92 Der Bayerische Rundfunk (BR) berichtete: https://www.br.de/nachrichten/deutschland-welt/medientage-wo-die-chancen-von-ki-liegen-und-wo-die-risiken,TttxJQe.

93 Internet: https://www.heise.de/hintergrund/Der-KI-Papst-in-Daunenmantel-sollte-eine-Warnung-sein-8146920.html.

94 BR-Bericht: https://www.br.de/nachrichten/netzwelt/scholz-deepfake-sind-ki-faelschungen-verboten,TwzZ6nE.

zu sperren, sodass die darin gespeicherten Informationen nicht mehr öffentlich zugänglich sind.

Wenn Sie etwa Ihr Facebook-Konto deaktivieren möchten, können Sie dies unter „Deaktivierung und Löschung“ in den Kontoeinstellungen tun. Beachten Sie, dass dies Ihr Konto nur vorübergehend deaktiviert und Sie es später reaktivieren können, wenn Sie sich erneut anmelden. Möchten Sie Ihr Konto dauerhaft löschen, wählen Sie die Option „Dein Konto und deine Informationen löschen“. Befolgen Sie die Anweisungen, um den Löschvorgang abzuschließen. Bedenken Sie, dass dies irreversibel ist und alle Ihre Daten dauerhaft entfernt werden.

8.1.5 Hinweise für bayerische öffentliche Stellen

Auch bayerische öffentliche Stellen posten mitunter Fotos oder Videoclips, auf denen Personen zu erkennen sind, oder stellen Beiträge mit anderen personenbezogenen Daten ein. Einige Beispiele:

- Eine Gemeinde veröffentlicht auf einer Webseite Momente aus öffentlichen Veranstaltungen mit darauf erkennbaren Bürgerinnen und Bürgern.
- Ein Landratsamt teilt eine Liste von Bürgerinnen und Bürgern, die in bestimmten Programmen oder Projekten engagiert sind.
- Ein kommunales Kulturzentrum veröffentlicht Fotos von Veranstaltungen oder Konzerten, auf denen Einzelpersonen erkennbar sind.
- Eine Feuerwehr stellt eine Liste von Bürgerinnen und Bürgern online, die an Erste-Hilfe-Kursen teilgenommen haben.
- Eine öffentliche Schule teilt auf ihrer Website Bilder von Schulveranstaltungen, auf denen Schülerinnen und Schüler erkennbar sind.

Ungeachtet der Frage, ob die jeweilige Veröffentlichung in dieser Form überhaupt für bayerische öffentliche Stellen zulässig war, verweisen alle diese Beispiele auf mangelnde „KI-Disziplin“: Machine Learning-Modellen Trainingsmaterial bereitzustellen ist nicht Aufgabe bayerischer öffentlicher Stellen. (Noch) mehr als bisher sollte bei der öffentlichen Bereitstellung insbesondere von Foto- und Videodateien Zurückhaltung geübt werden, wenn Personen erkennbar sind. Dies gilt gerade dann, wenn diese in begleitenden Texten auch noch namhaft gemacht werden.

Bayerische öffentliche Stellen sind grundsätzlich gut beraten, eine datensparsame Öffentlichkeitsarbeit zu betreiben. Auch wenn eine Rechtsgrundlage für eine Offenlegung personenbezogener Daten zur Verfügung stehen sollte: Nicht immer „braucht“ die „Message“ ein Gesicht – eine Gemeindehomepage darf ihre Stärke in guter Information haben. Das hilft den Bürgerinnen und Bürgern mehr als bunte Fotos von Beschäftigten.

Sollen dennoch Bilder mit Personen veröffentlicht werden, sollte eine „Verpixelung“ geprüft werden; dies gilt insbesondere für Personen „im Hintergrund“. Metadaten braucht es in den seltensten Fällen – also: weg damit! Apps bieten hier eine Vielzahl an Funktionen und Filtern, mit denen es etwa möglich ist, zu zeigen,

dass eine Veranstaltung gut besucht war, ohne dass dabei einzelne Besucherinnen und Besucher identifizierbar sind. Zurückhaltung ist auch bei Bildbeschreibungen angebracht – nicht jede oder jeder muss namhaft gemacht werden.

Ein weiterer Aspekt ist die Zugänglichmachung: Werden die Daten und Medien öffentlich gemacht oder kann der Personenkreis sinnvoll eingeschränkt werden – etwa auf einen „internen" zugangsgeschützten Bereich? Neben diesem „harten" Zugangsschutz, gibt es die „noindex"-Funktion, mit der Suchmaschinen und Indizierungstools angewiesen werden, die so markierten Inhalte oder Unterseiten nicht zu indexieren oder zu berücksichtigen.[95]

8.1.6 Fazit

Es passiert schnell, dass man mehr personenbezogene Daten und Informationen veröffentlicht, als man möchte. Das gilt für Einzelne ebenso wie für bayerische öffentliche Stellen. Insbesondere die erst einmal nicht sichtbaren (weil von den gängigen Foto-Apps normalerweise nicht angezeigten) Exif-Daten sind in diesem Zusammenhang relevant. Neben diesem eher auf Fotos beschränkten Problem ist ganz allgemein vor Risiken zu warnen, die mit der Veröffentlichung personenbezogener Daten einhergehen. Diese zum Teil bereits seit längerem – etwa im Zusammenhang mit Suchmaschinen – bestehenden Risiken haben sich im Zuge des jüngsten Verbreitungsschubs von KI und insbesondere des „unkontrollierten" Crawlings öffentlich zugänglicher Informationen zur Gewinnung von Trainingsdaten noch einmal verschärft. Insofern ist zu empfehlen, das „Ob" neuer und bestehender Veröffentlichungen kritisch zu prüfen. Außer an Verzicht und Löschung sollte auch an eine Entfernung oder Minimierung von Personenbezügen gedacht werden.

8.2 Fehlversand von Schreiben, insbesondere durch Finanzämter

Der Fehlversand von Schreiben war bereits häufiger Gegenstand meiner Tätigkeitsberichte (siehe den 27. Tätigkeitsbericht 2016 unter Nr. 5.5.3, den 28. Tätigkeitsbericht 2018 unter Nr. 3.1.6, den 29. Tätigkeitsbericht 2019 unter Nr. 12.8.1 und den 32. Tätigkeitsbericht 2022 unter Nr. 7.6). Dennoch häuften sich zuletzt bei Finanzämtern Meldungen von Verletzungen des Schutzes personenbezogener Daten wegen des unsachgemäßen Versands von Unterlagen an unberechtigte Empfänger. Häufige Fehlerquellen waren hier die unkorrekte Adressierung, Verwechslungen aufgrund von Namensgleichheit, eine fehlerhafte Zusammenstellung oder eine falsche Kuvertierung von Unterlagen.

8.2.1 Maßnahmen des Verantwortlichen zur Verhinderung des Fehlversands

Nach Art. 24 Abs. 1 DSGVO setzt der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen

[95] Siehe etwa für OpenAI die Dokumentation zu ChatGPT: https://platform.openai.com/docs/gptbot.

zu können, dass die Verarbeitung der Datenschutz-Grundverordnung gemäß erfolgt.

In Konkretisierung des Grundsatzes der Integrität und Vertraulichkeit (Art. 5 Abs. 1 Buchst. f DSGVO) verlangt Art. 32 Abs. 1 DSGVO von dem Verantwortlichen also, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen sind in erforderlichem Umfang zu überprüfen und zu aktualisieren (vgl. Art. 24 Abs. 1 Satz 2 DSGVO).

Versehentliche Fehlversendungen lassen sich zwar auch mit ausgefeilten technisch-organisatorischen Maßnahmen nicht vollständig verhindern. Vorausgesetzt ist dabei aber, dass die nötigen technisch-organisatorischen Maßnahmen überhaupt ergriffen, regelmäßig überprüft und gegebenenfalls aktualisiert werden. Insbesondere eine Namensgleichheit dürfte bei der mitunter hohen Anzahl beispielsweise der von Finanzämtern verarbeiteten personenbezogenen Daten keine Seltenheit sein, so dass diesbezüglich möglichst zuverlässige Maßnahmen getroffen werden müssen, um Fehladressierungen zu vermeiden. Prozessabläufe sind so zu gestalten, dass Fehlversendungen verhindert werden.

8.2.2 Ausnahme von der Meldepflicht

Die Meldepflicht für Verletzungen des Schutzes personenbezogener Daten nach Art. 33 Abs. 1 DSGVO besteht ausnahmsweise nicht, wenn voraussichtlich kein (relevantes) Risiko für die Rechte und Freiheiten natürlicher Personen zu erwarten ist.

