Der Bayerische Landesbeauftragte für den Datenschutz informiert die Öffentlichkeit

28. Tätigkeitsbericht

Berichtszeitraum
2017/2018

28. Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz

gemäß Art. 59 Datenschutz-Grundverordnung

Berichtszeitraum: 1. Januar 2017 bis 31. Dezember 2018
Veröffentlichungsdatum: 20. Mai 2019

Inhaltsverzeichnis

Hinweis zu Abkürzungen:

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

BayDSG	**Bayerisches Datenschutzgesetz** vom 15. Mai 2018 (GVBl. S. 230), geändert durch § 6 Gesetz vom 18. Mai 2018 (GVBl. S. 301)
BayDSG-alt	**Bayerisches Datenschutzgesetz** vom 23. Juli 1993 (GVBl. S. 498), zuletzt geändert durch Art. 40 Abs. 2 Nr. 1 Bayerisches Datenschutzgesetz vom 15. Mai 2018 (GVBl. S. 230) – bis zum 24. Mai 2018 geltende Fassung
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (**Datenschutz-Grundverordnung**, ABl. L 119 vom 4. Mai 2016, S. 1, berichtigt ABl. L 314 vom 22. November 2016, S. 72, und ABl. L 127 vom 23. Mai 2018, S. 2)
RLDSJ	**Datenschutz-Richtlinie für Polizei und Strafjustiz**; die vollständige Bezeichnung lautet: Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4. Mai 2016, S. 89)

1 Überblick

1.1 EU: Die Datenschutz-Grundverordnung – ein Rechtsakt mit Doppelcharakter

Das Jahr 2018 stand im Zeichen einer umfassenden Datenschutzreform. Im Mittelpunkt des zuvor national geprägten Datenschutzrechts steht nun die seit dem 25. Mai 2018 geltende Datenschutz-Grundverordnung, die in der gesamten Europäischen Union im Grundsatz einheitliche Maßstäbe setzt.

Nach dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV) wirkt eine Verordnung in den Mitgliedstaaten unmittelbar und allgemein (Art. 288 AEUV).

Art. 288 AEUV
Für die Ausübung der Zuständigkeiten der Union nehmen die Organe Verordnungen, Richtlinien, Beschlüsse, Empfehlungen und Stellungnahmen an.
Die Verordnung hat allgemeine Geltung. Sie ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.
Die Richtlinie ist für jeden Mitgliedstaat, an den sie gerichtet wird, hinsichtlich des zu erreichenden Ziels verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel.
Beschlüsse sind in allen ihren Teilen verbindlich. Sind sie an bestimmte Adressaten gerichtet, so sind sie nur für diese verbindlich.
Die Empfehlungen und Stellungnahmen sind nicht verbindlich.

Eine Verordnung ist auch die Datenschutz-Grundverordnung. Anders als eine Richtlinie ist sie in weiten Teilen nicht an den nationalen Gesetzgeber gerichtet, der ihre Vorgaben auch nicht mehr in eigenen Rechtsakten umsetzen muss. Die Datenschutz-Grundverordnung begründet für die Bürgerinnen und Bürger, für den Staat, die Unternehmen und viele andere für die Verarbeitung personenbezogener Daten Verantwortliche unmittelbar Rechte und Pflichten. So können sich etwa die Bürgerinnen und Bürger auf die Betroffenenrechte in Art. 12 ff. DSGVO berufen, und die Verantwortlichen müssen sich beispielsweise an die Regelungen zu den Rechtsgrundlagen von Verarbeitungen nach Art. 6 DSGVO oder an die Vorgaben zum technisch-organisatorischen Datenschutz in Art. 23 f. DSGVO halten.

Gleichwohl hat es vor allem im Jahr 2018 eine umfangreiche Anpassungsgesetzgebung auf der Bundes- wie auf der Landesebene gegeben. Wie kommt das?

Die Antwort auf diese Frage lautet: Die Datenschutz-Grundverordnung ist keine gewöhnliche Verordnung – darauf deutet bereits der Name hin: Datenschutz-**Grund**verordnung. Die Vorgaben der Datenschutz-Grundverordnung wirken auf unterschiedliche Weise, je nachdem, ob die Verarbeitung personenbezogener Daten im privaten oder im öffentlichen Interesse erfolgt.

Bei der **Verarbeitung personenbezogener Daten im privaten Interesse** sind die Regelungen der Datenschutz-Grundverordnung nahezu abschließend – die Mitgliedstaaten haben insoweit fast keine Möglichkeiten, die unionsrechtlichen Vorgaben noch zu konkretisieren oder gar auszugestalten. Eine „nationale Note“ kann

hier nur der Normvollzug haben, wie beispielsweise in den Orientierungshilfen, Arbeitspapieren und anderen Handreichungen der Aufsichtsbehörden oder in der Rechtsprechung. Im Unionsrecht vorgesehene Instrumente zur Förderung der Konvergenz wirken aber auch hier auf eine Vereinheitlichung unter den Mitgliedstaaten hin (siehe etwa Art. 70 DSGVO).

Die **Verarbeitung personenbezogener Daten im öffentlichen Interesse** hingegen setzt in vielfacher Hinsicht voraus, dass der nationale Gesetzgeber durch eigenes Recht die Vorgaben der Datenschutz-Grundverordnung näher konkretisiert. Nach Art. 6 Abs. 1 DSGVO gibt es insbesondere zwei Rechtsgrundlagen für Verarbeitungen personenbezogener Daten, die für Verarbeitungen im öffentlichen Interesse in Betracht kommen. Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO ermöglicht die Verarbeitung zur Erfüllung von rechtlichen Pflichten, die dem Verantwortlichen auferlegt sind. Nach Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO kann eine Verarbeitung rechtmäßig sein, wenn sie für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

Dazu stellt Art. 6 Abs. 3 UAbs. 1 DSGVO klar, dass Art. 6 Abs. 1 UAbs. 1 Buchst. c und e DSGVO selbst **keine** Verarbeitungsbefugnisse enthalten, sondern solche Verarbeitungsbefugnisse gerade voraussetzen, welche der Unionsgesetzgeber oder die Mitgliedstaaten erst schaffen müssen. Die Mitgliedstaaten sind bei der Formulierung der konkretisierenden Regelungen in ihrem nationalen Recht allerdings nicht frei. Insbesondere Art. 6 Abs. 2 und 3 DSGVO geben den Mitgliedstaaten Leitlinien an die Hand, wie die ihnen eingeräumten Spielräume zu nutzen sind. Im Übrigen unterliegt das nationale Recht dem Anwendungsvorrang des Unionsrechts und damit auch der Datenschutz-Grundverordnung.

Bei der Verarbeitung personenbezogener Daten im öffentlichen Interesse gewährt die Datenschutz-Grundverordnung den Mitgliedstaaten Gestaltungsspielräume auch in Bezug auf die Betroffenenrechte nach Art. 12 ff. DSGVO. Die Bestimmung des Art. 23 DSGVO lässt insofern Beschränkungen zu – allerdings nur, soweit diese den Wesensgehalt der Grundrechte und Grundfreiheiten achten und in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme darstellen. Eine Beschränkung muss einem der in Art. 23 Abs. 1 DSGVO aufgeführten Ziele verpflichtet sein. Dies hindert den Gesetzgeber, mit Beschränkungen andere öffentliche Interessen zu verfolgen.

Der Bundesgesetzgeber wie auch die Landesgesetzgeber haben vor diesem Hintergrund das nationale Datenschutzrecht umfassend reformiert. Dies gilt sowohl für das allgemeine Datenschutzrecht – namentlich das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze – als auch für das bereichsspezifische Datenschutzrecht des öffentlichen Sektors – zahlreiche Gesetze des Bundes- wie des Landesrechts enthalten in mehr oder minder großem Umfang datenschutzrechtliche Vorschriften. Viele der Gesetzgebungsverfahren des Bundes und des Freistaats Bayern konnte ich begleiten. Diese Arbeiten haben die Tätigkeit meiner Geschäftsstelle im Berichtszeitraum wesentlich geprägt (siehe näher Nr. 1.2 sowie Nr. 1.3).

1.2 Anpassungsgesetzgebung des Bundes

In einer ersten Novellierungsphase hat der Bundesgesetzgeber zunächst das **allgemeine Datenschutzrecht des Bundes** grundlegend überarbeitet. Mit dem Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU) vom 30. Juni 2017 hat der Bundestag eine neue Fassung des Bundesdatenschutzgesetzes (BDSG) verabschiedet (veröffentlicht in BGBl. I S. 2097). In erster Linie gilt das neue Bundesdatenschutzgesetz für die Verarbeitung personenbezogener Daten durch öffentliche Stellen des Bundes sowie durch nichtöffentliche Stellen. Für bayerische öffentliche Stellen ist dieses Gesetz relevant, soweit sie als Unternehmen am Wettbewerb teilnehmen.

Art. 1 BayDSG
Anwendungsbereich des Gesetzes
(3) [1]Soweit öffentliche Stellen als Unternehmen am Wettbewerb teilnehmen, gelten für sie selbst, ihre Zusammenschlüsse und Verbände die Vorschriften für nichtöffentliche Stellen. […]

§ 1 BDSG
Anwendungsbereich des Gesetzes
(1) […] [2]Für nichtöffentliche Stellen gilt dieses Gesetz für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, es sei denn, die Verarbeitung durch natürliche Person erfolgt zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.

Mit dem Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 17. Juli 2017 (BGBl. I S. 2541) hat der Bund im Zuge der ersten Novellierungsphase auch das im Zehnten Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – geregelte bereichsspezifische **Datenschutzrecht für Sozialdaten** reformiert und außerdem **datenschutzrechtliche Bestimmungen** in das **Abgabenrecht** aufgenommen.

Dieses Gesetzgebungsverfahren verlief aus verfassungsrechtlicher Sicht nicht optimal. Die immerhin zweijährige Anpassungsfrist der Datenschutz-Grundverordnung hätte eine Vorgehensweise erlaubt, bei der ein frühzeitig erarbeiteter Entwurf in der Fachöffentlichkeit diskutiert, anschließend optimiert und im Parlament eingehend beraten wird. Bei einer so weitreichenden Reform wäre diese Vorgehensweise nach meiner Auffassung auch die einzig seriös mögliche gewesen. Stattdessen wurde ein umfangreiches datenschutzrechtliches Gesetzgebungspaket gleichsam „über Nacht" im Wege einer Ausschussempfehlung an einen dem Titel nach „unverfänglichen" Gesetzentwurf „angehängt" (siehe Bundestags-Drucksachen 18/12041 und 18/12611). Dies geschah, obwohl die betroffenen Rechtsmaterien – das bereichsspezifische Datenschutzrecht der Sozialdaten und der Steuerdaten – nicht nur deutschlandweit eine erhebliche praktische Relevanz haben, sondern auch für die Verwirklichung des Datenschutzgrundrechts von wesentlicher Bedeutung sind (siehe zu diesen Themen auch Nr. 9.1 und 10.1).

Am Ende des Berichtszeitraums (31. Dezember 2018) war die zweite Novellierungsphase noch nicht abgeschlossen, die sich vor allem auf eine **Anpassung des bereichsspezifischen Datenschutzrechts** bezieht.

Von besonderer Bedeutung ist hier der Entwurf eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU) (Bundestags-Drucksache 19/4674), der auf eine Änderung von über 150 Bundesgesetzen abzielt.

Für Belange der Justiz besonders bedeutsam ist der Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679 (Bundestags-Drucksache 19/4671). Dieser Entwurf zielt unter anderem auf eine Änderung der Bestimmungen des Strafverfahrensrechts (siehe dazu auch Nr. 6.1.3).

In den dargestellten Gesetzgebungsverfahren habe ich – soweit ich dazu Gelegenheit erhielt – auf datenschutzfreundliche Regelungslösungen hingewirkt.

1.3 Bayerische Gesetzgebung zur Anpassung des Datenschutzrechts an die Datenschutz-Grundverordnung und zur Umsetzung der Datenschutz-Richtlinie für Polizei und Strafjustiz

1.3.1 Bayerisches Datenschutzgesetz

Auch der bayerische Gesetzgeber hat die datenschutzrechtlichen Bestimmungen des Landesrechts an das EU-Datenschutzrecht anpassen müssen. Sehr intensiv habe ich das Gesetzgebungsverfahren zum Bayerischen Datenschutzgesetz vom 15. Mai 2018 (GVBl. S. 230) begleitet.

Im Unterschied zum Bund hat der Freistaat Bayern die Reform seines allgemeinen Datenschutzrechts mit Änderungen weiterer Rechtsvorschriften verbunden (zu Einzelaspekten siehe insbesondere den Beitrag unter Nr. 2). So sieht jetzt Art. 24 Abs. 4 GO eine neue Regelung für den Einbau und Betrieb elektronischer Wasserzähler mit Funkbetrieb vor (siehe Nr. 7.3.3).

Was bereichsspezifische Reformen im Zusammenhang mit der Datenschutz-Grundverordnung und der Datenschutz-Richtlinie für Polizei und Strafjustiz anbelangt, möchte ich weiterhin auf das Gesetz zur datenschutzrechtlichen Anpassung der bayerischen Vollzugsgesetze vom 24. Juli 2018 (GVBl. S. 574), das Gesetz zur Änderung personalaktenrechtlicher und weiterer dienstrechtlicher Vorschriften vom 18. Mai 2018 (GVBl. S. 286), das Gesetz zur Neuordnung des bayerischen Polizeirechts (PAG-Neuordnungsgesetz) vom 18. Mai 2018 (GVBl. S. 301) sowie das Gesetz zum weiteren Nachvollzug der Datenschutz-Grundverordnung im Landesrecht vom 18. Mai 2018 (GVBl. S. 341) hinweisen.

Alle Gesetzgebungsvorhaben zur Anpassung an die Datenschutz-Grundverordnung sowie zur Umsetzung der Datenschutz-Richtlinie für Polizei und Strafjustiz habe ich beratend begleitet, wie sich aus den nachfolgenden Kapiteln ergibt.

1.3.2 Das PAG-Neuordnungsgesetz und die PAG-Begleitkommission

Von heftigen politischen Protesten begleitet war insbesondere die Verabschiedung des PAG-Neuordnungsgesetzes. Angesichts der politischen Debatte hat der

Ministerrat am 12. Juni 2018 beschlossen, eine **Expertenkommission zur Begleitung des neuen Polizeiaufgabengesetzes (PAG)** einzurichten. Sie steht unter Vorsitz des Präsidenten des Bayerischen Verfassungsgerichtshofs a. D., Dr. Karl Huber und setzt sich aus sechs Mitgliedern zusammen. Die Kommission hat den Auftrag, die Umsetzung des neu gefassten Polizeiaufgabengesetzes eng zu begleiten und unabhängig zu prüfen.

Auch ich bin von der Staatsregierung ersucht worden, an dieser PAG-Begleitkommission mitzuwirken. Dieser Bitte bin ich nachgekommen – allerdings unter der ausdrücklichen Bedingung, dass die Tätigkeit als Kommissionsmitglied die Unabhängigkeit meiner Amtsführung als Bayerischer Landesbeauftragter für den Datenschutz nicht beeinträchtigen darf. Die Kommission wird grundsätzlich nicht zur Verfassungskonformität des PAG-Neuordnungsgesetzes Stellung nehmen, sondern sich auf eine Evaluierung des Gesetzesvollzugs beschränken (zu meiner Stellungnahme im Gesetzgebungsverfahren siehe den Beitrag Nr. 4.1.1).

1.4 Rechtsprechung

1.4.1 Europäischer Gerichtshof

Im Berichtszeitraum sind zahlreiche Urteile des Europäischen Gerichtshofs ergangen, die für die Verarbeitung personenbezogener Daten durch bayerische öffentliche Stellen Auswirkungen haben können. Ganz überwiegend betrafen die Entscheidungen die Auslegung der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, welche durch die Datenschutz-Grundverordnung abgelöst worden ist. In Anbetracht von Kontinuitäten im Regelungsbestand sind die Aussagen in diesen Gerichtsentscheidungen regelmäßig auch für das Verständnis von Vorschriften der Datenschutz-Grundverordnung von Bedeutung.

In besonderem Maße gilt dies für mehrere Entscheidungen, die der Europäische Gerichtshof zur **datenschutzrechtlichen Verantwortlichkeit** getroffen hat. So hat der Gerichtshof mit Urteil vom 5. Juni 2018 (Az.: C-210/16) eine Mitverantwortlichkeit von Fanpagebetreibern an der Verarbeitung personenbezogener Daten durch Facebook im Grundsatz bejaht, dabei allerdings die Frage nach dem Umfang dieser Mitverantwortlichkeit nicht abschließend geklärt. Maßgeblich für eine datenschutzrechtliche Verantwortlichkeit ist die Fähigkeit einer Stelle, die Zwecke und Mittel der Verarbeitung zu beeinflussen. Sind mehrere Stellen an einer Verarbeitung beteiligt, ist die Mitverantwortlichkeit nicht nur deshalb ausgeschlossen, weil ein anderer Mitverantwortlicher im stärkeren Maß über die Zwecke und Mittel der Verarbeitung entscheiden kann.

In einer weiteren Entscheidung hat der Europäische Gerichtshof festgestellt, dass die datenschutzrechtliche Verantwortung selbst dann nicht ausgeschlossen ist, wenn der (Mit-)Verantwortliche keinen Zugriff auf die verarbeiteten Daten ausgeübt hat. In diesem Fall ging es um eine Religionsgemeinschaft, die ihre Mitglieder zu Missionstätigkeiten angehalten hatte und dabei das handschriftliche Führen von Besuchsheften eingefordert hatte (Urteil vom 10. Juli 2018, Az.: C-25/17). Speziell in Bezug auf die Mitverantwortlichkeit von Fanpagebetreibern hat die Datenschutzkonferenz mehrere Entschließungen gefasst, die ich im Ergebnis unter

stützt habe (siehe dazu Nr. 13.1.). Ein weiteres, zum Redaktionsschluss noch anhängiges Verfahren vor dem Europäischen Gerichtshof wird die Rechtslage hoffentlich klären (Az.: C-40/17).

Im Berichtszeitraum hat sich der Europäische Gerichtshof mehrmals mit der **Vorratsspeicherung personenbezogener Daten zu Zwecken der öffentlichen Sicherheit** auseinandersetzen müssen.

In einem Gutachten zu einem geplanten Abkommen zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Flugpassagierdaten hat der Gerichtshof beispielsweise seine bisherige Rechtsprechung zur Vorratsverarbeitung personenbezogener Daten bestätigt (Gutachten vom 26. Juli 2017, Az.: 1/15). Danach verlangt das Grundrecht auf Schutz personenbezogener Daten aus Art. 8 Charta der Grundrechte der Europäischen Union (GRCh), dass im Fall der Übermittlung personenbezogener Daten aus der Union in ein Drittland der Fortbestand des durch das Unionsrecht gewährten hohen Niveaus des Schutzes der Grundfreiheiten und Grundrechte gewährleistet wird. Die in den Art. 7 und 8 GRCh niedergelegten Rechte können zwar keine uneingeschränkte Geltung beanspruchen, sondern müssen im Hinblick auf ihre gesellschaftliche Funktion gesehen werden. Eine Einschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten muss aber gesetzlich vorgesehen sein (Art. 52 Abs. 1 Satz 1 GRCh). Dies bedeutet, dass die gesetzliche Grundlage für den Eingriff den Umfang der Einschränkung selbst festlegen muss (Gutachten, Rn. 39). **Mit Blick auf den Grundsatz der Verhältnismäßigkeit müssen sich Ausnahmen und Einschränkungen des Schutzes personenbezogener Daten auf das absolut Notwendige beschränken**. (Gutachten, Rn.140) Hierfür muss die betreffende Vorschrift klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren Daten übermittelt wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen. Sie muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisch verarbeitet werden (Gutachten, Rn.141). Regelungen über die Speicherung personenbezogener Daten müssen unter anderem stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden personenbezogenen Daten und dem verfolgten Ziel herstellen. Was die Verwendung rechtmäßig gespeicherter personenbezogener Daten durch eine Behörde betrifft, darf sich eine Unionsregelung nicht darauf beschränken, dass der Zugang zu solchen Daten einem der in der Regelung genannten Zwecke zu entsprechen hat. Vielmehr muss sie auch die materiell- und verfahrensrechtlichen Voraussetzungen für die Verwendung der Daten festlegen.

Das hier vorgestellte Gutachten verdeutlicht, dass die Rechtsprechung des Europäischen Gerichtshofs zur grundrechtlichen Relevanz der Vorratsdatenspeicherung nicht nur im Zusammenhang mit der rechtspolitisch umstrittenen Vorratsspeicherung von Telekommunikationsverkehrsdaten zu beachten ist. Als besonders problematisch habe ich deshalb den Vorschlag der EU-Kommission für eine E-Evidence-Verordnung angesehen, mit der die Kommission eine Alternative zum förmlichen Rechtshilfeverfahren schaffen will (siehe dazu Nr. 6.3.1).

Für die Beschäftigten der bayerischen Behörden und öffentlichen Stellen relevant ist eine Entscheidung, die der Europäische Gerichtshof am 14. Februar 2019 zur

Videoaufzeichnung von Beamtinnen und Beamten einer Polizeidienststelle durch Private gefällt hat (Az.: C-345/17). Unter anderem hat der Gerichtshof nochmals klargestellt, dass das allgemeine Datenschutzrecht nicht aus dem Grund keine Anwendung findet, dass Polizeibeamte im Rahmen der Ausübung ihres Amtes auf Video aufgezeichnet werden. Einfacher ausgedrückt: Auch Beschäftigte bei der öffentlichen Verwaltung können sich auf ihr Datenschutzgrundrecht berufen. Dies gilt selbstverständlich nicht nur für die Verarbeitung durch Private, sondern gegenüber der öffentlichen Hand selbst.

1.4.2 Höchstrichterliche deutsche Rechtsprechung

Im Rahmen einer Entscheidung, welche die Verpflichtung einer bayerischen öffentlichen Stelle zur Beantwortung einer Presseanfrage betraf, hat sich das Bundesverwaltungsgericht gegen Ende des Berichtszeitraums erstmals zu der Übermittlungsvorschrift in Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG geäußert (Bundesverwaltungsgericht, Urteil vom 27. September 2018, Az.: 7 C 5/17). Eine Stellungnahme zu dieser Entscheidung habe ich auf meiner Internetpräsenz (https://www.datenschutz-bayern.de) in der Rubrik „Datenschutzreform 2018“ veröffentlicht.

1.5 Öffentlichkeitsarbeit

Öffentlichkeitsarbeit hat eine zentrale Bedeutung für den Datenschutz. Informationen und datenschutzrechtliche Positionen sollen – über den unmittelbaren Kontakt mit der Politik, der Presse, den Behörden und den im Einzelfall betroffenen Personen hinaus – allgemein bekannt und verfügbar gemacht werden. Auch so kann ich die Verwaltung dabei unterstützen, datenschutzkonform zu handeln. Bürgerinnen und Bürgern helfe ich damit, ihre Rechte und Schutzmöglichkeiten zu (er)kennen und wahrzunehmen. Wegen der Neuordnung des Europäischen Datenschutz-Rechtsrahmens und der daraus folgenden Änderungen hat es im Berichtszeitraum einen erheblich erhöhten Informationsbedarf gegeben.

Ein wesentlicher Baustein der Öffentlichkeitsarbeit ist der Internetauftritt meiner Dienststelle (https://www.datenschutz-bayern.de). Erfreulicherweise steigen die Zugriffszahlen von Berichtszeitraum zu Berichtszeitraum weiterhin deutlich an. Über neue sowie aktualisierte Inhalte des Internetauftritts kann sich jeder per RSS-Feed informieren lassen.

Darüber hinaus ist es mir wichtig, auch Bevölkerungsgruppen zu erreichen, die meine Webseite normalerweise nicht besuchen. Daher werde ich meinen Informationsstand weiter nutzen, um Bürgerinnen und Bürger vor Ort zu informieren, sie darüber hinaus zu beraten und mit ihnen zu diskutieren. Im Berichtszeitraum war der Stand am 15. Oktober 2017 beim Tag der offenen Tür der Stadt Nürnberg.

Außerdem haben Angehörige meiner Dienststelle und ich erneut an zahlreichen Informations- und Diskussionsveranstaltungen als Referentinnen beziehungsweise Referenten teilgenommen und Vorlesungen oder Vorträge gehalten.

Meine Broschüren und Informationsmaterialien werden weiter rege bei mir bestellt und von meiner Webseite heruntergeladen.

Pressearbeit ist besonders wichtig, um die Öffentlichkeit zu informieren und datenschutzrechtliche Positionen darzustellen. Vor dem Hintergrund der Datenschutz-Grundverordnung waren deutlich mehr Presseanfragen zu beantworten und Interviews zu geben. Daneben habe ich eine Reihe von Pressemitteilungen herausgegeben und Hintergrundgespräche geführt. Außerdem machen Fake-News auch vor dem Thema Datenschutz nicht halt. Hier konnte ich auch in Zusammenarbeit mit Presse und Medien so manches „Gerücht" durch Tatsachen und zutreffende Bewertungen entkräften.

1.6 Schlussbemerkung

Die nachfolgenden Kapitel geben unter anderem einen Überblick über meine Beteiligung an Gesetzgebungsvorhaben und meine Datenschutzkontrolle der bayerischen öffentlichen Stellen im Berichtszeitraum 2017/2018.

2 Allgemeines Datenschutzrecht / Datenschutzreform 2018

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

Das Jahr 2018 stand aus Datenschutzsicht im Zeichen einer **weitreichenden Datenschutzreform**: Die bereits am 24. Mai 2016 in Kraft getretene **Datenschutz-Grundverordnung** gilt seit dem 25. Mai 2018 in der gesamten Europäischen Union (EU) – und damit auch im Freistaat Bayern – unmittelbar. Zudem war bis zum 6. Mai 2018 die Richtlinie (EU) 2016/680 (**Datenschutz-Richtlinie für Polizei und Strafjustiz**) in nationales Recht umzusetzen. Dieser neue europäische Rechtsrahmen hat es erfordert, das nationale Datenschutzrecht zu ändern und anzupassen. Dies betrifft sowohl das allgemeine Datenschutzrecht als auch (fach-) bereichsspezifische Datenschutzregelungen. Im Zuge dieser Anpassung wurde neben dem Bundesdatenschutzgesetz auch das **Bayerische Datenschutzgesetz** (BayDSG) neu gefasst (Bayerisches Datenschutzgesetz vom 15. Mai 2018, GVBl. S. 230, geändert durch § 6 des Gesetzes vom 18. Mai 2018, GVBl. S. 301).

In materiell-rechtlicher Hinsicht behält die Datenschutz-Grundverordnung viele aus dem nationalen Datenschutzrecht bekannten und vertrauten Vorgaben im Wesentlichen bei und entwickelt diese fort. Insoweit bringt sie also für die bayerischen öffentlichen – insbesondere staatlichen und kommunalen – Stellen keine grundlegenden Veränderungen mit sich. Allerdings birgt sie auch eine ganze Reihe neuer und abgewandelter institutioneller und organisatorischer Vorgaben, welche auch von den bayerischen öffentlichen Stellen zu beachten sind. Durch die Verzahnung von europäischen und nationalen Vorschriften ist zudem die **Regelungssystematik** des Datenschutzrechts deutlich **komplexer** geworden – insbesondere im öffentlichen Bereich. Während etwa das bisherige Bayerische Datenschutzgesetz grundsätzlich eine „Vollregelung“ des allgemeinen Datenschutzrechts für bayerische öffentliche Stellen enthielt, kann die Neufassung im Anwendungsbereich der Datenschutz-Grundverordnung nur ergänzende Bestimmungen treffen.

Im Bereich der bayerischen öffentlichen Verwaltung sind insbesondere die **staatlichen und kommunalen öffentlichen Stellen selbst** für die Umsetzung des neuen Datenschutzrechts **verantwortlich**. Dies ist eine bewältigbare, aber sicherlich anspruchsvolle Aufgabe.

Um die bayerischen öffentlichen Stellen bei ihrem Vollzug des neuen Datenschutzrechts zu unterstützen, habe ich im Berichtszeitraum ein **umfassendes Informationsangebot** erarbeitet und bereitgestellt:

— Am 26. Mai 2017 – also ein Jahr vor Geltungsbeginn der Datenschutz-Grundverordnung – habe ich meine Informationsreihe „Datenschutzreform 2018“ gestartet. Die einzelnen Veröffentlichungen in dieser Informationsreihe widmen sich jeweils ausgewählten Themen des neuen Daten-

schutzrechts. Sie sind im Internet unter https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018“ abrufbar und können darüber hinaus bequem mittels eines RSS-Feeds bezogen werden.

— Neben Überblicksbeiträgen, die sich mit Inhalt und Systematik der Datenschutz-Grundverordnung und des neu gefassten Bayerischen Datenschutzgesetzes befassen, sind mittlerweile insbesondere mehrere, teils umfangreiche Praxis- und Orientierungshilfen erschienen. Diese haben unter anderem den behördlichen Datenschutzbeauftragten, die Informationspflichten, die Datenschutz-Folgenabschätzung und die Auftragsverarbeitung zum Thema. Die Orientierungs- und Praxishilfen vermitteln dabei den jeweiligen rechtlichen Hintergrund und geben praxisnahe Hinweise zur Umsetzung datenschutzrechtlicher Anforderungen. Soweit erforderlich, werden die Orientierungs- und Praxishilfen zu gegebener Zeit aktualisiert.

— Im Juni 2018 habe ich zudem mit der Veröffentlichung von „Aktuellen Kurz-Informationen“ begonnen. Diese behandeln kurz und prägnant jeweils spezifische Fragestellungen, meist solche, die in meiner täglichen Beratungspraxis häufig an mich herangetragen wurden. Bis Ende des Jahres 2018 sind bereits 16 solcher „Aktuellen Kurz-Informationen“ erschienen.

— Um die bayerischen öffentlichen Stellen bei der Durchführung einer Datenschutz-Folgenabschätzung zu unterstützen, stelle ich auf meiner Internetseite unter der Rubrik „Datenschutzreform 2018“ zudem eine von der französischen Datenschutz-Aufsichtsbehörde entwickelte Software in deutscher Sprache zur Verfügung. Die Software (das „PIA-Tool“) ermöglicht es, eine vollständige Datenschutz-Folgenabschätzung (im Englischen: Privacy Impact Assessment – PIA) durchzuführen. Die Software kann frei verwendet und weiterentwickelt werden (GPL v3.0) und ist für Windows, Linux und für Mac OS als eigenständiges Programm sowie auch als Web-Anwendung verfügbar.

Mein Informationsangebot hat nicht nur bei den bayerischen öffentlichen Stellen, sondern auch, wie mir zahlreiche Reaktionen zeigen, darüber hinaus **breiten Anklang** gefunden. Auch zukünftig werde ich dieses Informationsangebot erweitern.

2.2 Versand von Newslettern durch bayerische öffentliche Stellen

Oftmals nutzen bayerische öffentliche Stellen für die Kommunikation mit Bürgerinnen und Bürgern das Instrument „Newsletter“. Das Einsatzspektrum reicht vom behördlichen Presseverteiler bis zu aktuellen Kundeninformationen durch gemeindliche Tourismusbüros. Newsletter werden gegenwärtig meist kostengünstig per E-Mail verbreitet. Dabei werden personenbezogene Daten der Adressatinnen und Adressaten verwendet. Insbesondere werden E-Mail-Adressen gespeichert und durch die Übermittlung des jeweiligen Newsletters genutzt. Doch können die Datensätze in der entsprechenden Versandliste, häufig in Form einer Excel-Tabelle, auch weitere Angaben enthalten, etwa für eine individuelle Anrede oder für eine Selektion nach gruppenspezifischen Interessenlagen.

2.2.1 Erforderlichkeit einer Rechtsgrundlage

Für die Verarbeitung der Kontaktdaten von Adressatinnen und Adressaten des Newsletters ist eine Rechtsgrundlage erforderlich (Art. 6 Abs. 1 DSGVO). Dafür kommen grundsätzlich nur Einwilligungen der betroffenen Personen in Betracht (Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO). Eine bayerische öffentliche Stelle kann Newsletter also regelmäßig nur versenden, soweit sie über wirksame Einwilligungen der Adressatinnen und Adressaten verfügt.

2.2.2 Einwilligung als Rechtsgrundlage

Die Einwilligung ist wirksam, wenn sie die Anforderungen erfüllt, welche Art. 4 Nr. 11, Art. 6 Abs. 1 UAbs. 1 Buchst. a und Art. 7 Abs. 2 und 3 DSGVO vorsehen. Über diese Anforderungen informiert die Praxishilfe „Die Einwilligung nach der Datenschutz-Grundverordnung", die im Internet auf der Seite https://www.datenschutz-bayern.de unter „Datenschutzreform 2018 – Orientierungs- und Praxishilfen" veröffentlicht ist. Die Einwilligung muss danach insbesondere freiwillig (Art. 4 Nr. 11 DSGVO), informiert (Art. 4 Nr. 11 DSGVO), auf einen bestimmten Zweck (Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO) und auf eine bestimmte Verarbeitung bezogen (Art. 4 Nr. 11 DSGVO) sowie unmissverständlich (Art. 4 Nr. 11 DSGVO) sein. Sie wirkt grundsätzlich bis zu ihrem Widerruf (Art. 7 Abs. 3 Satz 1, 2 DSGVO).

2.2.3 Nachweispflicht

Die öffentliche Stelle muss die Einwilligung im Rahmen ihrer Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) nachweisen können (Art. 7 Abs. 1 DSGVO). Zu empfehlen ist insofern die Nutzung eines sogenannten Double-Opt-in-Verfahrens. Dabei meldet sich eine interessierte Person zunächst – regelmäßig – per Webformular mit einer E-Mail-Adresse für den Bezug des Newsletters an. An diese E-Mail-Adresse sendet der Anbieter eine Kontrollmitteilung, in der um Bestätigung des Bezugswunsches gebeten wird. Erst wenn diese Bestätigung – etwa über eine entsprechende Schaltfläche – erteilt ist, wird die interessierte Person in die Verteilerliste aufgenommen. Auf diese Weise ist ausgeschlossen, dass der Newsletter unerwünscht „zu Lasten" eines Dritten abonniert wird.

2.2.4 Bestandsdaten

Bereits vorhandene Datensätze von Adressatinnen und Adressaten können nur dann weiter für den Versand von Newslettern genutzt werden, wenn der Verantwortliche für diese Datensätze über Einwilligungen verfügt. Einwilligungen, die auf der Grundlage des bisherigen Rechts eingeholt wurden, sind unter der Geltung des neuen Rechts allerdings nur dann weiter wirksam, wenn sie auch dessen Voraussetzungen erfüllen (vgl. Erwägungsgrund 171 DSGVO). Das wird häufig nicht der Fall sein. Dann sollte der Verantwortliche eine neue Einwilligung einholen, welche Art. 4 Nr. 11, Art. 6 Abs. 1 UAbs. 1 Buchst. a und Art. 7 Abs. 2 und 3 DSGVO voll entspricht.

Die Nutzung vorhandener Datensätze für die Abfrage, ob eine solche Einwilligung erteilt wird, ist aus aufsichtsbehördlicher Sicht auch nach dem 25. Mai 2018 zulässig. Dies gilt jedenfalls dann, wenn die Abfrage alsbald erfolgt und nicht mit der Zusendung des nächsten Newsletters verbunden ist.

Da eine Einwilligung nur Wirksamkeit entfaltet, wenn sie freiwillig erteilt ist, sollte besonders darauf geachtet werden, dass die freie Willensentschließung der betroffenen Person nicht beeinträchtigt wird. Daher ist die Verknüpfung der Einwilligung mit der Teilnahme an einem Gewinnspiel ebenso unzulässig wie jede andere „Belohnung", wobei der Empfang des Newsletters nicht als eine solche anzusehen ist. Zumindest problematisch sind E-Mails an Bestandskundinnen und Bestandskunden, in denen die Einwilligung als eine Art „moralische Verpflichtung" und ihre Verweigerung als „Treuebruch" dargestellt wird.

2.2.5 Verzeichnis der Verarbeitungstätigkeiten

Eine Verarbeitungstätigkeit mit dem Zweck „Versand eines Newsletters" ist auch in das Verzeichnis der Verarbeitungstätigkeiten aufzunehmen. Rechtsgrundlage für diese Verarbeitungstätigkeit ist Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO. Eine aufgabenzuweisende Vorschrift kann mitzitiert werden, so etwa beim Newsletter einer gemeindlichen Volkshochschule Art. 57 Abs. 1 Satz 1 Gemeindeordnung (Aufgabe, Einrichtungen der Erwachsenenbildung zu betreiben).

Betroffene Personen sind die Abonnentinnen und Abonnenten; zu den Kategorien personenbezogener Daten zählen regelmäßig der Name und der Vorname sowie die E-Mail-Adresse, gegebenenfalls noch weitere Angaben (zum Beispiel das Geburtsdatum). Kategorien von (dritten) Empfängern können beispielsweise dann anzugeben sein, wenn die öffentliche Stelle für den Versand des Newsletters mit einem Auftragsverarbeiter kooperiert (vgl. Art. 28 DSGVO, näher dazu die Orientierungshilfe „Auftragsverarbeitung", die im Internet auf der Seite https://www.datenschutz-bayern.de unter „Datenschutzreform 2018 – Orientierungs- und Praxishilfen" veröffentlicht ist). Was die Löschfristen betrifft, ist im Verzeichnis der Verarbeitungstätigkeiten darauf hinzuweisen, dass der Datensatz einer Bezieherin oder eines Beziehers gelöscht wird, wenn sie oder er die Einwilligung widerruft. Im Übrigen ist der Bezug eines Newsletters in der Regel auf Dauer angelegt.

2.2.6 Informationspflichten

Im Zusammenhang mit dem Angebot, den Newsletter zu abonnieren, muss die öffentliche Stelle auch ihre Informationspflichten nach Art. 13 DSGVO erfüllen. Wird ein Webformular verwendet, sollten Interessentinnen und Interessenten vor Abgabe der Erklärung, dass der Newsletter bezogen werden soll, und vor Erteilung der Einwilligung in eine Verarbeitung der hierfür erforderlichen personenbezogenen Daten die Möglichkeit haben, die Hinweise zu den in Art. 13 Abs. 1 und 2 DSGVO aufgeführten Punkten medienbruchfrei zur Kenntnis zu nehmen. Dies kann etwa durch einen gut sichtbar platzierten und entsprechend bezeichneten Link geschehen. Vor der Einwilligung ist zudem unmissverständlich über das Widerrufsrecht aufzuklären (Art. 7 Abs. 3 Satz 2 DSGVO).

2.2.7 Sonderfall: Werbung per Newsletter

Will eine Behörde einen Newsletter zur Direktwerbung nutzen, beispielsweise eine gemeindliche Volkshochschule hinsichtlich ihres Kursangebots, kann sie dies nicht auf Art. 6 Abs. 1 UAbs. 1 Buchst. f mit Erwägungsgrund 47 DSGVO stützen.

Die Vorschrift ist für Behörden nicht anwendbar (Art. 6 Abs. 1 UAbs. 2 DSGVO), weil andernfalls Vorgaben zur Gesetzesbindung überspielt werden könnten.

Für öffentliche Stellen, die keine Behörden sind, so etwa Stadtwerke in der Rechtsform einer Kapitalgesellschaft, ist die Vorschrift allerdings nicht gesperrt. Insofern ist aber derzeit § 7 Gesetz gegen den unlauteren Wettbewerb zu beachten (künftig möglicherweise Art. 16 Abs. 2 Verordnung über Privatsphäre und elektronische Kommunikation, Entwurf dazu im Internet unter http://eur-lex.europa.eu, CELEX-Nr. 52017PC0010).

2.3 Aufbewahren von Einwilligungen

Die Einwilligung der betroffenen Person ist eine wichtige Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Das Gesetz nennt sie sogar an erster Stelle (Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO). Auch wenn bayerische öffentliche Stellen personenbezogene Daten oftmals auf der Grundlage von gesetzlich geregelten Befugnissen verarbeiten können (Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO) und daher insoweit keine Einwilligung benötigen, kommen auch bei ihnen einwilligungsbasierte Verarbeitungen vor. Das ist beispielsweise beim Versand von Newslettern der Fall (siehe dazu Beitrag Nr. 2.2 dieses Tätigkeitsberichts). Hat eine öffentliche Stelle eine Einwilligung für die Verarbeitung personenbezogener Daten eingeholt, stellt sich die Frage, wie lange diese Einwilligung aufgehoben werden muss.

2.3.1 Ausgangspunkt: Rechenschaftspflicht

Ausgangspunkt bei der Beantwortung dieser Frage ist die Rechenschaftspflicht, die Art. 5 Abs. 2 DSGVO dem Verantwortlichen – und damit der öffentlichen Stelle – auferlegt:

„Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können (‚Rechenschaftspflicht').“

Diese allgemeine Pflicht hat der Gesetzgeber in Bezug auf Einwilligungen durch Art. 7 Abs. 1 DSGVO zu einer spezifischen Nachweispflicht verdichtet. Die Bestimmung lautet:

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

Eine Aufbewahrungsfrist ist für die Einwilligung nicht geregelt. Sie muss daher im Einzelfall anhand des Erforderlichkeitskriteriums bemessen werden.

2.3.2 Verarbeitungen im Zusammenhang mit einer Einwilligung

Die Einwilligung ist Rechtsgrundlage für diejenige Verarbeitung, auf die sie sich bezieht. Das ist Regelungsgehalt von Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO. Hat die öffentliche Stelle beispielsweise eine Einwilligung für den Versand eines Newsletters eingeholt, so wird die Einwilligung – ihre Wirksamkeit vorausgesetzt – insbesondere die Speicherung und Nutzung des Datensatzes zulassen, den der

einwilligende Bezieher des Newsletters dem Verantwortlichen zur Verfügung gestellt hat.

Die Einwilligung enthält aber auch selbst Daten der betroffenen Person, insbesondere die Angabe ihrer Identität sowie die mit dieser verbundene Aussage: „Ich bin mit einer näher bezeichneten Verarbeitung meiner näher bezeichneten Daten einverstanden“. Diese personenbezogenen Daten werden durch den Verantwortlichen freilich nach Art. 6 Abs. 1 UAbs. 1 Buchst. c, Abs. 3 UAbs. 1 Buchst. a DSGVO verarbeitet. Die vom Verantwortlichen zu erfüllende gesetzliche Verpflichtung ist hier die Nachweispflicht aus Art. 7 Abs. 1 DSGVO.

2.3.3 Umfang der Nachweispflicht

Eine bayerische öffentliche Stelle muss in der Lage sein, die Nachweispflicht aus Art. 7 Abs. 1 DSGVO jedenfalls so lange zu erfüllen, wie noch Verarbeitungen stattfinden, die von der Einwilligung gedeckt sein sollen. Eine Einwilligung kann sich auf einen längeren Zeitraum beziehen, in dem eine andauernde Verarbeitung (etwa eine Speicherung von personenbezogenen Daten) oder wiederkehrende Verarbeitungen stattfinden, so beim Versand von Newslettern.

Bei der Formulierung eines Einwilligungsformulars sollte daher immer darauf geachtet werden, dass die entsprechende Erklärung alle geplanten Verarbeitungen erfasst. Stellt sich heraus, dass der Text insofern unzureichend ist, dürfen nicht berücksichtigte Verarbeitungen nur durchgeführt werden, wenn eine ergänzende Einwilligung eingeholt wird oder eine andere Rechtsgrundlage zur Verfügung steht.

2.3.4 Widerruf der Einwilligung

Ein Widerruf der Einwilligung führt nicht zwingend zu deren sofortiger Löschung: Mit der Verarbeitung der Einwilligung selbst wird nämlich die Nachweispflicht aus Art. 7 Abs. 1 DSGVO erfüllt; diese Verarbeitung beruht aber gerade nicht auf der Einwilligung, über die Nachweis zu führen ist (siehe oben unter 2.3.3). Daher kann die betroffene Person die Herausgabe einer schriftlichen Einwilligung oder einen entsprechenden Löschungsnachweis bei einer elektronisch erteilten Einwilligung nicht verlangen. Allerdings muss der Verantwortliche im Rahmen seiner allgemeinen Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) den Widerruf der betroffenen Person dokumentieren. Eine widerrufene Einwilligung kann er selbstverständlich auch nicht mehr dazu verwenden, zeitlich nachgelagerte Verarbeitungen zu legitimieren.

2.3.5 Fazit

Verarbeiten bayerische öffentliche Stellen personenbezogene Daten auf der Grundlage von Einwilligungen, sollten sie das „Verarbeitungsprogramm“ vorausschauend planen, Einwilligungsformulare entsprechend gestalten und auch von vornherein festlegen, wo, auf welche Weise und für welche Dauer die erteilten Einwilligungen aufgehoben werden müssen. Nach Maßgabe dieser Planung sollten sie entscheiden, welche Ressourcen sie für die Erfüllung der gesetzlichen Rechenschafts- und Nachweispflichten einzusetzen haben.

2.4 Keine gesonderte Entgeltpflicht für Kontrollen bei der Auftragsverarbeitung

Die Datenschutzreform 2018 veranlasst zahlreiche Auftragsverarbeiter, ihre Geschäftsbedingungen neu zu fassen sowie auf Anpassungen in den mit ihren Auftraggebern vereinbarten Regelungen hinzuwirken. Bayerische öffentliche Stellen wurden von Auftragsverarbeitern in diesem Zusammenhang unter anderem mit dem Ansinnen konfrontiert, einer Vertragsklausel zuzustimmen, die dem Auftraggeber eine Vor-Ort-Kontrolle nur gegen ein besonderes Entgelt ermöglicht. In datenschutzrechtlicher Hinsicht kann ich dazu folgende Hinweise geben:

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

Bei der Auftragsverarbeitung verbleibt der Verantwortliche grundsätzlich in dieser Stellung (vgl. Art. 4 Nr. 8 DSGVO); er ist umfassend weisungsberechtigt (vgl. Art. 28 Abs. 3 Satz 2 Buchst. a DSGVO), entscheidet allein über den Zweck der Verarbeitung und hat auch dafür einzustehen, dass diese von einer Rechtsgrundlage gedeckt ist. Die Auftragsverarbeitung ist gerade kein datenschutzrechtliches „Rundum-sorglos-Paket".

Vor diesem Hintergrund sieht Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO Kontrollrechte vor, die ohne besondere Begründung seitens des Verantwortlichen als Auftraggeber und ohne Abwehrmöglichkeit seitens des Auftragsverarbeiters (Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO: „und dazu beiträgt") auszuüben sein müssen. Andernfalls könnte der Verantwortliche nämlich seinen bei ihm auch nach Einbindung eines Auftragsverarbeiters verbleibenden Pflichten insbesondere gegenüber den betroffenen Personen nicht angemessen nachkommen.

Daher darf die Wahrnehmung der Kontrollrechte des Auftraggebers aus datenschutzrechtlicher Sicht nicht von einem besonderen Entgelt abhängig gemacht werden. Dies gilt gerade auch für Vor-Ort-Kontrollen beim Auftragsverarbeiter. Ein gesondertes Entgelt würde einer Ausübung der Kontrollrechte entgegenwirken. Die Vereinbarung eines Entgelts, einer Aufwandsentschädigung oder eines sonstigen Kostenbeitrags, auch die Vereinbarung, hierzu im Bedarfsfall nachträglich eine die Auftragsverarbeitungs-Vereinbarung ergänzende Regelung zu treffen, führt dazu, dass eine Inspektion beim Auftragsverarbeiter als etwas „Außergewöhnliches" wahrgenommen wird, das dem Auftraggeber „eigentlich" nicht zusteht und gerade deshalb außerhalb der wechselseitigen Austauschbeziehung zu vergüten ist. Davon abgesehen kann ein solches Entgelt entweder auf Grund seiner bereits erkennbaren (absoluten) Höhe oder der vertraglich angelegten Unklarheit seiner Berechnung abschreckende Wirkung entfalten.

Dem berechtigten Interesse des Auftragsverarbeiters, nicht von seinen Auftraggebern „überrannt" zu werden, ist dadurch Rechnung getragen, dass jede Partei einer Auftragsverarbeitungs-Vereinbarung nach Treu und Glauben zur Rücksichtnahme auf die jeweils andere Partei verpflichtet ist. Diese Verpflichtung kann in der Vereinbarung durchaus näher ausgestaltet werden. In Betracht kommen etwa Bestimmungen, dass eine Vor-Ort-Kontrolle grundsätzlich mit einer bestimmten

Frist anzukündigen oder abzustimmen ist, oder dass anlasslose Inspektionen mengenmäßig kontingentiert sind.

Unbenommen bleibt dem Auftragsverarbeiter selbstverständlich auch, die ihm durch Vor-Ort-Kontrollen seines Auftraggebers entstehenden Kosten von vornherein pauschal in das Angebot der vertraglichen Leistung einzurechnen („Einpreisung"). Dabei ist zu berücksichtigen, dass der Auftraggeber auf die von der Datenschutz-Grundverordnung als Regelungsgegenstände einer Auftragsverarbeitungs-Vereinbarung obligatorisch vorgesehenen Kontrollrechte nicht verzichten kann.

Bayerische öffentliche Stellen sollten bei der Prüfung von neuen Auftragsverarbeitungs-Bedingungen sowie bei Verhandlungen über Anpassungen in bestehenden Vertragsbeziehungen stets darauf achten, dass sie sich für die Ausübung ihrer gesetzlichen Kontrollrechte nicht zu einem besonderen Entgelt verpflichten lassen.

2.5 Datenschutzbeauftragte bei bayerischen öffentlichen Stellen im Wettbewerb

Die Pflicht, einen Datenschutzbeauftragten zu benennen, trifft jede bayerische öffentliche Stelle. Gleichwohl haben mich bereits mehrere Anfragen solcher Stellen erreicht, die als Unternehmen am Wettbewerb teilnehmen und deshalb so behandelt werden möchten wie ihre privaten Konkurrenten. Für diese gilt unter anderem § 38 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG):

„Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 [das ist die Datenschutz-Grundverordnung] benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen."

Diese „Zehn-Personen-Regel" ist auf bayerische öffentliche Stellen nicht anwendbar. Soweit öffentliche Stellen als Unternehmen am Wettbewerb teilnehmen, gelten zwar nach Art. 1 Abs. 3 Satz 1 BayDSG für sie selbst, ihre Zusammenschlüsse und Verbände die Vorschriften für nicht öffentliche Stellen. Zu diesen Vorschriften gehört auch § 38 Abs. 1 Satz 1 BDSG. Die Datenschutz-Grundverordnung bestimmt allerdings in Art. 37 Abs. 1 Buchst. a DSGVO:

„Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird […]."

§ 38 Abs. 1 Satz 1 BDSG ergänzt ausdrücklich die in Art. 37 Abs. 1 Buchst. b und c DSGVO geregelten Benennungstatbestände, die an die Qualität sowie die Quantität der Verarbeitungen bei dem betreffenden Verantwortlichen anknüpfen. § 38 Abs. 1 Satz 1 BDSG ist jedoch nicht zugleich als Einschränkung von Art. 37 Abs. 1 Buchst. a DSGVO konzipiert. Mit der Formulierung „Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679" hat der Bundesgesetzgeber gerade auf den Anwendungsvorrang des Unionsrechts reagiert.

Es bleibt also dabei: Jede bayerische öffentliche Stelle muss einen Datenschutzbeauftragten haben. Rechtsträger mit nur wenigen oder gar keinen eigenen Beschäftigten können von der Möglichkeit Gebrauch machen, eine externe Person zu benennen. Dies darf auch ein Bediensteter einer anderen öffentlichen Stelle sein, mit der eine entsprechende Vereinbarung (Art. 37 Abs. 6 DSGVO: „Dienstleistungsvertrag“) geschlossen werden kann.

2.6 Geldbußen nach Art. 83 Datenschutz-Grundverordnung gegen bayerische öffentliche Stellen

Mit der Datenschutzreform 2018 haben die Datenschutz-Aufsichtsbehörden zahlreiche neue Befugnisse gewonnen. So können bestimmte Verstöße gegen Vorschriften der Datenschutz-Grundverordnung mit Geldbußen geahndet werden. Soweit allerdings „Behörden und öffentliche Stellen“ betroffen sind, dürfen die Mitgliedstaaten nach Art. 83 Abs. 7 DSGVO festlegen, ob und in welchem Umfang Geldbußen verhängt werden können. Von dieser Möglichkeit hat der bayerische Gesetzgeber mit Art. 22 BayDSG Gebrauch gemacht. Dort heißt es:

„Gegen öffentliche Stellen im Sinne des Art. 1 Abs. 1 und 2 [BayDSG] dürfen Geldbußen nach Art. 83 DSGVO nur verhängt werden, soweit diese als Unternehmen am Wettbewerb teilnehmen.“

2.6.1 Geldbuße als Regelfall

Ob Regelungen wie in Art. 22 BayDSG der Datenschutz-Aufsichtsbehörde eine ansonsten nicht bestehende Sanktionsbefugnis verschaffen oder aber eine ansonsten bestehende Sanktionsbefugnis begrenzen, hängt vom Verständnis des Art. 83 Abs. 7 DSGVO ab. Die Vorschrift wird teils als Ermächtigung gewertet, Sanktionen gegen Behörden und öffentliche Stellen zuzulassen. Teils wird sie aber auch als Ermächtigung angesehen, Behörden und öffentliche Stellen von Sanktionen freizustellen.

Systematisch ist Letzteres besser begründbar: Der zentrale Geldbußtatbestand in Art. 83 Abs. 4 Buchst. a DSGVO ist unmittelbar an Verantwortliche und Auftragsverarbeiter adressiert. Weitere Geldbußtatbestände erhalten diese Adressierung mittelbar durch Verweise auf Verhaltensnormen (vgl. Art. 83 Abs. 5 DSGVO). Wenn die Datenschutz-Grundverordnung aber von Verantwortlichen und Auftragsverarbeitern spricht, sind grundsätzlich auch Behörden und öffentliche Stellen gemeint (vgl. Art. 37 Abs. 3 DSGVO). Sollen sie ausgenommen sein, ist dies besonders angeordnet (vgl. etwa Art. 27 Abs. 2 Buchst. b DSGVO).

In der Sache regelt Art. 22 BayDSG daher einen Anwendungsausschluss der Vorschriften zu Geldbußen, und zwar, soweit eine öffentliche Stelle im Sinne von Art. 1 Abs. 1 und 2 BayDSG nicht als Unternehmen am Wettbewerb teilnimmt.

Im vorliegenden Zusammenhang sind in den Datenschutzgesetzen anderer Bundesländer sowie anderer Mitgliedstaaten der Europäischen Union übrigens auch positiv formulierte Anwendungsausschlüsse vorzufinden (so etwa in § 43 Abs. 3 Bundesdatenschutzgesetz, § 28 Landesdatenschutzgesetz [Baden-Württemberg] oder § 30 Abs. 5 Datenschutzgesetz [Österreich]).

2.6.2 Teilnahme am Wettbewerb als Unternehmen

Bei der Anwendung von Art. 22 BayDSG ist zu prüfen, ob eine bayerische öffentliche Stelle als Unternehmen am Wettbewerb teilnimmt. Da Art. 22 BayDSG die Reichweite der in Art. 83 DSGVO geregelten Geldbußtatbestände betrifft, ist insofern Unionsrecht maßgeblich.

Erwägungsgrund 150 Satz 3 DSGVO weist darauf hin, dass bei der Verhängung einer Geldbuße gegenüber einem Unternehmen der entsprechende Begriff in Art. 101 f. Vertrag über die Arbeitsweise der Europäischen Union (AEUV) zu beachten ist. Es liegt nahe, diesen – Art. 4 Nr. 18 DSGVO jedenfalls bei der Abgrenzung zum hoheitlichen Bereich konkretisierenden – Begriff auch dann heranzuziehen, wenn der nationale Gesetzgeber die Ermächtigung in Art. 83 Abs. 7 DSGVO dazu nutzt, eine Ausnahme von einem Anwendungsausschluss (unter anderem) an die Eigenschaft als Unternehmen anzuknüpfen.

Die Bestimmungen in Art. 101 f. AEUV richten sich an Unternehmen unabhängig von ihrer Rechtsform. Ausgenommen sind dabei hoheitliche Betätigungen. Der Europäische Gerichtshof hat insofern ausgeführt (Urteil vom 12. Juli 2012, C-138/11, Rn. 35 ff.):

„Nach ständiger Rechtsprechung [des Gerichtshofs] ist eine wirtschaftliche Tätigkeit jede Tätigkeit, die darin besteht, Güter oder Dienstleistungen auf einem bestimmten Markt anzubieten […]. Somit können der Staat selbst oder eine staatliche Einheit als Unternehmen tätig sein […].
Dagegen haben Tätigkeiten, die in Ausübung hoheitlicher Befugnisse erfolgen, keinen wirtschaftlichen Charakter, der die Anwendung der im [Vertrag über die Arbeitsweise der Europäischen Union] vorgesehenen Wettbewerbsregeln rechtfertigen würde […].
Soweit eine öffentliche Einheit […] eine wirtschaftliche Tätigkeit ausübt, die von der Ausübung ihrer hoheitlichen Befugnisse losgelöst werden kann, handelt sie in Bezug auf diese Tätigkeit als Unternehmen; ist die wirtschaftliche Tätigkeit dagegen mit der Ausübung ihrer hoheitlichen Befugnisse untrennbar verbunden, bleiben sämtliche Tätigkeiten dieser Einheit Tätigkeiten in Ausübung hoheitlicher Befugnisse […].
Darüber hinaus reicht der Umstand, dass die öffentliche Einheit […] eine Dienstleistung, die mit der Ausübung ihrer hoheitlichen Befugnisse in Zusammenhang [steht], gegen ein gesetzlich vorgesehenes und nicht unmittelbar oder mittelbar von ihr bestimmtes Entgelt […] erbringt, für sich genommen nicht aus, um die ausgeübte Tätigkeit als wirtschaftliche Tätigkeit und die Einheit, die sie ausübt, als Unternehmen einzustufen […].“

Der Gerichtshof unterscheidet danach eine Sphäre wirtschaftlicher Betätigung von einer Sphäre der Ausübung hoheitlicher Befugnisse. Die beiden Sphären sind regelmäßig getrennt; ist die Trennung im Einzelfall nicht durchführbar, finden die für Unternehmen geltenden Wettbewerbsregeln grundsätzlich keine Anwendung.

Eine Ausübung hoheitlicher Befugnisse ist regelmäßig nicht bereits dadurch belegt, dass die betreffende Stelle eine ihr zugewiesene öffentliche (auch: Pflicht-) Aufgabe wahrnimmt, dass sie auf dem einschlägigen Markt in einer faktischen oder auch rechtlich (etwa durch gebietsbezogenen Benutzungszwang) verfestigten Monopolposition agiert, oder dass sie ein ihr zu zahlendes Entgelt (auch) durch Leistungsbescheid erheben kann (vgl. näher Gericht der Europäischen Union, Urteil vom 16. Juli 2014, T-309/12, Rn. 58 ff.).

Die Ausübung hoheitlicher Tätigkeiten kann typischerweise nicht ohne weiteres auf Private übertragen werden; sie bringt Vorrechte zur Geltung, die grundsätzlich nur dem Staat zustehen, während sich eine wirtschaftliche Betätigung häufig in einem (mindestens) kostendeckenden Entgelt zu erkennen gibt.

2.6.3 Folgen für bayerische öffentliche Stellen

Kommt in einem Einzelfall die Verhängung einer Geldbuße in Betracht, ist anhand eines unionsrechtlichen Maßstabs zu prüfen, ob die betreffende bayerische öffentliche Stelle hinsichtlich des konkreten Tätigkeitsfelds (Art. 22 BayDSG: „soweit") als Unternehmen am Wettbewerb teilnimmt.

War eine öffentliche Stelle nach dem bisherigen Datenschutzrecht (insbesondere nach Art. 3 Abs. 1 Satz 1 BayDSG-alt) nicht als Wettbewerbsunternehmen anzusehen, bedeutet dies somit nicht in jedem Fall, dass sie auch umfassend von dem Anwendungsausschluss profitieren kann, den Art. 22 BayDSG hinsichtlich der Ahndungsmöglichkeiten nach Art. 83 DSGVO bewirkt.

3 Informations- und Kommunikationstechnik und Organisation

3.1 Grundsatzthemen

3.1.1 Die Datenschutz-Grundverordnung aus technisch-organisatorischer Sicht

Bisher waren die rechtlichen Vorgaben zu den technischen und organisatorischen Maßnahmen, die für bayerische öffentliche Stellen relevant sind, insbesondere in Art. 7 BayDSG-alt geregelt. Seit der Datenschutzreform 2018 sind maßgebliche Regelungen in der Datenschutz-Grundverordnung enthalten.

Art. 24 Abs. 1 Satz 1 und Art. 32 Abs. 1 Halbsatz 1 DSGVO begründen Pflichten des Verantwortlichen, technische und organisatorische Maßnahmen zu treffen, damit Verarbeitungen personenbezogener Daten mit den Vorgaben der Datenschutz-Grundverordnung in Einklang stehen und ein ausreichendes Niveau von Schutz gegenüber Risiken für die Rechte und Freiheiten natürlicher Personen gewährleistet ist.

Diese technischen und organisatorischen Maßnahmen folgen nicht mehr den aus Art. 7 Abs. 2 BayDSG-alt bekannten „10 Geboten“ sondern umfassen nun insbesondere die folgenden Punkte:

- Vertraulichkeit,
- Integrität,
- Verfügbarkeit,
- Belastbarkeit,
- Wiederherstellbarkeit,
- Data protection by design/Datenschutz durch Technikgestaltung,
- Data protection by default/datenschutzfreundliche Voreinstellungen,
- Pseudonymisierung, Verschlüsselung.

Einige dieser Aspekte waren bereits in Art. 7 Abs. 2 BayDSG-alt zu finden und stellen daher keine neuen Anforderungen. Die Vorgaben zum Datenschutz durch Technikgestaltung sowie durch datenschutzfreundliche Voreinstellungen wirken nun darauf hin, dass Fragen des Datenschutzes bereits bei der Konzeption und Einführung von Verfahren und der Auswahl von Produkten – also auch bei Vergabeentscheidungen – berücksichtigt werden.

Ausgangspunkt bei der „Bemessung“ der erforderlichen technischen und organisatorischen Maßnahmen muss immer eine Risikoanalyse sein, die in bestimmten Fällen in der neu eingeführten Form einer Datenschutz-Folgenabschätzung durchzuführen ist (näheres hierzu siehe Nr. 3.1.3)

In den Vordergrund rücken ferner die Anforderungen an die Dokumentation und – damit zusammenhängend – an die Nachweisbarkeit der getroffenen Maßnahmen (vgl. Art. 5 Abs. 2 DSGVO). Insofern kann die Nutzung eines Datenschutzmanagementsystems von Nutzen sein (siehe Nr. 3.1.2).

3.1.2 Datenschutzmanagement in bayerischen öffentlichen Krankenhäusern

Die Datenschutz-Grundverordnung stellt im Vergleich mit dem bisherigen Recht erhöhte Anforderungen an die Rechenschafts- und Nachweispflicht des Verantwortlichen (siehe Art. 5 Abs. 2, Art. 24 Abs. 1 Satz 1 DSGVO). Diese Pflichten treffen auch bayerische öffentliche Krankenhäuser. Dem (behördlichen) Datenschutzbeauftragten eines Krankenhauses kommt in diesem Zusammenhang eine Beratungs- und Überwachungsaufgabe zu (vgl. Art. 39 Abs. 1 DSGVO).

Die Erfüllung der Nachweispflicht setzt insbesondere voraus, dass die Auswahl, Umsetzung und Wirksamkeitskontrolle von technischen und organisatorischen Maßnahmen (siehe vor allem Art. 24 Abs. 1 und 2, Art. 32 Abs. 1 DSGVO) dokumentiert werden; die Maßnahmen müssen in der Folge jederzeit umfassend und schnell – etwa im Rahmen einer Datenschutzprüfung – dargelegt werden können.

Die Datenschutz-Grundverordnung konkretisiert zudem weitere, bisher nur zurückhaltend geregelte Pflichten oder begründet diese neu, sodass auch im Bereich der Krankenhäuser eine eingehende Befassung mit dem Thema Datenschutz mehr denn je erforderlich ist. Zu nennen sind etwa die folgenden Pflichten:

— die Pflicht zur Meldung von Datenschutzverletzungen an die Datenschutz-Aufsichtsbehörde sowie zur Benachrichtigung betroffener Personen (Art. 33, 34 DSGVO). Diese Pflichten waren bisher auf Fälle mit drohenden schwerwiegenden Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen begrenzt. Die nun umfangreichere Meldepflicht erfordert festgelegte interne Strukturen und Regelungen zur Feststellung und Weitergabe von Datenschutzverletzungen, so dass diese grundsätzlich innerhalb der geforderten 72 Stunden an die Datenschutz-Aufsichtsbehörde gemeldet werden können (siehe Nr. 3.1.6).

— die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO). Diese Pflicht war bisher überhaupt nicht vorgesehen und erfordert eine strukturierte Vorgehensweise bei der Prüfung von Risiken und technischen Verfahren (siehe Nr. 3.1.3).

— Auch der Umgang mit Beschwerden oder Auskunftsersuchen von Bürgerinnen und Bürgern erfordert Regelungen zu Ansprechpersonen sowie Verfahrensweisen.

Insgesamt betrachtet erscheint es nach der Datenschutzreform 2018 umso mehr geboten, dass Krankenhäuser funktionsfähige Datenschutzmanagementsysteme aufbauen, die dabei helfen, knappe Ressourcen effektiv zu nutzen. Was die Implementierung eines solchen Datenschutzmanagementsystems betrifft, steht auf meiner Internetpräsenz https://www.datenschutz-bayern.de unter „Veröffentlichungen – Orientierungshilfen“ ein in Zusammenarbeit mit dem Bayerischen Landesamt für Datenschutzaufsicht entstandener Leitfaden „Anforderungen an das Datenschutzmanagement in bayerischen öffentlichen und privaten Krankenhäusern“ bereit.

3.1.3 Datenschutz-Folgenabschätzung

Was die Gefährdungsbeurteilung im Arbeitsschutz und die Risikoanalyse auf der Basis von IT-Grundschutz bei der IT-Sicherheit sind, ist die Folgenabschätzung im

Datenschutz. Alle drei Instrumente dienen in ihrem jeweiligen Anwendungsbereich der Risikobewertung und – falls notwendig – der anschließenden Risikoreduzierung durch technische und organisatorische Maßnahmen. Im Vergleich zur Gefährdungsbeurteilung und zur IT-Sicherheits-Risikoanalyse ist die Datenschutz-Folgenabschätzung zum einen ein relativ neues Instrument, das die Datenschutz-Grundverordnung in einem eigenen Abschnitt eingeführt hat. Zum anderen besteht im öffentlichen Bereich die Besonderheit, dass jede Verarbeitung personenbezogener Daten durch öffentliche Stellen zunächst einmal als Grundrechtseingriff zu werten ist, der im Einzelfall gerechtfertigt sein kann, wenn er auf einer Rechtsgrundlage beruht, insbesondere auf eine gesetzliche Verarbeitungsbefugnis zu stützen ist.

Mit Hilfe der Datenschutz-Folgenabschätzung sind Verarbeitungsvorgänge, die ein hohes Risiko für die persönlichen Rechte und Freiheiten betroffener Personen mit sich bringen, vor ihrem Beginn auf ihr mögliches Schadenspotenzial zu prüfen und zu bewerten. Ziel der Datenschutz-Folgenabschätzung ist es, auf Basis der gewonnenen Erkenntnisse geeignete technische und organisatorische Maßnahmen nachhaltig umzusetzen und damit die ermittelten Risiken auf ein vertretbares Maß zu reduzieren. Folglich ist eine dokumentierte Datenschutz-Folgenabschätzung besonders gut geeignet, den Nachweis zu erbringen, dass eine öffentliche Stelle gegenüber einer betroffenen Person die datenschutzrechtlichen Schutzstandards einhält.

Die notwendigen Vorarbeiten, die doch recht hohe Komplexität sowie die noch fehlende Standardisierung führen dazu, dass sich Datenschutz-Folgenabschätzungen bei den von mir betreuten Stellen überwiegend noch in der Erprobungsphase befinden. Dies ist Anlass, auf wichtige Aspekte der Datenschutz-Folgenabschätzung näher einzugehen:

— Grundsätzliche Fragen, wie etwa die Erforderlichkeit und die Durchführung einer Datenschutz-Folgenabschätzung, sind ausführlich in meiner Orientierungshilfe „Datenschutz-Folgenabschätzung“ erörtert und werden dort aktuell gehalten. Die Orientierungshilfe ist auf meiner Internetpräsenz https://www.datenschutz-bayern.de unter „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Datenschutz-Folgenabschätzung“ abrufbar.

— Art. 35 Abs. 4 DSGVO verpflichtet die Datenschutz-Aufsichtsbehörden, Listen von Verarbeitungsvorgängen zu erstellen und zu veröffentlichen, für die in jedem Fall eine Datenschutz-Folgenabschätzung erforderlich ist (sogenannte „Blacklist“). Diese Liste steht ebenfalls im Rahmen meiner Internetpräsenz bereit.

  Befindet sich die Verarbeitungstätigkeit einer öffentlichen Stelle auf der Blacklist, ist der Verantwortliche zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet. Die Beurteilung, ob die Verarbeitung „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ zur Folge hat, ist in diesen Fällen bereits durch mich als Aufsichtsbehörde erfolgt und wird dem Verantwortlichen insoweit abgenommen.

— Befindet sich eine Verarbeitungstätigkeit hingegen nicht auf der Blacklist, muss der Verantwortliche im nächsten Schritt eigenständig beurteilen, ob die Verarbeitung auf Grundlage einer eigenen Risikoabschätzung „voraus-

sichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ zur Folge hat. Meine Orientierungshilfe „Datenschutz-Folgenabschätzung“ enthält dazu ein Prüfungsschema.

— Für viele bayerische öffentliche Stellen von besonderem Interesse ist die Frage, wie eine Datenschutz-Folgenabschätzung konkret durchzuführen ist, wenn die Risikobeurteilung dies erforderlich macht. Zwar kann der Verantwortliche die Methode zur Erstellung einer Datenschutz-Folgenabschätzung frei wählen. Er muss aber gewährleisten, dass die gesetzlichen Mindestanforderungen erfüllt werden. Da eine Veranschaulichung am Beispiel hilfreich ist, habe ich die oben genannte Orientierungshilfe um eine Fallstudie ergänzt, die auch eine mögliche Methode für die Durchführung einer Datenschutz-Folgenabschätzung erläutert.

3.1.4 Externe behördliche Datenschutzbeauftragte

Öffentliche Stellen benennen meist eigene Beschäftigte als behördliche Datenschutzbeauftragte. Auf diese Weise kann regelmäßig am besten sichergestellt werden, dass die nötigen Kenntnisse im spezifischen Datenschutzrecht des öffentlichen Bereichs sowie die nötigen Erfahrungen mit der Aufbau- und Ablauforganisation von Behörden vorhanden sind. Gleichwohl können bei Wahrung der fachlichen Anforderungen auch für öffentliche Stellen externe Datenschutzbeauftragte benannt werden (vgl. Art. 37 Abs. 6 DSGVO).

Ein externer Datenschutzbeauftragter oder eine externe Datenschutzbeauftragte kann auf Grundlage eines **Dienstleistungsvertrags** benannt werden, der mit einer natürlichen oder juristischen Person außerhalb der öffentlichen Stelle geschlossen wird. Zu beachten ist allerdings, dass nur eine **natürliche Person** als Datenschutzbeauftragter oder Datenschutzbeauftragte benannt werden kann, da nur eine natürliche Person die personenbezogenen Anforderungen des Art. 37 Abs. 5 DSGVO erfüllen kann. Die Benennung einer juristischen Person als Datenschutzbeauftragte ist nicht möglich. Wird der Dienstleistungsvertrag mit einer juristischen Person geschlossen, ist daher ein Beschäftigter oder eine Beschäftigte dieser juristischen Person konkret als Datenschutzbeauftragter oder Datenschutzbeauftragte für die öffentliche Stelle zu benennen.

Bei der Benennung eines externen Datenschutzbeauftragten muss der Dienstleistungsvertrag so ausgestaltet sein, dass eine unabhängige Erfüllung der gesetzlichen Aufgaben insbesondere durch entsprechende Kündigungsfristen, Zahlungsmodalitäten, Haftungsfreistellungen und Dokumentationspflichten gewährleistet wird.

Die Datenschutz-Grundverordnung unterwirft auch externe Datenschutzbeauftragte Vertraulichkeitspflichten. Vor diesem Hintergrund können sich ihre **Kontrollrechte** auf personenbezogene Daten erstrecken, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis (§ 30 Abgabenordnung) unterliegen.

Auch externe Datenschutzbeauftragte müssen über die nach der Datenschutz-Grundverordnung erforderliche **Sachkunde und Zuverlässigkeit** verfügen. Dies muss vor der Benennung überprüft werden. Der Umfang der Sachkunde muss sich an der Schutzbedürftigkeit der vorhandenen personenbezogenen Daten orientieren. In einem gewissen Maß setzt Sachkunde auch voraus, dass der oder die

Datenschutzbeauftragte mit den typischen Verwaltungsabläufen der öffentlichen Stelle vertraut ist.

3.1.5 Formular zur Meldung des behördlichen Datenschutzbeauftragten

Nach Art. 37 Abs. 7 DSGVO muss ein Verantwortlicher die Kontaktdaten des Datenschutzbeauftragten der Datenschutz-Aufsichtsbehörde mitteilen.

Seit dem 1. März 2018 biete ich im Rahmen meiner Internetpräsenz für Meldungen behördlicher Datenschutzbeauftragter ein Online-Formular an, das im Internet auf https://www.datenschutz-bayern.de in der Rubrik „Online-Meldungen" aufgerufen werden kann. Die frühzeitige Verfügbarkeit dieses Online-Formulars hat wesentlich zu einer effizienten, papiersparenden Verarbeitung beigetragen. Bereits innerhalb der ersten Monate seit Verfügbarkeit der Option zur elektronischen Meldung haben mehrere tausend öffentliche Stellen das Formular genutzt. Mir wurden bis zu 425 Datensätze innerhalb eines Tages mitgeteilt.

Kommunale Behörden habe ich gebeten, behördliche Datenschutzbeauftragte über das BayernPortal (https://www.freistaat.bayern) zu veröffentlichen. Eine Veröffentlichung dort erfüllt zugleich die Mitteilungspflicht nach Art. 37 Abs. 7 DSGVO. Die Erfassung und Änderung der Informationen der oder des behördlichen Datenschutzbeauftragten im BayernPortal muss über das Redaktionssystem für Verwaltungsinformationen in Bayern durch die Redakteure der jeweiligen Behörde erfolgen. Jede kommunale Behörde, die Zugang zum Redaktionssystem hat, soll ihren behördlichen Datenschutzbeauftragten oder ihre behördliche Datenschutzbeauftragte als Ansprechperson aufnehmen und die zugehörigen Kontaktdaten einpflegen. Eine Anleitung hierfür steht im Redaktionssystem des BayernPortals unter „Weiterführende Informationen – Benutzerhandbücher und Anleitungen" zur Verfügung.

Eine Pflicht zur Mitteilung einer Vertreterin oder eines Vertreters des oder der behördlichen Datenschutzbeauftragten besteht im Übrigen nicht. Selbstverständlich muss aber jede Stelle eventuell nötige Vertretungen so regeln, dass die Aufgabenerfüllung jederzeit sichergestellt ist. Insbesondere bietet es sich auch an, eine Funktionsadresse wie beispielsweise datenschutz@... oder bdsb@... einzurichten, auf die der oder die Datenschutzbeauftragte und im Fall der Vertretung die dazu vorgesehene Person zugreifen können. Dieser E-Mail-Kontakt ist dann auch in die Meldung an mich aufzunehmen.

