30. Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz

gemäß Art. 59 Datenschutz-Grundverordnung

Berichtszeitraum:	1. Januar 2020 bis 31. Dezember 2020
Veröffentlichungsdatum:	25. Mai 2021

Inhaltsverzeichnis

Hinweis zu Abkürzungen

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

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

1 Überblick

1.1 Datenschutz in der COVID-19-Pandemie

Spätestens seit dem Frühjahr 2020 prägen das neuartige Coronavirus (SARS-CoV-2) und die von ihm verursachte Krankheit COVID-19 auch zahlreiche politische Entscheidungen, die sich auf die Verarbeitung personenbezogener Daten auswirken. Im Berichtszeitraum standen etwa datenschutzrechtliche Fragen bei der Kontaktnachverfolgung und bei der Befreiung von der Maskenpflicht zeitweise besonders im Fokus der öffentlichen Aufmerksamkeit.

1.1.1 Kontaktnachverfolgung

Zu Beginn der COVID-19-Pandemie sah sich die Bayerische Staatsregierung gezwungen, mit der Ersten und Zweiten **Bayerischen Infektionsschutzmaßnahmenverordnung** (1. und 2. BayIfSMV) die zwischenmenschlichen Kontakte so weit wie möglich zu reduzieren. Das führte zu zeitweisen Schließungen von Dienstleistungsbetrieben mit Kundenkontakt, wie etwa Gastronomiebetrieben und Freizeiteinrichtungen. Gerade im Zusammenhang mit deren Wiedereröffnung stellt die Nachverfolgung von kritischen Kontakten durch die Gesundheitsbehörden eine Schlüsselstrategie der Pandemiebekämpfung dar. Dabei werden infizierte Personen befragt, welche Kontakte sie innerhalb einer Zeit möglicher „Ansteckungsfähigkeit" hatten. Benannte Kontaktpersonen werden anschließend von den Gesundheitsbehörden kontaktiert und auf den Risikokontakt hingewiesen. Ein solche Information geht regelmäßig mit Anweisungen einher, wie sich die Kontaktpersonen zu verhalten haben. Dies gilt insbesondere für die Anordnung, sich in Quarantäne zu begeben.

Um Risikokontakte besser ermitteln zu können, sah bereits die Dritte Bayerische Infektionsschutzmaßnahmenverordnung gegen Ende ihrer Geltungsdauer ausdrücklich vor, dass Besucherinnen und Besucher von pflegebedürftigen Personen namentlich bei der Einrichtung registriert sein müssen. Mit der Änderung der Vierten Bayerischen Infektionsschutzmaßnahmenverordnung vom 14. Mai 2020 (BayMBl. Nr. 269) wurde eine vorsichtige Öffnung von Gastronomiebetrieben ermöglicht – allerdings nur bei Vorliegen eines Schutz- und Hygienekonzepts, das die Gastronomiebetriebe auf der Grundlage eines Rahmenkonzepts zu erstellen hatten. Dieses Rahmenkonzept „**Hygienekonzept Gastronomie**" (vom 14. Mai 2020, BayMBl. Nr. 270) wurde von den Bayerischen Staatsministerien für Gesundheit und Pflege sowie für Wirtschaft, Landesentwicklung und Energie bekannt gemacht und sah unter Abschnitt 3.2.9 ebenfalls eine Kontaktdatenerfassung durch die Gastronomiebetriebe vor. Diese Kontaktdatenerfassung durch Gastronomiebetriebe, später durch andere Unternehmen und auch durch öffentliche Stellen, führte bei mir zu zahlreichen Beschwerden und Beratungsanfragen. Neben der Speicherdauer (siehe dazu Nr. 3.4 dieses Berichts) bewegte zahlreiche Besucherinnen und Besucher die Frage, zu welchen Zwecken die Daten verwendet werden dürften. Das „Hygienekonzept Gastronomie" schien insoweit eindeutig zu sein: Eine Erfassung diente ausschließlich dem Zweck der Auskunfterteilung auf Anforderung gegenüber den zuständigen Gesundheitsbehörden.

1.1.2 Speziell: Polizeilicher Zugriff auf Gästelisten

Es dauerte allerdings nicht lange, bis in einigen Fällen auch die Polizei die Kontaktlisten von Gastwirtschaften zur Strafverfolgung einsah. Einfachgesetzlich wurde dieser polizeiliche Zugriff auf Kontaktlisten zumeist über die Regeln der Sicherstellung beziehungsweise der Beschlagnahme nach den §§ 94 ff. StPO gerechtfertigt. Wie unter Nr. 1.1.1 erwähnt, sah das „Hygienekonzept Gastronomie" zwar vor, dass Gästelisten „ausschließlich" zur Vorlage bei den Gesundheitsämtern geführt werden sollten. Streng genommen waren die Strafverfolgungsbehörden aber wohl nicht an Zweckbestimmungen aus den Infektionsschutzverordnungen der Länder gebunden – denn die Strafprozessordnung geht als Bundesrecht bekanntlich entgegenstehendem Landesrecht vor. Gleichwohl führten diese sicherheitsbehördlichen Zugriffe auf Kontaktlisten zu einer erheblichen Irritation in Teilen der Öffentlichkeit. In erster Linie aufgrund verfassungsrechtlicher Bedenken setzte ich mich dafür ein, dass derartige Zugriffe durch Strafverfolgungsbehörden möglichst bundesgesetzlich geregelt werden und allenfalls bei besonderer Beachtung der Verhältnismäßigkeit gestattet werden sollten.

Dieser Forderung trug zunächst die Bayerische Staatsregierung durch eine Vorschrift in der Neunten Bayerischen Infektionsschutzmaßnahmenverordnung vom 30. November 2020 (BayMBl. Nr. 683) Rechnung, die sinngemäß klarstellte, dass die an und für sich strikte Zweckbindung die Befugnisse der Strafverfolgungsbehörden unberührt lässt.

Erfreulicherweise hat der Bundesgesetzgeber meine datenschutzrechtlichen Bedenken aufgegriffen und dem zulässigen polizeilichen Zugriff auf die Gästelisten mit einer Änderung des Infektionsschutzgesetzes nun rechtlich ein Ende gesetzt. § 28a Abs. 4 Satz 3 Infektionsschutzgesetz (IfSG) sieht eine Zweckbindung dahingehend vor, dass Kontaktlisten zu keinem anderen Zweck als der Aushändigung auf Anforderung durch die Gesundheitsbehörden verwendet werden dürfen. Diese bundesgesetzliche Zweckbindung steht mit dem Strafprozessrecht im Gleichrang und erlaubt keinen Zugriff auf die Kontaktlisten zu Strafverfolgungszwecken mehr. Fordern die Gesundheitsbehörden Kontaktlisten an, dürfen sie diese Listen nach § 28a Abs. 4 Satz 6 IfSG ebenfalls nicht an Strafverfolgungsbehörden weitergeben.

§ 28a IfSG
Besondere Schutzmaßnahmen zur Verhinderung der Verbreitung der Coronavirus-Krankheit-2019 (COVID-19)
(1) Notwendige Schutzmaßnahmen im Sinne des § 28 Absatz 1 Satz 1 und 2 zur Verhinderung der Verbreitung der Coronavirus-Krankheit-2019 (COVID-19) können für die Dauer der Feststellung einer epidemischen Lage von nationaler Tragweite nach § 5 Absatz 1 Satz 1 durch den Deutschen Bundestag insbesondere sein […]
17. Anordnung der Verarbeitung der Kontaktdaten von Kunden, Gästen oder Veranstaltungsteilnehmern, um nach Auftreten einer Infektion mit dem Coronavirus SARS-CoV-2 mögliche Infektionsketten nachverfolgen und unterbrechen zu können.
(4) Im Rahmen der Kontaktdatenerhebung nach Absatz 1 Nummer 17 dürfen von den Verantwortlichen nur personenbezogene Angaben sowie Angaben zum Zeitraum und zum Ort des Aufenthaltes erhoben und verarbeitet werden, soweit dies zur Nachverfolgung von Kontaktpersonen zwingend notwendig ist. Die Verantwortlichen haben sicherzustellen, dass eine Kenntnisnahme der erfassten Daten durch Unbefugte ausgeschlossen ist. Die Daten dürfen nicht zu einem anderen

Zweck als der Aushändigung auf Anforderung an die nach Landesrecht für die Erhebung der Daten zuständigen Stellen verwendet werden und sind vier Wochen nach Erhebung zu löschen. Die zuständigen Stellen nach Satz 3 sind berechtigt, die erhobenen Daten anzufordern, soweit dies zur Kontaktnachverfolgung nach § 25 Absatz 1 erforderlich ist. Die Verantwortlichen nach Satz 1 sind in diesen Fällen verpflichtet, den zuständigen Stellen nach Satz 3 die erhobenen Daten zu übermitteln. Eine Weitergabe der übermittelten Daten durch die zuständigen Stellen nach Satz 3 oder eine Weiterverwendung durch diese zu anderen Zwecken als der Kontaktnachverfolgung ist ausgeschlossen. Die den zuständigen Stellen nach Satz 3 übermittelten Daten sind von diesen unverzüglich irreversibel zu löschen, sobald die Daten für die Kontaktnachverfolgung nicht mehr benötigt werden.

Der nun verwehrte Zugriff auf Gästelisten wird eine effektive Strafverfolgung sicher nicht in Frage stellen, zumal solche Listen bis vor Kurzem auch nicht existierten und die polizeilichen Zugriffe in relativ seltenen Einzelfällen erfolgten.

1.1.3 Corona-Warn-App der Bundesregierung

Die Weichen für die Corona-Warn-App der Bundesregierung wurden während des ersten „Lockdowns" im Frühjahr 2020 gestellt. Zu dieser Zeit setzten zahlreiche europäische Staaten auf die Entwicklung von Tracing- und Tracking-Apps für die Kontaktnachverfolgung eine hohe Priorität. Sie entschieden sich dabei oftmals gegen datenschutzfreundliche, dezentrale Lösungen. Jedenfalls im EU-Raum scheiterten diese Lösungen bereits an der mangelnden Akzeptanz. Beispielsweise gab es in Frankreich immerhin drei Monate nach ihrem Start gerade einmal 2,3 Millionen Downloads der französischen App „StopCovid France" (mittlerweile: „TousAntiCovid". Vor diesem Hintergrund habe ich auf Landes-, Bundes- und EU-Ebene eine datenschutzfreundliche dezentrale Lösung empfohlen, weil ansonsten mangels einer auseichenden Zahl von Downloads bereits die erste wichtige Voraussetzung für den Erfolg der App fehlt.

Auch die Bundesregierung entschied sich für ein datenschutzfreundliches Konzept. Und zunächst gab ihr der Erfolg auch Recht: Im Auftrag der Bundesregierung veröffentlichte das Robert-Koch-Institut die App am 16. Juni 2020. Bereits einen Tag danach wurden 6,5 Millionen Downloads der Corona-Warn-App verzeichnet. Bis Ende des Jahres 2020 haben rund 25 Millionen Menschen die App auf ihr Smartphone heruntergeladen. Bereits der zahlenmäßige Vergleich der Downloads in Frankreich und Deutschland legt zumindest nahe: Ein hohes Datenschutzniveau ist ein nicht unwesentlicher Akzeptanzfaktor für die jeweilige App gewesen. Das bringt auch eine Pressemitteilung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zum Ausdruck.

Pressemitteilung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 16. Juni 2020

Datenschutzfreundliches Grundkonzept der Corona-Warn-App – Freiwilligkeit darf nicht durch zweckwidrige Nutzung untergraben werden!

Mit der am 16. Juni 2020 durch den Bund vorgestellten Corona-Warn-App steht ein freiwilliges Instrument mit einer dezentralen Speicherung auf dem jeweiligen Smartphone zur Nachverfolgung eventueller Infektionen zur Verfügung.

Die Datenschutzkonferenz sieht das datenschutzfreundliche Grundkonzept als Realisierung des Grundsatzes von Datenschutz by Design. Sie weist allerdings darauf hin, dass insbesondere der Ansatz der Freiwilligkeit nicht durch eine zweckentfremdende Nutzung untergraben werden darf:

Der Zugang zu behördlichen Einrichtungen, Arbeitsstätten, Handelsgeschäften, Gastronomiebetrieben und Beherbergungsstätten, Sportstätten, etc. darf nicht vom Vorweisen der App abhängig gemacht werden.

Hierbei würde es sich um eine zweckwidrige Verwendung handeln, die bereits mit dem Konzept der Freiwilligkeit nicht vereinbar ist. Eine Diskriminierung von Personen, die die App nicht anwenden, ist auszuschließen.

Bei näherer Betrachtung hat die Corona-Warn-App allerdings nur eine begrenzte Wirkung entfaltet. Dies hat wohl weniger mit dem Datenschutz zu tun als vielmehr mit der Frage, welche Funktionalitäten die App hat und vor allem, wie sie in ein stimmiges Gesamtkonzept eingebunden worden ist. So soll die Corona-Warn-App erst im Laufe des Jahres 2021 mit einer Funktion nachgerüstet werden, die in geschlossenen Räumen Risikobegegnungen von Personen zutreffend erkennt. Letztlich hat es für die Nutzerinnen und Nutzer der App auch keine wirklich starken Anreize gegeben, die App nicht nur herunterzuladen, sondern auch tatsächlich zu nutzen.

Vergleicht man die Corona-Warn-App mit alternativen Lösungen (wie etwa der Luca-App oder der App „Darfichrein"), fällt das unterschiedliche Grundkonzept dieser technischen Hilfsmittel auf: Während die meisten Alternativlösungen gerade Risikobegegnungen erfassen und an die zuständigen Gesundheitsbehörden weiterleiten sollen, zielt die Corona-Warn-App der Bundesregierung darauf, die Gesundheitsämter davon zu entlasten, Risikokontakte zu ermitteln und (meist telefonisch) zu unterrichten.

Gleich welche Lösung in den Blick genommen wird: Apps sind stets lediglich technische Hilfsmittel. Ihr Erfolg hängt immer davon ab, wie sie in ein stimmiges Gesamtkonzept eingebunden werden. Dazu gehört immer ein Maß an Datenschutz, das vor einer Manipulation oder einem Missbrauch der erhobenen Daten hinreichend zuverlässig schützt.

1.1.4 Befreiung von der Pflicht zum Tragen einer Mund-Nasen-Bedeckung

Abstandsgebot und Maskenpflicht wurden mit der Vierten Bayerischen Infektionsschutzmaßnahmenverordnung vom 5. Mai 2020 (BayMBl. Nr. 240) ausdrücklich im bayerischen Infektionsschutzrecht etabliert. Aus datenschutzrechtlicher Sicht stellte sich damit auch die Frage, unter welchen Voraussetzungen Ausnahmen von der **Pflicht zum Tragen einer Mund-Nasen-Bedeckung** eingreifen. Auch diese Frage wurde in der Vierten Bayerischen Infektionsschutzmaßnahmenverordnung beantwortet. Unter anderem sah sie sinngemäß vor, dass Personen von der Pflicht zum Tragen einer Mund-Nasen-Bedeckung befreit sind, wenn sie glaubhaft machen können, dass ihnen das Tragen aufgrund einer Behinderung oder aus gesundheitlichen Gründen nicht möglich oder unzumutbar ist. Diese Bestimmung wurde in den nachfolgenden Infektionsschutzmaßnahmenverordnungen mehrfach geändert. Mitte April 2021 bestimmte § 1 Abs. 2 12. Bayerische Infektionsschutzmaßnahmenverordnung:

„[1]Soweit in dieser Verordnung die Verpflichtung vorgesehen ist, eine Mund-Nasen-Bedeckung zu tragen (Maskenpflicht) oder eine medizinische Gesichtsmaske zu tragen, gilt:

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

[2]Soweit in dieser Verordnung die Verpflichtung vorgesehen ist, eine FFP2-Maske oder eine Maske mit mindestens gleichwertigem genormten Standard zu tragen (FFP2-Maskenpflicht), gilt Satz 1 entsprechend mit der Maßgabe, dass Kinder zwischen dem sechsten und dem 15. Geburtstag nur eine Mund-Nasen-Bedeckung tragen müssen."

Vor allem im schulischen Bereich erreichten mich zu diesem Thema zahlreiche Anfragen und Beschwerden. Deshalb habe ich speziell die wichtigsten schuldatenschutzrechtlichen Fragen zur Befreiung von der Maskenpflicht im Rahmen einer Aktuellen Kurz-Information beantwortet.[1] Die dort gegebenen Hinweise betreffen das Schulverhältnis an bayerischen öffentlichen Schulen, nicht jedoch andere Lebenssituationen, in denen eine Maskenpflicht zu beachten ist. Daher bleibt auch die Frage außer Betracht, ob und auf welche Weise Regelungen über Atteste zur Befreiung von einer Maskenpflicht zwischen dem öffentlichen und dem nichtöffentlichen Sektor differenzieren müssen.