In einer Meldung über den Fehlversand eines Bescheides an einen anderen Empfänger als den Bescheidadressaten erhielt ich die Risikoeinschätzung „daher besteht ein hohes Risiko, dass die Daten einem Fremden offenbart wurden". Das trifft zwar zu, allerdings muss die Risikoeinschätzung des Verantwortlichen darauf zielen, mögliche Nachteile für die betroffene Person zu identifizieren und die Eintrittswahrscheinlichkeit einzuschätzen. Zu denken ist etwa an folgende Nachteile (vgl. Erwägungsgrund 75 und 85 DSGVO):

- Verlust der Kontrolle über die personenbezogenen Daten;
- Einschränkung der Rechte der betroffenen Person;
- Diskriminierung;
- Identitätsdiebstahl oder -betrug;
- finanzielle Verluste;
- unbefugte Aufhebung der Pseudonymisierung;
- Rufschädigung;
- Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder
- andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile.

Zur Meldepflicht und Risikoabschätzung habe ich eine Orientierungshilfe „Meldepflicht und Benachrichtigungspflicht des Verantwortlichen“ bereitgestellt,[96] die auch zur Risikobewertung anleitet.

Bei einem versehentlichen und zufälligen Fehlversand, etwa eines Zurechnungsfortschreibungsbescheids, hat der Verantwortliche zu prüfen, ob ein relevantes Risiko für die Rechte und Freiheiten natürlicher Personen besteht, was wohl regelmäßig zu verneinen ist, wenn beispielsweise der unberechtigt empfangene Brief ungeöffnet sofort wieder zurücksendet wurde.

Insbesondere angesichts des häufig möglichen finanziellen Aspekts bei Schreiben von Finanzämtern können auch hier durch unbefugte Empfänger Risiken dadurch entstehen, dass zwischen diesen und den betroffenen Personen eine Bekanntheit oder ein Verwandtschaftsverhältnis besteht und der Bruch der Vertraulichkeit beispielsweise bestehende Erbstreitigkeiten zusätzlich belasten könnte.

8.2.3 Ausführlichkeit der Meldung

Ich stellte fest, dass eingehende Meldungen insbesondere von Fehlversendungen mitunter mangelhaft abgegeben wurden und nur einen spärlichen Informationsgehalt aufwiesen, was mir deren Beurteilung erschwert oder sogar unmöglich gemacht hat.

Aus diesem Grund möchte ich darauf hinweisen, dass alle eingehende Meldungen von mir insbesondere auf folgende Kriterien geprüft werden:

— Ist die inhaltliche Darstellung ausreichend?
— Ist die Risikobewertung nachvollziehbar?
— Sind die bereits ergriffenen Maßnahmen ausreichend?
— Ist eine Informierung der betroffenen Personen nötig oder bereits erfolgt?
— Wurde die Meldefrist eingehalten?

Um Rückfragen zu vermeiden, bitte ich alle Meldenden diesbezüglich auch eine eigene Prüfung durchzuführen und die Meldungen gegebenenfalls entsprechend zu ergänzen.

8.2.4 Zuständigkeit für Finanzämter

Insbesondere von Finanzämtern erreichen mich häufig Meldungen in Bezug auf Fehlversendungen, für die ich nicht zuständig bin: Bayerische Finanzämter unterliegen zwar als bayerische öffentliche Stellen grundsätzlich meiner Datenschutzaufsicht. Hinsichtlich der Verarbeitung personenbezogener Daten im Anwendungsbereich der Abgabenordnung (AO) begründet jedoch § 32h Abs. 1 Satz 1 AO eine Ausnahme; insofern ist die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständige Datenschutz-Aufsichtsbehörde. Das gilt, soweit die Finanzämter Steuern verwalten, die durch Bundesrecht oder das Recht der Europäischen Union geregelt sind (vgl. § 1 Abs. 1 Satz 1 AO). Für die Verwaltung der landesrechtlich geregelten Grundsteuer hat der Landesgesetzgeber

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

zwar auf die Regelungen der Abgabenordnung zurückgegriffen, die Datenschutzaufsicht aber bei mir belassen (Art. 10 Abs. 2 Satz 2 Bayerisches Grundsteuergesetz). Davon abgesehen bin ich für die staatlichen Finanzbehörden außerhalb ihrer steuerverwaltenden Tätigkeit uneingeschränkt zuständig, etwa im Bereich des Personaldatenschutzes (vgl. näher meinen 28. Tätigkeitsbericht 2018 unter Nr. 10.1 sowie meinen 32. Tätigkeitsbericht 2022 unter Nr. 8.1).

Im Falle einer fälschlich an mich gerichteten Meldung werde ich diese zwar regelmäßig an die Bundesbeauftragte abgeben. Dennoch bitte ich zur Vermeidung von Verzögerungen und Verwaltungsaufwand insbesondere die Finanzämter, bei Meldungen vorab selbst zu prüfen, an welche Aufsichtsbehörde diese zu richten sind, und dann auch direkt an diese zu melden.

8.3 Geleakte BayernCloud Schule-Zugangsdaten

In den 1960er Jahren wurden erstmals Passwörter als Schutzmaßnahme für den Zugriff auf Rechner genutzt. Was sich seitdem nicht geändert hat: Passwörter verlieren ihre Schutzwirkung, sobald sie Unbefugten bekannt werden. Kommt es zur Offenlegung von Benutzerkennungen und Passwörtern in großem Umfang, spricht man von einem sogenannten „Password-Leak". Hauptursachen für Passwort-Leaks sind insbesondere Hackerangriffe, Schadsoftware, ungesicherte Zugriffsmöglichkeiten auf Datenbanken und Phishing-Attacken.

Bei großen Leaks können Millionen oder sogar Milliarden von Datensätzen betroffen sein, wie beispielsweise bei dem „RockYou2024"-Leak mit angeblich fast 10 Milliarden Passwörtern im Juli 2024.[97]

Das Landesamt für Sicherheit in der Informationstechnik prüft einschlägige Webseiten, ob Zugangsdaten von Stellen in seinem Zuständigkeitsbereich betroffen sind. Dabei werden auch immer wieder Zugangsdaten von Schülerinnen und Schülern sowie Lehrkräften für die BayernCloud Schule (ByCS) gefunden. Im Jahr 2024 erreichten mich daher wiederholt Meldungen von Schulen nach Art. 33 DSGVO über geleakte Zugangsdaten von ByCS-Accounts.

8.3.1 Starke und individuelle Passwörter

Nutzerinnen und Nutzer können selbst mit zwei Maßnahmen ihren eigenen Schutz gegen Passwort-Leaks signifikant erhöhen. Komplexe Passwörter mit Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen sind schwieriger zu „knacken". Selbst wenn starke Passwörter in einem Leak verschlüsselt auftauchen – Angreifer benötigen dann zumindest mehr Zeit und Ressourcen, um sie zu entschlüsseln, was wiederum den Betroffenen mehr Zeit gibt, ihre Passwörter zu ändern. Komplexe Passwörter schützen zudem besser vor sogenannten Brute-Force- oder Wörterbuch-Angriffen, da Länge und Komplexität automatisierte Angriffe erschweren, bei denen systematisch alle möglichen Kombinationen durchprobiert werden. Trotz dieses Vorteils sollten bei einem Passwort-Leak alle betroffenen Passwörter unabhängig von ihrer Stärke umgehend geändert werden.

[97] Nähere Ausführungen dazu etwa bei Schurter, Aufregung um „grössten Passwort-Leak aller Zeiten", Internet: https://www.swisscybersecurity.net/news/2024-07-10/aufregung-um-groessten-passwort-leak-aller-zeiten.

Passwörter sollten zudem nur einmal, also für jeweils einen einzigen Dienst beziehungsweise nur für ein Benutzerkonto verwendet werden. Dies bietet Schutz vor sogenannten Credential-Stuffing-Angriffen. Dabei werden gestohlene Zugangsdaten automatisiert auf verschiedenen Websites ausprobiert. Einzigartige Passwörter reduzieren so das Risiko, dass Angreifer mit denselben Zugangsdaten auch andere Dienste angreifen und dort weiteren Schaden anrichten können. Hilfsmittel wie Passwort-Manager können die individuelle Nutzung und Generierung von sicheren Passwörtern vereinfachen. Wobei auch hier durch sorgfältige Auswahl und sicheren Betrieb des Passwort-Managers darauf geachtet werden muss, dass nicht ein erfolgreicher Angriff auf den Passwort-Manager zu einem erneuten Passwort-Leak führt.