3.1.6 Meldungen von Verletzungen des Schutzes personenbezogener Daten

Seit dem 2. März 2018 steht auf meiner Internetpräsenz https://www.datenschutz-bayern.de in der Rubrik Online-Meldungen ein Formular zur Meldung von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DSGVO zur Verfügung. Das Formular setzt – ohne zusätzlichen Aufwand für die Meldenden – neben einer SSL-Transportverschlüsselung („https") eine zusätzliche Ende-zu-Ende-Verschlüsselung („pgp") ein, sodass Meldungen sicher und ohne Kenntnisnahme durch unbefugte Dritte vertraulich an mich gesendet werden können.

Innerhalb des Berichtzeitraums wurde das Online-Formular auf meiner Homepage bereits für eine beträchtliche Zahl an Meldungen genutzt. Viele der gemel-

deten Datenschutzverletzungen entstammten Bereichen, in denen sensible medizinische Daten oder Sozialdaten verarbeitet werden. Im Einzelnen ist zu bemerken:

— In zahlreichen gemeldeten Fälle gingen die Ausführenden unsachgemäß mit schutzwürdigen Daten um, so dass Unterlagen versehentlich an unberechtigte Empfänger oder Empfängerinnen übermittelt wurden. Die Ursache solcher „**Datenfehlübermittlungen**“ lag bei diesen Vorfällen in einer unzutreffenden Adressierung, Zusammenstellung oder Kuvertierung von Unterlagen, die jeweils manuell ausgeführt oder angestoßen wurde. So wurden beispielsweise an Patienten die Arztbriefe von anderen Patienten ausgehändigt oder übersandt.

— Zudem hat sich gezeigt, dass in vielen Fällen ein unsachgemäßer Versand per Telefax erfolgt. Die Meldungen zeigen deutlich, wie schnell durch **Falscheingabe einer Telefaxnummer** vertrauliche Unterlagen an unberechtigte Empfänger oder Empfängerinnen versendet werden. Mit der Fehleranfälligkeit von Telefax habe ich mich bereits in meinem 27. Tätigkeitsbericht 2016 unter Nr. 5.5.3 ausgiebig beschäftigt. Ebenso verweise ich auf die Orientierungshilfe „Datensicherheit beim Telefax-Dienst“, die das Thema ausführlich behandelt und auf meiner Homepage im Bereich „Themengebiete – Technik und Organisation“ abrufbar ist. Gerade für den Versand sensibler Daten wie Gesundheits- oder Sozialdaten sollte der Telefaxversand nur in Ausnahmefällen, und dann exakt und kontrolliert genutzt werden.

— In Bezug auf E-Mails wurde mir ebenfalls öfters angezeigt, dass versehentlich **E-Mails an falsche Adressaten oder Adressatinnen** versendet wurden. Häufig wurden dabei E-Mails, die eigentlich an interne Adressen geschickt werden sollten, an unbefugte Empfänger oder Empfängerinnen außerhalb der Behörde versandt. Dies führte in der Regel zu zwei Datenschutzverletzungen – einmal zum Versand an einen unberechtigten Empfänger oder eine unberechtigte Empfängerin und einmal zu einem unverschlüsselten Versand über ungeschützte Netze. Insbesondere bei der E-Mail-Nutzung in sensiblen Bereichen ist daher besondere Sorgfalt bei der Auswahl der Adressaten und Adressatinnen – etwa aus einem Adressbuch oder einer systemseitigen „Vorschlagsliste“ – sowie auch hinsichtlich der Sensibilität der zu versendenden Daten anzuwenden. Zudem sollten Verschlüsselungslösungen zur Außenkommunikation bereitgestellt und auch genutzt werden.

— Grundsätzlich sollte insbesondere bei **Fehlversand von Gesundheitsdaten** oder Sozialdaten der unberechtigte Empfänger oder die unberechtigte Empfängerin ermittelt und kontaktiert werden und dieser oder diese aufgefordert werden, die sensiblen Daten gesichert zurückzusenden oder zu vernichten, unabhängig davon, welcher Transportweg zur Übermittlung gewählt wird.

— Erstaunlich häufig erhielt ich Meldungen über bei der Post verloren gegangene **USB-Sticks**, bei denen die Briefumschläge durch Sortiermaschinen aufgerissen wurden und die USB-Sticks nicht am vorgesehenen Ziel ankamen. Sollte es – ausnahmsweise – für nötig erachtet werden, USB-Sticks zu versenden, muss auf eine sichere Verpackung besonders geachtet werden (stabile wattierte, gut verschlossene Umschläge). Im Übrigen sollte

stets geprüft werden, ob nicht auch eine verschlüsselte elektronische Übersendung der Daten möglich ist.

— In wenigen Fällen brachten mir Meldungen zur Kenntnis, dass bei **Einbrüchen** dienstliche Notebooks und andere elektronische Geräte gestohlen oder von ihrem Benutzer oder ihrer Benutzerin verloren worden waren. Diese Fälle zeigen, dass es zwingend nötig ist, sensible Daten auf mobilen Geräten verschlüsselt abzuspeichern oder Virtualisierungslösungen zu verwenden, bei denen die Daten zentral gehostet werden.

— Die Meldungen zeigen weiterhin, dass auch Behörden und andere öffentliche Stellen von **Hackerangriffen, Schadsoftware oder Systemausfällen** betroffen sind. So wurden mir immer wieder Fälle gemeldet, bei denen sich Schadsoftware im Netz verbreiten konnte. Medienwirksam und besonders schwerwiegend war hierbei die – in Anbetracht der Umstände beachtenswerterweise fristgerechte – Meldung eines Klinikums, bei dem es für einige Tage zu einem vollständigen Ausfall der Krankenhaus-IT kam. Insgesamt waren mehrere hundert Rechner von dem Angriff betroffen. Die Klinik musste sich bei der Integrierten Leitstelle abmelden und konnte ihren Versorgungsauftrag nicht in gewohnter Weise erfüllen. Der Fall stimmt umso nachdenklicher, als es sich wohl um ein bekanntes Angriffsmuster handelte, vor dem gängige Anti-Viren-Software und regelmäßige Software-Updates schützen sollten.

  Aus einem anderen Krankenhaus erhielt ich die Nachricht, dass nach einem meldepflichtigen Systemausfall die Daten der letzten planmäßigen Sicherung eingespielt werden sollten. Allerdings stellte sich heraus, dass die Sicherungen seit eineinhalb Jahren zwar regelmäßig, jedoch nicht ordnungsgemäß durchgeführt worden waren. Deshalb waren sämtliche Daten von Patienten und Patientinnen verloren, die innerhalb der letzten eineinhalb Jahre behandelt worden waren. Bayerische öffentliche Krankenhäuser sollten vor diesem Hintergrund nicht nur regelmäßig prüfen, ob Datensicherungen stattfinden, sondern auch, ob im „Ernstfall“ brauchbare Sicherungsdateien zur Verfügung stünden.

Die bisherigen Meldungen zeigen, dass das Bewusstsein für die Meldepflichten sehr unterschiedlich ausgeprägt ist. Einige Stellen melden eine Vielzahl von Vorfällen, von denen nicht alle meldepflichtig gewesen wären. Andere Stellen haben noch gar keine Meldung abgegeben. In diesen Fällen sollte geprüft werden, ob ausreichende Prozesse zum Datenschutzmanagement sowie zur Feststellung von Datenschutzverletzungen etabliert wurden. Gerade um störungsfreie Arbeitsabläufe gewährleisten zu können, ist es wesentlich, die Beschäftigten fortwährend für das Thema Datenschutz und die Erkennung von Datenschutzverletzungen zu sensibilisieren. Es ist insbesondere festzulegen, wer derartige Meldungen durchführen soll. Bei zukünftigen Prüfungen werde ich auf die eingerichteten Prozesse zur Meldung von Verletzungen des Schutzes personenbezogener Daten besonderes Augenmerk legen.

3.1.7 Zertifizierung

In der bis zum 24. Mai 2018 geltenden Fassung kannte das Bayerische Datenschutzgesetz keine Vorschriften zur Zertifizierung von Produkten, öffentlichen

Stellen oder Verfahren. Art. 42 und 43 DSGVO regeln nun die Vergabe und die Durchführung von Zertifizierungen.

Nach Art. 42 Abs. 5 Satz 1 DSGVO können Zertifizierungen im Sinne der Datenschutz-Grundverordnung nur von Zertifizierungsstellen nach Art. 43 DSGVO oder von der zuständigen Datenschutz-Aufsichtsbehörde erteilt werden. Zum Stand der Veröffentlichung dieses Berichts gibt es in Deutschland keine derartigen Zertifizierungsstellen. Auch gibt es bislang keine genehmigten Kriterien in Deutschland, die als Grundlage für eine Zertifizierung dienen könnten.

Somit können sich bayerische öffentliche Stellen noch nicht von Zertifizierungsstellen zertifizieren lassen, und es gibt auch noch keine Möglichkeiten für nichtöffentliche Anbieter, zertifizierte Produkte oder Dienstleistungen für bayerische öffentliche Stellen anzubieten.

Abgesehen davon ist es aber auch denkbar, dass andere „Datenschutz-Prüfsiegel“ oder „Datenschutz-Zertifikate“ unabhängig von der Mitwirkung der Datenschutz-Aufsichtsbehörden und nicht den Anforderungen der Art. 42 und 43 DSGVO entsprechend durch Dritte vergeben werden. Hier ist aber zu bedenken, dass diese dann grundsätzlich nicht mit den Datenschutz-Aufsichtsbehörden abgestimmt wurden und insofern auch bei Prüfungen oder Sanktionen nicht gleichwertig berücksichtigt werden können.

Die unabhängigen Aufsichtsbehörden des Bundes und der Länder erarbeiten aktuell entsprechende Kriterien für Zertifizierungsstellen und stimmen diese mit dem Europäischen Datenschutzausschuss ab. Erst dann kann mit entsprechenden Zertifizierungsverfahren begonnen werden.

3.2 Prüfungen, Beanstandungen und Beratungen

3.2.1 Prüfungen

Im Berichtszeitraum habe ich eine ganze Reihe von öffentlichen Stellen unter technisch-organisatorischen Datenschutzaspekten geprüft. Ein besonderes Augenmerk lag dabei auf dem Bayerischen Landesamt für Gesundheit und Lebensmittelsicherheit, da dieses sowohl das neue bayernweite Krebsregister als auch eine Vielzahl weiterer Systeme zu sensiblen Gesundheitsdaten betreibt.

Zum einen stellt das Landesamt das Labor für den öffentlichen Gesundheitsdienst. Übliche Einsender sind unter anderem die Gesundheitsämter, etwa im Rahmen des Infektionsschutzes oder der Erstuntersuchung von Asylbewerberinnen und Asylbewerbern. Die Ergebnisse werden im Laborsystem des Landesamts gespeichert und auf elektronischem Weg an die Einsender zurückgemeldet. Das Landesamt nimmt zudem statistische Auswertungen zur Verbreitung und Entwicklung von Infektionen vor und übermittelt diese in anonymisierter Form an andere Stellen wie beispielsweise das Robert Koch-Institut zur deutschlandweiten Auswertung.

Des Weiteren werden beim Landesamt die Untersuchungsergebnisse des Stoffwechsels-Screenings sowie des Hör-Screenings von Neugeborenen, das in der jeweiligen Geburtsklinik durchgeführt wird (siehe mein 23. Tätigkeitsbericht 2008,

Nr. 13.1.2) gespeichert und zu statistischen Zwecken sowie zu Forschungszwecken ausgewertet.

Für die Schuleingangsuntersuchungen stellt das Landesamt den Gesundheitsämtern eine Software zur Verfügung, in der die relevanten Daten und Untersuchungsergebnisse der Kinder erfasst werden können. Allerdings werden die Datensätze hier lokal in den Gesundheitsämtern gespeichert; das Landesamt erhält von diesen nur statistische Informationen.

Zudem werden am Landesamt in den verschiedenen Bereichen Forschungsprojekte insbesondere auch hinsichtlich der Gesundheit von Kindern und Jugendlichen durchgeführt. Dies geschieht in der Regel auf Basis einer Einwilligung der Erziehungsberechtigten; im Rahmen der Auswertung wird mit pseudonymisierten oder anonymisierten Daten gearbeitet.

In der Regel kommt es nicht zu einer Verknüpfung der in verschiedenen Bereichen des Landesamts vorhandenen Daten, sondern es wird mit den Daten des jeweiligen Bereichs und eventuell weiteren eigens für die jeweilige Studie erhobenen Daten gearbeitet.

Häufig werden beim Landesamt medizinische Daten verarbeitet, die dem Ansehen des Betroffenen besonders schaden können, da gerade kritische Infektionen wie AIDS oder andere ansteckende Krankheiten analysiert werden. Infolge der Eigenschaft als „Zentrallabor" für Bayern werden vom Landesamt in großem Umfang medizinische Daten verarbeitet. Betroffen sind auch Daten von besonders schutzwürdigen Personengruppen wie Kindern, die nach der Datenschutz-Grundverordnung ebenfalls einen besonderen Schutz genießen.

Das Landesamt als bayernweit tätige Einrichtung treffen daher in besonderem Umfang Anforderungen der Datenschutz-Grundverordnung im technisch-organisatorischen Bereich (siehe Nr. 3.2.3). Deshalb ist es hier von herausragender Bedeutung ein einheitliches und nachweisbares Schutzniveau für alle technischen Verfahren sicherzustellen sowie Prozesse für das Datenschutzmanagement zu etablieren. Ich habe daher dem Landesamt insbesondere nahegelegt, eine Risikoabschätzung für die vorhandenen Verfahren vorzunehmen und im Bedarfsfall Datenschutz-Folgenabschätzungen durchzuführen. Die Erarbeitung von Maßnahmen werde ich kritisch begleiten und auch kontrollieren.

3.2.2 Beanstandungen im Bereich des technisch-organisatorischen Datenschutzes

Leider musste ich im Berichtszeitraum im Bereich des technisch-organisatorischen Datenschutzes mehrere Beanstandungen aussprechen. Beachtliche Verstöße gegen Vorschriften zur Datensicherheit hatten in diesen Fällen zu einer unbefugten Offenbarung von sensiblen personenbezogenen Daten geführt:

— Das Internet-Portal einer öffentlichen Stelle, über das sensible personenbezogene Daten zum Abruf bereitgestellt werden, hatte für den Anmeldevorgang keine Systemroutine, die dabei ein Minimum von Komplexität bei der Vergabe von Passworten erzwingt, eingerichtet (siehe die Orientierungshilfe „Passwortvergabe, -wahl und -verwaltung", abrufbar auf meiner Homepage https://www.datenschutz-bayern.de unter „Veröffentlichungen – Orientierungshilfen"). Dies führte dazu, dass teilweise Passwörter

verwendet wurden, die leicht zu erraten waren. Hierüber hatte sich ein Bürger bei mir beschwert. Besonders Brisanz erhielt dies dadurch, dass ich diesen Mangel bereits einige Jahre zuvor festgestellt hatte und mir damals die Behebung zugesichert worden war. Nachdem dies offensichtlich nicht geschehen war, habe ich den Verstoß gegen datenschutzrechtliche Vorschriften beanstandet.

— Eine weitere Beanstandung sprach ich gegenüber einem großen Klinikum aus, nachdem es mehrfach zum Fehlversand von Arztbriefen gekommen war. Üblicherweise muss die Einwilligung des Patienten eingeholt werden, wenn Arztbriefe an den einweisenden Arzt, den Hausarzt oder andere Ärzte im Anschluss an die Behandlung übermittelt werden sollen. In den beanstandeten Fällen wurden Briefe an einen Arzt versandt, bei dem der Patient nicht mehr in Behandlung war. Der Patient hatte dem Klinikum bei seiner Wiederaufnahme den Arztwechsel mitgeteilt, dennoch wurden die Arztbriefe mehrfach an den bisherigen Arzt versandt, da der Arztwechsel im Krankenhausinformationssystem oder in der Patientenakte nicht so dokumentiert war, dass dies im Rahmen der Fertigung und des Versands klar ersichtlich war. Wie mehrere Meldungen von Datenschutzverletzungen nach Art. 33 DSGVO aus diesem Krankenhaus gezeigt haben, kam es in weiteren Fällen zu ähnlichen Fehlversendungen. Ich habe das Klinikum aufgefordert, seine Prozesse zu überprüfen und geeignete Maßnahmen zu ergreifen.

  Meldungen von Datenschutzverletzungen sowie Beschwerden aus anderen Krankenhäusern zeigen, dass die Problematik des Fehlversands von Arztbriefen verbreitet ist und die datenschutzrechtliche Sensibilität von Patienten erfreulich zunimmt. Krankenhäuser sollten daher sowohl ihre Prozesse bei der Fertigung und dem Versand von Arztbriefen kritisch hinterfragen als auch die Dokumentation im Krankenhausinformationssystem nicht außer Betracht lassen.

3.2.3 Technische Anforderungen an das Bayerische Krebsregister

Durch das neue Bayerische Krebsregistergesetz (siehe Nr. 8.3) hat sich auch die technische Struktur des Krebsregisters grundlegend geändert. Bisher verfügten die regionalen klinischen Krebsregister jeweils für ihre Region über eine eigene Datenhaltung. Daraus wurden die erforderlichen Daten an das zentrale epidemiologische Krebsregister übermittelt. In jedem regionalen Register kamen eigene Server, Datenformate und Verfahren/Software zum Einsatz. Es mussten somit auch jeweils geeignete technische und organisatorische Sicherheitsmaßnahmen ergriffen werden.

Das neue Krebsregistergesetz sieht nun vor, alle Daten zentral beim Bayerischen Landesamt für Gesundheit und Lebensmittelsicherheit zu speichern und den Regionalzentren, die aus den ehemals eigenständigen regionalen klinischen Krebsregistern hervorgegangen und mittlerweile dem Landesamt zugeordnet sind, in dem erforderlichem Umfang Zugriff auf die Daten zu geben. Wichtig ist hierbei zum einen, dass die Daten des Krebsregisters getrennt von den anderen Verfahren des Landesamt gehalten werden (siehe Nr. 8.3), und zum anderen, dass ein ausreichendes Sicherheitsniveau geschaffen wird.

Die im neuen bayerischen Krebsregister verarbeiteten Daten haben einen deutlich größeren Umfang als im bisherigen epidemiologischen Krebsregister, da nun

zusätzlich ein zentrales klinisches Krebsregister geführt wird. Medizinische Daten und identifizierende Daten der Patienten und Patientinnen werden getrennt in einer Vertrauensstelle und bei der Zentralstelle für Krebsfrüherkennung und Krebsregistrierung gespeichert. Aus Sicht der Zentralstelle handelt es sich zwar um anonymisierte Daten, bei einer Gesamtbetrachtung über alle beteiligten Stellen hinweg (Zentralstelle, Vertrauensstelle und Regionalzentren) ist jedoch festzustellen, dass die Daten zumindest für einen Teil der Beschäftigten in den Regionalzentren mit Personenbezug abrufbar sind, beispielsweise, um weitere Meldungen zu einem Patienten oder einer Patientin einzupflegen. Zudem ist eine Abrufmöglichkeit für die behandelnden Ärzte und Ärztinnen vorgesehen, für die ebenfalls ein Personenbezug nötig ist.

Aufgrund der der Sensibilität der Daten und hohen Anzahl betroffener Personen halte ich eine Datenschutz-Folgenabschätzung (siehe Nr. 3.1.3) für erforderlich. Hinzu kommt, dass die Freiheit der Patienten und Patientinnen zur Ausübung ihrer Rechte eingeschränkt wird, da für die Ärzte und Ärztinnen eine Meldepflicht besteht und den Patienten und Patientinnen nur ein Widerspruchsrecht zukommt. Bei erfolgreichem Widerspruch werden nicht alle Daten eines Patienten oder einer Patientin, sondern nur die ihn oder sie identifizierenden Daten bei der Vertrauensstelle gelöscht.

Ich begrüße es, dass das Landesamt mit der Datenschutz-Folgenabschätzung bereits begonnen hat. Diese soll parallel zum Aufbau des zentralen Registers und der Migration der bisherigen klinischen Krebsregister zum Landesamt fertiggestellt werden. Diesen Prozess werde ich engmaschig begleiten.

3.3 Interessenkonflikt bei der Benennung eines IT-Sicherheitsbeauftragten als Datenschutzbeauftragter

Während die Benennung behördlicher Datenschutzbeauftragter gesetzlich vorgeschrieben ist, besteht hinsichtlich IT-Sicherheitsbeauftragter grundsätzlich keine derartige Verpflichtung.

Im Rahmen meiner Prüfungen im technisch-organisatorischen Bereich ist mir allerdings aufgefallen, dass viele Behörden Datenschutzbeauftragten auch die Funktion von IT-Sicherheitsbeauftragten übertragen haben. Insofern ist zu bemerken:

Nach Art. 38 Abs. 6 Satz 1 DSGVO kann der Datenschutzbeauftragte andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche muss aber sicherstellen, dass derartige Aufgaben und Pflichten nicht zu einem **Interessenkonflikt** führen (vgl. Art. 38 Abs. 6 Satz 2 DSGVO). Diese Vorgabe bringt insbesondere mit sich, dass Datenschutzbeauftragte innerhalb einer Behörde keine Position innehaben können, auf welcher sie Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegen.

Bei der Benennung von IT-Sicherheitsbeauftragten als Datenschutzbeauftragte ist ein derartiger Interessenkonflikt nicht ausgeschlossen. IT-Sicherheitsbeauftragte legen die IT-Sicherheitsstandards der jeweiligen Behörde fest und müssten sie als Datenschutzbeauftragte anschließend selbst überprüfen. Eine solche Kontrolle mag im Einzelfall weniger kritisch ausfallen als dies bei einer Trennung der beiden Funktionen der Fall wäre. Außerdem haben IT-Sicherheitsbeauftragte oftmals ein Interesse daran, Datenverarbeitungen über möglichst lange Zeiträume zu

protokollieren, um Sicherheitsvorfälle erkennen zu können. Datenschutzbeauftragte wirken demgegenüber regelmäßig darauf hin, dass nicht mehr für die Aufgabenerfüllung erforderliche Daten alsbald gelöscht werden.

Vor diesem Hintergrund sollten die Rollen „Datenschutzbeauftragter“ und „IT-Sicherheitsbeauftragter“ grundsätzlich nicht derselben Person zugewiesen werden.

4 Polizei

4.1 Allgemeines

4.1.1 Reform des Polizeiaufgabengesetzes

Die umfassende Reform des Polizeirechts hat mich im Berichtszeitraum stark beansprucht. Gleich zweimal wurde das Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei (Polizeiaufgabengesetz – PAG) innerhalb von nur einem Jahr geändert. Am 24. Juli 2017 verabschiedete der Bayerische Landtag das Gesetz zur effektiveren Überwachung gefährlicher Personen, das am 1. August 2017 in Kraft trat. Nur zehn Monate später beschloss er am 18. Mai 2018 das Gesetz zur Neuordnung des bayerischen Polizeirechts, das am 25. Mai 2018 in Kraft trat.

Aufgrund der gestiegenen Terrorgefahr sah sich der bayerische Gesetzgeber veranlasst, die Normierung einzelner Befugnisse und Regelungen mit dem **Gesetz zur effektiveren Überwachung gefährlicher Personen** vom 24. Juli 2017 (GVBl. S. 388) zeitlich vorzuziehen. Hierbei handelte es sich im Wesentlichen um die Einführung der elektronischen Aufenthaltsüberwachung („elektronische Fußfessel"), die Ergänzung des Platzverweises um Aufenthaltsgebote und Aufenthaltsverbote sowie Kontaktverbote, zu deren Überwachung ebenfalls die elektronische Aufenthaltsüberwachung angeordnet werden kann. Des Weiteren wurde eine Rechtsgrundlage für die präventivpolizeiliche Quellen-Telekommunikationsüberwachung geschaffen, die bisherige Befristung des Präventivgewahrsams von 14 Tagen aufgehoben sowie bei offenen Bild- und Tonaufzeichnungen nach Art. 32 Polizeiaufgabengesetz in der bis zum 24. Mai 2018 geltenden Fassung (PAG-alt) (jetzt: Art. 33 PAG) sowie Art. 21a BayDSG-alt (jetzt: Art. 24 BayDSG) die Höchstspeicherfrist von drei Wochen auf zwei Monate ausgeweitet. Zugleich nahm der Gesetzgeber die Reform zum Anlass, den Begriff der sogenannten drohenden Gefahr als zusätzliche Gefahrenkategorie einzuführen. Die drohende Gefahr wurde in Art. 11 Abs. 3 PAG legaldefiniert.

Art. 11 PAG
Allgemeine Befugnisse
(3)[1]Die Polizei kann unbeschadet der Abs. 1 und 2 die notwendigen Maßnahmen treffen, um den Sachverhalt aufzuklären und die Entstehung einer Gefahr für ein bedeutendes Rechtsgut zu verhindern, wenn im Einzelfall

1. *das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet oder*
2. *Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen den Schluss auf ein seiner Art nach konkretisiertes Geschehen zulassen,*

wonach in absehbarer Zeit Angriffe von erheblicher Intensität oder Auswirkung zu erwarten sind (drohende Gefahr), soweit nicht die Art. 12 bis 65 die Befugnisse der Polizei besonders regeln. [2]Bedeutende Rechtsgüter sind:

1. *der Bestand oder die Sicherheit des Bundes oder eines Landes,*
2. *Leben, Gesundheit oder Freiheit,*
3. *die sexuelle Selbstbestimmung,*

4. erhebliche Eigentumspositionen oder
5. Sachen, deren Erhalt im besonderen öffentlichen Interesse liegt.

Der Begründung des Gesetzentwurfs zufolge soll die neue Kategorie der drohenden Gefahr einer besseren Erfassung vor allem von Vorbereitungshandlungen dienen.

Dies sehe ich aus datenschutzrechtlicher Sicht jedoch kritisch. Die Definition der drohenden Gefahr ist so weit und unbestimmt gefasst, dass unklar ist, welche Abgrenzungsmöglichkeiten zu den bereits bestehenden Gefahrkategorien bleiben, zumal das Polizeiaufgabengesetz bereits zahlreiche Gefahrkategorien kennt. Zudem wird der Begriff der drohenden Gefahr weder auf verdeckte Maßnahmen noch auf die Terrorismusbekämpfung beschränkt. Es findet eine erhebliche Vorverlagerung der polizeilichen Einschreitschwelle bei den Standardbefugnissen statt, wie beispielsweise Identitätsfeststellung oder Durchsuchung. Die Gesetzesänderung führt dazu, dass die polizeilichen Standardbefugnisse faktisch auf einen deutlich größeren Personenkreis abzielen, der mit der aktuellen Sicherheitslage in keinem Zusammenhang steht.

Bereits frühzeitig habe ich auf dieses Problem aufmerksam gemacht und mich für eine ersatzlose Streichung der neuen Gefahrenkategorie eingesetzt. Damit konnte ich nicht durchdringen. Allerdings konnte ich eine Einschränkung des ursprünglich noch weiter gefassten Gefahrentatbestands erreichen. Insbesondere wurde auf meine Veranlassung hin der Begriff der drohenden Gefahr auf „bedeutende Rechtsgüter“ sowie auf „Gewalttaten von erheblicher Intensität oder Auswirkung“ beschränkt (siehe Landtags-Drucksache 17/16299, S. 5). Letzteres wurde jedoch im parlamentarischen Gesetzgebungsverfahren durch einen Änderungsantrag wieder aufgeweicht.

Weiterhin konnte ich etwa bei der elektronischen Aufenthaltsüberwachung (EAÜ) die Normierung zusätzlicher Verfahrenssicherungen erreichen, auch wenn ich einen vollständigen Verzicht auf die EAÜ für vorzugswürdig gehalten hätte. Denn die EAÜ ist bereits nicht zur Terrorismusbekämpfung geeignet, mit welcher ihre Einführung begründet wurde. So kann die EAÜ allenfalls den Weg nachzeichnen, den ein tatentschlossener Gefährder oder eine tatentschlossene Gefährderin nimmt. Die EAÜ wird ihn oder sie jedoch nicht von der Begehung eines Anschlags abhalten können.

Der ersten Reform des Polizeiaufgabengesetzes folgte nur kurze Zeit später die **zweite, deutlich umfangreichere Novelle**. Mit dem **Gesetz zur Neuordnung des bayerischen Polizeirechts** (PAG-Neuordnungsgesetz) vom 18. Mai 2018 (GVBl. S. 301) sollten das Urteil des Bundesverfassungsgerichts vom 20. April 2016, Az.: 1 BvR 966/09 und 1 BvR 1140/09, BVerfGE 141, 220, zum Bundeskriminalamtgesetz (sogenanntes BKAG-Urteil) sowie die Datenschutz-Richtlinie für Polizei und Strafjustiz umgesetzt werden. Zugleich wurde das Polizeiaufgabengesetz um zahlreiche weitere Befugnisse ergänzt. So nahm der Gesetzgeber insbesondere die präventive DNA-Analyse, die Durchsuchung elektronischer Speichermedien (einschließlich Clouds), die DNA-Analyse zur Feststellung äußerlicher Merkmale, Übersichtsaufzeichnungen bei großen Veranstaltungen oder Ansammlungen, den Einsatz von Bodycams und von sogenannter intelligenter Videoüberwachung, die präventive Postsicherstellung sowie den Einsatz unbemannter Luftfahrtsysteme (Drohnen) neu in das Polizeiaufgabengesetz auf.

Das Bayerische Staatsministerium des Innern, für Sport und Integration beteiligte mich frühzeitig an dem Reformvorhaben. Ich erhielt mehrfach die Gelegenheit, zu dem Gesetzentwurf (Landtags-Drucksache 17/20425) Stellung zu beziehen. Mein Hauptaugenmerk legte ich dabei auf die neuen Befugnisse, die zum Teil erhebliche Grundrechtseingriffe zur Folge haben. Zudem überprüfte ich den Gesetzentwurf dahingehend, ob er die aus dem BKAG-Urteil und der Datenschutz-Richtlinie für Polizei und Strafjustiz resultierenden Vorgaben richtig und vollständig umsetzt. Vor allem **folgende Punkte** sah ich **sehr kritisch**:

— Die neu eingeführte Durchsuchungsmöglichkeit elektronischer Speichermedien gemäß Art. 22 Abs. 2 Satz 1 PAG halte ich für problematisch. Denn elektronische Daten sind keine „Sachen" im Sinne des Art. 22 Abs. 1 PAG, da ihnen die für den Sachbegriff kennzeichnende abgrenzbare Körperlichkeit (siehe § 90 Bürgerliches Gesetzbuch) fehlt. Zudem sieht die neue Befugnis keinerlei flankierende Regelungen, insbesondere keinen Richtervorbehalt vor, obwohl die Maßnahme einem Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nahekommt. Auch § 110 Abs. 3 Strafprozessordnung (StPO), dem Art. 22 Abs. 2 PAG nachgebildet ist, setzt grundsätzlich eine vom Ermittlungsrichter angeordnete Durchsuchung (§ 105 Abs. 1 StPO) voraus.

— Art. 32 Abs. 1 Satz 2 PAG erlaubt nunmehr die molekulargenetische Untersuchung aufgefundenen Spurenmaterials unbekannter Herkunft zur Feststellung des Geschlechts, der Augen-, Haar- und Hautfarbe, des biologischen Alters und der biogeographischen Herkunft des Spurenverursachers. Diese Erweiterung der DNA-Analyse lehne ich jedoch ab. Die DNA-Analyse zur Feststellung äußerer Merkmale ermöglicht nur Wahrscheinlichkeitsvorhersagen, keine gesicherten Erkenntnisse. Sie ist daher zur rechtssicheren Feststellung äußerlicher Merkmale und zielgenauen Eingrenzung des Spurenverursacherkreises ungeeignet. Es besteht zudem die Gefahr der Diskriminierung bestimmter Bevölkerungskreise, insbesondere aufgrund der Hautfarbe und biogeographischen Herkunft. Darüber hinaus bedarf die Bestimmung äußerer Merkmale wie der Haarfarbe unter anderem der Untersuchung codierender Bereiche des Genoms, welche Erbinformationen enthalten. Durch die Untersuchung codierender Bereiche kann der „absolut geschützter Kernbereich der Persönlichkeit" betroffen sein, „in den auch aufgrund eines Gesetzes nicht eingegriffen werden dürfte" (siehe Bundesverfassungsgericht, Beschluss vom 14. Dezember 2000, Az.: 2 BvR 1741/99, BVerfGE 103, 21, 31 f. Rn. 50 – genetischer Fingerabdruck).

— Nach Art. 33 Abs. 4 Satz 3 PAG dürfen zukünftig Bodycams auch in Wohnungen eingesetzt werden. Diese Regelung halte ich mangels Richtervorbehalt für verfassungswidrig. Bodycams sind technische Überwachungsmittel im Sinne des Art. 13 Abs. 4 Grundgesetz (GG). Zwar hatte der Grundgesetzgeber bei dessen Schaffung in erster Linie heimliche Überwachungsmaßnahmen im Blick, eine dahingehende Beschränkung wurde jedoch gerade nicht vorgenommen. Art. 13 Abs. 5 GG ist demgegenüber – anders als die Gesetzesbegründung annimmt – nicht anwendbar, da Bodycams nicht als „technische Mittel ausschließlich zum Schutze der bei einem Einsatz in Wohnungen tätigen Personen vorgesehen" sind. Art. 13 Abs. 7 GG scheidet als Bewertungsmaßstab ebenfalls aus. Denn dieser Tatbestand kommt nur „im Übrigen", also subsidiär zur Anwendung.

— Weiterhin begegnet die Beschränkung der parlamentarischen Kontrolle erheblichen Bedenken. Nach Art. 52 Abs. 1 PAG unterrichtet das Innenministerium zukünftig nicht mehr den Landtag insgesamt, sondern nur noch das Parlamentarische Kontrollgremium (PKG). Das PKG entspricht jedoch nicht dem Landtag, sondern ist ein von diesem gewähltes, aus wenigen Mitgliedern bestehendes Kontrollgremium. Da dessen Mitglieder zur Geheimhaltung verpflichtet sind, entziehen sich die zu kontrollierenden Themen, insbesondere deren Details, der Kenntnis der übrigen Abgeordneten. Diese Regelung steht in Widerspruch zu den Ausführungen des Bundesverfassungsgerichts im BKAG-Urteil, wonach es „zur Gewährleistung von Transparenz und Kontrolle […] einer gesetzlichen Regelung von Berichtspflichten [bedarf]. Da sich die Durchführung von heimlichen Überwachungsmaßnahmen der Wahrnehmung der Betroffenen und der Öffentlichkeit entzieht und dem auch Benachrichtigungspflichten oder Auskunftsrechte mit der Möglichkeit anschließenden subjektiven Rechtsschutzes nur begrenzt entgegenwirken können, sind hinsichtlich der Wahrnehmung dieser Befugnisse regelmäßige Berichte des Bundeskriminalamts gegenüber Parlament und Öffentlichkeit gesetzlich sicherzustellen“ (Bundesverfassungsgericht, Urteil vom 20. April 2016, Az.: 1 BvR 966/09 und 1 BvR 1140/09, BVerfGE 141, 220, 285 Rn. 142 f.). Über diese eindeutige Vorgabe kann sich der Gesetzgeber nicht hinwegsetzen. Zudem lässt sich die Beschränkung der parlamentarischen Kontrolle auch nicht mit einer Parallele zu Art. 20 Abs. 1 Satz 1 Bayerisches Verfassungsschutzgesetz begründen. Denn aufgrund des sogenannten Trennungsprinzips kann es grundsätzlich keinen Gleichlauf zwischen dem Polizeiaufgabengesetz und dem Bayerischen Verfassungsschutzgesetz geben.

— Schließlich begegnet auch die neue Regelung des Art. 92 Abs. 3 PAG zur richterlichen Bestätigung von Eilmaßnahmen erheblichen Bedenken.

Art. 92 PAG
Verfahren und Zuständigkeit für gerichtliche Entscheidungen, Wegfall der Anordnungsvoraussetzungen
(3) [1]Wurde bei Maßnahmen, die einem Richtervorbehalt unterliegen, bei Gefahr im Verzug jedoch durch bestimmte Polizeivollzugsbeamte angeordnet werden können, von der Eilfallkompetenz Gebrauch gemacht, ist unverzüglich eine richterliche Bestätigung der Maßnahme einzuholen. [2]Satz 1 gilt außer in Fällen des Art. 41 Abs. 1 nicht, wenn die Maßnahme bereits vorher erledigt ist. [3]Die Maßnahme tritt außer Kraft, soweit sie nicht binnen drei Werktagen richterlich bestätigt wird.

Nach Art. 92 Abs. 3 Satz 2 PAG ist in Eilfällen eine richterliche Bestätigung nicht einzuholen „wenn die Maßnahme bereits vorher erledigt ist“. Dies hat zur Folge, dass der Richtervorbehalt bei zahlreichen Eilmaßnahmen ins Leere läuft. So könnte etwa bei Gefahr im Verzug kurzzeitig eine Quellen-Telekommunikationsüberwachung oder Online-Durchsuchung durchgeführt werden. Die Einholung der richterlichen Bestätigung würde dann hinfällig, wenn die Maßnahme – jedenfalls vor Ablauf der Drei-Tages-Frist des Art. 92 Abs. 3 Satz 3 PAG – abgebrochen würde. Zwar wurde auf meine massive Kritik hin die Wohnraumüberwachung (Art. 41 PAG) als Rückausnahme vorgesehen. Allerdings verstößt der Art. 92 Abs. 3 Satz 2 PAG für Fälle des Bodycam-Einsatzes in Wohnungen (Art. 33 Abs. 4 Satz 3 PAG) weiterhin gegen Art. 13 Abs. 4 GG, insbesondere dann, wenn etwaige Bildaufnahmen bereits gelöscht wurden und die Maßnahme daher nicht mehr

fortwirkt. Art. 13 Abs. 4 GG sieht zwingend eine richterliche Anordnung und bei Eilfällen eine richterliche Bestätigung vor. Diese Vorgaben dürfen durch einfachgesetzliche Reglungen nicht umgangen werden.

Zudem konnte ich mich im Zusammenhang mit der Speicherung von Daten nicht mit der gesetzlichen Regelung einer sogenannten **Negativprognose** in Art. 54 Abs. 2 Satz 1 PAG durchsetzen, wie sie auf Bundesebene bereits § 18 Abs. 5 Satz 1 Nr. 2 BKAG vorsieht. Mir ist zwar bewusst, dass der Bayerische Verfassungsgerichtshof in einer älteren Entscheidung (vom 19. Oktober 1994, Az.: Vf. 12-VII/92 und Vf. 13-VII/92) die bisherige Vorschrift des Art. 38 Abs. 1 PAG-alt nicht beanstandet hat. Allerdings halte ich eine täterbezogene Einzelprognose für erforderlich, um die Speicherung und Weiterverarbeitung von personenbezogenen Daten auf das unbedingt Erforderliche zu beschränken sowie der Kategorisierung der betroffenen Personen im Sinne des Art. 6 RLDSJ und Art. 30 Abs. 4 PAG Genüge zu tun.

Des Weiteren war es mir ein Anliegen, in Art. 54 Abs. 2 PAG eigene Prüfungsintervalle für **personengebundene Hinweise (PHW)** vorzusehen. PHW werden auf der Basis von Katalogwerten und zugehörigen Vergabekriterien vergeben und stellen teilweise besondere Kategorien personenbezogener Daten nach Art. 10 RLDSJ beziehungsweise Art. 30 Abs. 2 PAG dar, an deren Verarbeitung besonders strenge Anforderungen zu stellen sind. So handelt es sich etwa beim PHW Ansteckungsgefahr (ANST) um ein Gesundheitsdatum. Nach Art. 4 Abs. 1 Buchst. d RLDSJ haben Daten zudem sachlich richtig und erforderlichenfalls auf dem neuesten Stand zu sein, was vor allem beim PHW Betäubungsmittelkonsument (BTMK) von Bedeutung ist, da sich die den Kriterien zugrundeliegenden Lebensumstände ändern und verbessern können. Leider fand mein Anliegen im Rahmen des Gesetzgebungsverfahrens keine Berücksichtigung.

Ebenso konnte ich mich nicht mit einer ersatzlosen Streichung der sogenannten **Mitziehklausel** in Art. 54 Abs. 2 Satz 6 PAG durchsetzen, deren Folgen (teilweise sehr lange Speicherungsdauer) ich für unverhältnismäßig halte (siehe hierzu mein ausführlicher Beitrag unter Nr. 4.4.3).

Neben diesen und zahlreichen weiteren Kritikpunkten konnte ich jedoch auch **positive Änderungen** verzeichnen. Unter anderem habe ich etwa Folgendes erreicht:

— Die Befugnisse zu DNA-Analysen nach Art. 14 Abs. 4 Satz 2 und Art. 32 Abs. 1 Satz 3 PAG wurden auf meine Anregung hin jeweils um eine Zweckbindungsregelung (Feststellungsverbot) ergänzt, Art. 32 Abs. 1 Satz 2 PAG zudem um eine Subsidiaritätsklausel.

— Ebenso hat der Gesetzgeber die neue Befugnis zur Sicherstellung von Daten in Art. 25 Abs. 3 Satz 1 PAG unter einen Subsidiaritätsvorbehalt gestellt.

— In Art. 27 Abs. 3 Satz 5 PAG (Verwertung und Vernichtung sichergestellter Sachen) wurde des Weiteren aufgenommen, dass „bei der Verwertung von Datenträgern […] sicherzustellen [ist], dass zuvor personenbezogene Daten dem Stand der Technik entsprechend gelöscht wurden“, um zu verhindern, dass bei der Verwertung von Datenträgern personenbezogene Daten des vormaligen Benutzers unzulässigerweise „in fremde Hände gelangen“.

— Auch Art. 36 Abs. 2 PAG wurde auf meine Forderung hin mit einer Subsidiaritätsklausel versehen, damit die besonderen Mittel der Datenerhebung aufgrund ihrer Eingriffsintensität nur als „ultima ratio“ eingesetzt werden. Zudem stellte der Gesetzgeber in Art. 36 Abs. 4 PAG die längerfristige Observation sowie das Abhören oder Aufzeichnen des außerhalb von Wohnungen nichtöffentlich gesprochenen Wortes unter Richtervorbehalt. Des Weiteren wurden polizeiliche Anordnungen auf meine Anregung hin mit einer Höchstfrist von drei Monaten versehen (siehe Art. 36 Abs. 5 Satz 3 PAG).

— In Art. 41 Abs. 1 Satz 2 Nr. 1 Buchst. a PAG (Einsatz technischer Mittel in Wohnungen) hat der Gesetzgeber den Berufsgeheimnisschutz auf alle Berufsgeheimnisträger erstreckt und damit die im bisherigen Art. 34 Abs. 1 Satz 2 Nr. 2 Buchst. a PAG-alt angelegte Differenzierung nach bestimmten Berufsgruppen aufgegeben.

— Für die längerfristige Observation wurden in Art. 49 PAG sowohl ein Berufsgeheimnisträgerschutz als auch ein Kernbereichsschutz auf Erhebungsebene etabliert.

— In Art. 51 Abs. 2 Satz 3 PAG (Protokollierung, Kontrolle durch den Landesbeauftragten für den Datenschutz) wurde nunmehr geregelt, dass die Protokolle über Datenlöschungen und die Vernichtung von Unterlagen ebenfalls zu löschen sind.

— Des Weiteren normierte der Gesetzgeber in Art. 54 Abs. 2 Satz 2 PAG (Speicherung, Veränderung und Nutzung von Daten), dass die Löschung von Daten bei Wegfall des der Speicherung zugrunde liegenden Verdachts nunmehr „unverzüglich“ zu erfolgen hat. In Art. 54 Abs. 4 Satz 4 PAG hat er hinsichtlich der Datenverarbeitung zu wissenschaftlichen Zwecken zudem ein Verwendungsverbot für Daten aus der besonders eingriffsintensiven Wohnraumüberwachung und Online-Durchsuchung geregelt. Zudem legte er in einem eigenständigen Art. 54 Abs. 5 PAG fest, dass die Polizei ihre gespeicherten Daten regelmäßig auf Richtigkeit, Vollständigkeit, Zuverlässigkeit und Aktualität kontrollieren soll.

— Auf meine Empfehlung hin wurde zudem ein eigenständiges Übermittlungsverbot aufgrund möglicher Menschenrechtsverletzungen (Art. 58 Abs. 1 Satz 3 Nr. 3 PAG) geschaffen. Darüber hinaus wurde in Art. 58 Abs. 4 Satz 2 PAG eine Hinweispflicht der Polizei auf die Zweckbindung gegenüber Empfängern in Drittstaaten aufgenommen.

— Weiterhin wurden in Art. 13, 14 PAG (Zentrale Datenprüfstelle) zahlreiche Anregungen aufgegriffen, um die vollständige Unabhängigkeit der Zentralen Datenprüfstelle zu gewährleisten. Zudem darf die Zentrale Datenprüfstelle im Falle einer Ablehnung der Freigabe nach Art. 14 Abs. 1 Satz 3 PAG der zuständigen Polizeidienststelle nur eine Entscheidungsausfertigung ohne Gründe bekanntgeben, um zu vermeiden, dass diese vom konkreten Inhalt der Daten Kenntnis erlangt.

— Auch bei Art. 29 Abs. 3 bis 6 BayDSG (DNA-Untersuchungen) konnte ich einige Verbesserungen erreichen, etwa das Erfordernis einer schriftlichen Zustimmung der betroffenen Personen sowie deren Belehrung hierüber,

des Weiteren die Protokollierung der Abgleiche und Verwendung der Protokolldaten nur zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung sowie die Vernichtung der entnommenen Körperzellen spätestens drei Jahre nach dem letzten Kontakt.

Meine ausführliche Stellungnahme zur zweiten PAG-Reform ist auf meiner Homepage https://www.datenschutz-bayern.de unter „Themengebiete" – „Polizei" eingestellt.

4.1.2 (Mit-)Zuständigkeit der Polizei beim Vollzug des Prostituiertenschutzgesetzes (ProstSchG)

Zum 1. Juli 2017 trat das Gesetz zum Schutz von in der Prostitution tätigen Personen (Prostituiertenschutzgesetz – ProstSchG) in Kraft, für dessen Vollzug nach § 64a Satz 1 Halbsatz 1 Zuständigkeitsverordnung (ZustV) grundsätzlich die Kreisverwaltungsbehörden zuständig sind.

§ 9 Abs. 2 ProstSchG regelt unter anderem, dass die „zuständige Behörde" unverzüglich erforderliche Schutzmaßnahmen zu veranlassen hat, wenn sich tatsächliche Anhaltspunkte für das Vorliegen von Zwangsprostitution ergeben.

Für diese Fälle hat der bayerische Gesetzgeber, leider ohne mich zuvor nach Art. 32 Abs. 3 BayDSG-alt zu unterrichten, in § 64a Satz 1 Halbsatz 2 ZustV festgelegt, dass neben den Kreisverwaltungsbehörden auch die Polizei „zuständige Behörde" ist.

Ich halte diese (Mit-)Zuständigkeit der Polizei aus datenschutzrechtlicher Sicht für problematisch. Der Bundesgesetzgeber hat Schutzmaßnahmen (und damit in der Regel einhergehende Datenübermittlungen an die Polizei) nur dann vorgesehen, wenn die Voraussetzungen des § 9 Abs. 2 ProstSchG erfüllt sind. Die bayerische Regelungslage führt nun dazu, dass die Polizei über alle unter das Prostituiertenschutzgesetz fallenden Personen pauschal Informationen erhalten kann, also nicht nur dann, wenn sich tatsächliche Anhaltspunkte für das Vorliegen von Zwangsprostitution ergeben.

Konkret bedeutet dies, dass die Polizei schon im Vorfeld tatsächlicher Anhaltspunkte für das Vorliegen erzwungener oder ausbeuterischer Prostitution alle Daten aus dem Prostituiertenanmeldeverfahren bei den Kreisverwaltungsbehörden zugeliefert bekommen soll. Da zu diesem Zeitpunkt aber noch kein Erfordernis für konkrete Schutzmaßnahmen absehbar ist, hat der bayerische Gesetzgeber der Polizei somit die Möglichkeit einer pauschalen Gefahren**erforschung** eröffnet. Die Datenschutzinteressen der legal im Prostitutionsgewerbe tätigen Personen werden hierdurch nicht hinreichend gewahrt. Nach meiner Auffassung widerspricht dies dem Sinn und Zweck des Prostituiertenschutzgesetzes.

Vor diesem Hintergrund habe ich, unabhängig von meiner grundsätzlichen Kritik an § 64a Satz 1 Halbsatz 2 ZustV, gegenüber dem Innenministerium zum Ausdruck gebracht, dass bei der Verarbeitung von im genannten Zusammenhang erlangten Informationen durch die Polizei die Grundsätze der Erforderlichkeit und Zweckbindung besonders zu beachten sind.

4.1.3 Verwaltungsvorschriften bezüglich polizeilicher Speicherungen

In zwei Punkten konnte ich erreichen, dass die einschlägigen Verwaltungsvorschriften bezüglich polizeilicher Speicherungen aus datenschutzrechtlicher Sicht verbessert wurden:

Wesentliche Voraussetzung dafür, eine Person als Beschuldigten zu speichern, ist, dass gegen sie ein sogenannter polizeilicher Restverdacht besteht (vgl. zu diesem Begriff 27. Tätigkeitsbericht 2016 unter Nr. 3.6.5). Wie ich in meinem 27. Tätigkeitsbericht 2016 unter Nr. 3.6.1 bereits dargelegt habe, halte ich es für wichtig, dass die Entscheidung, ob ein solcher Restverdacht besteht, nachvollziehbar dokumentiert wird. Das Innenministerium ist zwischenzeitlich meiner Auffassung gefolgt und hat die einschlägigen Verwaltungsvorschriften um einen entsprechenden Passus ergänzt.

In meinem 27. Tätigkeitsbericht 2016 unter Nr. 3.6.6 habe ich außerdem darüber berichtet, dass ein Polizeipräsidium meine Anregung aufgenommen hat, die Regelspeicherfrist im Kriminalaktennachweis auf zwei Jahre zu reduzieren, wenn Jugendliche oder Heranwachsende erstmals wegen strafbaren Erwerbs oder Besitzes von geringen Mengen Cannabis in Erscheinung treten. Erfreulicherweise hat sich das Innenministerium dieser Verfahrensweise im Grundsatz angeschlossen und durch eine Regelung in den entsprechenden Verwaltungsvorschriften veranlasst, dass alle Polizeiverbände in solchen Fällen verkürzte Speicherfristen festzulegen haben.

4.1.4 Einsatz der Software „iFinder“

Die Ausgangslage dürfte auch vielen privaten Nutzinnen und Nutzern von EDV-Geräten bekannt sein: Während man früher durch begrenzte Speicherkapazitäten diszipliniert wurde, nicht alles zu speichern, gibt es heute nahezu keinerlei Beschränkungen mehr in dieser Hinsicht. Eine Begleiterscheinung dieser neu gewonnenen Freiheit liegt darin, dass man gerade dringend benötigte Dokumente und dazugehörige Begleitinformationen im vermeintlichen Dschungel der elektronischen Ablage nicht oder nicht sofort auffindet. Aussichtslos kann die Suche sein, wenn in großen elektronischen Netzwerken von vielen Beschäftigten unübersehbare Datenmengen verarbeitet und analysiert werden sollen. Für solche Big-Data-Szenarien bedient man sich im professionellen Umfeld daher spezieller Recherchesoftware.

Im Rahmen einer Prüfung bei einer Fachabteilung des Bayerischen Landeskriminalamts wurde ich zufällig auf die Verwendung eines derartigen Tools namens „iFinder“ aufmerksam. Bei der Software „iFinder“ handelt es sich um eine nach Angaben der entwickelnden Firma „intelligente, hochskalierbare und äußerst leistungsfähige Suchlösung“, die eine dokumenten- und verzeichnisübergreifende Volltextsuche in (polizeilichen) Datenbeständen ermöglicht.

In datenschutzrechtlicher Hinsicht stellte sich mir die Frage, ob diese Software möglicherweise imstande ist – eventuell auch unbeabsichtigt – festgelegte Nutzungsbeschränkungen, insbesondere eingerichtete Zugangsberechtigungen, zu umgehen. Die Behörde legte mir im Rahmen eines Vor-Ort-Termins dar, dass die Software „iFinder“ nur innerhalb einer Fachabteilung genutzt werde, die mit der strategischen und operativen Auswertung von Informationen zu terroristischen Straftaten und der entsprechenden Informationssteuerung befasst sei. Außerdem

werde das Trefferbild einer Suchanfrage ausschließlich aus Datensätzen generiert, für die der jeweilige Anwender aufgrund seiner Funktion mit entsprechenden Zugriffsrechten ausgestattet sei.

Im Ergebnis kam ich zu dem Schluss, dass der derzeitige Einsatz dieser aus Sicht des Datenschutzes möglicherweise riskanten Software zur Auswertung von Massendaten beim Bayerischen Landeskriminalamt im zugrunde liegenden Fall datenschutzrechtlich vertretbar ist. Gleichwohl habe ich gegenüber der Behörde sowie dem Innenministerium zum Ausdruck gebracht, dass der Einsatz von derartigen Suchsystemen bestehende Nutzungsbeschränkungen nicht umgehen darf. Ich habe das Bayerische Landeskriminalamt daher gebeten, den Verwendungsrahmen der Software „iFinder“ schriftlich in Form einer Errichtungsanordnung festzuhalten und mich über weitere Entwicklungen auf dem Laufenden zu halten.

4.2 Polizeiliche Ermittlungen

4.2.1 Beanstandung wegen unverhältnismäßiger Datenerhebungen

Der rechtsstaatliche Grundsatz der Verhältnismäßigkeit ist auch bei der polizeilichen Sachverhaltsaufklärung zu beachten. Er setzt hier insbesondere der Erhebung personenbezogener Daten Grenzen. In Einzelfällen verlässt der behördliche „Erkenntnisdrang“ auch einmal den Rahmen des Zulässigen, wie ich anlässlich einer Eingabe feststellen musste.

Aufgrund eines anonymen Hinweises auf eine angebliche Nötigung bei der privaten Vermietung von Wohnungen setzte eine bayerische Polizeibehörde gegen einen bei ihr beschäftigten Beamten umfangreiche Hintergrundermittlungen in Gang. Unter anderem kam es zu Bestandsdatenabfragen bei Internet- und E-Mail-Providern, zu Rufnummernabfragen bei einem Telefonnetzbetreiber sowie zu einer Abfrage von Kontodaten. Hierbei wurden nicht nur Daten des in Verdacht geratenen Polizeibeamten, sondern auch seiner Ehefrau gezielt erhoben. Ohne jemals im Verlauf der Ermittlungen auch an den Beschuldigten selbst herangetreten zu sein, übermittelte die Polizeibehörde das Ergebnis ihrer Ermittlungen mit der Bitte um strafrechtliche Prüfung an die zuständige Staatsanwaltschaft. Diese sah von einer weiteren Verfolgung ab beziehungsweise stellte das Verfahren kurzerhand ein. Erst als sich der Polizeibeamte im Rahmen eines Disziplinarverfahrens mit den Ergebnissen der geschilderten Ermittlungsmaßnahmen konfrontiert sah, erlangte er Kenntnis von den umfangreichen Datenerhebungen.

Eine solche Intensität der polizeilichen Recherchen ist nach meiner Einschätzung eher bei Finanzermittlungen mit Bezug zu organisierten kriminellen Strukturen als bei der Aufklärung eines anonymen Hinweises auf eine mögliche Nötigung von Mietern angebracht. Insbesondere die Kontodatenabfrage zulasten des Polizeibeamten und seiner Ehefrau habe ich als schwerwiegenden, nicht gerechtfertigten Grundrechtseingriff gewertet.

Auch in Bezug auf die „Heimlichkeit“ aller durchgeführten Datenerhebungen konnte ich dem Argument der ermittelnden Polizeidienststelle hinsichtlich einer pauschal unterstellten „möglichen Zeugenbeeinflussung“ durch den Beschuldigten nicht folgen, da sich dafür keinerlei belastbare Hinweise ergaben. Außerdem bezog sich keine der Recherchen auf „flüchtige Daten“, die man selbst im Fall ei-

nes unkooperativen Verhaltens des Tatverdächtigen nicht nachträglich – insbesondere in Absprache mit der zuständigen Staatsanwaltschaft – noch hätte erheben können.

Ich habe die von der Polizeibehörde betriebene Sachverhaltsaufklärung im Einzelfall datenschutzrechtlich beanstandet. Für zukünftige vergleichbare Fälle habe ich der Polizeibehörde empfohlen, künftig möglichst frühzeitig eine Einbindung der zuständigen Staatsanwaltschaft herbeizuführen und weitreichende Ermittlungsschritte sorgfältig abzustimmen. Auch wenn an Polizeibeamtinnen und Polizeibeamte hinsichtlich ihres außerdienstlichen Verhaltens strengere Anforderungen zu stellen sind als an Beschäftigte in den meisten anderen Verwaltungszweigen, gilt der Grundsatz der Verhältnismäßigkeit auch für sie, erst recht aber für ihre Familienmitglieder.

4.2.2 Informatorische Befragung bei Beschuldigten

Immer wieder ist festzustellen, dass es bei der Unterscheidung zwischen der förmlichen Vernehmung eines oder einer Beschuldigten und der informatorischen Befragung einer Person, die (noch) nicht beschuldigt ist, in der polizeilichen Praxis zu Unsicherheiten kommt.

In einem von mir geprüften Fall rief eine Mitarbeiterin eines Wohnheims die Polizei, da aus dem Zimmer eines Bewohners Marihuanageruch dringe. Die eingetroffenen Beamten stellten in dem stark verqualmten Zimmer ebenfalls Marihuanageruch fest. Einer der zwei Zimmerinsassen hatte stark gerötete Augen. Laut Sachverhaltsbericht der Polizei wurden die beiden Personen „informatorisch befragt“, ob sie noch weitere Betäubungsmittel besäßen, und das Zimmer wurde durchsucht. Trotz dieser polizeilichen Maßnahmen wurden die beiden Personen weiterhin nicht über ihre Beschuldigtenrechte belehrt.

Auch an einem weiteren Beispiel zeigen sich die Unsicherheiten, die bei diesem Thema bestehen. So stieß ich im Rahmen einer Prüfung auf einen Ermittlungsbericht, in dem von einer „informatorischen Befragung“ der „Beschuldigten“ die Rede war.

Problematisch ist eine fehlerhafte Bewertung im Rahmen einer polizeilichen Befragung deshalb, weil nach § 136 Abs. 1 Strafprozessordnung (StPO) Beschuldigte vor einer Befragung über ihre Beschuldigtenrechte belehrt werden müssen, was bei einer rein informatorischen Befragung gerade nicht erforderlich ist.

§ 136 StPO
(1) [1]Bei Beginn der ersten Vernehmung ist dem Beschuldigten zu eröffnen, welche Tat ihm zu Last gelegt wird und welche Strafvorschriften in Betracht kommen. [2]Er ist darauf hinzuweisen, daß es ihm nach dem Gesetz freistehe, sich zu der Beschuldigung zu äußern oder nicht zur Sache auszusagen und jederzeit, auch schon vor seiner Vernehmung, einen von ihm zu wählenden Verteidiger zu befragen. [3]Möchte der Beschuldigte vor seiner Vernehmung einen Verteidiger befragen, sind ihm Informationen zur Verfügung zu stellen, die es ihm erleichtern, einen Verteidiger zu kontaktieren. [4]Auf bestehende anwaltliche Notdienste ist dabei hinzuweisen.[5]Er ist ferner darüber zu belehren, daß er zu seiner Entlastung einzelne Beweiserhebungen beantragen und unter den Voraussetzungen des § 140 Absatz 1 und 2 die Bestellung eines Verteidigers nach Maßgabe des § 141 Absatz 1 und 3

beanspruchen kann; zu Letzterem ist er dabei auf die Kostenfolge des § 465 hinzuweisen. [6]In geeigneten Fällen soll der Beschuldigte auch darauf, dass er sich schriftlich äußern kann, sowie auf die Möglichkeit eines Täter-Opfer-Ausgleichs hingewiesen werden.

Diese Belehrung soll sicherstellen, dass ein Beschuldigter oder eine Beschuldigte nicht im Glauben an eine vermeintliche Aussagepflicht Angaben macht und sich damit unfreiwillig selbst belastet. Die informatorische Befragung einer bereits unter Straftatenverdacht stehenden Person ist unzulässig; dabei gewonnene Erkenntnisse sind grundsätzlich unverwertbar. Entscheidend für die Beurteilung, von welchem Zeitpunkt an die Belehrung nach § 136 Abs. 1 Satz 2 StPO erforderlich ist, ist einerseits die Stärke des Tatverdachts, der gegenüber der befragten Person gehegt wird. Hierbei hat die Polizei einen Beurteilungsspielraum, der nicht mit dem Ziel missbraucht werden darf, den Zeitpunkt der erforderlichen Belehrung möglichst weit hinauszuschieben. Daneben ist zum anderen von Bedeutung, wie sich das Verhalten der Polizei aus Sicht des oder der Befragten darstellt. Polizeiliche Verhaltensweisen wie beispielsweise die Durchsuchung der Wohnung einer von der Befragung betroffenen Person belegen schon ihrem äußeren Befund nach, dass die Polizei dem oder der Befragten als beschuldigter Person begegnet. Den betroffenen Polizeibehörden habe ich daher nahegelegt, die geschilderte Thematik intern aufzuarbeiten.

4.3 Heraufsetzung der Höchstspeicherfrist bei polizeilicher Videoüberwachung

Wie bei vielen polizeilichen Maßnahmen ist auch bei der Videoüberwachung zu beachten, dass die Intensität des bewirkten Grundrechtseingriffs von dessen Dauer abhängt. Wer einen von der Polizei videoüberwachten Bereich durchquert, ist scheinbar nur für einen minimalen Zeitraum von dieser Maßnahme betroffen. Werden die Aufnahmen aber gespeichert, kann sich die Eingriffsintensität erheblich erhöhen.

Aus datenschutzrechtlicher Sicht ist es daher bedauerlich, dass im Rahmen des Gesetzes zur effektiveren Überwachung gefährlicher Personen (Einzelheiten unter Nr. 4.1.1) die gesetzlich im Polizeiaufgabengesetz (PAG) verankerte Höchstspeicherfrist für polizeiliche Bild- und Tonaufnahmen oder -aufzeichnungen von höchstens drei Wochen auf maximal zwei Monate ausgedehnt wurde.

In der Folge dauerte es auch nicht lange, bis verschiedene Polizeipräsidien ihre Speicherfristen, die nach meinem Eindruck im Durchschnitt bei zwei Wochen lagen, auf drei oder sogar vier Wochen erhöhten. Dies ist für mich nicht nachvollziehbar. Denn losgelöst von der gesetzlichen Höchstspeicherdauer bemisst sich eine angemessene Speicherdauer von Videoaufzeichnungen nach dem Gebot der Erforderlichkeit. So ist mir aufgrund meiner umfassenden Prüfpraxis kein Vorgang bekannt, in dem die Polizei längere als die bisherigen Speicherfristen benötigt hätte, um in einem Fall von wesentlicher Bedeutung ihrer Aufgabenstellung gerecht werden zu können. Schließlich können Aufzeichnungen, die mit konkreten Straftaten in Verbindung zu bringen sind, ohnehin sofort als Beweismittel in das jeweilige Strafverfahren einfließen und unterliegen dann nicht mehr den Vorgaben des Polizeiaufgabengesetzes.

Vor dem Hintergrund, dass die Videoüberwachung öffentlicher Bereiche in den letzten Jahren erheblich ausgebaut wurde, Polizeistreifen in naher Zukunft kaum

mehr ohne Body-Cams anzutreffen sind und zugleich eine immer höher entwickelte Videotechnik zum Einsatz kommt, bedarf es nach meiner Ansicht dringend ausgleichender Korrektive. Eine polizeiliche (Selbst-)Beschränkung im Sinne einer sehr eng am Gebot der Erforderlichkeit orientierten Festlegung der Speicherfrist kann einen solchen Ausgleich bewirken helfen. Die konkrete Festlegung der Speicherfristen bei einzelnen polizeilichen Videoüberwachungsmaßnahmen werde ich daher weiter kritisch begleiten.

4.4 Speicherungen in polizeilichen Dateien

4.4.1 Prüfung der Speicherungsvoraussetzung „polizeilicher Restverdacht“

Im Anschluss an frühere Prüfungen (siehe meinen 27. Tätigkeitsbericht 2016 unter Nr. 3.6.1 und Nr. 3.6.5 sowie meinen 26. Tätigkeitsbericht 2014 unter Nr. 3.5.3 und Nr. 5.3.5) habe ich abermals (anlassunabhängig) bei drei Polizeipräsidien polizeiliche Speicherungen auf ihre Zulässigkeit hin kontrolliert. Mein Augenmerk richtete sich darauf, ob die Polizei Personen als Beschuldigte speichert, obwohl die zuständige Staatsanwaltschaft ausdrücklich festgestellt hat, dass die betroffenen Personen unschuldig sind, beziehungsweise dass gegen sie kein begründeter Verdacht einer Straftat (mehr) besteht.

Wesentliche Voraussetzung dafür, eine Person als Beschuldigten zu speichern, ist, dass gegen sie ein sogenannter polizeilicher Restverdacht besteht (siehe zu diesem Begriff mein 27. Tätigkeitsbericht 2016 unter Nr. 3.6.5). Ein solcher Restverdacht ist bei den oben genannten Feststellungen der Staatsanwaltschaft gerade nicht begründbar. Dennoch konnte ich bei meiner Prüfung erneut mehrere Fälle auffinden, in welchen trotz der beschriebenen staatsanwaltschaftlichen Entscheidungen die entsprechenden polizeilichen Speicherungen nicht ausreichend berichtigt worden waren. Teilweise hatten die Polizeipräsidien im Vorgangsverwaltungssystem den Beschuldigtenstatus nicht geändert, teilweise hatten sie den Ausgang des Verfahrens nicht vermerkt. In drei dieser Fälle lag sogar eine Speicherung als Beschuldigter im Kriminalaktennachweis vor.

Die Ursachen für diese Fehlspeicherungen lagen teilweise in der unzureichenden Übermittlung der Einstellungsbegründung durch die zuständige Staatsanwaltschaft an die Polizei, teilweise wurden die Einstellungsbegründungen aber auch einfach nicht beachtet.

Die geprüften Polizeipräsidien haben die von mir gerügten fehlerhaften Eintragungen berichtigt. Für die Zukunft habe ich das Innenministerium gebeten, die nachgeordneten Polizeibehörden regelmäßig auf die Beachtung der von mir kritisierten Punkte hinzuweisen. Das Innenministerium hat seinerseits wesentliche Verbesserungen bei der Informationsweitergabe von den Staatsanwaltschaften an die Polizei in Aussicht gestellt. So haben das Innen- sowie das Justizministerium eine Arbeitsgruppe initiiert, die mittelfristig eine elektronische Schnittstelle zur direkten Übermittlung und Übernahme des Verfahrensausgangs in die polizeiliche Vorgangsverwaltung umsetzen soll.

4.4.2 Verzicht auf Speicherung im Kriminalaktennachweis bei Nachbarschaftsstreitigkeiten

Nachbarschaftsstreitigkeiten sind oftmals Anlass für ein polizeiliches Einschreiten. Regelmäßig geht es dabei nicht um schwerwiegende und die Öffentlichkeit verunsichernde Delikte. Oftmals werden wechselseitig begangene Beleidigungen oder Tätlichkeiten auch wechselseitig zur Anzeige gebracht. Die Polizei legt für diese Vorfälle gewöhnlich einen Kriminalaktennachweis (KAN) an.

Anschließend können diese Vorfälle von jeder bayerischen Polizeidienststelle abgerufen werden. Der Kriminalaktennachweis dient der Informationsgewinnung für Zwecke der Strafverfolgung sowie der Gefahrenabwehr. Solche Speicherungen sind legitim, sofern es sich um Fälle ernstzunehmender Kriminalität handelt, die über die jeweiligen Zuständigkeitsgrenzen hinaus von Bedeutung sein können. In vielen Bagatellfällen fehlt es aber an einer überörtlichen Relevanz aber gerade. Die Polizei sollte bei Nachbarschaftsstreitigkeiten deshalb darauf achten, dass erstattete Strafanzeigen nicht zu einer unangebrachten „Kriminalisierung" der Beteiligten führen.

Aus datenschutzrechtlicher Sicht habe ich daher positiv zur Kenntnis genommen, dass eine Polizeidienststelle aus den vorgenannten Gründen selbständig und bewusst auf Einträge im Kriminalaktennachweis verzichtet hat, wenn es um geringfügige Tatvorwürfe im Zusammenhang mit Nachbarschaftsstreitigkeiten geht. So unterblieben mehrjährige KAN-Speicherungen zu den beschuldigten Personen. Die Vorfälle wurden lediglich in der polizeilichen Vorgangsverwaltung (IGVP) registriert. Dieses Vorgehen wird auch dem Grundsatz der „Datenminimierung" (Art. 5 Abs. 1 Buchst. c DSGVO) gerecht, der über die Verweisung in Art. 28 Abs. 2 Nr. 2 BayDSG auch für die Polizei gilt und einen sparsamen Umgang mit erlangten personenbezogenen Daten fordert.

Ich hoffe, dass sich weitere bayerische Polizeidienststellen an diesem datenschutzfreundlichen Vorbild orientieren.

4.4.3 Auswirkungen der sogenannten „Mitziehklausel"

Im Rahmen meiner oben genannten Stellungnahme zur Neufassung des Polizeiaufgabengesetzes (PAG) habe ich mich, leider ohne Erfolg, für die Streichung der sogenannten „Mitziehklausel" des Art. 38 Abs. 2 Satz 6 Polizeiaufgabengesetz in der bis zum 24. Mai 2018 geltenden Fassung (PAG-alt; jetzt Art. 54 Abs. 2 Satz 6 PAG) ausgesprochen. Nach dieser Regelung verlängert eine neue polizeiliche Speicherung die Speicherdauer aller „alten" Speicherungen, da sich die Speicherdauer für alle Speicherungen nach der längsten Speicherfrist richtet. Dies halte ich aus verschiedenen Gründen für problematisch. So kann diese Regelung etwa dazu führen, dass die Polizei eine Eintragung länger speichert als die zugrundeliegende Verfahrensakte bei der Staatsanwaltschaft aufzubewahren ist. Zudem werden aufgrund der Mitziehklausel teilweise Jugendverfehlungen oder strafrechtlich nicht nachzuweisende Taten über sehr lange Zeiträume gespeichert.

Art. 38 PAG-alt
Speicherung, Veränderung und Nutzung von Daten
(2) [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, verändern und nutzen,

soweit dies zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. […] [3]Die nach Art. 37 Abs. 3 festzulegenden Prüfungstermine oder Aufbewahrungsfristen betragen in der Regel bei Erwachsenen zehn Jahre, bei Jugendlichen fünf Jahre und bei Kindern zwei Jahre (Regelfristen). [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, […]. [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.

Aufgrund ihrer Auswirkungen für die Betroffenen ist in Fällen, in denen die Mitziehautomatik greift, eine besondere Sorgfalt an den Tag zu legen, wenn es darum geht, die Speicherdauer polizeilicher Eintragungen festzulegen. Einer Veranschaulichung der Thematik dienen die beiden nachfolgenden Praxisbeispiele:

Ein Petent hatte eine Speicherung aus dem Jahr 2003 wegen gefährlicher Körperverletzung. 2012 – also ein Jahr vor Löschung der gefährlichen Körperverletzung – kam eine Speicherung wegen Beleidigung dazu. Laut der Polizei sollten beide Eintragungen bis 2022 gespeichert werden, weil die Speicherfrist bei Erwachsenen grundsätzlich zehn Jahre beträgt und im Jahr 2012 für die Beleidigung zu laufen begann. Im Rahmen meiner Prüfung stellte sich heraus, dass es sich bei der Beleidigung um einen Fall von geringerer Bedeutung handelte, der eine verkürzte Speicherfrist von fünf Jahren ermöglichte. Beide Speicherungen wurden daher mit Ablauf des Jahres 2017 aus dem Kriminalaktennachweis gelöscht.

Der Fall zeigt, wie wichtig es ist, ein besonderes Augenmerk auf die gesetzlichen Speicherverkürzungsmöglichkeiten zu legen, um die Folgen der Mitziehklausel etwas einzudämmen.

In einem anderen Fall wurde ein Petent 2009 als Siebzehnjähriger wegen des Besitzes einer geringen Menge Cannabis (0,1 Gramm) und des Missbrauchs von Ausweispapieren polizeilich gespeichert, mit dem Personenhinweis „BtM-Konsument“ versehen und erkennungsdienstlich behandelt. Eigentlich wären die Eintragungen, da der Petent zum Tatzeitpunkt Jugendlicher war, nach fünf Jahren, also 2014, zu löschen gewesen. Im Jahr 2013 allerdings wurde der Petent als Teilnehmer einer Sachbeschädigung und eines Hausfriedensbruchs im Kriminalaktennachweis (KAN) gespeichert. Aufgrund der Mitziehklausel wäre er wegen einer einmaligen Jugendverfehlung somit bis 2023, also bis zu seinem 32. Lebensjahr, als „BtM-Konsument“ gespeichert worden. Im Rahmen meiner Prüfung zeigte sich, dass der Geschädigte der Sachbeschädigung und des Hausfriedensbruchs kein Interesse an einer Strafverfolgung hatte und die Speicherung des Vorwurfes aus dem Jahr 2013 im Kriminalaktennachweis von der Polizei nicht weiter benötigt wurde. Alle Speicherungen im Kriminalaktennachweis, der Personenhinweis „BtM-Konsument“ und die erkennungsdienstlichen Unterlagen wurden daher gelöscht.

Auch hier wird deutlich, welche Auswirkungen die Mitziehautomatik haben kann und wie wichtig es daher ist, polizeiliche Speicherungen, die andere ältere Speicherungen verlängern, stets einer genauen Betrachtung zu unterziehen.

4.4.4 Speicherung wegen BtM-Delikt ohne Vorliegen eines Anfangsverdachts

„Ich und Drogenhandel?!“ Aus allen Wolken fiel eine antragstellende Person, als sie im Rahmen einer Akteneinsicht zu einem belanglosen Nachbarschaftsstreit zufällig auf einen entsprechenden polizeilichen Vermerk stieß. Darin teilte eine Polizeiinspektion der Staatsanwaltschaft die Erkenntnis mit, dass vor neun Jahren gegen dieselbe Person bereits wegen des Verdachts des Handels mit Betäubungsmitteln ermittelt worden war.

Die betroffene Person hatte von den polizeilichen Ermittlungen, die auf einem vagen anonymen Hinweis beruhten, nie etwas erfahren. Die Staatsanwaltschaft hatte die Ermittlungen rasch beendet und die Polizei darauf aufmerksam gemacht, dass im konkreten Fall kein Anfangsverdacht für eine verfolgbare Straftat vorliege.

Dennoch wurde die Person, ohne davon Kenntnis zu haben, über Jahre mit diesem nicht unerheblichen Tatvorwurf in polizeilichen Dateien gespeichert. Es kann zwar zulässig sein, dass die Polizei auch Erkenntnisse aus eingestellten Strafverfahren zunächst einmal behält. Allerdings gilt dies nicht in Fällen, in denen die Staatsanwaltschaft – immerhin Herrin des Ermittlungsverfahrens – den Anfangsverdacht einer verfolgbaren Straftat für nicht gegeben erachtet.

Der Praxisfall führt vor Augen, wie leicht Bürgerinnen und Bürger in polizeiliche Dateien geraten und darin verbleiben können, ohne davon auch nur ansatzweise etwas zu wissen.

Als positiven Aspekt möchte ich nicht unerwähnt lassen, dass das zuständige Polizeipräsidium die Speicherung auf meine Anfrage hin als rechtlich nicht haltbar erkannte und aus eigenem Antrieb die datenschutzrechtlich gebotenen Maßnahmen, insbesondere eine unverzügliche Löschung, veranlasste.