1.1.5 Datenschutz und COVID-19-Pandemie in Deutschland und Europa

Auch der Europäische Datenschutzausschuss und die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) haben sich vielfach mit den datenschutzrechtlichen Auswirkungen der Pandemiebekämpfung befasst. Ich verweise beispielhaft auf die in **Anlage 1** abgedruckte Entschließung der Datenschutzkonferenz vom 3. April 2020 zu den Datenschutz-Grundsätzen bei der Bewältigung der Corona-Pandemie. Zahlreiche weitere Fragen im Zusammenhang mit der Corona-Pandemie werden in einem **Schwerpunktbeitrag „Datenschutzrechtliche Themen im Zusammenhang mit der COVID-19-Pandemie"** (Nr. 3 in diesem Tätigkeitsbericht) sowie in einzelnen weiteren Beiträgen behandelt.

[1] Bayerischer Landesbeauftragter für den Datenschutz, Befreiung von der Maskenpflicht an bayerischen öffentlichen Schulen, Aktuelle Kurz-Information 33, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Aktuelle Kurz-Informationen".

1.2 Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten

Auch in diesem Berichtszeitraum betrafen wieder zahlreiche Beschwerden die Verarbeitung personenbezogener Daten im Rahmen der Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten. Hierzu zählen unter anderem Parkverstöße im ruhenden und Geschwindigkeitsverstöße im fließenden Verkehr. Da das Thema nahezu alle Bürgerinnen und Bürger im Freistaats betrifft, habe ich einige bedeutsame datenschutzrechtliche Fragen in einem **Schwerpunktbeitrag „Datenschutzrechtliche Themen im Zusammenhang mit Verkehrsordnungswidrigkeiten“** (Nr. 2 in diesem Tätigkeitsbericht) zusammengefasst.

1.3 Microsoft-Produkte und Datenschutz

Nahezu alle bayerischen öffentlichen Stellen setzen bei der Datenverarbeitung Produkte von Microsoft ein. Auch vor dem Hintergrund, dass am 14. Januar 2020 der Produktsupport für Windows 7 endete, wurde insbesondere vielfach die Beratungsfrage an mich gerichtet, inwieweit der Einsatz von **Windows 10** und **Microsoft 365** im Einklang mit datenschutzrechtlichen Anforderungen zu bringen ist.

Mir erschien es allerdings wenig sinnvoll, dass ich als bayerische Datenschutz-Aufsichtsbehörde im Alleingang die zu beachtenden Datenschutzanforderungen für Microsoft-Anwendungen definiere. Zielführender ist hier die Entwicklung von deutschen, besser noch von gesamteuropäischen Datenschutzstandards. Auch wenn es zwischenzeitlich zu Meinungsverschiedenheiten in Detailfragen kam: Nach meiner Einschätzung verfolgen alle Datenschutz-Aufsichtsbehörden des Bundes und der Länder grundsätzlich einvernehmlich das Ziel, im Rahmen eines intensiven Dialogs mit dem Anbieter zu technischen und rechtlichen Verbesserungen des Datenschutzniveaus zu kommen. Insoweit verweise ich beispielhaft auf einen Beschluss, den die Datenschutzkonferenz am 26. November 2020 zu Telemetriefunktionen und Datenschutz beim Einsatz von Windows 10 Enterprise gefasst hat.[2] In Bezug auf Microsoft 365 wurde eine Taskforce eingerichtet, die Verhandlungen mit dem Anbieter mit dem Ziel aufnehmen soll, nachhaltige datenschutzrechtliche Verbesserungen zu erreichen. Dabei ist auch der Umstand in den Blick zu nehmen, dass Microsoft personenbezogene Daten in Drittländer ohne angemessenes Datenschutzniveau transferiert. Auf diese Problematik geht dieser Tätigkeitsbericht allgemein unter Nr. 11.2 ein.

Spezielle datenschutzrechtliche Fragen ergaben sich im Hinblick auf den Einsatz der Anwendung **Microsoft Teams** insbesondere an bayerischen Schulen. Bei Microsoft Teams handelt es sich um einen Bestandteil verschiedener Microsoft 365-Angebote. Unter anderem wegen der angedeuteten Problematiken im Zusammenhang mit der Telemetriefunktion sowie von Drittlandtransfers stand ich allerdings mit dem Bayerischen Staatsministerium für Unterricht und Kultus im intensiven Kontakt, um die im Zusammenhang mit Microsoft Teams bestehenden rechtlichen Unsicherheiten zu klären.

Erfreulicherweise hat das Kultusministerium im Sommer 2020 entschieden, die bayerische Bildungsplattform mebis durch ein nachhaltig datenschutzkonformes

[2] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Telemetriefunktionen und Datenschutz beim Einsatz von Windows 10 Enterprise, Beschluss vom 26. November 2020, Internet: https://www.datenschutz-bayern.de, Rubrik „Konferenzen“.

Kommunikationswerkzeug zu ergänzen. Ein bereits laufendes Ausschreibungsverfahren war im Berichtszeitraum noch nicht abgeschlossen. Es zeichnete sich jedoch bereits ab, dass das Kultusministerium den Schulen im Laufe des Jahres 2021 ein solches Kommunikationswerkzeug anbieten kann.

Bis dahin gilt: Ungeachtet der gesetzlichen Verarbeitungsbefugnisse der Schule gemäß Art. 85 Abs. 1 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG) in Verbindung mit § 19 Abs. 4 Bayerische Schulordnung (BaySchO) und § 46 Abs. 1 BaySchO in Verbindung mit Anlage 2 Abschnitt 7 zur BaySchO kommt der Einsatz des Videokonferenzwerkzeugs Microsoft Teams aufgrund hierzu bestehender, offener datenschutzrechtlicher Fragen nur aufgrund einer wirksamen datenschutzrechtlichen Einwilligung der betroffenen Personen in Betracht. Unter dieser Voraussetzung trete ich vor dem Hintergrund der COVID-19-Pandemie dem vorübergehenden Einsatz von Microsoft Teams an öffentlichen Schulen derzeit nicht entgegen.

Die Freiwilligkeit der Einwilligung der Betroffenen ist durch echte Alternativangebote sicherzustellen. In Betracht kommt zum Beispiel die Zuschaltung per Telefon oder eine weitgehende anonyme Nutzung. Eine solche anonyme Nutzung kann insbesondere erreicht werden, indem die Schule

— „anonyme“ Konten (das heißt ohne Namensbestandteile in der Kennung oder in sonstigen Nutzerdaten) oder

— als Endgerät ein schulisches Leihgerät

zur Verfügung stellt.

Datenschutzrechtliche Fragen zur Regelung des Distanzunterrichts werden in diesem Tätigkeitsbericht unter Nr. 10.1.2 behandelt. Allgemeine technisch-organisatorische Hinweise zum Einsatz von Videokonferenzsystemen sind dem Beitrag Nr. 12.4 zu entnehmen.

1.4 Schlussbemerkung

Die nachfolgenden Beiträge geben einen Überblick über die Tätigkeit meiner Behörde im Jahr 2020. Sie zeigen, dass ich auch außerhalb des Themenkreises „Datenschutz in der COVID-19-Pandemie“ zahlreiche Gesetzgebungsverfahren begleiten konnte. Das Aufkommen an behördlichen Beratungsanfragen, an Beschwerden wie auch an Meldungen von Datensicherheitsverletzungen ist unvermindert hoch, sodass ich insofern nur eine kleine Zahl von Fällen auswählen konnte. Ich hoffe, dass meine Hinweise den bayerischen öffentlichen Stellen dabei helfen, ihrer datenschutzrechtlichen Verantwortung noch besser gerecht zu werden, als dies drei Jahre nach dem Geltungsbeginn der Datenschutz-Grundverordnung vielerorts in Bayern ohnehin schon der Fall ist.

2 Schwerpunkt I

Datenschutzrechtliche Themen im Zusammenhang mit Verkehrsordnungswidrigkeiten

Datenschutzrechtliche Themen im Zusammenhang mit der Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten habe ich in meinen Tätigkeitsberichten wiederholt erörtert, so unter anderem im 29. Tätigkeitsbericht 2019 unter Nr. 4.5, im 27. Tätigkeitsbericht 2016 unter Nr. 5.6 und im 26. Tätigkeitsbericht 2014 unter Nr. 5.5.1, Nr. 5.5.2 und Nr. 5.5.3. Zu den Verkehrsordnungswidrigkeiten zählen insbesondere Parkverstöße im ruhenden und Geschwindigkeitsverstöße im fließenden Verkehr.

Auch im Berichtszeitraum erreichten mich zahlreiche Anfragen und Beschwerden zum Datenschutz in Verfahren wegen Verkehrsordnungswidrigkeiten. Im Folgenden möchte ich insofern bedeutsame datenschutzrechtliche Fragen zusammenzufassend erläutern und insbesondere die Erfahrungen darstellen, die ich in meiner Prüfungs- und Beratungspraxis hierzu gewinnen konnte.

So gehe ich einleitend auf die Frage der **Zuständigkeit** zur Verfolgung und Ahndung von Verkehrsverstößen (Nr. 2.1) ein, sodann auf die zentrale Thematik der **Zulässigkeit von Bildaufnahmen** und ihre Grenzen (Nr. 2.2.1 und Nr. 2.2.2). Darüber hinaus stelle ich die datenschutzrechtlichen Bezüge der **Fahrzeughalter- und Fahrzeugführerermittlung** vor (Nr. 2.3 und Nr. 2.4). In diesen Zusammenhang gehören neben der Versendung von **Anhörungs- und Zeugenfragenbögen** (Nr. 2.4.1) unter anderem **Lichtbildanforderung, -übermittlung und -abgleich** (Nr. 2.4.2) sowie die **Recherche des Fahrzeugführers im familiären Umfeld** des Fahrzeughalters (Nr. 2.4.3). Außerdem zeige ich auf, welche datenschutzrechtlichen Vorgaben bei der **Zustellung von Bescheiden** (Nr. 2.5) sowie bei **Speicherungen** in den zuständigen Behörden (Nr. 2.6) zu beachten sind. Abschließend gehe ich auf die datenschutzrechtlichen **Informationspflichten und auf die Betroffenenrechte** ein (Nr. 2.7).

Vorab möchte ich darauf hinweisen, dass sich die folgenden Ausführungen auf **typische Fallkonstellationen** in Verkehrsordnungswidrigkeitenverfahren beziehen. Es mag **Einzelfälle** geben, in denen sich die datenschutzrechtliche Bewertung abweichend darstellen kann. Jede bei mir eingehende Beschwerde und Anfrage in diesem Zusammenhang überprüfe ich daher individuell.

Auch möchte ich anmerken, dass ein Verstoß gegen datenschutzrechtliche Vorschriften im Rahmen einer späteren gerichtlichen Beweiserhebung kein **Beweisverwertungsverbot** zur Folge haben muss. Die Entscheidung über die Verwertbarkeit trifft das zuständige Gericht im Rahmen einer Interessenabwägung in richterlicher Unabhängigkeit.

2.1 Zuständigkeit zur Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten

Nach § 35 Abs. 1 Gesetz über Ordnungswidrigkeiten (OWiG) ist für die **Verfolgung von Ordnungswidrigkeiten** die Verwaltungsbehörde zuständig, soweit nicht die Staatsanwaltschaft oder an ihrer Stelle für einzelne Verfolgungshandlungen der Richter hierzu berufen ist. Für die **Ahndung von Ordnungswidrigkeiten** ist ebenfalls die Verwaltungsbehörde zuständig, soweit nicht das Gericht hierzu berufen ist, vgl. § 35 Abs. 2 OWiG. Wer zuständige Verwaltungsbehörde ist, regelt in Bayern die sogenannte **Zuständigkeitsverordnung (ZustV)**.

Die **Zuständigkeit der Bayerischen Polizei** zur Verfolgung und Ahndung von Verkehrsverstößen gemäß § 24 StVG, insbesondere von Verstößen im ruhenden Verkehr und von Geschwindigkeitsverstößen, folgt aus § 91 Abs. 1 und 2 ZustV.

Für die Verfolgung und Ahndung von Ordnungswidrigkeiten im Sinne des § 24 Straßenverkehrsgesetz (StVG) besteht gemäß § 26 Abs. 1 StVG die Möglichkeit, neben der Polizei auch den **Gemeinden die Befugnis zur Verfolgung und Ahndung hierfür zu übertragen** („Behörde […], die von der Landesregierung durch Rechtsverordnung näher bestimmt wird"). Hiervon hat der bayerische Verordnungsgeber Gebrauch gemacht und eine Übertragung dieser Zuständigkeit auch an die Gemeinden angeordnet, vgl. § 88 Abs. 3 Satz 1 ZustV. Diese Zuständigkeitsregelung betrifft neben Ordnungswidrigkeiten im ruhenden Straßenverkehr (Parkraumüberwachung) vor allem auch Geschwindigkeitsverstöße. Die Gemeinde kann in diesen Fällen neben der Polizei die Verkehrsüberwachung selbst durchführen (sogenannte **kommunale Verkehrsüberwachung**) und etwaige Verstöße im Rahmen eines Ordnungswidrigkeitenverfahrens (§§ 46 ff. OWiG) verfolgen und ahnden. Die Gemeinden können die Aufgabe an **kommunale Zweckverbände** (Zweckverbände für kommunale Verkehrsüberwachung) übertragen, die als Körperschaften des öffentlichen Rechts Aufgaben ihrer Mitgliedsgemeinden wahrnehmen. Sie können teilweise auch anderen Gemeinden die Aufgabenwahrnehmung im Rahmen einer Zweckvereinbarung anbieten.

Eine **Übertragung dieser hoheitlichen Aufgabe der Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten auf Private** ist demgegenüber nur sehr bedingt zulässig. Mit dieser Frage hat sich das Bayerische Oberste Landesgericht in seinem Beschluss vom 29. Oktober 2019, 202 ObOWi 1600/19, eingehend befasst. Dabei ist es zu folgendem Ergebnis gelangt (Auszug aus den Leitsätzen):[3]

„1. Die Heranziehung privater Dienstleister zur eigenständigen Feststellung und Verfolgung von Geschwindigkeitsverstößen im Rahmen der kommunalen Verkehrsüberwachung ist unzulässig. Macht die Gemeinde von der gesetzlichen Befugnis zur Verkehrsüberwachung Gebrauch, darf sie sich hierbei privater Dienstleister nur bedienen, wenn sichergestellt ist, dass sie ‚Herrin' des Verfahrens bleibt, wozu insbesondere die Vorgaben über Ort, Zeit, Dauer und Häufigkeit der Messungen, die Kontrolle des Messvorgangs, die Verantwortung für den ordnungsgemäßen Einsatz technischer Hilfsmittel und die Kontrolle über die Ermittlungsdaten gehören sowie die Entscheidung darüber, ob und gegen wen ein Bußgeldverfahren einzuleiten ist […].

[3] Bayerisches Oberstes Landesgericht, Beschluss vom 29. Oktober 2019, 202 ObOWi 1600/19, BeckRS 2019, 31169 (gekürzt).

2. Nimmt die Gemeinde als Verfolgungsbehörde bei der Durchführung von Geschwindigkeitsmessungen oder deren Auswertung einen privaten Dienstleister in Anspruch, der ihr Personal nach den Bestimmungen des AÜG überlässt, und ist dieses Personal – unter Aufgabe der Abhängigkeiten und des Weisungsrechts der Entleihfirma – hinreichend in die räumlichen und organisatorischen Strukturen der Gemeinde integriert sowie der für das Verfahren zu-ständigen Organisationseinheit der Gemeinde zugeordnet und deren Leiter unterstellt, so ist das Handeln des überlassenen Mess- bzw. Auswertepersonals unmittelbar der Gemeinde als hoheitliche Tätigkeit zuzurechnen […]. Im Rahmen der Auswertung von Messdaten durch Leiharbeitnehmer ist eine hinreichende Kontrolle der Gemeinde über die (digitalen) Ermittlungsdaten grundsätzlich nur dann hinreichend gewährleistet, wenn sich die Messdatensätze auf einem ausschließlich der Gemeinde oder dem von ihr mit der Auswertung betrauten Leiharbeitnehmer zugänglichen Speichermedium befinden. […]

3. Auch sonst darf sich die Gemeinde der (technischen) Hilfe eines privaten Dienstleisters bedienen, wenn diese nicht in Bereiche eingreift, die ausschließlich hoheitliches Handeln erfordern und sichergestellt ist, dass die Verantwortung für den ordnungsgemäßen Einsatz technischer Hilfsmittel sowohl bei der Messung selbst als auch bei der Auswertung bei ihr verbleibt. […]

4. Die Gemeinde bleibt jedenfalls dann ‚Herrin' des Verfahrens, wenn sich die Tätigkeit des Dienstleisters auf die Aufbereitung der Daten einer Messreihe (etwa durch Vergrößerung bzw. Aufhellung von Bildern oder sonstige rein qualitative Bildbearbeitungen) beschränkt und die Resultate anschließend durch die Gemeinde selbst oder das an sie entliehene Auswertepersonal einer Kontrolle auf Vollständigkeit, Authentizität und Integrität sowie Verwertbarkeit unterzogen werden. Dabei muss sichergestellt sein, dass die Bestimmungen des Datenschutzes durch den privaten Dienstleister strikt eingehalten werden und dieser nach der Rückübertragung keinen Zugriff mehr auf die Daten hat. Dies schließt eine Vorselektion der Daten, etwa durch Vorenthaltung wegen mangelnder Beweiseignung, seitens des privaten Dienstleisters aus […]."