8.3.2 Phishing

Phishing ist eine weit verbreitete Form des Cyberangriffs, bei der Betrüger versuchen, durch gefälschte Nachrichten, insbesondere E-Mails, aber auch Messenger-Nachrichten an sensible Informationen wie Passwörter (oder etwa Kreditkartendaten) zu gelangen. Ziel ist es dabei, den Empfänger zu einer Handlung zu verleiten, wie etwa das Preisgeben von Login-Daten oder finanziellen Informationen. Es wird meist versucht, mittels möglichst echt und dringlich wirkenden Nachrichten Personen dazu zu bewegen, eine bestimmte URL aufzurufen. Die URL ist dann entweder bereits direkt mit Schadcode versehen, der über Browserlücken versucht, den Rechner des Opfers zu infizieren, oder es wird Nutzenden eine zum Teil täuschend echt aussehende Website angezeigt, auf der sie ihre Zugangsdaten eingeben sollen. Diese Daten landen dann in den Händen der Angreifer.

Um sich vor Phishing zu schützen, können folgende Maßnahmen hilfreich sein:

- Entwickeln Sie ein gesundes Misstrauen gegenüber unerwarteten E-Mails, besonders solchen mit dringenden Aufforderungen oder auch Drohungen.

- Überprüfen Sie immer die Absenderadresse und insbesondere Links in E-Mails, bevor Sie irgendwo draufklicken: Viele E-Mail-Programme zeigen die URL eines Links bereits an, wenn man mit dem Mauszeiger darüberfährt, **ohne jedoch darauf zu klicken** (das ist tunlichst zu vermeiden). Meist lässt sich an der URL erkennen, dass es sich um keinen vertrauenswürdigen Link handelt – etwa, wenn diese anders lautet, als der in der E-Mail angezeigte Link. Oft sind Links als Knöpfe getarnt, die zu einer Aktion aufrufen (sogenannte Call-to-Action-Buttons), etwa „Jetzt Gewinn abholen“ oder „Hier Passwort ändern“.

- Denken Sie lieber kurz nach, bevor Sie eine E-Mail von einem unbekannten Empfänger öffnen.

- Wenn Sie die Wahl haben: Blockieren sie jedenfalls bei E-Mails von externen Absendern die HTML-Ansicht.

- Geben Sie niemals vertrauliche Informationen per E-Mail preis.

- Öffnen Sie keine Anhänge oder Links in verdächtigen E-Mails.

- Loggen Sie sich von Diensten aus, die Sie gerade nicht nutzen.

- Nutzen Sie bewusst verschlüsselte Verbindungen („https://“) für sensible Transaktionen.

- Wenn Sie behördlicher Datenschutzbeauftragter sind: Klären Sie Ihre Kolleginnen und Kollegen im Rahmen Ihrer Updates zu datenschutzrelevanten Fragen der IT-Sicherheit regelmäßig auch über aktuelle Phishing-Taktiken auf. Gestalten Sie die Unterweisung möglichst realitätsnah.

Allgemein lässt sich feststellen, dass durch generative KI die Qualität der Phishing-Angriffe zugenommen hat (und auch wohl noch zunehmen wird); falsche und bösartige E-Mails sind von harmlosen immer schwieriger zu unterscheiden. Dennoch lässt sich durch Wachsamkeit und ein gewisses Grundmisstrauen das Risiko, Opfer eines Phishing-Angriffs zu werden, weiterhin erheblich reduzieren.

Aufgrund der hohen Anzahl von Meldungen von geleakten Zugangsdaten zu ByCS-Accounts im Jahr 2024 bitte ich vor allem **Lehrkräfte** als direkte Kommunikationspartner der Schülerinnen und Schülern, diese auf die Risiken von Passwortangriffen hinzuweisen und zum sorgfältigen Umgang damit anzuleiten. Mich erreichte allerdings auch eine Meldung, bei dem ein begründeter Verdacht entstand, dass ein Schüler Lehrerzugangsdaten zur schulinternen Lernplattform mebis erlangen und damit weitreichende Zugriffsrechte bekommen konnte. Lehrkräfte seien deshalb auch auf die Notwendigkeit zum sorgfältigen Umgang mit ihren eigenen Zugangsdaten hingewiesen.

Die Gefahren, die dadurch entstehen, dass Angreifer Kenntnis von einem Passwort erlangen, lassen sich zuverlässig nur durch eine **Zwei-Faktor-Authentifizierung** minimieren. Ein Angreifer kann dann alleine durch Kenntnis des Passworts noch nicht auf den Dienst zugreifen, er benötigt immer noch den zweiten Faktor, also beispielsweise eine Chip-Karte oder ein Gerät, auf das nur der berechtigte Nutzer Zugriff hat. Für jedes Verfahren sollten Verantwortliche daher prüfen, ob nicht auf eine Zwei-Faktor-Authentifizierung umgestellt werden kann oder gar umzustellen ist.

8.4 Vertraulichkeit im Homeoffice von Justizvollzugsbediensteten

Fragen des technisch-organisatorischen Datenschutzes bei der Arbeit im Homeoffice, auch in Form von Telearbeit, hatten während der COVID-19-Pandemie Konjunktur (siehe mein 30. Tätigkeitsbericht 2020 unter Nr. 3.6). Die Möglichkeit, im Homeoffice zu arbeiten, gehört bei vielen bayerischen öffentlichen Stellen weiterhin zum Alltag. In diesem Rahmen haben Kommunikations- und Kollaborationssysteme aber auch die eAkte Bayern einen Verbreitungsschub erfahren.

Aktuell hatte ich mich mit der Vertraulichkeit bei der Arbeit im Homeoffice von Justizvollzugsbediensteten befasst. Anlass dazu gab die Prüfanregung eines Gefangenen aus einer bayerischen Justizvollzugsanstalt, der um den Schutz der personenbezogenen Daten besorgt war. Insbesondere während der COVID-19-Pandemie seien seiner Schilderung zufolge Gespräche von Gefangenen mit dem medizinischen Dienst der Justizvollzugsanstalt per Videokonferenz geführt worden. Dabei habe sich das medizinische Personal zum Teil im Homeoffice befunden. Der Gefangene befürchtete, dass die Vertraulichkeit der Gespräche durch Kenntnisnahmemöglichkeiten von Haushaltsangehörigen oder Mitbewohnern gefährdet sein könnte.

Dies habe ich zum Anlass genommen, mich bei der Justizvollzugsanstalt zu diesem Thema näher zu informieren. Ich gelangte zu den folgenden Erkenntnissen:

8.4.1 Dienstvereinbarung des Bayerischen Staatsministeriums der Justiz

Mit Bekanntmachung des Bayerischen Staatsministeriums der Justiz über die Dienstvereinbarung über Telearbeit und Mobile Arbeit im Geschäftsbereich des bayerischen Justizvollzugs[98] (im Folgenden: Dienstvereinbarung) hat das Justizministerium für alle Einrichtungen im bayerischen Justizvollzug unter anderem festgelegt, dass die

„Sicherheit und Ordnung in den Justizvollzugseinrichtungen, die Effektivität der Organisationseinheiten und der ordentliche Dienstbetrieb […] durch die Einrichtung von Telearbeit oder Mobilen Arbeitens nicht beeinträchtigt werden [dürfen].“

Um sicherzustellen, dass alle im Homeoffice bearbeiteten Vorgänge der Einsichtnahme durch Familienangehörige und Dritte entzogen und die datenschutzrechtlichen Bestimmungen eingehalten werden, umfasst die Dienstvereinbarung insbesondere Regelungen zum Transport von Akten, zur Aufbewahrung von Unterlagen und Geräten, zu Einschränkungen für die Mitnahme von Akten und zur Vernichtung von außerhalb der Dienststelle erstellten Unterlagen.

Ergänzend zur Aufbewahrung der Geräte stellt die Dienstvereinbarung fest, dass die von der Dienststelle zur Verfügung gestellten Rechner und Datenträger ganz allgemein gegen den Zugriff Unberechtigter zu schützen sind. Rechner sind insofern nicht nur mit einer Sicherheitskomponente gegen die Inbetriebnahme durch Unbefugte abzusichern, sondern auch im laufenden Betrieb bei kurzfristigem Verlassen des Arbeitsplatzes (ohne Herunterfahren) zu sperren.

Für eine Tätigkeit im medizinischen Dienst (oder vergleichbar sensiblen Dienstbereichen, etwa dem psychologischen oder seelsorgerischen Dienst) kann Mobile Arbeit oder Telearbeit außerdem nur in besonderen und begründeten Einzelfällen genehmigt werden.

Die betroffene Justizvollzugsanstalt gab mir gegenüber an, dass Bedienstete des medizinischen Dienstes derzeit nicht die Möglichkeit zum Homeoffice nutzen würden und lediglich in der Zeit der COVID-19-Pandemie eine Nutzung notwendig gewesen sei. Ansonsten werde in Übereinstimmung mit dem ärztlichen und krankenpflegerischen Dienst der Grundsatz vertreten, dass medizinische und ärztliche Leistungen und Arbeiten nur vor Ort erledigt werden können.