Vor dem Hintergrund dieses Falles empfehle ich, in Zweifelsfällen das gesetzlich vorgesehene Auskunftsrecht (Art. 65 Polizeiaufgabengesetz) zu nutzen.

Weitere Informationen zu Auskunftsrechten gegenüber den bayerischen öffentlichen Stellen sind auf meiner Homepage https://www.datenschutz-bayern.de in der Rubrik „Themengebiete – Polizei – Speicherung personenbezogener Daten durch die Polizei“ zu finden.

4.5 Datenübermittlungen

4.5.1 Pressemitteilung über einen Geschwindigkeitsverstoß

Die Grundsätze zur datenschutzkonformen Pressearbeit der Polizei habe ich bereits in meinem 24. Tätigkeitsbericht 2010 unter Nr. 3.6 dargelegt. Meiner Auffassung nach kann eine personenidentifizierende Pressearbeit der Polizei regelmäßig nur bei Verbrechen, insbesondere bei Fällen der Gewaltkriminalität, in Betracht kommen. Ansonsten ist eine personenidentifizierende Pressearbeit datenschutzrechtlich allenfalls dann vertretbar, wenn besondere Kriterien hinzukommen, die ein überwiegendes Interesse der Öffentlichkeit an der Berichterstattung begründen.

Im Rahmen meiner Tätigkeit stoße ich immer wieder auf Fälle, in denen diese Grundsätze nicht beachtet wurden. So wurde ich etwa im Berichtszeitraum auf Zeitungsartikel aufmerksam, in denen ein Geschwindigkeitsverstoß einer Angehörigen eines europäischen Adelshauses geschildert wurde. Wie ich feststellen konnte, war Ausgangspunkt für den Zeitungsbericht eine Pressemitteilung der zuständigen Verkehrspolizeiinspektion. In dieser Pressemitteilung wurde nicht nur der Geschwindigkeitsverstoß beschrieben, sondern es wurden zusätzlich auch der Anfangsbuchstabe des Nachnamens der betroffenen Person, ihr Alter sowie insbesondere ihre Zugehörigkeit zum Hochadel eines bestimmten Landes erwähnt. Damit war für die Allgemeinheit die Identifizierbarkeit der betroffenen Person gegeben.

Das zuständige Polizeipräsidium teilte mir mit, Zweck der Pressemitteilung sei es gewesen, durch die Darstellung von eklatanten Verkehrsverstößen die Öffentlichkeit zu sensibilisieren und mit dem Hinweis auf verstärkte Kontrollmaßnahmen für eine erhöhte Verkehrssicherheit zu sorgen. Gleichwohl sei man aber auch der Auffassung, dass der Informationsgehalt der Pressemitteilung für die Öffentlichkeit nicht beeinträchtigt worden wäre, wären die Individualisierungsmerkmale nicht benannt worden. Das Polizeipräsidium hat daher die zuständige Verkehrspolizeiinspektion darauf hingewiesen, künftig bei Pressemitteilungen auf eine datenschutzrechtlich gebotene Anonymisierung zu achten.

4.5.2 Übermittlung eines ungeschwärzten Auszugs aus einem Haftbuch der Polizei

Als überraschend auskunftsfreudig erwies sich ein Polizeipräsidium bei der Aktenvorlage an ein Amtsgericht: Der Betroffene einer Ingewahrsamnahme erstrebte die nachträgliche gerichtliche Überprüfung seiner von der Polizei angeordneten Freiheitsentziehung. Das Polizeipräsidium legte dem zuständigen Amtsgericht die entsprechenden Akten vor. Übermittelt wurde dabei unter anderem die Kopie eines Auszuges aus dem sogenannten Haftbuch. Das Haftbuch dokumentiert, welche Personen sich zu welchem Zeitpunkt und aus welchen Gründen in den Hafträumen der betreffenden Polizeidienststelle aufhielten.

Obwohl dem Gericht lediglich die Umstände der Freiheitsentziehung der antragstellenden Person darzulegen waren, blieben auf der Kopie die Daten von sieben anderen vorübergehend in Gewahrsam genommenen Personen ungeschwärzt. Eine Anonymisierung wäre insofern notwendig gewesen, weil Angaben zu anderen Personen als dem Antragsteller keinerlei Bedeutung für die nachträgliche richterliche Kontrolle hatten. Insbesondere kamen diese anderen Personen aufgrund des fehlenden zeitlichen Bezugs auch nicht als Zeugen für das konkrete Verfahren in Betracht. Die ungeschwärzte Kopie gelangte im Rahmen der Akteneinsicht an die eingangs erwähnte antragstellende Person. Diese konnte dadurch selbst einen Einblick gewinnen, wer sonst noch aus welchen Gründen in Hafträumen der Polizeidienststelle festgehalten worden war.

Von der Sorge motiviert, dass auch die eigenen Haftdaten auf vergleichbare Weise im Rahmen einer Akteneinsicht an Dritte übermittelt werden könnten, wandte sich die betroffene Person an mich und bat um eine datenschutzrechtliche Prüfung dieses Sachverhalts.

Das um eine Stellungnahme gebetene Polizeipräsidium räumte ein, dass eine ungeschwärzte Kopie versehentlich in die bei Gericht vorgelegte Akte gelangt war.

Auch nach meiner Einschätzung handelte es sich um einen Fehler im Einzelfall und nicht um ein strukturelles Problem. Gleichwohl habe ich dem Polizeipräsidium mitgeteilt, dass ich den Vorgang in datenschutzrechtlicher Hinsicht sehr ernst nehme. Schließlich waren die Daten von sieben anderen Personen unnötig weitergegeben worden. Das damit befasste Polizeipräsidium teilte meine kritische Bewertung des Sachverhalts und berichtete mir von konstruktiven Maßnahmen zur internen Aufarbeitung des Vorgangs.

4.5.3 „Überschießende" Datenübermittlung mittels unverschlüsselter E-Mail

Eine Petentin teilte mir mit, österreichische Behörden seien zur Ermittlung ihrer Wohnanschrift mit unverschlüsselter E-Mail unter Nennung ihres Namens sowie des Hintergrunds der Anfrage an die „Kontaktstelle Grenze der Bayerischen Polizei" herangetreten. Der weitere Schriftverkehr erfolgte auch von deutscher Seite per unverschlüsselter E-Mail, wobei auch Daten (insbesondere frühere Wohnsitze der Petentin) übermittelt wurden, die weder angefragt noch erkennbar für die Sachbearbeitung erforderlich waren. Eine E-Mail schloss mit dem Satz: „Sonst keine weiteren polizeilichen Erkenntnisse."

Öffentliche Stellen haben bei der Verarbeitung personenbezogener Daten technische und organisatorische Maßnahmen zum Schutz dieser Daten zu treffen. Außerdem bedarf die Übermittlung eines jeden einzelnen personenbezogenen Datums einer Rechtfertigung. Die Datenübermittlung muss insbesondere erforderlich sein.

Ich habe das betroffene Polizeipräsidium darauf hingewiesen, dass personenbezogene Daten an andere Behörden, besonders wenn sich diese im Ausland befinden, per E-Mail ausschließlich verschlüsselt und nur im erforderlichen Umfang übermittelt werden dürfen. Auch habe ich das Polizeipräsidium gebeten, die Beschäftigten entsprechend zu sensibilisieren. Bei einer Datenanforderung kann nicht ohne weiteres davon ausgegangen werden, dass die anfragende Behörde über die angefragten Daten hinaus weitere Daten benötigt. Ein Zusatz, der Rückschlüsse darauf zulässt, ob bei der Daten übermittelnden Behörde weitere Erkenntnisse vorliegen (sogenannte Negativauskunft) stellt ebenfalls ein personenbezogenes Datum dar, das nicht grundlos übermittelt werden darf.

4.5.4 Erstellung eines Lagebildes Bayern zur sogenannten „Reichsbürgerbewegung in Bayern"

Als Reaktion auf die tödlichen Schüsse eines sogenannten „Reichsbürgers" auf Polizeibeamte im Oktober 2016 und weiterer bereits im Vorfeld bekannt gewordener Sicherheitsstörungen führte das Innenministerium ein Meldeverfahren mit dem erklärten Ziel ein, Kenntnis von allen der „Reichsbürgerbewegung" zugehörigen Personen zu erlangen und von diesem Personenkreis ausgehende Gefahren zu unterbinden (beispielsweise durch die Versagung von Waffen- oder sonstigen sicherheitsrechtlichen Erlaubnissen, die eine Zuverlässigkeit des Erlaubnisinhabers voraussetzen). Hierfür wurden alle Behörden aufgefordert, anfallende Erkenntnisse zu „Reichsbürgern" an die jeweiligen Polizeipräsidien als zentrale Ansprechpartner zu übermitteln, um dort eine entsprechende Überprüfung vornehmen zu lassen.

Dieses Meldeverfahren, das bezüglich der Polizei im Wesentlichen auf den entsprechenden Rechtsgrundlagen im Polizeiaufgabengesetz (Art. 42 PAG-alt beziehungsweise Art. 60 PAG) beruht, habe ich angesichts des oben erwähnten Anlasses im Grundsatz mitgetragen. Gleichzeitig habe ich aber unter anderem darauf hingewiesen, dass entsprechende Mitteilungen an die Polizei nur unter Beachtung der Verhältnismäßigkeit im engeren Sinn zulässig sind und insbesondere die Einstufung als „Reichsbürger" bereits von der übermittelnden Stelle auf eine hinreichend konkrete Tatsachenbasis gestützt sein muss. Des Weiteren habe ich angemerkt, dass die Einhaltung von besonderen Übermittlungsvoraussetzungen und besonderen Schweigepflichten zu beachten ist. Bezüglich der konkreten Ausgestaltung des Meldeverfahrens stehe ich nach wie vor in Kontakt mit dem Innenministerium. Hierbei werde ich weiterhin darauf achten, dass datenschutzrechtliche Belange ausreichend berücksichtigt werden.

4.6 Auskunftsrecht

Sie möchten wissen, welche Informationen bei der Bayerischen Polizei über Sie gespeichert sind? Dann können Sie einen Antrag auf Auskunft nach Art. 65 Polizeiaufgabengesetz (PAG) stellen. Diese Vorschrift wurde im Rahmen der Polizeirechtsreform (siehe Nr. 4.1.1) überarbeitet und im Ergebnis datenschutzfreundlicher als ihre Vorgängernorm (Art. 48 PAG-alt) gestaltet. Angesichts der Vielzahl von Dateien, die von der Polizei zur Erfüllung ihrer Aufgaben vorgehalten werden, dient dieses spezialgesetzliche Auskunftsrecht dazu, das Handeln der Polizei transparenter und nachvollziehbarer zu machen. Die Bürgerinnen und Bürger sollen grundsätzlich erfahren können, was die Polizei über sie weiß.

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

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

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

1. *die Erfüllung polizeilicher Aufgaben gefährdet oder wesentlich erschwert würde,*
2. *die öffentliche Sicherheit oder Ordnung gefährdet würde oder*

3. die im Einzelfall erforderliche Geheimhaltung verarbeiteter Daten gefährdet würde und das Interesse der antragstellenden Person an der Auskunftserteilung nicht überwiegt.

So überrascht es auch nicht, dass mich zum polizeirechtlichen Auskunftsrecht im Berichtszeitraum viele Bürgereingaben erreicht haben.

Eine Anfrage bezog sich darauf, ob auch der sogenannte Kurzsachverhalt innerhalb der Vorgangsverwaltung (Integrationsverfahren Polizei – IGVP) vom gesetzlichen Auskunftsanspruch mit umfasst ist.

Für mich ist insofern maßgeblich, dass der antragstellenden Person ein gesetzlicher Anspruch auf Auskunft über die **sie** betreffenden personenbezogenen Daten zusteht. Sind mehrere Personen innerhalb eines IGVP-Vorgangs erfasst – wie dies regelmäßig der Fall ist –, so hat die auskunftsbegehrende Person allgemein nur ein Recht auf die Bekanntgabe der zu **ihrer** Person gespeicherten Daten. Folglich erstreckt sich das Auskunftsrecht nicht auf die Übermittlung fremder personenbezogener Daten, auch wenn diese zum selben Sachverhalt von der Polizei gespeichert wurden. Der Auskunftsanspruch bezieht sich also allein auf die Daten des jeweiligen Antragstellers. Sind im freitextlichen Kurzsachverhalt der Vorgangsverwaltung diverse Angaben zu mehreren Beteiligten dargelegt, so erfährt eine antragstellende Person die Passagen, welche Informationen gerade über sie enthalten. Bezieht sich der gesamte Kurztext einzig auf die antragstellende Person, so hat sie einen Anspruch auf umfassende Beauskunftung. Umfasst der Kurztext hingegen ausschließlich Informationen zu anderen Personen, hat die antragstellende Person keinen Anspruch auf eine teilweise oder gar vollständige Mitteilung des dieses Kurztextes. Der Auskunftsanspruch ist gerade kein Akteneinsichtsrecht.

Auf dieser Grundlage habe ich das Bayerische Landeskriminalamt ersucht, gegenüber Personen, die von ihrem Auskunftsrecht nach dem Polizeiaufgabengesetz Gebrauch machen, **alle zu ihrer Person** gespeicherten Daten mitzuteilen. Zumindest auf entsprechende Nachfrage sind damit gegebenenfalls auch Kurzsachverhalte aus der Vorgangsverwaltung (einzelfallbezogen ganz oder teilweise) mitzuteilen, sofern keine generellen gesetzlichen Versagungsgründe nach Art. 65 Abs. 2 PAG eingreifen.

Weitere Hinweise zum Auskunftsrecht gegenüber der Bayerischen Polizei, aber auch in Bezug auf andere bayerische öffentliche Stellen finden Sie auf meiner Homepage https://www.datenschutz-bayern.de in der Rubrik „Themengebiete – Polizei – Speicherung personenbezogener Daten durch die Polizei“.

5 Verfassungsschutz

5.1 Reform des Bayerischen Verfassungsschutzgesetzes 2018

Seit der umfassenden Novellierung des Bayerischen Verfassungsschutzgesetzes (BayVSG) im Jahr 2016 (siehe hierzu meinen Beitrag im 27. Tätigkeitsbericht 2016 unter Nr. 4.1) wurde das Gesetz im Berichtszeitraum bereits weitere zwei Male geändert.

Die **erste Änderung vom 15. Mai 2018** (GVBl. S. 230) betraf die Anpassung des Bayerischen Verfassungsschutzgesetzes an die neuen Datenschutzbestimmungen. Der Verfassungsschutz als Teil der Infrastruktur zum Schutz der nationalen Sicherheit ist zwar im Hinblick auf Art. 4 Abs. 2 Satz 3 Vertrag über die Europäische Union von der Regelungszuständigkeit der Europäischen Union ausgenommen und fällt daher weder in den Anwendungsbereich der Datenschutz-Grundverordnung (vgl. Art. 2 Abs. 2 Buchst. a DSGVO) noch in den Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz (vgl. Art. 2 Abs. 3 Buchst. a RLDSJ). Allerdings waren aufgrund der Neustrukturierung des Datenschutzrechts einige Anpassungen notwendig. Anders als bislang kommt im Bereich des Verfassungsschutzes zukünftig nicht mehr das Bayerische Datenschutzgesetz, sondern – durch Verweise hierauf – das Bundesdatenschutzgesetz zur Anwendung. Für die Tätigkeit des Bayerischen Landesamts für Verfassungsschutz wie auch des Bundesamts für Verfassungsschutz sind nun im Wesentlichen die gleichen datenschutzrechtlichen Regelungen maßgeblich. Damit soll dem Gedanken eines Verbunds der Verfassungsschutzbehörden und dem Interesse an einem einheitlichen Rechtsrahmen Rechnung getragen werden. Im Rahmen des Gesetzgebungsverfahrens konnte ich einige Klarstellungen und Ergänzungen im Gesetzestext bewirken.

Die **zweite, grundlegendere Reform vom 12. Juni 2018** (GVBl. S. 382) betraf die Anpassung des Bayerischen Verfassungsschutzgesetzes an Vorgaben, die sich aus dem Urteil des Bundesverfassungsgerichts vom 20. April 2016, Az.: 1 BvR 966/09 und 1 BvR 1140/09, BVerfGE 141, 220, ergeben. Dieses Urteil betraf das Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (sogenanntes BKAG-Urteil). Auch wenn das Urteil ausschließlich Befugnisse des Bundeskriminalamts würdigt, ist eine Übertragung der Vorgaben auf rechtliche Grundlagen für die Arbeit anderer Sicherheitsbehörden, insbesondere der Nachrichtendienste, angezeigt. Nachrichtendienstlicher Tätigkeit ist die heimliche Informationsbeschaffung geradezu immanent. Die durch die Heimlichkeit begründete besondere grundrechtliche Gefährdungslage kann im Einzelfall bei Datenerhebungen durch Nachrichtendienste sogar höher sein als bei verdeckten Maßnahmen von Polizeibehörden.

Des Weiteren sollten mit der zweiten Gesetzesänderung auch Regelungsideen des von der Innenministerkonferenz entwickelten sogenannten „harmonisierten Rechtsrahmens im Verfassungsschutzverbund“(Materialien dazu im Internet unter https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/20171207-08.html als Anlage zu TOP 29) mit Richtungsvorgaben umgesetzt werden. Die Innenministerkonferenz empfahl in ihrer Herbstsitzung 2017 Bund

und Ländern, den „harmonisierten Rechtsrahmen“ in die Überlegungen zur Novellierung ihrer jeweiligen Verfassungsschutzgesetze einzubeziehen.

Das Bayerische Staatsministerium des Innern, für Sport und Integration beteiligte mich frühzeitig an dem Reformvorhaben. Ich erhielt mehrfach die Gelegenheit, zum Gesetzentwurf (Landtags-Drucksache 17/20763) Stellung zu beziehen. Mein Hauptaugenmerk legte ich dabei auf datenschutzrechtliche Defizite, welche die Novellierung mit sich brachte oder nicht beseitigte. Vor allem folgende Punkte sah ich kritisch:

— Das Bundesverfassungsgericht fordert eine umfassende Protokollierungspflicht, „die es ermöglicht, die jeweiligen Überwachungsmaßnahmen sachhaltig zu prüfen“. Gerade für den Einsatz nachrichtendienstlicher Mittel halte ich aufgrund des hohen Eingriffsgewichts eine umfassende und detaillierte Protokollierungsregelung für angezeigt. Eine entsprechende Protokollierungspflicht fehlt bislang im Bayerischen Verfassungsschutzgesetz. Eine Dokumentation zumindest des angewandten Mittels, der verantwortlichen Stelle, von Ort, Zeitpunkt und Dauer der Anwendung, der Zielperson sowie erheblich mitbetroffener Personen, ferner der erhobenen personenbezogenen Daten und ihrer Weiterverarbeitung sowie des wesentlichen Ergebnisses der Maßnahme ist notwendig.

— Gleiches gilt für die Protokollierung von Datenübermittlungen des Bayerischen Landesamts für Verfassungsschutz an Drittstaaten und internationale Organisationen, um eine sachgerechte Kontrolle dieser Datenübermittlungen sicherzustellen. Was den Umfang der Protokollierung betrifft, gilt das oben Gesagte.

— Vorzusehen ist weiterhin eine Benachrichtigungspflicht zugunsten der betroffenen Personen. Ohne Kenntnis eines heimlichen Eingriffs ist effektiver Rechtsschutz praktisch erschwert oder gar unmöglich. Fällt der Zweck einer Maßnahme weg oder ist dieser erreicht, sind Betroffene über diese grundsätzlich zu unterrichten. Etwaige Geheimhaltungsinteressen können allenfalls das Absehen von einer Benachrichtigung im Einzelfall, nicht aber das Absehen von einer gesetzlichen Regelung insgesamt rechtfertigen.

— Des Weiteren sind sowohl die Berichtspflichten des Innenministeriums gegenüber dem Parlamentarischen Kontrollgremium gemäß Art. 20 Abs. 1 Satz 1 BayVSG als auch die Berichtspflichten des Parlamentarischen Kontrollgremiums gegenüber dem Landtag gemäß Art. 20 Abs. 1 Satz 2 BayVSG unzureichend. So fehlt etwa in Art. 20 Abs. 1 Satz 2 BayVSG entgegen den Vorgaben des Bundesverfassungsgerichts eine Berichtspflicht direkt gegenüber dem Landtag über Datenübermittlungen des Bayerischen Landesamtes für Verfassungsschutz an Drittstaaten und internationale Organisationen. Das Gleiche gilt für eine fehlende Berichtspflicht über den Einsatz von Verdeckten Mitarbeitern und Vertrauensleuten.

— Auch die Ausgestaltung des Kernbereichsschutzes halte ich für defizitär. Zwar hat der bayerische Gesetzgeber mit Art. 8a BayVSG eine allgemeine Regelung zum Schutz des Kernbereichs privater Lebensgestaltung und der Berufsgeheimnisträger geschaffen. Allerdings ist diese Regelung ausbaubedürftig. Denn um einen umfassenden Schutz kernbereichsrelevanter Daten zu gewährleisten, darf die G 10-Kommission etwa nicht nur mit der Sichtung automatisierter Aufzeichnungen befasst werden (Art. 8a Abs. 1

Satz 5 BayVSG in Verbindung mit § 3a Satz 4 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses), sie müsste vielmehr generell bereits dann beteiligt werden, wenn Zweifel an der Verwertbarkeit erhobener Daten (also etwa auch bei nicht-automatischen Aufzeichnungen oder etwa im Wege der Online-Durchsuchung erlangten Daten) bestehen.

— Auch der Schutz von Berufsgeheimnisträgern in dem neu eingefügten Art. 8a BayVSG ist meiner Meinung nach nicht optimal ausgestaltet. Zwar wurden in Art. 8a Abs. 1 Satz 1 Nr. 2 BayVSG – in Anpassung an die Vorgaben des BKAG-Urteils – die Rechtsanwälte und Kammerrechtsbeistände den Strafverteidigern gleichgestellt. Um eine Zersplitterung der Schutzniveaus zu vermeiden, sollte aber der absolute Schutz des Art. 8a Abs. 1 Satz 1 Nr. 2 BayVSG allen Berufsgeheimnisträgern zugutekommen. Mir ist zwar bewusst, dass das Bundesverfassungsgericht im BKAG-Urteil keinen strikten Schutz von Berufsgeheimnisträgern gefordert, sondern dem Gesetzgeber einen Gestaltungsspielraum eingeräumt hat. Gleichwohl sollte dennoch ein umfassender Schutz für alle im Strafprozessrecht geschützten Berufsgeheimnisträger beim Einsatz nachrichtendienstlicher Mittel eingeführt werden. Insbesondere kann ich keinen sachlichen Grund für die konkret getroffene Differenzierung zwischen „privilegierten“ und „anderen“ Berufsgeheimnisträgern erkennen. Die Unterscheidung führt zu einem Zwei-Klassen-System, das unter Gleichbehandlungsgesichtspunkten (Art. 3 Abs. 1 GG) nur schwer zu rechtfertigen ist (siehe hierzu bereits meine Ausführungen im 24. Tätigkeitsbericht 2010 unter Nr. 3.1.1 und im 26. Tätigkeitsbericht 2014 unter Nr. 3.1.2).

— Darüber hinaus wurde die vormals in Art. 15 Abs. 2 Satz 2 Bayerisches Verfassungsschutzgesetz in der bis zum 30. Juni 2018 geltenden Fassung (BayVSG-alt) enthaltene Eingriffsschwelle für Auskunftsersuchen im Schutzbereich des Brief-, Post- und Fernmeldegeheimnisses bei Bestrebungen nach § 3 Abs. 1 Nr. 1 Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (BVerfSchG) gestrichen. Um eine weitere Absenkung des an Art. 10 GG zu messenden Schutzniveaus zu verhindern, halte ich die erhöhten Eingriffsvoraussetzungen des Art. 15 Abs. 2 Satz 2 BayVSG-alt für unverzichtbar.

Im Rahmen des Gesetzgebungsverfahrens konnte ich immerhin einige datenschutzrechtliche Verbesserungen erreichen. So wurde in Art. 19a BayVSG eine eigene Rechtsgrundlage für die längerfristige Observation und das Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes außerhalb von Wohnungen geschaffen (siehe hierzu auch Landtags-Drucksache 17/20763, S. 15 f.). Diese eingriffsintensiven Maßnahmen müssen zukünftig nicht mehr auf die niedrigschwellige Generalklausel des Art. 8 Abs. 1, 5 Abs. 1 BayVSG gestützt werden.

Unter dem Gesichtspunkt einer hinreichenden Normenbestimmtheit und Normenklarheit hatte ich bereits mehrfach in der Vergangenheit gefordert, eine ausdrückliche Befugnis zu besonderen Mitteln der Datenerhebung aufzunehmen (siehe hierzu etwa meine kritische Stellungnahme vom 22. Februar 2016 zur BayVSG-Novelle 2016, S. 6 f., im Internet abrufbar auf https://www.datenschutz-bayern.de unter „Themengebiete – Verfassungsschutz“). Die bloß beispielhafte Aufzählung der nachrichtendienstlichen Mittel in Art. 8 Abs. 1 Satz 1 BayVSG halte ich für nicht ausreichend. Welche Arten von nachrichtendienstlichen Mitteln dem

Bayerischen Landesamt für Verfassungsschutz zustehen und unter welchen Voraussetzungen diese eingesetzt werden dürfen, entzieht sich so weitgehend der Kenntnis der Öffentlichkeit und der betroffenen Personen. Darüber hinaus fehlen besondere Zulässigkeitsvoraussetzungen, die nach der jeweiligen Eingriffstiefe des angewendeten Mittels zu bemessen sind. Eine pauschale Bezugnahme allein auf die allgemeine Befugnisnorm in Art. 5 Abs. 1 BayVSG und damit auf die Aufgabenerfüllung des Bayerischen Landesamtes für Verfassungsschutz ist jedenfalls dann bedenklich, wenn ein Eingriff seiner Art nach besonders gewichtig ist (etwa in Fällen der längerfristigen Observation oder des Abhörens und Aufzeichnens des nichtöffentlich gesprochenen Wortes außerhalb von Wohnungen). Daher freut mich, dass der Gesetzgeber meinem langjährigen Petitum endlich entsprochen hat.

Im Ergebnis ist festzuhalten, dass sich der Gesetzgeber mit der Reform vom 12. Juni 2018 zwar um eine verfassungsrechtlich angezeigte „Nachjustierung" des Bayerischen Verfassungsschutzgesetzes bemüht hat, hierbei aber hinter meinen Forderungen und Empfehlungen zurückgeblieben ist.

5.2 Prüfung Antiterrordatei (ATD)

In der Antiterrordatei (ATD) werden seit 2007 Erkenntnisse von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder aus dem Bereich des internationalen, vor allem islamistisch motivierten Terrorismus vernetzt. Einzelheiten zur Antiterrordatei sind im Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz – ATDG) geregelt, darunter auch die Verpflichtung, mindestens alle zwei Jahre „die Durchführung des Datenschutzes" zu kontrollieren. Aus diesem Anlass erfolgte durch mich im Berichtszeitraum eine Vor-Ort-Prüfung beim Bayerischen Landesamt für Verfassungsschutz bezüglich der von dort in die ATD eingespeicherten Datensätze.

Hierbei habe ich stichprobenartig die Speicherungen von sogenannten „Hauptpersonen" und hierzu verknüpften „Kontaktpersonen" überprüft. Alle dargelegten Speicherungen von Hauptpersonen entsprachen den gesetzlichen Vorgaben des Antiterrordateigesetzes. Es lagen verlässliche Informationen vor, dass die betreffenden Personen Terrororganisationen angehören, unterstützen oder am bewaffneten Jihad teilnehmen wollen.

Als sogenannte „Kontaktperson" im Sinne des Antiterrordateigesetzes gilt jemand, bei dem tatsächliche Anhaltspunkte vorliegen, dass er mit einer „Hauptperson" nicht nur flüchtig oder in zufälligem Kontakt in Verbindung steht und durch ihn weiterführende Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus zu erwarten sind (siehe § 3 Abs. 2 Satz 1 ATDG). Bei einer Kontaktperson aus meiner Prüfungsstichprobe waren diese Voraussetzungen nicht hinreichend belegt, nachdem lediglich ein gemeinsamer Aufenthalt mit einer Hauptperson in einer Moschee nachgewiesen war.

Meinen Bedenken gegen diese Speicherung hat das Bayerische Landesamt für Verfassungsschutz noch während der stattfindenden Prüfung Rechnung getragen; nach nochmaliger fachlicher Überprüfung wurde der Datensatz der betreffenden Kontaktperson gelöscht.

5.3 Prüfung Rechtsextremismus-Datei (RED)

Als Reaktion auf die Mordserie der Terrorgruppe „Nationalsozialistischer Untergrund“ (NSU) werden seit 2012 Daten zur Bekämpfung des gewaltbezogenen Rechtsextremismus in der Rechtsextremismus-Datei (RED) gespeichert. Gesetzliche Grundlage hierfür ist das Gesetz zur Errichtung einer standardisierten zentralen Datei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus (Rechtsextremismus-Datei-Gesetz – RED-G), das hinsichtlich der Rahmenbedingungen vergleichbar mit dem Antiterrordateigesetz (siehe Nr. 5.2) ist und ebenfalls mindestens alle zwei Jahre datenschutzrechtliche Pflichtprüfungen vorsieht.

Dem Rechnung tragend prüfte ich im Berichtszeitraum vor Ort beim Bayerischen Landesamt für Verfassungsschutz Datensätze, die von dort in die Rechtsextremismus-Datei eingespeichert wurden. Entsprechend dem Vorgehen bei der Antiterrordatei (siehe Nr. 5.2) wurden auch hier stichprobenartig die Speicherungen von sogenannten „Hauptpersonen“ und hierzu verknüpften „Kontaktpersonen“ geprüft.

Während die geprüften Speicherungen der Hauptpersonen unzweifelhaft den gesetzlichen Vorgaben des Rechtsextremismus-Datei-Gesetzes entsprachen, war eine solche Eindeutigkeit in den Fällen der geprüften Kontaktpersonen nicht gegeben. Nach dem Rechtsextremismus-Datei-Gesetz sind Kontaktpersonen im Wesentlichen Personen, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie nicht nur flüchtig oder in zufälligem Kontakt zu einer Hauptperson stehen und durch sie (die Kontaktperson) weiterführende Hinweise für die Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus zu erwarten sind (siehe § 3 Abs. 2 Satz 1 RED-G). Das Vorliegen dieser Voraussetzungen war jedenfalls bei den Kontaktpersonen aus meiner Prüfungsstichprobe fraglich.

Nach nochmaliger fachlicher Prüfung hat das Bayerische Landesamt für Verfassungsschutz meinen Bedenken Rechnung getragen und die Datensätze zu den betroffenen Kontaktpersonen aus der Rechtsextremismus-Datei gelöscht.

5.4 Besonderes Interesse bei Auskunftsersuchen

Das Bayerische Verfassungsschutzgesetz gewährt in Art. 23 Abs. 1 BayVSG ein Recht auf Selbstauskunft. Bürgerinnen und Bürgern können mit einem entsprechenden Antrag in Erfahrung bringen, ob und welche personenbezogenen Daten das Bayerische Landesamt für Verfassungsschutz über sie gespeichert hat. Im Gegensatz zum polizeirechtlichen Gegenstück (Art. 65 Abs. 1 Polizeiaufgabengesetz) ist hier jedoch ein „besonderes Interesse an einer Auskunft“ darzulegen. In der Praxis beruft sich das Bayerische Landesamt für Verfassungsschutz bei der Ablehnung von Auskunftsanträgen immer wieder auf das Fehlen dieses Merkmals. Art. 23 Abs. 1 BayVSG lautet auszugsweise:

„(1) [1]Das Landesamt erteilt dem Betroffenen auf Antrag, in dem ein besonderes Interesse an einer Auskunft dargelegt ist, kostenfrei Auskunft über die zu seiner Person gespeicherten Daten. [2]Legt der Betroffene nach Aufforderung ein besonderes Interesse nicht dar, entscheidet das Landesamt über den Antrag nach pflichtgemäßem Ermessen. […]“

Die Darlegung eines solchen besonderen Interesses wurde trotz meiner Kritik im Gesetzgebungsverfahren als Voraussetzung des Auskunftsrechts verankert. Die Darlegung des besonderen Interesses soll dem Bayerischen Landesamt für Verfassungsschutz eine Prüfung des Auskunftsbegehrens ermöglichen und dabei auf einer ersten Stufe einer für die nachrichtendienstliche Arbeit unzuträglichen Ausforschung vorbeugen. Aus datenschutzrechtlicher Sicht sollten jedoch grundsätzlich an die Darlegung des besonderen Interesses keine allzu hohen Anforderungen gestellt werden. Auskunftsuchende Personen sollen insbesondere nicht gezwungen werden, dem Bayerischen Landesamt für Verfassungsschutz nur zur Geltendmachung des Auskunftsanspruchs eventuell weitere nachrichtendienstlich relevante Informationen zu offenbaren. Aus diesem Grund überprüfe ich regelmäßig Sachverhalte, in welchen Anhaltspunkte dafür sprechen, dass die Anforderungen an die Darlegung des besonderen Interesses zulasten der Bürgerinnen und Bürger überspannt werden.

So wurde einer antragstellenden Person, die aus meiner Sicht nachvollziehbar angab, ihr sei wegen Einwänden einer Verfassungsschutzbehörde eine bestimmte Beschäftigung verwehrt worden, eine Selbstauskunft verweigert. Das Bayerische Landesamt für Verfassungsschutz hielt die Ausführungen der antragstellenden Person im Hinblick auf das besondere Auskunftsinteresse für „zu abstrakt und unsubstanziiert". Ich hob demgegenüber hervor, dass ich eine noch detailliertere Darlegung nicht zwingend für geboten erachte und die Anforderung von konkreten Belegen allenfalls in begründeten Einzelfällen in Betracht komme, so beim konkreten Verdacht einer Ausforschung. Im Übrigen hat der Gesetzgeber das Bayerische Landesamt für Verfassungsschutz verpflichtet, selbst im Fall eines nicht dargelegten besonderen Interesses nach pflichtgemäßem Ermessen über den Antrag zu entscheiden (vgl. Art. 23 Abs. 1 Satz 2 BayVSG). Der antragstellenden Person wurde schließlich nach entsprechender Substantiierung des besonderen Interesses Auskunft erteilt, zudem wurde später einem Antrag auf Löschung beim Bayerischen Landesamt für Verfassungsschutz gespeicherter personenbezogener Daten entsprochen.

Weitere Hinweise zum Auskunftsrecht gegenüber dem Bayerischen Landesamt für Verfassungsschutz finden sich auf meiner Internetpräsenz https://www.datenschutz-bayern.de in der Rubrik „Themengebiete – Verfassungsschutz – Häufige Fragen".

5.5 Prüfung der Vollständigkeit und Richtigkeit von Auskünften

Auch im Berichtszeitraum habe ich die Richtigkeit und Vollständigkeit der Antworten des Bayerischen Landesamts für Verfassungsschutz auf Auskunftsersuchen von Bürgerinnen und Bürgern geprüft.

Nach meiner Erfahrung bearbeitet das Landesamt für Verfassungsschutz derartige Anträge grundsätzlich datenschutzkonform. Aufgrund der Komplexität des zentralen Nachrichtendienstlichen Informationssystems (NADIS) und der Sensibilität der dortigen Speicherungen ist es mir gleichwohl ein wichtiges Anliegen, dieses Thema stets im Blick zu behalten.

Anhand konkreter Fälle habe ich daher geprüft, ob

— Personen, die eine Auskunft (ohne Hinweis auf eine mögliche Teilauskunft) erhalten haben, tatsächlich eine vollständige Auskunft erhielten (Fallgruppe 1),

— Personen, denen die (negative) Auskunft erteilt wurde, es seien keine Daten von ihnen gespeichert, sich nicht doch in Dateien (insbesondere im NADIS) recherchieren ließen (Fallgruppe 2) und

— Personen, denen eine vollständige Löschung ihrer Daten zugesagt wurde, anschließend nicht doch noch recherchierbar blieben (Fallgruppe 3).

Zusammenfassend ist festzuhalten, dass die im Berichtszeitraum geprüften Auskünfte rechtlich korrekt waren.

Aufgrund des Umstandes, dass es sich bei NADIS um einen Datenverbund des Bundesamts und der Landesämter für Verfassungsschutz handelt, stieß ich aber auf die folgende systembedingte Problematik:

So fand ich in der Fallgruppe 2, welche die Überprüfung von sogenannten Negativauskünften betrifft („vom Bayerischen Landesamt für Verfassungsschutz sind keine Daten zu Ihrer Person in Dateien oder Akten gespeichert") einen Fall, in dem die betroffene Person dennoch in der Verbunddatei NADIS recherchierbar war. Allerdings gingen die Speicherungen auf außerbayerische Verfassungsschutzbehörden zurück. Die Negativauskunft des Bayerischen Landesamts für Verfassungsschutz war daher rechtlich korrekt, weil diese Behörde eben keine Daten gespeichert hatte.

In der Fallgruppe 3, die auf die Überprüfung einer vollständigen Löschung ausgerichtet ist, stieß ich auf einen ähnlichen Fall. Das Bayerische Landesamt für Verfassungsschutz hatte einem Rechtsanwalt mitgeteilt, dass man „alle zur Person Ihres Mandanten gespeicherten Daten gelöscht" habe. Meine Prüfung bestätigte auch, dass in NADIS keine in der Verantwortung des Bayerischen Landesamts für Verfassungsschutz gespeicherten Daten mehr vorhanden waren. Insofern war auch diese Auskunft rechtlich korrekt. Allerdings existierten in NADIS noch Speicherungen von Daten der betroffenen Person, die von anderen Verfassungsschutzbehörden verantwortet waren und ursprünglich bayerische Bezüge aufwiesen. In diesem Fall hatte das Bundesamt für Verfassungsschutz einen „Mitbesitz" an den Speicherungen erklärt, mit der Folge, dass die Daten trotz der Löschung durch das Bayerische Landesamt für Verfassungsschutz in NADIS weiter einsehbar waren.

Nach meiner Erfahrung verfahren die Verfassungsschutzbehörden des Bundes und der Länder regelmäßig so, dass sie im Rahmen von Auskunfterteilungen nicht auf Speicherungen hinweisen, die nicht in der eigenen Verantwortung stehen. Auch wenn dies rechtlich nicht zu beanstanden sein mag, finde ich es sehr bedauerlich, dass es hierdurch im Einzelfall zu derart intransparenten und letztlich missverständlichen Auskünften gegenüber Bürgerinnen und Bürgern kommen kann, wie ich sie oben geschildert habe. Einer antragstellenden Person dürften die Mechanismen eines Speicherverbundes wie NADIS, insbesondere was den (Mit)besitz mehrerer Verfassungsschutzbehörden an Speicherungen angeht, kaum bewusst sein.

Ich habe diese Problematik daher zum Anlass genommen, die Erläuterungen auf meiner Homepage (https://www.datenschutz-bayern.de) in der Rubrik „Themengebiete – Verfassungsschutz – Häufige Fragen“ um einen entsprechenden Hinweis zu ergänzen. Dort empfehle ich, gegebenenfalls Auskunftsanträge bei mehreren Verfassungsschutzbehörden der Länder und des Bundes in Erwägung zu ziehen. Dies gilt vor allem dann, wenn die Umstände, die das „besondere Auskunftsinteresse“ (siehe Nr. 5.4) begründen, auch außerhalb Bayerns von Bedeutung sind oder in einem anderen Bundesland ihren Ursprung haben.

6 Justiz

6.1 Gesetze

6.1.1 Bayerisches Psychisch-Kranken-Hilfe-Gesetz

Im Berichtszeitraum habe ich gegenüber dem Bayerischen Staatsministerium für Familie, Arbeit und Soziales sowie dem Bayerischen Staatsministerium für Gesundheit und Pflege zu einem Referentenentwurf für ein Bayerisches Psychisch-Kranken-Hilfe-Gesetz (BayPsychKHG) kritisch Stellung genommen. Zudem wurde ich vor dem Bayerischen Landtag als Sachverständiger in einer Expertenanhörung zum Gesetzentwurf gehört.

Der Gesetzentwurf hatte zunächst für viel Kritik von Fachleuten und in der Presse gesorgt. Eine zentrale Rolle spielten dabei – nicht nur aus datenschutzrechtlicher Sicht – die Einführung einer sogenannten „Unterbringungsdatei" sowie stigmatisierende Verweisungen auf andere Gesetze, namentlich das Gesetz über den Vollzug der Maßregeln der Besserung und Sicherung sowie der einstweiligen Unterbringung (Bayerisches Maßregelvollzugsgesetz – BayMRVG), das Gesetz über den Vollzug der Freiheitsstrafe und der Jugendstrafe (Bayerisches Strafvollzugsgesetz – BayStVollzG) sowie das Gesetz über den Vollzug der Sicherungsverwahrung und der Therapieunterbringung (Bayerisches Sicherungsverwahrungsvollzugsgesetz – BaySvVollzG).

Ich habe vor allem die Erforderlichkeit einer „Unterbringungsdatei" in Frage gestellt. Eine zentrale Speicherung unter anderem von medizinischen Daten, die der ärztlichen Schweigepflicht unterliegen, begegnet wegen der damit verbundenen intensiven Grundrechtseingriffe erheblichen verfassungsrechtlichen Bedenken; aus datenschutzrechtlicher Sicht ist sie entschieden abzulehnen. Auch vor dem Hintergrund der Gefahren eines Missbrauchs der erfassten und in der „Unterbringungsdatei" zu speichernden Daten setzte ich mich nachdrücklich dafür die Abschaffung dieser Datei ein. Nicht zuletzt aufgrund meiner Bedenken hat der Gesetzgeber auf die Einrichtung einer „Unterbringungsdatei" schließlich verzichtet.

Die vielen Verweise auf das Bayerische Maßregelvollzugsgesetz, das Bayerische Strafvollzugsgesetz und das Bayerische Sicherungsverwahrungsvollzugsgesetz erweckten einen falschen Eindruck dahingehend, dass die öffentlich-rechtliche Unterbringung mit der Strafhaft, dem Maßregelvollzug oder einer Sicherungsverwahrung vergleichbar sei. Da die Begründung für die Schaffung des Bayerischen Psychisch-Kranken-Hilfe-Gesetzes gerade darauf abzielt, psychisch kranken Menschen die erforderliche Unterstützung zu bieten und den Begriff der psychischen Krankheit zu entstigmatisieren, stünden Verweise auf die drei genannten Gesetze mit dem verfolgten Regelungskonzept nicht in Einklang. Es ist daher zu begrüßen, dass – wiederum auch aufgrund meiner Bedenken – von derartigen Verweisungen überwiegend Abstand genommen wurde und eigenständige Regelungen in den Gesetzentwurf Aufnahme fanden.

Trotz dieser Verbesserungen des ursprünglichen Gesetzentwurfs weist das beschlossene Gesetz aus datenschutzrechtlicher Sicht weiterhin Schwächen auf:

— So halte ich es für bedenklich, dass die Regelungen zur Besuchs- und zur Schriftverkehrsüberwachung bei öffentlich-rechtlich untergebrachten Personen keine expliziten Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung vorsehen.

— Kritisch zu betrachten sind des Weiteren in dem Gesetz vorgesehene Mitteilungs- und Benachrichtigungspflichten der Unterbringungseinrichtungen gegenüber der zuständigen Kreisverwaltungsbehörde und Polizeidienststelle. Diese Datenübermittlungsvorschriften sehen vor, dass das zuständige Kreisverwaltungsreferat und die zuständige Polizeidienststelle zu informieren sind, wenn eine vorläufige öffentlich-rechtliche Unterbringung nicht in Betracht kommt, da die Voraussetzungen dafür nicht vorliegen, oder wenn das Ende der öffentlich-rechtlichen Unterbringung bevorsteht. Auch bei einer bevorstehenden Entlassung sind die zur Gefährdungseinschätzung notwendigen Informationen zu übermitteln. Solche weitgehenden und pauschalen Datenübermittlungen halte ich für nicht erforderlich. Zwar sieht das Gesetz vor, dass im Falle einer ausschließlichen Selbstgefährdung keine Daten übermittelt werden, allerdings kann diese Einschränkung nicht als ausreichend erachtet werden. Vielmehr sollte eine einzelfallbezogene Differenzierung sowohl hinsichtlich der generellen Mitteilungspflicht als auch in Bezug auf die zu übermittelnden Informationen erfolgen. Dies würde dem Grundsatz der Erforderlichkeit und der Datensparsamkeit eher gerecht werden.

6.1.2 Gesetz über den Vollzug des Jugendarrestes

Am 26. Juni 2018 verabschiedete der Landtag das Gesetz über den Vollzug des Jugendarrestes (Bayerisches Jugendarrestvollzugsgesetz – BayJAVollzG), welches am 1. Januar 2019 in Kraft trat.

Mit der Schaffung eines eigenständigen Bayerischen Jugendarrestvollzugsgesetzes hat der bayerische Gesetzgeber eine langjährige Forderung von mir umgesetzt (siehe mein 27. Tätigkeitsbericht 2016 unter Nr. 5.4). Die bisherigen Regelungen zum Jugendarrestvollzug wurden den verfassungsrechtlichen Anforderungen nicht mehr gerecht, nachdem das Bundesverfassungsgericht bereits 1972 eine gesetzliche Grundlage für Grundrechtseingriffe gegenüber erwachsenen Strafgefangenen gefordert (Bundesverfassungsgericht, Beschluss vom 14. März 1972, Az.: 2 BvR 41/71, BVerfGE 33, 1 – Strafgefangene) und dieses Erfordernis im Jahr 2006 auf den Jugendstrafvollzug ausgeweitet hatte (Bundesverfassungsgericht, Urteil vom 31. Mai 2006, Az.: 2 BvR 1673/04 und 2 BvR 2402/04, BVerfGE 116, 69 – Jugendstrafvollzug). Ich begrüße daher ausdrücklich, dass durch das Bayerische Jugendarrestvollzugsgesetz eine rechtsstaatliche Grundlage für den Vollzug des Jugendarrestes und die damit verbundenen Eingriffe in die Grundrechte der Arrestanten und Arrestantinnen geschaffen wurde.

Im Rahmen des Gesetzgebungsverfahrens gab mir das Bayerische Staatsministerium der Justiz mehrfach die Gelegenheit, zum Entwurf des Bayerischen Jugendarrestvollzugsgesetzes Stellung zu beziehen. Mein Hauptaugenmerk legte ich hierbei auf zwei kritische Themen, namentlich die Kontrolle des Schriftverkehrs und die Videoüberwachung des besonders gesicherten Arrestraums.

Art. 18 Abs. 1 Satz 1 BayJAVollzG regelt den **Schriftwechsel der Arrestanten und Arrestantinnen** und normiert ausdrücklich dessen Förderung. Nach Art. 18 Abs. 1 Satz 2 BayJAVollzG finden hierbei Art. 31 bis 34 und Art. 44 Abs. 6 und 7 Gesetz über den Vollzug der Freiheitsstrafe und der Jugendstrafe (Bayerisches Strafvollzugsgesetz – BayStVollzG) entsprechende Anwendung. Mit der Verweisung des Art. 18 Abs. 1 Satz 2 BayJAVollzG wird jedoch auch Art. 32 Abs. 3 BayStVollzG in Bezug genommen, der die grundsätzliche Überwachung des Schriftverkehrs vorsieht. Einen Gleichlauf mit dem Bayerischen Strafvollzugsgesetz halte ich an dieser Stelle für bedenklich. Der Jugendarrestvollzug ist aufgrund seiner primär pädagogisch orientierten Ausrichtung deutlich vom Jugend- und Erwachsenenstrafvollzug abzugrenzen. Eine starre Parallelität zu den Regelungen des Bayerischen Strafvollzugsgesetzes wird den Bedürfnissen der Arrestanten und Arrestantinnen nicht gerecht. Jugendliche werden durch die Briefkontrolle nicht zum Schreiben motiviert, sondern in der Regel geradezu davon abgehalten. Das in Art. 18 Abs. 1 Satz 1 BayJAVollzG ausgegebene Ziel der Förderung der schriftlichen Kommunikation wird damit verfehlt. Vor diesem Hintergrund habe ich gegenüber dem Justizministerium gefordert, im Jugendarrestvollzug auf die Briefkontrolle zu verzichten.

Auch die ursprünglich geplante Videoaufzeichnung des besonders gesicherten Arrestraums begegnete datenschutzrechtlichen Bedenken. Nach dem ursprünglichen Entwurf eines Art. 22 Abs. 2 Nr. 2 BayJAVollzG sollte „bei der Beobachtung mit technischen Mitteln nach Art. 96 Abs. 2 Nr. 2 BayStVollzG [...] eine Aufzeichnung zulässig sein, soweit dies zur Abwendung einer in Art. 96 Abs. 1 BayStVollzG genannten Gefahr erforderlich ist". Bereits die **Videobeobachtung** mit Kameras als besondere Sicherungsmaßnahme ist indes nicht unumstritten. Grundsätzlich halte ich die reine Videobeobachtung eines besonders gesicherten Haftraums zwar für vertretbar (siehe zur Videoüberwachung des besonders gesicherten Haftraums im Strafvollzug auch meine Ausführungen unter Nr. 6.4.3). Eine zusätzliche Aufzeichnung der Videobilder lehne ich jedoch entschieden ab. Denn diese ist „zur Abwendung einer in Art. 96 Abs. 1 BayStVollzG genannten Gefahr" weder geeignet noch erforderlich. Art. 96 Abs. 1 BayStVollzG sieht vor, dass gegen Gefangene besondere Sicherungsmaßnahmen angeordnet werden können, wenn nach ihrem Verhalten oder aufgrund ihres seelischen Zustands in erhöhtem Maß Fluchtgefahr oder die Gefahr von Gewalttätigkeiten gegen Personen oder Sachen oder die Gefahr des Selbstmordes oder der Selbstverletzung besteht. Durch die Speicherung der übertragenen Bilder kann aber keine der vorgenannten Gefahren abgewendet werden. Lediglich die Live-Beobachtung ermöglicht oder erleichtert schnelles Reagieren. Der zusätzlichen Aufzeichnung der Situation kommt hingegen keinerlei gefahrenabwehrende Wirkung zu.

Mit meinen Bedenken konnte ich zum Teil durchdringen. Von der ursprünglich vorgesehenen Videoaufzeichnung des besonders gesicherten Arrestraums nahm das Justizministerium aufgrund meiner erheblichen Kritik wieder Abstand. Daher ist nur eine reine Videobeobachtung erlaubt. Die Briefkontrolle im Jugendarrestvollzug wurde hingegen beibehalten. Das Justizministerium begründete dies damit, dass sich aus dem Inhalt von Schreiben regelmäßig Behandlungsansätze für die Arrestanten und Arrestantinnen gewinnen ließen. Zudem könnten hierdurch auch eine etwaige Suizidgefährdung erkannt und gegebenenfalls rechtzeitig Maßnahmen ergriffen werden. Einen Verzicht auf die Briefkontrolle halte ich zwar nach wie vor für vorzugswürdig, doch konnte ich mich den Argumenten des Justizministeriums nicht ganz verschließen.

6.1.3 Mitziehklausel in der Strafprozessordnung

Ebenso wie das Polizeiaufgabengesetz (siehe hierzu den Beitrag Nr. 4.4.3) enthält auch die Strafprozessordnung (StPO) eine sogenannte Mitziehklausel. § 489 StPO regelt für staatsanwaltschaftliche Dateien die Berichtigung, Löschung und Sperrung der gespeicherten Daten:

§ 489 StPO
Berichtigung, Löschung und Sperrung von Daten
(6) [1] Werden die Daten einer Person für ein weiteres Verfahren in der Datei gespeichert, so unterbleibt die Löschung, bis für alle Eintragungen die Löschungsvoraussetzungen vorliegen. […]

Diese Mitziehklausel hat zur Folge, dass Daten einer Person unter Umständen Jahrzehnte gespeichert bleiben, insbesondere dann, wenn wiederholt neue Verfahren zu dieser Person eingetragen werden. Hierbei ist es nach dem Wortlaut des § 489 Abs. 6 StPO unerheblich, ob die Person in dem neuen Ermittlungsverfahren als Beschuldigter oder als Anzeigeerstatter, Geschädigter oder Zeuge geführt wird. Somit kann zum Beispiel die Zeugeneigenschaft einer Person dazu führen, dass zurückliegende Strafverfahren aufgrund des neuen Datensatzes nicht gelöscht werden, auch wenn die Löschungsvoraussetzungen für diese Speicherungen eigentlich vorlägen. Die offene Formulierung des § 489 Abs. 6 StPO führt somit unter Umständen zu nicht absehbaren Speicherungsfristen und ausufernden Datensammlungen. Dies widerspricht den Grundsätzen der Erforderlichkeit und Datensparsamkeit.

Weitere Folge einer solchen im Einzelfall dauerhaften Speicherung ist ein Auseinanderfallen von Aktenaufbewahrung und Datenspeicherung. Die Aufbewahrungsfristen für Akten sind in Bayern in der Verordnung über die Aufbewahrung von Schriftgut der Gerichte, Staatsanwaltschaften und Justizvollzugsbehörden (Aufbewahrungsverordnung) geregelt, wonach etwa die Akten eines eingestellten Ermittlungsverfahrens grundsätzlich für die Dauer von fünf Jahren nach dem Jahr der Weglegung aufbewahrt werden. Da die Aufbewahrungsverordnung keine Mitziehung kennt, werden die Akten nach Fristablauf ausgesondert, während die entsprechenden Datensätze hierzu weiter gespeichert bleiben. Eine Überprüfung möglicherweise unrichtig gespeicherter Daten anhand der zugrundeliegenden Akten ist dann nicht mehr möglich.

Die sehr weitgehende Formulierung des § 489 Abs. 6 StPO begegnet auch europarechtlichen Bedenken. Nach Art. 6 RLDSJ ist bei der Datenverarbeitung zwischen den verschiedenen Kategorien betroffener Personen zu differenzieren. Die Richtlinie trifft hierbei eine ausdrückliche Unterscheidung zwischen Beschuldigten, Verurteilten, Opfern sowie sonstigen Personen, etwa Zeugen. Eine Mitziehklausel, die gleichermaßen bei Beschuldigten wie auch Anzeigeerstattern und Geschädigten zur Anwendung gelangt, wird diesen Vorgaben nicht gerecht. Erforderlich ist vielmehr ein Verzicht auf den Mitzieheffekt bei Anzeigeerstattern, Geschädigten und Zeugen.

Weiterhin haben nach Art. 7 Abs. 2 RLDSJ die zuständigen Behörden alle angemessenen Maßnahmen zu ergreifen, um zu gewährleisten, dass personenbezogene Daten, die unrichtig, unvollständig oder nicht mehr aktuell sind, nicht bereitgestellt werden. Zu diesem Zweck hat jede zuständige Behörde die Qualität der personenbezogenen Daten grundsätzlich vor ihrer Bereitstellung zu überprüfen.

Eine Überprüfung gespeicherter Daten ist jedoch dann nicht mehr möglich, wenn die hierzu geführten Akten bereits vernichtet wurden.

Vor diesem Hintergrund habe ich mich im Berichtszeitraum an das Bayerische Staatsministerium der Justiz gewandt und dieses gebeten, bei der Umsetzung der Datenschutz-Richtlinie für Polizei und Strafjustiz auf eine Einschränkung des § 489 Abs. 6 StPO hinzuwirken. Das Justizministerium trug meinem Anliegen Rechnung und schlug im Rahmen der StPO-Reform (Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679) eine Einschränkung der Mitziehklausel vor.

Die Bundesregierung griff den Vorschlag auf und änderte im Gesetzentwurf vom 7. September 2018 (Bundesrats-Drucksache 433/18) den Gesetzeswortlaut der Mitziehklausel entsprechend ab:

Entwurf eines § 489 StPO
Löschung und Einschränkung der Verarbeitung von Daten
(5) Werden die Daten des Beschuldigten für ein weiteres Verfahren in dem Dateisystem oder einem Informationssystem gespeichert, so kann die Löschung dieser Daten unterbleiben, bis für alle Eintragungen die Löschungsvoraussetzungen vorliegen.

Zum einen ist die Mitziehklausel so auf „Beschuldigte“ beschränkt. Sie gilt damit nicht mehr für Anzeigeerstatter, Geschädigte und Zeugen. Zum anderen handelt es sich um eine Ermessensvorschrift („kann“) und nicht mehr um eine starre Anwendungsregel.

Die Regierungsbegründung (Bundesrats-Drucksache 433/18, S. 75) führt hierzu aus:

„Der neue § 489 Absatz 5 tritt an die Stelle des bisherigen § 489 Absatz 6 StPO. Die so genannte Mitziehklausel wurde auf die Daten des Beschuldigten beschränkt. Hiermit soll verhindert werden, dass etwa auch die Zeugeneigenschaft einer Person zur Folge hat, dass Daten zu einem früheren Strafverfahren gespeichert bleiben. Dies wäre nach der bisherigen Regelung der Fall, was sich besonders gravierend auswirken kann, wenn beispielsweise gegen den ehemaligen Beschuldigten wiederholt neue Verfahren eingeleitet werden, und hierdurch die Daten von Zeugen aus früheren Verfahren kontinuierlich ‚mitgezogen‘ werden.“

Ich freue mich zwar, dass das Bayerische Staatsministerium der Justiz sowie das Bundesministerium der Justiz und für Verbraucherschutz meiner Auffassung gefolgt sind und sich für eine Eingrenzung der Norm entschieden haben. Zugleich wurde jedoch von der Bundesregierung die Mitziehklausel um polizeiliche „Informationssysteme“ erweitert. Dieser Zusatz ist missverständlich, da er fälschlicherweise so verstanden werden kann, dass auch polizeiliche Datenspeicherungen einer Löschung entgegenstehen können. Eine vollständige Streichung der Mitziehklausel halte ich daher für vorzugswürdig.

6.2 Aus der Justiz allgemein

6.2.1 Bekanntgabe von Prüfungsergebnissen im Staatsexamen

Ein Juraabsolvent hat sich im Berichtszeitraum an mich gewandt und mich um datenschutzrechtliche Bewertung der Notenbekanntgabe im juristischen Staatsexamen gebeten. Er teilte mir mit, dass die Prüfungskommission nach der mündlichen Prüfung die Ergebnisse jedem einzelnen Prüfling in Anwesenheit der übrigen Prüflinge bekanntgebe, sodass jeder Prüfling die Einzelnoten und Gesamtergebnisse der anderen Prüflinge erfahre. Der Juraabsolvent sah sich hierdurch in seinen Datenschutzrechten verletzt, zumal er von unbeteiligten Dritten auf seine persönliche Prüfungsnote angesprochen worden sei.

Bereits 1996 hatte ich diese Thematik mit dem Justizministerium erörtert. Ich konnte damals erreichen, dass die Noten auf vorheriges Verlangen eines Prüflings nur in Abwesenheit der anderen Prüflinge bekanntgegeben werden dürfen. Zudem wurde in die Ladung zur mündlichen Prüfung standardmäßig ein Hinweis auf diese Widerspruchsmöglichkeit aufgenommen.

Diese Vorgehensweise hielt ich jedoch für nicht mehr zeitgemäß. Das Bewusstsein der Gesellschaft für datenschutzrechtliche Belange hat sich grundlegend gewandelt, zumal die Ergebnisse der juristischen Staatsprüfungen maßgeblichen Einfluss auf den späteren Werdegang der Absolventen und Absolventinnen haben und eine „überschießende" Weitergabe der Noten in jedem Fall vermieden werden sollte. Davon abgesehen erfordert auch die Datenschutz-Grundverordnung eine Anpassung der bis dato praktizierten **„Widerspruchslösung"**. Die Bekanntgabe der Noten an die übrigen Prüflinge stellt eine Datenübermittlung dar, für die eine Rechtsgrundlage notwendig ist.

Ich forderte daraufhin das Landesjustizprüfungsamt zur Anpassung der bisherigen Verfahrensweise auf. Ich schlug vor, die Prüfungsergebnisse zukünftig nur noch unter Ausschluss der übrigen Prüflinge bekanntzugeben. Damit würde dem informationellen Selbstbestimmungsrecht der Absolventen und Absolventinnen – auch vor dem Hintergrund einer im Zusammenhang mit einer Prüfung nicht auszuschließenden stressbedingten Ausnahmesituation – ausreichend Rechnung getragen.

Das Landesjustizprüfungsamt entschied sich demgegenüber für eine **„Einwilligungslösung"**: Künftig hat der oder die Vorsitzende der Prüfungskommission jeden einzelnen Prüfling im Vorgespräch ausdrücklich zu befragen, ob Einverständnis mit einer Notenbekanntgabe in Anwesenheit der übrigen Prüflinge bestehe. Prüflingen, die ihre Einwilligung nicht erteilen, werden die Noten individuell bekanntgegeben. Zudem wurde in die Ladung zur mündlichen Prüfung ein expliziter Hinweis auf die grundsätzlich individuelle Notenbekanntgabe sowie die Möglichkeit der Einwilligung in eine gemeinsame Notenbekanntgabe aufgenommen.

Ich freue mich, dass das Landesjustizprüfungsamt die bisherige Praxis der Notenbekanntgabe geändert hat. Eine schriftliche Einwilligung halte ich zwar für vorzugswürdig, doch lassen Art. 4 Nr. 11, 7 Abs. 1 DSGVO auch eine dokumentierte, mündliche Einwilligungserteilung genügen. Ausdrücklich begrüße ich, dass die Prüflinge bereits in der Ladung zur mündlichen Prüfung über die Einwilligungs-

möglichkeit aufgeklärt werden. Damit wird sichergestellt, dass die Prüflinge rechtzeitig informiert und in die Lage versetzt werden, die Tragweite ihrer Entscheidung sorgfältig zu beurteilen.

6.2.2 Videotechnik im Hochsicherheitsgerichtssaal

Der auf dem Gelände der Justizvollzugsanstalt München neu errichtete Hochsicherheitsgerichtssaal für Strafprozesse wurde im Herbst 2016 in Betrieb genommen. Die erste Sitzung im Hochsicherheitsgerichtssaal wurde von äußerst negativer Presseberichterstattung begleitet. In den Medien wurde mehrfach die Befürchtung geäußert, dass die im Gerichtssaal angebrachten Videokameras möglicherweise Verteidigerunterlagen abfilmten (siehe etwa Süddeutsche Zeitung vom 16. November 2016, „Neuer Gerichtssaal in Stadelheim – und kein Anwalt will dort verhandeln").

Diese Kritik nahm ich zum Anlass, den Gerichtssaal und insbesondere die dortige Videoüberwachung, einer näheren Prüfung zu unterziehen. Bei der Vor-Ort-Besichtigung konnte ich feststellen, dass der Sitzungssaal mit insgesamt neun Videokameras ausgestattet ist, wovon jedoch nur zwei Kameras über eine Aufzeichnungsfunktion verfügen. Die beiden Kameras werden nur außerhalb der Sitzungszeiten zur Raumüberwachung in Betrieb genommen. Äußerlich sind die beiden Kameras mit Aufzeichnungsfunktion zwar als solche kaum zu erkennen, da sie eher einem Rauchmelder gleichen. Ich konnte dennoch erreichen, dass das Oberlandesgericht München die Kameras während laufender Gerichtsverhandlungen mit einer Abdeckung versieht. Damit soll den – ohnehin angespannten – Prozessbeteiligten und dem Publikum das Gefühl des Beobachtetwerdens genommen werden. Weitere Mängel konnte ich diesbezüglich nicht feststellen.

Bei den übrigen sieben Kameras handelt es sich um sogenannte Dome-Kameras. Diese werden ausschließlich für Projektionen an eine Leinwand innerhalb des Gerichtssaals, beispielsweise für die bessere Darstellung von Zeugenvernehmungen oder Dokumenten, eingesetzt und vom Gericht gesteuert. Eine Dome-Kamera, die hinter der Verteidigerbank angebracht ist, wurde eigens mit einem Sichtschutz ausgestattet, um eine Einsichtnahme in Verteidigerunterlagen zu verhindern. Damit wurde entsprechenden Vorbehalten der Anwaltschaft Rechnung getragen.

Auch in rechtlicher Hinsicht begegnet der Einsatz der Videokameras im Gerichtssaal keinen durchgreifenden Bedenken. Der Betrieb der zwei Videokameras mit Aufzeichnungsfunktion erfolgt auf Grundlage von Art. 21a BayDSG-alt (jetzt: Art. 24 BayDSG) und ist zulässig, soweit er – außerhalb von Sitzungszeiten – aus Sicherheitsgründen zur Raumüberwachung erforderlich ist. Für die reine Videobeobachtung innerhalb des Gerichtssaals durch Live-Übertragung der Bilder an eine Leinwand lässt sich zwar weder der Strafprozessordnung (§§ 58a, 58b, 168e, 247a, 255a StPO) noch dem Gerichtsverfassungsgesetz (§ 169 Satz 2 GVG) eine explizite Rechtsgrundlage entnehmen. In Literatur und Rechtsprechung werden gerichtliche Ton- und Filmaufzeichnungen zu justizinternen Zwecken allerdings grundsätzlich für zulässig erachtet, sofern sie vor Missbrauch und Fälschung gesichert werden. Videobeobachtungen sind demgegenüber weniger eingriffsintensiv. Denn die vernommenen Personen müssen nicht befürchten, dass ihre Aussagen vom Gericht immer wieder vorgeführt, analysiert und überprüft werden. Vor diesem Hintergrund konnte ich keinen Datenschutzverstoß feststellen.

6.2.3 Verwendung eines nicht hinreichend anonymisierten Gerichtsbeschlusses durch einen Gerichtsvollzieher

Eine Petentin wandte sich im Berichtszeitraum an mich, nachdem ihr von einem Gerichtsvollzieher ein nur teilweise geschwärzter Beschluss betreffend einen anderen Schuldner als Anlage zu einem Schreiben übersandt wurde. Der Gerichtsvollzieher bezweckte mit der Übersendung dieses Beschlusses, die Rechtmäßigkeit seines Handelns zu untermauern. Auf dem nicht hinreichend geschwärzten Beschluss war zudem handschriftlich vermerkt, dass der andere Schuldner wegen seines Handelns gegenüber dem Gerichtsvollzieher zu einer Geldstrafe verurteilt wurde. Auch fand sich ein handschriftlicher Vermerk auf dem Dokument, dass dieser Beschluss zur Kenntnis in den Umlauf bei den Gerichtsvollzieherkollegen gegeben werden solle. Ich informierte den Direktor des zuständigen Amtsgerichts über die Vorgehensweise eines seiner Gerichtsvollzieher sowie die Tatsache, dass sich ein nur teilweise geschwärzter Beschluss im Umlauf befindet und dieser mindestens an eine dritte Person versendet wurde. Auf mein Betreiben wies der Direktor des zuständigen Amtsgerichts alle Gerichtsvollzieherinnen und Gerichtsvollzieher des Bezirks auf die Notwendigkeit einer ausreichenden Anonymisierung von Entscheidungen und anderen Schriftstücken vor einer Weitergabe hin.

Auch das Bayerische Staatsministerium der Justiz nahm den Fall zum Anlass, die Praxis entsprechend zu sensibilisieren.

6.3 Strafverfolgung

6.3.1 Vorratsdatenspeicherung

Mit der Vorratsdatenspeicherung von Telekommunikationsdaten habe ich mich in den letzten Jahren regelmäßig auseinandergesetzt (siehe 24. Tätigkeitsbericht 2010 unter Nr. 3.3, 25. Tätigkeitsbericht 2012 unter Nr. 3.1, 26. Tätigkeitsbericht 2014 unter Nr. 1.2.2 und 27. Tätigkeitsbericht 2016 unter Nr. 5.1.2).

Vor dem Bundesverfassungsgericht sind derzeit mehrere Verfahren betreffend das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I S. 2218) anhängig, welches die sogenannte Vorratsdatenspeicherung in Deutschland wieder einführte. Im Rahmen dieser Verfahren bat mich das Bundesverfassungsgericht um Abgabe einer Stellungnahme zu den Verfassungsbeschwerden.

In meiner Stellungnahme gegenüber dem Bundesverfassungsgericht war es mir vor allem ein Anliegen, auf die aktuellen technischen Gegebenheiten einzugehen und darzustellen, mit welcher Intensität die Regelungen des Gesetzes und auf ihrer Grundlage mögliche Maßnahmen in die Grundrechte der Bürgerinnen und Bürger eingreifen. Seit dem Jahr 2010, in welchem das Bundesverfassungsgericht mit Urteil vom 2. März 2010, Az.: 1 BvR 256/08 u. a., BVerfGE 125, 260, die damals geltenden Regelungen zur sogenannten Vorratsdatenspeicherung für verfassungswidrig erklärte, ist die technische Entwicklung weit fortgeschritten. So haben sich nicht nur der Umfang und die Art der durchschnittlichen Internetnutzung geändert, sondern auch die dabei eingesetzten Geräte und Techniken. Die Art der Nutzung des Internets hat ihren Schwerpunkt vom „Surfen auf Webseiten“ hin zu mobilen Anwendungen („Apps“) verlagert. Der Gebrauch von Smartphones und digitalisierten Alltagsgeräten ist fester Bestandteil des Lebens geworden.

Ich sehe es kritisch, dass das Gesetz diese Entwicklung nicht angemessen zu berücksichtigen scheint.

Von Bedeutung für die datenschutzrechtliche Bewertung Themenkomplex „Vorratsdatenspeicherung“ könnte auch das Urteil des Europäischen Gerichtshofs vom 21. Dezember 2016, Az.: C-203/15 und C-698/15, sein. Eine der Kernaussagen diese Urteils ist, dass die Bekämpfung des internationalen Terrorismus sowie die Bekämpfung schwerer Kriminalität eine „dem Gemeinwohl dienende Zielsetzung“ ist, diese aber dennoch eine Vorratsdatenspeicherung nicht zu rechtfertigen vermag, wenn der damit verbundene Grundrechtseingriff nicht „auf das absolut Notwendige“ beschränkt wird. Die Hauptkritik des Europäischen Gerichtshofs, die sich gegen eine alle Nutzerinnen und Nutzer erfassende, anlasslose, flächendeckende und personell, zeitlich wie auch geografisch undifferenzierte Speicherung aller relevanten Telekommunikations-Verkehrsdaten richtet, hat der deutsche Gesetzgeber nicht aufgegriffen. So fehlt etwa eine Begrenzung auf das „absolut Notwendige“, wenn eine Ausnahme für Kommunikationsvorgänge nicht vorgesehen wird, die einem Berufsgeheimnis unterliegen.

Meine ausführliche Stellungnahme zu den Verfassungsbeschwerden betreffend das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten habe ich auf meiner Internetpräsenz https://www.datenschutz-bayern.de in der Rubrik „Themengebiete – Polizei“ zum Abruf bereitgestellt.

Zwischenzeitlich hat die Europäische Kommission den Entwurf einer E-Evidence-Verordnung – Vorschlag für eine Verordnung des Europäischen Parlaments und des Rats über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen vom 17. April 2018, Az.: COM(2018) 225 final, im Internet abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52018PC0225 – veröffentlicht. Mit den darin vorgeschlagenen Regelungen würden die Eingriffsintensitäten im Zusammenhang mit der Vorratsdatenspeicherung weiter erhöht. Die daher gegen diese Verordnung bestehenden datenschutzrechtlichen Bedenken hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 7. November 2018 klar zum Ausdruck gebracht.

Entschließung der 96. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 7. November 2018 in Münster

Der Vorschlag der EU-Kommission für eine E-Evidence-Verordnung führt zum Verlust von Betroffenenrechten und verschärft die Problematik der sog. Vorratsdatenspeicherung

Mit ihrem Vorschlag für eine E-Evidence-Verordnung (Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (COM (2018) 225 final)) möchte die EU-Kommission eine Alternative zum förmlichen Rechtshilfeverfahren schaffen und den Ermittlungsbehörden einen schnelleren Zugang zu Kommunikationsdaten ermöglichen. Die Strafverfolgungsbehörden der EU-Mitgliedstaaten sollen die Befugnis erhalten, Anbieter von Telekommunikations- und Internetdienstleistungen in anderen Mitgliedstaaten der EU und auch in Staaten außerhalb der EU (Drittstaaten) unmittelbar zur Herausgabe von Bestands-, Zugangs-, Transaktions- und Inhaltsdaten zu verpflichten.

Die DSK weist hierzu auf die kritische Stellungnahme des Europäischen Datenschutzausschusses hin […]. Diese stellt bereits das Vorliegen einer Rechtsgrundlage in Frage. Mit Besorgnis sieht die DSK vor allem auch die vorgeschlagene Abkehr vom Grundsatz der doppelten bzw. beiderseitigen Strafbarkeit.

Erstmals im Bereich der internationalen Zusammenarbeit in Strafsachen soll die Herausgabe von Daten nicht mehr davon abhängig sein, ob die verfolgte Tat dort, wo die Daten ersucht werden, überhaupt strafbar ist. Im Ergebnis könnten Unternehmen mit Sitz in Deutschland also zur Herausgabe von Daten an Ermittlungsbehörden in anderen EU-Mitgliedstaaten verpflichtet werden, obwohl die verfolgte Tat in Deutschland überhaupt keine Straftat ist. Das könnte zum Beispiel ein in Deutschland erlaubter Schwangerschaftsabbruch sein oder eine politische Meinungsäußerung, wenn diese im ersuchenden Staat strafbewehrt ist.

Zu befürchten ist hierbei auch, dass Drittstaaten die Regelung der EU als Blaupause für eigene Regelungen heranziehen werden. Provider in EU-Mitgliedstaaten würden sich dann vermehrt Herausgabeanordnungen von Drittstaaten ausgesetzt sehen, mit denen möglicherweise Straftaten aus einer völlig anderen Rechtstradition verfolgt werden.

Kritisch sieht die DSK auch, dass im Regelfall jegliche Information und Beteiligung der Justizbehörden des Staates, in dem der Provider seinen Sitz hat, unterbleibt und damit ein wichtiges verfahrensrechtliches Korrektiv fehlt. Ob die Rechtmäßigkeit eines Ersuchens überprüft wird, hängt im vorgeschlagenen Verfahren ausschließlich vom Verhalten der Provider ab. Nur wenn sich das Unternehmen weigert, Daten zu übermitteln, muss der ersuchende Staat bei den Behörden vor Ort um Vollstreckungshilfe bitten. Nur dann können diese noch in das Verfahren eingreifen. Werden Daten herausgegeben, erlangen die zuständigen Justizbehörden hiervon jedoch keine Kenntnis. Der Vorschlag sieht keine Informationspflicht gegenüber den Behörden am Sitz des Unternehmens vor. Provider verfolgen aber in der Regel wirtschaftliche Interessen und unterliegen in ihren Entscheidungen anderen Verpflichtungen als die Justizbehörden Hierdurch werden Betroffene deutlich schlechter gestellt.

Provider als Adressaten eines Ersuchens sehen sich künftig nicht mehr den Justizbehörden des eigenen Staates gegenüber, sondern müssen sich mit den Behörden des anordnenden Staates auseinandersetzen. Den Betroffenen wiederum steht, wenn überhaupt, nur ein Rechtsbehelf im ersuchenden Mitgliedsstaat zu, dessen Rechtsordnung ihnen in der Regel aber fremd ist.

Ein besonderes Verfahren ist vorgesehen, wenn sich Provider mit Sitz in Drittstaaten darauf berufen, dass die angeordnete Übermittlung gegen das dortige Recht verstößt. Für diesen Fall sieht der Vorschlag eine gerichtliche Überprüfung im anordnenden Staat vor. Wenn das Gericht zu der Auffassung gelangt, dass tatsächlich ein Rechtskonflikt vorliegt, muss es die zuständigen Behörden im Zielstaat der Anordnung beteiligen. Das Ergebnis der Konsultation ist für das Gericht verbindlich. Diese Regelung ist ausdrücklich zu begrüßen. Denn auch hier wird eine Blaupause geschaffen für die Frage, welche Rechte europäische Unternehmen in der umgekehrten Situation haben sollten, wenn sie aus Drittstaaten auf der Grundlage von deren Gesetzen (wie z. B. US-Cloud-Act) zu einer Übermittlung verpflichtet werden und welche Verbindlichkeit eine Konsultation der zuständigen Behörden in Europa für Gerichte in Drittstaaten haben sollte.