Die nachfolgenden Ausführungen gelten für die Durchführung von Ermittlungsverfahren in Bayern durch die Bayerische Polizei, die Gemeinden und die Zweckverbände für kommunale Verkehrsüberwachung als zuständige Verwaltungsbehörden.

2.2 Ermittlung, Feststellung und Nachweis eines Verstoßes

2.2.1 Bildaufnahmen im ruhenden Verkehr

Ausgehend von Bürgereingaben und Behördenanfragen habe ich mich mit der Frage beschäftigt, unter welchen Voraussetzungen bei der Verfolgung von Verkehrsordnungswidrigkeiten im Zusammenhang **mit Parkverstößen** von den Behörden **Bildaufnahmen** angefertigt werden dürfen. Bei der Anfertigung von Bildaufnahmen handelt es sich um eine Verarbeitung in Form der Erhebung personenbezogener Daten (in der Regel des Kraftfahrzeugs mit Kfz-Kennzeichen) zum Zwecke der Feststellung und der Nachweisbarkeit eines Verstoßes.

Die Anfertigung von Lichtbildern zur Verfolgung von Parkverstößen findet ihre **Rechtsgrundlage** in **§ 100h Abs. 1 Satz 1 Nr. 1 Strafprozessordnung (StPO) in Verbindung mit § 46 Abs. 1 OWiG**.

§ 100h StPO
Weitere Maßnahmen außerhalb von Wohnraum
(1) [1]Auch ohne Wissen der betroffenen Personen dürfen außerhalb von Wohnungen
1. Bildaufnahmen hergestellt werden,
2. sonstige besondere für Observationszwecke bestimmte technische Mittel verwendet werden,
wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise weniger erfolgversprechend oder erschwert wäre. [2]Eine Maßnahme nach Satz 1 Nr. 2 ist nur zulässig, wenn Gegenstand der Untersuchung eine Straftat von erheblicher Bedeutung ist.
(2) [1]Die Maßnahmen dürfen sich nur gegen einen Beschuldigten richten. [2]Gegen andere Personen sind
1. Maßnahmen nach Absatz 1 Nr. 1 nur zulässig, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre,
2. Maßnahmen nach Absatz 1 Nr. 2 nur zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass sie mit einem Beschuldigten in Verbindung stehen oder eine solche Verbindung hergestellt wird, die Maßnahme zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Beschuldigten führen wird und dies auf andere Weise aussichtslos oder wesentlich erschwert wäre.
(3) Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar mitbetroffen werden.
(4) § 100d Absatz 1 und 2 gilt entsprechend.

§ 46 Abs. 1 OWiG
Anwendung der Vorschriften über das Strafverfahren
(1) Für das Bußgeldverfahren gelten, soweit dieses Gesetz nichts anderes bestimmt, sinngemäß die Vorschriften der allgemeinen Gesetze über das Strafverfahren, namentlich der Strafprozeßordnung, des Gerichtsverfassungsgesetzes und des Jugendgerichtsgesetzes.
[…]

Grundsätzlich begegnet die Anfertigung von Lichtbildern der betreffenden Fahrzeuge oder des betreffenden Umfeldes bei Parkverstößen durch die zuständigen Ordnungswidrigkeitenbehörden an sich keinen Einwänden. Dies gilt jedenfalls, soweit Lichtbilder von dem betreffenden Fahrzeug und der **konkreten Verkehrssituation** angefertigt werden, die zur Verfolgung des Vorwurfs erforderlich sind und dabei nicht gezielt etwa Personen oder Fahrzeuge erfasst werden, die mit der Verfolgung des Verkehrsverstoßes in keinerlei Zusammenhang stehen. Grundlegende **datenschutzrechtliche Bedenken** habe ich hingegen, soweit personenbezogene Inhalte der – gegebenenfalls zulässig angefertigten – Lichtbilder, welche zur Verfolgung des Parkverstoßes nicht erforderlich sind, **nicht unkenntlich** gemacht werden. Dazu zählen insbesondere Passanten im Hintergrund oder Kennzeichen anderer unbeteiligter Fahrzeuge. Bereits bei der Anfertigung der Lichtbilder ist darauf zu achten, solche überschießenden Datenerhebungen zu vermeiden. Gelingt dies im Einzelfall nicht, ist eine entsprechende Schwärzung

von unbeteiligten Personen (Gesichter) und unbeteiligten Fahrzeugen (Kennzeichen) auf den Fotos erforderlich. Dabei ist die gebotene Schwärzung zur Sicherung des Rechts auf informationelle Selbstbestimmung so früh als möglich und damit nicht erst auf den eventuellen Ausdrucken der Fotos, sondern grundsätzlich bereits im elektronischen Bearbeitungssystem selbst durchzuführen.

Entscheidend ist damit auch, dass ein **konkreter Vorwurf** im Raum steht und **anlassbezogen Bildaufnahmen** getätigt werden. Unzulässig ist es hingegen, vorsorglich Bildaufnahmen herzustellen, wenn noch gar kein Verstoß – beispielweise vor Ablauf der bezahlten Parkzeit – im Raum steht.

Das Anfertigen von Lichtbildaufnahmen zur Feststellung und Dokumentation von Parkverstößen kann auch **zusätzlich zu einer Zeugenaussage grundsätzlich als erforderlich angesehen werden**. Die Lichtbilder sind als Augenscheinsobjekt im Bußgeldverfahren – auch vor Gericht – grundsätzlich verwertbar und stellen damit neben der Zeugenaussage der Beschäftigten der Verkehrsüberwachung ein weiteres Beweismittel dar, welches zudem von anderer Art (Augenschein statt Zeugenbeweis) und damit anderer Qualität ist.

Hinsichtlich des technisch-organisatorischen Verfahrens der Erstellung und Speicherung der Fotos sind dem Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit und die Unversehrtheit der Daten gewährleisten.

2.2.2 Bildaufnahmen zur Feststellung von Geschwindigkeits- und Abstandsverstößen

Im fließenden Verkehr kommen zur Feststellung von Verstößen gegen Geschwindigkeitsbeschränkungen oder Regeln zum Mindestabstand neben **Bildaufnahmen** – wie dem Messfoto bei einer Radarmessung – auch **videogestützte Messungen** in Betracht. Dabei werden neben dem Kfz-Kennzeichen im Fahrgastraum befindliche Personen – insbesondere die Fahrerin oder der Fahrer – aufgenommen, also personenbezogene Daten verarbeitet. **Rechtsgrundlage** für die Anfertigung solcher Aufnahmen – sowohl von statischen Lichtbildern als auch von Videos – ist **§ 100h Abs. 1 Satz 1 Nr. 1, Abs. 3 StPO in Verbindung mit § 46 Abs. 1 OWiG**.

Das Bundesverfassungsgericht hat bereits 2009 festgestellt,[4] dass eine **videogestützte Verkehrskontrolle**, bei der der gesamte Verkehr **ohne konkreten Tatverdacht** überwacht wird, unzulässig ist. Es liege insofern ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung vor, der einer gesetzlichen Grundlage bedürfe. Ein Jahr später hat das Bundesverfassungsgericht bestätigt,[5] dass § 100h Abs. 1 Satz 1 Nr. 1 StPO als Rechtsgrundlage für die Anfertigung von Bildaufnahmen zum Beweis von Verkehrsverstoßen herangezogen werden könne. Die Erhebung personenbezogener Daten dürfe sich jedoch nur auf die das Fahrzeug führende Personen richten, die selbst Anlass zur Anfertigung von Bildaufnahmen gegeben hätten, bei denen also der Verdacht eines bußgeldbewehrten Verkehrsverstoßes bestehe.

4 Bundesverfassungsgericht, Beschluss vom 11. August 2009, 2 BvR 941/08, BeckRS 2009, 37658.

5 Bundesverfassungsgericht, Beschluss vom 5. Juli 2010, 2 BvR 759/10, BeckRS 2010, 50877.

Wird ein Geschwindigkeitsverstoß mittels **Lasermessung** festgestellt, so erfolgt in der Regel keine Bildaufnahme. Dies ist auch nicht erforderlich, da der Fahrzeugführer anschließend unmittelbar angehalten wird und seine personenbezogenen Daten zur weiteren Verfolgung und Ahndung des Verstoßes erhoben werden können. Es bedarf demnach keiner weiteren Identifizierung mittels Lichtbildaufnahme der Person, die den Verstoß zu verantworten hat.

2.3 Ermittlung der Fahrzeughalterin oder des Fahrzeughalters

Sowohl Verstöße im ruhenden Verkehr als auch Verstöße im fließenden Verkehr können es erforderlich machen, die jeweilige Fahrzeughalterin oder den jeweiligen Fahrzeughalter zu ermitteln. Diese müssen nicht immer Eigentümerin oder Eigentümer des Kraftfahrzeugs sein. Auch im Falle eines Leasingvertrages ist meist die Leasingnehmerin oder der Leasingnehmer – obwohl nicht Eigentümerin oder Eigentümer – Halterin oder Halter des Kraftfahrzeugs. Halterin oder Halter ist in der Regel diejenige Person, die bei der Zulassungsstelle als Halter(in) vermerkt und in der Zulassungsbescheinigung Teil II (früher Fahrzeugbrief) eingetragen ist.

Für das Verhalten des Fahrzeugs im Verkehr ist zwar in erster Linie die das Fahrzeug führende Person **verantwortlich**, die Halterin oder den Halter trifft aber eine Mitverantwortung unter anderem **für die Auswahl** und unter Umständen auch für die **Überwachung der Fahrzeugführerin oder des Fahrzeugführers**. Dies gilt auch dann, wenn die Halterin oder der Halter selbst nicht am Verkehr teilnimmt.

Die **Fahrzeughalterin oder der Fahrzeughalter** wird in der Regel mittels einer Abfrage des Kfz-Kennzeichens beim Kraftfahrtbundesamt ermittelt. Auf die Angabe des Kfz-Kennzeichens hin übermittelt das Kraftfahrtbundesamt die für eine Kontaktaufnahme erforderlichen personenbezogenen Daten. Rechtsgrundlage für die Anfrage beim Kraftfahrtbundesamt und damit für eine Erhebung personenbezogener Daten durch die für die Ahndung der jeweiligen Verkehrsordnungswidrigkeit zuständige Verwaltungsbehörde ist die sogenannte **Ermittlungsgeneralklausel in § 161 Abs. 1 StPO in Verbindung mit § 46 Abs. 1 und 2 OWiG**. Eine Übermittlungsbefugnis für das Kraftfahrtbundesamt ergibt sich aus § 35 Abs. 1 Nr. 3 StVG. Danach ist eine Übermittlung an Behörden zulässig, wenn dies zur Verfolgung von Ordnungswidrigkeiten erforderlich ist.

§ 161 StPO
Allgemeine Ermittlungsbefugnis der Staatsanwaltschaft
(1) [1]Zu dem in § 160 Abs. 1 bis 3 bezeichneten Zweck ist die Staatsanwaltschaft befugt, von allen Behörden Auskunft zu verlangen und Ermittlungen jeder Art entweder selbst vorzunehmen oder durch die Behörden und Beamten des Polizeidienstes vornehmen zu lassen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln. [2]Die Behörden und Beamten des Polizeidienstes sind verpflichtet, dem Ersuchen oder Auftrag der Staatsanwaltschaft zu genügen, und in diesem Falle befugt, von allen Behörden Auskunft zu verlangen.
[…]

§ 46 OWiG
Anwendung der Vorschriften über das Strafverfahren
(1) Für das Bußgeldverfahren gelten, soweit dieses Gesetz nichts anderes bestimmt, sinngemäß die Vorschriften der allgemeinen Gesetze über das Strafverfahren, namentlich der Strafprozeßordnung, des Gerichtsverfassungsgesetzes und des Jugendgerichtsgesetzes.
(2) Die Verfolgungsbehörde hat, soweit dieses Gesetz nichts anderes bestimmt, im Bußgeldverfahren dieselben Rechte und Pflichten wie die Staatsanwaltschaft bei der Verfolgung von Straftaten.
[…]

§ 35 Abs. 1 StVG
Übermittlung von Fahrzeugdaten und Halterdaten
(1) Die nach § 33 Absatz 1 gespeicherten Fahrzeugdaten und Halterdaten dürfen an Behörden und sonstige öffentliche Stellen im Geltungsbereich dieses Gesetzes sowie im Rahmen einer internetbasierten Zulassung an Personen im Sinne des § 6g Absatz 3 zur Erfüllung der Aufgaben der Zulassungsbehörde, des Kraftfahrt-Bundesamtes oder der Aufgaben des Empfängers nur übermittelt werden, wenn dies für die Zwecke nach § 32 Absatz 2 jeweils erforderlich ist
[…]
3. zur Verfolgung von Ordnungswidrigkeiten,
[…]

Eine solche Abfrage der Fahrzeughalterin oder des Fahrzeughalters erachte ich grundsätzlich dann als **nicht erforderlich**, wenn die Fahrzeugführerin oder der Fahrzeugführer an Ort und Stelle bereits identifiziert ist, wie beispielsweise im Falle einer Lasermessung (siehe Nr. 2.2.2). Es ist dabei in der Regel unerheblich, ob die das Fahrzeug führende Person auch Fahrzeughalterin oder Fahrzeughalter ist. Die oder der Verantwortliche ist dann bereits ermittelt und der Verstoß kann gegebenenfalls geahndet werden.

Auch im **ruhenden Verkehr** ist eine Anforderung der personenbezogenen Daten der Fahrzeughalterin oder des Fahrzeughalters beim Kraftfahrtbundesamt zur Verfolgung und Ahndung einer Verkehrsordnungswidrigkeit nicht stets erforderlich. Eine von mir durchgeführte datenschutzrechtliche Prüfung bei Gemeinden und Zweckverbänden betreffend den Datenschutz bei der Verfolgung von Ordnungswidrigkeiten im ruhenden Verkehr (siehe mein 29. Tätigkeitsbericht 2019 unter Nr. 4.5) kam zu dem Ergebnis, dass personenbezogene Daten von Kraftfahrzeughalterinnen und Kraftfahrzeughaltern zu oft abgerufen wurden. So kam es bereits routinemäßig zu einem automatisierten Abruf der Halterinnen- oder Halterdaten beim Kraftfahrtbundesamt, wenn wegen eines Parkverstoßes eine Verwarnung erteilt wurde. Aus datenschutzrechtlicher Sicht ist eine solche Datenerhebung noch vor Ablauf der im Ordnungswidrigkeitengesetz eingeräumten einwöchigen Zahlungsfrist nicht erforderlich. Wird das Verwarnungsgeld fristgerecht bezahlt, ist eine Erhebung der Halterinnen- oder Halterdaten zum falschgeparkten Kraftfahrzeug entbehrlich. Erst nach erfolgslosem Ablauf der Zahlungsfrist oder für den Fall, dass aus technischen Gründen kein Verwarnungszettel angebracht oder ausgestellt werden kann, ist für die Kontaktaufnahme ein Abruf der Halterinnen oder Halterdaten beim Kraftfahrtbundesamt erforderlich.

Ich konnte erreichen, dass die verwendeten Softwareprogramme so umprogrammiert wurden, dass erst nach erfolglosem Ablauf der Zahlungsfrist eine automatisierte Abfrage der Halterinnen- oder Halterdaten beim Kraftfahrtbundesamt erfolgt. Als datenschutzrechtlich zulässig erachte ich hingegen die Möglichkeit eines

manuellen Abrufs der Halterdaten für den Fall, dass aus technischen Gründen kein Strafzettel ausgestellt oder angebracht werden kann, so dass der Halter direkt angeschrieben werden muss.

2.4 Ermittlung der Fahrzeugführerin oder des Fahrzeugführers

Die für einen Verkehrsverstoß mit einem Kraftfahrzeug verantwortliche Person ist nicht immer dessen Halterin oder Halter. Beispielsweise kann es sich um einen Firmenwagen handeln, oder ein Familienmitglied ist mit dem Kraftfahrzeug gefahren.

Im Falle von **Verstößen gegen die Geschwindigkeitsbeschränkungen und Vorgaben zum Mindestabstand** ist es zur Verfolgung und Ahndung erforderlich, die jeweiligen Fahrzeugführerin oder den jeweiligen Fahrzeugführer zu ermitteln. In den Fällen einer Lasermessung ist diese Person in der Regel bereits identifiziert (siehe Nr. 2.2.2).

2.4.1 Anhörungs- und Zeugenfragebogen

Ist eine Feststellung der Person erforderlich, die den Verstoß im **fließenden Verkehr** begangen hat, erhält die Fahrzeughalterin oder der Fahrzeughalter entweder einen sogenannten Anhörungsbogen oder einen Zeugenfragebogen.