Ein konkreter Sachverhalt, bei dem es im Rahmen der ausnahmsweisen Nutzung von Homeoffice im medizinischen Dienst während der COVID-19-Pandemie zu unberechtigter Kenntnisnahme von personenbezogenen Daten gekommen wäre, wurde mir nicht bekannt.

Ich stellte fest, dass die Vertraulichkeit der Verarbeitung von personenbezogenen Daten in den jetzt bestehenden Regelungen eine zentrale Beachtung findet. Mögliche Gefährdungen, wie etwa durch Familienangehörige und andere im Haushalt

[98] Vom 19. Februar 2024 (BayMBl. Nr. 196).

lebende Personen, wurden ausreichend erkannt und durch technische und organisatorische Maßnahmen adressiert.

8.4.2 Empfehlungen

Nach Art. 32 Abs. 1 DSGVO müssen Verantwortliche geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Das müssen sie im Rahmen von Art. 5 Abs. 2 DSGVO auch nachweisen können. Regelungen für die häusliche Arbeitssituation in Bezug auf die Durchführung von Telefongesprächen oder Videokonferenzen sollten so gestaltet werden, dass sie in Umsetzung und Dokumentation alltagstauglich sind.

Den Beschäftigten muss deutlich werden, dass insbesondere Gesprächsinhalte schützenswert sind und dass deshalb keine unbefugten Dritten mithören oder zuschauen dürfen. Türen und Fenster sollten gegebenenfalls geschlossen werden, um ungewollte Zuhörer auszuschließen. Neugierige Blicke – etwa durchs Fenster auf den Monitor – sollten soweit nötig mittels Vorhänge oder Displayfolien unterbunden werden. Die Nutzung von Headsets ist empfehlenswert, um zu verhindern, dass die eingehenden Gesprächsinhalte von Dritten im Raum mitgehört werden.

Außerdem sollten Beschäftigte zum Zweck des Selbstschutzes darauf achten, dass während Videokonferenzen keine sensiblen Informationen (über sich oder auch Familienangehörige oder Dritte) im Hintergrund erkennbar werden, die Rückschlüsse auf das Privatleben, gegebenenfalls auch den Wohnort erlauben. Geräte mit Sprachassistenten (etwa Microsoft Cortana, Google Assistant, Apple Siri, Amazon Alexa usw.), insbesondere also private Smartphones aber auch Echo Dots und andere Smart Home-Geräte dürfen sensible Dienstgespräche nicht mitanhören und müssen gegebenenfalls deaktiviert werden.

Zusammenfassend lässt sich sagen, dass die Wahrung der Vertraulichkeit dienstlicher Informationen im Homeoffice durch eine Vielzahl von Maßnahmen verbessert werden kann. Sowohl technische als auch organisatorische Aspekte müssen berücksichtigt werden, um die Einhaltung datenschutzrechtlicher Regelungen zu gewährleisten. Nur im Verbund von Sensibilisierung der Beschäftigten, Einsatz sicherer Technologien und klaren Regelungen für die häusliche Arbeitssituation kann die Vertraulichkeit von Informationen ausreichend geschützt werden.

8.5 Postversand von elektronischen Medien

Die Bearbeitung einer Beschwerde hat die Frage aufgeworfen, was im Hinblick auf den technisch-organisatorischen Schutz beim postalischen Versand von elektronischen Medien, das heißt beim Versand von Speichermedien (zum Beispiel USB-Sticks oder Speicherkarten) und beim Versand von Geräten, in denen solche Speichermedien eingebaut sind (zum Beispiel Smartphones), zu beachten ist.

Insbesondere zu dem Teilaspekt, ob elektronische Medien beim Postversand zu verschlüsseln sind, lassen sich derzeit unterschiedliche datenschutzrechtliche Ausführungen – teilweise bezogen auf bestimmte Einzelfälle – finden. Die folgende Konkretisierung der relevanten Anforderungen zeigt, dass auf den ersten Blick widersprüchliche Standpunkte für bestimmte Einzelfälle durch eine detailliertere datenschutzrechtliche Betrachtung nicht selten auf eine gemeinsame Prüflogik zurückgeführt werden können.

Vor dem Postversand von elektronischen Medien, auf denen personenbezogene Daten gespeichert sind, hat eine bayerische öffentliche Stelle datenschutzrechtlich folgende Prüfschritte zu beachten:

Der Postversand ist eine gängige Form für die Übermittlung personenbezogener Daten. Daneben können situativ und in bestimmten Einzelfällen auch alternative Formen möglich sein, bei denen die Übermittlung datenschutzfreundlicher gestaltet werden kann (zum Beispiel eine persönliche Übergabe oder die Nutzung eines geeigneten digitalen Kommunikationsportals).

Aufgrund des bestehenden Postgeheimnisses (§ 64 Postgesetz) sowie der Strafbewehrung in § 202 Strafgesetzbuch (StGB) ist grundsätzlich anzunehmen, dass unbefugte Dritte auf dem Postweg keinen Zugriff auf die in einer Postsendung befindlichen elektronischen Medien erhalten und damit die Vertraulichkeit sowie Datenintegrität der personenbezogenen Daten gewahrt ist. Verantwortliche, die sich auf diesen Grundsatz berufen möchten, müssen zuvor allerdings folgende Fragen stellen – und sachgerechte Antworten auf sie finden:

— **Entspricht die Umverpackung den Anforderungen des Postdienstleisters?**

  Die Möglichkeit, dass eine Postsendung nicht beim angegebenen Empfänger ankommt, ist den Postdienstleistern bekannt. Eine Ursache dafür kann sein, dass nicht geeignet verpackte Postsendungen mit sperrigem Inhalt durch eine automatische Sortiermaschine oder bei einer anderen maschinellen Bearbeitung in den Brief- oder Paketzentren beschädigt werden und Teile ihres Inhalts dabei verlieren. Daher gibt beispielsweise die Deutsche Post AG gesonderte Hinweise an Absender, wie bestimmte elektronische Speichermedien vor ihren Versand zu verpacken sind.[99] Eine Verpackung nach der einschlägigen Empfehlung des beauftragten Postdienstleisters ist eine technische und organisatorische Maßnahme, die einen wichtigen Aspekt des Verlustrisikos geeignet reduziert und die durch eine gleichwertige alternative Schutzmaßnahme in der Regel nicht ersetzt werden kann.

— **Sind die Versandoptionen richtig ausgewählt?**

  Die Versandoptionen, die vom Postdienstleister angeboten werden und eine höhere Sicherheit der Sendung vermitteln, können von der versendenden Stelle als geeignete Schutzmaßnahmen gewählt und aktiviert werden (zum Beispiel eine allgemeine Sendungsverfolgung oder eine besondere Sendungsverfolgung im Rahmen eines Einschreibens, wodurch insbesondere eine höhere Ermittlungsquote bei nicht termingerecht zugestellten Postsendungen erzielt werden kann).

— **Müssen kontextspezifische Vorgaben beachtet werden?**

  Sind weitere Schutzmaßnahmen durch spezifische normative Vorgaben oder durch eine Selbstverpflichtung der Stelle für den postalischen Versand von elektronischen Medien vorgesehen, so sind diese Maßnahmen von der Stelle umzusetzen. Beispielsweise kann mit Sicherheitsverschlüssen und mit Sicherheitsaufklebern der Postversand zusätzlich abgesichert werden.

[99] Internet: https://www.deutschepost.de/de/c/clever-briefe-versenden.html.

— **Sind weitere Maßnahmen erforderlich?**

Nach der Datenschutz-Grundverordnung ist jede verantwortliche Stelle verpflichtet, mittels der wirksamen Umsetzung von technischen und organisatorischen Maßnahmen 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 werden.[100] Denn die Datenschutz-Grundverordnung schreibt insbesondere in Art. 32 DSGVO nicht die Umsetzung bestimmter technischer und organisatorischer Maßnahmen fest vor, sondern verpflichtet die verantwortliche Stelle zu einer Abwägung zwischen den Risiken der Verarbeitung und den Implementierungskosten sowie der Art, dem Umfang, der Umstände und dem Zweck der Verarbeitung. Die verantwortliche Stelle hat somit zu prüfen, welche Risiken sich aus dem Postversand von elektronischen Medien im Einzelfall ergeben können und welche Maßnahmen geboten sind, um das Risiko angemessen zu vermindern

Anders als Papierunterlagen können Dateien und elektronische Medien grundsätzlich nach dem Stand der Technik verschlüsselt und vom Empfänger mit dem dazugehörigen Schlüssel, der auf einem geeigneten, separaten Kommunikationsweg zugesendet wird, wieder entschlüsselt werden. Diese technische Schutzmöglichkeit könnte als Argument herangezogen werden, dass nach Art. 32 DSGVO elektronische Medien mit personenbezogenen Daten, die auf dem Postweg versendet werden, stets verschlüsselt werden müssen.