Besonders kritisch ist jedoch, dass in Deutschland Telekommunikationsdienstleister verpflichtet sind, u.a. sämtliche Verkehrsdaten für zehn Wochen zu speichern. Aus diesen Daten lassen sich genaue Schlüsse auf das Privatleben der Betroffenen, insbesondere deren Kontakt- und Interessenprofil ziehen. Die Problematik dieser sog. Vorratsdatenspeicherung verschärft sich deutlich, wenn ausländische Strafverfolgungsbehörden einen direkten Zugriff auf derartige Informationen erhalten.

Die DSK appelliert daher an alle im Gesetzgebungsverfahren Beteiligten, den Vorschlag für eine E-Evidence-Verordnung zu stoppen!

6.3.2 Ausgestaltung des Betreffs in staatsanwaltschaftlichen Schreiben

Im Berichtszeitraum wandte sich ein Petent mit einer Eingabe an mich, weil auf Schreiben der Staatsanwaltschaften in Ermittlungs- und Strafverfahren in der Betreffzeile die jeweils zur Last gelegte Straftat genannt werde. Vor dem Hintergrund der Unschuldsvermutung sehe ich eine Nennung der zur Last gelegten Straftat generell und ohne jegliche Eingrenzung, wie beispielsweise durch den Zusatz „wegen des Verdachts des/der […]“ oder „wegen des Vorwurfs des/der […]“, als problematisch. Auch Nr. 4a Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) sieht vor, dass eine nicht durch den Zweck des Ermittlungsverfahrens bedingte Bloßstellung des Beschuldigten zu vermeiden ist.

Nr. 4a RiStBV
Der Staatsanwalt vermeidet alles, was zu einer nicht durch den Zweck des Ermittlungsverfahrens bedingten Bloßstellung des Beschuldigten führen kann. Das gilt insbesondere im Schriftverkehr mit anderen Behörden und Personen. Sollte die Bezeichnung des Beschuldigten oder der ihm zur Last gelegten Straftat nicht entbehrlich sein, ist deutlich zu machen, dass gegen den Beschuldigten lediglich der Verdacht einer Straftat besteht.

Ich konnte erreichen, dass die im staatsanwaltschaftlichen Fachverfahren hinterlegten Schreiben und Formulare betreffend den Ermittlungsabschluss sowie Begleit- und Anschreiben im Betreff dahingehend neu gestaltet wurden, dass der Zusatz „wegen des Verdachts der/des […]“ eingefügt wurde. Meine weitergehende Forderung – die Änderung der Betreffzeile bei Schreiben und Formularen betreffend Ermittlungsanträge – wurde bis dato noch nicht umgesetzt. Allerdings wird das staatsanwaltschaftliche Fachverfahren in den kommenden Jahren modernisiert.

In diesem Zusammenhang hat mir das Bayerische Staatsministerium der Justiz signalisiert, man werde dabei die aus Sicht des Datenschutzes zu Recht erbetene konsequente Umsetzung von Nr. 4a RiStBV im Rahmen der Möglichkeiten im Auge behalten. Ich werde mich daher in dieser Sache mit dem Justizministerium weiterhin konstruktiv austauschen.

6.3.3 Strafantragsstellung durch eine Behörde

Ein Jobcenter stellte, vertreten durch seine Geschäftsführung, gegen einen Kunden einen Strafantrag wegen Verleumdung. Als Zeugen wurden die Geschäftsführerin sowie ein Mitarbeiter benannt und als deren **ladungsfähige Anschrift** die des

Jobcenters angegeben. Die zuständige Staatsanwaltschaft vermerkte als Anzeigeerstatterin fälschlicherweise die Geschäftsführerin und nicht das Jobcenter. In der Folge wurde die Einstellungsverfügung der Staatsanwaltschaft an die bei der Staatsanwaltschaft aufgrund einer anderen Anzeige bekannte Privatanschrift der Geschäftsführerin geschickt. Da der Versuch, die Einstellungsverfügung an den geschädigten Mitarbeiter unter der Adresse des Jobcenters zuzustellen, scheiterte, ermittelte die Staatsanwaltschaft außerdem die Privatanschrift des Mitarbeiters, was zu einer Dokumentation von dieser in der Strafakte führte. Vor diesem Hintergrund bestand die Besorgnis, dass der Beschuldigte über eine Akteneinsicht private Adressdaten erlangen könnte. Ich habe die zuständige Staatsanwaltschaft auf diese Bedenken hingewiesen und darauf aufmerksam gemacht, dass die Verwendung der Privatadressen vermeidbar gewesen wäre, wäre das Jobcenter als Anzeigeerstatter geführt worden. Die Staatsanwaltschaft teilte mir daraufhin mit, sie habe die Adressdaten in einen Sonderband der Strafakte überführt, welcher bei einer Akteneinsichtsgewährung einer besonderen Prüfung wegen der darin enthaltenen personenbezogenen Daten unterzogen werde. Außerdem wurden die Mitarbeiter der Staatsanwaltschaft durch ihren Leiter in Hinblick auf zukünftige vergleichbare Fälle sensibilisiert.

6.4 Strafvollzug

6.4.1 Eigengeldeinzahlung für Gefangene

Ein Gefangener bat mich um Überprüfung der von seiner Justizvollzugsanstalt ausgegebenen Überweisungsvordrucke für Eigengeldeinzahlungen. Solche Überweisungsvordrucke erhalten Gefangene, um Dritten (zum Beispiel Angehörigen und Bekannten) die Einzahlung von Geldbeträgen für sie zu ermöglichen. Diese Eigengeldeinzahlungen werden über die Landesjustizkasse abgewickelt und den für die Gefangenen von der Justizvollzugsanstalt geführten Konten für Einkäufe gutgeschrieben.

Die von der Justizvollzugsanstalt (JVA) bisher verwendeten Überweisungsvordrucke für Eigengeldeinzahlungen waren so ausgestaltet, dass als Verwendungszweck „JVA“, „Eigengeld für“ und „Geb.Dat.“ voreingetragen waren. Damit war anhand des ausgefüllten Überweisungsträgers für Dritte (zum Beispiel Bankbeschäftigte) ersichtlich, dass sich die namentlich genannte Person in der Justizvollzugsanstalt befindet.

Auf meine Anfrage hin hat die Justizvollzugsanstalt – in Absprache mit der Landesjustizkasse – die Überweisungsvordrucke abgeändert. Nun werden im Verwendungszweck die Bezeichnung „JVA“ durch eine Buchungsnummer ersetzt und der Begriff „Eigengeld“ zu „EG“ verkürzt, so dass keine Rückschlüsse mehr auf die Gefangeneneigenschaft der genannten Person möglich sind.

In der Folge trat ich an das Bayerische Staatsministerium der Justiz heran und ersuchte dieses, die Überweisungsvordrucke aller bayerischen Justizvollzugsanstalten datenschutzkonform auszugestalten.

Das Justizministerium schloss sich meiner Auffassung an. Es bat alle Leiterinnen und Leiter der Justizvollzuganstalten um eine einheitliche, datenschutzkonforme Ausgestaltung der Überweisungsträger für Eigengeldeinzahlungen.

6.4.2 Herausgabe einer Urteilsabschrift an einen Insolvenzverwalter

Ein Insolvenzverwalter wandte sich an die Justizvollzugsanstalt eines Gefangenen, über dessen Vermögen das Insolvenzverfahren eröffnet worden war. Der Insolvenzverwalter bat um Übersendung des rechtskräftigen Gerichtsurteils, das den Inhaftierungsgrund darstellte. Daraufhin ließ ihm die Justizvollzugsanstalt eine Ablichtung des betreffenden Strafurteils zukommen.

Ich forderte daraufhin die Justizvollzugsanstalt zur Stellungnahme auf. Die Justizvollzugsanstalt war der Auffassung, dass es sich bei einem Insolvenzverwalter um eine öffentliche Stelle handelt. Gemäß der Bestimmung des Art. 4 Abs. 2 Satz 4 BayDSG-alt (jetzt: Art. 1 Abs. 4 BayDSG) sei eine nicht-öffentliche Stelle, die hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehme, insoweit öffentliche Stelle. Ein derartiger Aufgabenkreis liege bei einem Insolvenzverwalter vor.

Die Haltung der Justizvollzugsanstalt teile ich nicht. Meiner Auffassung nach handelt es sich bei einem Insolvenzverwalter um keine öffentliche, sondern um eine private Stelle. Unter den öffentlichen Stellen im Sinne des Art. 4 Abs. 2 Satz 4 BayDSG-alt sind Beliehene, wie etwa Notare, zu verstehen. Insolvenzverwalter fallen nicht hierunter. Zwar ist deren Status im Detail umstritten, doch ist allen hierzu vertretenen Theorien (Vertretungstheorie, Organtheorie, Amtstheorie) gemeinsam, dass Insolvenzverwalter die Stellung eines privaten Treuhänders innehaben.

Die Justizvollzugsanstalt hätte dem Insolvenzverwalter daher gemäß Art. 197 Abs. 5 Satz 1 Nr. 2 Gesetz über den Vollzug der Freiheitsstrafe und der Jugendstrafe (Bayerisches Strafvollzugsgesetz – BayStVollzG) nur mitteilen dürfen, ob sich der Betroffene in Haft befindet, ob und wann seine voraussichtliche Entlassung bevorsteht und wie seine Entlassungsadresse lautet. Die Übersendung einer vollständigen Urteilsabschrift war hingegen nicht von der Befugnis des Art. 197 Abs. 5 Satz 1 BayStVollzG gedeckt. Ich habe die Justizvollzugsanstalt auf diesen Umstand hingewiesen und um zukünftige Beachtung gebeten. Die Justizvollzugsanstalt sagte mir zu, fortan meiner Rechtsauffassung zu folgen.

6.4.3 Videoüberwachung einer Justizvollzugsanstalt

Die regelmäßige datenschutzrechtliche Prüfung von Justizvollzugsanstalten ist mir ein wichtiges Anliegen. Im Berichtszeitraum habe ich eine neu errichtete Justizvollzugsanstalt kontrolliert. Mein Hauptaugenmerk lag hierbei auf der Videoüberwachung. Die Justizvollzugsanstalt verfügte sowohl im Innen- wie im auch Außenbereich über zahlreiche Videokameras. Gegen deren Einsatz bestehen keine grundlegenden Bedenken.

Wesentlich ist, dass – insbesondere bei den Außenkameras – deutlich sichtbar auf die Videoüberwachung hingewiesen wird. Dies betrifft vor allem den Besucherparkplatz und Eingangsbereich einer Justizvollzugsanstalt. Zudem dürfen schwenkbare Kameras mit Zoom-Funktion keine Einsichtnahme in Privaträume – wie etwa in umliegende Privathäuser – ermöglichen. Des Weiteren ist die nach dem Gesetz zulässige Höchstspeicherfrist für Videoaufzeichnungen von grundsätzlich zwei Monaten einzuhalten (zu den wichtigsten Gesichtspunkten der Videoüberwachung im Justizvollzug siehe mein 27. Tätigkeitsbericht 2016 unter Nr. 5.5.1 und mein 26. Tätigkeitsbericht 2014 unter Nr. 5.4.4).

Diese Voraussetzungen wurden von der geprüften Justizvollzugsanstalt sorgfältig beachtet. Insbesondere die Hinweisbeschilderung war vorbildlich. So wies die Justizvollzugsanstalt bereits einige Meter vor der Parkplatzeinfahrt mit einem großen Schild auf die Videoüberwachung hin. Im Übrigen befanden sich entlang der Außenmauern zahlreiche und in kurzen Abständen angebrachte Piktogramme, die ebenfalls über die Videoüberwachung aufklärten. Darüber hinaus waren die Bilder der Videokameras nur in der Torwache und Sicherheitszentrale vom Vollzugspersonal einsehbar. Auf sämtlichen Monitoren waren Sichtschutzfolien angebracht und die Monitore – besonders in der verglasten Sicherheitszentrale – so positioniert, dass Dritte keinen Einblick erhalten konnten.

Weiterhin überprüfte ich die Videoüberwachung in den sogenannten besonders gesicherten Hafträumen. Diese Räume dienen einer besonderen Sicherungsmaßnahme nach Art. 96 Gesetz über den Vollzug der Freiheitsstrafe und der Jugendstrafe (Bayerisches Strafvollzugsgesetz – BayStVollzG). Gemäß Art. 96 Abs. 1 BayStVollzG können gegen Gefangene besondere Sicherungsmaßnahmen angeordnet werden, wenn nach ihrem Verhalten oder aufgrund ihres seelischen Zustands in erhöhtem Maß Fluchtgefahr oder die Gefahr von Gewalttätigkeiten gegen Personen oder Sachen oder die Gefahr des Selbstmordes oder der Selbstverletzung besteht. In den besonders gesicherten Hafträumen ist nur eine reine Videobeobachtung, keine Videoaufzeichnung zulässig.

Bei der Prüfung konnte ich feststellen, dass die Videobeobachtung nur von gleichgeschlechtlichem Vollzugspersonal durchgeführt wurde. Das begrüße ich ausdrücklich. Denn was die Überwachung am Monitor durch das Vollzugspersonal anbelangt, erachte ich eine geschlechterübergreifende Beobachtung als sehr problematisch. Zwar enthalten das Bayerische Strafvollzugsgesetz und die Verwaltungsvorschriften hierzu keine Vorgaben. Lediglich Art. 91 Abs. 1 Satz 2 BayStVollzG sieht vor, dass männliche Gefangene nur von Männern und weibliche Gefangene nur von Frauen durchsucht werden dürfen. Dies gilt jedoch nur für die Durchsuchung – einen Vorgang mit unmittelbarem körperlichem Kontakt, oftmals auch im Intimbereich. Eine vergleichbare Regelung enthält das Gesetz für die Videoüberwachung gerade nicht. Allerdings halte ich aus Gründen der Menschenwürde und des Schamgefühls der Gefangenen eine geschlechtergetrennte Videoüberwachung für geboten. Daher habe ich in der Vergangenheit gegenüber dem Bayerischen Staatsministerium der Justiz bereits mehrfach gefordert, dass die Beobachtung der in besonders gesicherten Hafträumen untergebrachten Personen nur von Bediensteten gleichen Geschlechts vorgenommen werden darf.

Insgesamt verlief die Prüfung der Justizvollzugsanstalt erfreulich. Ich konnte keine Mängel feststellen. Bei der Ausgestaltung der Videoüberwachung wurde meinen in der Vergangenheit an das Justizministerium herangetragenen Forderungen Rechnung getragen. Insofern zeitigt meine Arbeit erkennbar Erfolge.

7 Inneres und Kommunales

7.1 Nicht dienstlich veranlasste Abfrage von Meldedaten im Bayerischen Behördeninformationssystem (BayBIS)

Meldedaten bilden gleichsam das Rückgrat einer auf Informationen angewiesenen bürgerorientierten Verwaltung. Dazu hält das Melderegister für die Meldebehörde wie auch für eine Vielzahl anderer Behörden einen recht umfassenden Datenbestand über jede meldepflichtige Person bereit (siehe § 3 Bundesmeldegesetz – BMG). Nach näherer Maßgabe des Melderechts ermöglicht das Bayerische Behördeninformationssystem (BayBIS) staatlichen und kommunalen Behörden in Bayern, Meldedaten aus einem zentralen Datenbestand automatisiert abzurufen. Der Datenbestand wird aus den Melderegistern aller bayerischen Meldebehörden gespeist und täglich aktualisiert.

Rechtsgrundlage für den Abruf von Meldedaten durch öffentliche Stellen ist primär § 5 Abs. 1 Verordnung zur Übermittlung von Meldedaten (Meldedatenverordnung – MeldDV). In dieser Norm des bayerischen Landesrechts ist geregelt, dass öffentliche Stellen bestimmte Grunddaten gemeldeter Personen automatisiert abrufen können, **soweit** es **zur Erfüllung ihrer Aufgaben erforderlich** ist.

§ 5 MeldDV
Automatisierte Behördenauskunft
(1) Soweit es zur Erfüllung ihrer Aufgaben erforderlich ist, können öffentliche Stellen aus dem nach Art. 7 Abs. 1 BayAGBMG geschaffenen zentralen Meldedatenbestand gemäß § 38 Abs. 1 BMG vorbehaltlich abweichender Bestimmungen in dieser Verordnung folgende Daten automatisiert abrufen:
Familienname
1. frühere Namen
2. Vornamen
3. Doktorgrad
4. Ordensname, Künstlername
5. Geburtsdatum und Geburtsort sowie bei Geburt im Ausland auch den Staat
6. Geschlecht
7. derzeitige Anschriften oder Wegzugsanschrift
8. Sterbedatum und Sterbeort
(2) […]

Im Berichtszeitraum musste ich jedoch leider einige nicht dienstlich veranlasste Abfragen durch Beschäftigte bayerischer Behörden im BayBIS feststellen. Anlass meiner diesbezüglichen Nachforschungen waren insbesondere Hinweise vom Abruf betroffener Meldebehörden auf den Verdacht unberechtigter Meldedatenabrufe. In den meisten der von mir näher untersuchten Fälle konnten die abrufenden Beschäftigten jeweils keinen hinreichenden dienstlichen Grund für die Abfrage nennen und haben ihr Fehlverhalten eingeräumt.

Vor dem Hintergrund solcher Fälle empfehle ich bayerischen öffentlichen Stellen vor allem folgende **Maßnahmen**, um einen **Missbrauch des BayBIS** durch eigene Beschäftigte wirksam präventiv **zu verhindern**:

1. Beschäftigte, die Zugriff auf das BayBIS erhalten, sind – vorzugsweise durch eine von dem oder der behördlichen Datenschutzbeauftragten angebotene oder veranlasste Schulung – **umfassend datenschutzrechtlich zu belehren**. Dabei ist besonders auf das Verbot dienstlich nicht veranlasster Abfragen hinzuweisen. Den Beschäftigten sollte verdeutlicht werden, dass die unberechtigte Nutzung des BayBIS durch Stichproben (dazu nachfolgend 3.) sowie durch Systemroutinen – insbesondere dann, wenn die Abfrage eine Person betrifft, bei der eine Auskunftssperre im Melderegister eingetragen ist – entdeckt werden kann. In diesem Zusammenhang sollte auch über mögliche arbeits- oder dienstrechtliche Folgen (Abmahnung, Kündigung, disziplinarische Ahndung) sowie über mögliche straf- und ordnungswidrigkeitenrechtliche Konsequenzen aufgeklärt werden (siehe etwa Art. 23 BayDSG). In regelmäßigen Abständen (mindestens jährlich) sollten alle Beschäftigten mit Zugriffsrechten zum BayBIS an die vorstehenden Hinweise erinnert werden. Idealerweise geschieht dies im Rahmen einer auffrischenden Schulung, doch kann auch ein Rundschreiben oder eine entsprechende E-Mail verschickt werden. Die präventiven Maßnahmen sind zu dokumentieren (siehe Art. 5 Abs. 2 DSGVO).

2. Durch organisatorische Maßnahmen (etwa eine Dienstanweisung an die Bediensteten, die über einen Zugang zum BayBIS verfügen) sollte weiterhin sichergestellt werden, dass bei jeder Abfrage im BayBIS der **Grund der Abfrage in aussagekräftigen Worten kurz beschrieben und** auch (soweit vorhanden) das **Aktenzeichen des betroffenen Vorgangs angegeben** wird. Diese Angaben können im BayBIS-Feld „Abfragegrund“ eingetragen werden, wobei der Abfragegrund schon jetzt ein Pflichtfeld darstellt. Meines Erachtens erleichtert gerade auch die behördeninterne Pflicht zur Angabe des Aktenzeichens im Nachgang die Kontrolle und führt den Beschäftigten das Erfordernis des dienstlichen Anlasses in jedem Einzelfall plastisch vor Augen.

3. In regelmäßigen Abständen (mindestens jährlich) sollten nicht angekündigte **Stichproben** der BayBIS-Abfragen durchgeführt werden. Mit dieser Aufgabe kann etwa der oder die Fachvorgesetzte, auch der oder die behördliche Datenschutzbeauftragte betraut werden. Der Umfang dieser Stichproben sollte ein angemessenes Entdeckungsrisiko vermitteln und ist abhängig von der Zahl der Beschäftigten mit Zugang zum BayBIS. Sollte sich zeigen, dass hierdurch keine effektive Verhinderung von missbräuchlichen Abrufen erreicht wird, sollten häufigere Stichproben durchgeführt werden.

Ich werde im Rahmen meiner Datenschutzaufsicht weiterhin besonders darauf achten, dass bayerische öffentliche Stellen wirksame Maßnahmen zur Verhütung von „Neugierabfragen“ im BayBIS durch die eigenen Beschäftigten treffen.

7.2 Rechtsverordnung zur Regelung der öffentlich-rechtlichen Auftragsverarbeitungsverhältnisse: Beteiligung im Normsetzungsverfahren

7.2.1 Auftragsverarbeitung im Zeitalter der Digitalisierung

Bei der Auftragsverarbeitung wird ein Dienstleister in die Verarbeitung personenbezogener Daten einbezogen. Sie ermöglicht arbeitsteiliges Handeln. Dem Auftragsverarbeiter wird nicht die eigentliche (Verwaltungs-)Aufgabe übertragen, sondern nur eine Hilfstätigkeit. Er unterliegt den Weisungen des Auftraggebers, während dieser für die Erfüllung der Aufgabe und auch datenschutzrechtlich weiterhin verantwortlich bleibt.

Die Auftragsverarbeitung ist nicht nur in der Privatwirtschaft, sondern auch in der öffentlichen Verwaltung seit langem verbreitet (siehe allgemein meine Orientierungshilfe „Auftragsverarbeitung“, im Internet abrufbar auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen“). Auftragsverarbeiter übernehmen etwa den Versand von Mitteilungsblättern, Unterstützungsleistungen bei der Datenerfassung, bei der Archivierung oder bei der Löschung von Daten. Bei diesen Fällen ist die Praxis aber nicht stehengeblieben. Gerade durch die rasanten technologischen Entwicklungen der letzten Jahre haben sich die Anwendungsfälle der Auftragsverarbeitung deutlich ausgeweitet.

Speziell im Zuge der Digitalisierung werden IT-Verfahren heute oftmals nicht mehr lokal, sondern zunehmend zentral in großen staatlichen Rechenzentren für viele bayerische Behörden betrieben. Insbesondere kleinere Behörden oder Kommunen verfügen häufig auch gar nicht mehr über ausreichende personelle und fachliche Kapazitäten, um den Aufwand für eine ordnungsgemäße Handhabung von immer mehr Daten in immer komplexeren Verfahren noch allein bewältigen zu können. Werden die erforderlichen Ressourcen am Markt beschafft, liegen häufig Fälle von Auftragsverarbeitungen vor.

7.2.2 Handlungsbedarf aufgrund Änderung der rechtlichen Grundlagen

Bis zum 24. Mai 2018 stand die Regelung der Verarbeitung personenbezogener Daten im Auftrag den jeweiligen Mitgliedstaaten zu. Innerhalb der Bundesrepublik Deutschland bestanden dazu aufgrund der föderalen Struktur landesrechtliche Vorgaben. In Bayern enthielt Art. 6 BayDSG-alt eine Regelung zur damals so genannten Auftragsdatenverarbeitung.

Seit dem 25. Mai 2018 gilt in der gesamten Europäischen Union die Datenschutz-Grundverordnung. Art. 28 ff. DSGVO regeln die Einschaltung eines Auftragsverarbeiters in die Verarbeitung personenbezogener Daten umfassend. Die Vorschriften greifen zwar viele der schon bisher geltenden Anforderungen an den Verantwortlichen (bisher: Auftraggeber) im Wesentlichen unverändert auf. Gerade für den Auftragsverarbeiter (bisher: Auftragnehmer oder Auftragsdatenverarbeiter) stellen sie aber neu detaillierte Anforderungen auf.

Auftragsverarbeitungsverhältnisse wurden in der Vergangenheit regelmäßig mittels eines Vertrags zwischen den beiden Parteien begründet. Solche nach altem Recht abgeschlossenen Verträge genießen aber keinen Bestandsschutz. Die Regelungen der Datenschutz-Grundverordnung sind nicht nur beim Abschluss

neuer Verträgen zu beachten, auch bereits bestehende Verträge müssen gegebenenfalls an die Neuregelungen angepasst werden. Für die im Zuge der Digitalisierung immer wichtiger werdenden staatlichen Rechenzentren würde dies bedeuten, dass eine Vielzahl von bereits bestehenden Verträgen individuell neu abgeschlossen werden müsste. Insbesondere müsste auch bei zentral eingesetzten IT-Verfahren eine Vielzahl von einzelnen, inhaltsgleichen Verträgen (neu) begründet werden.

7.2.3 Rechtsverordnung zur Regelung der öffentlich-rechtlichen Auftragsverarbeitungsverhältnisse

Vor diesem rechtlichen Hintergrund hat mich das Bayerische Staatsministerium der Finanzen und für Heimat – zwischenzeitlich ist auch das Bayerische Staatsministerium für Digitales ressortzuständig geworden – in den Entstehungsprozess einer Rechtsverordnung zur Regelung der öffentlich-rechtlichen Auftragsverarbeitungsverhältnisse eingebunden. Diese Rechtsverordnung soll auf Grundlage des Gesetzes über die elektronische Verwaltung in Bayern erlassen werden und – abgesehen von den Bereichen, die dem Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz unterfallen – bayernweit Auftragsverarbeitungsverhältnisse staatlicher und sonstiger öffentlicher Stellen einheitlich regeln. Damit soll der Abschluss einer Vielzahl gleichartiger Auftragsverarbeitungsvereinbarungen zukünftig entbehrlich werden.

Mit dem vorgelegten Verordnungsentwurf soll von einer in Art. 28 Abs. 3 Satz 1 DSGVO vorgesehenen neuen Möglichkeit der Begründung von Auftragsverarbeitungsverhältnissen Gebrauch machen. Neben dem bereits bisher bekannten Weg des Vertrags kann eine Auftragsverarbeitung nun auch auf Grundlage eines „anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten“ erfolgen. Mit der neuen Regelung soll in Bayern erstmals ein solches anderes Rechtsinstrument erprobt werden.

Im Rahmen meiner Beteiligung am Normsetzungsprozess habe ich gegen die Wahl eines durch Rechtsverordnung geregelten nichtvertraglichen Rechtsverhältnisses als einem anderen Rechtsinstrument keine grundsätzlichen Bedenken erhoben. Ich habe jedoch insbesondere gefordert, dass die nach Art. 28 Abs. 3 DSGVO notwendigen Mindestinhalte in der geplanten Rechtsverordnung Berücksichtigung finden.

In diesem Zusammenhang habe ich insbesondere gefordert, dass eventuelle Verweisungen aus der Rechtsverordnung auf andere Dokumente oder Verzeichnisse transparent gestaltet sein müssen. Letztlich kommt es darauf an, dass die Beteiligten der Auftragsverarbeitung zu jedem Zeitpunkt in der Lage sind, darüber Auskunft zu geben, ob, seit wann, für welche Bereiche und mit welchem genauen Inhalt ein nichtvertragliches Auftragsverarbeitungsverhältnis zwischen ihnen besteht.

Art. 28 DSGVO
Auftragsverarbeiter
[...]
(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung,

Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

c) alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;

d) die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

e) angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;

f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;

g) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt und die vorhandenen Kopien löscht, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;

h) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

[…]

Daneben habe ich gefordert, dass schon aus Gründen der Rechtsklarheit das Schicksal bereits bestehender Verträge zur Auftragsverarbeitung geklärt werden muss und die bislang geplante hilfsweise Regelung für Fälle einer gemeinsamen Verantwortlichkeit gestrichen wird. Den Entstehungsprozess der Rechtsverordnung zur Regelung der öffentlich-rechtlichen Auftragsverarbeitungsverhältnisse werde ich auch in Zukunft weiterhin aufmerksam begleiten.

7.3 Datenschutz beim Einbau und Betrieb elektronischer Wasserzähler mit Funkmodul

7.3.1 Gefahr von Grundrechtseingriffen

Elektronische Wasserzähler mit Funkmodul sind Wasserzähler, die – anders als herkömmliche („analoge“) mechanische Wasserzähler – eine Vielzahl von Daten

messen, speichern und über Funkmodule in die nähere Umgebung senden können. Nach meiner Kenntnis können elektronische Wasserzähler – je nach Bauart und Programmierung – insbesondere folgende Daten verarbeiten: Zählernummer, tagesaktueller Verbrauchsstand, Verbrauchssumme (Tage, Wochen, Monate und Jahre), Durchflusswerte, eventuelle Fehler oder Alarmmeldungen (Leckage, Rohrbruch, Rückwärtslauf, Trockenlauf, Dauerlauf, Defekt oder Manipulationsversuch) sowie durchschnittliche Temperatur des Wassers und der Umgebung für bestimmte Zeitpunkte. Über ihr eingebautes Funkmodul können elektronische Wasserzähler innerhalb eines festgelegten Zeitraums (beispielsweise mehrfach pro Minute) Datensignale aussenden, welche außerhalb des Gebäudes mit entsprechenden Lesegeräten erfasst und ausgewertet werden können.

Bereits frühzeitig haben Bürgerinnen und Bürger mir gegenüber ihre datenschutzrechtlichen Bedenken gegen den Einbau und Betrieb solcher elektronischer Funkwasserzähler artikuliert. Ich nehme diese Sorgen sehr ernst, da hier wichtige Grundrechte betroffen sind: Soweit die in den elektronischen Wasserzählern gespeicherten Daten Rückschlüsse auf das Wohnverhalten der Anschlussinhaber und -inhaberinnen beziehungsweise der Hausbewohner und -bewohnerinnen zulassen – dies ist jedenfalls bei Einfamilienhäusern typischerweise der Fall – liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz für die Bundesrepublik Deutschland – GG) vor, weil personenbezogene Daten gespeichert werden. Weiter kann es zusätzlich zu einem Eingriff in das Recht auf Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG) kommen.

Vor diesem Hintergrund hatte ich bereits im vergangenen Berichtszeitraum mit Nachdruck auf die verfassungsrechtliche Notwendigkeit einer gesetzlichen Rechtsgrundlage für den Einbau und Betrieb elektronischer Wasserzähler mit Funkmodul hingewiesen (siehe nur meine Ausführungen im 27. Tätigkeitsbericht 2016 unter Nr. 6.3.1). Hierauf hat der Gesetzgeber zwischenzeitlich reagiert und im Mai 2018 mit dem Erlass des neuen Bayerischen Datenschutzgesetzes die erforderliche gesetzliche Rechtsgrundlage geschaffen (dazu sogleich Nr. 7.3.3).

7.3.2 Übergangsregelung bis zum 24. Mai 2018

Um die bis zur Schaffung der von mir geforderten Rechtsgrundlage bestehenden Unsicherheiten zu beseitigen, habe ich mich mit den (damaligen) Bayerischen Staatsministerien des Innern, für Bau und Verkehr, für Gesundheit und Pflege, für Umwelt und Verbraucherschutz sowie dem Bayerischen Gemeindetag auf folgende – bis zum 24. Mai 2018 maßgebliche – Übergangsregelung verständigt (den Gemeinden durch Rundschreiben des Innenministeriums vom 29. März 2017 bekannt gegeben):

„1. Die in elektronischen Wasserzählern gespeicherten Daten stellen personenbezogene Daten der Anschlussinhaber bzw. der Bewohner von Häusern dar, soweit ein Rückschluss auf einzelne Personen möglich ist. Einbau und Betrieb elektronischer Wasserzähler begründen daher jedenfalls bei Einfamilienhäusern Eingriffe in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG), weil personenbezogene Daten gespeichert werden, und stellen zusätzlich einen Eingriff in das Recht auf Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG) dar, soweit diese Daten aus der Wohnung heraus an den Wasserversorger übermittelt werden.

2. *Die mit dem Einbau und dem Betrieb elektronischer Wasserzähler verbundenen Eingriffe in diese Rechtspositionen erfordern eine spezifische gesetzliche Regelung, die dem gemeindlichen Satzungsgeber die wesentlichen ‚Leitplanken' vorgibt.*
3. *Bis zur Schaffung einer solchen speziellen Grundlage durch den Parlamentsgesetzgeber hat sich der Landesbeauftragte für den Datenschutz bereit erklärt, den Einbau und Betrieb der genannten Wasserzähler übergangsweise unter folgenden Bedingungen nicht zu beanstanden:*
   - *Ob elektronische Wasserzähler eingesetzt werden und ob diese mit einem ‚Funkmodul' ausgestattet werden, legt die zuständige Gemeinde durch Satzung fest; hierzu hat das Innenministerium eine Mustersatzung formuliert.*
   - *Für Wasserversorger, die privatrechtlich organisiert sind, und bei denen eine Satzungslösung nicht in Betracht kommt, haben die Gemeinden als Gesellschafter auf andere Weise die Beachtung der oben genannten Vorgaben sicherzustellen.*
   - *Die behördlichen Datenschutzbeauftragten der Gemeinde bzw. des gemeindlichen Wasserversorgungsunternehmens (Art. 25 Abs. 2 BayDSG) haben vor dem Einsatz elektronischer Wasser-zähler eine datenschutzrechtliche Freigabe nach Art. 26 BayDSG zu erteilen, in der die Erhebung, Verarbeitung und Nutzung personenbezogener Daten in den Zählern und in den Abrechnungs- bzw. Netzmanagementprogrammen genau, abschließend und für Betroffene zugänglich (vgl. Art. 27 Abs. 3 Satz 1 BayDSG) festgelegt werden; auch hierzu hat das Innenministerium ein Muster formuliert.*
   - *Die Aufgabenträger der Wasserversorgung berücksichtigen, dass einem Betroffenen über den aus der Wasserabgabesatzung oder der zugehörigen Gebührensatzung heraus Berechtigten und Verpflichteten nach Maßgabe des Art. 15 Abs. 5 BayDSG ein Widerspruchsrecht gegen den Einbau und den Betrieb elektronischer Wasserzähler mit Funkmodul eingeräumt wird. Bei dessen Vollzug sind die berührten Grundrechtspositionen angemessen zu berücksichtigen, so dass an das Vorliegen überwiegender besonderer persönlicher Interessen der Betroffenen am Ausschluss der Datenverarbeitung im Sinne von Art. 15 Abs. 5 Satz 1 BayDSG keine strengen Anforderungen gestellt werden sollen, vertiefte Darlegungen der datenschutzrechtlichen Belastungen nicht notwendig sind und insgesamt Widersprüche unbürokratisch und verwaltungsökonomisch anerkannt werden.*
   - *Wird ein Widerspruch erhoben, darf nur ein mechanischer Wasserzähler oder ein elektronischer Wasserzähler ohne oder mit deaktiviertem Funkmodul eingebaut werden.*
   - *Werden elektronische Wasserzähler ausgebaut (etwa nach Ablauf der Eichfristen), haben die Wasserversorger sicherzustellen, dass die in den Zählern gespeicherten Daten datenschutzgerecht in eigener Verantwortung vernichtet werden."*

Des Weiteren wurde § 19 Muster für eine gemeindliche Wasserabgabesatzung für die Übergangszeit wie folgt ergänzt:

„(1a) [1]Die Gemeinde ist berechtigt, einen defekten oder nach eichrechtlichen Vorschriften zu wechselnden Wasserzähler durch einen elektronischen Wasserzähler mit Funkmodul zu ersetzen. [2]Mithilfe dieser elektronischen Funkwasserzähler dür-

fen verbrauchsbezogene und trinkwasserhygienisch relevante Daten erhoben, gespeichert und verarbeitet werden. [3]Es dürfen insbesondere folgende Daten erhoben, gespeichert und verarbeitet werden:

- *Zählernummer;*
- *aktueller Zählerstand;*
- *Verbrauchssummen für Tage, Wochen, Monate und Jahre;*
- *Durchflusswerte;*
- *die Wasser- und Umgebungstemperatur für bestimmte Zeitpunkte;*
- *Betriebs- und Ausfallzeiten;*
- *Speicherung von Alarmcodes (z.B. Leckage- oder Rückflusswerte).*

[4]Die in einem elektronischen Wasserzähler mit Funkmodul gespeicherten Daten dürfen durch Empfang des Funksignals turnusmäßig (in der Regel einmal jährlich) ausgelesen werden, soweit dies zur Abrechnung oder Zwischenabrechnung erforderlich ist. [5]Sie dürfen in gleicher Weise anlassbezogen ausgelesen werden, soweit dies im Einzelfall zur Abwehr von Gefahren für den ordnungsgemäßen Betrieb der gemeindlichen Wasserversorgungsanlage erforderlich ist. [6]Zu anderen Zwecken ist eine Auslesung der gespeicherten Daten, auch durch Empfang des Funksignals, nicht zulässig. [7]Ausgelesene Daten dürfen nur zu den Zwecken von Satz 4 und Satz 5 genutzt oder verarbeitet werden. [8]Die in einem solchen Zähler gespeicherten Daten sind spätestens nach 500 Tagen zu löschen. [9]Nach Satz 5 ausgelesene Daten sind, soweit sie für die dort genannten Zwecke nicht mehr benötigt werden, spätestens aber fünf Jahre nach ihrer Auslesung zu löschen. [10]Dem Einbau und Betrieb solcher Zähler kann ein Betroffener über den aus dieser Satzung oder aus der Gebührensatzung heraus Berechtigten und Verpflichteten nach Maßgabe von Art. 15 Abs. 5 Satz 1 Bayerisches Datenschutzgesetz schriftlich widersprechen.

(2) wie geltender Abs. 2.

(3) wie geltender Abs. 3.

(4) Mechanische sowie elektronische Wasserzähler ohne Funkmodul werden von einem Beauftragten der Gemeinde möglichst in gleichen Zeitabständen oder auf Verlangen der Gemeinde vom Grundstückseigentümer selbst abgelesen bzw. ausgelesen. Bei elektronischen Wasserzählern mit Funkmodul, bei denen nicht sämtliche gespeicherte Daten per Funk übermittelt werden, erfolgt eine Auslesung vor Ort nur mit Zustimmung des Grundstückseigentümers. Dieser hat dafür zu sorgen, dass die Wasserzähler leicht zugänglich sind."

7.3.3 Seit 25. Mai 2018 gesetzliche Rechtsgrundlage vorhanden

Mit der Datenschutzreform 2018 trat am 25. Mai 2018 auch eine Vorschrift in Kraft, die eine Rechtsgrundlage für den Einbau und Betrieb elektronischer Wasserzähler mit Funkmodul enthält. Art. 39b Abs. 3 Nr. 2 BayDSG fügte diese Bestimmung in die Gemeindeordnung für den Freistaat Bayern (GO) als neuen als Art. 24 Abs. 4 GO ein:

„(4) [1]In Satzungen nach Abs. 1 Nr. 2 kann für Einrichtungen der Wasserversorgung bestimmt werden, dass die Gemeinde berechtigt ist, elektronische Wasserzähler mit oder ohne Funkmodul einzusetzen und zu betreiben. [2]In einem elektronischen Wasserzähler dürfen nur Daten gespeichert und verarbeitet werden, die zur Erfüllung der Pflichtaufgabe der Wasserversorgung und zur Gewährleistung der Betriebssicherheit und Hygiene der gesamten Wasserversorgungseinrichtung erforderlich sind. [3]Die gespeicherten Daten dürfen nur ausgelesen und verwendet werden

1. zur periodischen Abrechnung oder Zwischenabrechnung des Wasserverbrauchs und
2. anlassbezogen, soweit dies im Einzelfall zur Abwehr von Gefahren für den ordnungsgemäßen Betrieb der Wasserversorgungseinrichtung und zur Aufklärung von Störungen im Wasserversorgungsnetz erforderlich ist.

[4]Jahresverbrauchswerte dürfen ferner zur Berechnung und Festsetzung der Gebühren für die Benutzung einer Abwasserbeseitigungseinrichtung ausgelesen und verwendet werden. [5]Soll ein Wasserzähler mit Funkmodul eingesetzt werden, weist die Gemeinde den Gebührenschuldner und den Eigentümer des versorgten Objekts spätestens drei Wochen vorher in einer verständlichen und von anderen Informationen getrennten Form darauf hin, dass sie oder ein berechtigter Nutzer dem Betrieb eines Wasserzählers unter Verwendung der Funkfunktion innerhalb einer Ausschlussfrist von zwei Wochen nach Zugang des Hinweises jeweils unabhängig voneinander schriftlich widersprechen können. [6]Übt einer der Berechtigten das Widerspruchsrecht fristgerecht aus, darf ein elektronischer Wasserzähler nicht unter Verwendung der Funkfunktion betrieben werden. [7]Die Sätze 5 und 6 finden keine Anwendung, soweit in einem versorgten Objekt mehrere Einheiten einen gemeinsamen Wasserzähler haben."

Für den Fall, dass Gemeinden die Wasserversorgung nicht selbst betreiben, sondern dies durch Unternehmen in Privatrechtsform wahrnehmen lassen, an welchen die Gemeinden Anteile besitzen, führte Art. 39b Abs. 3 Nr. 3 BayDSG in Art. 94 Abs. 4 GO folgende eine neue Regelung ein:

„(4) [1]Gehören der Gemeinde Anteile an einem Unternehmen der öffentlichen Versorgung mit Wasser (Wasserversorgungsunternehmen) in dem in § 53 HGrG bezeichneten Umfang oder bedient sie sich zur Durchführung der Wasserversorgung eines Dritten, so hat sie dafür Sorge zu tragen, dass Art. 24 Abs. 4 Satz 5 bis 7 zur entsprechenden Anwendung kommt. [2]Ist eine Beteiligung der Gemeinde an einem Wasserversorgungsunternehmen keine Mehrheitsbeteiligung im Sinn des § 53 HGrG, so soll sie darauf hinwirken, dass Art. 24 Abs. 4 Satz 5 bis 7 zur entsprechenden Anwendung kommt."

7.3.4 Datenschutzrechtliche Fortschritte für die Bürgerinnen und Bürger

Der neue Art. 24 Abs. 4 GO ist das Ergebnis eines längeren parlamentarischen Prozesses, den ich zugunsten des Datenschutzes kritisch und intensiv begleitet habe. Besonders hinweisen möchte ich insoweit auf folgende Punkte:

— Ein besonderer Gewinn aus Datenschutzsicht ist das von mir stets geforderte voraussetzungslose Widerspruchsrecht nach Art. 24 Abs. 4 Satz 5 bis 7 GO, welches dem Gebührenschuldner, dem Eigentümer und dem berechtigten Nutzer des versorgten Objekts zusteht. Es richtet sich speziell gegen den Einsatz von Funkmodulen und damit nicht gegen den elektronischen Wasserzähler an sich. Die Gemeinde hat den Gebührenschuldner und den Eigentümer spätestens drei Wochen vor dem geplanten Einbau des elektronischen Wasserzählers mit Funkmodul in einer verständlichen und von anderen Informationen getrennten Form auf dieses Widerspruchsrecht hinweisen.

  Bedauerlicherweise konnte ich insoweit nicht erreichen, dass die Gemeinde neben dem Gebührenschuldner und dem Eigentümer kraft Gesetzes auch den berechtigten Nutzer über das Widerspruchsrecht nach

Art. 24 Abs. 4 Satz 5 bis 7 GO informieren muss. Insoweit habe ich daher in intensiven Gesprächen mit dem Innenministerium unter Beteiligung des Gemeindetags und des Städtetags gefordert, dass im Zuge einer Überarbeitung des Musters für eine gemeindliche Wasserabgabesatzung die Gemeinde zumindest ermächtigt wird, berechtigte Nutzer dennoch freiwillig auf ihr Widerspruchsrecht hinzuweisen.

Das Widerspruchsrecht aus Art. 24 Abs. 4 Satz 5 bis 7 GO ist inhaltlich (materiell) nicht an bestimmte Gründe gebunden, wohl aber an formelle Voraussetzungen: So muss der Widerspruch vom Berechtigten schriftlich und innerhalb einer Ausschlussfrist von zwei Wochen nach Zugang des Hinweises erhoben werden. Übt einer der Berechtigten das Widerspruchsrecht fristgerecht aus, darf ein elektronischer Wasserzähler nicht unter Verwendung der Funkfunktion betrieben werden (Art. 24 Abs. 4 Satz 6 GO). Dies bedeutet, dass dann nur ein elektronischer Wasserzähler ohne Funkmodul oder mit deaktiviertem Funkmodul eingebaut und betrieben werden darf. Der Zählerstand des elektronischen Wasserzählers wird in diesem Fall – wie bei einem herkömmlichen mechanischen Wasserzähler – entweder von einer durch die Gemeinde beauftragten Person vor Ort abgelesen oder der vom Gebührenschuldner beziehungsweise dem Eigentümer selbst auf Verlangen der Gemeinde ausgelesen und gemeldet. Das Widerspruchsrecht aus Art. 24 Abs. 4 Satz 5 bis 7 GO vermittelt jedoch keinen Anspruch darauf, dass ein herkömmlicher mechanischer Wasserzähler (wieder) eingebaut wird.

– Neben dem Widerspruchsrecht gemäß Art. 24 Abs. 4 Satz 5 bis 7 GO, der ausschließlich dem Grundrecht auf Unverletzlichkeit der Wohnung Rechnung tragen soll, besteht das datenschutzrechtliche Widerspruchsrecht nach Art. 21 Abs. 1 DSGVO. Anders als das Widerspruchsrecht aus Art. 24 Abs. 4 Satz 5 bis 7 GO, welches sich (nur) gegen die Verwendung des Funkmoduls von elektronischen Wasserzählern richtet, umfasst das Widerspruchsrecht gemäß Art. 21 Abs. 1 DSGVO ganz allgemein die Verarbeitung personenbezogener Daten. Mit anderen Worten: Dieses Widerspruchsrecht kann – unabhängig vom Einsatz eines Funkmoduls – auch ganz generell gegen die Verarbeitung personenbezogener Daten beispielsweise durch elektronische Wasserzähler geltend gemacht werden.

  Jedoch hängt dieses Widerspruchsrecht nach Art. 21 Abs. 1 DSGVO von inhaltlichen (materiellen) Voraussetzungen ab. So muss der Betroffene Gründe, die sich aus seiner besonderen Situation ergeben, vortragen. Zudem ist die Verarbeitung nach einem Widerspruch nach Art. 21 Abs. 1 DSGVO nur dann untersagt, wenn der Verantwortliche keine zwingenden schutzwürdigen Gründe für die Verarbeitung nachweisen kann, welche die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder wenn die Verarbeitung nicht der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient. Insoweit war mir in meinen intensiven Gesprächen unter anderem mit dem Innenministerium wichtig, dass bei der Überarbeitung des Musters für eine gemeindliche Wasserabgabesatzung zumindest ein Hinweis auf diese Parallelität eingefügt wird.

– Desweiteren hat der Gesetzgeber – wie von mir stets gefordert und im Übrigen grundrechtlich sowie datenschutzrechtlich geboten –, den Kommunen beim Umfang der Datenverarbeitung keine freie Hand gelassen, sondern vielmehr strikte Vorgaben gemacht. So enthalten Art. 24 Abs. 4 Satz 2

bis Satz 4 GO unmittelbar geltende Anforderungen an die Verarbeitung von Daten in einem elektronischen Wasserzähler. Die zentralen datenschutzrechtlichen Grundsätze der Erforderlichkeit (Datenminimierung) und der Zweckbindung bilden dabei die relevanten Maßstäbe. Insoweit habe ich daher in Gesprächen mit dem Innenministerium unter Beteiligung des Gemeindetags und des Städtetags auf eine Klarstellung im neuen Muster für eine gemeindliche Wasserabgabesatzung hingewirkt, dass periodisches autonomes Funken über das Jahr hinweg grundsätzlich weder für die Jahresabrechnung noch für die Sicherstellung der Wasserversorgungssicherheit und der Trinkwasserhygiene erforderlich ist. Auch soll hervorgehoben werden, dass diese Maßgaben zur Datenminimierung bei zukünftigen Ausschreibungen zu berücksichtigen sind.

Aufgrund seiner großen Bedeutung für den Grundrechtsschutz der Bürgerinnen und Bürger werde ich das Thema weiter intensiv begleiten und mich für weitere Verbesserungen einsetzen.

7.4 Syndikusrechtsanwälte: Übermittlung der Zulassungsart an Bayerische Rechtsanwalts- und Steuerberaterversorgung

Syndikusrechtsanwälte sind erst seit dem Jahr 2016 in § 46 Abs. 2 Bundesrechtsanwaltsordnung (BRAO) legaldefiniert als Rechtsanwälte, die im Rahmen eines Anstellungsverhältnisses bei einem selbst nicht anwaltlich tätigen Arbeitgeber beschäftigt sind. In der Praxis findet man sie aber schon seit langem und häufig, vor allem bei Unternehmen, Verbänden oder Stiftungen.

Nachdem das Bundessozialgericht 2014 in mehreren Entscheidungen der bis dato wohl faktisch weitgehend praktizierten Befreiung der Syndikusrechtsanwälte von der Rentenversicherungspflicht auf der Basis der damaligen Rechtslage ein Ende gesetzt hatte, wurde diese Möglichkeit im Jahr 2016 durch eine Änderung der Bundesrechtsanwaltsordnung mittels des Gesetzes zur Neuordnung des Rechts der Syndikusanwälte und zur Änderung der Finanzgerichtsordnung vom 21. Dezember 2015 (BGBl. I S. 2517) ausdrücklich geschaffen. Auf Antrag werden Syndikusrechtsanwälte nunmehr (wieder) von der gesetzlichen Rentenversicherungspflicht befreit. Die (Alters-/Kranken-/Hinterbliebenen-)Versorgung für diesen Personenkreis wird dann über ein berufsständisches Versorgungswerk – in Bayern: die Bayerische Rechtsanwalts- und Steuerberaterversorgung – sichergestellt.

Die Bayerische Rechtsanwalts- und Steuerberaterversorgung ist die berufsständische Pflichtversorgungseinrichtung für die Mitglieder der Rechtsanwalts- und Steuerberaterkammern in Bayern sowie für die Mitglieder der Patentanwaltskammer mit Kanzleisitz in Bayern, Nordrhein-Westfalen oder Hamburg. Die Mitgliedschaft in der Bayerischen Rechtsanwalts- und Steuerberaterversorgung ist an die Mitgliedschaft in der jeweiligen Kammer geknüpft, das heißt die Mitgliedschaft im Versorgungswerk beginnt und endet grundsätzlich mit der Mitgliedschaft in der Rechtsanwalts- oder Steuerberaterkammer.

Im Verzeichnis der von den Rechtsanwaltskammern geführten Listen der zugelassenen Rechtsanwälte gemäß § 31 BRAO ist bei Syndikusrechtsanwälten seit 2016 gemäß § 46c Abs. 5 BRAO insoweit zusätzlich die Angabe aufzunehmen, dass die Zulassung zur Rechtsanwaltschaft als Syndikusrechtsanwalt erfolgt ist. Bei mehreren Tätigkeiten hat für jede der Tätigkeiten eine gesonderte Eintragung zu

erfolgen. Die **Kenntnis darüber,** ob eine **Zulassung als Syndikusrechtsanwalt erfolgt ist,** sowie gegebenenfalls deren genaue Daten (Beginn und Ende) kann nicht nur **Auswirkungen** auf Beginn und Ende der Mitgliedschaft im Versorgungswerk generell haben, sondern auch auf die konkrete Beitragsfestsetzung. Für die Bayerische Rechtsanwalts- und Steuerberaterversorgung ist die **Kenntnis** dieser bei den Rechtsanwaltskammern erhobenen und gespeicherten Daten von Syndikusrechtsanwälten damit **für die eigene Aufgabenerfüllung erforderlich.** Das Versorgungswerk ist daher konsequenterweise an der Übermittlung dieser Daten durch die Rechtsanwaltskammern interessiert.

Jedoch regelte der Art. 39 Abs. 1 Gesetz über das öffentliche Versorgungswesen (VersoG) in der bis zum 30. Juni 2018 geltenden Fassung nur die Übermittlung folgender Daten durch die Rechtsanwaltskammern in Bayern an die Bayerische Rechtsanwalts- und Steuerberaterversorgung, sofern dies für die Mitgliedschaft beim Versorgungswerk von Bedeutung sein konnte: Name, Geburtsdatum, Anschrift sowie Beginn und Ende der Kammermitgliedschaft. **Nicht ausdrücklich umfasst** war damit gerade die zusätzliche Information „**Zulassungsart**".

Da die Bundesrechtsanwaltsordnung die Mitgliedschaft in einer Rechtsanwaltskammer nicht an die konkrete Zulassungsart, sondern nur an die Zulassung als solche knüpft, kann aus der Kammermitgliedschaft als solcher auch nicht auf sonstige Weise rückgeschlossen werden, ob es sich um einen „normalen" Rechtsanwalt oder einen Syndikusrechtsanwalt handelt.

Insoweit habe ich dem mit der Bitte um Beratung an mich herangetretenen Versorgungswerk folgende Hinweise gegeben:

Bei der Beurteilung der Norm daraufhin, ob diese auch die Übermittlung der Zulassungsart durch die Rechtsanwaltskammern abdeckt, ist besonderes Augenmerk auf den mit „sofern" eingeleiteten Nebensatz zu legen. Aus diesem ergibt sich die generelle Aussage des Gesetzgebers, dass dem berufsständischen Versorgungsträger die zur ordnungsgemäßen Beurteilung einer Beitragspflicht erforderlichen Statusangaben übermittelt werden sollen. Das gesetzgeberische Ziel, durch die Zulassungsentscheidung Klarheit hinsichtlich der Zuordnung zu einem der in Betracht kommenden Sicherungssysteme zu schaffen, kann insoweit letztlich nur dann erreicht werden, wenn auch dem berufsständischen Versorgungsträger bekannt ist, bei welchen Personen es sich um Syndikusrechtsanwälte handelt. Vor diesem Hintergrund habe ich daher **keine grundsätzlichen datenschutzrechtlichen Bedenken** dagegen erhoben, dass sich eine Datenübermittlung durch die Kammern zu Beginn und Ende der Kammermitgliedschaft **auch** auf die jeweilige **Art der Zulassung** erstreckte.

Ich habe mich aber dennoch für eine **Anpassung von Art. 39 Abs. 1 VersoG an die seit 2016 geänderten bundesrechtlichen Rahmenbedingungen** ausgesprochen, da schon aus Gründen der Rechtsklarheit die Art der Zulassung als weiteres Datum ausdrücklich Aufnahme in die Vorschrift finden sollte. Eine entsprechende **Gesetzesänderung** hat der bayerische Gesetzgeber im Rahmen des Gesetzes zur Änderung des Gesetzes über das öffentliche Versorgungswesen und weiterer Rechtsvorschriften vom 12. Juni 2018 (GVBl. S. 391) **bereits vorgenommen** und diese hierbei auch auf die parallele Fragestellung bei Syndikuspatentanwälten erstreckt.

Art. 39 VersoG
Datenübermittlung
(1) Die Rechtsanwalts- und die Steuerberaterkammern in Bayern übermitteln der Bayerischen Rechtsanwalts- und Steuerberaterversorgung jeweils den Namen, das Geburtsdatum, die Anschrift, die Art der Zulassung oder Bestellung sowie den Beginn und das Ende der Kammermitgliedschaft ihrer Mitglieder, sofern dies für deren Mitgliedschaft bei der Bayerischen Rechtsanwalts- und Steuerberaterversorgung von Bedeutung sein kann.
(2) Die Patentanwaltskammer übermittelt der Bayerischen Rechtsanwalts- und Steuerberaterversorgung jeweils den Namen, das Geburtsdatum, die Anschrift und die Art der Zulassung der Kammermitglieder mit Kanzleisitz in Bayern sowie den jeweiligen Zeitpunkt der Einrichtung und der Aufgabe des Kanzleisitzes in Bayern.

7.5 Landpachtverkehrsgesetz: kein Beteiligungsrecht des Bayerischen Bauernverbandes bei der Beanstandung von Landpachtverträgen

Mit den Beteiligungsrechten des Bayerischen Bauernverbandes als land- und forstwirtschaftliche Berufsvertretung habe ich mich in datenschutzrechtlicher Hinsicht bereits in der Vergangenheit intensiv befasst. So war Gegenstand meines 16. Tätigkeitsberichts 1994 unter Nr. 8.6 dessen Anhörung bei Verfahren nach dem Gesetz über Maßnahmen zur Verbesserung der Agrarstruktur und zur Sicherung land- und forstwirtschaftlicher Betriebe (Grundstücksverkehrsgesetz – GrdstVG). Im aktuellen Berichtszeitraum war ich nun aufgrund einer Eingabe mit der Frage befasst, ob und in welchem Umfang behördlicherseits eine Einbindung des Bayerischen Bauernverbandes beim Vollzug des Gesetzes über die Anzeige und Beanstandung von Landpachtverträgen (Landpachtverkehrsgesetz – LPachtVG) zulässig ist.

Gemäß §§ 2, 3 LPachtVG hat ein Verpächter den Abschluss eines Landpachtvertrages sowie bestimmte wesentliche Änderungen eines solchen Vertrages grundsätzlich der in Bayern für den Vollzug des LPachtVG gemäß Art. 1 Gesetz zur Sicherung der bäuerlichen Agrarstruktur sachlich und nach § 6 LPachtVG örtlich zuständigen Kreisverwaltungsbehörde anzuzeigen. Diese kann gemäß § 4 Abs. 1 LPachtVG einen anzuzeigenden Landpachtvertrag oder eine anzuzeigende Vertragsänderung im Wesentlichen beanstanden, wenn die Verpachtung eine ungesunde Verteilung der Bodennutzung bedeutet, oder eine unwirtschaftliche Nutzungsaufteilung darstellt beziehungsweise die Pacht unangemessen ist.

§ 4 LPachtVG
Beanstandung
(1) Die zuständige Behörde kann einen anzuzeigenden Landpachtvertrag oder eine anzuzeigende Vertragsänderung beanstanden, wenn
1. *die Verpachtung eine ungesunde Verteilung der Bodennutzung, insbesondere eine ungesunde Anhäufung von land- und forstwirtschaftlichen Nutzflächen, bedeutet,*
2. *durch die Verpachtung ein Grundstück oder eine Mehrheit von Grundstücken, die räumlich oder wirtschaftlich zusammenhängen, unwirtschaftlich in der Nutzung aufgeteilt wird oder*
3. *die Pacht nicht in einem angemessenen Verhältnis zu dem Ertrag steht, der bei ordnungsmäßiger Bewirtschaftung nachhaltig zu erzielen ist.*

(2) […]

Meine Überprüfung ergab insoweit, dass beim Abschluss von Landpachtverträgen häufig ein vom Bayerischen Bauernverband herausgegebenes Musterformular verwendet wurde, welches die Verbandsbeteiligung im Rahmen des Anzeigeverfahrens gegenüber der Kreisverwaltungsbehörde vorsah. Dies führte in der Praxis dazu, dass Anzeigen nach §§ 2, 3 LPachtVG gegenüber den Kreisverwaltungsbehörden regelmäßig in Gestalt eines bereits mit einem Begutachtungsvermerk des Bayerischen Bauernverbandes versehenen Formulars erfolgten. Zusätzlich verfuhren Kreisverwaltungsbehörden im Falle einer im Zeitpunkt der ihnen gegenüber erfolgten Anzeige noch fehlenden Verbandsbeteiligung teilweise seit vielen Jahren dergestalt, dass sie im Rahmen des Beanstandungsverfahrens nach § 7 LPachtVG den Landpachtvertrag zunächst dem Bayerischen Bauernverband zur fachlichen Prüfung hinsichtlich der Voraussetzungen des § 4 LPachtVG zuleiteten.

Während jedoch für die Genehmigung der rechtsgeschäftlichen Veräußerung eines (potentiell) land- und forstwirtschaftlichen Grundstücks gemäß §§ 1, 2 GrdstVG in § 19 GrdstVG geregelt ist, dass die Genehmigungsbehörde vor der Entscheidung über einen Genehmigungsantrag die land- und forstwirtschaftliche Berufsvertretung zu hören hat, ist eine solche **Beteiligung im Rahmen des Landpachtverkehrsgesetzes gerade nicht vorgesehen.** Eine **Rechtsgrundlage für die Übermittlung personenbezogener Daten** durch die Kreisverwaltungsbehörde an den Bayerischen Bauernverband im Vollzug des Landpachtverkehrsgesetzes **besteht** insoweit gerade **nicht**.

Wegen der übergeordneten Bedeutung des Sachverhalts habe ich mich insoweit an das fachlich zuständige Bayerische Staatsministerium für Ernährung, Landwirtschaft und Forsten gewandt. Dieses teilte meine Einschätzung, dass eine formelle Beteiligung des Bayerischen Bauernverbandes beim Vollzug des Landpachtverkehrsgesetzes vom Gesetzgeber nicht vorgesehen ist. Das Landwirtschaftsministerium hat gegenüber den nachgeordneten Behörden die Rechtslage klargestellt, um gegebenenfalls dort bestehende Missverständnisse zu beseitigen. Zukünftig sollen die Kreisverwaltungsbehörden erforderliche Informationen zur fachlichen Beurteilung der Beanstandungsgründe des § 4 LPachtVG vornehmlich bei den Ämtern für Ernährung, Landwirtschaft und Forsten einholen. Der Bayerische Bauernverband hat sich auf Veranlassung des Landwirtschaftsministeriums mit der Anpassung seiner Muster-Landpachtverträge einverstanden erklärt. Es soll der entstandene Eindruck beseitigt werden, der Bayerische Bauernverband sei eine vorgeschriebene „Hürde“ auf dem Weg zur wirksamen Anzeige des Landpachtvertrages.

Ergänzend weise ich auf Folgendes hin: Sofern die Vertragsparteien ihre abgeschlossenen beziehungsweise geänderten Landpachtverträge im Rahmen der zur Verfügung stehenden Monatsfrist des § 2 Abs. 2 LPachtVG vor deren Anzeige bei der Kreisverwaltungsbehörde einer anderen Stelle, wie zum Beispiel dem Bayerischen Bauernverband vorlegen möchten, ist ihnen dies natürlich unbenommen. Diese Vorlage kann jedoch von der Behörde weder eingefordert noch selbst bewirkt werden. Sofern im Rahmen des Beanstandungsverfahrens nach § 7 LPachtVG behördlicherseits Auskünfte beim Bayerischen Bauernverband eingeholt werden sollen, dürfen keine personenbezogenen Daten an diesen übermittelt werden.

7.6 Durchsetzung eines Hausverbots mittels Foto des Betroffenen

Behörden müssen auch mit aus ihrer Sicht schwierigen Besuchern und Besucherinnen zurechtkommen und diese ihr Anliegen grundsätzlich ungehindert vortragen lassen. Der Ausspruch eines Hausverbots kann aber auch für eine noch so bürgerfreundliche Verwaltung zum Thema werden, wenn Personen den Dienstablauf nachhaltig stören, beispielsweise Bedienstete beleidigen oder bedrohen und eine Wiederholung derartiger Vorfälle zu besorgen ist. Ein solches behördliches Hausverbot findet – auch im Fall des Fehlens ausdrücklicher (gesetzlicher) Regelung – seine rechtliche Grundlage im Hausrecht, welches notwendiger Annex der Sachkompetenz eines Hoheitsträgers bei der Erfüllung ihm übertragenen Verwaltungsaufgaben ist. Dieses Hausrecht gibt dem Hoheitsträger insbesondere das Recht, zur Wahrung der Zweckbestimmung der im Verwaltungsgebrauch stehenden Gebäude und Räumlichkeiten sowie zur Abwehr von Störungen des Dienstbetriebs den Aufenthalt von Personen in den Dienstgebäuden zu regeln.

Mit der Frage, welche datenschutzrechtlichen Anforderungen bei der effektiven Durchsetzung derartiger behördlicher Hausverbote zu beachten sind, wurde ich auch im Berichtszeitraum konfrontiert. So wollte beispielsweise eine Gemeinde wissen, ob die Übermittlung eines bei der Kreisverwaltungsbehörde im dortigen Aufgabenbereich erstellten Lichtbildes an die Gemeinde, welche ein Hausverbot gegen dieselbe Person ausgesprochen hatte, datenschutzrechtlich zulässig ist. Hieran anschließend ging es der Gemeinde darum, ob auch das Aushängen dieses Fotos in den Verwaltungsgebäuden der Gemeinde zulässig ist. Hierzu habe ich folgende Hinweise gegeben:

Bei einer hinreichend scharfen Lichtbildaufnahme der vom ausgesprochenen Hausverbot betroffenen Person, welche deren Identifizierung ermöglicht, handelt es sich unproblematisch um ein personenbezogenes Datum im Sinne des Art. 4 Nr. 1 DSGVO.

Sowohl die Übermittlung des Fotos von der Kreisverwaltungsbehörde an die Gemeinde als auch das anschließende Aushängen dieses Fotos in den Verwaltungsgebäuden der Gemeinde stellen jeweils eigenständige Verarbeitungen personenbezogener Daten gemäß Art. 4 Nr. 2 DSGVO dar. Für beide Datenverarbeitungen sind daher Rechtsgrundlagen nach Art. 6 Abs. 1 DSGVO erforderlich. Das können auch Verarbeitungsbefugnisse des nationalen Rechts sein (vgl. Art. 6 Abs. 1 UAbs. 1 Buchst. e, und Abs. 3 UAbs. 1 Buchst. b DSGVO).

Wenn sich spezialgesetzlich geregelte Datenverarbeitungsbefugnisse zu Fragen der Sicherstellung des Hausrechts nicht verhalten, was regelmäßig der Fall ist, und diesen Vorschriften keine abschließende Sperrwirkung hinsichtlich der Nutzung von Lichtbildern auch für diesen Zweck entnommen werden kann, kommen als subsidiäre mitgliedstaatliche Verarbeitungsbefugnisse auch Art. 4 Abs. 1 und Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG in Betracht.

Art. 4 BayDSG
Rechtmäßigkeit der Verarbeitung
(1) Die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle ist unbeschadet sonstiger Bestimmungen zulässig, wenn sie zur Erfüllung einer ihr obliegenden Aufgabe erforderlich ist.
(2) […]

Art. 5 BayDSG
Übermittlung
(1) [1]Eine Übermittlung personenbezogener Daten ist zulässig, wenn
1. sie zur Erfüllung einer der übermittelnden oder der empfangenden öffentlichen Stelle obliegenden Aufgabe erforderlich ist oder
2. […]

Maßgeblich für die Rechtmäßigkeit einer **Übermittlung** des bei der Kreisverwaltungsbehörde im dortigen Aufgabenbereich entstandenen Fotos an die Gemeinde war danach, ob dies gemäß Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG „zur Erfüllung einer der […] empfangenden öffentlichen Stelle obliegenden Aufgabe erforderlich ist".

Dies ließ sich mit folgender Erwägung bejahen: Die Übermittlung des Fotos bezweckt, der Gemeinde die effektive Durchsetzung des von ihr in Ausübung des Hausrechts gegen die betroffene Person verhängten Hausverbots zu ermöglichen. Ohne Kenntnis des Aussehens der betroffenen Person können die Mitarbeiterinnen und Mitarbeiter nicht das Betreten der gemeindlichen Verwaltungsgebäude durch diese verhindern.

Dem steht auch nicht entgegen, dass Art. 24 Abs. 1 BayDSG für den Fall einer Videoüberwachung zwischen der Erfüllung öffentlicher Aufgaben und der Ausübung des Hausrechts differenziert. Der theoretisch hieraus ableitbare Schluss, die Ausübung des Hausrechts durch die Gemeinde sei keine dieser obliegende Aufgabe im Sinne der Art. 4 Abs. 1 und Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG, trägt nicht. Zunächst einmal ist darauf hinzuweisen, dass schon der Wortlaut der Bestimmungen nicht identisch ist. So sprechen Art. 4 Abs. 1, Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG von einer „obliegenden Aufgabe", während Art. 24 Abs. 1 BayDSG den Begriff der „öffentlichen Aufgabe" verwendet. Vor allem aber wird im Rahmen der Auslegung des Art. 24 Abs. 1 BayDSG mit überzeugender Argumentation vertreten, dass innerhalb von Gebäuden und Grundstücken beide Alternativen nebeneinander treten, da öffentliche Aufgabe nämlich gerade auch die Aufrechterhaltung der Funktionsfähigkeit der öffentlichen Stelle, insbesondere der Möglichkeit eines ungestörten Besucherverkehrs oder einer ungestörten Nutzung sei (siehe auch Wilde/Ehmann/Niese/Knoblauch, Datenschutz in Bayern, Stand Juni 2018, Art. 24 BayDSG Rn. 19 f.).

Vor diesem Hintergrund ist auch das **Aushängen** des Fotos in den betroffenen Einrichtungen der Gemeinde grundsätzlich nach Art. 4 Abs. 1 BayDSG gerechtfertigt. Allerdings ist bei der Prüfung der Erforderlichkeit des konkreten Datenumgangs darauf zu achten, dass das Foto durch den Aushang nur den Bediensteten der Einrichtung selbst zur Kenntnis gebracht wird. Konkret bedeutet dies, dass das Foto nur in den Diensträumen selbst (vorzugsweise – soweit vorhanden– im Pförtnerbüro, im Übrigen in den Mitarbeiterbüros) und auch dort nur so anzubringen ist, dass Besucherinnen und Besucher keine Sicht auf das Foto haben. Nicht erforderlich wäre dagegen der Aushang in Publikumsbereichen wie zum Beispiel einem Warteraum. Insoweit läge dann nämlich eine zusätzliche und eigenständiger datenschutzrechtlicher Rechtfertigung bedürfende Übermittlung eines personenbezogenen Datums an eine unbestimmte Zahl nicht öffentlicher Stellen (die Besucher und Besucherinnen) vor. Deren Rechtfertigung wird aber wegen der Gefahr einer „Prangerwirkung" regelmäßig ausscheiden.

7.7 Personenbezogene Angaben auf Parkausweisen

7.7.1 Parkerleichterungen für kurzzeitig schwerbehinderte Menschen mit vorübergehender Gehbehinderung

Mit der Problematik personenbezogener Angaben auf regulären Parkausweisen für Schwerbehinderte habe ich mich in der Vergangenheit bereits mehrfach befasst, zuletzt in meinem 25. Tätigkeitsbericht 2012 unter Nr. 12.6. Meine diesbezüglichen Hinweise – eine Namensangabe auf dem bayerischen Parkausweis für Schwerbehinderte auf der Ausweisvorderseite ist nicht erforderlich; soweit Namenseintrag zu Kontrollzwecken unverzichtbar sein sollte, kann der Name auf der Ausweisrückseite eingetragen oder das Abdecken des Namensfeldes auf der Vorderseite des Ausweismusters „nur Bayern“ zugelassen werden, wenn das kombinierte doppelseitige Ausweismuster Verwendung findet und damit ein Eintrag des Namens auf der Rückseite des Ausweises nicht mehr möglich ist – wurden vom damaligen Bayerischen Staatsministerium des Innern bei der Neufassung der Anwendungshinweise zum Vollzug der Straßenverkehrs-Ordnung bereits berücksichtigt.

Im Berichtszeitraum wurde nun die Frage an mich herangetragen, was bei der Erteilung von Ausnahmegenehmigungen zur Gewährung von Parkerleichterungen für kurzzeitig schwerbehinderte Menschen mit vorübergehender Gehbehinderung nach § 46 Abs. 1 Nr. 11 Straßenverkehrs-Ordnung (StVO) gilt. Konkret: Ist auf der beim Parken sichtbar auszulegenden Vorderseite der Ausnahmegenehmigung der jeweilige Name des Genehmigungsinhabers zwingend einzutragen?

Aussehen und Inhalt des Parkausweises zur Gewährung von Parkerleichterungen bei vorübergehender Gehbehinderung sind in den Anwendungshinweisen zum Vollzug des § 46 Abs. 1 StVO – anders als hinsichtlich regulärer Parkausweise – bislang nicht verbindlich geregelt. Ich vertrete hierzu – entsprechend den Vorgaben für reguläre Parkausweise – folgende Auffassung: Falls ein Genehmigungsinhaber mit der Nennung seines Namens auf der Vorderseite der Ausnahmegenehmigung nicht einverstanden ist, sollte die Genehmigungsbehörde auf seinen Wunsch hin das Namensfeld freilassen und den Namen auf der Rückseite oder einer der Folgeseiten eintragen. Alternativ ist aber auch möglich, bei der formlos ausfertigbaren Ausnahmegenehmigung die **Abdeckung des Namensfeldes auf der Vorderseite durch den Genehmigungsinhaber** während der sichtbaren Auslegung beim Parken zuzulassen.

Insoweit konnte ich erreichen, dass das Innenministerium meine Anregungen im Rahmen der Fortschreibung der Anwendungshinweise zum Vollzug der Straßenverkehrs-Ordnung bei nächster Gelegenheit berücksichtigen wird. Es ist derzeit vorgesehen, hinsichtlich der inhaltlichen und grafischen Ausgestaltung der Gewährung von Parkerleichterungen für kurzzeitig schwerbehinderte Menschen mit vorübergehender Gehbehinderung darauf hinzuweisen, dass keine Bedenken dagegen bestehen, wenn das Namensfeld auf der sichtbar auszulegenden Seite der Ausnahmegenehmigung nicht erscheint oder das Namensfeld auf der sichtbar auszulegenden Seite vom Genehmigungsinhaber so abgedeckt wird, dass die Abdeckung zu Kontrollzwecken jederzeit wieder leicht entfernt werden kann.

7.7.2 Parkerleichterungen für Handwerksbetriebe

Gemäß § 46 Abs. 1 StVO können die Straßenverkehrsbehörden in bestimmten Einzelfällen oder allgemein für bestimmte Antragsteller Ausnahmen genehmigen, etwa von Parkverboten, vom Verbot des Parkens auf Gehwegen, von der Betätigung von Parkscheinautomaten und vom Verbot der Benutzung von Fußgängerbereichen. Sachlich hiervon umfasst sind auch Parkerleichterungen für Handwerksbetriebe. Fachliche Voraussetzung für die Erteilung einer solchen Ausnahmegenehmigung ist insbesondere, dass ein Handwerker zur Erfüllung seiner Aufgaben zwingend auf die Benutzung eines Kraftfahrzeuges am Einsatzort angewiesen ist.

Das Innenministerium hat das Verfahren hinsichtlich dieser Ausnahmegenehmigungen durch Anwendungshinweise zum Vollzug der Straßenverkehrs-Ordnung geregelt. Diese sehen insoweit vor, dass neben dem Parkausweis, welcher den Namen des Handwerksbetriebs, die Genehmigungsbehörde, die Geltungsdauer und das amtliche Kennzeichen des Fahrzeugs enthält, zusätzlich ein schriftlicher Hinweis darauf, wo und seit wann gearbeitet wird (sogenannter Arbeitsstättennachweis) stets gut lesbar hinter der Windschutzscheibe auszulegen ist.

Zu dieser Thematik haben mich seit Geltungsbeginn der Datenschutz-Grundverordnung mehrere Anfragen von Handwerkerinnen und Handwerkern erreicht. Diese können als Einzelunternehmer für ihre personenbezogenen Daten (zum Beispiel Name und Anschrift auf dem Parkausweis oder auf dem Arbeitsstättennachweis) das Grundrecht auf informationelle Selbstbestimmung sowie das unionsrechtliche Datenschutzgrundrecht geltend machen (vgl. auch Erwägungsgrund 14 DSGVO). Die datenschutzrechtliche Prüfung ergab insofern Folgendes:

Werden Parkausweis und Arbeitsstättennachweis mit personenbezogenen Daten hinter der Windschutzscheibe des Handwerkerfahrzeuges ausgelegt, handelt es sich nach meiner seit jeher vertretenen Rechtsauffassung um deren Bereitstellung zur Erhebung der darin enthaltenen personenbezogenen Daten durch öffentliche Stellen, wobei die Möglichkeit der Kenntnisnahme durch die Allgemeinheit eine bloße Nebenfolge ist. Diese Form der Datenverarbeitung habe ich daher stets anhand der Bestimmungen über die Datenerhebung durch öffentliche Stellen gemessen.