Nimmt die Verwaltungsbehörde in Anbetracht der vom Kraftfahrtbundesamt übermittelten Daten (siehe Nr. 2.3) an, dass auf einem Lichtbild oder Video die Halterin oder der Halter selbst als fahrzeugführende Person zu sehen ist (etwa weil das Geschlecht und ungefähre Alter übereinstimmen), versendet sie einen sogenannten **Anhörungsbogen** an die Fahrzeughalterin oder den Fahrzeughalter. Rechtsgrundlage hierfür ist § 55 OWiG. Sie oder er erhält damit den **Status einer oder eines Betroffenen** im Ordnungswidrigkeitenverfahren.

§ 55 OWiG
Anhörung des Betroffenen
(1) § 163a Abs. 1 der Strafprozeßordnung ist mit der Einschränkung anzuwenden, daß es genügt, wenn dem Betroffenen Gelegenheit gegeben wird, sich zu der Beschuldigung zu äußern.
(2) [1]Der Betroffene braucht nicht darauf hingewiesen zu werden, daß er auch schon vor seiner Vernehmung einen von ihm zu wählenden Verteidiger befragen kann. [2]§ 136 Absatz 1 Satz 3 bis 5 der Strafprozeßordnung ist nicht anzuwenden.

Verpflichtend hat in den Anhörungsbögen eine **Belehrung** zu erfolgen. Die oder der Betroffene, der oder dem eine Ordnungswidrigkeit zur Last gelegt wird, ist darüber zu belehren, dass es ihr oder ihm nach dem Gesetz **freisteht, sich zur Beschuldigung zu äußern oder nicht zur Sache auszusagen** (§ 46 Abs. 1 OWiG in Verbindung mit § 136 Abs. 1 Satz 2 StPO). Lediglich zu den Angaben über ihre oder seine Person ist die oder der Betroffene verpflichtet (§ 111 OWiG).

§ 136 StPO
Erste Vernehmung
(1) […] [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. […]

§ 111 OWiG
Falsche Namensangabe
(1) Ordnungswidrig handelt, wer einer zuständigen Behörde, einem zuständigen Amtsträger oder einem zuständigen Soldaten der Bundeswehr über seinen Vor-, Familien- oder Geburtsnamen, den Ort oder Tag seiner Geburt, seinen Familienstand, seinen Beruf, seinen Wohnort, seine Wohnung oder seine Staatsangehörigkeit eine unrichtige Angabe macht oder die Angabe verweigert.
(2) Ordnungswidrig handelt auch der Täter, der fahrlässig nicht erkennt, daß die Behörde, der Amtsträger oder der Soldat zuständig ist.
(3) Die Ordnungswidrigkeit kann, wenn die Handlung nicht nach anderen Vorschriften geahndet werden kann, in den Fällen des Absatzes 1 mit einer Geldbuße bis zu eintausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu fünfhundert Euro geahndet werden.

Bestehen dagegen bei einem Lichtbild oder einem Video Zweifel, dass die Halterin oder der Halter die fahrzeugführende Person ist (dies ist in der Regel der Fall, wenn Geschlecht oder ungefähres Alter nicht übereinstimmen), wird an die Fahrzeughalterin oder den Fahrzeughalter ein sogenannter **Zeugenfragebogen** versendet.

Ist die **Fahrzeughalterin oder** der **Fahrzeughalter Zeugin oder Zeuge**, weil sie oder er das Fahrzeug zum Zeitpunkt des Verstoßes nicht geführt hat, ist **sie oder er grundsätzlich verpflichtet**, wahrheitsgemäß anzugeben, wer das Kraftfahrzeug geführt hat (§ 46 Abs. 1, 2 OWiG in Verbindung mit § 161a Abs. 1 Satz 1 StPO).

Zeuginnen und Zeugen sind darüber **zu belehren**, dass sie die Antwort auf solche Fragen **verweigern dürfen**, durch deren wahrheitsgemäße Beantwortung sie **sich selbst oder in § 52 Abs. 1 StPO bezeichnete Angehörige** (Verlobte, Ehegatten, Lebenspartner, bestimmte verwandte und verschwägerte Personen) der Gefahr der Verfolgung wegen einer Straftat oder einer Ordnungswidrigkeit aussetzen würden (§ 46 Abs. 1 OWiG in Verbindung mit § 55 StPO). Liegt ein solcher (Ausnahme-)Fall vor, müssen keine Angaben zur Fahrzeugführerin oder zum Fahrzeugführer gemacht werden.

Erforderlich ist also eine Belehrung über das **Zeugnisverweigerungs-** (§ 46 Abs. 1 OWiG in Verbindung mit § 52 StPO) und das **Auskunftsverweigerungsrecht** (§ 46 Abs. 1 OWiG in Verbindung mit § 55 StPO).

§ 52 StPO
Zeugnisverweigerungsrecht der Angehörigen des Beschuldigten
(1) Zur Verweigerung des Zeugnisses sind berechtigt
1. der Verlobte des Beschuldigten;
2. der Ehegatte des Beschuldigten, auch wenn die Ehe nicht mehr besteht;
2a. der Lebenspartner des Beschuldigten, auch wenn die Lebenspartnerschaft nicht mehr besteht;
3. wer mit dem Beschuldigten in gerader Linie verwandt oder verschwägert, in der Seitenlinie bis zum dritten Grad verwandt oder bis zum zweiten Grad verschwägert ist oder war.
(2) [1]Haben Minderjährige wegen mangelnder Verstandesreife oder haben Minderjährige oder Betreute wegen einer psychischen Krankheit oder einer geistigen

oder seelischen Behinderung von der Bedeutung des Zeugnisverweigerungsrechts keine genügende Vorstellung, so dürfen sie nur vernommen werden, wenn sie zur Aussage bereit sind und auch ihr gesetzlicher Vertreter der Vernehmung zustimmt. [2]Ist der gesetzliche Vertreter selbst Beschuldigter, so kann er über die Ausübung des Zeugnisverweigerungsrechts nicht entscheiden; das gleiche gilt für den nicht beschuldigten Elternteil, wenn die gesetzliche Vertretung beiden Eltern zusteht.
(3) [1]Die zur Verweigerung des Zeugnisses berechtigten Personen, in den Fällen des Absatzes 2 auch deren zur Entscheidung über die Ausübung des Zeugnisverweigerungsrechts befugte Vertreter, sind vor jeder Vernehmung über ihr Recht zu belehren. [2]Sie können den Verzicht auf dieses Recht auch während der Vernehmung widerrufen.

§ 55 StPO
Auskunftsverweigerungsrecht
(1) Jeder Zeuge kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihm selbst oder einem der in § 52 Abs. 1 bezeichneten Angehörigen die Gefahr zuziehen würde, wegen einer Straftat oder einer Ordnungswidrigkeit verfolgt zu werden.
(2) Der Zeuge ist über sein Recht zur Verweigerung der Auskunft zu belehren.

Eine solche Belehrung sollte vorsichtshalber aber im Anhörungsbogen an die oder den Betroffenen – neben der Belehrung gemäß § 46 Abs. 1 OWiG in Verbindung mit § 136 Abs. 1 Satz 2 StPO, sogenanntes **Aussageverweigerungsrecht** – aufgenommen werden, wenn dort die Möglichkeit vorgesehen ist, die tatsächliche Fahrerin oder den tatsächlichen Fahrer anzugeben. Ist die Empfängerin oder der Empfänger des Anhörungsbogens nämlich entgegen der Vermutung der Verwaltungsbehörde nicht die Fahrerin oder der Fahrer, so hat sie oder er die Rolle einer Zeugin oder eines Zeugen – und sollte als solche oder solcher nicht „unbelehrt" bleiben.

Sowohl auf dem Anhörungs- als auch dem Zeugenfragebogen ist regelmäßig ein „Blitzerfoto", abgebildet, damit die Fahrzeughalterin oder der Fahrzughalter entweder sich selbst erkennen oder die das Fahrzeug führende Person identifizieren kann. Im Rahmen der Ermittlung sind Bilder in der Form vorzulegen, dass unbeteiligte (insbesondere mitfahrende) Personen nicht zu erkennen sind.

In den vergangenen Jahren war ich schließlich mit mehreren Eingaben befasst, die sich gegen den **Umfang der abgefragten Daten in Anhörungsbögen** kommunaler Behörden wandten. So sollte insbesondere die Telefonnummer erhoben werden, die mit dem Hinweis auf die Sanktionierung nach § 111 OWiG als Pflichtangabe bezeichnet war. In einem Fall war zudem mit dem gleichen Hinweis nach dem „Wohnungsgeber" gefragt worden. Nach § 111 OWiG handelt ordnungswidrig, wer einer zuständigen Behörde über seinen Vor-, Familien- oder Geburtsnamen, den Ort oder Tag seiner Geburt, seinen Familienstand, seinen Beruf, seinen Wohnort, seine Wohnung oder seine Staatsangehörigkeit eine unrichtige Angabe macht oder die Angabe verweigert. Nicht aufgeführt in diesem Katalog sind die Telefonnummer sowie die Wohnungsgeberin oder der Wohnungsgeber.

Auf den von mir überprüften Anhörungsbögen fehlte nicht nur der Hinweis auf die Freiwilligkeit dieser Angaben. Im Gegenteil wurde durch den Hinweis auf § 111 OWiG gerade der Eindruck erweckt, dass die Verweigerung auch dieser Angaben bußgeldbewehrt sei. Die von mir geprüften Anhörungsbogenmuster wurden in der

Folge neu gestaltet. Dabei wurden meiner Anregung entsprechend die Angabenblöcke „Pflichtangaben“ und „freiwillige Angaben“ geschaffen, räumlich getrennt und die Angabe „Telefonnummer“ entsprechend korrekt zugeordnet. Der unklare Begriff „Wohnungsgeber“ wurde durch „evtl. Hauptmieter“ ersetzt.

2.4.2 Zulässigkeit eines Personalausweis- oder Passbildabgleichs

Richtet sich **der Verdacht einer Verkehrsordnungswidrigkeit gegen die Fahrzeughalterin oder den Fahrzeughalter**, so hat diese oder dieser regelmäßig einen Anhörungsbogen erhalten. Sendet sie oder er diesen nicht innerhalb einer angemessenen Frist zurück oder äußert sie oder er sich darin nicht zur Sache, halte ich den Abgleich eines aufgezeichneten Lichtbilds oder Videos mit dem Personalausweis- oder Passregister ohne weitere Zwischenschritte für zulässig. Die Halterin oder der Halter gibt in diesem Fall nämlich klar zu erkennen, dass sie oder er nicht bereit ist, an einer Aufklärung des Sachverhalts mitzuwirken.

Lassen die Umstände diese Annahme hingegen nicht zu, so ist entsprechend den im Folgenden dargestellten gesetzlichen Regelungen grundsätzlich zunächst zu versuchen, die benötigten Daten bei der Halterin oder dem Halter zu erheben.[6] Äußert sich diese oder dieser beispielsweise dahingehend, dass sie oder er sich nicht mehr sicher sei, ob sie oder er selbst oder eine dritte Person gefahren sei, so ist sie oder er entweder aufzusuchen, vorzuladen oder um die Übersendung eines Lichtbildes ihrer oder seiner Person zu bitten.

Richtet sich der **Verdacht gegen eine bestimmte andere Person** wie beispielsweise gegen eine oder einen bestimmte(n) Beschäftigte(n) bei einem Firmenwagen oder einen Familienangehörigen der Fahrzeughalterin oder des Fahrzeughalters, so halte ich es ebenfalls in der Regel für unzulässig, ohne weitere Ermittlungsversuche bezüglich der bestimmten anderen Person einen Lichtbildabgleich mit dem Personalausweis- oder Passregister durchzuführen.[7]

Die Erhebungsbefugnis für die Ordnungswidrigkeitenbehörde Daten – insbesondere Lichtbilder – von den Personalausweis- und Passbehörden anzufordern, ergibt sich aus § 161 Abs. 1 StPO in Verbindung mit § 46 Abs. 1 und 2 OWiG

Gemäß § 24 Abs. 2 Personalausweisgesetz (PAuswG) sowie § 22 Abs. 2 Passgesetz (PassG) dürfen Personalausweis- oder Passbehörden anderen Behörden – und damit auch den Ordnungswidrigkeitenbehörden – auf deren Ersuchen Daten aus dem Personalausweis- oder Passregister (dazu zählen auch die Lichtbilder) nur übermitteln, wenn

6 **COVID-19-Pandemie:** Das Innenministerium ist an mich herangetreten und hat darum gebeten, während der COVID-19-Pandemie und den geltenden Kontaktbeschränkungen gerade von den persönlichen Nachschauen bei den betroffenen Personen oder auch den Halterinnen und Haltern Abstand nehmen zu dürfen, um Kontakte zu vermeiden beziehungsweise zu verringern und damit die Gefährdung sowohl der betroffenen Personen als auch des Personals zu minimieren. Vor dem Hintergrund des Infektionsgeschehens sei eine Datenerhebung bei den betroffenen Personen nicht oder nur mit unverhältnismäßig hohem Aufwand im Sinne der § 24 Abs. 2 Satz 1 Nr. 3 PAuswG und § 22 Abs. 2 Satz 2 Nr. 3 PassG möglich. Hiergegen habe ich nach Abwägung der Interessen – Infektions-, Gesundheits- und Datenschutz – unter der Prämisse zeitlicher Befristungen und jeweils neuer Prüfung der aktuell vorherrschenden Pandemielage keine Einwände erhoben.

7 Vgl. insoweit die vorige Fußnote.

1. die ersuchende Behörde auf Grund von Gesetzen oder Rechtsverordnungen berechtigt ist, solche Daten zu erhalten,

2. die ersuchende Behörde ohne Kenntnis der Daten nicht in der Lage wäre, eine ihr obliegende Aufgabe zu erfüllen und

3. die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können oder nach der Art der Aufgabe, zu deren Erfüllung die Daten erforderlich sind, von einer solchen Datenerhebung abgesehen werden muss.

Die Verantwortung für derartige Lichtbildübermittlungen trägt die ersuchende Behörde (vgl. § 24 Abs. 3 Satz 1 PAuswG, § 22 Abs. 3 Satz 1 PassG). Die ersuchende Behörde hat den Anlass des Ersuchens und die Herkunft der übermittelten Daten und Unterlagen **aktenkundig** zu machen (vgl. § 24 Abs. 3 Satz 3 PAuswG, § 22 Abs. 3 Satz 3 PassG).

§ 24 PAuswG
Verwendung im Personalausweisregister gespeicherter Daten
[…]
(3) Die ersuchende Behörde trägt die Verantwortung dafür, dass die Voraussetzungen des Abs. 2 vorliegen. Ein Ersuchen nach Abs. 2 darf nur von Bediensteten gestellt werden, die vom Behördenleiter dazu besonders ermächtigt sind. Die ersuchende Behörde hat den Anlass des Ersuchens und die Herkunft der übermittelten Daten und Unterlagen zu dokumentieren. Wird die Personalausweisbehörde vom Bundesamt für Verfassungsschutz, den Landesbehörden für Verfassungsschutz, dem Militärischen Abschirmdienst, dem Bundesnachrichtendienst, dem Bundeskriminalamt oder dem Generalbundesanwalt oder der Generalbundesanwältin um die Übermittlung von Daten ersucht, so hat die ersuchende Behörde den Familiennamen, die Vornamen und die Anschrift des Betroffenen unter Hinweis auf den Anlass der Übermittlung aufzuzeichnen. Die Aufzeichnungen sind gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Übermittlung folgt, zu vernichten.
[…]

Aus datenschutzrechtlicher Sicht ist es daher erforderlich, dass die zuständige Sachbearbeiterin oder der zuständige Sachbearbeiter einen entsprechenden **Aktenvermerk** fertigt, der die Voraussetzungen für eine Lichtbildübermittlung dokumentiert und aus dem sich ergibt, dass ein **ernsthafter Kontaktversuch** unternommen worden ist.

Zu beachten ist, dass eine Lichtbildübermittlung aus dem Pass- beziehungsweise Personalausweisregister **per E-Mail ohne die Anwendung entsprechender Verschlüsselungsverfahren datenschutzrechtlich nicht zulässig ist**. Zwar kann eine Lichtbildübermittlung gemäß § 22 Abs. 2 PassG beziehungsweise § 24 Abs. 2 PAuswG nach den gesetzlichen Bestimmungen des § 22a Abs. 1 PassG und § 25 Abs. 1 PAuswG auch durch Datenübertragung erfolgen. Es gelten aber § 6a Abs. 1 Satz 3 PassG beziehungsweise § 12 Abs. 1 Satz 3 PAuswG entsprechend. Danach haben die beteiligten Stellen dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit und Unversehrtheit der Daten sowie die Feststellbarkeit der übermittelnden Stelle gewährleisten. Im Falle

der Nutzung allgemein zugänglicher Netze sind Verschlüsselungsverfahren anzuwenden, die dem jeweiligen Stand der Technik entsprechen.