Eine solche pauschale Schlussfolgerung würde jedoch die Risikoreduzierung durch das Postgeheimnis fast vollständig außer Acht lassen. Wäre die datenschutzrechtliche Wirkung des Postgeheimnisses tatsächlich so unbedeutend, wäre dies auch beim Papierversand zu berücksichtigen. Denn beim Vergleich des datenschutzrechtlichen Risikos macht es bei Erfüllung der Anforderungen (1) und (2) grundsätzlich keinen Unterschied, ob vergleichbare personenbezogene Daten in der üblichen Papierform oder elektronisch auf einem unverschlüsselten Speichermedium postalisch versendet werden.

Allerdings können bei der Versendung elektronischer Medien zu den allgemeinen Postversandrisiken spezifische digitale Risikoaspekte hinzutreten (im Folgenden als Digitalrisiken bezeichnet). Insbesondere ist dabei zu beachten, dass marktübliche elektronische Speichermedien eine sehr hohe Speicherkapazität besitzen. Unter der Annahme, dass jedes Gigabyte (GB) einer Datenmenge von 100.000 bedruckten Seiten DIN-A4 Papier entspricht, könnten auf einem USB-Stick mit einer Speicherkapazität von 128 GB über 12 Millionen bedruckte Seiten gespeichert werden. Hinzu kommt auch die Besonderheit, dass digitale Medien die Speicherung von Datenformaten erlauben, zu denen es in der Papierwelt kein Gegenstück gibt (zum Beispiel Videos). Somit können personenbezogene Daten, die auf elektronischen Medien gespeichert sind, in einem Umfang sowie in einer

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

Art und Weise postalisch versendet werden, die sich im datenschutzrechtlichen Risiko deutlich vom Postversand eines Papierkonvoluts unterscheidet.

Vor diesem Hintergrund kann als Ergebnis festgehalten werden:

- Beim postalischen Versand eines elektronischen Mediums ist die sachgerechte Verschlüsselung der Dateien, die auf dem Medium gespeichert sind, oder die Verschlüsselung des Mediums selbst eine Schutzmaßnahme, die das Risiko einer Vertraulichkeits- und Datenintegritätsverletzung auf dem Versandweg deutlich vermindert. Sind insbesondere die Implementierungskosten für eine solche Verschlüsselung – was regelmäßig der Fall sein dürfte – verhältnismäßig, wird eine solche Verschlüsselung empfohlen.

- Eine derartige Verschlüsselung oder eine vergleichbare alternative Schutzmaßnahme kann neben dem bestehenden Schutz des Postgeheimnisses technisch-organisatorisch regelmäßig dann gefordert werden, falls der Postversand des elektronischen Mediums mindestens mit einem spezifischen Digitalrisiko verbunden ist und zudem ein hohes Verarbeitungsrisiko aufweist.

- In Art. 35 Abs. 1 DSGVO ist im Zusammenhang mit der Datenschutz-Folgenabschätzung und im Hinblick auf die Form einer Verarbeitung von einem voraussichtlich hohen Risiko für die Rechte und Freiheiten natürlicher Personen die Rede. Nach der von der Artikel 29-Datenschutzgruppe – dem Vorgängergremium des Europäischen Datenschutzausschusses – veröffentlichten Leitlinien zur Datenschutz-Folgenabschätzung[101] müssen neun Kriterien berücksichtigt werden, um Verarbeitungsvorgänge zu ermitteln, für die aufgrund ihres hohen Risikos eine Datenschutz-Folgenabschätzung (DSFA) erforderlich ist. Diese Bewertungsmethode auf Grundlage der neun DSFA-Kriterien kann entsprechend für die Beurteilung, ob ein bestimmter Postversand von elektronischen Medien ein hohes Verarbeitungsrisiko aufweist, genutzt werden.

8.6 Massive Hackerangriffe auf öffentliche Stellen

8.6.1 Erhöhte Gefahrenlage

Leider musste ich in diesem Berichtszeitraum eine massive Zunahme an erfolgreichen Hackerangriffen auf öffentliche Stellen in Bayern verzeichnen. Erfolgreich meint im Hinblick auf den Datenschutz, dass es den Angreifern gelang, die Sicherheitssysteme der angegriffenen Stellen zu überwinden und Zugriff auf die (virtuellen) Server und die darauf gespeicherten Daten zu erhalten. Dies äußerte sich häufig darin, dass die IT-Systeme der betroffenen Stellen (komplett) verschlüsselt

[101] Artikel 29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 wahrscheinlich ein hohes Risiko mit sich bringt, WP 248 rev.01, Internet: https://www.datenschutz-bayern.de, Rubrik „DSFA“.

wurden und die betroffenen Stellen tage- oder wochenlang lahmgelegt waren. Zudem werden von den Angreifern häufig auch Daten kopiert und im Darknet zum Verkauf angeboten. Das Darknet Monitoring des Bayerischen Landeskriminalamts konnte Daten von bayerischen öffentlichen Stellen auf einschlägigen Angebotsplattformen auffinden.

Derartige Datenabflüsse wiegen besonders schwer, wenn es sich bei den betroffenen Stellen um Kommunen, Schulen, Krankenhäuser oder psychiatrische Kliniken handelt, weil bei diesen Verantwortlichen regelmäßig auch Sozialdaten, Daten von Kindern, besondere Kategorien personenbezogener Daten wie etwa Gesundheitsdaten, sowie Daten betroffen sind, die einer Auskunftssperre unterliegen.

Ursache für derartige Vorfälle sind häufig keine komplizierten Angriffe wie Zero-Day-Exploits, bei denen bisher unbekannte Sicherheitslücken ausgenutzt werden, sondern etwa über ein halbes Jahr nach Erscheinen immer noch nicht eingespielte Patches und Updates oder schlecht gesicherte Benutzerkonten, insbesondere auch auf kritischen Systemen wie Firewalls. Leider musste ich feststellen, dass in vielen Fällen selbst für privilegierte Benutzerkonten keine Zwei-Faktor-Authentifizierung eingerichtet war, die mittlerweile sogar für „Normalbürger" zum Schutz von Bankkonten oder Social Media Accounts als Stand der Technik anzusehen ist.

In den meisten mir nach Art. 33 DSGVO gemeldeten Fällen hatten die Verantwortlichen keine ausreichenden technisch-organisatorischen Maßnahmen nach Art. 32 DSGVO ergriffen; daher habe ich in einigen Fällen Beanstandungen ausgesprochen. Diese Fälle sollen im Folgenden exemplarisch dargestellt werden.

8.6.2 Beanstandungen

8.6.2.1 Beanstandung der unzureichenden technischen Absicherung von IT-Systemen eines Klinikums

Ein bayerisches Klinikum wurde Opfer eines Cyberangriffs, bei dem die IT-Systeme durch Ransomware namens „RA World" verschlüsselt wurden und etwa 3.600 Gigabyte Daten abgeflossen sind. Auf eine damit verbundene Lösegeldforderung ging das Klinikum gemäß dem Rat der Polizei nicht ein.

Der Angriff führte zu erheblichen Störungen im Klinikbetrieb, da die elektronisch gespeicherten Daten nicht mehr zugreifbar waren. Er erforderte eine Abmeldung von der Notfallversorgung. Die Sicherheit und Versorgung der Patienten wurde konnte durch die Aktivierung bestehender Notfallpläne und unter Verwendung von Papierakten gewährleistet werden.

Die forensischen Untersuchungen haben ergeben, dass öffentlich bekannte Sicherheitslücken ausgenutzt wurden. Es standen auch bereits Patches zur Verfügung, die jedoch nicht installiert waren. Zudem wurde keine wirksame Netzwerkssegmentierung umgesetzt, was die Ausweitung des Angriffs im gesamten Netzwerk des Klinikums ermöglichte.

Nach dem Vorfall wurden im Rahmen der Aufarbeitung neben dem unzureichenden Patch-Management noch einige weitere konzeptionelle Sicherheitsmängel

festgestellt. Dementsprechend wurde nach dem Vorfall ein komplettes Neuaufsetzen aller Systeme begonnen, um eine IT-Infrastruktur gemäß dem Stand der Technik zu erreichen.

Den eklatanten Verstoß gegen die Anforderungen von Art. 32 Abs. 1 Buchst. b DSGVO insbesondere hinsichtlich der Vertraulichkeit und der Verfügbarkeit habe ich förmlich beanstandet. Zudem habe ich das Klinikum gebeten, längerfristig eine Darknet-Überwachung hinsichtlich des Verkaufs der abgeflossenen Daten durchzuführen.