Eine Erhebung durch die zuständige Straßenverkehrsbehörde ist nach Art. 4 Abs. 1 BayDSG zulässig, wenn die Kenntnis der Daten zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben erforderlich ist.

Personenbezogene Daten einer Handwerkerin oder eines Handwerkers erhebt die zuständige Straßenverkehrsbehörde in solchen Fällen, um bei Kontrollen feststellen zu können, ob tatsächlich eine Ausnahmegenehmigung erteilt wurde. Zudem sind die Angaben auf dem Parkausweis – Firmenname und Anschrift – ohnehin oftmals bereits auf dem Firmenfahrzeug selbst sichtbar angebracht. Ein schutzwürdiges Interesse der Handwerkerin oder des Handwerkers am Ausschluss der Erhebungsmöglichkeit dieser Daten ist daher nicht erkennbar.

Für die Erhebung personenbezogener Daten von Kundinnen oder Kunden – Stichwort: Arbeitsstättennachweis – müssen aber zusätzlich die Voraussetzungen des Art. 4 Abs. 2 Sätze 2 und 3 BayDSG vorliegen, da die Kundendaten insoweit bei einem Dritten, dem Handwerksbetrieb erhoben werden.

Nach Ansicht des hierzu von mir um Stellungnahme gebetenen Innenministeriums ist die Erhebung des Ortes, an dem gerade gearbeitet wird, beim Handwerksbetrieb gemäß Art. 4 Abs. 2 Satz 2 Nr. 2 BayDSG erforderlich; eine Erhebung bei den Kundinnen oder Kunden selbst wäre gemäß Art. 4 Abs. 2 Satz 2 Nr. 3 BayDSG unverhältnismäßig, wenn die Straßenverkehrsbehörde kontrollieren will, ob berechtigterweise von einer Parkerleichterung Gebrauch gemacht wird. Auch würden keine Anhaltspunkte gemäß Art. 4 Abs. 2 Satz 3 BayDSG für die Betroffenheit schutzwürdiger Kundeninteressen bestehen. Zum einen sei es für interessierte Außenstehende ohnehin regelmäßig leicht möglich herauszufinden, wo gearbeitet wird. Zum anderen handele es sich bei der Tatsache, dass jemand einen Handwerksbetrieb beschäftigt, nicht um besonders schutzwürdige (besondere Kategorien) personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO.

Ich bin dieser Auffassung nicht grundsätzlich entgegengetreten. Maßgeblich sind jeweils die konkreten Umstände des Einzelfalles. Von daher habe ich beim Innenministerium angeregt, auf den Hinweis im Arbeitsstättenhinweis wo und seit wann gearbeitet wird, zumindest dann zu verzichten, falls Handwerksbetriebe glaubhaft darlegen können, dass ihre Kundinnen oder Kunden dies berechtigterweise überwiegend wünschen. Zu denken ist hier vor allem an pflegebedürftige Kundinnen oder Kunden von Handwerksbetrieben mit dem Schwerpunkt barrierefreie Umgestaltung des Wohnraums oder von Sicherheitsfirmen mit dem Schwerpunkt Objektsicherung. Diese Kundinnen und Kunden können durchaus ein überwiegendes schutzwürdiges Interesse gemäß Art. 4 Abs. 2 Satz 3 BayDSG geltend machen, da etwa ein Hinweis auf die Wohnung einer pflegebedürftigen oder einer gefährdeten Person in dem geparkten Handwerkerfahrzeug auch von Außenstehenden gelesen werden kann, welche Informationen dieser Art zum Nachteil einer betroffenen Person verwenden wollen. Den berechtigten Kontrollinteressen der Straßenverkehrsbehörden könnte in solchen Fällen auch durch die Angabe der telefonischen Erreichbarkeit der Handwerkerin oder des Handwerkers im Arbeitsstättennachweis – anstelle von Angaben zu Kundinnen oder Kunden – Rechnung getragen werden.

Insoweit konnte ich erreichen, dass das Innenministerium meine vorgenannte Anregung im Rahmen der Fortschreibung der Anwendungshinweise zum Vollzug der Straßenverkehrs-Ordnung bei nächster Gelegenheit berücksichtigen wird.

7.8 Datenschutz im Vorfeld von Wahlen

Im Berichtszeitraum war ich aufgrund der Landtags- und Bezirkswahl 2018 verstärkt mit Anfragen zum Datenschutz im Vorfeld von Wahlen befasst. Exemplarisch darstellen möchte ich folgende zwei an mich herangetragene Fragestellungen:

7.8.1 Meldedatenübermittlungen für Wahlwerbung

Sowohl Bürgerinnen und Bürger als auch Meldebehörden wollten häufig wissen, ob es unter dem Datenschutzregime der Datenschutz-Grundverordnung weiterhin zulässig ist, Meldedaten für Wahlwerbung insbesondere an politische Parteien zu übermitteln. Hierzu habe ich unter Ergänzung der zuletzt in meinem 26. Tätigkeitsbericht 2014 unter Nr. 6.15 gemachten Anmerkungen folgende Hinweise gegeben:

Meldedaten stellen personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO dar. Werden diese von der Meldebehörde an einen externen Dritten, wie etwa eine politische Partei übermittelt, liegt eine Datenverarbeitung gemäß Art. 4 Nr. 2 DSGVO vor. Jede Datenverarbeitung bedarf gemäß Art. 6 Abs. 1 DSGVO einer Rechtsgrundlage, da es sich andernfalls um einen rechtswidrigen Eingriff in das informationelle Selbstbestimmungsrecht der hiervon betroffenen Personen handelt. Für den Bereich der hier thematisch einschlägigen Erfüllung einer Aufgabe im öffentlichen Interesse gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO eröffnet die Norm in deren Absätzen 2 und 3 auch den Mitgliedstaaten Regelungsspielräume.

Artikel 6 DSGVO
Rechtmäßigkeit der Verarbeitung
(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
[…]
e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
[…]
(2) Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.
(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch
a) Unionsrecht oder
b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.
[…]

Von diesen Regelungsspielräumen hat der nach dem Grundgesetz für das Melderecht zuständige Bundesgesetzgeber mit dem Bundesmeldegesetz (BMG) Gebrauch gemacht und speziell für Meldedatenübermittlungen im Zusammenhang mit Wahlen eine Regelung in § 50 Abs. 1 BMG getroffen. Nach dieser Norm darf die Meldebehörde Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit Wahlen in den sechs Monaten vor der Wahl Auskunft aus dem Melderegister erteilen. Mitgeteilt werden nur Familienname, Vornamen, Doktorgrad und die derzeitigen Anschriften sowie, sofern die Person verstorben ist, diese Tatsache.

§ 50 BMG
Melderegisterauskünfte in besonderen Fällen
(1) [1]Die Meldebehörde darf 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 Absatz 1 Satz 1 bezeichneten Daten von Gruppen von Wahlberechtigten erteilen, soweit für deren Zusammensetzung das Lebensalter bestimmend ist. [2]Die Geburtsdaten der Wahlberechtigten dürfen dabei nicht mitgeteilt werden. [3]Die Person oder Stelle, der die

Daten übermittelt werden, darf diese nur für die Werbung bei einer Wahl oder Abstimmung verwenden und hat sie spätestens einen Monat nach der Wahl oder Abstimmung zu löschen oder zu vernichten.
[…]
(5) Die betroffene Person hat das Recht, der Übermittlung ihrer Daten nach den Absätzen 1 bis 3 zu widersprechen; hierauf ist bei der Anmeldung nach § 17 Absatz 1 sowie einmal jährlich durch ortsübliche Bekanntmachung hinzuweisen.

§ 44 BMG
Einfache Melderegisterauskunft
(1) [1]Wenn eine Person zu einer anderen Person oder wenn eine andere als die in § 34 Absatz 1 Satz 1 oder § 35 bezeichnete Stelle Auskunft verlangt, darf die Meldebehörde nur Auskunft über folgende Daten einzelner bestimmter Personen erteilen (einfache Melderegisterauskunft):
1. Familienname,
2. Vornamen unter Kennzeichnung des gebräuchlichen Vornamens,
3. Doktorgrad und
4. derzeitige Anschriften sowie,
5. sofern die Person verstorben ist, diese Tatsache.
[…]

Durch § 50 Abs. 1 BMG möchte der Gesetzgeber Parteien, Wählergruppen und Trägern von Wahlvorschlägen eine altersspezifische Wahlwerbung ermöglichen und damit die Durchführung von Wahlen unterstützen. Die Auskunftsberechtigten sollen Mitglieder 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 Datenempfänger.

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 BMG eine Widerspruchsmöglichkeit vorgesehen. Auf diese Möglichkeit ist seit Inkrafttreten des Bundesmeldegesetzes zum 1. November 2015 sowohl bei jeder Anmeldung von Bürgerinnen und Bürgern sowie einmal jährlich durch ortsübliche Bekanntmachung hinzuweisen. Der Widerspruch nach Art. 50 Abs. 5 BMG kann schriftlich oder mündlich bei der Meldebehörde eingelegt werden. Er ist nicht von bestimmten Voraussetzungen abhängig und muss nicht begründet werden. § 50 Abs. 5 BMG wird voraussichtlich durch Art. 16 Zweites Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 geändert. Danach soll § 50 Abs. 5 BMG durch einen Satz 2 ergänzt werden, in dem auf einen neuen § 36 Abs. 2 Satz 2 BMG verwiesen wird. Diese Vorschrift soll bei einem Widerspruch der betroffenen Person gegenüber der Meldebehörde ein Recht auf unentgeltliche Eintragung einer Übermittlungssperre einräumen und war bisher in § 9 Satz 1 Nr. 5 BMG enthalten.

7.8.2 Bescheinigung der Unterstützung von Wahlkreisvorschlägen

Aufgrund einer an mich gerichteten Eingabe weise ich ergänzend zu meinen Ausführungen im 24. Tätigkeitsbericht 2010 unter Nr. 6.12 nochmals auf die bei der Bescheinigung der Unterstützung von Wahlkreisvorschlägen zu beachtenden Datenschutzanforderungen hin. So müssen nach Art. 27 Abs. 1 Nr. 4 Satz 2 Gesetz

über Landtagswahl, Volksbegehren, Volksentscheid und Volksbefragung Wahlkreisvorschläge mit einer bestimmten Zahl von Unterstützungsunterschriften versehen sein:

Art. 27
Inhalt und Form der Wahlkreisvorschläge
(1) Die Wahlkreisvorschläge müssen folgende Voraussetzungen erfüllen:
[…]
4. […] [2]Sie müssen außerdem von 1 v. T. der Stimmberechtigten des Wahlkreises bei der letzten Abstimmung nach diesem Gesetz, jedoch höchstens von 2 000 Stimmberechtigten persönlich unterzeichnet sein, sofern nicht die Partei oder Wählergruppe bei der letzten Landtagswahl im gesamten Wahlgebiet mindestens 1,25 v. H. der abgegebenen gültigen Stimmen erhalten hat; das Stimmrecht muss im Zeitpunkt der Unterzeichnung gegeben sein und ist bei Einreichung des Wahlkreisvorschlags nachzuweisen.
[…]

Ergänzend ordnet § 31 Abs. 3 Nr. 3 Wahlordnung für Landtagswahlen, Volksbegehren und Volksentscheide (Landeswahlordnung – LWO) an, für jeden Unterzeichner auf einem amtlichen Formblatt oder gesondert eine Bescheinigung der Gemeinde, bei welcher der Unterzeichner im Wählerverzeichnis eingetragen ist, beizufügen mit der Bestätigung, dass er im betreffenden Wahlkreis stimmberechtigt ist. Dabei ist jedoch zu beachten, dass gemäß § 31 Abs. 3 Nr. 4 LWO jeder stimmberechtigte Bürger nur einen Wahlkreisvorschlag unterstützen darf. In der Konsequenz bestimmt § 31 Abs. 5 Satz 2 LWO, dass die Gemeinde für jede stimmberechtigte Person die Bescheinigung des Stimmrechts nur einmal zu einem Wahlkreisvorschlag erteilen, hierbei aber nicht festhalten darf, für welchen Wahlkreisvorschlag die erteilte Bescheinigung bestimmt ist.

§ 31 LWO
Inhalt und Form der Wahlkreisvorschläge
[…]
(3) Die nach Art. 27 Abs. 1 Nr. 4 Satz 2 LWG erforderlichen Unterstützungsunterschriften von Stimmberechtigten sind auf amtlichen Formblättern nach Anlage 5 unter Beachtung folgender Vorschriften zu erbringen:
[…]
3. [1]Für jeden Unterzeichner ist auf dem Formblatt oder gesondert eine Bescheinigung der Gemeinde, bei der er im Wählerverzeichnis einzutragen ist, beizufügen, dass er im betreffenden Wahlkreis stimmberechtigt ist. [2]Gesonderte Bescheinigungen des Stimmrechts sind vom Träger des Wahlkreisvorschlags bei der Einreichung des Wahlkreisvorschlags mit den Unterstützungsunterschriften zu verbinden. [3]Wer für einen anderen eine Bescheinigung des Stimmrechts beantragt, muss nachweisen, dass der Betreffende den Wahlkreisvorschlag unterstützt.
4. [1]Eine stimmberechtigte Person darf nur einen Wahlkreisvorschlag unterzeichnen. [2]Hat jemand mehrere Wahlkreisvorschläge unterzeichnet, so ist seine Unterschrift auf allen weiteren Wahlkreisvorschlägen ungültig.
[…]
(5) […] [2]Die Gemeinde darf für jede stimmberechtigte Person die Bescheinigung des Stimmrechts nur einmal zu einem Wahlkreisvorschlag erteilen; dabei darf sie nicht festhalten, für welchen Wahlkreisvorschlag die erteilte Bescheinigung bestimmt ist.

Der letztgenannte Hinweis wird, da von zentraler Bedeutung, nochmals im Formblatt gemäß Anlage 5 zu § 31 Abs. 3 LWO unter Fußnote 2 wiederholt. Als datenschutzkonforme Möglichkeit, dieser Pflicht nachzukommen, empfiehlt das Bayerische Staatsministerium des Inneren, für Sport und Integration den Gemeinden in seinem Merkblatt „Hinweise für Gemeinden zur Bescheinigung des Wahlrechts für Unterstützungsunterschriften und der Wählbarkeit von Bewerbern“ (im Internet abrufbar unter https://www.wahlen.bayern.de/vernichtung3) eine alphabetische Liste oder Datei, in welcher lediglich die Namen aller Wahlberechtigten festgehalten werden, für die eine Bescheinigung erteilt wurde. Zusätzlich darf lediglich vermerkt werden, für welche Wahl die Bescheinigung erteilt wurde. Unzulässig ist laut Hinweisen des Innenministeriums das Anfertigen von Kopien der Unterstützungsunterschriften, auch dann, wenn der Name des unterstützten Wahlvorschlags abgedeckt oder geschwärzt wird. In dem Merkblatt wird zusätzlich darauf hingewiesen, dass die Erteilung der Bescheinigung nicht im Wählerverzeichnis vermerkt werden darf.

In dem aufgrund der Eingabe von mir geprüften Fall hatte die öffentliche Stelle die Formblätter vollumfänglich eingescannt und hierbei auch festgehalten, welcher Wahlkreisvorschlag unterstützt wurde. Aufgrund meiner Hinweise hat die Kommune ihr Verfahren umgehend geändert und nur noch eine Excel-Liste geführt, welche lediglich die Namen der Unterstützer enthält. Die bereits eingescannten Unterschriftenlisten wurden unverzüglich, die Excel-Tabelle nach der Wahl vollständig gelöscht. Aufgrund der schnellen und effektiven Abhilfemaßnahmen konnte ich ausnahmsweise von einer Beanstandung absehen.

7.9 Flüchtlinge und Asylsuchende: Videoüberwachung einer Unterkunft für Asylbewerber

Im 27. Tätigkeitsbericht 2016 habe ich mich unter Nr. 7.2.1 allgemein zur Zulässigkeit der Videoüberwachung von Unterkünften für Asylsuchende geäußert. Aufgrund einer Eingabe bin ich nunmehr konkret mit der Videoüberwachung einer von einem Landratsamt betriebenen Gemeinschaftsunterkunft für Asylbewerber und Asylbewerberinnen befasst.

Der Außenbereich der Unterkunft wird annähernd flächendeckend, die Flure der vier Bauteile werden komplett erfasst. Dem Lageplan sind Anzahl und Standort der insgesamt 23 Kameras zu entnehmen, nicht aber die Überwachungsradien. Die Auflösung der Kameras erlaubt eine personenscharfe Darstellung, ein Zoomen ist aber nicht möglich. Durch Infrarottechnik kann auch nachts erkennbar aufgezeichnet werden.

Die laufend aufgezeichneten Daten werden innerhalb von 60 Stunden automatisch überschrieben. Die gesicherten Daten werden so lange aufbewahrt, bis der Zweck der Auswertung (Verfolgung von Ordnungswidrigkeiten oder von Straftaten oder Geltendmachung von Rechtsansprüchen) erreicht wurde oder hinfällig ist. Die Löschung der gesicherten Daten erfolgt durch die zugriffsberechtigten Beschäftigten des Landratsamts. Die Zugriffe auf die aufgezeichneten Daten der Vergangenheit (nicht die Live-Ansicht) werden automatisch protokolliert. Die Auswertungskriterien werden in der Verfahrensbeschreibung wie folgt festgelegt:

„Eine Auswertung erfolgt nur, wenn sie zum Schutz der Rechtsgüter Leben, Gesundheit und Eigentum bzw. zur Durchsetzung von Schadensersatzforderungen

dienlich ist. Dies kann vor Eintritt eines Gefahrenfalls (z. B. Aufklärung von Manipulationen an der Brandmeldeanlage oder aber auch nach Eintritt eines Schadensfalls (z. B. zur Verfolgung von Straftaten) erforderlich sein. Die Auswertung wird nur durch die beiden zugriffsberechtigten Mitarbeiter des Landratsamts bzw. durch berechtigte Dritte (z. B. Polizei, Strafverfolgungsbehörde) getätigt."

Anzahl und Intensität der im Vorfeld der Maßnahme erfassten Vorfälle rechtfertigen grundsätzlich die Errichtung und den Betrieb einer Videoüberwachungsanlage.

Allerdings ergibt sich weder aus der Einschätzung der Polizei noch aus der fortgeführten Vorfallsdokumentation, dass Anzahl und Intensität der Vorfälle mit Installation und Inbetriebnahme der Anlage abgenommen hätten. Erfolg und Wirkung der Videoüberwachung sind nicht ausreichend dokumentiert. Dies gilt insbesondere für die Aussage, erst durch die Videoüberwachung sei es möglich, den Schadensverursacher zu identifizieren, sein Fehlverhalten strafrechtlich verfolgen zu lassen und den Schaden auf ihn umzulegen.

Da die Ermöglichung einer repressiven Strafverfolgung – beispielsweise hinsichtlich Vandalismus – nicht Aufgabe des Landratsamts, sondern Aufgabe von Polizei und Staatsanwaltschaft ist, kann dies allenfalls Nebenzweck einer der Gefahrenabwehr dienenden Videoüberwachung sein. Das Landratsamt kann aber auch nicht ausreichend plausibel belegen, dass die Videoüberwachung im Sinne einer Verhaltenssteuerung zur präventiven Abschreckung und somit zur Gefahrenabwehr geeignet und erforderlich ist und andere weniger eingreifende Maßnahmen nicht in Betracht kommen.

Angesichts der hohen Eingriffsintensität (Aufzeichnung rund um die Uhr, Flure komplett, Außenbereich annähernd komplett) gegenüber Bewohnern und Bewohnerinnen, Beschäftigten, Ehrenamtlichen sowie Besuchern und Besucherinnen erscheint der Weiterbetrieb der Anlage in der derzeitigen Form nicht möglich. Ich habe das Landratsamt deshalb aufgefordert, zumindest eine Reduzierung des Umfangs der Videoüberwachung zu prüfen. Eine zahlenmäßige, zeitliche und/oder räumliche Einschränkung der Maßnahme kann sich etwa aus folgenden Überlegungen ergeben:

— Festlegung besonders gefährdeter Bereiche (etwa Zugang zur Brandmeldeanlage, Eingangsbereiche, „tote Winkel"),

— Prüfung des Standorts jeder einzelnen Kamera sowie deren Erfassungswinkel,

— Beschränkung in zeitlicher Hinsicht auf das erforderliche Maß (etwa außerhalb der Bürozeiten oder zu Zeiten, in denen kein Sicherheitsdienst vor Ort ist) und

— Überarbeitung des gesamten Sicherheitskonzepts (insbesondere Reduzierung der Belegung, Veränderung der Bewohnerstruktur, Ausbau der Sozialbetreuung, Erweiterung des Sicherheitsdienstes).

Zudem habe ich das Landratsamt um konkrete Darlegung der Fälle gebeten, in denen mit Hilfe der Videoüberwachung Vorfälle aufgeklärt und Ansprüche gegen die Verursacher geltend gemacht werden konnten.

Das Landratsamt hat sich zuletzt bereit erklärt, auf neun von 23 Kameras zu verzichten und die Videoüberwachung der Zugänge zu den Waschräumen zu schwärzen.

Eine abschließende Bewertung der Sach- und Rechtslage wird erst nach Fertigstellung dieses Berichts möglich sein.

8 Gesundheitswesen

8.1 Themen von länderübergreifender Bedeutung

8.1.1 Medizininformatik-Initiative der Bundesregierung

Die Arbeitskreise Gesundheit und Soziales sowie Wissenschaft und Forschung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder wurden vom Nationalen Steuerungsgremium der Medizininformatik-Initiative des Bundesministeriums für Bildung und Forschung eingeladen, am Dialogforum der Medizininformatik-Initiative, einem externen Beratergremium, mitzuwirken. Ich habe für den Arbeitskreis Gesundheit und Soziales am Dialogforum teilgenommen. Der Arbeitskreis Wissenschaft wurde von meinem hessischen Kollegen vertreten.

Die Projektstruktur der Initiative besteht aus dem Nationalen Steuerungsgremium, das Arbeitsgruppen einsetzt und die konsortienübergreifende Koordination übernimmt. Der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. (TMF), der Medizinische Fakultätentag (MFT) und der Verband der Universitätsklinika Deutschlands (VUD) nehmen Geschäftsstellenfunktionen wahr. Das Dialogforum ist ein begleitendes Diskussionsforum.

Aus der Pressemitteilung des Bundesforschungsministeriums vom 16. November 2015 lässt sich ein Eindruck von der Dimension der geförderten Initiative der Bundesregierung gewinnen.

„16. November 2015 Pressemitteilung: 158/2015
Datenschätze heben, Patientenversorgung verbessern

Bundesforschungsministerium stärkt Medizininformatik/Wanka: „Mit Hilfe von Daten bessere Diagnosen und Therapien entwickeln“

Das Bundesministerium für Bildung und Forschung (BMBF) stärkt die Medizininformatik in Deutschland. Mit einem neuen Förderkonzept will das BMBF die technischen und strukturellen Voraussetzungen schaffen, damit Wissen aus der Krankenversorgung und der medizinischen Forschung besser zusammengeführt werden kann.

Der bereits jetzt riesige Datenschatz in Medizin und Forschung wächst kontinuierlich weiter, wird aber noch unzureichend genutzt. „Täglich werden unzählige gesundheitsrelevante Daten in Kliniken, Arztpraxen und auch in der biomedizinischen Forschung erhoben. Die neue Strategie zur Medizininformatik wird dazu beitragen, dass mit Hilfe dieser Informationen genauere Diagnosen und bessere Therapien erfolgen können“, sagte Bundesforschungsministerin Johanna Wanka bei der heutigen Vorstellung der Strategie auf der MEDICA in Düsseldorf. Zur Förderung der Medizininformatik stellt das BMBF in den kommenden fünf Jahren 100 Millionen Euro bereit.

Die Strategie ist langfristig und in zeitlich gestuften Modulen angelegt: In einem ersten Schritt sollen an Universitätskliniken Datenintegrationszentren aufgebaut und vernetzt werden. In den Zentren sollen die Voraussetzungen geschaffen werden, um Forschungs- und Versorgungsdaten standortübergreifend zu verknüpfen. Gleichzeitig werden innovative IT-Lösungen für konkrete Anwendungen entwickelt. Dabei ist es eine unabdingbare Voraussetzung, dass die in Deutschland sehr strengen datenschutzrechtlichen Standards und Rahmenbedingungen eingehalten werden, zum Beispiel hinsichtlich des Erfordernisses einer Einwilligung der Patientinnen und Patienten.

Anwendungen könnten zum Beispiel die Entwicklung einer individualisierten Krebstherapie oder die IT-basierte Unterstützung von Diagnose und Therapiewahl bei seltenen Erkrankungen sein. So dauert es bei Patienten, die an einer seltenen Erkrankung leiden, häufig sehr lange, bis eine korrekte Diagnose und optimale Therapie gefunden sind. Ein computergestütztes Informationssystem, das über Befunde und Therapieerfolge bei Patienten mit ähnlichen Symptomen informiert und Mediziner so bei ihrer Diagnose unterstützt, könnte gerade bei seltenen Erkrankungen die Patientenversorgung beschleunigen und verbessern. Solche Experten-Systeme können heute mit Hilfe von modernen Informationstechnologien und medizinischen Datensammlungen entwickelt werden.

Langfristiges Ziel der neuen Strategie ist ein leistungsfähigeres, digital vernetztes Gesundheitssystem. Die Medizininformatik in Deutschland zu stärken, ist Teil der Digitalen Agenda der Bundesregierung. Diese ressortübergreifende Strategie will die Innovationspotentiale der Digitalisierung nutzen und widmet sich vielfältigen Aspekten – vom Breitbandausbau über die Digitalisierung in Gesellschaft, Wirtschaft und Wissenschaft bis hin zum Thema IT-Sicherheit.

Weitere Informationen unter:
http://www.gesundheitsforschung-bmbf.de/de/medizininformatik.php“

Am 30. August 2016 hat in München das Kick-Off-Meeting stattgefunden.

Das Bundesforschungsministerium fördert die Initiative mittlerweile mit einem Betrag von 150 Mio. Euro. Derzeit werden vier von ursprünglich sieben Konsortien unterstützt, die jeweils mindestens zwei Universitätsklinika sowie weitere Partner, insbesondere aus den Bereichen Hochschulen, private Kliniken und Industrieunternehmen umfassen. In den Universitätsklinika sollen Datenintegrationszentren eingerichtet werden, die einen umfassenden Datenaustausch gewährleisten sollen. Nach dreieinhalb Jahren soll ein Audit durch das Bundesforschungsministerium stattfinden.

Es sind Universitätsklinika aus dem gesamten Bundesgebiet an den ursprünglich sieben Konsortien beteiligt. Die sieben Konsortien bezeichnen sich wie folgt:

1. ADMIRE (Münster, Köln, Bonn, Essen, Düsseldorf);
2. DIFUTURE (LMU München, TU München, Augsburg, Tübingen);
3. HD4CR (Charité Berlin, Ulm, Würzburg);
4. HIGHmed (Hannover, Göttingen, Heidelberg, Deutsches Krebsforschungszentrum);
5. MIRACUM (Erlangen-Nürnberg, Gießen, Mainz, Freiburg, Marburg, Mannheim, Heidelberg, Frankfurt a. M.);
6. Share-it (Kiel, Rostock, Lübeck, Hamburg, Greifswald, Dresden);
7. SMITH (Leipzig, Jena, Aachen).

Alle Konsortien haben das Ziel einer vernetzten Kommunikation zwischen allen Beteiligten auf einer sicheren IT-Basis.

Ich habe im Dialogforum darauf hingewiesen, dass zunächst die Benennung verantwortlicher Stellen im Sinne des Datenschutzrechts erfolgen solle, um eine Beteiligung der jeweils zuständigen Aufsichtsbehörden sicherzustellen. Ferner solle die Förderung durch das Bundesforschungsministerium an die Erstellung eines allgemeinen und sich weiter entwickelnden spezifischen Datenschutzkonzepts gebunden werden. Darüber hinaus sollen die Datenschutzbeauftragten der in den Konsortien beteiligten Stellen frühzeitig eingebunden werden. Es seien die rechtlichen Rahmenbedingungen insbesondere die Datenschutz-Grundverordnung mit ihren Anpassungsregelungen, die Landeskrankenhausgesetze, die Gesundheitsgesetze und die Sozialgesetzbücher zu beachten.

Maßgebliche Rechtsgrundlagen für die entsprechenden Verarbeitungen von Gesundheitsdaten werden Einwilligungserklärungen von Patientinnen und Patienten sein. Dazu wurde den Arbeitskreisen ein Mustertext einer Einwilligungserklärung vorgelegt, der nach eingehender Diskussion mit der Maßgabe angenommen wurde, dass die von den Datenschutz-Aufsichtsbehörden gemachten Vorgaben und Anmerkungen, insbesondere zur sogenannten „breiten Einwilligung“ (broad consent) berücksichtigt werden. Im Vordergrund steht insoweit eine umfassende Aufklärung der Patientinnen und Patienten über die grundsätzlichen Zwecke der Verarbeitung von Daten, um selbstbestimmt über die Teilnahme an einer entsprechenden Forschungsstudie entscheiden zu können. Dies erschien den Arbeitskreisen mit den Mustertexten einer Patienteninformation und der Patienteneinwilligung als im Ergebnis sichergestellt.

Soweit ich mit einem Konsortium unter Führung einer bayerischen Universitätsklinik unmittelbar befasst war, haben meine Hinweise zu einer Überarbeitung des Datenschutzkonzepts dieses Konsortiums geführt, insbesondere im Hinblick auf die Darstellung der Verfahrensweisen und die Frage der standortübergreifenden Zusammenführung von personenbezogenen Patientendaten in sogenannten Datenintegrationszentren. Diesbezüglich wurde im Datenschutzkonzept ausdrücklich klargestellt, dass in der ersten Projektphase keine personenbezogenen Daten zwischen den einzelnen Standorten der im Konsortium zusammenarbeitenden Stellen ausgetauscht werden sollen. Die Datenhaltung blieb zunächst auf den jeweiligen Standort beschränkt, Auswertungen wurden nur intern vorgenommen. Externe Forscher erhielten keine personenbezogenen Patientendaten, sondern nur aggregierte Statistiken. Das Landesrecht bot dazu in Art. 27 Abs. 4 Satz 1 Bayerisches Krankenhausgesetz eine ausreichende Rechtsgrundlage; demnach dürfen Krankenhausärzte Patientendaten nutzen, soweit dies zu Forschungszwecken im Krankenhaus oder im Forschungsinteresse des Krankenhauses erforderlich ist. Einer Einwilligung der betroffenen Patienten und Patientinnen bedurfte es hierfür nicht.

Allerdings erhob das Datenschutzkonzept ausdrücklich nicht den Anspruch, auch alle weiteren Projektphasen abzubilden. Insoweit habe ich darauf gedrängt, das Konzept anzupassen und zu ergänzen, sobald die geplanten Ausbaustufen eingerichtet und umgesetzt werden sollen.

Das Gesamtprojekt der Medizininformatik-Initiative begleite ich auch weiterhin intensiv.

8.1.2 Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO durch Krankenhäuser

Am Beispiel der Krankenhäuser lässt sich gut veranschaulichen, wie die Datenschutz-Grundverordnung bereits weit im Vorfeld des Anwendungszeitraums schwierige Rechts-und Umsetzungsfragen aufgeworfen hat. Die Deutsche Krankenhausgesellschaft, der Bundesverband Gesundheits-IT und der Arbeitskreis „Datenschutz und IT-Sicherheit im Gesundheitswesen" der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie haben gemeinsam den Versuch unternommen, insbesondere Krankenhäusern Hilfestellungen zur Anwendung der Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO zu geben. Dazu haben sie mir in meiner Funktion als Vorsitzender des Arbeitskreises Gesundheit und Soziales der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder umfangreiche Papiere mit der Bitte um Bewertung vorgelegt.

Da das Thema Datenschutz-Folgenabschätzung im Grunde für nahezu alle Sach- und Rechtsbereiche relevant ist, habe ich in Abstimmung mit den Mitgliedern des insoweit federführenden Arbeitskreises Gesundheit und Soziales weitere Gremien der Datenschutz-Aufsichtsbehörden, insbesondere den Arbeitskreis Technik, den Arbeitskreis Grundsatzfragen und die eigens begründete Unterarbeitsgruppe Datenschutz-Folgenabschätzung eingebunden. Es wurden zahlreiche Anmerkungen zu den vorgelegten Unterlagen abgegeben. Dabei wurde darauf hingewiesen, dass die Papiere zwar einen guten Überblick über die Rechtslage enthalten, aber nur an einzelnen Stellen konkret anwendbare Hinweise. Zum Beispiel fehlten detaillierte Angaben zu Gefährdungen und Angriffsszenarien speziell für IT-Systeme im Krankenhaus sowie detaillierte Vorgaben zur Durchführung einer Risikoanalyse. Auch fehlten Angaben zur Methodik der Risikobewertung.

Leider ist es nicht gelungen, schon vor Geltungsbeginn der Datenschutz-Grundverordnung ein speziell für Krankenhäuser konzipiertes Papier mit abgestimmten detaillierten Hinweisen für die Umsetzung der Datenschutz-Folgenabschätzung zu entwickeln. Letztendlich hat dieser Umstand aufgezeigt, dass die Verantwortlichen sich mit den neuen Instrumenten der Datenschutz-Grundverordnung noch besser vertraut machen müssen. Zwischenzeitlich liegen von Seiten der Datenschutz-Aufsichtsbehörden Orientierungshilfen und Empfehlungen vor, die es den Verantwortlichen ermöglichen sollten, die Anforderungen zu erfüllen. Eine dazu von mir entwickelte Orientierungshilfe kann auf meiner Homepage https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Datenschutz-Folgenabschätzung" abgerufen werden.

8.1.3 Konstituierung der Unterarbeitsgruppe „Digitalisierung im Gesundheitswesen"

Die Weiterentwicklung der Digitalisierung im Gesundheitswesen war und ist eines der erklärten politischen Ziele der Bundesregierung. Die Datenschutz-Aufsichtsbehörden waren im Berichtszeitraum deshalb noch mehr als bisher gefordert, sich mit datenschutzrechtlichen Themen der Digitalisierung im Gesundheitswesen zu befassen. Um dafür entsprechend vorbereitet zu sein, hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder auf Vorschlag des von mir geleiteten Arbeitskreises Gesundheit und Soziales sowie des Arbeitskreises Technik einstimmig beschlossen, eine Unterarbeitsgruppe einzurichten, die

sich ausschließlich mit dieser komplexen Materie beschäftigen soll. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat aufgrund der bundesweiten Bedeutung den Vorsitz der Unterarbeitsgruppe übernommen.

Bislang sind insbesondere folgende Themen als wesentlich erkannt und beraten worden:

- Big Data im Gesundheitswesen;
- Medizininformatik-Initiative der Bundesregierung (siehe dazu oben unter Nr. 8.1.1);
- Elektronische Patientenakte/elektronische Gesundheitsakte;
- Gesundheits-Apps;
- Datenverarbeitung im Auftrag im Gesundheitswesen/Nutzung von Cloud-Diensten;
- Infrastruktur zur mobilen Kommunikation, insbesondere Messengerdienste;
- Interoperabilität/Standards;
- Videosprechstunde;
- Wartung von medizinischen Geräten;
- Bildung/Sensibilisierung der Beteiligten;
- Ambient Assisted Living (AAL).

Die Unterarbeitsgruppe beabsichtigt, Orientierungshilfen, Entschließungen, Empfehlungen und Leitlinien zu entwickeln. Die darin enthaltenen Hinweise zur datenschutzkonformen Umsetzung der Digitalisierung im Gesundheitswesen sollen der Politik, der Verwaltung sowie den Bürgerinnen und Bürgern nutzbar gemacht werden.

8.2 Krebsregister

Das Bayerische Krebsregistergesetz ist am 1. April 2017 in Kraft getreten. Zum Gesetzentwurf habe ich mich bereits in meinem 27. Tätigkeitsbericht 2016 unter Nr. 7.3 ausführlich geäußert.

Ein Hauptpunkt der parlamentarischen Diskussion war bei diesem Gesetz bis zuletzt der Datenschutz. Im Kern ging es darum, ob das Krebsregistergesetz aus sich heraus für die betroffenen Patienten und Patientinnen verständlich ist und gesetzliche Grundlage für die Einschränkung des Grundrechts auf informationelle Selbstbestimmung sein kann, weil sich bereits aus dem Gesetz deren Voraussetzungen und Umfang klar ergeben und seine Regelungen damit dem rechtsstaatlichen Gebot der Normenklarheit entsprechen (zu diesem siehe Beschluss des Bundesverfassungsgerichts vom 23. Februar 2007, Az.: 1 BvR 2368/06).

Für mich war unabdingbar, dass zumindest in der Zusammenschau aus dem Gesetz und der dazu erlassenen Ausführungsverordnung (Verordnung über die Durchführung des Bayerischen Krebsregistergesetzes – Krebsregisterverordnung) klar erkennbar sein muss, wie das Bayerische Krebsregister organisiert ist und welche Stellen welche Aufgaben und – insbesondere datenschutzrechtlichen – Befugnisse haben sollen. Ich habe mich deshalb von Beginn an und wiederholt in das Verfahren zum Erlass der Krebsregisterverordnung eingebracht. Die Verordnung ist am 1. Mai 2018 in Kraft getreten und enthält unter anderem

Regelungen zu Struktur und Organisation des Bayerischen Krebsregisters, insbesondere die Unterteilung in Vertrauensstelle, Regionalzentren und Zentralstelle für Krebsfrüherkennung und Krebsregistrierung (ZKFR).

Auch den derzeit laufenden Aufbau des Bayerischen Krebsregisters werde ich weiter begleiten.

Zu den technischen Anforderungen an das Bayerische Krebsregister siehe den Beitrag Nr. 3.2.3.

8.3 Veterinär- und Lebensmittelüberwachung: TIZIAN

Das Verfahren TIZIAN war wiederholt Gegenstand meiner Tätigkeitsberichte. Auch im Berichtszeitraum habe ich mich mit TIZIAN beschäftigt. TIZIAN ist die Bezeichnung einer behördenübergreifend eingesetzten Software für die Veterinär-, Lebensmittel- und Futtermittelüberwachung, die vom Bayerischen Landesamt für Gesundheit und Lebensmittelsicherheit betrieben wird. Sie soll den über 100 Verbraucherschutz-, Lebensmittel- und Veterinärbehörden, die die Verbunddatei derzeit nutzen, eine effiziente und qualitätsgesicherte Erfüllung ihrer Aufgaben im Rahmen der Lebensmittel-, Veterinär- und Futtermittelkontrolle ermöglichen.

Angesichts der Vielzahl der verarbeiteten Daten, der oft umfangreichen Zugriffsmöglichkeiten und der damit verbundenen Gefahr einer missbräuchlichen Datenverarbeitung habe ich unter Hinweis auf die Eingriffe in das Grundrecht auf informationelle Selbstbestimmung seit den Planungen zur Einführung der Datenbank eine hinreichend klare und bestimmte gesetzliche Grundlage gefordert (siehe zuletzt meine Ausführungen im 25. Tätigkeitsbericht 2012 unter Nr. 8.5).

Es ist vor diesem Hintergrund zu begrüßen, dass der bayerische Gesetzgeber mit Art. 30a Gesetz über den öffentlichen Gesundheits- und Veterinärdienst, die Ernährung und den Verbraucherschutz sowie die Lebensmittelüberwachung (Gesundheitsdienst- und Verbraucherschutzgesetz – GDVG) mein langjähriges Postulat nun im Interesse der Rechtssicherheit umgesetzt und eine spezialgesetzliche Rechtsvorschrift für das Verfahren TIZIAN erlassen hat.

Art. 30a GDVG
Gemeinsames Verfahren
(1) Das Landesamt betreibt für die in Abs. 3 genannten Zwecke ein automatisiertes gemeinsames Verfahren.
(2) [1]Das Landesamt und die mit dem Vollzug der in Abs. 3 genannten Zwecke betrauten oder beliehenen Stellen können die hierfür erforderlichen Daten verarbeiten. [2]Das Staatsministerium für Umwelt und Verbraucherschutz kann die in Satz 1 genannten Daten zu den in Abs. 3 Nr. 5 genannten Zwecken auslesen und verwenden.
(3) Die Verarbeitung der Daten nach Abs. 2 Satz 1 erfolgt zu folgenden Zwecken:
1. Vollzug der Art. 19 bis 21,
2. Aufsicht durch die in Art. 3 Abs. 1 Nr. 2 und Art. 5 genannten öffentlichen Stellen,
3. Steuerung der in Art. 3 Abs. 1 Nr. 2 und 3, Art. 4, 5 und 5a genannten sowie gemäß Art. 7 beliehenen öffentlichen Stellen,
4. Personalbewirtschaftung, aber ohne Personenbezug der Betriebs- und Kontrolldaten,

5. Planung, Steuerung und Aufsicht durch das Staatsministerium für Umwelt und Verbraucherschutz, aber ohne Personenbezug der Betriebs- und Kontrolldaten.

(4) Der Verantwortliche hat personenbezogene Daten, die zur Erfüllung der Aufgaben nach Abs. 3 nicht mehr erforderlich sind, zu löschen.

8.4 Krankenhaus

8.4.1 Rechtsgrundlagen für Krankenhäuser nach neuem Datenschutzrecht

Die Öffnungsklauseln der Datenschutz-Grundverordnung und die Befugnis zur Konkretisierung ihrer allgemeinen Vorschriften ermöglichen die weitgehende Beibehaltung der bisherigen, gegenüber dem Bayerischen Datenschutzgesetz vorrangigen datenschutzrechtlichen Spezialvorschriften. Dies gilt auch im Krankenhausbereich:

Als besondere Rechtsvorschrift im Sinne des Art. 1 Abs. 5 BayDSG ist Art. 27 Bayerisches Krankenhausgesetz (BayKrG) auch weiterhin auf alle Krankenhäuser anwendbar, die gemäß Art. 2 BayKrG dem Geltungsbereich des Bayerischen Krankenhausgesetzes unterliegen.

Soweit Art. 27 BayKrG nichts anderes bestimmt, gelten für Patientendaten wegen Art. 1 Abs. 3 BayDSG die Vorschriften für nicht öffentliche Stellen. Denn regelmäßig nehmen öffentliche Krankenhäuser als Unternehmen am Wettbewerb teil.

Art. 27 BayKrG gilt grundsätzlich auch für **Bezirkskliniken**. Eine Ausnahme bildet hier nur der Bereich des Straf- und Maßregelvollzugs, einschließlich der Unterbringung nach dem Therapieunterbringungsgesetz (vgl. Art. 2 BayKrG, § 3 Satz 1 Nr. 2 Gesetz zur wirtschaftlichen Sicherung der Krankenhäuser und zur Regelung der Krankenhauspflegesätze).

Der **Wettbewerbscharakter von Bezirkskrankenhäusern** ist lediglich bei der Unterbringung nach dem Bayerischen Psychisch-Kranken-Hilfe-Gesetz, der Unterbringung im Straf- und Maßregelvollzug und der Unterbringung nach dem Therapieunterbringungsgesetz zu verneinen.

Universitätskliniken sind rechtsfähige Anstalten des öffentlichen Rechts (Art. 1 Abs. 1 Gesetz über die Universitätsklinika des Freistaates Bayern – Bayerisches Universitätsklinikagesetzes – BayUniKlinG) und damit sonstige öffentliche Stellen im Sinne von Art. 1 Abs. 1 Satz 1 BayDSG. Gemäß Art. 15 Abs. 2 BayUniKlinG gilt Art. 27 BayKrG für Universitätskliniken entsprechend.

Da Universitätskliniken Aufgaben der Krankenversorgung wahrzunehmen haben, die auch von privaten oder gemeinnützigen Krankenhäusern erbracht werden können, nehmen sie insoweit am **Wettbewerb** teil, auch wenn die Unikliniken die Krankenversorgung an den Aufgaben ihrer Universität in Forschung und Lehre auszurichten haben und diese hierdurch eine spezielle Prägung erfahren (siehe Art. 2 Abs. 1 Satz 1 BayUniKlinG).

8.4.2 Informationsaustausch zwischen Krankenhaus und Ermittlungsbehörden

Beim regelmäßigen Austausch mit Krankenhäusern werfen diese immer wieder die Frage auf, ob und inwieweit personenbezogene Daten von Beschäftigten oder von Patienten und Patientinnen an die Polizei übermittelt werden dürfen. Hier die häufigsten Fallgestaltungen:

— 1. Fall: Ein Mitarbeiter wird von einem Patienten angegriffen. Die Klinik stellt Strafanzeige. Die Polizei befragt den Bediensteten vor Ort zu seinen persönlichen Daten und zum Hergang des Vorfalls.

  Der Bedienstete ist nach Maßgabe von § 163 Abs. 3 Strafprozessordnung (StPO) als Zeuge zur Aussage verpflichtet. Über § 53a StPO gilt aber das Zeugnisverweigerungsrecht nach § 53 Abs. 1 Satz 1 Nr. 3 StPO.

  Die Weitergabe von Patientendaten ist nach Maßgabe von § 32 Abs. 2 Bundesmeldegesetz (BMG) zulässig:

  § 32 BMG
  Besondere Meldepflicht in Krankenhäusern, Heimen und ähnlichen Einrichtungen
  (2) [1]Der zuständigen Behörde ist Auskunft aus den Unterlagen der genannten Einrichtungen zu erteilen, wenn dies nach Feststellung der Behörde zur Abwehr einer erheblichen und gegenwärtigen Gefahr, zur Verfolgung von Straftaten oder zur Aufklärung des Schicksals von Vermissten und Unfallopfern im Einzelfall erforderlich ist. [2]Die Auskunft umfasst folgende Daten:
  1. Familienname,
  2. Vornamen,
  3. Geburtsdatum und Geburtsort sowie bei Geburt im Ausland auch den Staat,
  4. Staatsangehörigkeiten,
  5. Anschriften,
  6. Datum der Aufnahme und Datum der Entlassung.

— 2. Fall: Ein Patient zeigt einen Mitarbeiter an. Die Polizei befragt den Bediensteten vor Ort. Wie hat sich der Bedienstete zu verhalten?

  Als Beschuldigter ist der Mitarbeiter nicht zur Aussage verpflichtet (§ 136 Abs. 1 StPO). Zeugen steht das Auskunftsverweigerungsrecht nach § 55 StPO zu. Eine Weitergabe von Daten, die der Schweigepflicht unterliegen, ist nur in den engen Grenzen des § 34 Strafgesetzbuch (StGB) gerechtfertigt, zum Beispiel zur Abwehr der Gefahr einer unbegründeten strafrechtlichen Verfolgung oder einer unberechtigten Zivilklage (vgl. Eisele, in: Schönke/ Schröder, Strafgesetzbuch, 30. Aufl. 2019, § 203 Rn. 60).

— 3. Fall: Ein Patient zeigt einen anderen Patienten an. Mitarbeiter werden als Zeugen von der Polizei angesprochen.

  Die Weitergabe von Patientendaten ist nach Maßgabe von § 32 Abs. 2 BMG zulässig, etwa zur Abwehr einer erheblichen und gegenwärtigen Gefahr oder zur Verfolgung von Straftaten (siehe 1. Fall). Die Beschäftigten sind nach Maßgabe von § 163 Abs. 3 StPO als Zeugen zur Aussage verpflichtet. Über § 53a StPO gilt aber das Zeugnisverweigerungsrecht nach § 53 Abs. 1 Satz 1 Nr. 3 StPO.

— 4. Fall: Patienten zeigen einen Diebstahl im Krankenhaus an. Die Polizei ermittelt vor Ort.

  Die Mitarbeiter sind nach Maßgabe von § 163 Abs. 3 StPO als Zeugen zur Aussage verpflichtet. Über § 53a StPO gilt aber das Zeugnisverweigerungsrecht nach § 53 Abs. 1 Satz 1 Nr. 3 StPO. In einem ersten Schritt könnten die Mitarbeiter ihre Beobachtungen auch ohne Personenbezug mitteilen. Die Weitergabe von Patientendaten ist nach Maßgabe von § 32 Abs. 2 BMG zulässig (siehe 1. Fall).

— 5. Fall: Die Polizei hat im Rahmen von Ermittlungsverfahren Fragen zu Patienten.

  Im Hinblick auf die Sensibilität und besondere Schutzwürdigkeit von Patientendaten (vgl. § 97 StPO) empfehle ich in solchen Fällen, regelmäßig auf einem schriftlichen Herausgabeverlangen der Staatsanwaltschaft als Herrin des Verfahrens zu bestehen, aus dem hervorgeht, dass andernfalls Zwangsmaßnahmen wie etwa eine Beschlagnahme drohen.

— 6. Fall: Die Staatsanwaltschaft bittet das Krankenhaus darum, Straftaten zwischen zwei Patienten (meist körperliche Gewalt oder Diebstahl von Patienteneigentum) grundsätzlich zur Anzeige zu bringen.

  Eine Anzeige**pflicht** für geplante Straftaten ergibt sich aus § 138 StGB, für Ärzte und deren berufsmäßigen Gehilfen gilt § 139 Abs. 3 StGB.

  Eine Offenbarung kann nach § 34 StGB gerechtfertigt sein (rechtfertigender Notstand). Eine Verletzung der Schweigepflicht wird regelmäßig aber nur gerechtfertigt sein, wenn es um die Abwehr erheblicher Gefahren für die Rechtsgüter Leben und Gesundheit geht. Auch darf nur das offenbart werden, was zur Erreichung des Zwecks unbedingt erforderlich ist.

  Ist der Antragsberechtigte geschäftsunfähig oder beschränkt geschäftsfähig, so können der gesetzliche Vertreter in den persönlichen Angelegenheiten und derjenige, dem die Sorge für die Person des Antragsberechtigten zusteht, Strafanzeige stellen (§ 77 Abs. 3 StGB).

8.4.3 Übermittlung von Patientendaten an externe Verrechnungsstellen

Ein Universitätsklinikum übermittelte zur Abrechnung ärztlicher Leistungen innerhalb weniger Jahre wiederholt personenbezogene Daten ein und desselben Patienten ohne dessen Einverständnis an externe Abrechnungsfirmen. Da das Liquidationsrecht hinsichtlich der privatärztlichen Behandlungen in zwei Fällen beim Klinikum selbst lag, waren die Datenschutzverstöße dem Klinikum auch zuzurechnen. Ein dritter Verstoß zu Lasten des Patienten bezog sich auf die Abrechnung von ärztlichen Leistungen, für die das Liquidationsrecht nicht beim Klinikum, sondern beim Chefarzt selbst lag.

Gemäß § 17 Abs. 3 Satz 6 Gesetz über die Entgelte für voll- und teilstationäre Krankenhausleistungen dürfen bei der Abrechnung wahlärztlicher Leistungen personenbezogene Daten an eine beauftragte Abrechnungsstelle außerhalb des

Krankenhauses nur mit Einwilligung des Betroffenen übermittelt werden. In beiden dem Klinikum zuzurechnenden Fällen hatte der Patient eine entsprechende Einwilligung nicht erteilt.

Von einer förmlichen Beanstandung hatte ich nach dem ersten Verstoß noch abgesehen. So sei die Weitergabe der Daten nach Bekunden des Klinikums nur versehentlich erfolgt. Auch seien dem Wunsch des Patienten entsprechend sämtliche Klinikdirektoren darauf hingewiesen worden, dass eine externe Abrechnung seinerseits nicht gewünscht sei, so dass vergleichbare Datenschutzverstöße zu seinen Lasten künftig nicht mehr zu erwarten sein sollten.

Rund drei Jahre später kam es erneut zu einer unzulässigen Übermittlung von Patientendaten an eine externe Abrechnungsstelle. Die nach dem ersten Verstoß ergriffenen Maßnahmen waren offensichtlich nicht geeignet, den Mangel zu beheben und sicherzustellen, dass entsprechende Datenübermittlungen nur bei vorhandener Einwilligung erfolgen. Der wiederholte Datenschutzverstoß zu Lasten desselben Patienten ließ auf einen systematischen Fehler schließen und führte zu einer förmlichen Beanstandung.

Ob die nunmehr vom Klinikum angekündigten technisch-organisatorischen Maßnahmen Wirkung zeigen, werde ich zu gegebener Zeit im Rahmen einer Vor-Ort-Prüfung kontrollieren.

8.4.4 Weitergabe eines genetischen Befundes an Jugendamt

Folgender Fall führte zu einer förmlichen Beanstandung: Ein Universitätsklinikum informierte das örtliche Jugendamt über den genetischen Befund eines Patienten. Zudem gab der behandelnde Arzt die ermittelten genetischen Daten an neun weitere Therapiekollegen innerhalb des Klinikums weiter. Beides erfolgte ohne Befugnis und damit datenschutzwidrig.

Der minderjährige Patient befand sich in stationärer Behandlung. Im Rahmen der Behandlung willigte die Mutter des Patienten zwar in die genetische Untersuchung ihres Sohnes ein. Folgende Frage auf dem Formblatt „Einwilligung zur Genetischen Beratung/Untersuchung“ beantwortete sie durch Ankreuzen allerdings mit „Nein“:

„Ich bin damit einverstanden, dass mein Humangenetisches Gutachten/meine Befunde an folgende mitbehandelnde Ärzte geschickt werden: Frau/Herrn Dr.:“

In einem Schreiben an das örtliche Jugendamt (Gefährdungsmeldung nach § 8a Achtes Buch Sozialgesetzbuch – Kinder und Jugendhilfe –), das vom behandelnden Arzt und neun weiteren Therapiekollegen unterschrieben wurde, führte das Klinikum unter anderem aus:

„Während des stationären Aufenthaltes ergab sich kein Hinweis für eine neurometabolische, neuroimmunologische oder neuroendokrinologische bzw. neuroinfektiologische Störung. Es liegt somit kein somatischer Befund vor, der die Symptome von […] erklären könnte. Der einzige fassbare somatische Befund ist ein Mosaik 45 X0: Bei diesem Mosaik können Verhaltensauffälligkeiten bei Kindern auftreten, aber nicht die berichtete neurologische Symptomatik von […].“

Bei „Mosaik 45 X0“ handelt es sich um ein genetisches Datum. In seiner Stellungnahme räumte das Klinikum Zweifel an der Erforderlichkeit einer derart detaillierten Benennung des Befundes an das Jugendamt ein. Künftig sollten nur solche Daten Bestandteil von Gefährdungsmeldungen sein, deren Nennung zweckgebunden und erforderlich sei.

Die Mitteilung des genetischen Befundes an neun Therapiekollegen innerhalb der Klinik war aus Sicht des Klinikums erforderlich: Es habe sich hierbei um Ärzte gehandelt, die das Kind behandelt, damit zum Behandlungsteam gehört und daher auch ein entsprechendes Behandlungsmandat gehabt hätten.

§ 4 Gesetz zur Kooperation und Information im Kinderschutz (KKG) regelt die Befugnis von Geheimnisträgern wie Ärzten, beim Verdacht von Kindeswohlgefährdungen das Jugendamt zu informieren. Zu diesem Zweck dürfen dem Jugendamt die erforderlichen Daten mitgeteilt werden (§ 4 Abs. 3 Satz 2 KKG).

Die Mitteilung von Ergebnissen genetischer Untersuchungen ist nach § 11 Abs. 1 Gesetz über genetische Untersuchungen bei Menschen (Gendiagnostikgesetz – GenDG) nur gegenüber der betroffenen Person zulässig. Anderen Personen gegenüber darf die Mitteilung nur mit ausdrücklicher und schriftlicher Einwilligung des Betroffenen erfolgen (§ 11 Abs. 3 GenDG).

Nach Art. 27 Abs. 5 Satz 2 Bayerisches Krankenhausgesetz ist eine Offenbarung von Patientendaten an Vor-, Mit- oder Nachbehandelnde zulässig, soweit das Einverständnis der Patienten anzunehmen ist.

Die Mitteilung des genetischen Datums „Mosaik 45 X0“ an das Jugendamt erfolgte ohne Rechtsgrund: Sie erfolgte ohne Einverständnis der Eltern und war auch nicht erforderlich, um das Jugendamt über den Verdacht der Kindeswohlgefährdung zu informieren. Die Klinik hat selbst eingeräumt, dass das genetische Datum keine medizinische Relevanz für die vorliegenden klinischen Auffälligkeiten oder zur Erläuterung dieser gegenüber dem Jugendamt gehabt habe. Die Mitteilung kann demnach nicht auf die datenschutzrechtliche Befugnis gemäß § 4 Abs. 3 Satz 2 KKG gestützt werden und verstößt gegen § 11 Abs. 3 GenDG.

Auch die Weitergabe der ermittelten genetischen Daten durch den behandelnden Arzt an neun weitere Therapiekollegen innerhalb der Klinik stellt einen Verstoß gegen datenschutzrechtliche Vorgaben dar, da sie gegen den ausdrücklichen Willen der Mutter erfolgte. Insoweit greift auch Art. 27 Abs. 5 Satz 2 BayKrG nicht, weil der behandelnde Arzt gerade nicht von einem Einverständnis zur Weitergabe an Mitbehandler ausgehen konnte.

Die nach dem Gendiagnostikgesetz erhobenen Daten sind in besonderer Weise schutzwürdig. Die Übermittlung an das Jugendamt und die Weitergabe innerhalb der Klinik stellen deshalb schwerwiegende datenschutzrechtliche Verstöße dar, die zu beanstanden waren.

9 Sozialwesen

9.1 Bundesrecht: Reform des Sozialgesetzbuches

Das gesamte Sozialgesetzbuch enthält eine Vielzahl bereichsspezifischer Regelungen zum Datenschutz. Die seit dem 25. Mai 2018 geltende Datenschutz-Grundverordnung erlaubt den Mitgliedstaaten grundsätzlich, bereichsspezifische Regelungen gestützt auf Art. 6 Abs. 1 UAbs. 1 Buchst. c und e in Verbindung mit Abs. 2 und Abs. 3 UAbs. 1 Buchst. b DSGVO sowie insbesondere Art. 9 Abs. 2 Buchst. b, h und i DSGVO beizubehalten. Dies erforderte allerdings, das bereichsspezifische Datenschutzrecht auf die Vereinbarkeit mit der Datenschutz-Grundverordnung hin zu überprüfen und soweit nötig Anpassungen vorzunehmen.

Mitte März 2017 erreichte mich deshalb ein Gesetzentwurf des Bundesministeriums für Arbeit und Soziales zur Anpassung der Vorschriften des Ersten Buches Sozialgesetzbuch – Allgemeiner Teil – (SGB I) und des Zehnten Buches Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X) an die Datenschutz-Grundverordnung.

Zu diesem Gesetzentwurf hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder im Rahmen ihrer 93. Sitzung am 29./30. März 2017 aufgrund meiner Initiative folgenden Beschluss gefasst:

„I. Der Gesetzgeber wird aufgefordert, wegen des Ungleichgewichts zwischen Bürger und gesetzlichen Sozialversicherungsträgern oder sonstiger Sozialbehörden (Erwägungsgrund 43 DSGVO) im Bereich des Sozialrechts die Verarbeitung besonderer Kategorien von Daten im Sinne von Art. 9 Absatz [1] DSGVO nur auf der Grundlage von bereichsspezifischen Regelungen zuzulassen.

II. Bei der Verarbeitung von Gesundheitsdaten ist der Gesetzgeber aufgefordert, über die entsprechende Anwendung des § 22 Absatz 2 BDSG-E hinausgehend weitere, spezielle Anforderungen für technische und organisatorische Maßnahmen ausdrücklich gesetzlich vorzusehen. Dabei sollten beispielsweise die Grundsätze der Datenminimierung und Speicherbegrenzung sowie die Notwendigkeit einer Datenschutz-Folgenabschätzung besonders berücksichtigt werden.

III. Der Gesetzgeber sollte die in Artikel 4 Nr. 7 und Artikel 26 Absatz 1 Satz 2 der Verordnung (EU) 2016/679 angelegte Möglichkeit nutzen und – soweit seine Regelungskompetenz besteht – die europarechtlichen Vorgaben für gemeinsame Verfahren im nationalen Recht in Bezug auf Gesundheitsdaten präzisieren. Hierzu könnten beispielsweise entsprechende Landesgesetze als Vorlage herangezogen werden.

IV. Die Datenschutzkonferenz unterstützt ausdrücklich die in Nr. 32 der Stellungnahme des Bundesrats zu Artikel 1 (§ 29 Absatz 3 BDSG) des Entwurfs eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU),

erhobene Forderung, wonach die Bundesregierung gebeten wird, „die in § 29 Abs. 3 BDSG-E getroffenen Regelungen zugunsten einer zeitnahen, rechtssicheren und umfassenderen Gesamtregelung auf Grundlage der Anforderungen des Artikels 90 der Datenschutz-Grundverordnung zurückzustellen" (siehe BR-Drs. 110/17 [Beschluss], Seite 29)."

Darüber hinaus habe ich im Rahmen eines Positionspapiers eine Bewertung von Einzelfragen zu dem Gesetzentwurf abgegeben. Dieses Papier war das Ergebnis eines schriftlichen Umlaufverfahrens unter den unabhängigen Datenschutzbehörden des Bundes und der Länder, welches ich als Vorsitzender ihres Arbeitskreises Gesundheit und Soziales durchgeführt habe. Es hat sich insbesondere mit den Regelungen zur Datenerhebung von Sozialdaten mittels Einwilligungserklärung, mit der Verarbeitung von Sozialdaten zu Forschungszwecken und mit der Beschränkung der Betroffenenrechte auseinandergesetzt.

Bedauerlicherweise hat der Bundesgesetzgeber kaum Änderungsvorschläge übernommen und das betreffende Gesetz nahezu unverändert verabschiedet (siehe das Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 17. Juli 2017, BGBl. I S. 2541).

Ein kurzer Überblick über die wesentlichen Änderungen im Ersten und Zehnten Buch Sozialgesetzbuch ist auf meiner Homepage https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018 – Informationsreihe – Einzelthemen" abrufbar. Dabei sind überwiegend nur redaktionelle Anpassungen an die Datenschutz-Grundverordnung, insbesondere an die Begriffsbestimmungen aus Art. 4 DSGVO (siehe § 67 SGB X), vorgenommen worden. Wesentliche Neuerungen ergeben sich bei den Rechten der betroffenen Person (§§ 82 bis 84 SGB X). Zudem sind Regelungen bezüglich der neuen Rechtsschutzmöglichkeiten aufgenommen worden (§§ 81a f. SGB X).

Das Gesetzgebungsverfahren zur Anpassung der weiteren Bücher des Sozialgesetzbuches war bis zum Ende des Berichtszeitraums noch nicht abgeschlossen.

9.2 Gesetzliche Krankenversicherung

9.2.1 Anpassungen an die Datenschutz-Grundverordnung

Im Berichtszeitraum war ich verstärkt mit der Beratung von bayerischen **Krankenkassen** beschäftigt, die Fragen zur Anpassung ihrer Datenschutzhinweise an die Datenschutz-Grundverordnung hatten.

Dabei ging es zum einen um die Anpassung der **konkreten Datenschutzhinweise**, die zum Beispiel auf Antragsformularen verwendet werden, und zum anderen um die Erstellung **allgemeiner Hinweisblätter** zur Erfüllung der Informationspflichten nach Art. 13 und 14 DSGVO.

Dabei galt es auch zu berücksichtigen, dass die §§ 82 ff. Zehntes Buch Sozialgesetzbuch Einschränkungen der Informationspflichten sowie der Rechte der betroffenen Person regeln.

Ähnlich verhielt es sich mit dem Beratungsbedarf hinsichtlich der Anpassung von **Einwilligungserklärungen**.

Dadurch, dass aber das bisherige Sozialgesetzbuch bereits strenge Vorgaben im Zusammenhang mit der Einholung von Einwilligungserklärungen vorsah, haben sich durch die Geltung der Datenschutz-Grundverordnung keine wesentlichen Neuerungen ergeben. Das Merkmal der Freiwilligkeit ist nunmehr besonders sorgfältig zu prüfen (siehe Erwägungsgrund 43 DSGVO). Zudem bedarf es des zusätzlichen Hinweises auf Art. 7 Abs. 3 Satz 2 DSGVO. Danach ist die betroffene Person darüber in Kenntnis zu setzen, dass bei einem Widerruf der Einwilligung die bis zum Widerruf auf Grundlage dieser Einwilligung erfolgte Datenverarbeitung rechtmäßig bleibt.

9.2.2 Häusliche Krankenpflege

Über einen längeren Zeitraum habe ich mich mit dem Fragebogen einer bayerischen Krankenkasse beschäftigt, mit dem sie die versicherte Person hinsichtlich möglicher Ausschlussgründe für den Anspruch auf häusliche Krankenpflege nach § 37 Abs. 3 Fünftes Buch Sozialgesetzbuch– Gesetzliche Krankenversicherung – (SGB V) befragte.

§ 37 SGB V
Häusliche Krankenpflege
(3) Der Anspruch auf häusliche Krankenpflege besteht nur, soweit eine im Haushalt lebende Person den Kranken in dem erforderlichen Umfang nicht pflegen und versorgen kann.

In diesem Zusammenhang stellte die Krankenkasse unter anderem auch die **Frage nach den Gründen für die Ablehnung der Pflege durch eine im Haushalt lebende Person**.

Diese Nachfrage hielt ich jedoch für nicht erforderlich und daher für unzulässig. Meines Erachtens nach können unter Zugrundelegung der Urteile des Bundessozialgerichts vom 30. März 2000, Az.: B 3 KR 23/99 R, und des Landessozialgerichts Brandenburg vom 7. Juni 2005, Az.: L 24 KR 49/03, grundsätzlich nur drei Fragen gestellt werden:

- Leben noch weitere Personen im Haushalt der versicherten Person?
- Wäre eine dieser Personen bereit, die Pflege (teilweise) zu übernehmen?
- Wäre die versicherte Person mit der Pflege durch diese Person einverstanden? Falls nicht, dürfte die versicherte Person hinsichtlich der eigenen Gründe befragt werden.

Das Bundessozialgericht stellt nämlich den Grundsatz auf, dass der Anspruch auf häusliche Krankenpflege nur dann entfällt, wenn ein **beiderseitiges Einverständnis** bezüglich der Übernahme der Pflege durch eine im Haushalt lebende Person (sogenannte **aktive und passive Pflegebereitschaft**) gegeben ist. Des Weiteren besteht laut Gericht keine Möglichkeit der zwangsweisen Durchsetzung, wenn die im Haushalt lebende Person die Übernahme der Pflege verweigern würde. Gleichwohl darf sich die versicherte Person nicht ohne nachvollziehbaren Grund weigern.

Davon unberührt bleibt die Befugnis der Krankenkasse, sich an die verordnende Ärztin oder den verordnenden Arzt zu wenden, wenn diese oder dieser die Verordnung zur häuslichen Krankenpflege nicht oder nicht ordnungsgemäß ausgefüllt haben sollte.

Darüber hinaus habe ich auch empfohlen, die **Frage nach der Versorgung mit täglichen Mahlzeiten** durch eine im Haushalt lebende Person im Fragebogen zu streichen. Als Begründung für diese Frage hat die Krankenkasse angegeben, dass in diesem Zusammenhang auch Medikamente durch diese Person verabreicht werden könnten. Allerdings muss die Medikamentengabe nicht notwendigerweise mit der Nahrungsaufnahme verbunden sein (siehe Sozialgericht Dortmund, Urteile vom 9. April 2003, Az.: S 13 KR 141/02, und vom 20. Juni 2002, Az.: S 44 KR 251/99); dies gilt insbesondere für Medikamente, die nur bei Bedarf eingenommen werden müssen.

Die Krankenkasse ist schließlich meiner Rechtsauffassung gefolgt und hat den Fragebogen entsprechend angepasst.

9.2.3 Erhebung der steuerlichen Identifikationsnummer

Ein Bürger, der bei seiner gesetzlichen Krankenversicherung Verletztengeld beantragt hatte, legte mir ein Schreiben vor, mit dem die Krankenkasse die Angabe der steuerlichen Identifikationsnummer von ihm verlangte.

Grundsätzlich habe ich seit Einführung der steuerlichen Identifikationsnummer Bedenken hinsichtlich der möglichen Entwicklung der steuerlichen Identifikationsnummer hin zu einem einheitlichen Personenkennzeichen geäußert (siehe vor allem meinen 23. Tätigkeitsbericht 2008 unter Nr. 11.1.1). Die Gefahr, zum „gläsernen Bürger“ zu werden, ist im Zeitalter der Digitalisierung der Verwaltungen auch zehn Jahre später nicht geringer geworden.

Deshalb konnte ich die Besorgnis des Petenten nachvollziehen, dass die Erhebung der steuerlichen Identifikationsnummer durch eine Krankenkasse ungewöhnlich wirken muss, weil diese Datenerhebung dem ersten Anschein nach in keinem Zusammenhang mit den originären Aufgaben der gesetzlichen Krankenversicherung steht.

Allerdings sehen das Einkommensteuergesetz (EStG) sowie die Abgabenordnung (AO) hierfür ausreichend Rechtsgrundlagen vor. So hat der Bundesgesetzgeber die gesetzlichen Krankenversicherungen verpflichtet, die Daten über die im Kalenderjahr gewährten Leistungen (im konkreten Fall: Verletztengeld) sowie die Dauer des Leistungszeitraums an die Finanzverwaltung zu übermitteln (§ 32b Abs. 3 Satz 1 Halbsatz 1 EStG). Die Regelung ermöglicht es den Finanzbehörden, den sogenannten Progressionsvorbehalt zu berücksichtigen, womit auf das zu versteuernde Einkommen ein besonderer Steuersatz anzuwenden ist. Die Übermittlungspflicht führt dazu, dass die Träger der Sozialleistungen (hier: die gesetzliche Krankenversicherung) in das Besteuerungsverfahren eingebunden werden.

Damit die Krankenkasse ihrer Pflicht der Datenübermittlung an die Finanzbehörden nachkommen kann, besteht im Gegenzug eine Auskunftspflicht des Leistungsempfängers unter anderem über seine steuerliche Identifikationsnummer (§ 32b Abs. 3 Satz 1 Halbsatz 2 in Verbindung mit § 22a Abs. 2 Satz 1 EStG). Die anschließende Übermittlung der steuerlichen Identifikationsnummer soll eine eindeutige Zuordnung der eingehenden Daten und deren zielgerichtete Auswertung bei den Finanzbehörden ermöglichen.

Falls der Leistungsempfänger die Identifikationsnummer trotz Aufforderung nicht mitteilt, dürfte die Krankenkasse diese sogar unmittelbar beim Bundeszentralamt für Steuern erheben (§ 22a Abs. 2 Satz 2 EStG).

Die Krankenkasse darf die steuerliche Identifikationsnummer aber ausschließlich zu dem Zweck der Übermittlung – zusammen mit den Daten über die gewährte Leistung sowie die Dauer des Leistungszeitraums – verwenden (§ 93c Abs. 7 AO).

Die Eingabe führte dazu, dass die gesetzliche Krankenkasse ihre Datenschutzhinweise, die zum Teil unzureichende Informationen über die Rechtsgrundlagen zur Datenerhebung enthielten, im Sinne der obigen Ausführungen anpasste und richtigstellte.

9.3 Pflege

9.3.1 Vollzug des Pflege- und Wohnqualitätsgesetzes

Bereits in meinem 26. Tätigkeitsbericht 2014 unter Nr. 8.2.1 hatte ich angekündigt, die Einhaltung des mit dem Bayerischen Staatsministerium für Gesundheit und Pflege vereinbarten Verfahrens in Bezug auf die Prüfungen von Pflegeeinrichtungen zu überprüfen. Im 27. Tätigkeitsbericht 2016 unter 8.2.1 hatte ich dann über die Ergebnisse der schriftlichen Umfrage unter den Fachstellen für Pflege und Behinderteneinrichtungen – Qualitätsentwicklung und Aufsicht (FQA; früher Heimaufsicht) berichtet.

Im Nachgang dazu habe ich nunmehr im aktuellen Berichtszeitraum mehrere Prüfungen vor Ort durchgeführt. Aufgrund der dabei gewonnenen Erkenntnisse habe ich folgende allgemeingültige datenschutzrechtliche Hinweise für die Durchführung heimaufsichtsrechtlicher Prüfungen gegeben:

– Einwilligungsrelevanz

  Zunächst ist immer erst zu klären, ob für das jeweilige Tätigwerden der FQA eine Einwilligung benötigt wird.

  Das Gesetz sieht hierzu vor, dass jede Verarbeitung der im Rahmen der Prüfungstätigkeit gewonnenen personenbezogenen Daten der Zustimmung durch die Bewohnerin oder den Bewohner bedarf.

  Die Einsichtnahme in die Pflegedokumentation und die Inaugenscheinnahme des pflegerischen Zustands einer Bewohnerin oder eines Bewohners fallen unproblematisch darunter, ein allgemeines Gespräch mit einer Bewohnerin oder einem Bewohner, um die Einwilligungsfähigkeit zu klären, dagegen (noch) nicht.

– Einwilligungsformular

  Zur Einholung der Einwilligungserklärung ist das vom Gesundheitsministerium zur Verfügung gestellte Musterformular zu verwenden.

Darüber hinaus darf dieses Formular nicht (pauschal) vorab angekreuzt werden; vielmehr ist im Rahmen des „Einwilligungsgesprächs“ zu entscheiden, was tatsächlich Gegenstand der Qualitätsprüfung sein soll.

Zu jedem angekreuzten Punkt muss auch die Einwilligung gegeben worden sein. Das bedeutet, die FQA muss die einwilligende Person über die konkrete Prüftätigkeit (etwa Inaugenscheinnahme des Pflegezustandes oder Einsichtnahme in die Pflegedokumentation) informieren und hierfür jeweils das vorherige Einverständnis einholen.

Auf dem Einwilligungsformular darf im „Briefkopf“ nur die prüfende FQA zu finden sein. Die verantwortliche Stelle muss für die einwilligende Person unmissverständlich erkennbar sein.

Für den Fall, dass bereits im Voraus (nicht am Prüfungstag) eine Einwilligung eingeholt worden ist, kann im Formular das Feld „Datum der Prüfung“ gestrichen werden.

— Einholung der Einwilligung allein bei Bewohnerin oder Bewohner

Eine vorliegende Betreuung schließt zunächst nicht automatisch die Möglichkeit der alleinigen Erklärung der Einwilligung durch die Bewohnerin oder den Bewohner aus. Das in den §§ 1896 ff. Bürgerliches Gesetzbuch (BGB) geregelte Betreuungsrecht verfolgt vielmehr grundsätzlich das Ziel, dem Recht auf Selbstbestimmung sowie auf freie Entfaltung der Persönlichkeit des oder der Betreuten so weit wie möglich Rechnung zu tragen.

Deshalb sollte im Rahmen der Einholung von Einwilligungserklärungen immer erst geprüft werden, ob die Bewohnerin oder der Bewohner – trotz vorhandener (rechtlicher) Betreuung – noch selbst einwilligungsfähig wäre und die Einwilligung demzufolge alleine erklären könnte. Dies gilt insbesondere, wenn das Betreuungsgericht keinen einschlägigen Einwilligungsvorbehalt im Sinne des § 1903 BGB angeordnet hat.

Einwilligungsfähigkeit ist dabei die Fähigkeit der betroffenen Person, mögliche Folgen der Erhebung und Verwendung ihrer personenbezogenen Daten, somit den Umfang und die Tragweite ihrer Zustimmungserklärung, abschätzen zu können.

Falls eine Bewohnerin oder ein Bewohner einwilligungsfähig ist und selbst unterschrieben hat, liegt bereits eine schriftliche Zustimmung vor. Das Ausfüllen eines etwaigen Zusatzes „mündlich zugestimmt“, des „Grundes der nur mündlichen Zustimmung“ sowie ein Gegenzeichnen lassen durch die FQA und/oder durch eine dritte Person wäre in diesem Fall nicht erforderlich und sollte aus Gründen der Rechtsklarheit unterbleiben.