§ 12 PAuswG
Form und Verfahren der Datenerfassung, -prüfung und -übermittlung
(1) Die Datenübermittlung von den Personalausweisbehörden an den Ausweishersteller zum Zweck der Ausweisherstellung, insbesondere die Übermittlung sämtlicher Ausweisantragsdaten, erfolgt durch Datenübertragung. Die Datenübertragung kann auch über Vermittlungsstellen erfolgen. Die beteiligten Stellen haben dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit und Unversehrtheit der Daten sowie die Feststellbarkeit der übermittelnden Stelle gewährleisten; im Falle der Nutzung allgemein zugänglicher Netze sind Verschlüsselungsverfahren anzuwenden, die dem jeweiligen Stand der Technik entsprechen.
[…]

2.4.3 Recherche des Fahrzeugführers im familiären Umfeld

Ergibt sich im Rahmen eines Verfahrens wegen einer Verkehrsordnungswidrigkeit, dass der Verkehrsverstoß nicht durch die Halterin oder den Halter des Fahrzeugs begangen wurde, und macht sie oder er keine Angaben zur Fahrzeugführerin oder zum Fahrzeugführer, stellt sich die Frage, welche Person das Fahrzeug geführt hat. Oft liegt es nahe, dass Fahrzeugführerin oder Fahrzeugführer eine angehörige Person der Halterin oder des Halters ist. Daher kann als Ermittlungsansatz auch eine Abfrage von Meldedaten in Betracht kommen. Datenschutzrechtlich ist eine solche Vorgehensweise wie folgt zu beurteilen:

Eine Befugnis zur **Recherche im familiären Umfeld** und damit zur Erhebung personenbezogener Daten von Angehörigen besteht für die Ordnungswidrigkeitenbehörde aufgrund der sogenannten Ermittlungsgeneralklausel gemäß § 161 Abs. 1 StPO in Verbindung mit § 46 Abs. 1 und 2 OWiG.

Die Übermittlungsbefugnis betreffend Meldedaten von Angehörigen durch die Meldebehörde an die Ordnungswidrigkeitenbehörde ergibt sich aus dem Bundesmeldegesetz und der Meldedatenverordnung. Dabei ist danach zu differenzieren, ob eine Abfrage durch die Ordnungswidrigkeitenbehörde im Wege einer automatisierten Abfrage oder einer manuellen Abfrage erfolgt. Bei einer automatisierten Abfrage hat die Ordnungswidrigkeitenbehörde Zugriff auf einen zentralen Meldedatenbestand, vgl. Art. 7 Bayerisches Gesetz zur Ausführung des Bundesmeldegesetzes (BayAGBMG). Erfolgt eine manuelle Abfrage, so wendet sich die Ordnungswidrigkeitenbehörde an die zuständige Meldebehörde.

Die Zulässigkeit der Übermittlung von Meldedaten richtet sich **bei automatisierten Abfragen** nach § 38 Bundesmeldegesetz (BMG), Art. 10 Nr. 6 BayAGBMG sowie § 1 und §§ 5, 6 Meldedatenverordnung (MeldDV)**.** Polizeibehörden haben dabei – im Vergleich zu Gemeinden – einen über den in § 5 Abs. 1 und 2 MeldDV genannten Datenumfang hinausgehenden Zugriff auf Meldedaten (§ 6 MeldDV).

Erfolgt eine **manuelle Anfrage** an die zuständige Meldebehörde, darf diese nach § 34 BMG anderen Behörden bestimmte Daten aus dem Melderegister übermitteln, wenn dies zur Erfüllung der in ihrer Zuständigkeit oder der Zuständigkeit des Empfängers liegenden Aufgaben **erforderlich** ist.

Hat die Fahrzeughalterin oder der Fahrzeughalter im Rahmen einer Anhörung keine Angaben zu der das Fahrzeug führenden Person gemacht, halte ich die Abfrage und Übermittlung der Meldedaten von Angehörigen der Fahrzeughalterin oder des Fahrzeughalters **grundsätzlich für zulässig.** Sie muss jedoch auf die Abfrage sowie Übermittlung der Daten der Personen beschränkt werden, die tatsächlich als Fahrerin oder Fahrer in Betracht kommen.

Soweit eine Eingrenzung des in Betracht kommenden „Täterinnen- und Täterkreises" möglich ist, muss diese daher bereits in dem Auskunftsersuchen gegenüber der Meldebehörde erfolgen, um die Übermittlung nicht erforderlicher Daten zu vermeiden. Dies geschieht in der Praxis häufig dadurch, dass auf dem Formschreiben angekreuzt wird, auf welche Angehörigen (Ehepartner, Sohn, Tochter, Mutter, Vater) sich die Anfrage bezieht. Ein derart eingeschränktes Auskunftsersuchen halte ich grundsätzlich für zulässig.

Dies bedeutet ferner, dass beispielsweise Meldedaten von Kindern nicht übermittelt werden dürfen. Soweit anhand eines „Tatfotos" weitere Personen – beispielsweise aufgrund ihres Alters oder Geschlechts – als Fahrzeugführerin oder Fahrzeugführer ausgeschieden werden können, dürfen ihre Daten ebenfalls nicht übermittelt werden. Schließlich dürfen keine Meldedaten von Personen, hinsichtlich derer aus sonstigen Gründen keine Anhaltspunkte dafür vorliegen, dass sie das Fahrzeug geführt haben, übermittelt werden.

2.5 Zustellung von Bußgeldbescheiden

Bußgeldbescheide sind gemäß § 51 Abs. 2 OWiG förmlich zuzustellen. In der Regel erfolgt diese Zustellung durch die Post mit **Zustellungsurkunde (PZU)** (§ 51 Abs. 1 OWiG in Verbindung mit Art. 1 Abs. 1, Art. 3 Verwaltungszustellungs- und Vollstreckungsgesetz – VwZVG). Diese Art der Zustellung hat im Vergleich zur Zustellung mittels Einschreiben die Vorteile, dass der Zustellungsvorgang beurkundet wird und die Möglichkeit einer Zustellung durch Niederlegung besteht.

Bei der Zustellung mit PZU ist nach Art. 3 Abs. 2 Satz 3 VwZVG für den notwendigen verschlossenen Umschlag der Vordruck nach der Zustellungsvordruckverordnung (ZustVV) zu verwenden. Nach Anlage 2 zu § 1 Nr. 2 ZustVV ist das Aktenzeichen auf dem Umschlag anzugeben, wobei nach § 2 Abs. 2 ZustVV auch **Umschläge mit Sichtfenster** verwendet werden dürfen. Bei Verwendung von Sichtfenstern bedarf es der **Angabe des Aktenzeichens** auf dem Umschlag nicht zwingend (§ 2 Abs. 2 Satz 2 ZustVV; die Regelung geht offenbar davon aus, dass das Aktenzeichen dann auf dem Sichtfenster erscheint). Die Angabe des Aktenzeichens auf dem verschlossenen Umschlag (auf dem Umschlag an sich oder im Sichtfenster des Umschlages) dient zur beweiskräftigen Identifizierung und späteren Zuordnung der im Umschlag einliegenden Briefsendung zur Zustellungsurkunde.

Angesichts der gesetzlichen Vorgaben der Zustellungsvordruckverordnung und der Notwendigkeit, die Zustellung und Zuordnung des konkreten innenliegenden Schriftstücks nachzuweisen, bestehen **gegen die sichtbare Angabe des Aktenzeichens auf dem Umschlag oder im Sichtfenster keine datenschutzrechtlichen Bedenken.**

Weiterhin ist nach Anlage 2 zu § 1 Nr. 2 ZustVV der Absender auf dem Umschlag anzugeben. § 21 Abs. 1 Allgemeine Geschäftsordnung für die Behörden des Freistaates Bayern bestimmt ebenfalls, dass dienstliche Dokumente **Angaben über ihren Absender enthalten müssen**, wozu auch die Behördenbezeichnung zählt. Hierdurch soll sichergestellt werden, dass der Empfänger des Schreibens ohne jeden Zweifel erkennen kann, dass es sich um ein amtliches Schriftstück handelt und aus welchem Geschäftsbereich dieses stammt. Dies gilt umso mehr, wenn mit der Zustellung des Schriftstücks **Rechtsbehelfsfristen** in Lauf gesetzt werden.

Vereinzelt erreichen mich Beschwerden, wonach sich die betroffenen Personen gegen die Angabe „Bayerisches Polizeiverwaltungsamt – Zentrale Bußgeldstelle" auf den Briefumschlägen wenden. Die Angabe „Bayerisches Polizeiverwaltungsamt – Zentrale Bußgeldstelle" ist ein feststehender Behördenbegriff und dient der genauen Bezeichnung der für den Erlass des Bußgeldbescheids verantwortlichen Behörde beziehungsweise Abteilung. Denn die behördeninterne Zuständigkeit für den Erlass von Bußgeldbescheiden sowie die Durchführung des Bußgeldverfahrens obliegt regelmäßig der Abteilung III des Bayerischen Polizeiverwaltungsamts (PVA), mithin der Zentralen Bußgeldstelle (ZBS) in Viechtach. Diese Abteilung tritt nach außen ausdrücklich als ZBS auf, um sich bewusst von der Abteilung II (Zentrale Verkehrsordnungswidrigkeitenstelle – Zentrale VOWi-Stelle) des PVA abzugrenzen. Um Verwechslungen mit eben dieser Abteilung zu vermeiden, insbesondere bei Einspruchseinlegung gegen einen Bußgeldbescheid, mit dessen Erlass der Zuständigkeitswechsel einhergeht, ist der Behördenzusatz erforderlich. Vor diesem Hintergrund bestehen daher auch gegen die zusätzliche Angabe der ZBS auf dem Briefumschlag keine datenschutzrechtlichen Einwände.

Schließlich ist auch die ausdrückliche Bezeichnung der Zustellung als **„Förmliche Zustellung"** auf dem Briefumschlag nicht zu beanstanden, da diese Bezeichnung ebenfalls vom Vordruck der Anlage 2 zu § 1 Nr. 2 ZustVV gefordert wird. Mit dieser ausdrücklichen Bezeichnung soll die gesetzlich vorgeschriebene Zustellung als solche nochmals eigens hervorgehoben und auf einen möglicherweise damit einhergehenden Fristenlauf hingewiesen werden.

2.6 Speicherung und Speicherfristen

2.6.1 Speicherung von Personen- und Vorgangsdaten des Ordnungwidrigkeitenverfahrens

Die Ordnungswidrigkeitenbehörden dürfen Personen- und Vorgangsdaten **in Dateien** verarbeiten, insbesondere speichern, soweit dies zum Zwecke des laufenden Verfahrens, zum Zwecke der künftigen Verfolgung von Ordnungswidrigkeiten und zum Zwecke der Vorgangsverwaltung erforderlich ist.

Für **Zwecke des laufenden Verfahrens** sind die gespeicherten personen- und vorgangsbezogenen Daten mit der Erledigung des Ordnungswidrigkeitenverfahrens zu löschen, soweit ihre Speicherung nicht zum Zwecke der künftigen Verfolgung und zum Zwecke der Vorgangsverwaltung zulässig ist, vgl. § 489 Abs. 1 Satz 1 Nr. 1 StPO in Verbindung mit § 49c Abs. 1 OWiG.

Zum **Zwecke der künftigen Verfolgung von Ordnungswidrigkeiten** dürfen insbesondere die Personendaten der betroffenen Person, die zuständige Stelle

und das Aktenzeichen sowie die nähere Bezeichnung der Verkehrsordnungswidrigkeit gespeichert werden. Nach festgesetzten Fristen ist zu prüfen, ob die gespeicherten Daten zu löschen sind. Diese Prüffristen betragen gem. § 49c Abs. 5 OWiG bei zum Tatzeitpunkt volljährigen Personen, gegenüber denen eine Geldbuße von mehr als 250 Euro ausgesprochen wurde, fünf Jahre und in allen übrigen Fällen zwei Jahre.

Für zum **Zwecke der Vorgangsverwaltung** gespeicherte personen- und vorgangsbezogene Daten sind zu löschen, sobald ihre Kenntnis zu diesem Zweck nicht mehr erforderlich ist, vgl. § 489 Abs. 1 Nr. 3 StPO in Verbindung mit § 49c Abs. 1 OWiG

Neben der Speicherung von Personen- und Vorgangsdaten in Dateien ist die Aufbewahrungsdauer von Schriftgut, wie beispielsweise (elektronischen) Akten, zu berücksichtigen.

Die konkret in Betracht kommenden Aufbewahrungsfristen richten sich nach verschiedenen Faktoren, wie beispielsweise der Art und Höhe der Ahndung.

2.6.2 Speicherung von Fahrverboten

Eine **Speicherung von Fahrverboten** erfolgt durch das Kraftfahrtbundesamt im sogenannten Fahreignungsregister, vgl. §§ 28 ff. StVG. Die Speicherdauer richtet sich hier nach der sogenannten Fristen für die Tilgung, vgl. § 29 StVG.

Neben einer Speicherung im Fahreignungsregister kommt auch eine Speicherung in den örtlichen Fahrerlaubnisregistern bei den Fahrerlaubnisbehörden in Betracht, vgl. § 50 Abs. 2 StVG.

2.7 Informationspflichten und Betroffenenrechte

2.7.1 Regelungsgefüge

Die obigen Ausführungen legen dar, dass eine Erhebung personenbezogener Daten entweder direkt bei der betroffenen Person oder etwa beim Kraftfahrtbundesamt, beim Fahrzeughalter oder den Meldebehörden stattfindet. Grundsätzlich löst die Erhebung personenbezogener Daten Informationspflichten nach Art. 13 und 14 DSGVO aus. Im Falle der Verfolgung und Ahndung von Ordnungswidrigkeiten besteht allerdings eine rechtliche Besonderheit.

Neben der Datenschutz-Grundverordnung haben das Europäische Parlament und der Rat auch die **Datenschutz-Richtlinie für Polizei und Strafjustiz** erlassen. Diese Richtlinie enthält besondere Regelungen für die Verarbeitung personenbezogener Daten in den Bereichen der Strafverfolgung und -vollstreckung sowie der polizeilichen Gefahrenabwehr. In den Anwendungsbereich fällt aber auch die Verfolgung und Ahndung von Ordnungswidrigkeiten. Im Unterschied zur Datenschutz-Grundverordnung muss die Datenschutz-Richtlinie für Polizei und Strafjustiz in nationales Recht umgesetzt werden; unmittelbare Wirkungen im Verhältnis zwischen den betroffenen Personen und den öffentlichen Stellen kann sie grundsätzlich nicht entfalten.

Der bayerische Gesetzgeber hat für die Umsetzung der Datenschutz-Richtlinie für Polizei und Strafjustiz im BayDSG eine auf den ersten Blick ungewöhnliche Regelungslösung gewählt: Er hat die Geltung der Datenschutz-Grundverordnung auch für diesen Bereich angeordnet (Art. 2 Satz 1 BayDSG). In Teil 2 Kapitel 8 des Bayerischen Datenschutzgesetzes (Art. 28 ff. BayDSG) hat er dessen Regelungsgefüge dann für die Strafverfolgung und -vollstreckung sowie die polizeiliche Gefahrenabwehr, Ordnungswidrigkeitenverfolgung und -ahndung näher ausgestaltet.

Art. 28 Abs. 1 Satz 1 BayDSG nennt die Behörden, für die die Art. 28 ff. BayDSG gelten: Polizei, Gerichte in Strafsachen, Staatsanwaltschaften, Strafvollstreckungs- und Justizvollzugsbehörden sowie Behörden des Maßregelvollzugs. Darüber hinaus sind nach Art. 28 Abs. 1 Satz 2 BayDSG Behörden erfasst, die personenbezogene Daten verarbeiten, um Straftaten oder Ordnungswidrigkeiten zu verfolgen oder zu ahnden. Art. 28 Abs. 2 BayDSG regelt, welche Vorschriften der Datenschutz-Grundverordnung anzuwenden sind, während Art. 28 Abs. 3 BayDSG einzelne Bestimmungen in Teil 2 Kapitel 1 bis 7 des Bayerischen Datenschutzgesetzes von einer Anwendung ausschließt und damit Ausnahmen zum Grundsatz des Art. 2 Satz 1 BayDSG festlegt. In Art. 29 bis 37 BayDSG finden sich ergänzende und modifizierende Vorschriften zu einzelnen Regelungsgegenständen.