8.6.2.2 Beanstandung fehlender IT-Sicherheitsmaßnahmen bei einem kommunalen IT-Dienstleister

Ein kommunaler IT-Dienstleister wurde zum Ziel eines gravierenden Cyberangriffs durch die Ransomware-Gruppe Akira. Dieser Vorfall führte zur Verschlüsselung aller virtuellen Server und sogar zur Löschung wichtiger Backups. Betroffen waren personenbezogene Daten von bis zu 40.500 Bürgern, bei den Kunden des IT-Dienstleisters fielen teilweise zentrale Fachanwendungen aus.

Nach der Entdeckung des Angriffs wurden alle Verbindungen zum Rechenzentrum des IT-Dienstleisters getrennt, um eine Ausbreitung des Schadcodes zu verhindern. Ein nicht verschlüsselter physischer Server ermöglichte die teilweise Wiederherstellung von Daten, während die restlichen fehlenden Daten manuell eingepflegt werden mussten. Vollständige Datenverfügbarkeit wurde erst nach mehreren Wochen wieder erreicht.

Die Ermittlungen ergaben, dass die Angreifer mit den Zugangsdaten eines Mitarbeiters in die IT-Systeme eingedrungen waren. Diese Zugangsdaten waren nicht ausreichend gesichert; sie könnten möglicherweise gestohlen oder gekauft worden sein. Zudem stellte sich heraus, dass die Firewall des IT-Dienstleisters veraltet und nicht ausreichend konfiguriert war. Der IT-Dienstleister räumte ein, dass grundlegende Sicherheitsmaßnahmen nicht ausreichend umgesetzt waren.

Ich habe den Verstoß gegen die Anforderungen von Art. 32 Abs. 1 Buchst. b DSGVO insbesondere hinsichtlich der Vertraulichkeit und der Verfügbarkeit förmlich beanstandet und den IT-Dienstleister aufgefordert, eine vollständige Risikoanalyse sowie Nachweise über die Umsetzung von Sicherheitsanforderungen vorzulegen.

Leider zeigt dieser Vorfall, dass ein Outsourcing für Kommunen nicht immer zu einer Verbesserung des Sicherheitsniveaus führt. Auch ein IT-Dienstleister muss dafür sorgen, dass die Ausstattung mit genügend geeignetem Fachpersonal regelmäßig überprüft, die nötigen technisch-organisatorischen Maßnahmen ergriffen und in ihrer Effektivität nachhaltig überwacht werden.

8.6.2.3 Beanstandung der mangelnden Umsetzung von technischen und organisatorischen Schutzmaßnahmen bei einem Landratsamt

Bei einem Landratsamt wurde eine mögliche Kompromittierung einer VoIP-Telefon-Anlage festgestellt. Wie sich bei den anschließenden Ermittlungen herausstellte, konnten Angreifer eine Sicherheitslücke in einem Router ausnutzen. Um die Auswirkungen zu minimieren, wurde die gesamte IT des Landratsamts vorübergehend vom Netzwerk getrennt, was zu einem vollständigen Ausfall der

Kommunikationsmöglichkeiten für die Bürger führte. Etwa eine Woche waren weder Telefonate, Online-Anträge, E-Mail-Kommunikation noch Kfz-Zulassungen möglich.

In Rahmen der Aufarbeitung des Vorfalls wurde festgestellt, dass die Sicherheitslücke, die zu dem Angriff führte, bereits seit längerem bekannt war und seit Bestehen aktiv ausgenutzt wurde. Dabei handelte es sich um eine Schwachstelle in der Software einer Netzwerkkomponente, wodurch die Verfügbarkeit der Systeme und Dienstleistungen erheblich beeinträchtigt wurde. Auch wenn von den Angreifern wohl keine personenbezogenen Daten abgegriffen wurden, zeigte der Vorfall gravierende Mängel insbesondere in den Prozessen der IT-Sicherheit und des Datenschutzmanagements insbesondere hinsichtlich des Einspielens von Updates und Patches auf.

Ich habe die festgestellten Verstöße gegen Art. 32 Abs. 1 Buchst. b DSGVO förmlich beanstandet und gefordert, zeitnah Nachweise über die Behebung der bestehenden Mängel hinsichtlich der IT-Sicherheit vorzulegen.

Darüber hinaus habe ich dem Landratsamt regelmäßige Überprüfungen und Evaluierungen der IT-Sicherheitsmaßnahmen, die Implementierung eines effektiven Patch-Management-Systems sowie Schulungen für Mitarbeiter zur Sensibilisierung für Datenschutz- und Sicherheitsfragen nahegelegt. Wie diese Beispiele zeigen, könnten mit diesen Basismaßnahmen schon eine Vielzahl von Hackerangriffen abgewehrt werden.

8.6.3 Meldepflicht nach Art. 33 DSGVO

Sollte es zu einem Hackerangriff gekommen sein, weise ich noch einmal auf die Pflicht zur Abgabe einer (Erst-)Meldung einer Datenschutzverletzung nach Art. 33 DSGVO grundsätzlich innerhalb von 72 Stunden hin. Dies kann zu einer besonderen Herausforderung in der allgemeinen Hektik eines Hackerangriffs werden, insbesondere wenn alle IT-Systeme der öffentlichen Stelle abgeschaltet wurden. Es sollte daher im Rahmen der Notfallkonzeption festgelegt werden, über welche Kommunikationswege eine fristgerechte Meldung abgegeben werden soll.

Da in den ersten 72 Stunden nach dem Angriff normalerweise noch nicht alle Informationen zum Vorfall vorliegen und eine längere Aufklärungsphase nach sich zieht, habe ich Empfehlungen näheren Vorgehen in solchen Fällen erarbeitet.[102]

8.7 Datenpannen beim Auftragsverarbeiter – Beispiel Stay Informed

Die Firma Stay Informed bietet eine vielgenutzte App für Kindertageseinrichtungen und Schulen zur Kommunikation zwischen Einrichtung und Eltern. Leider kam es im Berichtszeitraum zu einer größeren Datenpanne. Infolge Fehlkonfiguration eines Webservers beim Anbieter waren personenbezogene Daten von Kindern und Eltern über einen längeren Zeitraum im Internet frei abrufbar. Einer breiteren Öffentlichkeit wurde dies durch die Berichterstattung einer großen deutschen Fachzeitschrift aus dem IT-Bereich bekannt. Das Beispiel zeigt deutlich die

[102] Bayerischer Landesbeauftragter für den Datenschutz, Meldung nach Art. 33 Datenschutz-Grundverordnung bei Hackerangriff, Aktuelle Kurz-Information 58, Stand 1/2025, Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

Schwierigkeiten auf, die bestehen können, wenn es im Rahmen einer Auftragsverarbeitung zu Datenpannen beim Auftragsverarbeiter kommt. Sowohl der Verantwortliche als auch der Auftragsverarbeiter sollten daher entsprechende Vorkehrungen treffen:

— **Klarheit bezüglich des bestehenden Vertragsverhältnisses**

In einigen Meldungen gaben Verantwortliche als Grund für eine verspätete Meldung an, dass man zwar die Datenpannenmeldungen von Stay Informed erhalten, aber nicht gewusst habe, was man damit anfangen solle. Man sei davon ausgegangen, dass Stay Informed diese Panne direkt an die Datenschutz-Aufsichtsbehörden gemeldet habe. Diesen Verantwortlichen war weder bewusst, welche Art von Vertragsverhältnis mit Stay Informed bestand, noch, welche Pflichten sich für die Beteiligten daraus ergaben.

Bei der Nutzung von Apps handelt es sich häufig um eine Auftragsverarbeitung mit der Folge, dass der Träger der nutzenden Einrichtung Verantwortlicher im Sinne des Datenschutzrechts bleibt – auch wenn die konkrete Datenpanne beim App-Anbieter aufgetreten ist. Der Verantwortliche ist unter anderem verpflichtet, Datenpannen an die zuständige Datenschutz-Aufsichtsbehörde zu melden und beim Auftragsverarbeiter auf eine angemessene Aufarbeitung sowie auf Umsetzung der gebotenen technisch-organisatorischen Maßnahmen hinzuwirken. Auftragsverarbeitung bedeutet für den Verantwortlichen also nicht „Problementsorgung“: Soweit sie reicht, bewirkt sie lediglich eine Schwerpunktverschiebung von einer Ausführungs- zu einer Überwachungsverantwortlichkeit.

— **Zügige Bearbeitung von Meldungen des Auftragsverarbeiters sicherstellen**

In einigen Fällen haben Verantwortliche die E-Mails des App-Anbieters zur Datenpanne gar nicht näher gesichtet, sondern als Werbemails angesehen und nicht weiter beachtet. Dementsprechend wurden die Datenpannenmeldungen erst deutlich verspätet abgeben.