Kann die einwilligungsbereite Bewohnerin oder der einwilligungsbereite Bewohner tatsächlich, zum Beispiel aufgrund körperlicher Einschränkungen, nicht mehr eigenhändig unterschreiben, käme im Ausnahmefall ein Rückgriff auf eine mündliche Einwilligung in Betracht, die auch dokumentiert werden müsste.

Es besteht allerdings kein Wahlrecht einwilligungsfähiger Bewohnerinnen und Bewohner dahingehend, nur mündlich einzuwilligen, falls sie in der Lage sind, selbst zu unterschreiben.

— Einholung der Einwilligung bei Betreuerin oder Betreuer

Falls die Bewohnerin oder der Bewohner nicht mehr einwilligungsfähig ist, kommt die Einholung einer Einwilligung bei einer betreuenden Person in Betracht. Die FQA muss diese Person über den Grund und Inhalt der Qualitätsprüfung aufklären sowie mit ihr das Einwilligungsformular durchgehen.

Wenn die betreuende Person nicht vor Ort anwesend ist, hat diese Aufklärung telefonisch zu erfolgen. Dabei sollte im Hinblick auf die Erklärung der Einwilligung zumindest gefragt werden, ob diese in Textform (etwa per Telefax) erklärt werden kann. Der Rückgriff auf eine mündliche Einwilligungserklärung darf nur im Ausnahmefall erfolgen (siehe 26. Tätigkeitsbericht 2014 unter Nr. 8.2.1 und 27. Tätigkeitsbericht 2016 unter Nr. 8.2.1).

Wenn die betreuende Person die Einwilligung nur mündlich erklären kann, sollte sich davon nicht nur die FQA, sondern auch die Pflegeeinrichtung tatsächlich überzeugen.

Darüber hinaus bin ich bei der Anpassung des Einwilligungsformulars an die Datenschutz-Grundverordnung zur Durchführung heimaufsichtsrechtlicher Prüfungen sowie bei der Erstellung von Hinweisblättern zur Erfüllung der Informationspflichten nach Art. 13 und 14 DSGVO beratend tätig gewesen.

Im Übrigen habe ich die ersten Überlegungen des Gesundheitsministeriums zur Novellierung des Gesetzes zur Regelung der Pflege-, Betreuungs- und Wohnqualität im Alter und bei Behinderung begleitet und werde dies auch in Zukunft tun.

9.3.2 Landespflegegeld

Das Bayerische Staatsministerium für Gesundheit und Pflege hat mich im Berichtszeitraum frühzeitig in das Gesetzgebungsverfahren zur Einführung eines Bayerischen Landespflegegeldes eingebunden. Ich habe die Gelegenheit wahrgenommen, hierzu aus datenschutzrechtlicher Sicht Stellung zu nehmen.

In diesem Zusammenhang habe ich insbesondere Bedenken bezüglich einer Regelung geäußert, mit der das neu zu schaffende Bayerische Landesamt für Pflege die Bescheinigung der Pflegebedürftigkeit, die von der Antragstellerin oder dem Antragsteller vorgelegt werden soll, überprüfen können sollte. Hierfür sollte eine Einwilligung der jeweiligen Person eingeholt werden. Ich habe dem Gesundheitsministerium hierzu mitgeteilt, dass ich es für zweifelhaft halte, ob die Einwilligung wirksam erteilt werden kann, da die Einwilligung in die Gewährung einer staatlichen Leistung eingebunden ist und insoweit die Freiwilligkeit in Frage stehen dürfte (siehe Erwägungsgrund 43 DSGVO). Stattdessen habe ich vorgeschlagen, gewisse Mitwirkungspflichten der Antragstellerin oder des Antragstellers vorzusehen.

Nunmehr erklärt das inzwischen verabschiedete Bayerische Landespflegegeldgesetz vom 24. Juli 2018 (GVBl. S. 613, 625) unter anderem das Erste Buch Sozialgesetzbuch (SGB I) sowie das Erste und Zweite Kapitel des Zehnten Buches

Sozialgesetzbuch für entsprechend anwendbar. Damit gelten die allgemeinen sozialdatenschutzrechtlichen Vorschriften im Zusammenhang mit der Gewährung des Landespflegegeldes, aber auch gewisse Mitwirkungspflichten der Antragstellerin oder des Antragstellers (siehe § 60 SGB I). Laut der Gesetzesbegründung soll hiermit auf der einen Seite die Antragstellerin oder der Antragsteller mit nur geringem Darlegungsaufwand hinsichtlich des Nachweises ihrer oder seiner Pflegebedürftigkeit belastet werden. Auf der anderen Seite sollen eine hohe Qualität gewährleistet und Missbrauch verhindert werden. Im Regelfall wird daher eine Kopie des Bescheides über die Pflegebedürftigkeit ausreichend sein. Anlassbezogen und stichprobenartig kann die zuständige Behörde aber weitere Beweismittel verlangen, beispielsweise Bestätigungen der Pflegekasse (vgl. Landtags-Drucksache 17/22033, S. 38). Auf eine Datenverarbeitungsbefugnis auf Grundlage einer Einwilligungserklärung ist dagegen verzichtet worden.

Darüber hinaus habe ich die datenschutzkonforme Gestaltung des Formulars zur Beantragung des Landespflegegeldes begleitet.

9.3.3 Alten- und Pflegeheime als Wettbewerbsunternehmen

Im Rahmen meiner Aufgabe, die Verwaltung in datenschutzrechtlichen Zweifelsfragen zu beraten, hatte ich zu klären, welche datenschutzrechtlichen Vorschriften für bayerische Alten- und Pflegeheime einschlägig sind. Eine Kommune war an mich deshalb herangetreten. Zu der aufgeworfenen Frage vertrete ich folgende Auffassung:

Zunächst ist vorrangig das Gesetz zur Regelung der Pflege-, Betreuungs- und Wohnqualität im Alter und bei Behinderung (Pflege- und Wohnqualitätsgesetz) einschlägig. Die darin getroffenen Regelungen stellen besondere Rechtsvorschriften im Sinne des Art. 1 Abs. 5 BayDSG dar.

Sollte das Pflege- und Wohnqualitätsgesetz zu einer konkreten datenschutzrechtlichen Fallkonstellation keine Regelung enthalten, ist auf die allgemeinen datenschutzrechtlichen Vorschriften zurückzugreifen. Ergänzend zur Datenschutz-Grundverordnung sind diese entweder dem Bayerisches Datenschutzgesetz oder dem Bundesdatenschutzgesetz zu entnehmen.

Entscheidend für die Frage, welche allgemeine datenschutzrechtliche Norm (Bayerisches Datenschutzgesetz oder Bundesdatenschutzgesetz) ergänzend zur Datenschutz-Grundverordnung herangezogen werden muss, ist, ob das Alten- oder Pflegeheim ein Wettbewerbsunternehmen darstellt. Denn soweit öffentliche Stellen als Unternehmen am Wettbewerb teilnehmen, gilt das Bundesdatenschutzgesetz (Art. 1 Abs. 3 BayDSG).

Alten- und Pflegeheime nehmen zwar mit der Sicherstellung einer bedarfsgerechten pflegerischen Versorgung der Bevölkerung grundsätzlich eine öffentliche Aufgabe wahr. Allerdings kann dieser Versorgungsauftrag nicht losgelöst von dem Kriterium der Wirtschaftlichkeit gesehen werden (§ 72 Abs. 3 Satz 1 Nr. 2 Elftes Buch Sozialgesetzbuch – Soziale Pflegeversicherung –). Laut der Gesetzesbegründung zu dieser Vorschrift sollte damit den Landesverbänden der Pflegekassen die Möglichkeit eingeräumt werden, Pflegeeinrichtungen auch über den aktuellen Versorgungsbedarf hinaus zur Pflege der Versicherten zuzulassen. Hierdurch sollte ein geschlossener Markt der zugelassenen Pflegeeinrichtungen verhindert, neuen innovativen Leistungsanbietern der Zugang zum „Pflegemarkt“

offen gehalten und so der Wettbewerb unter den Pflegeeinrichtungen gefördert werden. Diese Haltung des Bundesgesetzgebers führt dazu, dass von einer wettbewerblichen Situation auf dem Markt der Pflegeeinrichtungen ausgegangen werden muss.

Diese Sachverhalte und die daran anknüpfenden Überlegungen haben mich im Ergebnis zu der Auffassung gelangen lassen, dass als allgemeines Datenschutzrecht für bayerische Alten- und Pflegeheime, auch wenn sie durch eine öffentliche Stelle betrieben werden, neben der Datenschutz-Grundverordnung das Bundesdatenschutzgesetz anzuwenden ist.

9.4 Sozialbehörden: Verarbeiten von Sozialdaten durch Optionskommunen

9.4.1 Einschaltung des ärztlichen Dienstes

Im Berichtszeitraum habe ich mich weiterhin – wie bereits in der Vergangenheit (siehe 27. Tätigkeitsbericht 2016 unter Nr. 8.3.2 und 25. Tätigkeitsbericht 2012 unter Nr. 8.12) – mit der Verarbeitung medizinischer Daten durch Sozialbehörden, insbesondere durch Optionskommunen, beschäftigt.

Das Bayerische Staatsministerium für Familie, Arbeit und Soziales hat meine Erkenntnisse zum Anlass genommen, die bereits vorhandenen Vollzugshinweise für Optionskommunen zur Thematik Sozialdatenschutz um die Rubrik „Erhebung medizinischer Daten“ zu ergänzen. Darin wird unter anderem ein Verfahren zur Zusammenarbeit mit der begutachtenden Ärztin oder dem begutachtenden Arzt empfohlen.

— Vertragliche Vereinbarung

  Dabei stellte sich dann konkret die Frage, wie die Beauftragung einer niedergelassenen Ärztin oder eines niedergelassenen Arztes zur Vornahme einer ärztlichen Begutachtung durch eine Sozialbehörde rechtlich einzuordnen ist.

  Ich habe dabei die Auffassung vertreten, dass, wenn ein entsprechender Dienst- oder Beratungsvertrag mit der niedergelassenen Ärztin oder dem niedergelassenen Arzt geschlossen wird, es sich bei der Ärztin oder dem Arzt nicht um eine „Dritte“ oder einen „Dritten“, also nicht um eine Person außerhalb der verantwortlichen Stelle handelt (siehe hierzu auch meinen 27. Tätigkeitsbericht 2016 unter Nr. 8.3.9).

  Bezogen auf die Einschaltung von ärztlichen Beratern durch einen Sozialversicherungsträger hat das Bundessozialgericht in zwei Urteilen vom 5. Februar 2008, Az.: B 2 U 8/07 R und B 2 U 10/07 R, festgestellt, dass

  „die Beratungstätigkeit nicht auf Ärzte, die in einem Beschäftigungsverhältnis im Sinne des § 7 Viertes Buch Sozialgesetzbuch (SGB IV) bei dem jeweiligen Unfallversicherungsträger stehen, beschränkt ist […]. Entscheidend ist die Ausgestaltung der Rechtsbeziehung zu ihnen, so dass z. B. der Abschluss entsprechender Dienst- oder Beratungsverträge höherer Art mit sogenannten Beratungsärzten möglich ist, die dann als Teil des Unfallversicherungsträgers tätig werden“.

Das bedeutet, dass in diesen Fällen die Vertragsärztinnen und -ärzte nicht als sogenannte „Dritte“ anzusehen sind, sondern im Rahmen der Begutachtung Teil der verantwortlichen Stelle werden.

Dies hat zur Folge, dass das datenschutzrelevante Handeln der niedergelassenen Ärztin oder des niedergelassenen Arztes im Zusammenhang mit der Begutachtung der auftraggebenden Sozialbehörde zuzurechnen ist.

Hinsichtlich des notwendigen Inhalts einer entsprechenden Vereinbarung habe ich auf die im Rahmen des Urteils des Landessozialgerichts Baden-Württemberg vom 25. Oktober 2013, Az.: L 8 U 541/13, festgelegten Kriterien verwiesen (insbesondere Unterwerfung unter die entsprechenden Amts- und Verschwiegenheitspflichten, die auch für Angestellte sowie Beamtinnen und Beamten gelten; siehe auch Landessozialgericht Bayern, Urteil vom 13. Juni 2013, Az.: L 17 U 239/11).

– Schweigepflichtentbindungserklärung

Unabhängig davon habe ich im Rahmen einer Eingabe Kenntnis davon erlangt, dass die Gewährung einer Leistung nach dem Zweiten Buch Sozialgesetzbuch – Grundsicherung für Arbeitsuchende – zwingend von der Abgabe einer Schweigepflichtentbindungserklärung abhängig gemacht worden sei; obwohl die betroffene Person bereit war, medizinische Unterlagen selbst beizubringen oder sich einer ärztlichen Begutachtung zu unterziehen.

Ich habe hierzu die Auffassung vertreten, dass die Nichterteilung einer Schweigepflichtentbindungserklärung nicht in jedem Fall automatisch zu einer Entziehung oder Versagung der Leistungen führen darf. Die Erteilung einer Schweigepflichtentbindungserklärung stellt zwar eine Mitwirkungsobliegenheit nach § 60 Abs. 1 Nr. 1 Erstes Buch Sozialgesetzbuch (SGB I) dar, und die Nichterteilung ohne wichtigen Grund kann bei Vorliegen der übrigen gesetzlichen Voraussetzungen zu einer vollständigen oder teilweisen Versagung oder Entziehung der Leistungen führen (siehe § 66 SGB I).

Sofern der Leistungsberechtigte von sich aus aber ärztliche Unterlagen zum Beleg seiner Einschränkungen vorgelegt hat, liegt zunächst keine erhebliche Erschwerung der Sachverhaltsermittlung vor, da diese Unterlagen zunächst von der begutachtenden Ärztin oder dem begutachtenden Arzt ausgewertet werden können. Sollten die Unterlagen zum Nachweis nicht genügen, kann anschließend geprüft werden, ob zusätzlich eine Entbindung von der Schweigepflicht erforderlich ist.

9.4.2 Anpassung an die Datenschutz-Grundverordnung

Die bereits vorhandenen Vollzugshinweise des Sozialministeriums für Optionskommunen zur Thematik Sozialdatenschutz sind unter meiner Beteiligung an die Datenschutz-Grundverordnung angepasst worden. Neben allgemeinen datenschutzrechtlichen Grundsätzen enthalten diese Hinweise auch Ausführungen zu konkreten Einzelfällen (etwa zur Datenverarbeitung von Kontoauszügen).

9.5 Jugendhilfe

9.5.1 Jugendbefragungen

Im Berichtszeitraum habe ich von mehreren Befragungen junger Menschen Kenntnis erlangt. Dabei geht es um ein Instrument der Träger der öffentlichen Jugendhilfe, mit dem Wünsche, Bedürfnisse und Interessen junger Menschen bezüglich des unter anderem freizeitlichen Angebots abgefragt werden sollen (siehe § 80 Abs. 1 Nr. 2 Achtes Buch Sozialgesetzbuch – Kinder- und Jugendhilfe – SGB VIII). Das Ergebnis der Befragung soll dann in die sogenannte Jugendhilfeplanung einfließen.

Von wenigen Ausnahmen abgesehen – die meine datenschutzrechtliche Beratung vorab in Anspruch genommen haben –, zeigten sich dabei immer ähnliche datenschutzrechtliche Problemfelder.

Die Träger der öffentlichen Jugendhilfe gingen zunächst von einer anonymen Befragung der Kinder und Jugendlichen aus und hielten damit Hinweise zum Datenschutz für entbehrlich.

In den meisten Fällen war jedoch ein Personenbezug aufgrund der konkreten und umfangreichen Fragestellungen zumindest herstellbar. Dies ist bereits ausreichend, um von der Erhebung von „Sozialdaten“ im Sinne von § 67 Abs. 1 Satz 1 Zehntes Buch Sozialgesetzbuch (SGB X) zu sprechen.

Bei der Erhebung und Verwendung von Sozialdaten in der Jugendhilfe gelten dann gem. § 61 Abs. 1 Satz 1 SGB VIII die folgenden datenschutzrechtlichen Vorschriften: §§ 62 bis 68 SGB VIII, § 35 Erstes Buch Sozialgesetzbuch (SGB I) sowie §§ 67 bis 85a SGB X.

Diese Vorschriften gelten für alle Stellen des Trägers der öffentlichen Jugendhilfe, soweit sie Aufgaben nach dem Achten Buch Sozialgesetzbuch wahrnehmen. Dies gilt entsprechend für die Wahrnehmung von Aufgaben durch kreisangehörige Gemeinden und Gemeindeverbände, die nicht örtliche Träger sind (§ 61 Abs. 1 Satz 3 SGB VIII).

Das bedeutet, sobald ein Personenbezug herstellbar ist, müssen sozialdatenschutzrechtliche Vorgaben beachtet werden. Konkret müssten Datenschutzhinweise vorgesehen werden. Darin müssen insbesondere Ausführungen dazu enthalten sein, auf welche Rechtsgrundlagen im Sozialgesetzbuch oder allgemeinen Datenschutzrecht sich die Datenverarbeitungen gegenüber den befragten Personen stützen lassen. Zudem sollte aufgeführt sein, dass die Teilnahme freiwillig ist und eine Nichtteilnahme keine negativen Folgen hat.

Des Weiteren sollten dann die Eltern über die entsprechende Befragung im Vorfeld informiert und deren Einverständnis eingeholt werden. Das Gesetz sieht zwar ausdrücklich vor, dass junge Menschen selbst Adressat der Leistungen der Jugendarbeit sind (siehe Wortlaut des § 11 SGB VIII). Allerdings setzt laut Kommentarliteratur die Inanspruchnahme der Leistungen der Jugendarbeit durch Kinder und Jugendliche im Innenverhältnis die Zustimmung der Eltern voraus.

Auch nach der Datenschutz-Grundverordnung verdienen Kinder bei ihren personenbezogenen Daten besonderen Schutz, da sie sich der betreffenden Risiken

und Folgen bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind (siehe Erwägungsgrund 38 DSGVO).

Falls der Fragebogen online – etwa mittels QR-Code – ausgefüllt werden soll, müsste man sich darüber hinaus mit mindestens folgenden technischen und organisatorischen Fragen beschäftigen: technische Absicherung (insbesondere Verschlüsselung), Einbindung von weiteren Dienstleistern (etwa zum Betrieb der Website) und Protokollierung. IP-Adressen gelten im Allgemeinen als personenbezogene Daten. Eine Protokollierung der vollständigen IP-Adresse würde somit auch bedeuten, dass die Erhebung der Daten der Jugendumfrage nicht anonymisiert erfolgen würde.

Schließlich müssten bei der Einbindung von Dienstleistern, zum Beispiel auch für die Auswertung von Fragebögen, datenschutzrechtliche Vorgaben beachtet werden, die im Rahmen eines Vertrages niedergelegt werden sollten.

9.5.2 Informationsaustausch zwischen Jugendamt und Ermittlungsbehörden

Ich war im Berichtszeitraum des Öfteren mit der Beratung von Jugendämtern beschäftigt, die von Ermittlungsbehörden aufgefordert worden waren, personenbezogene Daten weiterzugeben; auch das Begehren nach Akteneinsicht oder Aktenherausgabe sowie von Zeugenaussagen waren Gegenstand meiner Beratungen.

Zur Klarstellung möchte ich vorab darauf hinweisen, dass nachfolgend (nur) die Zulässigkeit der Verarbeitung von Daten, die dem Sozialgeheimnis nach § 35 Abs. 1 Satz 1 Erstes Buch Sozialgesetzbuch (SGB I) unterfallen, dargestellt wird. Davon zu trennen ist die Frage nach einer etwaigen strafbewehrten Verletzung von Privatgeheimnissen (§ 203 Strafgesetzbuch – StGB).

— Datenübermittlungsbefugnis

  Das Sozialgeheimnis verpflichtet den Träger der öffentlichen Jugendhilfe grundsätzlich auch gegenüber den Ermittlungsbehörden. Eine Übermittlung von Daten ist somit nur zulässig, wenn eine entsprechende Befugnis nach dem Sozialgesetzbuch (etwa dem Achten oder Zehnten Buch – SGB VIII oder SGB X) besteht.

  Als Datenübermittlungsbefugnis können verschiedene Rechtsgrundlagen in Betracht kommen, die je nach Fallkonstellation einschlägig sein könnten; **insbesondere** zu prüfen sind:

  — Übermittlungsbefugnis gemäß § 68 SGB X:

    Nach dieser Vorschrift dürfen grundsätzlich nur gewisse Sozialdaten (etwa Name, Vorname, Geburtsdatum, derzeitige Anschrift der betroffenen Person) zur Erfüllung von Aufgaben unter anderem der Polizeibehörden im Einzelfall übermittelt werden, allerdings nur auf Ersuchen der in dieser Vorschrift genannten Stellen.

— Übermittlungsbefugnis gemäß § 73 SGB X:

Eine Übermittlung von Sozialdaten ist danach – auf Anordnung des Richters – zulässig, soweit sie zur Durchführung eines Strafverfahrens wegen eines Verbrechens oder wegen einer sonstigen Straftat von erheblicher Bedeutung erforderlich ist.

— Übermittlungsbefugnis gemäß § 69 Abs. 1 Nr. 1 SGB X:

Eine Übermittlung von Daten gemäß § 69 Abs. 1 **Nr. 1** SGB X ist zulässig, soweit sie erforderlich ist für die Erfüllung der Zwecke, für welche die Daten erhoben worden sind oder für die Erfüllung einer gesetzlichen Aufgabe des Jugendamts. Die Aufgaben des Jugendamts im Bereich der Jugendhilfe ergeben sich aus § 2 SGB VIII.

— Übermittlungsbefugnis gemäß § 69 Abs. 1 Nr. 2 SGB X:

Gemäß § 69 Abs. 1 **Nr. 2** SGB X wäre eine Übermittlung von Sozialdaten zulässig, soweit sie erforderlich ist für die Durchführung eines mit der Erfüllung einer Aufgabe nach § 69 Abs. 1 Nr. 1 SGB X zusammenhängenden gerichtlichen Verfahrens einschließlich eines Strafverfahrens. Nicht ausreichend ist ein lediglich örtlicher oder zeitlicher Zusammenhang mit der Tätigkeit des Jugendamts. Vielmehr muss ein sachlicher Zusammenhang zwischen der Aufgabenerfüllung und der Einleitung des gerichtlichen Verfahrens bestehen. Ob dieser Zusammenhang besteht, muss das Jugendamt – im Gegensatz zu § 73 SGB X – selbst entscheiden, da es für die Aufgabenerfüllung zuständig ist.

— Einschränkung der Datenübermittlungsbefugnis

Hinsichtlich der vorgenannten Datenübermittlungsbefugnisse müssen zusätzlich Vorschriften geprüft werden, die eine etwaig bestehende Befugnis wieder einschränken könnten; mit der Folge, dass eine Übermittlung doch nicht zulässig wäre.

— Einschränkung nach § 64 Abs. 2 SGB VIII:

Die Zulässigkeit der Übermittlung nach § 69 SGB X kann durch § 64 Abs. 2 SGB VIII eingeschränkt sein. Die Übermittlung darf danach den Erfolg einer zu gewährenden Leistung nicht in Frage stellen.

— Einschränkung nach § 65 SGB VIII:

Bei der Einschränkung nach § 65 SGB VIII handelt es sich um den Schutz von Informationen, die dem Jugendamt zum Zweck persönlicher und erzieherischer Hilfe anvertraut worden sind. Anvertraut sind Informationen laut der Kommentarliteratur nicht nur, wenn die Mitteilung „unter dem Siegel der Verschwiegenheit“ erfolgt, sondern immer dann, wenn derjenige, der die Information der Mitarbeiterin oder dem Mitarbeiter des Jugendamts preisgibt, im Sinne einer subjektiven Zweckbindung von dessen Verschwiegenheit ausgeht und

dies ausdrücklich signalisiert oder wenn dies aus dem Zusammenhang erkennbar ist.

Die Nummern 1 bis 5 des § 65 Abs. 1 Satz 1 SGB VIII enthalten jedoch auch wiederum Ausnahmen, die eine zulässige Weitergabe der anvertrauten Informationen ermöglichen. Im Verhältnis zur Polizei kommt überwiegend nur Nummer 5 in Betracht. Danach ist eine Weitergabe unter den Voraussetzungen zulässig, unter denen eine der in § 203 Abs. 1 oder 4 StGB genannten Personen dazu befugt wäre. Eine Rechtfertigung einer solchen Offenbarung könnte sich etwa aus rechtfertigendem Notstand, Nothilfe oder der Wahrnehmung rechtlicher Interessen des Verantwortlichen ergeben.

- Einschränkung nach § 76 SGB X:

  Bei der Übermittlung besonders schutzwürdiger Sozialdaten nach den §§ 68 bis 75 SGB X ist als Einschränkung § 76 SGB X zu beachten.

- Sonderregelung des § 68 SGB VIII

  Für den Schutz von Sozialdaten bei deren Erhebung und Verwendung im Rahmen der Tätigkeit des Jugendamts als Amtspfleger, Amtsvormund und Beistand gilt **nur** § 68 SGB VIII (siehe § 61 Abs. 2 SGB VIII).

- Zeugenaussage

  Für den Fall, dass eine Datenübermittlung **unzulässig** ist, besteht weder eine Pflicht zur Auskunft, zum Zeugnis noch zur Vorlage oder Auslieferung von Schriftstücken, nicht automatisierten Dateien und automatisiert verarbeiteten Sozialdaten. Dies ergibt sich aus § 61 Abs. 1 Satz 1 SGB VIII in Verbindung mit § 35 Abs. 3 SGB I.

  § 35 Abs. 3 SGB I richtet sich zunächst an die in § 35 Abs. 1 Satz 1 und 4 SGB I genannten Stellen, aber auch an deren Beschäftigte (siehe § 35 Abs. 1 Satz 5 SGB I); das heißt auch an jede Mitarbeiterin und jeden Mitarbeiter des Jugendamts. Den Bediensteten darf daher keine Genehmigung zur Aussage als Zeuge erteilt werden (siehe etwa Landgericht Braunschweig, Beschluss vom 13. Juni 1986, Az.: 32 Qs 48/86).

9.5.3 Kommunale Satzungen bayerischer Kindertageseinrichtungen

Ich habe Kenntnis darüber erlangt, dass eine Gemeinde per Satzung für ihre örtliche Kindertageseinrichtung festlegte, dass Eltern dazu verpflichtet sind, bei jeglicher Erkrankung des Kindes und einem dadurch bedingten Fehlen mitzuteilen, um welche Erkrankung es sich handelt und wie lange diese voraussichtlich dauern wird. Darüber hinaus wurde von den Eltern verlangt, das vollständige Nachweisheft für Vorsorgeuntersuchungen und den Impfpass vorzulegen.

Solche pauschalen Vorgaben sind datenschutzrechtlich allerdings in hohem Maße problematisch.

So lässt sich eine (allgemeine) Meldepflicht von Eltern gegenüber Kindertageseinrichtungen hinsichtlich jeglicher Erkrankung des Kindes sowie der Erkrankungsart und -dauer keiner gesetzlichen Regelung entnehmen. Weder in Gesetzen des Sozial- noch des Gesundheitsrechts gibt es derzeit einen Anknüpfungspunkt hierfür. Eine entsprechende Meldung der Eltern kann allenfalls auf freiwilliger Basis erfolgen. Lediglich das Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen (Infektionsschutzgesetz – IfSG) sieht eine Meldepflicht vor. Diese ist aber nicht pauschal ausgestaltet, sondern nimmt allein auf bestimmte übertragbare Erkrankungen Bezug (beispielsweise Cholera, Keuchhusten, Masern, siehe § 34 Abs. 4 und 5 IfSG).

Auch für eine verpflichtende Vorlage des vollständigen Nachweishefts für Vorsorgeuntersuchungen und des Impfpasses ist eine gesetzliche Grundlage nicht erkennbar. Vorgeschrieben ist hier lediglich, dass Eltern bei der Anmeldung des Kindes eine Bestätigung über dessen Teilnahme an der letzten fälligen altersentsprechenden Früherkennungsuntersuchung vorzulegen haben (Art. 9b Abs. 2 Satz 1 Bayerisches Gesetz zur Bildung, Erziehung und Betreuung von Kindern in Kindergärten, anderen Kindertageseinrichtungen und in Tagespflege), sowie, dass (lediglich) ein Nachweis über die erfolgte Impfberatung erbracht werden muss (§ 34 Abs. 10a IfSG).

Ich habe der Gemeinde meine datenschutzrechtlichen Einwände mitgeteilt, woraufhin die Satzung geändert wurde; die beanstandeten Vorgaben sind nun nicht mehr in der Satzung enthalten.

10 Steuer- und Finanzverwaltung

10.1 Neuregelung der Datenschutzaufsicht im Steuerwesen

Zum 25. Mai 2018 wurde die Zuständigkeit für die datenschutzrechtliche Aufsicht im Steuerwesen neu geregelt. Bislang habe ich sowohl die bayerischen staatlichen Finanzbehörden, insbesondere die Finanzämter, als auch die kommunalen Steuerbehörden umfassend datenschutzrechtlich kontrolliert. Der nun geltende § 32h Abs. 1 Satz 1 Abgabenordnung (AO) bringt im Freistaat Bayern eine **Aufteilung der Datenschutzaufsicht** zwischen dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (Bundesbeauftragter) und mir mit sich.

§ 32h AO
Datenschutzrechtliche Aufsicht, Datenschutz-Folgenabschätzung
(1) [1]Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit nach § 8 des Bundesdatenschutzgesetzes ist zuständig für die Aufsicht über die Finanzbehörden hinsichtlich der Verarbeitung personenbezogener Daten im Anwendungsbereich dieses Gesetzes. [2]Die §§ 13 bis 16 des Bundesdatenschutzgesetzes gelten entsprechend.

Die Datenschutzaufsicht durch den Bundesbeauftragten betrifft die Verwaltung bundesrechtlich geregelter Steuern im Anwendungsbereich der Abgabenordnung. Hinsichtlich nicht-steuerbezogener Tätigkeiten der staatlichen Finanzbehörden liegt die Datenschutzaufsicht weiterhin bei mir. Auch bei der Tätigkeit der kommunalen Steuerämter kommt es zu einer Zuständigkeitsteilung zwischen dem Bundesbeauftragten und mir.

Diese auf den ersten Blick etwas unübersichtliche Zuständigkeitsordnung möchte ich im Folgenden anhand der praktisch wichtigsten Fallgruppen veranschaulichen:

10.1.1 Einkommensteuer, Umsatzsteuer, Körperschaftsteuer und andere bundesgesetzlich geregelte Steuern

Die wichtigste Fallgruppe betrifft die Haupttätigkeit der Finanzämter, die Verwaltung der „großen" Steuern: Einkommen-, Umsatz- und Körperschaftsteuer. Der Bundesbeauftragte beaufsichtigt die staatlichen Finanzbehörden in datenschutzrechtlicher Hinsicht bei der Verwaltung dieser und anderer bundesrechtlich geregelter Steuern – wie Schenkungssteuer oder Erbschaftsteuer –, und zwar einschließlich des Vollstreckungs- und des Steuerfahndungsverfahrens.

Damit ist der **Bundesbeauftragte regelmäßig Ansprechpartner** für Bürgerinnen und Bürger bei datenschutzrechtlichen Fragen im Zusammenhang mit der Verwaltung der bundesrechtlich geregelten Steuern durch die Finanzämter.

10.1.2 Realsteuern (Grund- und Gewerbesteuer)

Differenzierter ist die Aufsichtszuständigkeit im Zusammenhang mit der Grund- und der Gewerbesteuer geregelt, weil diese teils von den staatlichen Finanzämtern und teils von den kommunalen Steuerbehörden verwaltet werden. Die datenschutzrechtliche Aufsicht ist hier zwischen dem Bundesbeauftragten und mir aufgeteilt:

— Soweit das **Finanzamt** im Bereich der Grund- und der Gewerbesteuer zuständig ist, unterliegt es der **Datenschutzaufsicht durch den Bundesbeauftragten**. Das entspricht der zur Einkommensteuer dargestellten Regelung, schließlich sind die Grund- und die Gewerbesteuer bundesgesetzlich geregelte Steuern, die (zunächst) das Finanzamt auf Grundlage der Abgabenordnung verwaltet.

— Handelt dagegen (sodann) die **Gemeinde**, ist die **datenschutzrechtliche Aufsicht zwischen dem Bundesbeauftragten und mir geteilt**. Die konkrete Zuständigkeit hängt davon ab, ob die Gemeinde auf Grundlage der Abgabenordnung tätig wird oder ob ihr Handeln auf einer anderen Rechtsgrundlage beruht.

— Handelt die Gemeinde bei der Verwaltung der Realsteuern im **Anwendungsbereich der Abgabenordnung**, unterliegt sie der Datenschutzaufsicht durch den Bundesbeauftragten. Das folgt aus § 1 Abs. 2 Nr. 1 AO, der insoweit die Regelung des § 32h AO für anwendbar erklärt:

> *§ 1 AO*
> *Anwendungsbereich*
> *(2) Für die Realsteuern gelten, soweit ihre Verwaltung den Gemeinden übertragen worden ist, die folgenden Vorschriften dieses Gesetzes entsprechend:*
> *1. die Vorschriften des Ersten, Zweiten, Vierten, Sechsten und Siebten Abschnitts des Ersten Teils (Anwendungsbereich; Steuerliche Begriffsbestimmungen; Datenverarbeitung und Steuergeheimnis; Betroffenenrechte; Datenschutzaufsicht, Gerichtlicher Rechtsschutz in datenschutzrechtlichen Angelegenheiten),*
> *[…]*

Die in § 1 Abs. 2 Nr. 1 AO vorgesehene Anwendung der Regeln zur Datenschutzaufsicht kann aus meiner Sicht nur bedeuten, dass die Gemeinden bei der Verwaltung der Realsteuern der Datenschutzaufsicht durch den **Bundesbeauftragten** unterliegen, wenn die Voraussetzungen von § 32h Abs. 1 Satz 1 AO im Übrigen erfüllt sind. Das betrifft insbesondere die **Festsetzung und Erhebung der Grund- und der Gewerbesteuer durch die Gemeinden**. Der Bundesbeauftragte hat sich meinem Verständnis der gesetzlichen Regelung ebenso angeschlossen wie die Datenschutz-Aufsichtsbehörden der anderen Länder.

— Im Rahmen der **Vollstreckung von Realsteuern sowie in außergerichtlichen Rechtsbehelfsverfahren** (Einspruchs- oder Widerspruchsverfahren) handeln die kommunalen Steuerämter dagegen nicht auf Grundlage der Abgabenordnung. Diese Verfahren richten sich nach anderen bundesrechtlichen Vorschriften wie der Verwaltungsgerichtsordnung (VwGO)

oder nach landesrechtlichen Vorschriften wie dem Bayerischen Verwaltungszustellungs- und Vollstreckungsgesetz (VwZVG). In diesen Verfahrensabschnitten bin **nach wie vor ich datenschutzaufsichtlich zuständig**.

10.1.3 Landesrechtliche Steuern (Kirchensteuer)

Auch für die datenschutzrechtliche Aufsicht über die Finanzbehörden bei der Anwendung von bayerischen Steuergesetzen bin ich weiterhin zuständig. Das betrifft in der Praxis vor allem die Kirchensteuer.

Für die Kirchensteuer gilt allerdings wie bislang, dass ich mir die Aufsicht mit den für die bayerischen Kirchensteuerämter zuständigen kirchlichen Datenschutz-Aufsichtsbehörden teile. Das bedeutet: Maßnahmen der Kirchensteuerämter unterliegen deren Datenschutzaufsicht, während sich meine Zuständigkeit auf die Maßnahmen der staatlichen Finanzbehörden (vor allem Finanzämter, Bayerisches Landesamt für Steuern) bei der Verwaltung der Kirchensteuer bezieht.

Soweit die Finanzämter im Zusammenhang mit der Kirchensteuer allerdings unmittelbar auf Grundlage der Abgabenordnung handeln, unterliegen sie gemäß § 32h Abs. 1 Satz 1 AO der Aufsicht des Bundesbeauftragten. Das gilt insbesondere für die in § 31 Abs. 1 Satz 1 AO geregelte Verpflichtung, den öffentlich-rechtlichen Religionsgemeinschaften die für die Festsetzung der Kirchensteuer erforderlichen Daten aus der Einkommensteuerveranlagung mitzuteilen.

10.1.4 Kommunale Steuern

Zu den kommunalen Steuergesetzen zählen die **örtlichen Verbrauch- und Aufwandsteuern** der Gemeinden (vgl. Art. 3 Kommunalabgabengesetz). Wichtigste Beispiele sind die **Zweitwohnungsteuer** und die **Hundesteuer**. Diese Steuern werden allein von den Kommunen verwaltet. Die datenschutzrechtliche Aufsicht liegt somit weiterhin bei mir.

10.1.5 Nicht-steuerbezogene Tätigkeit der Finanzämter

In datenschutzrechtlicher Hinsicht beaufsichtige ich die Finanzämter weiterhin, soweit sie nicht auf steuerlichem Gebiet tätig sind. Das betrifft beispielsweise den Umgang der Finanzämter mit personenbezogenen Daten ihrer Bediensteten, mithin Fragen des **Personaldatenschutzes**.

Auch soweit die Finanzämter nicht-steuerliche **Geldforderungen des Freistaates Bayern** aus Leistungsbescheiden staatlicher Behörden vollstrecken (vgl. Art. 25 VwZVG), unterliegen sie nach wie vor meiner datenschutzrechtlichen Aufsicht.

10.1.6 Bewertung der Neuverteilung der Datenschutz-Aufsichtszuständigkeiten

Die Neuregelung der datenschutzrechtlichen Aufsichtszuständigkeiten im Steuerwesen, wie sie § 32h Abs. 1 Satz 1 AO vorsieht, wurde damit begründet, dass sie im Interesse einer bundesweit einheitlichen Anwendung der Abgabenordnung liegt.

Gleichwohl ist festzustellen, dass die **Gesetzgebungskompetenz des Bundes** für die Zuständigkeitsverlagerung von den bisher nach Landesrecht zuständigen Datenschutz-Aufsichtsbehörden auf den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit **zweifelhaft** ist (siehe den Beschluss des Bundesrats vom 7. Juli 2017, Bundesrats-Drucksache 450/17, S. 2). Daher wird in der steuerrechtlichen Literatur die Verfassungsmäßigkeit von § 32h AO teilweise sehr kritisch beurteilt.

Wie praktikabel und effektiv eine zentralisierte datenschutzrechtliche Aufsicht über deutschlandweit mehr als 500 Finanzämter im Bereich der Bundessteuern ist, wird die Praxis zeigen. Zur Vermeidung der aufgezeigten Aufsichtsabgrenzungsschwierigkeiten erscheint mir jedenfalls – nicht zuletzt auch im Interesse der betroffenen Steuerbürgerinnen und -bürger – eine gesetzgeberische Lösung als **vorzugswürdig**, welche die bewährte **datenschutzrechtliche Aufsicht „aus einem Guss"** gegenüber allen mit dem Vollzug des Abgabenrechts befassten Landesbehörden beibehält.

10.2 Auskunft über Gewerbesteuerzahler an den Gemeinderat („Gewerbesteuer-Bestenliste")

Die Gewerbesteuer trägt einen nicht unerheblichen Teil zu den Einnahmen der bayerischen Städte, Märkte und Gemeinden bei. Insbesondere die steuerrechtlich eröffnete Option, durch Festlegung des Gewerbesteuer-Hebesatzes auf die „Schüttung" dieser Geldquelle Einfluss nehmen zu können, sorgt dafür, dass die Gewerbesteuer ein immer wieder beliebtes Diskussionsthema in kommunalen Gremien ist.

Viele Mandatsträgerinnen und Mandatsträger sind daher der Auffassung, dass ihnen für informierte Entscheidungen auch die wichtigsten örtlichen Unternehmen sowie deren jeweils mittels der Gewerbesteuer geleisteter Beitrag bekannt sein sollten. Gerade in kreisangehörigen Gemeinden gehören zu den Trägern dieser erfolgreichen Unternehmen oftmals natürliche Personen, die nicht nur das **Steuergeheimnis** gemäß § 30 Abgabenordnung (AO), sondern auch das **Grundrecht auf informationelle Selbstbestimmung** nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz für die Bundesrepublik Deutschland geltend machen können.

Vor diesem Hintergrund ist die in meiner Beratungspraxis immer wieder gestellte Frage, ob kommunale Gremien von der Gemeindeverwaltung eine „Bestenliste" der Gewerbesteuerschuldner, gar unter Nennung von Steuerschuld und Bemessungsgrundlage, erhalten dürfen, auch eine (steuer-)datenschutzrechtliche Frage. In diesem Zusammenhang ist zu bemerken:

Die Offenlegung von Daten über Gewerbesteuerschuldner gegenüber einem Stadt-, Marktgemeinde- oder Gemeinderat ist als „Offenbarung" im Sinne von **§ 30 Abs. 2 Nr. 1 AO** zu werten. Dort heißt es:

„(2) Ein Amtsträger verletzt das Steuergeheimnis, wenn er
1. personenbezogene Daten eines anderen, die ihm
a) in einem Verwaltungsverfahren, einem Rechnungsprüfungsverfahren oder einem gerichtlichen Verfahren in Steuersachen, […]
bekannt geworden sind […]
unbefugt offenbart […]."

Der erste Bürgermeister sowie seine für Steuerangelegenheiten zuständigen Mitarbeiterinnen und Mitarbeiter dürfen Daten über Gewerbesteuerschuldner einem Gremium gegenüber demnach nur offenbaren, wenn sie dazu befugt sind. **An einer solchen Offenbarungsbefugnis fehlt es jedoch für die Mitteilung einer „Gewerbesteuer-Bestenliste".** Im Einzelnen:

– Eine solche Befugnis ergibt sich nicht aus **§ 30 Abs. 4 Nr. 5 AO**. Nach dieser Vorschrift ist eine Offenbarung zulässig, soweit für sie ein zwingendes öffentliches Interesse besteht. Insofern sind auch drei Regelbeispiele vorgesehen:

  „(4) Die Offenbarung oder Verwertung geschützter Daten ist zulässig, soweit […]
  5. für sie ein zwingendes öffentliches Interesse besteht; ein zwingendes öffentliches Interesse ist namentlich gegeben, wenn
  a) die Offenbarung erforderlich ist zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit oder zur Verhütung oder Verfolgung von Verbrechen und vorsätzlichen schweren Vergehen gegen Leib und Leben oder gegen den Staat und seine Einrichtungen,
  b) Wirtschaftsstraftaten verfolgt werden oder verfolgt werden sollen, die nach ihrer Begehungsweise oder wegen des Umfangs des durch sie verursachten Schadens geeignet sind, die wirtschaftliche Ordnung erheblich zu stören oder das Vertrauen der Allgemeinheit auf die Redlichkeit des geschäftlichen Verkehrs oder auf die ordnungsgemäße Arbeit der Behörden und der öffentlichen Einrichtungen erheblich zu erschüttern, oder
  c) die Offenbarung erforderlich ist zur Richtigstellung in der Öffentlichkeit verbreiteter unwahrer Tatsachen, die geeignet sind, das Vertrauen in die Verwaltung erheblich zu erschüttern; […]."

  Das dem kommunalen Gremium nach Art. 30 Abs. 3 Gemeindeordnung für den Freistaat Bayern (GO) zustehende Überwachungsrecht kann ein **zwingendes öffentliches Interesse nicht** begründen, soweit Zugang zu einer „Gewerbesteuer-Bestenliste" begehrt wird.

  Nach Art. 30 Abs. 3 GO überwacht der Gemeinderat die gesamte Gemeindeverwaltung, insbesondere auch die Ausführung seiner Beschlüsse. Das Überwachungsrecht ist mit Art. 56 Abs. 1 GO verknüpft. Nach dieser Bestimmung muss die gemeindliche Verwaltungstätigkeit mit der Verfassung und den Gesetzen im Einklang stehen; sie darf nur von sachlichen Gesichtspunkten geleitet sein.

  Der Gemeinderat wirkt durch Gebrauch des Überwachungsrechts auf eine gesetzmäßige und zweckgerechte Verwaltung der Gemeinde hin. In der Regel wird sich das Überwachungsrecht daher auf **Einzelvorgänge** beziehen, in denen sich Anhaltspunkte für ein Vorgehen der Gemeindeverwaltung ergeben haben, das mit den Gesetzen, mit Richtlinien (siehe Art. 37 Abs. 1 Satz 2 GO) oder Beschlüssen (siehe Art. 30 Abs. 3 GO: „insbesondere auch die Ausführung seiner Beschlüsse") des Gemeinderats nicht vereinbar ist.

Einer Liste von Steuerschuldnern, welche auch die Höhe der Steuerschuld sowie die Bemessungsgrundlage anführen soll, fehlt ein solcher Einzelfallbezug gerade. **Das in Art. 30 Abs. 3 GO normierte Recht ist kein allgemeines gremienbezogenes Informationszugangsrecht, sondern auf die Überwachung der Gemeindeverwaltung hin fokussiert.** Diesen Zusammenhang habe ich bereits in dem Beitrag Nr. 16.2 meines 21. Tätigkeitsberichts 2004 für den Fall einer Datennutzung nach Art. 17 Abs. 1 Nr. 1 BayDSG-alt hervorgehoben.

Im Übrigen muss das von § 30 Abs. 4 Nr. 5 AO geforderte zwingende öffentliche Interesse ein Interesse von einigem Gewicht sein. Insofern kommt es auch auf die Motivation an, die das Gremium mit seinem Zugangsanliegen verfolgt. **Ein allgemeines kommunalpolitisches Erkenntnisinteresse genügt in diesem Zusammenhang nicht** (vergleiche nun auch Oberverwaltungsgericht Nordrhein-Westfalen, Urteil vom 6. November 2018, Az.: 15 A 2638/17, Juris Rn. 78 ff., insbesondere Rn. 92 ff.).

— Auch die im Zuge der Datenschutzreform 2018 neben § 30 Abs. 4 Nr. 5 AO getretene Befugnis nach § 30 Abs. 4 Nr. 1a in Verbindung mit § 29c Abs. 1 Satz 1 Nr. 6 AO deckt die Offenbarung von Gewerbesteuerdaten in einer „Bestenliste“ nicht. **§ 30 Abs. 4 Nr. 1a AO** lautet:

„(4) Die Offenbarung oder Verwertung geschützter Daten ist zulässig, soweit […]
1a. sie einer Verarbeitung durch Finanzbehörden nach Maßgabe des § 29c Absatz 1 Satz 1 Nummer 4 oder 6 dient, […].“

Nach dieser Vorschrift käme zwar grundsätzlich eine Offenbarung zur **Wahrnehmung von Aufsichts- oder Steuerungsbefugnissen innerhalb der Kommune als Finanzbehörde** in Betracht. Voraussetzung wäre hier jedoch im Hinblick auf § 29c Abs. 1 Satz 3, § 30 Abs. 1, 3 AO, dass es sich bei den ehrenamtlichen Stadt-, Marktgemeinderats- oder Gemeinderatsmitgliedern um Personen handelt, die nach § 30 AO zur Wahrung des Steuergeheimnisses verpflichtet sind, also um Amtsträger (§ 30 Abs. 1, § 7 AO) oder für den öffentlichen Dienst besonders Verpflichtete (§ 30 Abs. 3 Nr. 1 AO, § 11 Abs. 1 Nr. 4 Strafgesetzbuch). Das ist aber gerade nicht der Fall (siehe zum Parallelproblem im Strafrecht näher Bundesgerichtshof, Urteil vom 9. Mai 2006, Az.: 5 StR 453/05, BGHSt 51, 44).

Insgesamt sollte eine **„Bestenliste“ der Gewerbesteuerzahler** kommunalen Gremien daher – wenn überhaupt – nur nach sorgfältiger Prüfung bereitgestellt werden. Eine solche Bereitstellung **hat zu unterbleiben**, wenn dort betroffene Personen erscheinen würden, welche den Schutz des Grundrechts auf informationelle Selbstbestimmung oder des unionsrechtlichen Datenschutzgrundrechts geltend machen können.

11 Schulen und Hochschulen

11.1 Umsetzung der Datenschutz-Grundverordnung

Vor dem Hintergrund der ab 25. Mai 2018 anzuwendenden Datenschutz-Grundverordnung (DSGVO) waren im Bereich Schulen und Hochschulen die Normen, die die Verarbeitung personenbezogener Daten in diesen Feldern regeln, an die neue Rechtslage anzugleichen. Zum 25. Mai 2018 wurden das Bayerische Hochschulgesetz (BayHSchG) und das Bayerische Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG) angepasst. Ich habe bereits die Entstehung der Gesetzentwürfe aus datenschutzrechtlicher Sicht begleitet. Die Änderungen in den genannten Gesetzen beschränkten sich zum größten Teil auf terminologische Angleichungen.

Auch im Bereich der Schulen zeigt sich, dass es sich bei der Anpassung an die Datenschutz-Grundverordnung um einen Prozess handelt, der nicht am 25. Mai 2018 abgeschlossen ist. So sind auch untergesetzliche Normen und Verwaltungsvorschriften mit Blick auf die Datenschutz-Grundverordnung zu überarbeiten. Dies gilt etwa für die Bayerische Schulordnung (BaySchO) und die Verordnung zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes (Durchführungsverordnung). Besonders letzteres stellt eine Herausforderung dar, da diese Verordnung einerseits zentrale Bedeutung für die praxisgerechte Anwendung der datenschutzrechtlichen Vorgaben im Schulbereich hatte, andererseits Anknüpfungspunkte (datenschutzrechtliche Freigabe, Führung des Verfahrensverzeichnisses) nach dem Bayerischen Datenschutzgesetz in der bis zum 24. Mai 2018 geltenden Fassung durch die Datenschutz-Grundverordnung weggefallen sind.

Neben diesen legislatorischen Akten mussten auch Materialien an die Vorgaben der Datenschutz-Grundverordnung angepasst oder weiterentwickelt werden. Auch in diesem Zusammenhang arbeite ich intensiv mit dem Bayerischen Staatsministerium für Unterricht und Kultus zusammen. So habe ich das Kultusministerium bei der Überarbeitung der Musterformulare zur Einholung der Einwilligung in die Veröffentlichung von personenbezogenen Daten (einschließlich Fotos) – den sogenannten Muster-Einwilligungserklärungen – beraten und unterstützt. Auch in die Überarbeitung der „Erläuternden Hinweise für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes“ durch das Kultusministerium werde ich eingebunden.

Des Weiteren ist auch die Erstellung von Informationsmaterial als Hilfestellung zur Umsetzung der datenschutzrechtlichen Pflichten in den Schulen ein wichtiger Baustein. Das Kultusministerium stellt etwa ein Muster speziell für Schulen zur Erfüllung ihrer Informationspflichten nach Art. 13 Abs. 1 und 2 DSGVO zur Verfügung. Auch hier konnte ich wesentliche datenschutzrechtliche Positionen geltend machen.

Insgesamt zielt meine Beratung auf datenschutzfreundliche Lösungen, die auch praxistauglich umgesetzt werden können.

11.2 Einsatz digitaler Lernmittel (Arbeitshefte mit digitalen Zusatzübungen und digitale Schulbücher)

Im Berichtszeitraum war ich mit einer weiteren Facette der Digitalisierung in Schulen, nämlich dem Einsatz digitaler Lernmittel (Arbeitshefte mit digitalen Zusatzübungen und digitale Schulbücher), befasst. Sowohl Schulen als auch Schulbuchverlage wollen die neuen Möglichkeiten der Gestaltung von Lern- und Übungsprozessen, die die Digitalisierung bietet, nutzen. Mittelfristig soll hier eine zentrale Plattformlösung erarbeitet werden. Bis eine solche zentrale Lösung verwirklicht ist, hat das Bayerische Staatsministerium für Unterricht und Kultus in enger Abstimmung mit mir eine datenschutzkonforme Zwischenlösung erarbeitet. Sie beruht auf einer bedingten Zulassung digitaler Lernmittel durch das Kultusministerium, einer Einwilligung der Erziehungsberechtigten der Schülerinnen und Schüler (gegenüber den Verlagen und der Schule) sowie einer Selbstverpflichtung der Schulbuchverlage. Diese Selbstverpflichtung zielt darauf, die Einhaltung der datenschutzrechtlichen Vorgaben und die Wahrung der Datenschutzrechte der Schülerinnen und Schüler sowie der Erziehungsberechtigten sicherzustellen. In diesem Zusammenhang wurde auch ein mit mir abgestimmter Musterbrief an die Erziehungsberechtigte entworfen, der über die Zwischenlösung informiert und auch eine Muster-Einwilligungserklärung der Erziehungsberechtigten zum Einsatz digitaler Lernmittel in der Schule enthält.

Das Kultusministerium wirkt im Rahmen der mit den Schulbuchverlagen geschlossenen (Lizenz-)Vereinbarungen darauf hin, dass die Schulbuchverlage eine mit mir konsentierte Selbstverpflichtung zum datenschutzkonformen Umgang mit den personenbezogenen Daten der Schülerinnen und Schüler sowie der Erziehungsberechtigten gegenüber dem Kultusministerium abgeben.

Darin verpflichten sich die Verlage, die Daten einer Schülerin beziehungsweise eines Schülers

- der Schule nicht ohne Einwilligung eines Erziehungsberechtigten zugänglich zu machen,
- nur im Verhältnis zu der Schülerin oder dem Schüler zu nutzen,
- nicht an Dritte weiterzugeben, es sei denn, es besteht eine gesetzliche Verpflichtung,
- nicht zu Werbezwecken zu nutzen und
- ausschließlich auf verlagseigenen, gesicherten Servern innerhalb des EU/EWR-Bereichs zu verarbeiten.

Ferner verpflichten sich die Verlage,

- der Schülerin, dem Schüler und den Erziehungsberechtigten jederzeit Auskunft über die jeweils gespeicherten Daten zu erteilen,
- angelegte Profile und/oder darin abgelegte Daten, insbesondere Aufgabenbearbeitungen und Lernstände, auf Anforderung jederzeit unverzüglich zu löschen und

– angelegte Profile und/oder darin abgelegte Daten jedenfalls unaufgefordert zum Ende eines Schuljahres zu löschen, soweit mit der Schülerin, dem Schüler oder den Erziehungsberechtigten nichts anderes vereinbart ist.

Im Hinblick auf die Erklärung der Einwilligung gegenüber dem Schulbuchverlag ist zu differenzieren:

Bei digitalen Lernmitteln, die keine Lernstandsdatenspeicherung (Speicherung der von den Schulkindern eingetragenen Lösungen) vorsehen und bei denen die Schulkinder mittels eines im Lernmittel enthaltenen Codes über eine Webseite des Verlags zu den Übungen gelangen können, ist keine Registrierung und keine gesonderte Einwilligung der Erziehungsberechtigten des jeweiligen Schulkinds nötig.

Bei digitalen Lernmitteln, die eine Lernstandsdatenspeicherung vorsehen oder die individuelle Hervorhebungen, Unterstreichungen oder Notizen ermöglichen, ist hingegen eine Registrierung auf der Homepage des Verlags erforderlich. Hierzu muss eine private E-Mail-Adresse angegeben werden, die jedoch keinen Hinweis auf den Namen von Schülerinnen, Schülern oder Erziehungsberechtigten enthalten muss. Zudem bedarf es insofern einer Einwilligung gegenüber dem Verlag in dessen Datenschutzbestimmungen.

Daneben ist in jedem Fall (gegebenenfalls zusätzlich) eine gesonderte Einwilligung gegenüber der Schule zum Einsatz digitaler Lernmittel im Unterricht nötig. Zur Einholung dieser Einwilligung haben die Schulen auf die Muster-Einwilligungserklärung des Muster-Erziehungsberechtigten-Briefs zurückzugreifen.

Diese Lösung stellt sicher, dass digitale Lernmittel im Unterricht nur eingesetzt werden können, wenn **für alle Schülerinnen und Schüler einer Klasse oder Lerngruppe** die dargestellten Voraussetzungen erfüllt sind.

11.3 Unterrichtsvideografie durch Universitäten zur Lehrerausbildung

Zum Thema Videoaufnahmen im Schulunterricht habe ich mich bereits in meinem 27. Tätigkeitsbericht 2016 unter Nr. 10.3 ausführlich geäußert. Dabei bin ich unter anderem auch auf die datenschutzrechtliche Zulässigkeit von Videoaufnahmen angehender Lehrerinnen und Lehrern durch die jeweilige Schule selbst zum Zweck der schulinternen Fortbildung eingegangen. Unter den im genannten Beitrag dargelegten Vorgaben können – in einem moderaten Umfang – Videoaufnahmen von Unterrichtseinheiten nach Art. 85 Abs. 1 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG) zulässig sein.

11.3.1 Sachverhalt

Im Berichtszeitraum war ich mit einem anderen Phänomen von Bild- und Tonaufzeichnungen in Schulklassen konfrontiert: der Unterrichtsvideografie zur Lehrerausbildung, aber nicht durch die Schule selbst, sondern durch Universitäten. Im Rahmen von Förderprojekten zur Verbesserung der Lehrerausbildung sehen verschiedene Universitäten zunehmend Bedarf, von Unterrichtsstunden in Schulen Bild- und Tonaufnahmen aufzunehmen und zur Lehre (und Forschung) einzusetzen.

In einem von mir beurteilten Fall wurden an mehreren öffentlichen Schulen spezielle Klassenzimmer eingerichtet. Eine bayerische Universität stattete in den Schulen Klassenräume technisch mit Kameras und Deckenmikrofonen aus, sodass das Unterrichtsgeschehen sowohl zeitgleich in einem Nebenraum beobachtet als auch für eine zeitversetzte Auswertung aufgenommen werden kann. In dem Nebenraum können Ausbilderinnen und Ausbilder mit ihren Studierenden das Unterrichtsgeschehen „live" verfolgen und im Anschluss einzelne Abschnitte anhand der angefertigten Aufzeichnung nachbesprechen. Die Nutzung der Aufzeichnung erfolgt dabei nur an der Schule selbst.

11.3.2 Rechtliche Bewertung

Unabhängig von der schulrechtlichen Zulässigkeit (vergleiche § 24 Bayerische Schulordnung) ist für die beschriebene Unterrichtsvideografie durch Universitäten zur Lehrerausbildung datenschutzrechtlich Folgendes zu beachten:

Zunächst sind mehrere Verarbeitungen personenbezogener Daten zu differenzieren. So ist – **erstens** – die **Datenerhebung** durch Videobeobachtung und -aufzeichnung der Schule zuzurechnen und zwar unabhängig von den Eigentumsverhältnissen an den technischen Aufzeichnungsgeräten und auch dann, wenn die beobachtenden Personen allein Angehörige der Universität und nicht etwa der Schule zugewiesene Referendarinnen und Referendare sind. Dies gilt jedenfalls dann, wenn die Videobeobachtung und -aufzeichnung überwiegend während des (Pflicht)Unterrichts und auf dem Gelände der Schule stattfindet. Dies hat zur Folge, dass – **zweitens** – eine weitere Datenverarbeitung durch **Übermittlung** von der Schule an die Universität, nämlich durch Überlassung der Aufzeichnungen an die Universität in den Schulräumen, vorliegt. **Drittens** stellt auch die **Nutzung** der Videoaufzeichnungen durch die Universität, etwa durch Abspielen oder durch Bearbeitung des Videomaterials, eine eigenständige Datenverarbeitung durch diese dar.

Für jeden dieser Verarbeitungsvorgänge benötigen die Schule und die Universität je eine entsprechende **Rechtsgrundlage** (vergleiche Art. 6 Abs. 1 DSGVO). Eine solche kann sich – mangels gesetzlicher Verarbeitungsbefugnis – nur aus der **wirksamen Einwilligung** aller von der Videografie betroffenen Personen ergeben: also aus der Einwilligung der aufgenommenen unterrichtenden Lehrkraft, der volljährigen Schülerinnen und Schüler sowie bei Minderjährigen der Einwilligung der Erziehungsberechtigten der aufgenommenen Schulkinder und ab dem 14. Geburtstag zusätzlich der Schülerin respektive des Schülers (Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 7 DSGVO).

Zentrale Bedingungen für die Wirksamkeit der Einwilligung sind insbesondere die **Informiertheit** des Einwilligenden (Art. 4 Nr. 11, Art. 7 Abs. 2 Satz 1, Abs. 3 Satz 3 DSGVO) und die **Freiwilligkeit**. Ein Formular, mit dem die Einwilligung eingeholt wird, ist entsprechend zu gestalten. Aus Gründen der Praktikabilität ist es durchaus möglich, dass Schule und Universität ein gemeinsames Formular für die Einwilligung nutzen. Allerdings muss in dem Formular und dem beigefügten Informationsschreiben an die Erziehungsberechtigten, Lehrkräfte sowie Schülerinnen und Schüler klar und deutlich hervorgehoben werden, dass

— Urheber des Formblatts Schule **und** Universität sind;

– für die oben genannten verschiedenen Datenverarbeitungen der Schule und der Universität eine Einwilligung eingeholt wird;

– eine Teilnahme an der Erhebung freiwillig ist und die Einwilligung voraussetzt;

– Stillschweigen keine Einwilligung darstellt, sondern die Nichtabgabe des Einwilligungsformulars als Verweigerung der Einwilligung gilt. Hierüber ist insbesondere dann aufzuklären, wenn das Einwilligungsformular auch ein Ankreuzfeld für die ausdrückliche Verweigerung der Einwilligung enthält;

– die beschriebenen Video- und Audioaufzeichnungen nur dann stattfinden, wenn alle davon betroffenen Personen (Schülerin oder Schüler beziehungsweise deren Erziehungsberechtigte sowie die unterrichtende Lehrkraft) eingewilligt haben.

Des Weiteren sind die Erziehungsberechtigten und gegebenenfalls die einwilligenden Schülerinnen und Schüler anschaulich über die Folgen eines Widerrufs aufzuklären (Art. 7 Abs. 3 DSGVO) sowie über den Zweck und die Speicherdauer zu informieren.

Ferner ist klarzustellen, ob sich die Einwilligung auf eine konkrete Unterrichtsstunde beziehungsweise ein konkretes Einzelprojekt bezieht oder mehrere Unterrichtseinheiten erfassen soll. Wenn die Einwilligung über einen längeren Zeitraum gültig sein soll, so stellt das Schuljahr grundsätzlich den maximalen Zeitrahmen dar. Spätestens zum neuen Schuljahr wären die Einwilligungen neu einzuholen.

Zur Gewährleistung der Freiwilligkeit ist insbesondere darauf zu achten, dass weder durch bestimmte Formulierungen im Informationsschreiben beziehungsweise im Einwilligungsformular noch durch sonstige soziale Maßnahmen (Gruppen-)Druck erzeugt wird, der eine echte und freie Wahl verhindert.

Unzulässig, da diskriminierend und einer freiwilligen Entscheidung entgegenstehend, ist es, wenn ein Schulkind als Konsequenz einer Nichteinwilligung für die Dauer der aufgenommenen Unterrichtsstunde in eine Parallelklasse versetzt wird.

Allenfalls zulässig kann es sein, wenn ein Schulkind, für das eine Einwilligung in Videoaufnahmen nicht vorliegt, während der aufgezeichneten Unterrichtsstunde an einen Ort im Klassenzimmer gesetzt wird, der außerhalb des Erfassungsbereichs der Kamera liegt. Allerdings setzt diese Lösung voraus, dass das betroffene Kind ohne weitere Einschränkungen am aufgezeichneten Unterricht teilnehmen kann. In diesem Fall ist zwingend die Einholung der Einwilligung der Erziehungsberechtigten und gegebenenfalls zusätzlich des (mindestens) vierzehnjährigen Kindes notwendig, dass Audioaufnahmen aufgezeichnet werden dürfen („kleine Einwilligungslösung“). Zudem muss auch insofern sichergestellt sein, dass dennoch nicht vermeidbare gelegentliche Aufnahmen dieses Kindes (etwa auf dem Weg durch den Klassenraum zur Toilette) anonymisiert („verpixelt“) werden. Auch für diese Form der Datenverarbeitung ist die Einholung einer Einwilligung obligatorisch.

Auch wenn eine Video- und Tonaufzeichnung nach den dargelegten Vorgaben zulässig sein sollte, ist darauf zu achten, dass die Unterrichtsvideografie nicht zum Regelfall werden darf. In meinem 27. Tätigkeitsbericht 2016 habe ich unter

Nr. 10.3.1 hervorgehoben, dass grundsätzlich nur **gelegentliche** Videoaufzeichnungen im Unterricht aus Datenschutzsicht akzeptabel sind. Daher muss bereits das von der Universität verfolgte Konzept zur Unterrichtsvideografie so ausgelegt sein, dass eine Belastung der einzelnen Schulklasse nur einen geringen Anteil der Unterrichtszeit erreicht. So wäre zum Beispiel die Aufzeichnung von ein bis zwei Stunden pro Woche in einer Klasse bereits deutlich zu hoch.

Die Video- und Tonaufzeichnungen sind umgehend zu löschen, sobald sie zur Erfüllung ihres Zwecks (Lehrerausbildung) nicht mehr erforderlich sind (Art. 17 Abs. 1 Buchst. a DSGVO). Wenn sie gespeichert werden, sind die allgemeinen technisch-organisatorischen Vorgaben zur Wahrung des Datenschutzes zu beachten. Insbesondere muss der Zugang zu dem PC, auf dem die Aufzeichnungen gespeichert und auf dem die zur Herstellung und Nutzung nötigen Anwendungen aufgespielt sind, mittels personengebundener Kennwörter und regelmäßig zu wechselnder Passwörter gesichert sein. Der Nebenraum mit der technischen Ausrüstung ist verschlossen zu halten. Zudem ist ein Zugriffsrollenkonzept auszuarbeiten, das sich streng am Prinzip der Erforderlichkeit orientiert. Zugriff zum Nebenraum, zu den technischen Geräten und zu gespeicherten Aufzeichnungen darf nur erhalten, wer dies zur Erfüllung seiner Aufgaben benötigt. Diese Aufgaben müssen sich im Rahmen des durch die Einwilligung konsentierten Zwecks halten. Die Schulleitung als Vertretung des Verantwortlichen hat dies durch entsprechende datenschutzrechtliche Belehrungen, durch Einholung schriftlicher Zusicherungen und durch Kontrollen (Stichproben) sicherzustellen.

11.3.3 Vorgehen und Ausblick

Im untersuchten Fall konnte ich durch intensiven Austausch mit dem Bayerischen Staatsministerium für Unterricht und Kultus und der Universität erreichen, dass die verwendeten Einwilligungsformulare und Informationsschreiben an die dargestellten Vorgaben angepasst wurden. Allerdings stellt die hier bewertete Ausgestaltung der Unterrichtsvideografie durch Universitäten zur Lehrerausbildung nur eine Variante dar. Weitere datenschutzrechtliche Fragen stellen sich etwa, wenn die Unterrichtsvideografie durch Universitäten dazu verwendet wird, eine Falldatenbank zu erstellen, die dann im Rahmen der universitären Ausbildung von Lehrkräften genutzt wird. Auch diese besondere Art der Datenverarbeitung ist nur aufgrund einer wirksamen Einwilligung aller Betroffenen möglich. Besondere Herausforderungen stellen sich insoweit im Hinblick auf die zulässige Speicherdauer der in der Falldatenbank aufgenommenen Video- und Audio-Dateien. Auch insoweit arbeite ich mit dem Bayerischen Staatsministerium für Unterricht und Kultus sowie dem Bayerischen Staatsministerium für Wissenschaft und Kunst und den beteiligten Schulen und Hochschulen an einer datenschutzkonformen und praxisgerechten Lösung.

11.4 Datenschutz beim Online-Kartenvorverkauf öffentlicher Theater

11.4.1 Sachverhalt

Im Berichtszeitraum erreichte mich die Eingabe eines Bürgers, mit welcher sich dieser gegen eine Datenverarbeitung im Rahmen des Online-Kartenvorverkaufs eines öffentlichen Theaters wendete. Der Bürger rügte, dass kein „anonymer“ Kauf vorgenommen werden könne, sondern nicht benötigte personenbezogene

Daten wie Name, Kontaktdaten und Bankdaten angegeben werden müssten. Zudem würden die Daten länger gespeichert werden als es erforderlich wäre.

Das Theater teilte mir auf Nachfrage unter anderem mit, dass eine „anonyme" Kartenbestellung unter Nutzung bargeldloser Zahlungsinstrumente (Bankeinzug, Kreditkarte) aufgrund der besonderen Risikolage bei der rechtsgeschäftlichen Abwicklung des Erwerbs von Teilnahmeberechtigungen elektronisch – anders als beim Schalterverkauf – nicht möglich sei. Im Fall des Online-Kartenvorverkaufs sei nach den Benutzungsbedingungen „Jede [so ausdrücklich] Bestellung von Eintrittskarten [...] unmittelbar nach Bestätigung durch den Zentralen Kartenverkauf bindend und verpflichtet gemäß den bestehenden Regelungen zur Abnahme und Bezahlung der bestellten Karten." Daher müsse der Kunde zum Online-Kartenvorverkauf ein Kundenkonto anlegen.

11.4.2 Rechtslage

Nach eingehender Prüfung stellt sich die Rechtslage aus Datenschutzsicht wie folgt dar:

— Öffentliche Stellen benötigen für die Verarbeitung von personenbezogenen Daten eine Rechtsgrundlage (vgl. Art. 6 Abs. 1 DSGVO). Beim Verkauf von Teilnahmeberechtigungen (Eintrittskarten) kommt als Rechtsgrundlage insbesondere die allgemeine Verarbeitungsbefugnis aus Art. 4 Abs. 1 BayDSG in Betracht. Danach ist die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle zulässig, wenn sie zur Erfüllung einer ihr obliegenden Aufgabe erforderlich ist. Aufgabe des Theaters ist es auch, den Kartenvorverkauf für die Veranstaltungen durchzuführen und abzuwickeln. Beim (Bar-)Kauf einer Karte an der Tages- oder Abendkasse kommt es zum sofortigen Austausch „Geld gegen Eintrittskarte". Insoweit ist eine Verarbeitung von personenbezogenen Daten nicht erforderlich. Da bei einem Online-Kartenvorverkauf – je nach Art des bargeldlosen Zahlungsmittels – ein sofortiger Leistungsaustausch unterbleibt, vielmehr das Entgelt gegebenenfalls zeitlich nachgelagert entrichtet wird, ist hier eine Erhebung von zur Zahlungsabwicklung und zur Identifizierung und Kommunikation mit dem Kunden benötigten personenbezogenen Daten (wie etwa Name, Anschrift, E-Mail-Adresse und Bankverbindungsdaten) erforderlich, um das Rechtsgeschäft überhaupt durchführen und beim Scheitern des elektronischen Zahlungsvorgangs Rückgriff nehmen zu können. Die Erhebung des Datensatzes kann auch im Rahmen der Einrichtung eines Kundenkontos für den Bestell- und Bezahlvorgang erfolgen.

— Sobald feststeht, dass die bestellte Eintrittskarte bezahlt und die Veranstaltung durchgeführt ist, ist die weitere Speicherung des Datensatzes, einschließlich eines allein (siehe aber auch unten letzter Aufzählungsstrich) zur Durchführung des Zahlungsvorgangs automatisch oder zwingend angelegten Kundenkontos, für den Zweck der Abwicklung des Rechtsgeschäfts „Kartenverkauf" nicht mehr erforderlich; er ist daher zu löschen (vgl. Art. 17 Abs. 1 Buchst. a DSGVO). Soweit personenbezogene Daten (zum Beispiel Rechnungsdatensätze) zu einem anderen Zweck, etwa zur Erfüllung haushaltrechtlicher Aufbewahrungsfristen, gespeichert werden müssen, sind diese Daten gesondert aufzubewahren. Das heißt, sie müssen jedenfalls so zugriffsgesichert sein, dass eine Nutzung im laufenden Geschäftsbetrieb nicht mehr möglich ist.

— Um das informationelle Selbstbestimmungsrecht der Kunden zu wahren, muss es neben einer personalisierten Kartenvorkaufsmöglichkeit, wie eben für den Online-Vorverkauf beschrieben, auch eine alternative „anonyme“ Kaufmöglichkeit geben. Dies ist etwa beim Barkauf an der Tages- und Abendkasse der Fall. Über diese Möglichkeit ist klar und deutlich in der allgemeinen Datenschutzerklärung und auf der Online-Bestellplattform beziehungsweise im Rahmen der Online-Anmeldung des Kundenkontos hinzuweisen.

— Wenn aus Service-Gründen – etwa um zukünftige Online-Kartenkäufe zu erleichtern – die Führung eines dauerhaften (also über den einzelnen Zahlungsvorgang hinaus bestehenden) Kundenkontos mit den für die Abwicklung des Bestell- und Zahlungsvorgangs erhobenen Daten angeboten wird, ist dies nur aufgrund einer wirksamen Einwilligung (Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 7 DSGVO) zulässig. In einer Online-Umgebung bietet sich insoweit ein entsprechendes Opt-In-Kästchen an. Für die Bereithaltung von Bankverbindungsdaten im Rahmen eines Kundenkontos über den konkreten Geschäftsvorfall und dessen Dokumentation hinaus halte ich eine (zusätzliche und ausdrückliche) Einwilligung für erforderlich. Auch diese kann – etwa auf der Bestellplattform – abgefragt werden.

11.4.3 Vorgehen

Das System des Online-Kartenvorverkaufs des öffentlichen Theaters genügte diesen Vorgaben nicht in vollem Umfang. Ich habe bereits einige Verbesserungen erreichen können und weitere Optimierungen empfohlen. Da hierzu die Implementierung von weiteren Funktionalitäten in die verwendete Software notwendig ist, ist das Theater auf die Kooperation des Softwareanbieters angewiesen. Allerdings weise ich in diesem Zusammenhang auf den – im Rechtsstaat selbstverständlichen – Grundsatz hin, dass die Anforderungen an die technische Datenverarbeitung dem Datenschutzrecht zu folgen haben und nicht umgekehrt. Vor diesem Hintergrund werde ich weiterhin darauf drängen, dass die dargestellten Vorgaben zeitnah umgesetzt werden.

12 Personalwesen

12.1 Novellierung des Personalaktenrechts im Bayerischen Beamtengesetz

Personalakten enthalten eine Vielzahl an personenbezogenen Daten der betroffenen Beschäftigten. Diese Daten sind teils sehr sensibler Natur: So finden sich in Personalakten oftmals auch Daten, welche die Gesundheit der Beschäftigten betreffen oder deren Gewerkschafts- oder Religionszugehörigkeit erkennen lassen. Das Personalaktenrecht trägt dieser **besonderen Schutzbedürftigkeit** von Personalaktendaten durch detaillierte gesetzliche Vorgaben zum Umgang mit Personalakten Rechnung. Die für bayerische Beamtinnen und Beamte insoweit einschlägigen Regelungen sind – neben § 50 Beamtenstatusgesetz (BeamtStG) – insbesondere im Abschnitt 8 „Personalakten und Einsatz automatisierter Verfahren" des Bayerischen Beamtengesetzes (BayBG) normiert.

§ 50 BeamtStG
Personalakte
Für jede Beamtin und jeden Beamten ist eine Personalakte zu führen. Zur Personalakte gehören alle Unterlagen, die die Beamtin oder den Beamten betreffen, soweit sie mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten). Die Personalakte ist vertraulich zu behandeln. Personalaktendaten dürfen nur für Zwecke der Personalverwaltung oder Personalwirtschaft verwendet werden, es sei denn, die Beamtin oder der Beamte willigt in die anderweitige Verwendung ein. Für Ausnahmefälle kann landesrechtlich eine von Satz 4 abweichende Verwendung vorgesehen werden.

Auch wenn diese Regelungen unmittelbar nur für bayerische Beamtinnen und Beamte gelten, sind sie als allgemein gültige **Schutzprinzipien für alle öffentlichen Bediensteten** grundsätzlich auch auf die nicht-verbeamteten Beschäftigten des bayerischen öffentlichen Dienstes, insbesondere auf Tarifbeschäftigte, entsprechend anzuwenden.