Aus dem eben dargelegten Regelungsgefüge folgt, dass sowohl die **Informationspflichten der Art. 13 und 14 DSGVO als auch die Betroffenenrechte gemäß Art. 15 ff. DSGVO nicht für den Bereich der Ordnungswidrigkeitenverfolgung und -ahndung gelten**, vgl. Art. 28 Abs. 2 und 3 BayDSG. So findet sich in Art. 28 Abs. 2 BayDSG keine Verweisung auf Kapitel III der Datenschutz-Grundverordnung, wodurch die Art. 12 bis 23 DSGVO insgesamt von einer Anwendung ausgenommen sind. In Art. 28 Abs. 3 Nr. 2 BayDSG wird Teil 2 Kapitel 3 des Bayerischen Datenschutzgesetzes – Rechte der betroffenen Person – ebenfalls vollumfänglich ausgeschlossen. Hintergrund ist, dass die Informationspflichten sowie die Betroffenenrechte, deren Gewährleistung auch die Datenschutz-Richtlinie für Polizei und Strafjustiz fordert (Art. 12 ff. RLDSJ), in den jeweiligen Fachgesetzen geregelt sind. Damit möchte der Gesetzgeber den Bedürfnissen der jeweiligen fachspezifischen Rechtsmaterien besser gerecht werden.

Für den Bereich der Ordnungswidrigkeitenverfahren hat der Bundesgesetzgeber **§ 500 StPO** geschaffen.[8] Dieser ist über die Verweisung in § 46 Abs. 1 OWiG auch im Ordnungswidrigkeitenverfahren anwendbar.

Konsequenterweise müssen über die Verweisung nach § 500 Abs. 1 StPO in Ordnungswidrigkeitenverfahren neben der Strafprozessordnung (welche über § 46 Abs. 1 OWiG Anwendung findet) auch die §§ 45 ff. Bundesdatenschutzgesetz (BDSG) beachtet werden. Dies gilt allerdings nur, soweit die Strafprozessordnung nicht etwas anderes bestimmt, vgl. § 500 Abs. 2 Nr. 1 StPO.

2.7.2 Informationspflichten

§ 55 BDSG, welcher zu Teil 3 des Bundesdatenschutzgesetzes (§§ 45 bis 84 BDSG) gehört, regelt ausdrücklich die Informationspflichten. Diese gelten über

[8] Eingeführt durch Gesetz vom 20. November 2019 (BGBl. I S. 1724), in Kraft seit dem 26. November 2019.

die Verweisungskette des § 46 Abs. 1 OWiG in Verbindung mit § 500 Abs. 1 StPO auch im Ordnungswidrigkeitenverfahren.

Zur Umsetzung der Informationspflichten in der Praxis weise ich auf meine entsprechende Orientierungshilfe hin.[9] Die Empfehlungen können auch dann herangezogen werden, wenn § 55 BDSG eine verschlankte Art und Weise der Information im Gegensatz zu Art. 13 und 14 DSGVO verlangt. § 55 BDSG lautet:

§ 55 BDSG
Allgemeine Informationen zu Datenverarbeitungen
Der Verantwortliche hat in allgemeiner Form und für jedermann zugänglich Informationen zur Verfügung zu stellen über

1. *die Zwecke der von ihm vorgenommenen Verarbeitungen,*
2. *die im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten bestehenden Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung,*
3. *den Namen und die Kontaktdaten des Verantwortlichen und der oder des Datenschutzbeauftragten,*
4. *das Recht, die Bundesbeauftragte oder den Bundesbeauftragten anzurufen, und*
5. *die Erreichbarkeit der oder des Bundesbeauftragten.*

2.7.3 Betroffenenrechte

Über die Verweisung des § 500 Abs. 1 StPO in Teil 3 des Bundesdatenschutzgesetzes sind auch die Regelungen der §§ 56 ff. BDSG über die Rechte der betroffenen Person im Grundsatz anwendbar. Im Gegensatz zu § 55 BDSG – Informationspflichten – wird diesen Betroffenenrechten nur eine untergeordnete Bedeutung in der Praxis zukommen. Denn es ist zu berücksichtigen, dass die §§ 56 ff. BDSG nur dann zur Anwendung gelangen, soweit das Ordnungswidrigkeitengesetz sowie die Strafprozessordnung nicht selbst bereits ausdrücklich Betroffenenrechte vorsehen, vgl. § 46 Abs. 1 OWiG und § 500 Abs. 2 Nr. 1 StPO.

Insoweit ist im Ordnungswidrigkeitenverfahren hinsichtlich der Betroffenenrechte zunächst zu prüfen, ob das Ordnungswidrigkeitengesetz selbst Betroffenenrechte vorsieht. Ist dies nicht der Fall, ist zu prüfen, ob die Betroffenenrechte in der Strafprozessordnung einschlägig sind, welche über § 46 Abs. 1 OWiG auch im Ordnungswidrigkeitenverfahren anwendbar sind. Ist auch in der Strafprozessordnung kein Recht vorhanden, so ist zu prüfen, ob über die Verweisung des § 500 Abs. 1 StPO die §§ 56 ff. BDSG angewendet werden können.

Neben den Betroffenenrechen besteht für die betroffene Person auch ein **Akteneinsichtsrecht** (§ 49 OWiG).

§ 49 OWiG
Akteneinsicht des Betroffenen und der Verwaltungsbehörde
(1) [1]Die Verwaltungsbehörde gewährt dem Betroffenen auf Antrag Einsicht in die Akten, soweit der Untersuchungszweck, auch in einem anderen Straf- oder Buß-

[9] Bayerischer Landesbeauftragter für den Datenschutz, Informationspflichten des Verantwortliche, Stand 11/2028, Internet: https://www.datenschutz-bayern.de, Rubrik „Orientierungs- und Praxishilfen – Informationspflichten".

geldverfahren, nicht gefährdet werden kann und nicht überwiegende schutzwürdige Interessen Dritter entgegenstehen. [2]Werden die Akten nicht elektronisch geführt, können an Stelle der Einsichtnahme in die Akten Kopien aus den Akten übermittelt werden.

(2) [1]Ist die Staatsanwaltschaft Verfolgungsbehörde, so ist die sonst zuständige Verwaltungsbehörde befugt, die Akten, die dem Gericht vorliegen oder im gerichtlichen Verfahren vorzulegen wären, einzusehen sowie sichergestellte und beschlagnahmte Gegenstände zu besichtigen. [2]Akten, die in Papierform geführt werden, werden der Verwaltungsbehörde auf Antrag zur Einsichtnahme übersandt.

3 Schwerpunkt II

Datenschutzrechtliche Themen im Zusammenhang mit der COVID-19-Pandemie

Die COVID-19-Pandemie wirft auch im Bereich des Datenschutzes zahlreiche Probleme auf. Im Berichtszeitraum nahm die Beratung von Normgebern und öffentlichen Stellen wie auch die Bearbeitung von Beschwerden mit diesem Kontext einen erheblichen Teil der verfügbaren zeitlichen Ressourcen in Anspruch. Die nachfolgenden Beiträge werfen insofern nur einige Schlaglichter. Ergänzend hinweisen möchte ich auf die Materialien, die auf meiner Homepage https://www.datenschutz-bayern.de in einer eigenen Rubrik „Corona-Pandemie" bereitgestellt sind. Dort ist auch die Aktuelle Kurz-Information 33 „Befreiung von der Maskenpflicht an bayerischen öffentlichen Schulen" abrufbar, die fortlaufend der Entwicklung des Infektionsschutzrechts sowie der dazu ergehenden Rechtsprechung angepasst wird und daher nicht in diesem Bericht dokumentiert ist.

3.1 Filmaufnahmen im Krankenhaus: Einwilligung

Mich haben Beschwerden erreicht, die sich auf die Sendung „ARD extra: Die Corona-Lage" vom 14. April 2020 bezogen. Die Filmaufnahmen sollten unter anderem die hohe Belastung des Klinikpersonals im Blick haben. Neben Klinikpersonal wurde dabei auch die Behandlung eines sterbenden Patienten sowie eines weiteren schwer erkrankten Patienten mit Nennung der Zimmernummer gezeigt.

Mir war bewusst, dass die Kliniken extreme Herausforderungen bei der Bewältigung der COVID-19 Pandemie zu bewältigen hatten und es im Grundsatz ein legitimes Anliegen ist, auf die besonderen Belastungen des Klinikpersonals aufmerksam zu machen. Dennoch entbindet dieser Umstand die Kliniken weder von den rechtlichen Vorgaben der Datenschutz-Grundverordnung noch von der Beachtung der ärztlichen Schweigepflicht.

Auch wenn bei der Ausstrahlung im Fernsehen die Patienten durch Verpixelung unkenntlich gemacht wurden, ist vorgelagert zu berücksichtigen, dass Medienvertreterinnen und Medienvertretern gegenüber im Rahmen der Filmaufnahmen zwangsläufig personenbezogene Daten der Patientinnen und Patienten sowie des Klinikpersonals offen gelegt werden, vgl. Art. 4 Nr. 2 DSGVO. Bereits diese Offenlegung bedarf nach Art. 6 Abs. 1 DSGVO einer Rechtsgrundlage, und soweit Gesundheitsdaten der Patientinnen und Patienten betroffen sind, ist Art. 9 Abs. 2 DSGVO zu beachten

Art. 4 DSGVO
Begriffsbestimmungen
Im Sinne dieser Verordnung bezeichnet der Ausdruck:
[…]
1. „Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit

personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

[…]

Nach meinem Verständnis kann das verantwortliche Klinikum sich dabei nicht auf eine nachgelagerte Einwilligung der betroffenen Personen gegenüber der Rundfunkanstalt berufen (hier: Filmaufzeichnung und -ausstrahlung). Vielmehr muss das Klinikum vor der Weitergabe personenbezogener Daten an eine Rundfunkanstalt selbst die Einwilligung der betroffenen Personen einholen.[10] Eine andere Rechtsgrundlage etwa auf gesetzlicher Basis sehe ich nicht.

Ich empfehle Kliniken dringend, künftig bei vergleichbaren Medienanfragen eine tragfähige Rechtsgrundlage für die Offenlegung von Patienten- und Beschäftigtendaten sicherzustellen.

3.2 Weitergabe von personenbezogenen Daten durch Gesundheitsämter an die Polizei und Rettungsdienste

Bereits in einem frühen Stadium der COVID-19-Pandemie haben mich viele Anfragen erreicht, ob bayerische Gesundheitsämter **allgemein** Listen mit SARS-CoV-2 infizierter Personen an Dienststellen der Bayerischen Polizei herausgeben dürfen und ob **im Einzelfall** Informationen zu einer bestehenden Infektion mitgeteilt werden dürfen, damit Polizeibeamtinnen und Polizeibeamte im Fall eines Einsatzes Vorkehrungen gegen eine Ansteckungsgefahr treffen können.

Das Interesse von Einsatzkräften der Polizei, sich im Rahmen ihrer dienstlichen Tätigkeit vor einer Ansteckung zu schützen, konnte ich gut nachvollziehen. Insgesamt bedurfte und bedarf es in Zeiten der COVID-19-Pandemie geeigneter Maßnahmen, um insbesondere Angehörige systemrelevanter Berufe vor einer Infektion zu schützen.

Gleichwohl halte ich es – grundsätzlich im Einklang mit den Bayerischen Staatsministerien des Innern, für Sport und Integration sowie für Gesundheit und Pflege – für datenschutzrechtlich unzulässig, wenn bayerische Gesundheitsämter vorsorglich, also **anlassunabhängig**, Listen infizierter Personen an Polizeidienststellen übermitteln.

Bei den personenbezogenen Daten zu festgestellten Infektionen handelt es sich um Gesundheitsdaten im Sinne von Art. 4 Nr. 15 DSGVO.

Art. 4 DSGVO
Begriffsbestimmungen
Im Sinne dieser Verordnung bezeichnet der Ausdruck: […]
15. „Gesundheitsdaten" personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen; […].

[10] Vgl. Europäischer Gerichtshof, Urteil vom 29. Juli 2019, C 40/17, Rn. 102.

Diese Gesundheitsdaten dürfen nur unter den zusätzlichen Voraussetzungen von Art. 9 Abs. 2 DSGVO verarbeitet werden. Eine Rechtsgrundlage für eine anlassunabhängige Übermittlung von Infiziertendaten sieht das geltende Recht jedoch nicht vor. Sie wäre auch kaum mit dem datenschutzrechtlichen Grundsatz der Erforderlichkeit in Einklang zu bringen: Die Polizei erhielte auf diese Weise Zugriff auf Gesundheitsdaten einer sehr großen Zahl von Personen, mit welchen sie niemals in Kontakt treten wird; im Ergebnis käme es zu einer Vorratsdatenspeicherung.

Eine anlassunabhängige Übermittlung von Infiziertendaten an die Polizei wäre im Übrigen zur Erreichung des mit ihr verbundenen Zwecks ungeeignet. Die Heranziehung der Listen im Rahmen der allgemeinen polizeilichen Tätigkeit erscheint in vielen Einsatzsituationen als kaum praktikabel, so etwa, wenn zunächst (noch ungeschützt) Personalien erfragt werden, um dann einen Abgleich mit den übermittelten Daten durchzuführen, deren Aktualität sich jedoch ständig überholen dürfte. Erst anschließend könnten eigene Schutzmaßnahmen ergriffen werden. Unabhängig davon könnte durch solche Listen auch nicht ausgeschlossen werden, dass die Polizistinnen und Polizisten mit infizierten Personen in Kontakt kommen, die bislang nicht getestet worden und/oder noch symptomfrei sind.

Die Frage, ob eine Datenweitergabe **im Einzelfall** zulässig ist, hängt von der jeweiligen Fallkonstellation ab. Zu einer Fallkonstellation, bei der es um die Zulässigkeit einer Datenweitergabe an die Polizei im Rahmen einer zwangsweisen Vorführung einer Person im Auftrag des Gesundheitsamtes gegangen ist, habe ich mich bereits in meinem 27. Tätigkeitsbericht 2016 unter Nr. 7.4.2 geäußert.

Maßgeblich für die Übermittlung personenbezogener Daten durch die Gesundheitsämter an die Polizei sind Art. 30, 31 Gesundheitsdienst- und Verbraucherschutzgesetz (GDVG). Danach dürfen personenbezogene Daten offenbart werden, wenn dies zur Abwehr von Gefahren für Freiheit, Leben oder Gesundheit Dritter erforderlich ist (Art. 31 Abs. 5 Satz 1 Nr. 1, Art. 30 Abs. 2 Satz 2 Halbsatz 1 GDVG).

Art. 31 GDVG
Mitteilungen, Datenübermittlungen
(5) [1]Außer in den in den Abs. 1 bis 4 genannten Fällen und unbeschadet der Einschränkungen nach den Art. 6 und 8 des Bayerischen Datenschutzgesetzes dürfen die Behörden für Gesundheit, Veterinärwesen und Verbraucherschutz personenbezogene Daten, die keine Geheimnisse im Sinn des Art. 30 Abs. 1 sind, an die zuständigen öffentlichen Stellen nur übermitteln,
1. in den Fällen des Art. 30 Abs. 2 Satz 1 Nr. 1 und 2 sowie Satz 2,
[…].
[2]Eine Datenübermittlung nach Satz 1 ist nicht zulässig, soweit personenbezogene Daten der ärztlichen Schweigepflicht unterliegen.

Art. 30 GDVG
Datenschutz, Geheimhaltungspflichten
(2) [1][…] [2]Abweichend von Abs. 1 dürfen personenbezogene Daten von den Behörden für Gesundheit, Veterinärwesen und Verbraucherschutz an öffentliche Stellen offenbart oder an andere Teile der öffentlichen Stelle, deren Bestandteil die Behörde für Gesundheit, Veterinärwesen und Verbraucherschutz ist, übermittelt werden, wenn dies zur Abwehr von Gefahren für Freiheit, Leben oder Gesundheit Dritter erforderlich ist; die betroffene Person soll hierauf hingewiesen werden. [3][…]

Nach der gesetzlichen Regelung kommt es entscheidend darauf an, ob die Mitteilung der konkreten Krankheit beziehungsweise des konkreten Krankheitsverdachts **erforderlich** ist, um Gefahren für die Gesundheit der begleitenden Polizeikräfte abzuwehren.

Falls eine Weitergabe im Einzelfall an die Polizei zulässig sein sollte, ist die betroffene Person vom Gesundheitsamt auf diese Datenübermittlung an die Polizei grundsätzlich hinzuweisen („Soll-Vorschrift", siehe Art. 30 Abs. 2 Satz 2 Halbsatz 2 GDVG). Ausnahmen von dieser Informationspflicht wären begründungspflichtig.

Diese Ausführungen sind auf eine entsprechende Weitergabe an Rettungsdienste übertragbar.

3.3 Corona-Tests: Übermittlung von Ergebnissen an die Leitungen von Pflege- und Behinderteneinrichtungen

Datenverarbeitungen im Zusammenhang mit der COVID-19-Pandemie betreffen häufig Gesundheitsdaten, so etwa wenn es um die Infektion einer Person mit SARS-CoV-2 oder einem insoweit bestehenden Verdacht geht. Gesundheitsdaten unterliegen gemäß Art. 9 Abs. 1 DSGVO einem grundsätzlichen Verarbeitungsverbot, das nur in den von Art. 9 Abs. 2 DSGVO ausdrücklich genannten Fällen beiseitetritt. Diese datenschutzrechtliche Vorgabe mussten im Berichtszeitraum auch die bayerischen Gesundheitsämter berücksichtigen, wenn sie auf Grund infektionsschutz- oder gesundheitsrechtlicher Befugnisse personenbezogene Daten von Bürgerinnen und Bürgern verarbeiteten, die mit SARS-CoV-2 infiziert waren oder in einem entsprechenden Verdacht standen.