Verantwortliche sollten daher mit ihren Auftragnehmern abklären, auf welchen Kommunikationswegen sicherheitsrelevante Informationen mitgeteilt werden, und intern eine zeitnahe Weiterbehandlung sicherstellen.

— **Erstmeldung an die Aufsichtsbehörde innerhalb von 72 Stunden**

Die 72-Stunden-Regelfrist für die Meldung einer Datenpanne bei der zuständigen Datenschutz-Aufsichtsbehörde gilt auch für Datenpannen bei Auftragsverarbeitern. Die Datenpanne wird dem Verantwortlichen spätestens zu dem Zeitpunkt bekannt, in welchem er durch den Auftragsverarbeiter von der Datenpanne erfährt. Entsprechende Nachrichten sollten auch aus diesem Grund ernstgenommen werden.

— **Klärung der konkret betroffenen eigenen Daten**

Im Falle der Stay Informed-Datenpanne hat der Anbieter mitgeteilt, welche Datenkategorien von dem Vorfall grundsätzlich betroffen waren (PDF-Anhänge, CSV-Dateien, Avatare, verschlüsselte Unterschriften usw.). Dies mag für eine Erstmeldung ausreichend sein, in einem nächsten Schritt war

jedoch konkret zu klären, welche Funktionen der App in der eigenen Einrichtung tatsächlich genutzt wurden und welche Daten somit konkret betroffen waren. So nutzten nicht alle Einrichtungen die Unterschriftsfunktion, sodass dann diesbezüglich auch keine Risiken für eine missbräuchliche Nutzung bestanden. Außerdem war die Zahl der tatsächlich betroffenen Personen (Kinder, Eltern, Beschäftigte der Einrichtung usw.) zu ermitteln. Ausweichende oder inkonsistente Angaben – wie etwa der Verweis auf die vom Auftragsverarbeiteter angegebene Gesamtzahl der betroffenen Personen für alle Kunden– genügen dabei nicht.

– **Eigene Risikobewertung, Festlegung von Abhilfemaßnahmen**

Die Meldungen zur Stay Informed Datenpanne haben gezeigt, wie unterschiedlich die App in den verschiedenen Einrichtungen benutzt wurde. Dementsprechend hatte auch jeder Verantwortliche eine eigenständige Risikobewertung durchzuführen. Dies war insbesondere vor dem Hintergrund wichtig, dass bei hohen Risiken die betroffenen Personen nach Art. 34 DSGVO informiert werden müssen.

Der Dienstleister musste dem Verantwortlichen dazu Informationen zum technischen Hintergrund, zu Ermittlungsergebnissen, nachweisbaren unbefugten Zugriffen und ergriffenen Maßnahmen bereitstellen. Nur auf dieser Grundlage konnte ein Verantwortlicher die Risiken hinsichtlich der konkret betroffenen Daten und Personen bewerten. Dies musste er dann auch tun. Es genügte also nicht, lediglich den Input des App-Anbieters zu übernehmen.

– **Soweit erforderlich: unaufgeforderter Nachbericht**

Konnten in der Erstmeldung noch nicht alle Angaben gemacht werden, war die Meldepflicht aus Art. 33 DSGVO auch noch nicht vollständig erfüllt. Dann war ein unaufgeforderter Nachbericht angezeigt, der die noch fehlenden Informationen zu enthalten hatte.

8.8 Durchsetzung einer Anordnung nach Art. 58 Abs. 2 DSGVO mit Zwangsgeld

Wie bereits in meinem 33. Tätigkeitsbericht 2023 unter Nr. 11.11 dargestellt, erließ ich im Jahr 2022 eine Anweisung nach Art. 58 Abs. 2 Buchst. d DSGVO zur Umsetzung eines adäquaten Rollen- und Berechtigungssystems gegen ein bayerisches Klinikum und drohte für den Fall der Nichterfüllung ein Zwangsgeld an. Damit sollte meinen seit 2019 bestehenden Forderungen zur Umsetzung eines datenschutzgerechten Rollen- und Rechtekonzepts für das Krankenhausinformationssystem Nachdruck verliehen werden.

Das Klinikum setzte nicht alle geforderten Maßnahmen fristgerecht um. Daher wurde das Zwangsgeld nach Ablauf der eingeräumten Frist in Höhe von 17.500 Euro zur Zahlung fällig.

Um die Mängelbehebung weiter voranzutreiben, habe ich habe ich die Zwangsgeldandrohung wiederholt. Im Rahmen der Abwägung der mir zur Verfügung ste-

henden Möglichkeiten sehe ich dies derzeit als geeignetstes Mittel an, um den zeitnahen Abschluss der Arbeiten am Berechtigungskonzept zu erreichen. Ein Bußgeld nach Art. 83 DSGVO ist dadurch nicht ausgeschlossen.

8.9 Ausgewählte Beanstandungen

Im Lauf des Jahres habe ich auch außerhalb des Kontextes „Hackerangriffe“ (siehe Nr. 8.6.2) einige Beanstandungen ausgesprochen, die ihren Hintergrund in technisch-organisatorischen Mängel hatten. Zwei Beispiele möchte ich im Folgenden aufführen, um für die beschriebenen Konstellationen zu sensibilisieren.

8.9.1 Beanstandung mangelhafter Schutzmaßnahmen im Zusammenhang mit der Aufbewahrung sensibler Unterlagen

Ein städtisches Kinder- und Jugendhilfezentrum bewahrte über viele Jahre hinweg Akten von ehemaligen Bewohnerinnen und Bewohnern in einem Zimmer auf, das betreuten Jugendlichen als Wohnraum diente. Die Unterlagen befanden sich dort in einem Wandschrank, der lediglich mit einem lockeren Vorhängeschloss versehen war. So konnte eine Bewohnerin den Schrank so weit öffnen, dass sie auf Akten zugreifen konnte.

Die Stadt hat somit sensible Daten Minderjähriger in einem unzureichend gesicherten Schrank und an ungeeigneter Stelle aufbewahrt. Es konnte im Rahmen der Aufbereitung des Vorfalls nicht mehr nachvollzogen werden, warum und wie lange sich der Schrank schon dort befand. Auch fand offensichtlich keine Prüfung der Aufbewahrung statt Es handelt sich damit um einen Verstoß gegen Art. 32 Abs. 1 Buchst. b und d in Verbindung mit Art. 24 Abs. 1 DSGVO, nach dem der Verantwortliche geeignete technische und organisatorische Maßnahmen zur Sicherstellung der Vertraulichkeit auch von Papierakten zu ergreifen hat.

Ich habe den Verstoß beanstandet und die Stadt zur Abhilfe aufgefordert.

Alle öffentlichen Stellen haben dafür Sorge zu tragen, dass Papierakten mit personenbezogenen Daten in geeignet verschließbaren Schränken und ausschließlich in Räumlichkeiten aufbewahrt werden, die nur von berechtigen Personen betreten werden können.

8.9.2 Beanstandungen unverschlüsselten E-Mail-Versands an eine Vielzahl von Empfängern

Ein Mitarbeiter eines Universitätsklinikums verschickte im Rahmen einer medizinischen Studie eine Einladung zu einer Schulungsveranstaltung per unverschlüsselter E-Mail. Er nutzte dabei das Adressfeld „An“ anstelle von „Bcc“. Das hatte zur Folge, dass alle E-Mail-Adressen für alle Empfänger alle sichtbar waren. Titel und Inhalt der E-Mail ließen erkennen, dass alle angeschriebenen Personen Teilnehmer einer Studie zu einer bestimmten Erkrankung waren, also möglicherweise an dieser Krankheit litten.

Ein ähnlich gelagerter Fall fand in einem Landratsamt statt: Ein Mitarbeiter des beanstandeten Landratsamtes hatte im Rahmen eines Infektionsgeschehens eine E-

Mail mit sensiblen Gesundheitsdaten ohne angemessene Sicherheitsvorkehrungen über das Internet versandt und darüber hinaus statt des „Bcc“-Felds das „Cc“-Feld verwendet, wodurch die E-Mail-Adressen der Empfänger ebenfalls für alle sichtbar waren. Damit wurde zumindest ein Infektionsverdacht im Adressatenkreis offengelegt.

Wie unter anderem schon in meinem 27. Tätigkeitsbericht 2016 unter Nr. 2.1.3 dargestellt, handelt es sich bei einem Versand per „Cc“ um eine unbefugte Datenübermittlung, in diesem Fall von Gesundheitsdaten. Auch die Thematik des unverschlüsselten E-Mail-Versands wurde bereits in meinem Tätigkeitsbericht behandelt.