Im Zuge der Anpassung des bayerischen Landesrechts an die Datenschutz-Grundverordnung (DSGVO) ist mit dem „Gesetz zur Änderung personalaktenrechtlicher und weiterer dienstrechtlicher Vorschriften" vom 18. Mai 2018 (GVBl. S. 286) eine **Novellierung des Personalaktenrechts** im Bayerischen Beamtengesetz erfolgt. Das diesbezügliche Gesetzgebungsverfahren habe ich intensiv begleitet.

12.1.1 Anlass und Umfang der Novellierung

Der Anwendungsbereich der Datenschutz-Grundverordnung umfasst grundsätzlich auch personenbezogene Daten in Personalakten, und zwar unabhängig davon, ob diese Akten in Papier- oder in elektronischer Form geführt werden (siehe Art. 2 Abs. 1 DSGVO, vgl. auch Art. 2 BayDSG). Aufgrund ihrer unmittelbaren Geltung genießt die Datenschutz-Grundverordnung Anwendungsvorrang gegenüber dem nationalen Recht.

Der Freistaat Bayern war daher verpflichtet, sein Recht an die Datenschutz-Grundverordnung anzupassen. Im Hinblick auf die sogenannten „Öffnungsklauseln“ in Art. 6 Abs. 2 und 3 DSGVO sowie in Art. 88 DSGVO bestand dabei für ihn – wie für jeden nationalen Gesetzgeber – im Bereich des öffentlichen Dienst- und Arbeitsrechts ein gewisser Umsetzungsspielraum. Ein erheblicher Teil der bisherigen personalaktenrechtlichen Vorgaben im Bayerischen Beamtengesetz konnte daher im Wesentlichen beibehalten werden. Änderungen waren jedoch insbesondere in begrifflicher Hinsicht erforderlich.

Die danach erforderliche Anpassung des Personalaktenrechts im Bayerischen Beamtengesetz wurde zudem für Änderungen genutzt, welche nicht durch das neue europäische Datenschutzrecht veranlasst waren:

— Eine ursprünglich beabsichtigte Änderung sah dabei eine Verlängerung der Aufbewahrungsfrist für Beihilfeunterlagen auf zehn Jahre vor. Begründet wurde diese erhebliche Fristverlängerung mit dem Anliegen, Fälle des Beihilfemissbrauchs besser erkennen und verfolgen zu können.

  Auch wenn ich dieses Anliegen im Grundsatz nachvollziehen kann, bin ich der beabsichtigten Verlängerung der Aufbewahrungsfrist für Beihilfeunterlagen entschieden entgegengetreten:

  Beihilfeunterlagen, aus denen die Art der Erkrankung ersichtlich ist, sind in höchstem Maße sensibel. Die Verlängerung der Aufbewahrungsdauer für diese Unterlagen auf zehn Jahre hätte – jedenfalls im staatlichen Bereich – im Ergebnis zum Aufbau einer aussagekräftigen Gesundheitsdatenbank über alle aktiven und ehemaligen bayerischen Beamtinnen und Beamten sowie deren bei der Beihilfe berücksichtigungsfähigen Angehörigen geführt. Da auf der anderen Seite ein nennenswerter Umfang tatsächlichen Beihilfemissbrauchs lediglich spekulativ angenommen, aber nicht einmal im Ansatz belegt werden konnte, habe ich für einen solch intensiven Grundrechtseingriff keine belastbare Grundlage erkennen können. Auf meine Intervention hin hat die Staatsregierung von diesem Vorhaben letztlich Abstand genommen.

— Weitere Änderungen, etwa zur elektronischen Personalakte oder zur Auftragsverarbeitung von Personalaktendaten, konnten demgegenüber (in modifizierter Form) umgesetzt werden.

12.1.2 Regelungssystematik

Neben § 50 BeamtStG finden sich Vorschriften zum Personalaktenrecht – wie bislang – in Teil 4 Abschnitt 8 Bayerisches Beamtengesetz. Der Abschnitt „Personalakten und Einsatz automatisierter Verfahren“ hat nun drei Unterabschnitte: „Verarbeitung personenbezogener Daten“ (Art. 103 BayBG), „Personalakten“ (Art. 104 bis 110 BayBG) und „Einsatz automatisierter Verfahren“ (Art. 111 BayBG).

12.1.3 „Generalklausel“ für die Verarbeitung personenbezogener Daten (Art. 103 BayBG)

Bislang ergab sich aus **Art. 102** Bayerisches Beamtengesetz in der bis zum 24. Mai 2018 geltenden Fassung (**BayBG-alt**) die **Befugnis** zur **Erhebung** personenbezogener Daten von aktiven und ehemaligen Beamtinnen und Beamten sowie von Bewerberinnen und Bewerbern. Art. 103 BayBG-alt regelte den Zugang zur Personalakte und sah insoweit eine in personeller und sachlicher Hinsicht „doppelte Zugangsbeschränkung“ vor.

Der Regelungsgehalt dieser beiden Vorschriften wurde nun – unter Aufhebung des bisherigen Art. 102 BayBG-alt – im neuen Art. 103 BayBG zusammengeführt und zugleich erweitert. **Art. 103 BayBG** regelt nun die **„Verarbeitung personenbezogener Daten“** insgesamt. Der Regelung liegt dabei der **umfassende Verarbeitungsbegriff** von Art. 4 Nr. 2 DSGVO zugrunde. „Verarbeitung“ in diesem Sinne umfasst jeden Vorgang im Zusammenhang mit personenbezogenen Daten, etwa das Erheben, die Speicherung, die Offenlegung oder das Löschen.

Art. 103 BayBG
Verarbeitung personenbezogener Daten
[1]Der Dienstherr darf personenbezogene Daten über Bewerber und Bewerberinnen sowie aktive und ehemalige Beamte und Beamtinnen verarbeiten, soweit dies
1. zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere zu Zwecken der Personalverwaltung oder Personalwirtschaft erforderlich ist,
2. zusätzlich bei der Verarbeitung besonderer Kategorien personenbezogener Daten Art. 8 Abs. 1 Nr. 2, 3 und 5 sowie Abs. 2 des Bayerischen Datenschutzgesetzes (BayDSG) erlaubt
und nachfolgend nichts anderes bestimmt ist. [2]Die Verarbeitung darf nur durch Beschäftigte erfolgen, die vom Dienstherrn mit der Bearbeitung von Personalangelegenheiten betraut sind. 3Unbeschadet der Sätze 1 und 2 dürfen Daten nach Satz 1 auch zu Zwecken der Rechnungsprüfung verarbeitet werden.

Die bisherige „doppelte Zugangsbeschränkung“ wurde erweitert zu einer **„doppelten Zulässigkeitsbeschränkung“** (vgl. Landtags-Drucksache 17/20990, S. 23), welche im Grundsatz für jede Verarbeitung personenbezogener Daten von aktiven und ehemaligen Beamtinnen und Beamten sowie von Bewerberinnen und Bewerbern gilt. Die Verarbeitung darf demnach grundsätzlich nur zu den in Art. 103 Satz 1 Nr. 1 BayBG **genannten Zwecken** und gemäß Art. 103 Satz 2 BayBG **nur durch Beschäftigte** erfolgen, die vom Dienstherrn **mit der Bearbeitung von Personalangelegenheiten betraut** sind. Unbeschadet dessen ist allerdings auch eine Verarbeitung zum **Zwecke der Rechnungsprüfung** zulässig (Art. 103 Satz 3 BayBG). Für eine Verarbeitung „**besonderer Kategorien** personenbezogener Daten“ im Sinne des Art. 9 Abs. 1 DSGVO (dies betrifft zum Beispiel Gesundheitsdaten) muss **zusätzlich** noch einer der in Art. 103 Satz 1 Nr. 2 BayBG genannten Tatbestände des Art. 8 Abs. 1 BayDSG erfüllt sein. Weiterhin sind die Anforderungen von Art. 8 Abs. 2 BayDSG zu beachten.

Die generalklauselartige Verarbeitungsbefugnis in Art. 103 Satz 1 BayBG **gilt** gemäß Art. 103 Satz 1 BayBG allerdings **nur**, soweit „nachfolgend nichts anderes bestimmt ist“. Soweit ein Verarbeitungsvorgang also von einer **spezielleren Regelung der Art. 104 ff. BayBG** erfasst wird, kommt Art. 103 BayBG nicht zur Anwendung. Insbesondere richtet sich die Übermittlung von Personalakten nicht nach Art. 103 BayBG, sondern nach Art. 108 BayBG.

12.1.4 Elektronische Personalakte (Art. 104 Abs. 2 BayBG)

Entsprechend der bisherigen Rechtslage kann eine Personalakte entweder vollständig oder – als nunmehr legaldefinierte – „Hybridakte" lediglich in Teilen **elektronisch geführt** werden (Art. 104 Abs. 2 Satz 1 BayBG). Bei Führung einer Hybridakte ist im Verzeichnis nach Art. 104 Abs. 1 Satz 4 BayBG anzugeben, welche Aktenteile in welcher Form geführt werden (Art. 104 Abs. 2 Satz 5 BayBG); **unzulässig** ist auch weiterhin eine parallele Aktenführung, bei der identische Aktenteile sowohl in Papier- als auch in elektronischer Form vorliegen (vgl. Landtags-Drucksache 17/20990, S. 24). Auch für elektronische Personalakten gelten die **Art. 105 ff. BayBG unmittelbar**. Gemäß Art. 104 Abs. 2 Satz 4 BayBG ist entsprechend dem Stand der Technik sicherzustellen, dass die elektronischen Dokumente mit den Papierdokumenten bildlich und inhaltlich übereinstimmen, wenn sie lesbar gemacht werden.

Art. 104 BayBG
Führung der Personalakte
(2) [1]Die Personalakte kann in Teilen (Hybridakte) oder vollständig elektronisch geführt werden. [2]Gehen elektronische Unterlagen auf die Erfassung papiergebundener Unterlagen zurück, darf auch die ursprüngliche Papierfassung gesondert zu Beweiszwecken aufbewahrt werden. [3]Im Übrigen gelten für die Papierfassung die personalaktenrechtlichen Vorschriften entsprechend. [4]Bei der Erfassung ist entsprechend dem Stand der Technik sicherzustellen, dass die elektronischen Dokumente mit den Papierdokumenten bildlich und inhaltlich übereinstimmen, wenn sie lesbar gemacht werden. [5]Bei Hybridakten ist im Verzeichnis nach Abs. 1 Satz 4 anzugeben, welche Aktenteile in welcher Form geführt werden.

In Anbetracht des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) bewerte ich die Regelung des neuen Art. 104 Abs. 2 Satz 2 BayBG **kritisch**: Gehen elektronische Unterlagen auf die Erfassung papiergebundener Unterlagen zurück, darf hiernach auch die **ursprüngliche Papierfassung** gesondert (das heißt: nicht als Teil der Personalakte, sondern von dieser getrennt) **zu Beweiszwecken aufbewahrt** werden. Dies führt aber im Ergebnis dazu, dass in gewissem Umfang doch eine **„doppelte Datenhaltung"** stattfindet. Der Hintergrund und der Anwendungsbereich dieser Regelung werden in der Entwurfsbegründung ausführlich erläutert (vgl. Landtags-Drucksache 17/20990, S. 24). In der Praxis werden personalverwaltende Stellen darauf zu achten haben, dass die Vorschrift eine Aufbewahrung papiergebundener Unterlagen zwar erlaubt, jedoch **nicht hierzu verpflichtet** (siehe den Wortlaut des Art. 104 Abs. 2 Satz 2 BayBG: „darf"). Die Aufbewahrung darf zudem nur solange und soweit erfolgen, wie dies „zu Beweiszwecken**" erforderlich** ist. Diese enge Zweckbindung schließt es übrigens aus, dass die noch vorhandenen Papierakten für die alltägliche Arbeit der personalverwaltenden Stelle genutzt werden können. (Ausschließlich) für den Fall, dass die Unterlagen als „analoges Backup" benötigt werden, empfehle ich daher die Aufbewahrung in einem versiegelten Schrank. Ansonsten gelten auch für die aufbewahrten Papierfassungen die **personalaktenrechtlichen Vorschriften entsprechend** (Art. 104 Abs. 2 Satz 3 BayBG).

Papierunterlagen sind mittels eines sicheren technischen Verfahrens in die elektronische Form zu überführen. Dabei ist ausweislich der Entwurfsbegründung **zumindest** eine **fortgeschrittene elektronische Signatur** oder ein fortgeschrittenes elektronisches Siegel im Sinne von Art. 26 oder Art. 36 Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014

über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28. August 2014, S. 73; im Folgenden: eIDAS-VO) zu verwenden. Vorzugswürdig ist aus Datenschutzsicht jedoch stets eine **qualifizierte elektronische Signatur** oder ein qualifiziertes elektronisches Siegel (Art. 28 oder Art. 38 eIDAS-VO, vgl. Landtags-Drucksache 17/20990, S. 24).

12.1.5 Auskunft an Beamte und Beamtinnen (Art. 107 BayBG)

Gemäß Art. 15 Abs. 1 DSGVO hat die betroffene Person unter anderem ein **Auskunftsrecht**, welche ihrer personenbezogenen Daten ein Verantwortlicher verarbeitet. Dieses Recht steht grundsätzlich auch einem oder einer Beschäftigten gegenüber seinem oder ihrem Arbeitgeber zu. Der bislang auf eine Einsichtnahme zugeschnittene Art. 107 BayBG wurde an das neue Auskunftsrecht sprachlich und systematisch angepasst. Er regelt nunmehr umfassend die **„Auskunft an Beamte und Beamtinnen"**.

Art. 107 BayBG
Auskunft an Beamte und Beamtinnen
(1) [1]Während und nach Beendigung des Beamtenverhältnisses können Beamte und Beamtinnen Auskunft aus ihrer Personalakte und aus anderen Akten, die personenbezogene Daten über sie enthalten und für das Dienstverhältnis verarbeitet werden, in Form der Einsichtnahme verlangen. [2]Im Übrigen bestimmt die personalaktenführende Behörde, wie die Auskunft gewährt wird.
(2) Nicht der Auskunft unterliegen:
1. Feststellungen über den Gesundheitszustand, soweit zu befürchten ist, dass die betroffene Person bei Kenntnis des Befunds weiteren Schaden an der Gesundheit nimmt,
2. Sicherheitsakten,
3. in Form der Einsichtnahme Daten einer betroffenen Person, die mit Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist.
(3) [1]Auf Verlangen wird eine vollständige oder teilweise Kopie zur Verfügung gestellt, sofern dies keinen unverhältnismäßigen zeitlichen oder personellen Aufwand verursacht. [2]Für die Erteilung einer zweiten und jeder weiteren Kopie werden Schreibauslagen nach Art. 10 Abs. 2 des Kostengesetzes erhoben.

Beamte und Beamtinnen können, wie bislang auch, Auskunft in Form der **Einsichtnahme** in die eigene Personalakte sowie in andere Akten verlangen, die personenbezogene Daten über den betreffenden Beamten oder die betreffende Beamtin enthalten (Art. 107 Abs. 1 Satz 1 BayBG). Begehrt ein Beschäftigter oder eine Beschäftigte keine Akteneinsicht, sondern eine andere Form der Auskunft, bestimmt die aktenführende Behörde nach pflichtgemäßem Ermessen, auf welche Weise sie die Auskunft gewährt (Art. 107 Abs. 1 Satz 2 BayBG).

Einschränkungen des Auskunftsrechts enthält Art. 107 Abs. 2 BayBG. Sie entsprechen weitgehend den bisherigen Regelungen. Im Detail zeigen sich jedoch **Unterschiede**:

– Während früher zum Schutze der Gesundheit des Beamten oder der Beamtin eine Einsicht in Feststellungen über den **Gesundheitszustand**

ausnahmsweise verwehrt werden konnte, bezieht sich dieser Ausschlusstatbestand nunmehr auf jede Form einer diesbezüglichen Auskunft (Art. 107 Abs. 2 Nr. 1 BayBG). Diese Einschränkung greift jedoch nur, **soweit** durch die Auskunft ein weiterer Schaden an der Gesundheit der betroffenen Person zu befürchten ist.

– **Sicherheitsakten** waren schon bislang vom Recht auf Einsichtnahme ausgeschlossen (Art. 107 Abs. 2 Satz 1 Halbsatz 2 BayBG-alt). Dieser Ausschluss besteht für das neue Auskunftsrecht generell (Art 107 Abs. 2 Nr. 2 BayBG).

– Zum **Schutz von Daten Dritter oder von geheimhaltungsbedürftigen Daten** ohne Personenbezug konnte zudem bislang unter bestimmten Voraussetzungen eine Einsichtnahme in Sachakten, welche personenbezogene Daten der betroffenen Beamtin oder des betroffenen Beamten enthielten, unzulässig sein. In diesen Fällen musste lediglich Auskunft erteilt werden (Art. 107 Abs. 2 Satz 2 und 3 BayBG-alt). Diese Einschränkung wurde durch die Novellierung über Sachakten hinaus **auf Personalakten erweitert** (Art 107 Abs. 2 Nr. 3 BayBG). Wie die Entwurfsbegründung ausdrücklich klarstellt (vgl. Landtags-Drucksache 17/20990, S. 26), dürften Daten Dritter in Personalakten ohnehin aber nur ausnahmsweise vorhanden sein, sodass die dargestellte Einschränkung bei Personalakten **nur in wenigen Fällen einschlägig** sein wird.

Art. 107 Abs. 3 BayBG betrifft schließlich das Recht auf **Datenkopie** nach Art. 15 Abs. 3 DSGVO: Dieses Recht besteht – ausnahmsweise – nicht, sofern die Erteilung einer Kopie einen unverhältnismäßigen zeitlichen oder personellen Aufwand verursacht (Art. 107 Abs. 3 Satz 1 BayBG). Bei elektronisch vorliegenden Daten kommt ein solcher Ausnahmefall praktisch nicht in Betracht (vgl. Landtags-Drucksache 17/20990, S. 26). Eine erste Kopie ist unentgeltlich zu erteilen. Für jede weitere Kopie werden Schreibauslagen nach Art. 10 Abs. 2 Kostengesetz erhoben (Art. 107 Abs. 3 Satz 2 BayBG).

12.1.6 Übermittlung der Personalakte und Auskünfte an Dritte (Art. 108 BayBG)

Soll eine Personalakte für die in Art. 103 Satz 1 BayBG genannten Zwecke an Behörden eines **anderen Dienstherrn** übermittelt werden, setzt dies nach Art. 108 Abs. 1 BayBG – unverändert zur bisherigen Rechtslage – die **Einwilligung** der betroffenen Person voraus.

Art. 108 BayBG
Übermittlung von Personalakten und Auskunft an nicht betroffene Personen
(1) Eine Übermittlung oder eine Auskunft aus der Personalakte an Behörden eines anderen Dienstherrn ist für die in Art. 103 Satz 1 genannten Zwecke nur mit Einwilligung des Beamten oder der Beamtin zulässig.
(2) Ohne Einwilligung des Beamten oder der Beamtin darf die Personalakte den zuständigen Behörden oder anderen Stellen übermittelt werden, soweit dies erforderlich ist
1. zur Erstellung ärztlicher Gutachten im Auftrag der personalverwaltenden Behörde oder der Pensionsbehörde,
2. für die Festsetzung, Berechnung und Rückforderung der Besoldung, der Versorgung oder für die Prüfung der Kindergeldberechtigung,

3. für die Prüfung und Durchführung der Buchung von Einzahlungen von den Betroffenen oder von Auszahlungen an die Betroffenen oder
4. für die Durchführung von Auswertungen für anonymisierte Statistik- und Berichtszwecke und deren Abruf.

(4) [1]Auskünfte an Dritte dürfen nur mit Einwilligung des Beamten oder der Beamtin erteilt werden, es sei denn, dass die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz berechtigter, höherrangiger Interessen des Dritten die Auskunftserteilung zwingend erfordert. [2]Inhalt und Empfänger der Auskunft sind dem Beamten oder der Beamtin schriftlich mitzuteilen.

(5) [1]Ohne Einwilligung des Beamten oder der Beamtin können den zuständigen Behörden Auskünfte aus der Personalakte erteilt werden, soweit dies im Einzelfall
1. zu den in Abs. 2 genannten Zwecken,
2. zur Entscheidung über die Verleihung von staatlichen Orden, Ehrenzeichen oder sonstigen staatlichen Ehrungen oder
3. im Rahmen der Art. 8a bis 8e BayVwVfG zwingend
erforderlich ist. [2]Soweit eine Auskunft für die in Abs. 2 genannten Zwecke ausreichend ist, unterbleibt eine Übermittlung.

(6) [1]Übermittlung und Auskunft sind auf den jeweils erforderlichen Umfang zu beschränken. [2]Ein automatisierter Datenabruf durch andere Behörden ist unzulässig, soweit durch besondere Rechtsvorschrift nichts anderes bestimmt ist.

Fälle, in denen eine Personalakte **auch ohne vorherige Einwilligung** der betroffenen Person an zuständige Stellen desselben Dienstherrn übermittelt werden darf, sind in Art. 108 Abs. 2 BayBG normiert. Dies betrifft unter anderem Übermittlungen zur Erstellung ärztlicher Gutachten im Auftrag der personalverwaltenden Behörde (Art. 108 Abs. 2 Nr. 1 BayBG) oder zu Besoldungszwecken (Art. 108 Abs. 2 Nr. 2 BayBG). Voraussetzung ist allerdings, dass **die in dieser Vorschrift genannten Zwecke** eine **Übermittlung** der Personalakte im konkreten Fall auch tatsächlich **erfordern**. Soweit in diesem Zusammenhang eine Auskunft ausreicht, hat – wie bislang auch (vgl. Art. 108 Abs. 1 Satz 5 BayBG-alt) – die Übermittlung der Personalakte zu unterbleiben (Art. 108 Abs. 5 Satz 2 BayBG).

Art. 108 Abs. 4 und 5 BayBG regeln **Auskünfte** aus der Personalakte **an Dritte**. Dabei wurde der bisherige Art. 108 Abs. 2 BayBG-alt unverändert in Art. 108 Abs. 4 BayBG überführt. Art. 108 Abs. 5 BayBG entspricht inhaltlich im Wesentlichen Art. 108 Abs. 1 Satz 4 und 5, Abs. 3 BayBG-alt.

Die in Art. 111 Abs. 1 Satz 3 BayBG-alt enthaltene Regelung zum automatisierten Datenabruf durch andere Behörden findet sich aufgrund des näheren Sachzusammenhangs nun unverändert in Art. 108 Abs. 6 BayBG.

12.1.7 Auftragsverarbeitung (Art. 108 Abs. 3 BayBG)

Neu aufgenommen wurde in Art. 108 Abs. 3 BayBG eine Regelung zur **Auftragsverarbeitung**. Die Datenschutz-Grundverordnung beschränkt die Zulässigkeit einer Auftragsverarbeitung auch im Bereich der Personalverwaltung nicht; sie trifft in Art. 28 DSGVO umfassende inhaltliche Vorgaben über das „Wie“ der Auftragsverarbeitung. Mitgliedstaatliche Regelungen können allerdings im Rahmen bestehender „Öffnungsklauseln“ die Zulässigkeit einer Auftragsverarbeitung für bestimmte Verarbeitungstätigkeiten von Bedingungen abhängig machen oder gänzlich ausschließen, mithin das „Ob“ der Auftragsverarbeitung bestimmen.

Art. 108 BayBG
Übermittlung von Personalakten und Auskunft an nicht betroffene Personen
(3) [1]Die Verarbeitung von Personalaktendaten im Auftrag der personalverwaltenden Behörde im Sinn des Art. 28 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) ist nur zulässig, soweit sie als unterstützende Dienstleistung im Rahmen der überwiegend automatisierten Erledigung von Aufgaben der Behörde zur Vermeidung von Störungen im Geschäftsablauf des Dienstherrn oder zur Realisierung erheblich wirtschaftlicherer Arbeitsabläufe erforderlich ist. [2]Die Beauftragung einer nicht öffentlichen Stelle als Auftragsverarbeiter setzt voraus, dass die mit der Verarbeitung von Personalaktendaten befassten Beschäftigten nach dem Verpflichtungsgesetz zur Wahrung der Daten verpflichtet werden.

Im bayerischen Personalaktenrecht steht einer Auftragsverarbeitung durch externe Dienstleister an sich die „doppelte Zulässigkeitsbeschränkung" des Art. 103 BayBG entgegen. Art. 108 Abs. 3 BayBG lässt die Verarbeitung von Personalaktendaten im Auftrag allerdings – ausnahmsweise – in **begrenztem Umfang** zu. Eine Auftragsverarbeitung ist gemäß Art. 108 Abs. 3 Satz 1 BayBG jedoch **nur zulässig**, soweit sie als **unterstützende Dienstleistung** im Rahmen der überwiegend automatisierten Erledigung von Aufgaben der Behörde zur Vermeidung von Störungen im Geschäftsablauf des Dienstherrn oder zur Realisierung erheblich wirtschaftlicherer Arbeitsabläufe **erforderlich** ist.

Als Anwendungsfall nennt die Entwurfsbegründung (vgl. Landtags-Drucksache 17/20990, S. 27) „das Einscannen von Personalakten für die personalverwaltende Stelle im Zuge der Umstellung auf eine elektronische Personalakte". Soll eine nicht öffentliche Stelle als Auftragsverarbeiter beauftragt werden, sind deren Beschäftigte, soweit sie mit der Verarbeitung von Personalaktendaten befasst sind, nach dem **Verpflichtungsgesetz** zu verpflichten (Art. 108 Abs. 3 Satz 2 BayBG).

12.1.8 Einsatz automatisierter Verfahren (Art. 111 BayBG)

Von einer elektronischen Personalakte begrifflich zu trennen sind **automatisierte Verfahren** mittels derer (auch) Personalaktendaten verarbeitet werden können. Deren Einsatz ist wie bislang in Art. 111 BayBG geregelt. Aufbau und Inhalt der Vorschrift sind in mehrfacher Hinsicht umgestaltet worden.

Art. 111 BayBG
Einsatz automatisierter Verfahren
(1) [1]Für die in Art. 103 genannten Zwecke dürfen automatisierte Verfahren eingesetzt werden, in denen auch Personalaktendaten verarbeitet werden dürfen. [2]Werden Personalaktendaten verarbeitet, sind insoweit die Art. 103 sowie 108 bis 110 entsprechend anzuwenden. 3Personalaktendaten im Sinn des Art. 105 dürfen zudem nur im Rahmen ihrer Zweckbestimmung und nur von den übrigen Personaldateien technisch und organisatorisch getrennt verarbeitet werden.
(2) [1]Eine beamtenrechtliche Entscheidung darf nur dann auf einer ausschließlich automatisierten Verarbeitung von personenbezogenen Daten beruhen, wenn einem vorausgegangenen Antrag des Beamten oder der Beamtin vollständig entsprochen wird. [2]Die Kürzung auf Grund der Regelung in Art. 96 Abs. 3 Satz 5 ist insofern unschädlich. [3]Dem Beamten oder der Beamtin sind die über ihn oder sie in einem automatisierten Verfahren nach Abs. 1 Satz 1 gespeicherten Daten auf Verlangen mitzuteilen. [4]Die Verarbeitungs- und Nutzungsformen automatisierter

Personalverwaltungsverfahren sind zu dokumentieren und einschließlich des jeweiligen Verwendungszwecks sowie der regelmäßigen Empfänger und des Inhalts automatisierter Datenübermittlung allgemein bekanntzugeben.

Art. 111 Abs. 1 Satz 1 BayBG bestimmt zunächst, dass der Einsatz automatisierter Verfahren, in denen auch Personalaktendaten verarbeitet werden, in der Personalverwaltung (nur) für die **in Art. 103 BayBG genannten Zwecke** zulässig ist. Hinsichtlich der Verarbeitung von Personalaktendaten erklärt Art. 111 Abs. 1 Satz 2 BayBG die Vorschriften der Art. 103 sowie Art. 108 bis 110 BayBG für entsprechend anwendbar. Die einschränkende Regelung des Art. 111 Abs. 1 Satz 3 BayBG zur automatisierten Verarbeitung von „Beihilfedaten" entspricht inhaltlich dem bisherigen Art. 111 Abs. 2 BayBG-alt.

Art. 111 Abs. 2 Satz 1 und 2 BayBG betrifft die sehr eingeschränkte, im Ergebnis vor allem das Beihilfeverfahren betreffende Zulässigkeit einer beamtenrechtlichen Entscheidung, welche ausschließlich auf einer automatisierten Verarbeitung personenbezogener Daten beruht. Damit soll der europarechtlichen Vorgabe des Art. 22 DSGVO Rechnung getragen werden (vgl. Landtags-Drucksache 17/20990, S. 28 f.).

Bei erstmaliger Speicherung personenbezogener Daten in einem automatisierten Verfahren sowie bei wesentlichen Änderungen bestand gegenüber den betroffenen Beamtinnen und Beamten bislang eine Mitteilungs- oder Benachrichtigungspflicht (Art. 111 Abs. 5 Satz 1 BayBG-alt). Diese zugunsten der Beamtinnen und Beamten bestehende **Schutzvorschrift** sollte zunächst **ersatzlos entfallen**. Auf meine diesbezüglich geäußerten **Bedenken** hin wurde mit dem neuen Art. 111 Abs. 2 Satz 3 BayBG eine grundsätzlich jederzeit zu erfüllende **Informationspflicht eingeführt**: Auf Verlangen sind einem Beamten oder einer Beamtin die über ihn oder sie in einem automatisierten Verfahren nach Art. 111 Abs. 1 Satz 1 BayBG gespeicherten Daten mitzuteilen. Die bisher in Art. 111 Abs. 5 Satz 2 normierte Dokumentations- und Bekanntgabeverpflichtung findet sich nun inhaltlich unverändert in Art. 111 Abs. 2 Satz 4 BayBG.

12.1.9 Sonstige Änderungen

Weitere Änderungen betreffen unter anderem die Verwendung und Weitergabe von **Beihilfeunterlagen** (Art. 105 Satz 3 und 4 BayBG) sowie die **Aufbewahrung und Vernichtung von Personalakten** (Art. 110 BayBG).

Art. 105 BayBG
Beihilfeunterlagen
[1]Unterlagen über Beihilfen sind stets als Teilakte zu führen. [2]Diese ist von der übrigen Personalakte getrennt aufzubewahren. [3]Sie soll nur von Beschäftigten einer von der übrigen Personalverwaltung getrennten Organisationseinheit oder der zuständigen Rechnungsprüfung bearbeitet werden. [4]Die Beihilfeakte darf für andere als für Beihilfezwecke und Zwecke der Rechnungsprüfung nur verwendet oder weitergegeben werden, wenn der oder die Beihilfeberechtigte und bei der Beihilfegewährung berücksichtigte Angehörige im Einzelfall einwilligen, die Einleitung oder Durchführung eines im Zusammenhang mit einem Beihilfeantrag stehenden behördlichen oder gerichtlichen Verfahrens dies erfordert oder soweit es zur Abwehr erheblicher Nachteile für das Gemeinwohl, einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder einer schwerwiegenden Beeinträch-

tigung der Rechte einer anderen Person erforderlich ist. [5]Die erforderlichen personenbezogenen Daten aus Arzneimittelverordnungen im Sinn des § 1 des Gesetzes über Rabatte für Arzneimittel dürfen an den Treuhänder ausschließlich zum Zweck der Prüfung gemäß § 3 des Gesetzes über Rabatte für Arzneimittel übermittelt werden. [6]Sätze 1 bis 5 gelten entsprechend für Unterlagen über Heilfürsorge und Heilverfahren.

Art. 110
BayBG Aufbewahrung und Vernichtung von Personalakten
(1) [1]Personalakten sind nach ihrem Abschluss von der personalaktenführenden Behörde fünf Jahre aufzubewahren. [2]Personalakten sind abgeschlossen,

1. *wenn der Beamte oder die Beamtin ohne Versorgungsansprüche aus dem öffentlichen Dienst ausgeschieden ist, mit Erreichen der gesetzlichen Altersgrenze, in den Fällen des § 24 BeamtStG und des Art. 11 BayDG jedoch erst, wenn mögliche Versorgungsempfänger und Versorgungsempfängerinnen nicht mehr vorhanden sind,*
2. *wenn der Beamte oder die Beamtin verstorben ist, mit Ablauf des Todesjahres.*

[3]Kann der nach Satz 2 Nr. 2 maßgebliche Zeitpunkt nicht festgestellt werden, ist Art. 10 Abs. 3 Satz 3 des Bayerischen Archivgesetzes entsprechend anzuwenden.
(2) [1]Unterlagen über Beihilfen, Heilfürsorge, Heilverfahren, Unterstützungen, Erholungsurlaub, Erkrankungen sowie Umzugs- und Reisekosten sind fünf Jahre nach Ablauf des Jahres, in dem die Bearbeitung des einzelnen Vorgangs abgeschlossen wurde, aufzubewahren. [2]Sofern aus ihnen die Art der Erkrankung ersichtlich ist, sind sie unverzüglich zurückzugeben oder zu vernichten, wenn sie für den Zweck, zu dem sie vorgelegt worden sind, nicht mehr benötigt werden. [3]Elektronisch gespeicherte Beihilfebelege sind spätestens ein Jahr nach Ablauf des Jahres, in dem die Unterlagen elektronisch erfasst wurden, zu löschen, sofern sie nicht darüber hinaus für die Bearbeitung oder auf Grund sonstiger gesetzlicher Vorschriften benötigt werden. [4]Arzneimittelverordnungen im Sinn des § 1 des Gesetzes über Rabatte für Arzneimittel sind zur Geltendmachung von Rabatten nach diesem Gesetz nicht zurückzugeben. [5]Die Vernichtung dieser Arzneimittelverordnungen erfolgt unverzüglich, sobald sie für die dort geregelten Zwecke nicht mehr benötigt werden, spätestens jedoch zehn Jahre nach Ablauf des Jahres, in dem die Arzneimittelverordnungen elektronisch erfasst wurden.
(3) Versorgungsakten sind zehn Jahre nach Ablauf des Jahres, in dem die letzte Versorgungszahlung geleistet worden ist, aufzubewahren; besteht die Möglichkeit eines Wiederauflebens des Anspruchs, sind die Akten 30 Jahre aufzubewahren.
(4) Personalakten werden nach Ablauf der Aufbewahrungsfrist vernichtet, sofern sie nicht vom zuständigen öffentlichen Archiv übernommen werden.

12.1.10 Fazit

Die jüngste Novellierung des Personalaktenrechts im Bayerischen Beamtengesetz trägt einerseits dem durch die Datenschutz-Grundverordnung entstandenen Anpassungsbedarf Rechnung. Darüber hinaus sind aber auch Änderungen erfolgt, welche nicht zwingend durch das neue europäische Datenschutzrecht veranlasst waren. Eine grundlegende Umordnung des bayerischen Personalaktenrechts hat es in diesem Zusammenhang allerdings nicht gegeben.

Die personalverwaltenden Stellen sollten sich jedoch stets vergegenwärtigen, dass die Datenschutz-Grundverordnung auch bei der Verarbeitung von

Beschäftigtendaten grundsätzlich **unmittelbar zur Anwendung** kommt. Das bayerische Personalaktenrecht enthält insoweit ergänzende oder spezifizierende Vorschriften. Vor allem dort, wo es keine Regelung trifft, sind die jeweils einschlägigen Vorgaben der Datenschutz-Grundverordnung – gegebenenfalls modifiziert durch das neugefasste Bayerische Datenschutzgesetz – in den Blick zu nehmen.

Die neue Systematik des Datenschutzrechts gilt also auch hier: Zur Beurteilung datenschutzrechtlicher Fragestellungen sind die Datenschutz-Grundverordnung und das nationale Datenschutzrecht **im Zusammenhang zu lesen und anzuwenden.**

12.2 Förmliche Verpflichtung von Bediensteten bayerischer öffentlicher Stellen auf das Datengeheimnis?

Eine Verarbeitung personenbezogener Daten ist nur unter den Voraussetzungen von Art. 6 DSGVO zulässig. Den bayerischen öffentlichen Stellen stehen meist gesetzliche Verarbeitungsbefugnisse (Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 UAbs. 1 Buchst. b DSGVO) zur Verfügung. Ist eine Offenlegung personenbezogener Daten nicht erlaubt, muss sie unterbleiben. Art. 29 DSGVO bestimmt zudem, dass jede einem Verantwortlichen unterstellte Person ihr zugängliche personenbezogene Daten grundsätzlich nur auf dessen Weisung verarbeiten darf. Vor dem Hintergrund dieses unionsrechtlichen Regelungsrahmens steht **Art. 11 Satz 1 BayDSG**:

„Den bei öffentlichen Stellen beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis).“

Bayerische öffentliche Stellen fragten bei mir an, ob Beschäftigte auf die Einhaltung des Datengeheimnisses förmlich zu verpflichten seien. Ich habe die folgenden Hinweise gegeben:

Eine förmliche Verpflichtung auf das Datengeheimnis nach Art. 11 Satz 1 BayDSG – zumal mit konstitutiver Wirkung – sieht das Gesetz nicht vor. Die Beschäftigten bayerischer öffentlicher Stellen sind ab Beginn ihres Dienst- oder Arbeitsverhältnisses von Gesetzes wegen verpflichtet, das Datengeheimnis zu beachten. Gemäß Art. 11 Satz 2 BayDSG besteht das Datengeheimnis nach dem Ende der Tätigkeit fort. Eine förmliche Verpflichtung kennt das Bundesrecht für die Beschäftigten der Meldebehörden hinsichtlich des Meldegeheimnisses (§ 7 Bundesmeldegesetz).

Jedenfalls bei Aufnahme einer Tätigkeit für eine bayerische öffentliche Stelle sollten Beschäftigte über ihre Pflichten hinsichtlich des Schutzes personenbezogener Daten informiert werden. Danach sollten sie befähigt sein, die auf dem jeweiligen Dienstposten oder Arbeitsplatz zugänglichen personenbezogenen Daten sachgerecht zu handhaben und unzulässige Datenumgänge zu vermeiden. Dies gilt auch für unbefugte Abrufe aus dienstlich bereitgestellten Datenbanken wie dem Bayerischen Behördeninformationssystem (BayBIS, siehe dazu Nr. 7.1). Der behördliche Datenschutzbeauftragte sollte auf die Durchführung entsprechender Schulungen durch den Verantwortlichen hinwirken (vgl. Art. 39 Abs. 1 Buchst. b DSGVO), gegebenenfalls sie selbst anbieten.

12.3 Dienstweg und Zugang zum behördlichen Datenschutzbeauftragten bei bayerischen öffentlichen Stellen

Der behördliche Datenschutzbeauftragte ist ein wichtiger Ansprechpartner auch für die Beschäftigten bayerischer öffentlicher Stellen, wenn es um Fragen des Datenschutzes geht. Mich haben mehrere Anfragen erreicht, die sich auf eine Kontrolle des Zugangs zum behördlichen Datenschutzbeauftragten bezogen. So sollten diesem in einer Behörde beispielsweise entsprechende Gesuche nur über die Personalstelle zugeleitet werden dürfen. Insofern ist zu unterscheiden:

12.3.1 Beschäftigte als betroffene Personen

Sind Beschäftigte betroffene Person, weil die öffentliche Stelle etwa im Rahmen der Personalverwaltung ihre personenbezogenen Daten verarbeitet, so richtet sich der Zugang zum behördlichen Datenschutzbeauftragten nach Art. 38 Abs. 4 DSGVO. Dort heißt es:

„Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen zu Rate ziehen."

Die Vorschrift gewährleistet betroffenen Personen die Möglichkeit, mit dem Datenschutzbeauftragten unmittelbar, also ohne die Kenntnis, gar die Mitwirkung Dritter Kontakt aufzunehmen. Anders wäre auch die in Art. 38 Abs. 5 DSGVO angeordnete Vertraulichkeit nicht gewährleistet. Diese Vorgaben gelten zugunsten betroffener Personen unabhängig davon, ob sie zum Verantwortlichen in einem Beschäftigungsverhältnis stehen oder nicht.

Eine Vorgabe an Beschäftigte, den Datenschutzbeauftragten in eigenen Angelegenheiten nur über die Personalstelle, über die Behördenleitung oder auf dem Dienstweg kontaktieren zu dürfen, ist daher nicht zulässig.

12.3.2 Beschäftigte als Anfragesteller

Beschäftigte suchen den Rat des behördlichen Datenschutzbeauftragten aber nicht nur in der Rolle der betroffenen Person. Sie haben bei ihrer Arbeit oftmals mit Verarbeitungen personenbezogener Daten Dritter zu tun. In diesem Zusammenhang stellen sich ebenfalls regelmäßig datenschutzrechtliche oder datenschutzpraktische Fragen. Meinungsverschiedenheiten zwischen den ratsuchenden Beschäftigten und ihren Vorgesetzten bestehen in dieser Fallkonstellation häufig nicht; es steht vielmehr in Rede, wie die öffentliche Stelle als solche datenschutzgerecht agiert.

Art. 39 Abs. 1 Buchst. a DSGVO stellt dem Datenschutzbeauftragten die folgende Aufgabe:

„Unterrichtung und Beratung des Verantwortlichen […] und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten".

Trifft die öffentliche Stelle keine Regelungen, kann sich daher jeder oder jede Beschäftigte mit einer bei der eigenen Arbeit aufgetretenen datenschutzrechtlichen oder datenschutzpraktischen Frage unmittelbar an den behördlichen Datenschutzbeauftragten wenden.

Eine öffentliche Stelle darf durch innerdienstliche Regelung aber auch bestimmen, dass Anfragen dieser Art dem behördlichen Datenschutzbeauftragten über eine/n Vorgesetzte/n oder auf dem Dienstweg vorgelegt werden. Für einen unmittelbaren Zugang jedes oder jeder Beschäftigten spricht zwar das Interesse an einer möglichst optimalen Nutzung der Expertise des Datenschutzbeauftragten mittels einer zügigen Beratung, die so auch telefonisch in einer konkreten Arbeitssituation gewährleistet ist. Die mittelbare Befassung verschafft aber Vorgesetzten einen Eindruck von den auftretenden datenschutzrechtlichen und datenschutzpraktischen Problemen und versetzt sie in die Lage, die mit dem Datenschutzbeauftragten erarbeiteten Lösungen auch für andere Beschäftigte nutzbar zu machen. Welchem Ziel der Vorrang einzuräumen ist, sollte jeweils im Hinblick auf die konkrete Organisations- und Verantwortlichkeitsstruktur entschieden werden.

Regelungen zur Einbindung des behördlichen Datenschutzbeauftragten sollten möglichst in der für die öffentliche Stelle maßgeblichen Datenschutz-Dienstanweisung getroffen werden. Ein Muster ist in den vom Bayerischen Staatsministerium des Innern, für Sport und Integration herausgegebenen Arbeitshilfen zur praktischen Umsetzung der Datenschutz-Grundverordnung unter Nr. 4.1 zu finden (Internet: https://www.stmi.bayern.de/sus/datensicherheit/datenschutz/reform_arbeitshilfen/index.php).

12.3.3 Beschäftigte als Hinweisgeber

Beschäftigte wenden sich mitunter aber auch als Hinweisgeber an den behördlichen Datenschutzbeauftragten, weil sie ihn auf einen möglichen datenschutzrechtlichen Missstand aufmerksam machen möchten. Dies gilt insbesondere dann, wenn Beschäftigte mit Bedenken hinsichtlich konkreter Verarbeitungen bei ihren Vorgesetzten kein Gehör finden. Hier wird es also in erster Linie um die Frage gehen, wie sich die Beschäftigten selbst aus Datenschutzsicht rechtskonform verhalten sollen. Dazu sind sie in ihren Dienst- oder Beschäftigungsverhältnissen nämlich verpflichtet. Die Beratungssituation ist hier – anders als oben unter 12.3.1 – durch eine Meinungsverschiedenheit zwischen den Beschäftigten und ihren Vorgesetzten gekennzeichnet.

Auch insofern ist Art. 39 Abs. 1 Buchst. a DSGVO maßgeblich. Daran können die beamtenrechtlichen Bestimmungen zur Remonstration (§ 36 Abs. 2, 3 Beamtenstatusgesetz – BeamtStG) nichts ändern. Diese Vorschriften regeln, unter welchen Voraussetzungen einen Beamten oder eine Beamtin (ausnahmsweise) nicht die ihm oder ihr nach § 36 Abs. 1 BeamtStG zugewiesene Verantwortung trifft. Sie legen dagegen nicht fest, wessen Rat der Beamte oder die Beamtin in einer „kritischen“ Entscheidungssituation suchen darf.

Sollte eine innerdienstliche Regelung bei einer bayerischen öffentlichen Stelle den Kontakt mit dem behördlichen Datenschutzbeauftragten (auch) im Fall einer „kontroversen“ Beratungssituation nur unter Einbindung von Vorgesetzten beziehungsweise auf dem Dienstweg zulassen, würde sie auf eine Situation hinwirken, in welcher es vom Willen der jeweiligen Vorgesetzten abhängt, inwieweit der

Datenschutzbeauftragte seiner Aufgabe nach Art. 39 Abs. 1 Buchst. a DSGVO hinsichtlich der ihnen zugeordneten Beschäftigten nachkommen kann. Zudem könnte ihm eine wichtige Erkenntnisquelle für seine Überwachungsaufgabe (Art. 39 Abs. 1 Buchst. b DSGVO) verschlossen werden.

Wesentlich wäre im Übrigen die Rolle des Datenschutzbeauftragten berührt: Dass Art. 39 Abs. 1 Buchst. a DSGVO ihm die Aufgabe der Beratung gerade gegenüber dem Verantwortlichen und seinen Beschäftigten zuweist, legt ein Verständnis nahe, nach welchem der Datenschutzbeauftragte in einer „kontroversen" Beratungssituation gerade die Rolle eines „Vermittlers" einnimmt. Eine der Aufgabe adäquate Beratung erfordert hier nämlich eine Analyse der Pflichten beider Seiten und die Entwicklung einer allseits datenschutzkonformen Problemlösung.

Eine Regelung, wie sie **§ 14 des Musters für eine Datenschutz-Dienstanweisung** (siehe oben unter 12.3.2 am Ende) **im Bereich der Datenschutz-Richtlinie für Polizei und Strafjustiz** vorsieht, ist vor diesem Hintergrund ein Beispiel für eine auch in der Welt der Datenschutz-Grundverordnung positiv zu bewertende Fehlerkultur. Dort heißt es:

„[1]Erlangt ein Mitarbeiter von einem Datenschutzverstoß Kenntnis, kann er sich jederzeit unmittelbar an den behördlichen Datenschutzbeauftragten wenden. [2]Der behördliche Datenschutzbeauftragte behandelt die Meldung vertraulich. [3]Er darf Tatsachen, die ihm in Ausübung seiner Funktion anvertraut wurden, und die Identität der mitteilenden Person nicht ohne dessen Einverständnis offenbaren."

12.3.4 Fazit

Der Zugang zum behördlichen Datenschutzbeauftragten folgt grundsätzlich nicht dem Dienstweg. Den unmittelbaren Kontakt können Beschäftigte einer bayerischen öffentlichen Stelle insbesondere suchen, wenn sie dieser Stelle selbst als betroffene Personen gegenüberstehen. Das gleiche gilt in kontroversen Beratungssituationen, wenn der Datenschutzbeauftragte den Verantwortlichen und seine Beschäftigten bei der Suche nach einer beiderseits pflichtgemäßen Lösung zu einem Datenschutzproblem unterstützen soll. Allenfalls für nicht kontroverse Beratungssituationen kommen innerdienstliche Regelungen zur Einbindung von Vorgesetzten in Betracht.

12.4 Einwilligung bei Erteilung von Gutachtenaufträgen durch die Beihilfestelle

Richterinnen und Richter, Beamtinnen und Beamte sowie Versorgungsempfängerinnen und Versorgungsempfänger erhalten für sich und ihre berücksichtigungsfähigen Angehörigen **Beihilfen** zur Deckung von Kosten medizinischer Behandlungen (siehe Art. 96 Abs. 1 Bayerisches Beamtengesetz – BayBG). Diesbezügliche Aufwendungen werden aber nur ersetzt, soweit sie **medizinisch notwendig und angemessen** sind (siehe Art. 96 Abs. 2 Satz 1 BayBG).

Art. 96 BayBG
Beihilfe in Krankheits-, Geburts-, Pflege- und sonstigen Fällen
(1) [1]Beamte und Beamtinnen, Ruhestandsbeamte und Ruhestandsbeamtinnen, deren versorgungsberechtigte Hinterbliebene, Dienstanfänger und Dienstanfängerinnen sowie frühere Beamte und Beamtinnen, die wegen Dienstunfähigkeit oder Erreichen der Altersgrenze entlassen sind, erhalten für sich, den Ehegatten

oder den Lebenspartner (Lebenspartner und Lebenspartnerin im Sinn des § 1 des Lebenspartnerschaftsgesetzes), soweit dessen Gesamtbetrag der Einkünfte (§ 2 Abs. 3 des Einkommensteuergesetzes) im zweiten Kalenderjahr vor der Stellung des Beihilfeantrags 18 000 € nicht übersteigt, und die im Familienzuschlag nach dem Bayerischen Besoldungsgesetz berücksichtigungsfähigen Kinder Beihilfen als Ergänzung der aus den laufenden Bezügen zu bestreitenden Eigenvorsorge, solange ihnen laufende Besoldung, Unterhaltsbeihilfe nach Art. 97 BayBesG oder Versorgungsbezüge mit Ausnahme von Halbwaisengeld (Art. 39, 40 BayBeamtVG) zustehen. […]
(2) [1]Beihilfeleistungen werden zu den nachgewiesenen medizinisch notwendigen und angemessenen Aufwendungen in Krankheits-, Geburts- und Pflegefällen und zur Gesundheitsvorsorge gewährt. […]

Bestehen Streitigkeiten oder Unklarheiten über die Notwendigkeit und Angemessenheit einzelner geltend gemachter Aufwendungen, können diese in einem von der Beihilfestelle angestoßenen **speziellen Überprüfungsverfahren – insbesondere unter Einschaltung von Gutachterinnen und Gutachtern –** geklärt werden. Die Bayerische Beihilfeverordnung (BayBhV) sieht hierzu in § 48 Abs. 7 BayBhV im Einzelnen Folgendes vor:

§ 48 BayBhV
Verfahren
(7) [1]Zur Überprüfung von Notwendigkeit und Angemessenheit einzelner geltend gemachter Aufwendungen kann die Festsetzungsstelle Gutachterinnen bzw. Gutachter, Beratungsärztinnen bzw. Beratungsärzte und sonstige geeignete Stellen unter Übermittlung der erforderlichen Daten beteiligen, wobei personenbezogene Daten nur mit Einwilligung des Beihilfeberechtigten übermittelt werden dürfen. [2]Die Zuerkennung der Eignung setzt voraus, dass die mit der Bewertung betrauten Personen nach dem Verpflichtungsgesetz zur Wahrung der Daten verpflichtet werden.

Verweigern Beihilfeberechtigte das Einverständnis zur Übermittlung ihrer für die Begutachtung erforderlichen personenbezogenen Daten und kann die Berechtigung des Anspruchs nicht anderweitig, insbesondere nach Übermittlung pseudonymisierter Daten geklärt werden, werden Beihilfen nicht gewährt (vgl. Nr. 1 Satz 3 Verwaltungsvorschrift zu § 48 Abs. 8 [jetzt Abs. 7] BayBhV).

Diese Regelungen halte ich grundsätzlich für angemessen, um einen Ausgleich zwischen den Persönlichkeitsinteressen der Beihilfeberechtigten einerseits und dem Interesse an einer sparsamen Bewirtschaftung öffentlicher Mittel andererseits herzustellen. Bereits in meinem 23. Tätigkeitsbericht 2008 habe ich unter Nr. 21.1.2 darauf hingewiesen, dass der **Nachweis aus meiner Sicht in aller Regel mit pseudonymisierten Daten** geführt werden kann. Personenbezogene Daten müssen zum Zweck der Gutachtenerstellung nur ausnahmsweise übermittelt werden.

12.4.1 Ärztliche Behandlung von Beihilfeberechtigten

Das dargestellte Verfahren regelt datenschutzrechtlich befriedigend allerdings nur den Fall, dass Unklarheiten hinsichtlich der Erstattungsfähigkeit von Aufwendungen aus der Behandlung der **Person des oder der Beihilfeberechtigten** gutachterlich aufzuklären sind. § 48 Abs. 7 Satz 1 BayBhV stellt nämlich auf die Zustimmung gerade des oder der Beihilfeberechtigten zur Übermittlung von Daten

an den Gutachter oder die Gutachterin ab. Unberücksichtigt bleibt der Fall, dass die behandelte Person nicht zugleich der oder die Beihilfeberechtigte ist.

12.4.2 Ärztliche Behandlung von berücksichtigungsfähigen Angehörigen

Unter bestimmten Voraussetzungen hat der oder die Beihilfeberechtigte nämlich auch Anspruch auf Beihilfe zu den Kosten der **Behandlung seiner oder ihrer Familienangehörigen**. Datenschutzrechtlich kann in eine Datenübermittlung aber grundsätzlich nur die Person einwilligen, deren Daten übermittelt werden sollen. Entsprechendes gilt im Hinblick auf die Entbindung von der ärztlichen Schweigepflicht. Eine Einwilligung (allein) des oder der Beihilfeberechtigten kann nicht dazu führen, dass der behandelnde Arzt oder die behandelnde Ärztin Auskunft über das Bestehen und den Inhalt eines Behandlungsverhältnisses mit einem oder einer Familienangehörigen des oder der Beihilfeberechtigten erteilen darf. Für den Arzt oder die Ärztin ist grundsätzlich die **Einwilligung seines/ihres Patienten oder seiner/ihrer Patientin, nicht aber die des oder der (nicht behandelten) Beihilfeberechtigten für die Entbindung von der ärztlichen Schweigepflicht maßgebend** (vgl. § 203 Abs. 1 Nr. 1 Strafgesetzbuch).

Schon aus diesem Grund war das von den Beihilfestellen des Landesamts für Finanzen in der Regel praktizierte Verfahren, ausschließlich die Einwilligung des oder der Beihilfeberechtigten einzuholen, zwar in Bezug auf § 48 Abs. 7 Satz 1 BayBhV nachvollziehbar. Datenschutzrechtlich, vor allem im Hinblick auf die Entbindung von der ärztlichen Schweigepflicht, war es aber nur dann zielführend, wenn der oder die Beihilfeberechtigte die Einwilligung gemeinsam mit einer entsprechenden Schweigepflichtentbindungserklärung des oder der behandelten berücksichtigungsfähigen Angehörigen erteilte.

Um Missverständnissen über die **Notwendigkeit der zweifachen Einwilligung** – durch den oder die Beihilfeberechtigte/n und den oder die behandelte/n Angehörige/n – auch auf Seiten der Beihilfestellen vorzubeugen, habe ich eine entsprechende Eingabe zum Anlass genommen, mich an das Landesamt für Finanzen zu wenden, auf die Rechtslage hinzuweisen und die geschilderte Praxis kritisch zu hinterfragen.

Das für die Beihilfefestsetzung im bayerischen staatlichen Bereich grundsätzlich zuständige **Landesamt für Finanzen** hat die Kritik angenommen und die **entsprechenden Formulare geändert.** Künftig ist jetzt stets auch die Einwilligung des oder der behandelten berücksichtigungsfähigen Angehörigen des oder der Beihilfeberechtigten einzuholen, sofern nicht ohnehin – vorrangig – eine pseudonymisierte Prüfung durch einen Gutachter oder eine Gutachterin in Betracht kommt. Auch darauf habe ich das Landesamt für Finanzen nochmals gesondert hingewiesen.

Da sich die geschilderte Problematik nicht nur im Zuständigkeitsbereich des Landesamts für Finanzen stellt, **fordere ich alle bayerischen – insbesondere staatlichen und kommunalen – Beihilfestellen** dazu auf, bei der gutachterlichen Überprüfung der Notwendigkeit und Angemessenheit einzelner Aufwendungen für die Behandlung von berücksichtigungsfähigen Angehörigen **entsprechend zu verfahren**.

12.5 Weitergabe von Personalaktendaten an den gemeindlichen Rechnungsprüfungsausschuss

Die Gemeinden müssen ihre Haushalte sparsam und wirtschaftlich führen. Über die Bewirtschaftung der Mittel müssen sie Rechenschaft ablegen. Da ein bedeutender Anteil ihrer Ausgaben auf die Vergütung der kommunalen Bediensteten entfällt, sind auch diese Gegenstand der **Finanzkontrolle**.

In den Gemeinden wird diese Funktion – nach den Vorgaben der Gemeindeordnung für den Freistaat Bayern (GO) über das Prüfungswesen (Art. 103 bis 107 GO) – **örtlich durch den Gemeinderat oder einen von ihm gebildeten Rechnungsprüfungsausschuss** wahrgenommen; überörtlich wird sie durch den Bayerischen Kommunalen Prüfungsverband oder die staatlichen Rechnungsprüfungsstellen der Landratsämter ausgeübt.

12.5.1 Sachverhalt

Im Berichtszeitraum wandte sich nun eine Gemeindeverwaltung an mich, weil einzelne Mitglieder des **Rechnungsprüfungsausschusses** die **Vorlage sämtlicher Personalakten und der persönlichen Gehaltsabrechnungen aller gemeindlichen Bediensteten gefordert** hatten. Die Gemeindeverwaltung hielt das für datenschutzrechtlich unzulässig.

Nach Auffassung der Verwaltung müsse es genügen, dem Ausschuss anonymisierte Gehaltslisten beziehungsweise zusammenfassende Übersichten über die Vergütungen der Bediensteten zur Verfügung zu stellen, aus welchen sich im Wesentlichen nur die Anzahl der Bediensteten einer bestimmten Besoldungs- oder Entgeltgruppe in den einzelnen Sachgebieten ergebe. Der Ausschuss habe dagegen keinen Anspruch, diese Informationen in einer Weise zu erhalten, die eine konkrete Zuordnung bestimmter Zahlungen zu einzelnen Personen ermögliche. Einem umfassenden Einsichtsrecht in die Gehalts- und sonstigen Personalunterlagen stehe auch entgegen, dass damit Zugang zu Informationen ohne Bezug zur kommunalen Haushaltsführung gewährt würde. Dazu zählten etwa Informationen über die Steuerklassen einzelner Bediensteter oder über die Verwendung vermögensbildender Leistungen ebenso wie Abmahnungen oder (ältere) dienstliche Beurteilungen.

Der Rechnungsprüfungsausschuss beharrte dagegen auf einem umfassenden Einsichtsrecht. Diese Einsicht sei zur Wahrnehmung seiner Prüfungsaufgabe erforderlich.

12.5.2 Rechtliche Bewertung

Ausgangspunkt für den Interessenausgleich sind die **Vorschriften der Gemeindeordnung über die Rechnungsprüfung**. Art. 106 Abs. 6 Satz 1 GO verpflichtet die Gemeinden, den Organen der Rechnungsprüfung Unterlagen, die diese zur Erfüllung ihrer Aufgaben für erforderlich halten, vorzulegen oder zu übersenden:

Art. 106 GO
Inhalt der Rechnungs- und Kassenprüfungen
(1) Die Rechnungsprüfung erstreckt sich auf die Einhaltung der für die Wirtschaftsführung geltenden Vorschriften und Grundsätze, insbesondere darauf, ob

1. die Haushaltssatzung und der Haushaltsplan eingehalten worden sind,
2. die Einzahlungen und Auszahlungen sowie Erträge und Aufwendungen beziehungsweise die Einnahmen und Ausgaben begründet und belegt sind sowie der Jahresabschluss und der konsolidierte Jahresabschluss beziehungsweise die Jahresrechnung sowie die Vermögensnachweise ordnungsgemäß aufgestellt sind,
3. wirtschaftlich und sparsam verfahren wird,
4. die Aufgaben mit geringerem Personal- oder Sachaufwand oder auf andere Weise wirksamer erfüllt werden können.

[...]

(6) [1]Die Organe der Rechnungsprüfung der Gemeinde und das für sie zuständige überörtliche Prüfungsorgan können verlangen, dass ihnen oder ihren beauftragten Prüfern Unterlagen, die sie zur Erfüllung ihrer Aufgaben für erforderlich halten, vorgelegt oder ihnen innerhalb einer bestimmten Frist übersandt werden. [2]Auskünfte sind ihnen oder ihren beauftragten Prüfern zu erteilen. [3]Die Auskunftspflicht nach den Sätzen 1 und 2 besteht auch, soweit hierfür in anderen Bestimmungen eine besondere Rechtsvorschrift gefordert wird, und umfasst auch elektronisch gespeicherte Daten sowie deren automatisierten Abruf.

Das Gesetz räumt den Rechnungsprüfungsorganen damit ein **umfassendes Einsichtsrecht in Bezug auf Dateien und Akten** ein, auch soweit diese Sozial- oder Personaldaten enthalten, wenn die Rechnungsprüfungsorgane ihre Kenntnis zur Erfüllung ihrer Aufgaben für erforderlich halten (vgl. Landtags-Drucksache 15/1063, S 21). Der Gesetzgeber nimmt somit **grundsätzlich** einen **Vorrang des öffentlichen Interesses an einer umfassenden Rechnungsprüfung gegenüber persönlichen Vertraulichkeitsbelangen** an.

Bereits aus der gesetzlichen Formulierung des Art. 106 Abs. 6 Satz 1 GO ergibt sich jedoch, dass auch die **Rechnungsprüfungsorgane** dem allgemeinen Grundsatz der Datensparsamkeit verpflichtet sind (vgl. Art. 5 Abs. 1 Buchst. c DSGVO). Sie haben **kein generelles, voraussetzungsloses Einsichtsrecht, sondern in jedem Einzelfall konkret darzulegen, dass die Kenntnis der geforderten Daten für ihre Aufgabenerfüllung erforderlich ist.**

Deshalb musste der Rechnungsprüfungsausschuss auch im geschilderten Fall jeweils darlegen, dass die Kenntnis der geforderten personenbezogenen statt der angebotenen anonymisierten Daten für seine Aufgabenerfüllung erforderlich war. Nur wenn der Rechnungsprüfungsausschuss **plausibel erläutern** kann, weshalb etwa auch der umfassende Einblick in (ältere) dienstliche Beurteilungen, in die Verwendung vermögenswirksamer Leistungen oder in bestimmte, steuerlich relevante Daten der Bediensteten objektiv geeignet und angemessen ist, um den jeweiligen Prüfungsauftrag zu erfüllen, ist die Gemeindeverwaltung verpflichtet, diese Unterlagen umfassend vorzulegen.

Allerdings ist es vorrangig die Aufgabe des Rechnungsprüfungsausschusses, die Erforderlichkeit der Akteneinsicht zu beurteilen (siehe die Formulierung in Art. 106 Abs. 6 Satz 1 GO „für erforderlich halten"). Nur **in Fällen offensichtlich fehlender Erforderlichkeit** kann daher eine **Verweigerung der Herausgabe von angeforderten Unterlagen** in Betracht kommen.

Nichts anderes ergibt sich aus der personalaktenrechtlichen Regelung des Art. 103 Satz 3 Bayerisches Beamtengesetz (BayBG), die als allgemein gültige Schutzvorschrift für alle öffentlichen Bediensteten grundsätzlich auch auf die

nicht-verbeamteten Beschäftigten des bayerischen öffentlichen Dienstes entsprechend anzuwenden ist. Nach dieser Vorschrift dürfen Personalaktendaten „zu Zwecken der Rechnungsprüfung verarbeitet werden". Auch dieses Prüfungsrecht muss allerdings im Lichte des Grundsatzes der Datensparsamkeit gesehen werden. Art. 103 Satz 3 BayBG gibt den Rechnungsprüfungsorganen somit im Ergebnis kein über Art. 106 Abs. 6 Satz 1 GO hinausgehendes Einsichtsrecht in Personalakten.

Das **Einsichts- und Auskunftsrecht** steht im Übrigen **nur dem Rechnungsprüfungsausschuss als solchem und nicht einzelnen Mitgliedern** zu.

13 E-Government, Telemedienrecht, Soziale Medien

13.1 Soziale Medien, insbesondere Soziale Netzwerke

Die Nutzung Sozialer Medien durch bayerische öffentliche Stellen habe ich bereits in meinem 25. Tätigkeitsbericht 2012 unter Nr. 1.3, in meinem 26. Tätigkeitsbericht 2014 unter Nr. 12.4 und in meinem 27. Tätigkeitsbericht 2016 unter Nr. 12.4 behandelt. Auf dieser Basis habe ich grundsätzlich auch in diesem Berichtszeitraum bayerische öffentliche Stellen zur Nutzung Sozialer Medien beraten beziehungsweise die Nutzung stichprobenartig geprüft.

Zum Betrieb einer Facebook Fanpage hatte das Bundesverwaltungsgericht bereits 2016 ein bei ihm anhängiges Revisionsverfahren ausgesetzt und dem Europäischen Gerichtshof (EuGH) Fragen zur Vorabentscheidung vorgelegt (Beschluss vom 25. Februar 2016, Az.: 1 C 28.14). Der Europäische Gerichtshof hat die Vorlagefragen des Bundesverwaltungsgerichts nun mit Urteil vom 5. Juni 2018, Az.: C-210/16, beantwortet. Mit dieser Entscheidung ist das Ausgangsverfahren jedoch nicht beendet. Vielmehr ist nun wieder das Bundesverwaltungsgericht berufen, das dort anhängige Verfahren weiter zu führen. Wann das Bundesverwaltungsgericht entscheiden wird, ist derzeit nicht absehbar.

Die Verwaltungsstreitsache begann 2011, als sich die Wirtschaftsakademie Schleswig-Holstein GmbH gegen eine Anordnung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein wandte, das in diesem Bundesland die Aufgaben der Datenschutz-Aufsichtsbehörde wahrnimmt. Das Unternehmen vertrat die Auffassung, es dürfe eine Facebook-Fanpage betreiben, ohne sich darum kümmern zu müssen, ob Facebook Datenschutzrecht einhält. Insbesondere habe es keinerlei datenschutzrechtliche (Mit-) Verantwortung etwa für die Verarbeitung von Nutzungsdaten der Fanpage-Besucher. Der Europäische Gerichtshof stellte in seiner Entscheidung klar, dass diese Auffassung nicht mit dem europäischem Datenschutzrecht vereinbar ist:

„Der Umstand, dass ein Betreiber einer Fanpage die von Facebook eingerichtete Plattform nutzt, um die dazugehörigen Dienstleistungen in Anspruch zu nehmen, kann diesen nämlich nicht von der Beachtung seiner Verpflichtungen im Bereich des Schutzes personenbezogener Daten befreien."

Unabhängig von der noch ausstehenden Entscheidung des Bundesverwaltungsgerichts bin ich bereits nach dem Urteil des Europäischen Gerichtshofs auf verschiedenen Ebenen tätig geworden.

So hat die Datenschutzkonferenz unter meiner Mitwirkung zeitnah folgende Entschließung veröffentlicht:

Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 6. Juni 2018

Die Zeit der Verantwortungslosigkeit ist vorbei: EuGH bestätigt gemeinsame Verantwortung von Facebook und Fanpage-Betreibern

Die unabhängigen Datenschutzbehörden des Bundes und der Länder begrüßen das Urteil des Europäischen Gerichtshofs (EuGH) vom 5. Juni 2018, das ihre langjährige Rechtsauffassung bestätigt. Das Urteil des EuGH zur gemeinsamen Verantwortung von Facebook und den Betreibern einer Fanpage hat unmittelbare Auswirkungen auf die Seitenbetreiber. Diese können nicht mehr allein auf die datenschutzrechtliche Verantwortung von Facebook verweisen, sondern sind selbst mitverantwortlich für die Einhaltung des Datenschutzes gegenüber den Nutzenden ihrer Fanpage.

Dabei müssen sie die Verpflichtungen aus den aktuell geltenden Regelungen der Datenschutz-Grundverordnung (DS-GVO) beachten. Zwar nimmt das Urteil Bezug auf die frühere Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr, doch die vom EuGH festgestellte Mitverantwortung der Seitenbetreiber erstreckt sich auf das jeweils geltende Recht, insbesondere auf die in der DS-GVO festgeschriebenen Rechte der Betroffenen und Pflichten der Verarbeiter.

Im Einzelnen ist Folgendes zu beachten:

- *Wer eine Fanpage besucht, muss transparent und in verständlicher Form darüber informiert werden, welche Daten zu welchen Zwecken durch Facebook und die Fanpage-Betreiber verarbeitet werden. Dies gilt sowohl für Personen, die bei Facebook registriert sind, als auch für nicht registrierte Besucherinnen und Besucher des Netzwerks.*
- *Betreiber von Fanpages sollten sich selbst versichern, dass Facebook ihnen die Informationen zur Verfügung stellt, die zur Erfüllung der genannten Informationspflichten benötigt werden.*
- *Soweit Facebook Besucherinnen und Besucher einer Fanpage durch Erhebung personenbezogener Daten trackt, sei es durch den Einsatz von Cookies oder vergleichbarer Techniken oder durch die Speicherung der IP-Adresse, ist grundsätzlich eine Einwilligung der Nutzenden erforderlich, die die Anforderung der DS-GVO erfüllt.*
- *Für die Bereiche der gemeinsamen Verantwortung von Facebook und Fanpage-Betreibern ist in einer Vereinbarung festzulegen, wer von ihnen welche Verpflichtung der DS-GVO erfüllt. Diese Vereinbarung muss in wesentlichen Punkten den Betroffenen zur Verfügung gestellt werden, damit diese ihre Betroffenenrechte wahrnehmen können.*

Für die Durchsetzung der Datenschutzvorgaben bei einer Fanpage ist die Aufsichtsbehörde zuständig, die für das jeweilige Unternehmen oder die Behörde zuständig ist, die die Fanpage betreibt. Die Durchsetzung der Datenschutzvorgaben im Verantwortungsbereich von Facebook selbst obliegt primär der irischen Datenschutzaufsicht im Rahmen der europäischen Zusammenarbeit.

Die deutschen Aufsichtsbehörden weisen darauf hin, dass nach dem Urteil des EuGH dringender Handlungsbedarf für die Betreiber von Fanpages besteht. Dabei ist nicht zu verkennen, dass die Fanpage-Betreiber ihre datenschutzrechtlichen

Verantwortung nur erfüllen können, wenn Facebook selbst an der Lösung mitwirkt und ein datenschutzkonformes Produkt anbietet, das die Rechte der Betroffenen wahrt und einen ordnungsgemäßen Betrieb in Europa ermöglicht.

Im Juni 2018 habe ich zeitnah die Staatskanzlei und die Staatsministerien über die gefasste Entschließung informiert. Dabei habe ich darauf hingewiesen, dass Fanpage-Betreiber ihre datenschutzrechtliche Verantwortung zwar nur erfüllen können, wenn Facebook selbst an der Lösung mitwirkt. Doch können bayerische öffentliche Stellen nicht untätig bleiben, wenn sie zukünftig Fanpages betreiben wollen. Als einen maßgeblichen Schritt habe ich dabei das Einfordern der in der Entschließung genannten Vereinbarung nach Art. 26 DSGVO zur Festlegung der jeweiligen Verpflichtungen gesehen. Zudem habe ich auch an meine – fortgeltende – Empfehlung an bayerische öffentliche Stellen erinnert, keine Fanpages zu betreiben, jedenfalls solange, bis sichergestellt ist, dass ein Betrieb von Fanpages datenschutzkonform möglich ist.

Das (damalige) Bayerische Staatsministerium des Innern und für Integration als für den Datenschutz federführendes Ressort habe ich gebeten, entsprechende Schritte innerhalb der bayerischen Verwaltung zu koordinieren und mit Facebook Kontakt aufzunehmen.

Weiterhin habe ich in der von der Datenschutzkonferenz eingerichteten Task Force Fanpage mitgearbeitet. Facebook hatte auf das Urteil des Europäischen Gerichtshofs vom 5. Juni 2018 und auch auf die Entschließung der Datenschutzkonferenz vom 6. Juni 2018 hin über Monate nicht ersichtlich reagiert. Daher hat die Task Force Fanpage folgenden Beschluss der Datenschutzkonferenz vorbereitet:

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 5. September 2018

Beschluss der DSK zu Facebook Fanpages

Mit Urteil vom 5. Juni 2018 hat der Gerichtshof der Europäischen Union (EuGH), Aktenzeichen C-210/16, entschieden, dass eine gemeinsame Verantwortlichkeit von Facebook-Fanpage-Betreiberinnen und Betreibern und Facebook besteht. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in ihrer Entschließung vom 6. Juni 2018 deutlich gemacht, welche Konsequenzen sich aus dem Urteil für die gemeinsam Verantwortlichen – insbesondere für die Betreiberinnen und Betreiber einer Fanpage – ergeben.

Bei einer gemeinsamen Verantwortlichkeit fordert die Datenschutz-Grundverordnung (DSGVO) unter anderem eine Vereinbarung zwischen den Beteiligten, die klarstellt, wie die Pflichten aus der DSGVO erfüllt werden.

Seit dem Urteil des EuGH sind drei Monate vergangen. Zwar hat Facebook einige Änderungen in seinem Angebot – zum Beispiel bezüglich der Cookies – vorgenommen, doch weiterhin werden auch bei Personen, die keine Facebook-Nutzerinnen und Nutzer sind, Cookies mit Identifikatoren gesetzt, jedenfalls wenn sie über die bloße Startseite einer Fanpage hinaus dort einen Inhalt aufrufen.

Auch werden nach wie vor die Fanpage-Besuche von Betroffenen nach bestimmten, teilweise voreingestellten Kriterien im Rahmen einer sogenannten Insights-

Funktion von Facebook ausgewertet und den Betreiberinnen und Betreibern zur Verfügung gestellt.

Der EuGH hat unter anderem hervorgehoben, dass „die bei Facebook unterhaltenen Fanpages auch von Personen besucht werden können, die keine Facebook-Nutzer sind und somit nicht über ein Benutzerkonto bei diesem sozialen Netzwerk verfügen. In diesem Fall erscheint die Verantwortlichkeit des Betreibers der Fanpage hinsichtlich der Verarbeitung der personenbezogenen Daten dieser Personen noch höher, da das bloße Aufrufen der Fanpage durch Besucher automatisch die Verarbeitung ihrer personenbezogenen Daten auslöst."

Offizielle Verlautbarungen vonseiten Facebooks, ob und welche Schritte unternommen werden, um einen rechtskonformen Betrieb von Facebook-Fanpages zu ermöglichen, sind bisher ausgeblieben. Eine von Facebook noch im Juni 2018 angekündigte Vereinbarung nach Art. 26 DSGVO (Gemeinsam für die Verarbeitung Verantwortliche) wurde bislang nicht zur Verfügung gestellt. Die deutschen Datenschutzaufsichtsbehörden wirken daher auf europäischer Ebene auf ein abgestimmtes Vorgehen gegenüber Facebook hin.

Auch Fanpage-Betreiberinnen und Betreiber müssen sich ihrer datenschutzrechtlichen Verantwortung stellen. Ohne Vereinbarung nach Art. 26 DSGVO ist der Betrieb einer Fanpage, wie sie derzeit von Facebook angeboten wird, rechtswidrig.

Daher fordert die DSK, dass nun die Anforderungen des Datenschutzrechts beim Betrieb von Fanpages erfüllt werden. Dazu gehört insbesondere, dass die gemeinsam Verantwortlichen Klarheit über die derzeitige Sachlage schaffen und die erforderlichen Informationen den betroffenen Personen (= Besucherinnen und Besucher der Fanpage) bereitstellen.

Eine gemeinsame Verantwortlichkeit bedeutet allerdings auch, dass Fanpage-Betreiberinnen und Betreiber (unabhängig davon, ob es sich um öffentliche oder nicht-öffentliche Verantwortliche handelt) die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und dies nachweisen können. Zudem können Betroffene ihre Rechte aus der DSGVO bei und gegenüber jedem Verantwortlichen geltend machen (Art. 26 Abs. 3 DSGVO).