In diesem Zusammenhang erreichten mich zahlreiche Anfragen. Unter anderem wurde die Frage aufgeworfen, ob die Gesundheitsämter positive oder negative Ergebnisse von Corona-Tests direkt an Pflege- und Behinderteneinrichtungen übermitteln dürfen. Entsprechende Übermittlungen werden damit begründet, dass betroffene Personen in den Einrichtungen mitunter ihre Testergebnisse vergessen; auch teilen Betreuerinnen und Betreuer sowie Angehörige die Ergebnisse externer Tests von Bewohnerinnen und Bewohnern nicht rechtzeitig der jeweiligen Pflege- oder Behinderteneinrichtung mit, sodass erforderliche Schutzmaßnahmen nicht rechtzeitig ergriffen werden können.

Ich habe die folgenden datenschutzrechtlichen Hinweise gegeben:

Eine unmittelbare Übermittlung von Testergebnissen an die Einrichtungsleitung halte ich grundsätzlich für zulässig, soweit sie zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist und die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben (Art. 6 Abs. 1 UAbs. 1 Buchst. d, Art. 9 Abs. 2 Buchst. c DSGVO).

Falls diese Voraussetzungen nicht gegeben wären, könnte die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren, gemäß Art. 9 Abs. 2 Buchst. i DSGVO zulässig sein, wenn dies erforderlich und in einem nationalen Gesetz vorgesehen ist, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person vorsieht.

Für Datenverarbeitungen im Zusammenhang mit der Pandemiebekämpfung kommen grundsätzlich die Vorschriften des Infektionsschutzgesetzes (IfSG) in Betracht. Für die vorliegende Fallkonstellation – Weitergabe von Daten von positiv oder negativ auf SARS-CoV-2 getesteten Personen an Pflege- oder Behinderteneinrichtungen – bestehen nach dem Infektionsschutzgesetz allerdings insoweit keine Unterrichtungspflichten, Mitteilungspflichten oder entsprechende Befugnisse des Gesundheitsamtes.

Das Infektionsschutzgesetz erachte ich jedoch nicht als abschließend,[11] so dass grundsätzlich ergänzend auch das Gesundheitsdienst- und Verbraucherschutzgesetz (GDVG) herangezogen werden kann, welches Gesundheitsbehörden Verarbeitungsbefugnisse vermitteln kann.

Maßgeblich für die Übermittlung personenbezogener Daten durch die Gesundheitsämter ist unter anderem Art. 30 GDVG.

Art. 30 GDVG
Datenschutz, Geheimhaltungspflichten
(1) [1]Die Behörden für Gesundheit, Veterinärwesen und Verbraucherschutz dürfen Geheimnisse, die Amtsangehörigen in der Eigenschaft als Arzt, Tierarzt oder als andere gemäß § 203 Abs. 1 oder 3 des Strafgesetzbuchs (StGB) zur Wahrung des Berufsgeheimnisses verpflichtete Person
1. in Wahrnehmung der in Art. 13 und 14 genannten Aufgaben,
2. im Zusammenhang mit einer Untersuchung oder Begutachtung, der sich der Betroffene freiwillig unterzogen hat oder
3. bei einer Beratung von Tierhaltern
anvertraut oder sonst bekannt geworden sind, bei der Erfüllung einer anderen Aufgabe als der, bei deren Wahrnehmung die Erkenntnisse gewonnen wurden, nicht verarbeiten. [2]Ebenso dürfen die Behörden für Gesundheit, Veterinärwesen und Verbraucherschutz Geheimnisse, die den in Satz 1 genannten Personen außerhalb ihres dienstlichen Aufgabenbereichs anvertraut oder sonst bekannt geworden sind, bei der Erfüllung ihrer Aufgaben nicht verarbeiten. [3]Die Behörden für Gesundheit, Veterinärwesen und Verbraucherschutz dürfen Geheimnisse nach den Sätzen 1 und 2 nicht offenbaren oder an andere Teile der öffentlichen Stelle, deren Bestandteil die Behörde für Gesundheit, Veterinärwesen und Verbraucherschutz ist, übermitteln. [4]Persönliche Geheimhaltungspflichten der Amtsangehörigen bleiben unberührt. [5]Die Wahrung der Geheimhaltungspflichten und Verwertungsverbote ist von den Behörden für Gesundheit, Veterinärwesen und Verbraucherschutz durch angemessene Maßnahmen auch organisatorisch sicherzustellen.

Diese Vorschrift regelt zunächst besondere Geheimhaltungspflichten der Gesundheitsbehörden. Sie dürfen danach beispielsweise Geheimnisse, die Amtsangehörigen in der Eigenschaft als Arzt im Zusammenhang mit einer Untersuchung oder Begutachtung, der sich die betroffene Person freiwillig unterzogen hat, anvertraut oder sonst bekannt geworden sind, nicht offenbaren[12] (Art. 30 Abs. 1

11 Siehe Landtags-Drucksache 18/6945, S. 1 und Landtags-Drucksache 14/11831, S. 33; vgl. auch Bundestags-Drucksache 14/2530.

12 Neuer Wortlaut seit dem 1. August 2020, siehe das Gesetz zur Änderung des Gesundheitsdienst- und Verbraucherschutzgesetzes und anderer Gesetze vom 24. Juli 2020 (GVBl. S. 372, vorher „übermitteln" anstatt „offenbaren"); damit sollte laut Gesetzesbegründung nur eine Anpassung an die Begrifflichkeiten der Datenschutz-Grundverordnung erfolgen (siehe Landtags-Drucksache 18/8331, S. 21).

Satz 3 GDVG). Damit wird sichergestellt, dass persönliche Geheimnisse, in die eine Bürgerin oder ein Bürger „aus freien Stücken" Bediensteten einer Behörde des öffentlichen Gesundheitsdienstes Einsicht gewährt hat, nicht in anderem Zusammenhang personenbezogen verwertet werden.[13]

Bei Personen, die sich freiwillig einem Test auf SARS-CoV-2 durch das Gesundheitsamt unterziehen, dürfte ein solcher Fall von Art. 30 Abs. 1 Satz 3 GDVG ohne weiteres gegeben sein. Hiervon umfasst sehe ich zudem auch die Fallkonstellation, dass eine Ärztin oder ein Arzt ihrer oder seiner Meldepflicht nach § 8 IfSG nachgekommen ist und die Behörden für Gesundheit auf diesem Weg Kenntnis von einer Infektion mit SARS-CoV-2 erhalten haben (siehe Wortlaut in Art. 30 Abs. 1 Satz 1 GDVG: „sonst bekannt geworden sind").

Allerdings gilt das Verarbeitungsverbot nach Art. 30 Abs. 1 GDVG nicht, soweit die Verarbeitung durch Rechtsvorschrift ausdrücklich zugelassen ist oder die betroffene Person in die Verarbeitung ausdrücklich eingewilligt hat (Art. 30 Abs. 2 Satz 1 GDVG). Eine Vorschrift, die die Verarbeitung, also die Übermittlung der Testergebnisse von einem Gesundheitsamt an Pflege- oder Behinderteneinrichtungen ausdrücklich erlaubt, kann ich derzeit nicht erkennen. Somit verbliebe die Einholung einer Einwilligung der betroffenen Person als Rechtsgrundlage für die entsprechende Datenübermittlung durch das Gesundheitsamt. Die Bedingungen für die Einwilligung sind hier Art. 7 und Art. 9 Abs. 2 Buchst. a DSGVO zu entnehmen.[14]

Eine Übermittlung seitens des Gesundheitsamtes – auch auf Grundlage von Art. 6 Abs. 1 UAbs. 1 Buchst. d, Art. 9 Abs. 2 Buchst. c DSGVO – sollte jedoch ausschließlich an die jeweilige Leitung der Pflege- beziehungsweise Behinderteneinrichtung gerichtet sein (Rechtsgedanke des Art. 14 Abs. 5 Satz 3 GDVG).

3.4 Speicherdauer von Daten zur Kontaktnachverfolgung

Beschäftigt hat mich auch die Speicherdauer der Kontaktdaten, die zur Nachverfolgung bei einer Sars-CoV-2-Infektion erhoben werden. So hatte eine Hilfsorganisation in Bayern in den Datenschutzinformationen nach Art. 13 DSGVO bezüglich der Kontaktdaten von Besucherinnen und Besuchern in Pflegeeinrichtungen die Speicherdauer auf fünf Jahre festgelegt. Dieser lange Zeitraum war gewählt worden, um bei eventuell stattfindenden „staatsanwaltlichen Ermittlungen" auskunftsfähig zu sein. Diese Argumentation hat mich nicht überzeugt.

Da die Speicherdauer im vorliegenden Fall nicht ausdrücklich geregelt ist, sind die allgemeinen Grundsätze zur Aufbewahrung personenbezogener Daten heranzuziehen. Insbesondere gelten die Grundsätze der Erforderlichkeit und der Zweckbindung. Personenbezogene Daten sind demnach zu löschen, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind (Art. 17 Abs. 1 Buchst. a DSGVO).

13 Siehe Landtags-Drucksache 10/8972, S. 14.

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

Zweck der Datenerhebung war die Nachverfolgung von Infektionsketten im Zusammenhang mit einer Sars-CoV-2-Infektion. Ich habe die Auffassung vertreten, dass bei einer zu erwartenden Inkubationszeit von zwei Wochen und einem zeitlichen Sicherheitsaufschlag eine Aufbewahrung von vier Wochen noch als erforderlich angesehen werden kann.

Zum Beispiel wurde für die Kontaktdatenerhebung in Gastronomiebetrieben im „Hygienekonzept-Gastronomie“ der Bayerischen Staatsregierung geregelt, dass die Betreiber der Gastronomie die personenbezogenen Daten nach Ablauf eines Monats vernichten müssen.

Da der Zweck der Kontaktdatenerhebung bei Besucherinnen und Besuchern in Pflegeheimen sowie Besucherinnen und Besuchern eines Gastronomiebetriebes vergleichbar ist, sollte die Erforderlichkeit der Aufbewahrungsfrist nach denselben Kriterien bewertet werden.

Die Hilfsorganisation hat sich letztlich meiner Argumentation angeschlossen und die Speicherdauer von fünf Jahren datenschutzgerecht auf einen Monat verkürzt.

3.5 Elektronische Kommunikation beim Umgang mit COVID-19-Fällen

Die Infektionsbekämpfung im Rahmen der COVID-19-Pandemie bringt zum einen neue Anforderungen und Datenflüsse im Gesundheitsbereich mit sich, zeigt zum anderen jedoch auch die bestehenden Defizite insbesondere hinsichtlich einer zuverlässigen, sicheren und datenschutzkonformen elektronischen Kommunikation zwischen den beteiligten Stellen. Zu rechtlichen Fragestellungen bezüglich der Datenübermittlung zwischen den verschiedenen Stellen siehe Beiträge Nr. 3.2 und Nr. 3.3 dieses Tätigkeitsberichts.

3.5.1 Gesundheitsämter, Labore, Kontakt-Tracing

Die COVID-19-Pandemie hat aufgezeigt, wie schwierig sich die Kommunikation insbesondere zwischen Gesundheitsämtern, Ärzten und Krankenhäusern, Landesamt für Gesundheit und Lebensmittelsicherheit (LGL), Laboren, Pflegeeinrichtungen sowie Bürgerinnen und Bürgern im Hinblick auf den schnellen Austausch von Informationen etwa zu Testaufträgen, Infektionen oder Testergebnissen gestaltet. So war es zu Anfang der COVID-19-Pandemie ein gängiges Verfahren, dass die Listen mit Patientennamen, die in einem Testzentrum auf SARS-CoV-2 getestet werden sollten, zwar elektronisch in einer Excel-Tabelle erfasst, dann aber ausgedruckt und per Fax an die jeweils zuständigen Testzentren verschickt wurden. Dort wurden die Listen in mühsamer und fehleranfälliger Handarbeit wieder abgetippt, um dann im elektronischen System zur Testverwaltung die Ergebnisse zu dokumentieren.

Auch die Weiter- und Rückübermittlung der Testergebnisse von den Laboren zu den Einsendern erfolgte häufig per Fax oder per unverschlüsselter E-Mail. Auf die Problematik des Faxversands von medizinischen Unterlagen insbesondere hinsichtlich des hohen Risikos eines Fehlversands durch Vertippen habe ich bereits hingewiesen, so etwas in meiner Orientierungshilfe „Datensicherheit beim Telefax-Dienst“.[15] Zudem führte der mehrfache Medienbruch zu deutlichen zeitlichen

[15] Internet: https://www.datenschutz-bayern.de/technik/orient/telefax.htm.

Verzögerungen, unnötigem Mehraufwand und hoher Fehleranfälligkeit, was im Falle von COVID-19-Testergebnissen auch Risiken für Leib und Leben mit sich bringen kann. Unverschlüsselte und unsignierte E-Mails bieten für personenbezogene Gesundheitsdaten kein ausreichendes Schutzniveau, um insbesondere Vertraulichkeit und Integrität zu gewährleisten.

Die Kontaktverfolgung (Contact-Tracing) durch die Gesundheitsämter erfolgte zu Beginn komplett „von Hand", vor allem telefonisch. Jedes Gesundheitsamt stand zudem vor der Frage, wie die Kontaktpersonen, die Ergebnisse der Befragungen und vergleichbare Informationen dokumentiert werden sollen. Bayernweit soll hierfür nunmehr die Software SORMAS des Helmholtz-Zentrums für Infektionsforschung zum Einsatz kommen, die den Gesundheitsämtern eine einheitliche Möglichkeit zur Dokumentation und zum Datenaustausch bietet sowie Möglichkeiten zur täglichen elektronischen Kontaktaufnahme zwischen den betroffenen Index-/ Kontaktpersonen und dem Gesundheitsamt ermöglicht.

Im Zusammenhang mit der Einführung der Corona-Warn-App des Bundes wurde nunmehr auch an der elektronischen Anbindung der Labore gearbeitet, damit die Ergebnisse schnell und ohne die zu Beginn erforderliche Zwischenschaltung eines Call-Centers in die App eingebunden werden können.

Große Schwierigkeiten bereitete und bereitet in vielen Bereichen immer noch die sichere elektronische Kommunikation mit Bürgerinnen und Bürgern. Da weder die Verschlüsselung von E-Mails noch Lösungen wie das BayernPortal flächendeckend genutzt werden und die Verwendung der im Privatbereich verbreiteten Messenger-Dienste aus Datenschutzsicht kritisch zu sehen ist, kommen derzeit für viele Einzelbereiche unterschiedliche Apps zum Einsatz, insbesondere Contact-Tracing-Apps, Warn-Apps sowie Apps zur Übermittlung der Testergebnisse für Reiserückkehrer. Dabei handelt es sich jedoch zumeist um Insellösungen des jeweiligen Anbieters, die keine Daten mit anderen Lösungen austauschen können. Zudem müssen die Fragen der IT-Sicherheit und des Datenschutzes für jede App neu konzipiert und geprüft werden.

Es zeigt sich somit, dass in den letzten Monaten zwar für Teilbereiche elektronische Kommunikationsplattformen geschaffen wurden, es fehlt jedoch immer noch eine einheitliche IT-Basisinfrastruktur für eine sichere elektronische Kommunikation zwischen allen Beteiligten. Es wäre wünschenswert, wenn sich die derzeitigen technischen Entwicklungen nicht nur mit einzelnen Teilbereichen und Anwendungsfällen beschäftigen würden, sondern insbesondere auch eine Weichenstellung in Richtung einer sicheren bayern- oder bundesweiten Basisinfrastruktur vorgenommen würde. Hierbei sollte auch geprüft werden, inwieweit schon vorhandene Lösungen wie zum Beispiel die Telematikinfrastruktur oder das BayernPortal/Bürgerkonto genutzt werden könnten.

Ein weiterer denkbarer Ansatz speziell im Bereich des Infektionsschutzes wäre es, etwa beim LGL eine zentrale Plattform für alle Arten von Infektionskrankheiten zu schaffen und schon für andere Bereiche bestehende IT-Lösungen dementsprechend zu modernisieren und in Richtung eines zentralen Portals auszubauen.

3.5.2 Krankenhäuser

Auch im Bereich der Krankenhäuser haben sich im Rahmen der veränderten Arbeitsbedingungen durch die COVID-19-Pandemie einige Defizite bezüglich der

elektronischen Kommunikation gezeigt. So entstand beispielsweise aufgrund von Quarantäneregelungen vielfach der Bedarf, aus dem häuslichen Umfeld auf sensible Patientendaten zuzugreifen und aus der Ferne an der Behandlung beteiligt zu werden. Dabei waren aufgrund der Krisensituation jedoch nicht, wie zuletzt in meinem 26. Tätigkeitsbericht unter Nr. 2.3.5 gefordert, ausreichend dienstliche Geräte vorhanden, so dass vielfach auf Privatgeräte zurückgegriffen wurde.