Ich habe die festgestellten Verstöße in beiden Fällen förmlich beanstandet und die Stellen aufgefordert, alle Beschäftigten hinsichtlich der E-Mail-Kommunikation zu sensibilisieren. Besteht Bedarf an einer elektronischen Kommunikation von Gesundheitsdaten, muss der Verantwortliche den Beschäftigten entsprechend sichere Kommunikationsmöglichkeiten zur Verfügung stellen, siehe näher mein 32. Tätigkeitsbericht 2022 unter Nr. 12.5.5.

9 Datenschutzkommission

Der Datenschutzkommission beim Bayerischen Landtag gehörten im Berichtszeitraum folgende Mitglieder und stellvertretende Mitglieder an:

Aus dem Landtag:

Mitglieder:

Peter Tomaschko, CSU
Tobias Beck, FREIE WÄHLER
Benjamin Adjei, BÜNDNIS 90/DIE GRÜNEN
Horst Arnold, SPD
Dr. Alexander Dietrich, CSU
Thomas Holz, CSU
Gerd Mannes, AfD

Stellvertretende Mitglieder:

Leo Dietz, CSU
Felix Locke, FREIE WÄHLER
Verena Osgyan, BÜNDNIS 90/DIE GRÜNEN
Katja Weitzel, SPD
Josef Heisl, CSU
Thorsten Schwab, CSU
Roland Magerl, AfD

Auf Vorschlag der Staatsregierung:

Mitglied:

Leitende Ministerialrätin Christina Rölz, Datenschutzbeauftragte des Bayerischen Staatsministeriums des Innern, für Sport und Integration

Stellvertretendes Mitglied:

Leitende Ministerialrätin Ilka Bürger, Datenschutzbeauftragte des Bayerischen Staatsministeriums für Wirtschaft, Landesentwicklung und Energie

Auf Vorschlag der kommunalen Spitzenverbände in Bayern:

Mitglied:

Rudolf Schleyer, Vorstandsvorsitzender der Anstalt für Kommunale Datenverarbeitung in Bayern

Stellvertretendes Mitglied:

Cynthia Derra, Datenschutzbeauftragte des Bayerischen Landkreistags

Auf Vorschlag des Staatsministeriums für Gesundheit, Pflege und Prävention aus dem Bereich der gesetzlichen Sozialversicherungsträger:

Mitglied:

Werner Krempl, Erster Direktor und Geschäftsführer der Deutschen Rentenversicherung Nordbayern

Stellvertretendes Mitglied:

Dr. Irmgard Stippler, Vorsitzende des Vorstandes der AOK Bayern – Die Gesundheitskasse

Auf Vorschlag des Verbands Freier Berufe in Bayern e. V.:

Mitglied:

Dr. Till Schemmann, Notar

Stellvertretendes Mitglied:

Dr. Thomas Kuhn, Rechtsanwalt

Herr Peter Tomaschko, MdL, führt den Vorsitz in der Datenschutzkommission; stellvertretender Vorsitzender ist Herr Tobias Beck, MdL.

Die Datenschutzkommission beim Bayerischen Landtag tagte im Berichtszeitraum drei Mal.

10 Ländervertreter im EDSA

Seit 2021 bin ich der vom Bundesrat nach § 17 Abs. 1 Satz 2 Bundesdatenschutzgesetz für fünf Jahre gewählte Ländervertreter im Europäischen Datenschutzausschuss (EDSA; allgemein zu diesem Ausschuss und zu meinen Aufgaben als Ländervertreter siehe meinen 31. Tätigkeitsbericht 2021 unter Nr. 12).

Um die europaweit einheitliche Anwendung des Datenschutzrechts zu gewährleisten, beschließt der EDSA insbesondere Leitlinien und spricht Empfehlungen aus. Er gibt Stellungnahmen in Rechtsetzungsverfahren ab und entscheidet über Meinungsverschiedenheiten zwischen einzelnen Datenschutz-Aufsichtsbehörden (vgl. Art. 70 Abs. 1 DSGVO). Durch diese Tätigkeiten trägt der EDSA insbesondere zu einer verbesserten Zusammenarbeit in grenzüberschreitenden Sachverhalten bei.

Im Jahr 2024 hat der EDSA zwölfmal getagt. Folgende Arbeitsergebnisse des EDSA möchte ich besonders hervorheben:

- Die **Stellungnahme 08/2024 zur Wirksamkeit von Einwilligungen im Kontext von „Consent or Pay"-Modellen großer Online-Plattformen**[103] des EDSA betont, dass Einwilligungen in solchen Modellen nur als wirksam gelten, wenn sie freiwillig, spezifisch, informiert und unmissverständlich erteilt werden. Zudem wird hervorgehoben, dass eine „gleichwertige Alternative" angeboten werden sollte, die nicht an die Zahlung eines Entgelts geknüpft ist, um sicherzustellen, dass Nutzer nicht unter Druck gesetzt werden, ihre Zustimmung zu geben. Eine solche Alternative unterstützt die Annahme der Freiwilligkeit erklärter Einwilligungen.

- In der Stellungnahme 22/2024 äußert sich der EDSA zu bestimmten Verpflichtungen, die sich aus der Inanspruchnahme von Auftragsverarbeitern und Unterauftragsverarbeitern ergeben.[104] Die Stellungnahme steht im Kontext eines Verfahrens nach Art. 64 Abs. 2 DSGVO, das jede Aufsichtsbehörde einleiten kann, wenn die gestellten Fragen von europaweiter Relevanz sind. Aufgeworfen waren mehrere Fragen zur Auslegung von Art. 28 und 44 DSGVO. Die Fragen betrafen insbesondere die Rechenschaftspflicht des Verantwortlichen beim Einsatz mehrerer „in Kette" hintereinander geschalteter (Unter-)Auftragsverarbeiter. Daneben ging es um Fragen der vertraglichen Ausgestaltung von Vereinbarungen zur Auftragsverarbeitung. Diese Fragen betrafen sowohl Verarbeitungen innerhalb des Europäischen Wirtschaftsraums (EWR) als auch Konstellationen mit Drittstaatenbezug.

- Die **Stellungnahme 28/2024** behandelt **gewisse Datenschutzaspekte der Verarbeitung personenbezogener Daten im Zusammenhang mit**

[103] Internet: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_de.

[104] Internet: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-222024-certain-obligations-following_de.

KI-Modellen.[105] Die Stellungnahme behandelt insbesondere die Fragen, wann und unter welchen Voraussetzungen ein KI-Modell für „anonym" befunden werden kann, auf welche Weise Verantwortliche die Angemessenheit des berechtigten Interesses als Rechtsgrundlage nachweisen können, wobei zwischen Entwicklungs- und Einsatzphase zu unterscheiden ist, und welche Folgen eine rechtswidrige Verarbeitung personenbezogener Daten in der Entwicklungsphase eines KI-Modells auf die spätere Verarbeitung oder den späteren Betrieb des KI-Modells hat.

– Die **Leitlinien 1/2024 on processing of personal data based on Article 6(1)(f) GDPR**[106] befassen sich mit den Voraussetzungen und dem Anwendungsbereich dieses Rechtfertigungsgrundes. Zugleich behandeln sie beispielhaft Konstellationen, in denen Verantwortliche Datenverarbeitungen auf ein berechtigtes Interesse stützen.

  Für öffentliche Stellen ist besonders die Feststellung wichtig, dass sich Behörden nur in besonderen Ausnahmefällen auf diesen Rechtfertigungsgrund berufen können. Ausgeschlossen wird die Berufung auf berechtigte Interessen für Datenverarbeitungen im Zusammenhang mit der spezifischen Aufgabe der jeweiligen Behörde. Das entspricht Art. 6 Abs. 1 UAbs. 2 DSGVO.

[105] Internet: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_de.

[106] Internet: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en.

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
CSU	Christlich-Soziale Union in Bayern
DSFA	Datenschutzfolgenabschätzung
DSGVO	Datenschutz-Grundverordnung
EDV	Elektronische Datenverarbeitung
EG	Erwägungsgrund
FDP	Freie Demokratische Partei
ff.	(nach)folgende
GVBl.	Bayerisches Gesetz- und Verordnungsblatt
https	Hyper Text Transfer Protocol Secure
IP	Internet Protocol
IT	Informationstechnik
MdL	Mitglied des Landtages
Nr.	Nummer
PC	Personalcomputer
RLDSJ	Datenschutz-Richtlinie für Polizei und Strafjustiz
Rn.	Randnummer
sog.	sogenannt
SPD	Sozialdemokratische Partei Deutschlands
SSL	Secure Socket Layer
u. a.	unter anderem/und andere
UAbs.	Unterabsatz
vgl.	vergleiche
www	World Wide Web

Stichwortverzeichnis