Insbesondere die im Anhang aufgeführten Fragen müssen deshalb sowohl von Facebook als auch und von Fanpage-Betreiberinnen und Betreibern beantwortet werden können.

Anhang: Fragenkatalog

1. *In welcher Art und Weise wird zwischen Ihnen und anderen gemeinsam Verantwortlichen festgelegt, wer von Ihnen welche Verpflichtung gemäß der DSGVO erfüllt? (Art. 26 Abs. 1 DSGVO)*
2. *Auf Grundlage welcher Vereinbarung haben Sie untereinander festgelegt, wer welchen Informationspflichten nach Art. 13 und 14 DSGVO nachkommt?*
3. *Auf welche Weise werden die wesentlichen Aspekte dieser Vereinbarung den betroffenen Personen zur Verfügung gestellt?*
4. *Wie stellen Sie sicher, dass die Betroffenenrechte (Art. 12 ff. DSGVO) erfüllt werden können, insbesondere die Rechte auf Löschung nach Art. 17 DSGVO, auf Einschränkung der Verarbeitung nach Art. 18 DSGVO, auf Widerspruch nach Art. 21 DSGVO und auf Auskunft nach Art. 15 DSGVO?*

5. *Zu welchen Zwecken und auf welcher Rechtsgrundlage verarbeiten Sie die personenbezogenen Daten der Besucherinnen und Besucher von Fanpages? Welche personenbezogenen Daten werden gespeichert? Inwieweit werden aufgrund der Besuche von Facebook-Fanpages Profile erstellt oder angereichert? Werden auch personenbezogene Daten von Nicht-Facebook-Mitgliedern zur Erstellung von Profilen verwendet? Welche Löschfristen sind vorgesehen?*
6. *Zu welchen Zwecken und auf welcher Rechtsgrundlage werden beim Erstaufruf einer Fanpage auch bei Nicht-Mitgliedern Einträge im sogenannten Local Storage erzeugt?*
7. *Zu welchen Zwecken und auf welcher Rechtsgrundlage werden nach Aufruf einer Unterseite innerhalb des Fanpage-Angebots ein Session-Cookie und drei Cookies mit Lebenszeiten zwischen vier Monaten und zwei Jahren gespeichert?*
8. *Welche Maßnahmen haben Sie ergriffen, um Ihren Verpflichtungen aus Art. 26 DSGVO als gemeinsam für die Verarbeitung Verantwortlicher gerecht zu werden und eine entsprechende Vereinbarung abzuschließen?*

Am 11. September 2018 veröffentlichte Facebook in seinem Internet-Auftritt sowohl eine „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“ als auch „Informationen zu Seiten-Insights“.

Es ist anzunehmen, dass Facebook damit seinen Verpflichtungen aus Art. 26 DSGVO nachkommen möchte, auch wenn ein ausdrücklicher Verweis auf die Vorschrift fehlt.

Die von Facebook veröffentlichten Informationen lassen allerdings weiterhin viele Fragen offen. Es bestehen erhebliche Zweifel, ob die veröffentlichten Informationen den Anforderungen an eine Vereinbarung gemäß Art. 26 DSGVO genügen. Die gemeinsame Verantwortlichkeit hat außerdem zur Folge, dass auch Fanpage-Betreiber die Rechtmäßigkeit der (gemeinsam) zu verantwortenden Datenverarbeitung gewährleisten und dies nachweisen können müssen. Jedoch hat Facebook offenbar schon die Datenverarbeitungen im Zusammenhang mit Seiten-Insights nicht umfassend dargestellt. Denn der veröffentlichten Auflistung hat Facebook den Passus „werden Informationen wie die folgenden erfasst und verwendet“ vorangestellt. Der genaue Umfang der Datenverarbeitungen spielt jedoch auch eine Rolle für die Beurteilung, ob und gegebenenfalls auf welcher Rechtsgrundlage eine Fanpage betrieben werden kann.

Mir war es zudem ein Anliegen, dass die im Zusammenhang mit dem Betrieb einer Fanpage auftretenden Themen auch auf europäische Ebene vorangebracht werden. Unter anderem die Social Media Subgroup des Europäischen Datenschutzausschusses befasst sich nun ebenfalls mit der Thematik.

Ich werde mich auch weiterhin dafür einsetzen, gezielt auf Facebook einzuwirken. Unabhängig davon bleiben bayerische öffentliche Stellen in der Pflicht, ihre Nutzung Sozialer Medien, insbesondere den Betrieb von Fanpages, kritisch zu überprüfen. Der schon bislang hohe Beratungsbedarf hierzu wird sich im kommenden Berichtszeitraum voraussichtlich fortsetzen.

Auch anlässlich des Datenskandals um Facebook und Cambridge Analytica hat die Datenschutzkonferenz Konsequenzen gefordert:

Entschließung der 95. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 26. April 2018

Facebook-Datenskandal – Neues Europäisches Datenschutzrecht bei Sozialen Netzwerken durchsetzen!

Im März 2018 wurde in der Öffentlichkeit bekannt, dass über eine von November 2013 bis Mai 2015 mit Facebook verbundene App nach Angaben des Unternehmens Daten von 87 Millionen Nutzern weltweit, davon 2,7 Millionen Europäern und etwa 310.000 Deutschen erhoben und an das Analyseunternehmen Cambridge Analytica weitergeben wurden. Dort wurden sie offenbar auch zur Profilbildung für politische Zwecke verwendet.

Aus diesem Anlass hat der national zuständige Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ein Bußgeldverfahren gegen Facebook eingeleitet. Er steht dabei in engem Austausch mit seinen europäischen Kollegen, insbesondere mit dem Information Commissioner's Office in Großbritannien sowie der Artikel-29-Gruppe. Der Datenskandal um Facebook und Cambridge Analytica wirft ein Schlaglicht auf den Umgang mit Millionen Nutzerdaten. Zudem dokumentieren die Vorgänge um Cambridge Analytica, dass Facebook über Jahre hinweg den Entwicklern von Apps den massenhaften Zugriff auf Daten von mit den Verwendern der Apps befreundeten Facebook-Nutzenden ermöglicht hat. Das geschah ohne eine Einwilligung der Betroffenen. Tatsächlich ist der aktuell diskutierte Fall einer einzelnen App nur die Spitze des Eisbergs. So geht die Zahl der Apps, die das Facebook-Login-System nutzen, in die Zehntausende. Die Zahl der davon rechtswidrig betroffenen Personen dürfte die Dimension des Cambridge-Analytica-Falls in dramatischer Weise sprengen und dem Grunde nach alle Facebook-Nutzenden betreffen. Das Vorkommnis zeigt zudem die Risiken für Profilbildung bei der Nutzung sozialer Medien und anschließendes Mikrotargeting, das offenbar zur Manipulation von demokratischen Willensbildungsprozessen eingesetzt wurde.

Die Datenschutzkonferenz fordert aus diesen offenbar massenhaften Verletzungen von Datenschutzrechten Betroffener folgende Konsequenzen zu ziehen:

- *Soziale Netzwerke müssen ihre Geschäftsmodelle auf die neuen europäischen Datenschutzregelungen ausrichten und ihrer gesellschaftliche Verantwortung nachkommen. Dazu gehört auch, angemessene Vorkehrungen gegen Datenmissbrauch zu treffen.*

- *Facebook muss den wahren Umfang der Öffnung der Plattform für App-Anbieter in den Jahren bis 2015 offenlegen und belastbare Zahlen der eingestellten Apps sowie der von dem Facebook-Login-System betroffenen Personen nennen. Ferner gilt es Betroffene über die Rechtsverletzungen zu informieren.*

- *In Zukunft muss Facebook sicherstellen, dass die Vorgaben der Datenschutz-Grundverordnung (DS-GVO) rechtskonform umgesetzt werden: Die Vorstellung von Facebook zur Einführung der automatischen Gesichtserkennung in Europa lässt erhebliche Zweifel aufkommen, ob das Zustimmungsverfahren mit den gesetzlichen Vorgaben insbesondere zur Einwilligung vereinbar ist. Wenn Facebook die Nutzenden dazu drängt und es*

ihnen wesentlich leichter macht, der biometrischen Datenverarbeitung zuzustimmen, als sich ihr zu entziehen, führt dies zu einer unzulässigen Beeinflussung des Nutzers.

Die Reaktionen auf datenschutzwidriges Verhalten sind dabei nicht allein auf den Vollzug des Datenschutzrechts beschränkt, sondern betreffen auch das Wettbewerbs- und Kartellrecht. Die Forderung nach einer Entflechtung des Facebook-Konzerns wird in dem Maße zunehmen, wie sich dieser durch die systematische Umgehung des Datenschutzes wettbewerbswidrige Vorteile auf dem Markt digitaler Dienstleistungen zu verschaffen versucht. Es bedarf europäischer Initiativen, um monopolartige Strukturen im Bereich der sozialen Netzwerke zu begrenzen und Transparenz von Algorithmen herzustellen.

Weil Datenverarbeitungsprozesse zunehmend komplexer und für Betroffene intransparenter werden, kommt der Datenschutzaufsicht eine elementare Rolle zu. Ihre fachliche Expertise ist gefragt, sie muss organisatorisch und personell in der Lage sein, beratend und gestaltend tätig zu sein. Ein starkes Datenschutzrecht und effektive Aufsichtsbehörden vermindern gemeinsam die Risiken für die Bürgerinnen und Bürger in der digitalen Gesellschaft. Sollten Facebook und andere soziale Netzwerke nicht bereit sein, den europäischen Rechtsvorschriften zum Schutz der Nutzenden nachzukommen, muss dies konsequent durch Ausschöpfung aller vorhandenen aufsichtsbehördlichen Instrumente auf nationaler und europäischer Ebene geahndet werden.

13.2 Geplante ePrivacy-Verordnung

Die in der Datenschutz-Grundverordnung festgelegten allgemeinen Vorschriften sollen bezüglich „elektronischer Kommunikationsdaten“ durch eine Verordnung des Europäischen Parlaments und des Rats über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation, nichtamtlich: ePrivacy-Verordnung) ergänzt und präzisiert werden (siehe auch meine Ausführungen im 27. Tätigkeitsbericht 2016 unter Nr. 12.3). Diese speziellen und damit in ihrem Anwendungsbereich vorrangigen Bestimmungen betreffen unter anderem Datenverarbeitungen beim Betrieb von Webseiten (etwa Analyse und Verfolgen des Nutzerverhaltens) und können daher auch für bayerische Behörden bedeutsam sein.

Die ePrivacy-Verordnung befindet sich allerdings noch im europäischen Gesetzgebungsverfahren. Angesichts der Bedeutung dieser Verordnung informiere ich auf meiner Homepage https://www.datenschutz-bayern.de in der Rubrik „Themengebiete – Internet, Medien und Telekommunikation“ über das laufende Gesetzgebungsverfahren. Der aktuelle Entwurf nennt eine 24-Monate-Frist, die ab Inkrafttreten bis zur unmittelbaren Anwendbarkeit gelten soll.

Damit ergeben sich Fragen zur Anwendbarkeit nationalen Rechts neben der Datenschutz-Grundverordnung. Der Bundesgesetzgeber hat das Telemediengesetz (TMG) bisher nicht an die Datenschutz-Grundverordnung angepasst, doch sind die datenschutzrechtlichen Vorschriften des Telemediengesetzes (Abschnitt 4) weiterhin in Kraft. Für die Rechtsanwender stellt sich wegen des Anwendungsvorrangs der Datenschutz-Grundverordnung daher die Frage, ob die datenschutzrechtlichen Regelungen des Telemediengesetzes weiterhin anwendbar sind. Zur Anwendbarkeit des Telemediengesetzes für nicht-öffentliche Stellen ab dem

25. Mai 2018 veröffentlichte die 95. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder eine Positionsbestimmung. In der Diskussion auf Bundesebene habe ich auf die Besonderheiten für öffentliche Stellen hingewiesen, insbesondere kann Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO für eine durch „Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung" nicht die Rechtmäßigkeit begründen. Zu öffentlichen Stellen soll daher eine gesonderte Veröffentlichung vorbereitet werden.

Positionsbestimmung der 95. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 26. April 2018

Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018

Der Kommissionsentwurf zur ePrivacy-Verordnung vom Januar 2017 sieht vor, dass diese Verordnung, welche die ePrivacy-Richtlinie ersetzen soll, gemeinsam mit der Datenschutz-Grundverordnung (DSGVO) ab dem 25. Mai 2018 in Kraft tritt und Geltung erlangt. Die ePrivacy-Verordnung soll die DSGVO im Hinblick auf die elektronische Kommunikation präzisieren und ergänzen. Das Gesetzgebungsverfahren zur ePrivacy-Verordnung verzögert sich jedoch erheblich, so dass voraussichtlich nicht mehr mit einem Inkrafttreten im Jahr 2018 zu rechnen ist. Damit ergeben sich Fragen zur Anwendbarkeit nationalen Rechts neben der DSGVO. Der Gesetzgeber hat das Telemediengesetz (TMG) bisher nicht an die DSGVO angepasst, so dass die datenschutzrechtlichen Vorschriften des TMG (Abschnitt 4) voraussichtlich ab dem 25. Mai 2018 unverändert in Kraft sein werden. Für die Rechtsanwender stellt sich wegen des Anwendungsvorrangs der DSGVO daher die Frage, ob die datenschutzrechtlichen Regelungen des TMG weiterhin anwendbar sein werden.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vertritt hierzu folgende Position:

1. *Im Verhältnis zum nationalen Recht kommt ab dem 25. Mai 2018 die DSGVO für sämtliche automatisierte Verarbeitungen personenbezogener Daten vorrangig zur Anwendung, es sei denn nationale Vorschriften sind aufgrund einer Kollisions-regel, eines Umsetzungsauftrages oder einer Öffnungsklausel der DSGVO vorrangig anwendbar.*
2. *Die DSGVO enthält in Artikel 95 eine Kollisionsregel zum Verhältnis der DSG-VO zur ePrivacy-Richtlinie, wonach natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union durch die DSGVO keine zusätzlichen Pflichten auferlegt werden, soweit sie besonderen in der ePrivacy-Richtlinie festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.*
3. *Die Vorschrift des Artikels 95 DSGVO findet keine Anwendung auf die Regelungen im 4. Abschnitt des TMG. Denn diese Vorschriften stellen vorrangig eine Umsetzung der durch die DSGVO aufgehobenen Datenschutzrichtlinie dar und unterfallen – da sie auch nicht auf der Grundlage von Öffnungsklauseln in der DSGVO beibehalten werden dürfen – demgemäß dem Anwendungsvorrang der DSGVO. Hiervon betroffen sind damit auch etwaige unvollständige Umsetzungen der ePrivacy-Richtlinie in diesem Abschnitt, welche jedenfalls isoliert nicht mehr bestehen bleiben können.*

4. *Damit können die §§ 12, 13, 15 TMG bei der Beurteilung der Rechtmäßigkeit der Reichweitenmessung und des Einsatzes von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen, ab dem 25. Mai 2018 nicht mehr angewendet werden.*
5. *Eine unmittelbare Anwendung der ePrivacy-Richtlinie für die unter Ziffer 4 genannten Verarbeitungsvorgänge kommt nicht in Betracht (keine horizontale unmittelbare Wirkung von Richtlinien).*
6. *Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch Diensteanbieter von Telemedien kommt folglich nur Artikel 6 Absatz 1, insbesondere Buchstaben a), b) und f) DSGVO in Betracht. Darüber hinaus sind die all-gemeinen Grundsätze aus Artikel 5 Absatz 1 DSGVO, sowie die besonderen Vorgaben z. B. aus Artikel 25 Absatz 2 DSGVO einzuhalten.*
7. *Verarbeitungen, die unbedingt erforderlich sind, damit der Anbieter den von den betroffenen Personen angefragten Dienst zur Verfügung stellen kann, können ggf. auf Art. 6 Absatz 1 Buchstabe b) oder Buchstabe f) DSGVO gestützt werden.*
8. *Ob und inwieweit weitere Verarbeitungstätigkeiten rechtmäßig sind, muss durch eine Interessenabwägung im Einzelfall auf Grundlage des Artikel 6 Absatz 1 Buchstabe f) DSGVO geprüft werden.*
9. *Es bedarf jedenfalls einer vorherigen Einwilligung beim Einsatz von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen und bei der Erstellung von Nutzerprofilen. Das bedeutet, dass eine informierte Einwilligung i. S. d. DSGVO, in Form einer Erklärung oder sonstigen eindeutig bestätigenden Handlung vor der Datenverarbeitung eingeholt wer-den muss, d. h. z. B. bevor Cookies platziert werden bzw. auf dem Endgerät des Nutzers gespeicherte Informationen gesammelt werden.*

14 Spezielle datenschutzrechtliche Themen

14.1 EU-US Privacy Shield

Zum EU-US Privacy Shield (Privacy Shield) habe ich mich bereits ausführlich in meinem 27. Tätigkeitsbericht 2016 unter Nr. 13.2 geäußert. Am 18. Oktober 2017 veröffentlichte die Europäische Kommission den ersten jährlichen Prüfbericht (Dokument COM(2017) 611 final, im Internet abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=COM:2017:611:FIN). Sie hält weiterhin an ihrer Angemessenheitsentscheidung in Bezug auf Unternehmen fest, die sich den Privacy Shield-Regelungen unterwerfen und entsprechend registriert sind.

Im Berichtszeitraum erhielt ich keine Beschwerden von Bürgerinnen und Bürgern zur Verarbeitung ihrer personenbezogenen Daten spezifisch mit Blick auf die Regelungen des Privacy Shield.

Bei Beratungsanfragen bayerischer öffentlicher Stellen spielte der Privacy Shield hingegen durchaus eine Rolle, insbesondere im Zusammenhang mit Cloud Computing (siehe hierzu auch Nr. 14.2). Neben weiteren Aspekten muss insbesondere in jedem Einzelfall geprüft werden, ob sich das jeweils relevante Unternehmen in den Vereinigten Staaten von Amerika (USA) den Privacy Shield-Regelungen unterworfen hat, und ob es entsprechend registriert ist. Hierzu habe ich anfragende Stellen auf eine im Internet verfügbare Auflistung hingewiesen (https://www.privacyshield.gov/list).

Die Artikel 29-Datenschutzgruppe, Vorgängerin des Europäischen Datenschutzausschusses, sieht im Privacy Shield zwar Verbesserungen gegenüber Safe Harbor und gegenüber der bisherigen Praxis. Sie äußerte in Ihrem Bericht vom 28. November 2017 (WP 255, im Internet abrufbar unter https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612621) aber weiterhin Bedenken. Diese Bedenken sollten nach Wunsch der Artikel 29-Datenschutzgruppe grundsätzlich bis zum 25. Mai 2018 ausgeräumt werden, spätestens jedoch bis zur zweiten Überprüfung Ende 2018. Am 18./19. Oktober 2018 trafen sich Vertreter der Europäischen Kommission und der US-Regierung in Brüssel zur zweiten jährlichen Überprüfung. Im Fokus standen kommerzielle Aspekte sowie Datenverarbeitungen durch US-Dienste und Behörden für Zwecke der nationalen Sicherheit.

Dem Europäischen Gerichtshof (Az.: C-311/18) wurden bereits die Fragen vorgelegt, ob die Angemessenheitsentscheidung im EU-US Datenschutzschild bindende Wirkung für die Aufsichtsbehörden entfalte (Vorlagefrage 9), und ob die bestehenden Regelungen der USA zur Einrichtung einer Privacy Shield-Ombudsstelle ausreichend seien (Vorlagefrage 10). Zu diesem sogenannten Schrems II-Verfahren siehe die Information im ABl. C 249 vom 16. Juli 2018, S. 15, im Internet abrufbar unter https://eur-lex.europa.eu/.

Die weitere Entwicklung bleibt abzuwarten.

Auf meiner Homepage https://www.datenschutz-bayern.de berichte ich hierzu aktuell unter „Themengebiete – Internationaler Datenverkehr – EU-US Privacy Shield“ und halte weitere Informationen für bayerische öffentliche Stellen sowie für betroffene Personen vor.

14.2 Cloud Computing

Zum Cloud Computing habe ich mich schon in meinem 24. Tätigkeitsbericht 2010 unter Nr. 2.1.5, in meinem 25. Tätigkeitsbericht 2012 unter Nr. 1.2 und 2.3.3, in meinem 26. Tätigkeitsbericht 2014 unter Nr. 13.1 und in meinem 27. Tätigkeitsbericht 2016 unter Nr. 13.3 kritisch geäußert.

Auch im Berichtszeitraum erreichten mich zahlreiche Anfragen, vor allem von Schulen und Kommunen. Bei den Angeboten ist unter anderem zu berücksichtigen, ob der Dienstleister seine Leistung im Inland, im europäischen Ausland oder aber in einem Staat außerhalb der Europäischen Union beziehungsweise des Europäischen Wirtschaftsraums (und damit in einem sogenannten Drittland) erbringt. Den Schwerpunkt bildeten Verträge mit Anbietern aus den Vereinigten Staaten von Amerika (USA). Häufig musste ich auf Widersprüche der vorgelegten Verträge zu den Werbeaussagen der Anbieter hinweisen.

Ich wiederhole daher meine schon bislang ausgesprochene Empfehlung an bayerische öffentliche Stellen, auf die Nutzung von Public-Cloud-Diensten mit (auch nur eventuellen) Datenverarbeitungen in den USA zu verzichten und nach anderen, nationalen oder auch europäischen Lösungen zu suchen.

Bei entsprechenden Anfragen verweise ich im Übrigen regelmäßig auf das IT-Grundschutz-Kompendium des Bundesamts für Sicherheit in der Informationstechnik. Dort heißt es unter APP.1.1.A12: „Die in einigen Office-Produkten integrierten Cloud-Speicher-Funktionen SOLLTEN grundsätzlich deaktiviert werden. Alle Cloud-Laufwerke SOLLTEN deaktiviert werden. Alle Dokumente SOLLTEN auf zentral verwalteten File-Servern der Institution gespeichert werden. Um Dokumente für Dritte zur Sichtung oder Bearbeitung freizugeben, SOLLTEN spezialisierte Anwendungen wie beispielsweise geeignete Datenräume eingesetzt werden, die über Sicherheitsfunktionen wie eine verschlüsselte Datenablage und -versendung und ein geeignetes System zur Benutzer- und Rechteverwaltung verfügen.“

Das IT-Grundschutz-Kompendium des Bundesamts für Sicherheit in der Informationstechnik kann im Internet unter https://www.bsi.bund.de abgerufen werden.

Die Datenschutzaufsichtsbehörden in Deutschland streben insbesondere über Arbeitskreise der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder eine möglichst einheitliche Positionierung zum Einsatz von Microsoft Office 365 in der öffentlichen Verwaltung an. Dabei wurde auch der Kontakt zu Microsoft gesucht, um für eine Bewertung erforderliche Informationen und Unterlagen zu erlangen. Wann ein Ergebnis vorliegen wird, ist derzeit nicht absehbar, zumal zuletzt die Microsoft Cloud Deutschland im Vordergrund stand. Da die Microsoft Cloud Deutschland gemäß eigener Ankündigung von Microsoft für Neukunden nicht mehr zur Verfügung stehen soll, werden bei der Befassung wieder andere Angebote von Microsoft Office 365 in den Fokus rücken.

14.3 Einmaliger Meldedatenabgleich zur Erhebung des Rundfunkbeitrags

Regelmäßig erhalte ich Anfragen von Bürgerinnen und Bürgern, die sich gegen eine Übermittlung von Meldedaten an die öffentlich-rechtlichen Rundfunkanstalten und die dann dort vorgenommenen Datenverarbeitungen wenden. Anlass war zuletzt vielfach der im Jahr 2018 durchgeführte allgemeine Meldedatenabgleich.

Es handelte sich insoweit um die Durchführung eines „einmaligen" Abgleichs der Daten aller volljährigen Bürger, für den als Stichtag der 6. Mai 2018 festgelegt wurde. Aufgrund des Umfangs der Datenmenge beinhaltete die Planung die sukzessive Übermittlung der entsprechenden Daten an den Beitragsservice im Zeitraum vom 7. Mai bis 3. Juli 2018.

Rechtsgrundlage für diesen 2018 durchgeführten Meldedatenabgleich ist § 14 Abs. 9a Rundfunkbeitragsstaatsvertrag (RBStV). Ziel der Regelung war es, den Rundfunkanstalten ein geeignetes Instrumentarium zur Verfügung zu stellen, um ihren Datenbestand zu sichern und strukturelle Erhebungs- und Vollzugsdefizite zu beseitigen.

Ein solcher Meldedatenabgleich erfolgte nach einer ersten Durchführung im Jahr 2013 nun zum zweiten Mal, wobei Rechtsgrundlage für den Abgleich im Jahr 2013 § 14 Abs. 9 RBStV war.

§ 14 RBStV
Übergangsbestimmungen
(9) [1]Um einen einmaligen Abgleich zum Zwecke der Bestands- und Ersterfassung zu ermöglichen, übermittelt jede Meldebehörde für einen bundesweit einheitlichen Stichtag automatisiert innerhalb von längstens zwei Jahren ab dem Inkrafttreten dieses Staatsvertrages gegen Kostenerstattung einmalig in standardisierter Form die nachfolgenden Daten aller volljährigen Personen an die jeweils zuständige Landesrundfunkanstalt:

1. *Familienname,*
2. *Vornamen unter Bezeichnung des Rufnamens,*
3. *frühere Namen,*
4. *Doktorgrad,*
5. *Familienstand,*
6. *Tag der Geburt,*
7. *gegenwärtige und letzte Anschrift von Haupt- und Nebenwohnungen, einschließlich aller vorhandenen Angaben zur Lage der Wohnung, und*
8. *Tag des Einzugs in die Wohnung.*

[2]Hat die zuständige Landesrundfunkanstalt nach dem Abgleich für eine Wohnung einen Beitragsschuldner festgestellt, hat sie die Daten der übrigen dort wohnenden Personen unverzüglich zu löschen, sobald das Beitragskonto ausgeglichen ist. [3]Im Übrigen darf sie die Daten zur Feststellung eines Beitragsschuldners für eine Wohnung nutzen, für die bislang kein Beitragsschuldner festgestellt wurde; Satz 2 gilt entsprechend. [4]Die Landesrundfunkanstalt darf die Daten auch zur Aktualisierung oder Ergänzung von bereits vorhandenen Teilnehmerdaten nutzen. [5] § 11 Abs. 6 Satz 2 und 3 gilt entsprechend.
(9a) [1]Zur Sicherstellung der Aktualität des Datenbestandes wird zum 1. Januar 2018 ein weiterer Abgleich entsprechend Absatz 9 durchgeführt. [2]Die Meldebehörden übermitteln die Daten bis längstens 31. Dezember 2018. [3]Im Übrigen gelten Absatz 9 Satz 1 bis 4 und § 11 Abs. 6 Satz 2 und 3 entsprechend. [4]Der Abgleich wird nach seiner Durchführung evaluiert. [5]Die Landesrundfunkanstalten stellen den Ländern hierfür die erforderlichen Informationen zur Verfügung.

Daneben können die Meldebehörden dem Bayerischen Rundfunk beziehungsweise dem Beitragsservice zu bestimmten Anlässen (bei Anmeldungen, Abmeldungen oder Todesfällen) einen festgelegten Datensatz übermitteln. Rechtsgrundlage für diese regelmäßige Übermittlung ist der auf Grund von § 36 Abs. 1 Bundesmeldegesetz und Art. 10 Nr. 4 Bayerisches Gesetz zur Ausführung des Bundesmeldegesetzes erlassene § 35 Abs. 1 Verordnung zur Übermittlung von Meldedaten. Die übermittelten Daten dürfen nur für Zwecke der Beitragserhebung sowie zur Feststellung, ob eine Beitragspflicht nach dem Rundfunkbeitragsstaatsvertrag besteht, verarbeitet werden. Die Übermittlung der Daten durch die Meldebehörden ist in beiden Fallkonstellationen zulässig (siehe auch meinen 27. Tätigkeitsbericht 2016 unter Nr. 6.17).

Viele Bürgerinnen und Bürger haben sich ausdrücklich im Hinblick auf die Datenverarbeitungen durch den Bayerischen Rundfunk beziehungsweise durch den Beitragsservice an mich gewandt. Mangels Aufsichtszuständigkeit für die Datenverarbeitungen dieser Stellen konnte ich in solchen Fällen nur allgemeine Hinweise geben und im Übrigen an die zuständigen Datenschutzbeauftragten des Bayerischen Rundfunks beziehungsweise des Beitragsservice verweisen.

14.4 Datenschutz beim Mikrozenzus

Seit 1957 versorgt der Mikrozensus als amtliche Repräsentativstatistik politisch und wirtschaftlich Verantwortliche sowie die Öffentlichkeit mit Zahlen zur sozialen und wirtschaftlichen Lage der Bevölkerung. Jährlich ist ein Prozent aller Haushalte in Deutschland beteiligt. Von anderen Haushaltsbefragungen unterscheidet sich der Mikrozensus durch die vom Gesetzgeber vorgesehene Auskunftspflicht. Das Gesetz zur Durchführung einer Repräsentativstatistik über die Bevölkerung und die Arbeitsmarktbeteiligung sowie die Wohnsituation der Haushalte (Mikrozensusgesetz – MZG) wurde durch das Gesetz zur Neuregelung des Mikrozensus und zur Änderung weiterer Statistikgesetze geändert und als Artikel 1 des Gesetzes vom 7. Dezember 2016 (BGBl. I S. 2826) vom Bundestag neu beschlossen. Im Gegensatz zu den bisherigen Mikrozensusgesetzen ist eine zeitliche Befristung nicht mehr vorgesehen. Zudem wurden weitere, nach europäischem Recht vorgegebene statistische Erhebungen integriert. Das neue Mikrozensusgesetz trat am 1. Januar 2017 in Kraft (zum Mikrozensusgesetz 2005 siehe meine Ausführungen im 23. Tätigkeitsbericht 2008 unter Nr. 23.2)

Einige für die Teilnahme am Mikrozensus ausgewählte Bürgerinnen und Bürger wandten sich im Berichtszeitraum an mich und hinterfragten das Bestehen einer Auskunftspflicht nach § 13 MZG. Die betroffenen Personen habe ich aus datenschutzrechtlicher Sicht auf Folgendes aufmerksam gemacht:

— Das Bundesverfassungsgericht hat in seinem so genannten „Volkszählungsurteil“ vom 15. Dezember 1983, Az.: 1 BvR 209/83 u. a., darauf hingewiesen, dass das Grundrecht des Bürgers auf informationelle Selbstbestimmung nicht schrankenlos gewährleistet ist. Im Urteil vom 19. September 2018, Az.: 2 BvF 1/15 u. a., hielt es das Zensusgesetz 2011 für verfassungsgemäß und führte in diesem Zusammenhang aus, der Gesetzgeber habe auf die bereits vorliegenden Erfahrungen anderer von den statistischen Ämtern des Bundes und der Länder durchgeführter Erhebungen – wie etwa des Mikrozensus – zurückgreifen können.

- Das Erhebungsverfahren ist auf die Gewinnung anonymisierter Daten gerichtet. Der Erhebungsbogen und die einen Personenbezug herstellenden sogenannten „Hilfsmerkmale“ werden nach einer Plausibilitätskontrolle beim Bayerischen Landesamt für Statistik getrennt. Die erhobenen Daten unterliegen dem Statistikgeheimnis und sind von anderen Datenbeständen gesondert zu halten. Fälle einer Missachtung dieser Vorgaben sind mir bislang nicht bekannt geworden.

- Art. 6 Abs. 2 und 3 DSGVO gestatten dem Gesetzgeber, Rechtsgrundlagen für die Datenverarbeitung im öffentlichen Interesse (Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO) festzulegen. Der Mikrozensus dient einem öffentlichen Interesse, nämlich die Basis für politische Entscheidungen in Europa, Bund und Ländern zu finden.

- Darüber hinaus können nach Maßgabe von Art. 89 Abs. 2 DSGVO bei Datenverarbeitungen zu statistischen Zwecken im Recht der Mitgliedstaaten Ausnahmen von den Rechten nach Art. 15, 16, 18 und 21 DSGVO vorgesehen werden.

Im Ergebnis hatte ich in den mir vorgetragenen Fällen keine datenschutzrechtlichen Einwendungen gegen die im Rahmen des Mikrozensus erfolgten Datenerhebungen.

14.5 Vorbereitung der Volkszählung 2021

Der erste registergestützte Zensus (siehe meine Ausführungen in meinem 23. Tätigkeitsbericht 2008 unter Nr. 23.3, in meinem 24. Tätigkeitsbericht 2010 unter Nr. 12.1 und in meinem 25. Tätigkeitsbericht 2012 unter Nr. 12.4) ist abgeschlossen. Das Statistische Bundesamt veröffentlichte am 20. Mai 2016 den Qualitätsbericht nach § 17 Zensusgesetz 2011. Das Bundesverfassungsgericht hat mit Urteil vom 19. September 2018, Az.: 2 BvF 1/15 u. a., entschieden, dass die im dortigen Verfahren angegriffenen Normen des Zensusgesetzes 2011 mit dem Grundgesetz vereinbar sind. Daher ist nunmehr mit einem Gesetzgebungsverfahren zu einem Zensusgesetz 2021 zu rechnen.

Unabhängig davon sind die Vorbereitungen für die Volkszählung 2021 bereits angelaufen.

Am 10. März 2017 trat das vom Bundestag beschlossene, mittlerweile bereits geänderte Gesetz zur Vorbereitung eines registergestützten Zensus einschließlich einer Gebäude- und Wohnungszählung 2021 (Zensusvorbereitungsgesetz 2021) in Kraft.

Die Vorbereitung und die Durchführung der Volkszählung 2021 werde ich aus datenschutzrechtlicher Sicht kritisch begleiten.

15 Datenschutzkommission

Der Datenschutzkommission beim Bayerischen Landtag gehörten im Berichtszeitraum (bis zum Ende der 17. Wahlperiode) folgende Mitglieder und stellvertretende Mitglieder an:

Aus dem Landtag:

Mitglieder:

Eberhard Rotter, CSU
Max Gibis, CSU
Walter Nussel, CSU
Florian Ritter, SPD
Eva Gottstein, FREIE WÄHLER
Verena Osgyan, BÜNDNIS 90/DIE GRÜNEN

Stellvertretende Mitglieder:

Tobias Reiß, CSU
Thorsten Schwab, CSU
Andreas Schalk, CSU
Alexandra Hiersemann, SPD
Bernhard Pohl, FREIE WÄHLER
Ulrike Gote, BÜNDNIS 90/DIE GRÜNEN

Auf Vorschlag der Staatsregierung:

Mitglied:

Dr. Stephan Bobe, Ministerialrat im Staatsministerium der Finanzen, für Landesentwicklung und Heimat

Stellvertretendes Mitglied:

Michael Will, Ministerialrat im Staatsministerium des Innern, für Bau und Verkehr bzw. im Staatsministerium des Innern und für Integration

Auf Vorschlag der kommunalen Spitzenverbände in Bayern:

Mitglied:

Rudolf Schleyer, Mitglied des Vorstands (bis 31. Januar 2018) und Vorstandsvorsitzender (ab 1. Februar 2018) der Anstalt für Kommunale Datenverarbeitung in Bayern

Stellvertretendes Mitglied:

Gudrun Aschenbrenner, Abteilungsleiterin (bis 31. Januar 2018) und Mitglied des Vorstands (ab 1. Februar 2018) der Anstalt für Kommunale Datenverarbeitung in Bayern

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

Mitglied:

Werner Krempl, Erster Direktor und Vorsitzender der Geschäftsführung der Deutschen Rentenversicherung Nordbayern

Stellvertretendes Mitglied:

Dr. Helmut Platzer, Vorstandsvorsitzender der AOK Bayern (bis 31. März 2018)

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

Mitglied:

Dr. Till Schemmann, Notar

Stellvertretendes Mitglied:

Dr. Janusz Rat, Zahnarzt

Herr Eberhard Rotter, MdL, führte den Vorsitz in der Datenschutzkommission; stellvertretender Vorsitzender war Herr Florian Ritter, MdL.

Die Datenschutzkommission beim Bayerischen Landtag tagte im Berichtszeitraum vier Mal.

Anlage 1:
Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

Novellierung des Personalausweisgesetzes – Änderungen müssen bürger- und datenschutzfreundlich realisiert werden!

Die Bundesregierung plant grundlegende Änderungen des Personalausweisrechts. Nach dem vom Bundeskabinett beschlossenen Gesetzentwurf (BR-Drs. 787/16) werden das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger übergangen und Datenschutz sichernde Standards unterlaufen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert daher insbesondere folgende datenschutzrechtliche Anforderungen zu berücksichtigen:

— Die obligatorische Aktivierung der eID-Funktion ist dann hinnehmbar, wenn dauerhaft sichergestellt ist, dass daraus keine verpflichtende Nutzung der eID-Funktion des Personalausweises resultiert. Die Entscheidung über die Nutzung der eID-Funktion muss allein bei den Bürgerinnen und Bürgern liegen. Deren Selbstbestimmungsrecht muss gewahrt bleiben.

— An der bisherigen Verpflichtung der Ausweisbehörden, Bürgerinnen und Bürger über die eID-Funktion des Personalausweises schriftlich zu unterrichten, sollte festgehalten werden. Nur durch eine bundesweit einheitliche Vorgabe zu einer solchen Information wird sichergestellt, dass alle Bürgerinnen und Bürger in hinreichend verständlicher Form aufgeklärt werden.

— Vor einer Datenübermittlung aus dem Personalausweis müssen die Bürgerinnen und Bürger Kenntnis über den Zweck der Übermittlung erhalten; zur Wahrnehmung des Rechts auf informationelle Selbstbestimmung müssen die Betroffenen stets – wie bislang – nachvollziehen können, in welchem konkreten Kontext ihre Identitätsdaten übermittelt werden. Zudem sollte die bisherige Möglichkeit, die Übermittlung einzelner Datenkategorien auszuschließen, beibehalten werden.

— Die Einführung von organisationsbezogenen Berechtigungszertifikaten bei Diensteanbietern wird abgelehnt. Um sicherzustellen, dass Diensteanbieter nur die für den jeweiligen Geschäftsprozess erforderlichen Angaben übermittelt bekommen, sollte an der aktuellen Rechtslage festgehalten werden, nach der der antragstellende Diensteanbieter die Erforderlichkeit der aus der eID-Funktion des Personalausweises zu übermittelnden Angaben nachweisen muss und an den jeweils festgelegten Zweck gebunden ist.

— Berechtigungszertifikate dürfen nur an Diensteanbieter erteilt werden, die Datenschutz und Datensicherheit gewährleisten. Daher sollten antragstellende Diensteanbieter nach wie vor durch eine Selbstverpflichtung die Erfüllung dieser Anforderungen schriftlich bestätigen und nachweisen müssen.

- Die maßgeblichen Regelungen für die mit der Anlegung und Nutzung von Servicekonten einhergehende Erhebung und Verarbeitung von Identitätsdaten aus dem Personalausweis sowie die sicherheitstechnischen Rahmenbedingungen sollten im Personalausweisgesetz getroffen werden.

- Die Voraussetzungen für die Erstellung und Weitergabe von Personalausweisablichtungen sollten gesetzlich konkreter normiert werden. Insbesondere das Prinzip der Erforderlichkeit ist durch eine verpflichtende Prüfung der Notwendigkeit der Anfertigung einer Ablichtung sowie durch eine Positivliste von Erlaubnisgründen zu stärken. Die Einwilligung der Betroffenen als alleinige Voraussetzung birgt die Gefahr, dass in der Praxis Ablichtungen angefertigt werden, obwohl sie nicht erforderlich sind. Zudem dürfte fraglich sein, ob betroffene Personen in eine solche Maßnahme stets informiert und freiwillig einwilligen können.

- Die zum 1. Mai 2021 vorgesehene Einführung eines nahezu voraussetzungslosen Abrufs des Lichtbildes im automatisierten Verfahren durch die Polizeibehörden des Bundes und der Länder sowie die Verfassungsschutzbehörden und Nachrichtendienste wird abgelehnt. Bisher dürfen zur Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten insbesondere die Polizei- und Ordnungsbehörden Lichtbilder automatisiert abrufen, wenn die Personalausweisbehörde nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährdet. Diese gesetzlichen Einschränkungen für das Abrufverfahren sollen nun entfallen. Zudem sollen alle Nachrichtendienste künftig voraussetzungslos Lichtbilddaten abrufen können. Die bisherige Rechtslage ist völlig ausreichend.

Anlage 2: Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

Einsatz externer Dienstleister durch Berufsgeheimnisträger rechtssicher und datenschutzkonform gestalten!

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Bundesgesetzgeber auf, mit dem derzeit vorliegenden Gesetzentwurf der Bundesregierung „zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“ (BR-Drs. 163/17) den Einsatz externer Dienstleister durch Berufsgeheimnisträger rechtsicher und datenschutzkonform zu gestalten.

Die Schweigepflicht ist Grundlage des für die Berufsausübung notwendigen Vertrauensverhältnisses. Aber auch Berufsgeheimnisträger können heute nicht mehr wirtschaftlich agieren, ohne die moderne Informations- und Kommunikationstechnik zu nutzen. Kaum ein Anwalt oder Arzt verfügt über das notwendige Spezialwissen, um diese Technik selbst zu warten und vor ständig neuen Bedrohungen abzusichern. Der vorliegende Gesetzentwurf will deshalb eine Praxis legalisieren, die aus Gründen der Praktikabilität längst etabliert ist.

Der strafrechtliche Schutz von Privatgeheimnissen soll die Beauftragung externer Dienstleister durch Berufsgeheimnisträger nicht länger erschweren. Im Gegenzug

sollen diese Auftragnehmer künftig einer strafrechtlich sanktionierten Verschwiegenheitspflicht unterliegen. Dennoch versäumt es der Gesetzentwurf, insbesondere mit der vorgeschlagenen Formulierung zu § 203 StGB, klare Verhältnisse zu schaffen. Bisher sorgte unter Ärzten – und mitunter sogar Anwälten – der Umstand für Verwirrung, dass das, was datenschutzrechtlich legitim war, noch längst nicht strafrechtlich erlaubt sein musste. Was nach dem Gesetzentwurf nunmehr strafrechtlich erlaubt sein soll, könnte wiederum nach der neuen Europäischen Datenschutz-Grundverordnung mit empfindlichen Bußgeldern in Millionenhöhe sanktioniert werden. Denn es ist weder mit dem Schutzzweck von § 203 StGB vereinbar, noch datenschutzrechtlich zulässig, dass Berufsgeheimnisträger, wie im neuen § 203 StGB vorgesehen, die Verantwortung für die Datenverarbeitung ohne Einwilligung der Betroffenen an externe Dienstleister übertragen. Nicht absehbar ist zudem, ob die Zeugnisverweigerungsrechte und das Beschlagnahmeverbot in einem weiteren Gesetzgebungsverfahren entsprechend weitgehend auf alle denkbaren Dienstleister ausgeweitet werden, die an der Berufsausübung durch Berufsgeheimnisträger mitwirken.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder dringt daher darauf, den Gesetzentwurf nachzubessern und die geplanten straf- und berufsrechtlichen Regelungen mit den datenschutzrechtlichen Vorschriften zu synchronisieren. Es muss Berufsgeheimnisträgern möglich sein, externe Dienstleister zu Rate zu ziehen. Im Sinne der ungestörten Berufsausübung der Berufsgeheimnisträger und des Rechts auf informationelle Selbstbestimmung der Betroffenen sollten die Pflichten, die den Berufsgeheimnisträger dabei aus unterschiedlichen Rechtsgebieten treffen, aber soweit als möglich gleichlaufend ausgestaltet werden.

Anlage 3:
Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

Gesetzesentwurf zur Aufzeichnung von Fahrdaten ist völlig unzureichend!

Die Bundesregierung hat im Januar 2017 einen Entwurf zur Novellierung des Straßenverkehrsgesetzes (BT Drs. 18/11300) vorgelegt, um die Nutzung automatisierter Fahrfunktionen auf Deutschlands Straßen zu erlauben. Dabei sollen Fahrdaten aufgezeichnet werden, anhand derer bewertet werden kann, zu welchem Zeitpunkt das Auto jeweils durch den Fahrer oder durch eine „automatisierte Fahrfunktion“ gesteuert wurde und wann ein Fahrer die Aufforderung zur Übernahme der Steuerung erhalten hat. Ebenfalls aufgezeichnet werden sollen Daten zu technischen Störungen automatisierter Fahrfunktionen. Mit den Daten soll sich nach einem Unfall klären lassen, ob die Technik und damit der Hersteller oder der Fahrer für einen Unfall verantwortlich war. Welche Daten dies sind und wie das Speichermedium ausgestaltet werden soll, regelt der Gesetzentwurf nicht.

Auf Verlangen der nach Landesrecht für Verkehrskontrollen zuständigen Behörden müssen die Fahrdaten diesen Behörden übermittelt werden. Die Fahrdaten sind auch Dritten zu übermitteln, wenn diese glaubhaft machen können, dass sie die Fahrdaten zur Geltendmachung, Abwehr oder Befriedigung von Rechtsansprüchen aus Unfällen benötigen. Unklar ist, wer die Daten übermitteln muss. Es bleibt ebenfalls unbestimmt, ob gegebenenfalls auch die Behörden Fahrdaten

übermitteln dürfen. Im Gesetzesentwurf sind außerdem weder die Zwecke noch die zu übermittelnden Daten hinreichend konkretisiert. Weiterhin geht nicht hervor, wie die Integrität, Vertraulichkeit und Verfügbarkeit bei der Aufzeichnung und Übermittlung der Fahrdaten sichergestellt werden soll.

Sollte der Entwurf in der vorgelegten Form in Kraft treten, besteht in Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion die Gefahr elektronischer Fahrtenschreiber, die personenbezogene Profile bilden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Gesetzgeber zu einer dem datenschutzrechtlichen Bestimmtheitsgebot genügenden Novellierung des Straßenverkehrsgesetzes und zur Stärkung der Datenschutzrechte der Fahrer auf.

Sofern man eine Datenverarbeitung überhaupt für erforderlich hält, ist folgendes zu regeln:

— die abschließende Aufzählung derjenigen Daten, die aufgezeichnet und gespeichert werden dürfen,

— die Bestimmung des für die Verarbeitung Verantwortlichen,

— die Ergänzung einer Übermittlungs-/Zugriffsregelung für den Fahrer/Halter,

— die Konkretisierung der Daten, die den nach Landesrecht zuständigen Behörden zu übermitteln sind,

— die datenschutzgerechte Ausgestaltung des Speichermediums, insbesondere die Festlegung einer angemessenen Speicherdauer anhand der Erforderlichkeit und des Zwecks der Beweisführung für die Haftung,

— eindeutige Festlegungen für die Trennung der Daten von den in den Fahrzeugdatenspeichern der Fahrzeuge gespeicherten Daten,

— die Konkretisierung der Zwecke für die Übermittlung der gespeicherten Daten,

— die Nennung des Adressaten für das Übermittlungsverlangen,

— die abschließende Nennung berechtigter Übermittlungsempfänger und ihrer jeweiligen Verarbeitungsbefugnisse mit im Übrigen strikter Zweckbindung und

— die Konkretisierung des Löschzeitpunkts der übermittelten Daten.

Anlage 4:
Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

Neues Bundeskriminalamtgesetz – Informationspool beschneidet Grundrechte

Der „Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes“ (BTDrs. 18/11326 und 18/11163; BR-Drs. 109/17) ändert das polizeiliche Datenschutzrecht grundlegend und betrifft Polizeibehörden in Bund und Ländern gleichermaßen. Er beschränkt sich nicht darauf, die Vorgaben des Bundesverfassungsgerichts aus dem Urteil vom 20. April 2016 zum Bundeskriminalamtgesetz und aus der neuen EU-Richtlinie zum Datenschutz im Bereich Justiz und Inneres umzusetzen. Tatsächlich nimmt er sogar wichtige Datenschutzregeln und Verfahrenssicherungen zurück, die der Gesetzgeber nach dem Volkszählungsurteil des Bundesverfassungsgerichts geschaffen hatte.

Der Entwurf ändert den bisherigen Informationsverbund für alle Polizeibehörden grundlegend. Dieser ist nicht mehr nach Dateien untergliedert und führt zu unverhältnismäßig weitreichenden Speicherungen. In dieser Form ist dies weder durch das Urteil des Bundesverfassungsgerichts zum BKAG noch durch die EU-Richtlinie zum Datenschutz im Bereich Justiz und Inneres veranlasst. Das Urteil des Bundesverfassungsgerichts fordert, den Zweck der jeweiligen Ermittlungsmaßnahmen bei allen weiteren Schritten zu berücksichtigen, bei denen die ermittelten Daten verwendet werden. Nicht im Einklang damit steht es, Verfahrenssicherungen und datenschutzrechtliche Rahmenbedingungen aufzugeben.

Abzulehnen ist insbesondere der vorgesehene Verzicht auf Errichtungsanordnungen. Diese sind bislang Ausgangspunkt sowohl für datenschutzrechtliche Kontrollen als auch die Selbstkontrolle der Polizeibehörden. In ihnen wird festgelegt, zu welchen Zwecken personenbezogene Daten gespeichert sind. Dies ist eine wesentliche verfassungsrechtliche Vorgabe. Die neuen Regeln führen zu umfassenden themenübergreifenden Verknüpfungen und Abgleichen aller gespeicherten Personen. Sie verkürzen die Kontrollmöglichkeiten der Datenschutzaufsichtsbehörden von Bund und Ländern.

Ebenso sind die künftig durch die geplante „Mitziehautomatik“ erheblich längeren Speicherfristen abzulehnen. Die geplante Neuregelung hat zur Folge, dass alte Speicherungen – auch zu Personen, die lediglich im Verdacht standen, eine Straftat begangen zu haben und die nicht verurteilt wurden – bei jedem neuen Speicheranlass ungeprüft weiter fortgeschrieben werden. Dafür soll es schon genügen, wenn die betroffene Person als Zeuge oder Kontaktperson erneut in Erscheinung tritt. Auch dies verstößt gegen das durch die ständige Rechtsprechung des Bundesverfassungsgerichtes bekräftigte Übermaßverbot.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder fordert daher, den Gesetzentwurf in der parlamentarischen Beratung datenschutzkonform zu überarbeiten!

Anlage 5:
Entschließung der 93. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 29./30. März 2017

Göttinger Erklärung
Vom Wert des Datenschutzes in der digitalen Gesellschaft

Datenschutz ist zurzeit in aller Munde: Mit der Europäischen Datenschutzreform werden ab Mai 2018 in der ganzen Europäischen Union neue einheitliche Regeln gelten. Gegenwärtig sind die Gesetzgeber in Bund und Ländern mit Hochdruck dabei, das nationale Recht an die Europäischen Vorgaben anzupassen. Zugleich schreitet die Digitalisierung der Gesellschaft mit großen Schritten voran, etwa mit dem Internet der Dinge, der Wirtschaft 4.0 und künstlicher Intelligenz, und fordert die Wahrung des Datenschutzes und die Gewährleistung der Persönlichkeitsrechte heraus. Auch der Staat erweitert fortwährend seine Befugnisse zur Verarbeitung personenbezogener Daten, sei es zur Bekämpfung des Terrorismus und zur Gewährleistung der öffentlichen Sicherheit, sei es bei der Digitalisierung staatlicher Dienstleistungen.

Dabei gerät aber leichtfertig eines aus dem Blick: Datenschutz ist ein Grundrecht, wie die Meinungsfreiheit oder die Eigentumsgarantie. Es bindet alle Staatsgewalten unmittelbar, schützt die Menschenwürde und die freie Entfaltung der Persönlichkeit und kann auch Aspekte der Teilhabe und Chancengleichheit betreffen. Alle gesetzlichen Regelungen, sowie die Geschäftsmodelle und Anwendungen auch im Bereich der Wirtschaft, haben dies zu berücksichtigen. Immer häufiger stellen aber Verantwortliche in Politik und Wirtschaft dieses grundrechtlich geschützte Recht auf informationelle Selbstbestimmung implizit oder sogar explizit in Frage. Datenschutz wird als Hindernis diskreditiert.

Dies betrachtet die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder mit großer Sorge. Es befremdet sehr, wenn Mitglieder der Bundesregierung und andere Stimmen in der Politik in letzter Zeit immer wieder betonen, es dürfe kein Zuviel an Datenschutz geben und das Prinzip der Datensparsamkeit könne nicht die Richtschnur für die Entwicklung neuer Produkte sein. Stattdessen wird für eine vermeintliche Datensouveränität geworben, deren Zielrichtung aber im Unklaren bleibt.

Die Konferenz betont, dass Informationen über Personen keine Ware sind wie jede andere und nicht allein auf ihren wirtschaftlichen Wert reduziert werden dürfen. Gerade in Zeiten von Big Data, Algorithmen und Profilbildung bieten die digitalen Informationen ein nahezu vollständiges Abbild der Persönlichkeit des Menschen. Mehr denn je muss daher die Menschenwürde auch im digitalen Zeitalter der zentrale Maßstab staatlichen und wirtschaftlichen Handelns sein. Zu einer menschenwürdigen und freien Entfaltung der Persönlichkeit gehört die freie Selbstbestimmung über das eigene Ich.

„Datensouveränität“ verstanden als eigentumsähnliche Verwertungshoheit kann daher nur zusätzlich zum Recht auf informationelle Selbstbestimmung greifen, dieses jedoch keinesfalls ersetzen.

Die Konferenz fordert daher alle Entscheidungsträger in Politik und Wirtschaft auf, den hohen Wert des Rechts auf informationelle Selbstbestimmung für eine freiheitliche Gesellschaft zu achten und sich nachdrücklich vertrauensbildend für die Persönlichkeitsrechte einzusetzen. Datenschutz stellt kein Hindernis für die Digitalisierung dar, sondern ist wesentliche Voraussetzung für deren Gelingen.

Die Entwicklung datenschutzkonformer IT-Produkte und -Verfahren muss nachhaltig gefördert werden, um den Datenschutz zu einem Qualitätsmerkmal der europäischen Digitalwirtschaft zu machen.

Anlage 6: Entschließung der 93. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 29./30. März 2017

Einsatz von Videokameras zur biometrischen Gesichtserkennung birgt erhebliche Risiken

In Pilotprojekten wird derzeit der Einsatz von Videoüberwachungssystemen erprobt, die erweiterte Möglichkeiten der Verhaltensauswertung und der Identifizierung von Beobachteten bieten. Neben der Mustererkennung steht besonders die biometrische Gesichtserkennung im Fokus dieser Projekte. Dies verschärft die ohnehin schon vorhandene Problematik derartiger neuer Überwachungsverfahren, mit denen „abweichendes Verhalten" erkannt werden soll.

Der Einsatz von Videokameras mit biometrischer Gesichtserkennung kann die Freiheit, sich in der Öffentlichkeit anonym zu bewegen, gänzlich zerstören. Es ist kaum möglich, sich solcher Überwachung zu entziehen oder diese gar zu kontrollieren.

Anders als bei konventioneller Videoüberwachung könnten Passanten mit dieser Technik nicht nur beobachtet und anhand bestimmter Muster herausgefiltert werden, sondern während der Überwachung anhand von Referenzbildern (Templates) automatisiert identifiziert werden. Damit wird eine dauerhafte Kontrolle darüber möglich, wo sich konkrete Personen wann aufhalten oder bewegen und mit wem sie hierbei Kontakt haben. Ermöglicht wird so die Erstellung von umfassenden Bewegungsprofilen und die Verknüpfung mit anderen über die jeweilige Person verfügbaren Daten.

Neben den genannten massiven gesellschaftspolitischen Problemen bestehen auch erhebliche rechtliche und technische Bedenken gegen den Einsatz solcher Überwachungstechniken. Biometrische Identifizierung arbeitet mit Wahrscheinlichkeitsaussagen; bei dem Abgleich zwischen ermitteltem biometrischen Merkmal und gespeichertem Template sind falsche Identifizierungen keine Seltenheit. Beim Einsatz dieser Technik durch Strafverfolgungsbehörden kann eine falsche Zuordnung dazu führen, dass Bürgerinnen und Bürger unverschuldet zum Gegenstand von Ermittlungen und konkreten polizeilichen Maßnahmen werden. Dieselbe Gefahr besteht, falls sie sich zufällig im öffentlichen Raum in der Nähe von gesuchten Straftätern oder Störern aufhalten.

Es gibt keine Rechtsgrundlage für die Behörden von Bund und Ländern für den Einsatz dieser Technik zur Gefahrenabwehr und Strafverfolgung. Die bestehenden Normen zum Einsatz von Videoüberwachungstechnik erlauben nur den Einsatz technischer Mittel für reine Bildaufnahmen oder -aufzeichnungen, nicht hingegen für darüber hinausgehende Datenverarbeitungsvorgänge. Aufgrund des deutlich intensiveren Grundrechtseingriffs, der durch Videotechnik mit erweiterter Auswertung einhergeht, können die bestehenden gesetzlichen Regelungen nicht analog als Rechtsgrundlage herangezogen werden, da sie für einen solchen Einsatz verfassungsrechtlich zu unbestimmt sind.

Nach der Rechtsprechung des Bundesverfassungsgerichts sind Maßnahmen mit großer Streubreite ein erheblicher Grundrechtseingriff. So verlangt das Bundesverfassungsgericht bereits für das automatisierte Erfassen von KFZ-Kennzeichen zwecks Abgleichs mit dem Fahndungsbestand eine normenklare und verhältnismäßige Rechtsgrundlage, die einen anlasslosen und flächendeckenden Einsatz ausschließt. Da bereits die allgemeine Regelung zur Videoüberwachung nicht zur Erfassung von KFZ-Kennzeichen ermächtigt, muss dies erst recht für die viel stärker in die Grundrechte Betroffener eingreifende Videoüberwachung zwecks Abgleichs biometrischer Gesichtsmerkmale einzelner Personen gelten. Ein Einsatz der Videoüberwachung mit Gesichtserkennung darf daher auf derzeitiger Grundlage auch im Rahmen eines Pilotbetriebs nicht erfolgen.

Der europäische Gesetzgeber hat die enormen Risiken dieser Technik für die Privatsphäre erkannt und die Verarbeitung biometrischer Daten zur Identifizierung sowohl in der ab Mai 2018 wirksamen Datenschutz-Grundverordnung als auch in der bis Mai 2018 umzusetzenden Datenschutz-Richtlinie im Bereich Justiz und Inneres nur unter entsprechend engen Voraussetzungen für zulässig erachtet. Wird über den Einsatz dieser Technik nachgedacht, muss der Wesensgehalt des Rechts auf informationelle Selbstbestimmung gewahrt bleiben und es müssen angemessene und spezifische Regelungen zum Schutz der Grundrechte und -freiheiten der Betroffenen vorgesehen werden. Hierzu gehören u. a. eine normenklare Regelung für die Verwendung von Templates, etwa von Personen im Fahndungsbestand, für den Anlass zum Abgleich des Templates mit den aufgenommenen Gesichtern sowie zum Verfahren zur Zulassung von technischen Systemen für den Einsatz.

Etwaige gesetzliche Regelungen müssten die vorgenannten verfassungs- und europarechtlichen Bedingungen beinhalten und den mit dieser Technik verbundenen erheblichen Risiken für die Freiheitsrechte der Bürgerinnen und Bürger angemessen Rechnung tragen!

Anlage 7: Entschließung der 94. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 8./9. November 2017

Umsetzung der DSGVO im Medienrecht

Das Inkrafttreten der Datenschutzgrundverordnung (DSGVO) und deren Geltungsbeginn im Mai 2018 verlangt eine Anpassung der medienrechtlichen Datenschutzbestimmungen an die neuen Vorgaben. Dabei muss dem hohen Stellenwert der Meinungs- und Informationsfreiheit sowie der Presse-, Rundfunk- und

Medienfreiheit gemäß Art. 5 Grundgesetz (GG) und Art. 11 EU-Grundrechtecharta (GRCh) für die freiheitliche demokratische Grundordnung ebenso Rechnung getragen werden wie dem Recht auf Informationelle Selbstbestimmung gemäß Art. 1 in Verbindung mit Art. 2 GG und dem Recht auf Schutz personenbezogener Daten gemäß Art. 8 GRCh. Kollisionen der Schutzbereiche der Grundrechte sind im Sinne einer praktischen Konkordanz aufzulösen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder weist daher auf die Anpassungsklausel des Art. 85 DSGVO hin. Danach können die Mitgliedstaaten Ausnahmen und Abweichungen von bestimmten Vorgaben der DSGVO normieren, wenn „dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen". Das sich daraus ergebende Regel-Ausnahme-Verhältnis bedeutet, dass die Vorgaben der DSGVO grundsätzlich auch auf sämtliche Verarbeitungen personenbezogener Daten zu grundrechtlich besonders geschützten journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken angewendet werden sollen.

Bei der Umsetzung von Art. 85 DSGVO gilt es insbesondere folgende Anforderungen zu beachten:

— Ausnahmen oder Abweichungen von der Anwendung der DSGVO auf die Verarbeitung personenbezogener Daten im journalistischen Bereich müssen notwendig sein, um freie Meinungsäußerung und Informationsfreiheit gemäß Art. 11 GRCh sicherzustellen.

— Einen regelhaften Vorrang der Presse-, Rundfunk- und Medienfreiheit sieht die DSGVO nicht vor. Sie verlangt vielmehr, einen angemessenen Ausgleich zwischen den Grundrechten herzustellen, wenn diese in Widerstreit geraten (vgl. 153. Erwägungsgrund der DSGVO).

— Die Grundsätze des Datenschutzes (Art. 5 DSGVO) müssen hinreichend Beachtung finden.

  Jedenfalls steht es nicht im Einklang mit dem Recht auf Schutz personenbezogener Daten, wenn die Grundsätze des Datenschutzes im Journalismus in weitem Umfang ausgeschlossen werden. Eine Regelung kann keinesfalls als notwendig i. S. d. DSGVO angesehen werden, wenn sie zum Zwecke der Abwägung mit der Meinungs- und Informationsfreiheit die Transparenzrechte und Interventionsmöglichkeiten für betroffene Personen sowie Verfahrensgarantien über eine unabhängige Aufsicht missachtet.

— Über den eingeräumten Gestaltungsspielraum geht es hinaus, wenn die Verarbeitung personenbezogener Daten durch Hilfsunternehmen zu undifferenziert vom Geltungsbereich der DSGVO ausgenommen wird, ohne dass diese Aktivitäten unmittelbar der journalistischen Tätigkeit dienen. Die Reichweite der journalistischen Tätigkeit bedarf zudem einer Konkretisierung.

— Die künftige Aufsicht über den Datenschutz beim Rundfunk ist unabhängig auszugestalten. Sie bedarf wirksamer Abhilfebefugnisse bei Datenschutzverstößen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert daher für die Anpassung von Rundfunk-Staatsverträgen, Presse- und Mediengesetzen:

— Die gesetzlichen Anpassungen i. S. d. Art. 85 DSGVO müssen konkret und spezifisch – bezogen auf die jeweiligen Normen und Vorgaben der DS-GVO – Ausnahmen und Abweichungen regeln und diese begründen.

— Bei der Ausübung der jeweiligen Regelungskompetenz ist das europäische Datenschutzrecht zwingend zu beachten. Eine faktische Beibehaltung der bisherigen nationalen Rechtslage würde dem nicht gerecht.

Anlage 8: Entschließung der 94. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 8./9. November 2017

Keine anlasslose Vorratsspeicherung von Reisedaten

Der Gerichtshof der Europäischen Union (EuGH) hat in seinem Gutachten vom 26. Juli 2017 (Gutachten 1/15) zum Fluggastdaten-Abkommen der EU mit Kanada die langfristige Speicherung von Fluggastdaten (Passenger Name Records – PNR-Daten) sämtlicher Passagiere für nicht mit der Europäischen Grundrechtecharta vereinbar erklärt und seine Position zu anlasslosen Speicherungen personenbezogener Daten bekräftigt. Er erteilt damit einer anlasslosen Vorratsdatenspeicherung von personenbezogenen Daten erneut eine klare Absage. Die Aussagen des EuGH sind nicht nur auf alle geltenden PNR-Instrumente übertragbar und stellen Anforderungen an die Anpassung des Fluggastdatengesetzes, sie betreffen auch die auf europäischer Ebene angestrebte Einrichtung eines Entry-Exit-Systems (EES) sowie eines EU-weiten Reiseinformations- und -genehmigungssystems (ETIAS), die ebenfalls weitreichende anlasslose Speicherungen beabsichtigen.

Zwar hält der EuGH es grundsätzlich für zulässig, Fluggastdaten automatisiert zu übermitteln und auszuwerten, um Personen zu ermitteln, die eine potentielle Gefahr für die öffentliche Sicherheit darstellen und bei ihrer Einreise einer gewissenhaften Kontrolle unterzogen werden sollen. Das gilt jedoch nicht für sensible Daten, die Rückschlüsse etwa auf die rassische und ethnische Herkunft, religiöse Überzeugungen oder das Sexualleben ermöglichen. Der Übermittlungszweck rechtfertigt auch nicht automatisch die weitere Verwendung und Speicherung der Daten. Die übermittelten Daten haben vielmehr ihren Zweck erfüllt, wenn sich während des Aufenthaltes keine konkreten Anhaltspunkte für geplante terroristische oder andere schwere Straftaten ergeben haben. In diesem Fall sieht der EuGH keine Rechtfertigung für eine weitere Speicherung der Daten.

Das Fluggastdatengesetz, mit dem die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rats vom 27. April 2016 über die Verwendung von PNR-Daten zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität umgesetzt wurde, geht insbesondere durch die Einbeziehung der innereuropäischen Flüge, die im Widerspruch zu dem Grundsatz des freien Personenverkehrs im Schengen-Raum steht, noch über den verpflichtenden Teil der Richtlinie hinaus.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) sieht in den vom EuGH ausgesprochenen Feststellungen zur Rechtslage einen unverzichtbaren Maßstab für die Verordnungsvorschläge zur Einrichtung eines neuen Entry-Exit-Systems (EES) sowie eines EU-weiten Reiseinformations- und -genehmigungssystems (ETIAS).

Mit dem EES sollen alle Ein- und Ausreisen sowie Einreiseverweigerungen von Drittstaatlern in die EU zentral erfasst und für mehrere Jahre gespeichert werden (einschließlich biometrischer Identifizierungsmerkmale). Im ETIAS sollen zum Zwecke der Erleichterung der Grenzkontrollen vorab Daten von einreisewilligen visa-befreiten Drittstaatlern erhoben und ebenfalls für mehrere Jahre zentral gespeichert werden. In beiden Datenbanken sollen also Daten, die im Rahmen der Einreise und Grenzkontrolle erhoben werden, ebenso wie nach dem PNR-Abkommen, ohne konkreten Anlass zentral für einen langen Zeitraum vorgehalten werden. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hält dies nicht für vertretbar.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert die jeweils zuständigen Gesetzgeber auf, zeitnah und konsequent sämtliche PNR-Instrumente der EU im Sinne der EuGH-Rechtsprechung nachzubessern, insbesondere das deutsche Fluggastdatengesetz.

Sie fordert die Bundesregierung zudem auf, sich auf europäischer Ebene für eine den Anforderungen der EU-Grundrechtecharta und der Rechtsprechung des EuGH entsprechende Ausgestaltung der angestrebten Systeme EES und ETIAS einzusetzen.

Anlage 9:
Entschließung der 95. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 26. April 2018

Zuverlässigkeitsüberprüfungen bei öffentlichen und privaten Veranstaltungen nur im erforderlichen Maß und nach einem rechtsstaatlichen und transparenten Verfahren

Zunehmend werden im Rahmen von öffentlichen und privaten Veranstaltungen Personen, die in unterschiedlichen Funktionen auf einem Veranstaltungsgelände tätig werden wollen oder sonst Zutritt zu Sicherheitszonen begehren (beispielsweise Anwohner), durch Sicherheitsbehörden auf ihre Zuverlässigkeit überprüft. Auch bei privaten Veranstaltungen fordern die Polizeien die Veranstalter bisweilen dazu auf, dafür zu sorgen, dass alle im Rahmen der Veranstaltung Tätigen einer solchen Prüfung unterzogen werden. In den meisten Fällen ist alleinige Grundlage für diese Maßnahmen immer noch die Einwilligung der Betroffenen.

Bereits vor mehr als zehn Jahren haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 25./26. Oktober 2007 darauf hingewiesen, dass allein die Einwilligung der Betroffenen in eine Zuverlässigkeitsüberprüfung keine legitimierende Grundlage für solche tiefen Eingriffe in das Recht auf informationelle Selbstbestimmung darstellen kann. Die wiederholten Forderungen nach Schaffung gesetzlicher Grundlagen haben seitdem die Gesetzgeber nur weniger Bundesländer aufgegriffen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) fordert die Gesetzgeber und die Verantwortlichen deshalb erneut nachdrücklich auf, für ein rechtsstaatliches und transparentes Verfahren solcher Zuverlässigkeitsüberprüfungen zu sorgen, das auf das absolut erforderliche Maß beschränkt bleibt, sowohl was den Umfang der Überprüfung als auch den betroffenen Personenkreis betrifft. Dabei sind insbesondere folgende Rahmenbedingungen zu beachten:

Zuverlässigkeitsüberprüfungen nur aufgrund einer spezifischen Rechtsgrundlage

Die Gesetzgeber werden aufgefordert, bereichsspezifische Rechtsgrundlagen zu schaffen, die den Grundsatz der Verhältnismäßigkeit beachten und aus denen sich die Voraussetzungen und der Umfang der Überprüfungen klar und für die Bürgerinnen und Bürger erkennbar ergeben.

Zuverlässigkeitsüberprüfungen nur im erforderlichen Maß

Anwendung, Umfang, Kreis der betroffenen Personen und die Datenverarbeitung sind auf das Erforderliche zu beschränken. Generell dürfen Zuverlässigkeitsüberprüfungen nur bei solchen Veranstaltungen eingesetzt werden, die aufgrund ihrer spezifischen Ausprägung infolge einer belastbaren Gefahrenprognose als besonders gefährdet bewertet werden. Korrespondierend müssen die personenbezogenen Daten, die in den zum Abgleich herangezogenen Dateien und Informationssystemen gespeichert sind, nicht nur eine ausreichende Qualität haben, es dürfen auch nur hinreichend gewichtige Delikte in die Überprüfung einbezogen werden. Zudem müssen die Kriterien, die zur Annahme von Sicherheitsbedenken führen, einen konkreten Bezug zu den abzuwehrenden Gefahren haben.

Zuverlässigkeitsüberprüfungen nur in einem transparenten Verfahren

Die Rechte und Freiheiten der betroffenen Personen müssen durch ein transparentes Verfahren gewährleistet werden. Dazu müssen insbesondere Anhörungsrechte der betroffenen Personen rechtlich verankert werden. Im praktischen Verfahren kann im Einzelfall auch die Einrichtung einer Clearingstelle sinnvoll sein. Zudem sollten zumindest die Datenschutzbeauftragten der Verantwortlichen frühzeitig vorab beteiligt werden, damit eine datenschutzrechtliche Beratung für eine datensparsame Ausgestaltung und Beschränkung des konkreten Verfahrens stattfinden kann.

Anlage 10:
Entschließung der 95. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 26. April 2018

Datenschutzbeauftragten-Bestellpflicht nach Artikel 37 Abs. 1 lit. c Datenschutz-Grundverordnung bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs

1. Betreibt ein einzelner Arzt, Apotheker oder sonstiger Angehöriger eines Gesundheitsberufs eine Praxis, Apotheke oder ein Gesundheitsberufsunternehmen und sind dort einschließlich seiner Person in der Regel mindestens 10 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt, besteht eine gesetzliche Verpflichtung zur Benennung eines Datenschutzbeauftragten (DSB).

2. Bei Ärzten, Apothekern oder sonstigen Angehörigen eines Gesundheitsberufs, die zu mehreren in einer Berufsausübungsgemeinschaft (Praxisgemeinschaft) oder Gemeinschaftspraxis zusammengeschlossen sind oder die ihrerseits weitere Ärzte, Apotheker oder sonstige Angehörige eines Gesundheitsberufs beschäftigt haben, ist in der Regel nicht von einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten im Sinne von Art. 37 Abs. 1 lit. c DS-GVO auszugehen – in diesen Fällen ist unter Berücksichtigung von Punkt 3 dann kein DSB zu benennen, wenn weniger als 10 Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind.

3. Bei Ärzten, Apothekern oder sonstigen Angehörigen eines Gesundheitsberufs, die zu mehreren in einer Berufsausübungsgemeinschaft (Praxisgemeinschaft) oder Gemeinschaftspraxis zusammengeschlossen sind oder die ihrerseits weitere Ärzte, Apotheker oder sonstige Angehörige eines Gesundheitsberufs beschäftigt haben, bei denen ein hohes Risiko für die Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten zu erwarten ist, ist eine Datenschutzfolgenabschätzung vorgeschrieben und damit zwingend ein Datenschutzbeauftragter zu benennen. Dies kann neben einer umfangreichen Verarbeitung (zum Beispiel große Praxisgemeinschaften), die ohnehin nach Art. 37 Abs. 1 lit. c DS-GVO zu einer Benennungspflicht führt, beispielsweise beim Einsatz von neuen Technologien, die ein hohes Risiko mit sich bringen, der Fall sein. Der Datenschutzbeauftragte ist damit auch dann zu benennen, 2 wenn weniger als 10 Personen ständig mit der Verarbeitung personenbezogener Daten zu tun haben.

4. Der Begriff „Gesundheitsberuf“ ist im Sinne der Aufzählung nach § 203 Abs. 1 StGB auszulegen und umfasst die in § 203 Abs. 1 Nr. 1, 2, 4 und 5 StGB aufgezählten Berufsbilder.

Abkürzungsverzeichnis

ABl.	Amtsblatt der Europäischen Union
Abs.	Absatz
App	Application, Anwendungsprogramm auf Smartphone
Art.	Artikel
Az.	Aktenzeichen
BayDSG	Bayerisches Datenschutzgesetz
BayDSG-alt	Bayerisches Datenschutzgesetz in der bis zum 24. Mai 2018 geltenden Fassung
BDSG	Bundesdatenschutzgesetz
BGBl I	Bundesgesetzblatt (Teil 1)
BGHSt	Entscheidungen des Bundesgerichtshofes in Strafsachen
BR-Drs.	Bundesrats-Drucksache
Buchst.	Buchstabe
BVerfGE	Entscheidungen des Bundesverfassungsgerichts (zitiert nach Band und Seite)
CSU	Christlich-Soziale Union in Bayern
DNA	Desoxyribonuclein Acid, Träger der Erbinformation
DSB	Datenschutzbeauftragter
DSFA	Datenschutzfolgenabschätzung
DSGVO	Datenschutz-Grundverordnung
e. V.	eingetragener Verein
EDV	Elektronische Datenverarbeitung
EU	Europäische Union
EuGH	Europäischer Gerichtshof
FDP	Freie Demokratische Partei
ff.	(nach)folgende
GG	Grundgesetz
ggf.	gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
GVBl.	Bayerisches Gesetz- und Verordnungsblatt
https	Hyper Text Transfer Protocol Secure
IGVP	Integrationsverfahren der Bayerischen Polizei
IP	Internet Protocol
IT	Informationstechnik
JVA	Justizvollzugsanstalt
KAN	Kriminalaktennachweis
KFZ	Kraftfahrzeug
KKG	Gesetz zur Kooperation und Information im Kinderschutz
lit.	Buchstabe
MdL	Mitglied des Landtages
Nr.	Nummer
PC	Personalcomputer
QR	Quick Response
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
USB ..... Universal Serial Bus
vgl. ..... vergleiche
www ..... World Wide Web
z. B. ..... zum Beispiel

Stichwortverzeichnis

Der Bayerische
Landesbeauftragte
für den
Datenschutz

Wagmüllerstraße 18
80538 München
Postfach 22 12 19
80502 München
Telefon 089 21 26 72-0
Telefax 089 21 26 72-50

poststelle@datenschutz-bayern.de
www.datenschutz-bayern.de