Auch deutlich wurde der Bedarf an schneller elektronischer Kommunikation mit externen Stellen wie beispielsweise Vor-/Nachbehandlerinnen und -behandlern oder Gesundheitsämtern sowohl für organisatorische als auch für medizinische Fragestellungen. In der Regel verfügten die Krankenhäuser jedoch nicht über geeignete und datenschutzkonforme Messenger- und Videokonferenzdienste, so dass auf die üblichen, aus dem Privatbereich bekannten Dienste, die in der Regel von US-amerikanischen Anbietern bereitgestellt werden, zurückgegriffen wurde. Wie die von mir veröffentlichten Sonderinformationen zur Bewältigung der Corona-Pandemie[16] zeigten, war dies aufgrund der Neuheit der Situation grundsätzlich für einen Übergangszeitraum tolerierbar. Nunmehr muss jedoch geprüft werden, welche Kommunikationsformen weiterhin benötigt werden und wie diese Lösungen datenschutzgerecht umgesetzt werden können, gerade auch vor dem Hintergrund der Rechtsprechung des Europäischen Gerichtshofs zu Übermittlungen personenbezogener Daten an Drittländer. Zudem gibt es in der Datenschutz-Grundverordnung keine Ausnahmeregelungen für Krisenzeiten, so dass beispielsweise die in meinem 29. Tätigkeitsbericht unter Nr. 12.5 aufgestellten Anforderungen an Messenger-Dienste auch weiterhin gelten. Bezüglich der Telearbeit verweise ich auch auf Nr. 3.7 dieses Tätigkeitsberichts.

Einige Krankenhäuser hatten sich zudem zu Beginn der COVID-19-Pandemie mit der Frage an mich gewandt, ob die Beschränkungen der vorhandenen Berechtigungskonzepte krisenbedingt erweitert oder aufgehoben werden dürfen, um einen flexiblen Personaleinsatz zu ermöglichen. Auch hier gilt, dass eventuell vorgenommene Erweiterungen nunmehr dahingehend überprüft werden müssen, welche Berechtigungen tatsächlich erforderlich waren oder im Fall wieder ansteigender Zahlen COVID-19 erforderlich sind und wie diese entsprechend im Berechtigungskonzept umgesetzt werden können. Zugriffsrechte, die es ermöglichen, dass alle Mitarbeiter ohne Einschränkung auf die Daten aller Patienten zugreifen können, entsprechen nicht dem Erforderlichkeitsprinzip und damit nicht den Anforderungen des Datenschutzes. Die in der Orientierungshilfe Krankenhausinformationssysteme (2. Fassung)[17] formulierten Anforderungen gelten auch für Krisenzeiten. Gleichzeitig sind dort auch Lösungsmöglichkeiten für Zugriffe in Notfallsituationen definiert.

Dass gerade in Krisenzeiten besonderes Augenmaß hinsichtlich der zusätzlichen Ermöglichung von Zugriffen besteht, bestätigen auch einige Meldungen von Krankenhäusern nach Art. 33 DSGVO die „Neugier-Zugriffe“ auf Daten von Angehörigen betrafen (siehe Beitrag Nr. 12.10). Mitarbeitende sollten deutlich darauf hingewiesen werden, dass auch bei berechtigter Sorge um Familienmitglieder ein Zugriff aus privaten Gründen, selbst mit Einwilligung der betroffenen Person, nicht zulässig ist. Ein Zugriff darf nur erfolgen, wenn ein Behandlungszusammenhang besteht und der Zugriff dienstlich erforderlich ist.

16 Internet: https://www.datenschutz-bayern.de/corona/sonderinfo.html.

17 Internet: https://www.datenschutz-bayern.de, Rubrik „Veröffentlichungen“.

3.6 Telearbeit in Zeiten von COVID-19, Nutzung von Privatgeräten (Bring your own Device, BYOD)

Zur Telearbeit und insbesondere zur Verwendung von Privatgeräten (Bring your own Device, BYOD) habe ich mich zuletzt in meinem 26. Tätigkeitsbericht 2014 unter Nr. 2.3.5 geäußert. Auch nach Geltungsbeginn der Datenschutz-Grundverordnung haben diese Forderungen weiterhin Bestand. Dennoch haben die COVID-19-Pandemie und die damit verbundene große Verbreitung von Homeoffice und Telearbeit, die schnellstmöglich umgesetzt werden musste, dazu geführt, dass in vielen Bereichen für die Arbeit von zu Hause nur Privatgeräte zur Verfügung standen.

Derzeit zeichnet sich ab, dass Telearbeit weiterhin in viel größerem Umfang auch von öffentlichen Stellen genutzt werden soll, als es bisher der Fall war. Neben einem erhöhten Bedarf an elektronischer Kommunikation und Arbeitsorganisation beispielsweise im Rahmen von Videokonferenzen und Kollaborationsplattformen sowie der Nutzung von Messengerdiensten steigt auch der Bedarf für einen Vollzugriff auf Fachverfahren mittels der privaten Geräte der Beschäftigten.

Ich erhalte daher nach wie vor sehr viele Anfragen, in welcher Form Telearbeit insbesondere mit Privatgeräten zulässig ist und wie diese datenschutzgerecht ausgestaltet werden kann. Insbesondere wird häufig nach konkreten Produktempfehlungen sowie auslagerbaren Tätigkeiten gefragt. Leider kann ich diese Fragen nicht pauschal beantworten, da die Eignung und insbesondere auch die erforderlichen technisch-organisatorischen Maßnahmen immer stark vom Anwendungsfall abhängen und sich die Verfahrensweisen sowie die IT-Ausstattung der öffentlichen Stellen, selbst wenn es sich um die gleiche Behörde wie etwa ein Landratsamt handelt, unterscheiden.

Schwerpunkt dieses Beitrags sind insbesondere die Fragestellungen hinsichtlich der Nutzung von Privatgeräten und des Zugriffs auf Fachverfahren. Für das Thema Videokonferenz siehe auch Nr. 12.4 dieses Tätigkeitsberichts, für die Probleme hinsichtlich der Verwendung von Produkten von US-Anbietern im Zusammenhang mit dem Urteil des Europäischen Gerichtshofs zu Schrems II siehe auch Nr. 11.2 dieses Tätigkeitsberichts.

Möchte der Verantwortliche seinen Beschäftigten den Zugriff auf Fachverfahren über Privatgeräte ermöglichen, muss er für den konkreten Anwendungsfall systematisch prüfen, unter welchen Bedingungen dies möglich ist. Der in der Datenschutz-Grundverordnung hierfür formulierte risikobasierte Ansatz erfordert immer eine Abwägung der Risiken für die Rechte und Freiheiten der von einer Verarbeitung betroffenen Personen. Dies gilt auch für Verarbeitungen, die im Rahmen von Telearbeit durchgeführt werden sollen.

Im ersten Schritt ist daher zu klären, welche Daten im Rahmen der Telearbeit und eventuell auf Privatgeräten verarbeitet werden sollen. Daten eines Jugendamts, eines Gesundheitsamts oder eines Ausländeramts, werden oftmals besonders schutzbedürftig sein (vgl. Art. 9 Abs. 1 DSGVO). Es ist dann naheliegend, dass diese Daten, wenn überhaupt, nur sehr eingeschränkt oder mit hohen technisch-organisatorischen Schutzmaßnahmen im Homeoffice, insbesondere auf Privatgeräten verarbeitet werden dürfen. Sollen dagegen beispielsweise Dienstanweisungen, organisatorische Regelungen oder anderweitige Dokumente ohne oder mit geringem Personenbezug bearbeitet werden, stellen sich aus Datenschutzsicht deutlich geringere Anforderungen.

Gerade bei der Verwendung von Privatgeräten muss jedoch immer auch berücksichtigt werden, dass diese Sicherheitsrisiken für die gesamte IT der öffentlichen Stelle mit sich bringen können, so etwa durch darauf befindliche Schadsoftware (wie Viren, Trojaner, Keylogger).

Soll allgemein Telearbeit für alle Bereiche beispielsweise einer Gemeinde oder eines Landratsamts ermöglicht werden, richten sich die Gesamtbewertung und somit die erforderlichen Maßnahmen nach dem maximalen Schutzbedarf der verarbeiteten Daten.

Dies zeigt deutlich, dass der Verantwortliche für die Entscheidung über Telearbeit und die Nutzung von Privatgeräten eine mehrstufige Prüfung vornehmen und geeignete Schutzmaßnahmen definieren und umsetzen muss. Es bietet sich an, sich hierbei an der Methodik der Datenschutz-Folgenabschätzung (DSFA) zu orientieren, zumal insbesondere bei einer Verarbeitung von Daten nach Art. 9 Abs. 1 DSGVO ohnehin zu prüfen ist, ob eine DSFA erforderlich ist. Auch wenn die Prüfung der Erforderlichkeit zu dem Schluss kommt, dass keine DSFA erforderlich ist, sind insbesondere folgende Prüfungsschritte schriftlich zu dokumentieren, um die Rechenschaftspflichten zu erfüllen:[18]

- Welche Verarbeitung ist geplant?
- Im Fall einer Auftragsverarbeitung: Wie sind die Verpflichtungen der Auftragsverarbeiter klar definiert und vertraglich geregelt?
- Welche Kategorien personenbezogener Daten werden verarbeitetet?
- Welche Kategorien von Personen sind von der Verarbeitung betroffen?
- Werden Daten in Drittländer, insbesondere außerhalb der Europäischen Union übermittelt?
- Mit Hilfe welcher Betriebsmittel erfolgt die Datenverarbeitung?
- Wie wird die Erfüllung der Datensicherheitsziele gewährleistet?
- Wie wird die Erfüllung der Schutzbedarfsziele gewährleistet?
- Wie wird die Einhaltung der Datenschutz-Grundverordnung gewährleistet (Risikogesamtbewertung)?
- Wie bewertet die oder der behördliche Datenschutzbeauftragte die Erforderlichkeit einer DSFA?

Auch bezüglich einer Nutzung von Privatgeräten ist eine ausführliche Analyse insbesondere der Datensicherheitsziele nötig. Hierbei ist beispielsweise die Frage zu klären, ob in der gewählten Lösung Daten (temporär) auf dem Privatgerät gespeichert werden, welche Risiken ein eventuell von Schadsoftware befallenes Privatgerät hinsichtlich einer unbefugten Kenntnisnahme der Daten oder der Angriffsmöglichkeiten auf die IT der öffentlichen Stelle eröffnet.

[18] Nähere Informationen zur DSFA auf https://www.datenschutz-bayern.de, Rubrik „DSFA“, dort auch Formulare „DSFA-Erforderlichkeitsprüfung“ sowie „DSFA-Bericht“.

Auch die Frage, wie die über das Privatgerät zugreifbaren Daten geschützt werden, wenn das Privatgerät an andere Personen weitergegeben oder von Familienmitgliedern gemeinsam genutzt wird, ist detailliert zu bewerten.

Ich halte nach wie vor an meiner grundsätzlichen Bewertung aus dem 26. Tätigkeitsbericht 2014 unter Nr. 2.3.5 bezüglich der Verwendung von Privatgeräten fest. Kommt die schriftlich dokumentierte Risikoanalyse des Verantwortlichen zu dem Ergebnis, dass dank geeigneter technischer und organisatorischer Sicherheitsmaßnahmen keine hohen Risiken bestehen, kann in diesem konkreten Fall die Nutzung von Privatgeräten aber akzeptabel sein.

3.7 Gemeindegenaue statistische Daten zu COVID-19-Erkrankungen?

In der COVID-19-Pandemie stellt der Öffentliche Gesundheitsdienst in Bayern täglich statistische Daten zu Erkrankungen und Todesfällen, teilweise auch zu Hospitalisierungen bereit. Üblich sind „kreisgenaue" Aufstellungen, die auch in den Datenbestand des Bayerischen Landesamtes für Gesundheit und Lebensmittelsicherheit eingehen. Aus der Bürgerschaft wurde ich aber bereits mehrmals gefragt, ob die Gesundheitsämter auch „gemeindegenaue" statistische Daten herausgeben müssen. Insofern ist zu bemerken:

Als **Rechtsgrundlage** für einen Zugang zu gemeindegenauen statistischen Daten (insbesondere: Gesamtzahl der gemeldeten Erkrankungen seit Ausbruch der COVID-19-Pandemie) kommt **Art. 39 Abs. 1 Satz 1 BayDSG** in Betracht. Dort heißt es:

„Jeder hat das Recht auf Auskunft über den Inhalt von Dateien und Akten öffentlicher Stellen, soweit ein berechtigtes, nicht auf eine entgeltliche Weiterverwendung gerichtetes Interesse glaubhaft dargelegt wird und

1. *bei personenbezogenen Daten eine Übermittlung an nicht öffentliche Stellen zulässig ist und*
2. *Belange der öffentlichen Sicherheit und Ordnung nicht beeinträchtigt werden."*

Der Zugangsanspruch ist für den Bereich des Öffentlichen Gesundheitsdienstes nicht ausgeschlossen. Bürgerinnen und Bürger, die einen Zugang zu gemeindegenauen statistischen Daten begehren, können ein **berechtigtes Interesse** jedenfalls glaubhaft darlegen, wenn sie diese Angaben für ihre Wohnsitzgemeinde oder für Gemeinden der näheren Umgebung begehren. Die Daten dienen sodann einer Einschätzung persönlicher Gesundheitsrisiken. Auskunft kann aber nur hinsichtlich eines **Datenbestandes** verlangt werden, **der auch vorhanden ist**. Gesundheitsämter sind – zumal in der gegenwärtigen, mancherorts durch Ressourcenknappheit gekennzeichneten Situation – nicht verpflichtet, begehrte, jedoch nicht vorhandene Daten zu ermitteln oder Rohdaten nur für den Zweck auszuwerten, einem Gesuch nach Art. 39 Abs. 1 Satz 1 BayDSG zu entsprechen.

Im Übrigen unterliegen personenbezogene Angaben über eine Erkrankung als **Gesundheitsdaten** dem in Art. 30 Abs. 1 Satz 3 Gesundheitsdienst- und Verbraucherschutzgesetz angeordneten **Verarbeitungsverbot**. Eine Übermittlung an eine nicht öffentliche Stelle wäre somit grundsätzlich unzulässig. Da eine Regelung zu örtlichen Statistiken über das Infektionsgeschehen bei der COVID-19-Pandemie nicht besteht, können aus datenschutzrechtlicher Sicht im Rahmen von

Art. 39 Abs. 1 Satz 1 BayDSG **nur aggregierte anonymisierte Daten** bereitgestellt werden. Welche Anforderungen insofern zu stellen sind, hängt von der konkreten Lage ab.

Ob eine Bereitstellung von aggregierten anonymisierten Daten möglich ist, haben die Behörden des Öffentlichen Gesundheitsdienstes im Einzelfall zu entscheiden. Von Bedeutung sind insofern insbesondere die folgenden Gesichtspunkte:

- die **Einwohnerzahl** der Gemeinde,
- **Berichtszeiträume** (täglich/wöchentlich),
- die aktuelle **Entwicklung des Infektionsgeschehens**,
- **Datenkategorien** (etwa: Gesamtzahl der Erkrankungen seit Beginn der COVID-19-Pandemie, Zahl der genesenen, hospitalisierten oder verstorbenen Patientinnen und Patienten, Zahl der „aktiven" Fälle).

Beispiel: Ist für eine Gemeinde von 15.000 Einwohnern eine Gesamtzahl von 20 gemeldeten Erkrankungen seit Beginn der COVID-19-Pandemie auszuweisen, kann ein Rückschluss auf konkrete erkrankte Personen in der Regel nicht gezogen werden. Wird demgegenüber an einem bestimmten Tag in einer Gemeinde mit 1000 Einwohnern „vor aller Augen" ein Bürger durch den Rettungsdienst abgeholt, ließe die Bekanntgabe einer einzigen Neuinfektion für diese Gemeinde und das nämliche Datum jedenfalls den Verdacht zu, dass der betreffende Bürger an COVID-19 erkrankt ist.

Bei Gemeinden mit mindestens 10.000 Einwohnern erhebe ich im Regelfall keine datenschutzrechtlichen Bedenken gegen die Bekanntgabe täglich aufsummierter Gesamtzahlen der Erkrankungen seit Beginn der COVID-19-Pandemie. Was den tagesaktuellen Stand an Patientinnen und Patienten, die genesen, noch nicht genesen, stationär behandelt oder verstorben sind, wird das Risiko einer Rekonstruktion des Personenbezugs durch eine lediglich kreisgenaue Darstellung minimiert.

Grundsätzlich kann Art. 39 Abs. 1 Satz 1 BayDSG Zugang zu vorhandenen aggregierten anonymisierten Daten über das Infektionsgeschehen der COVID-19-Pandemie verschaffen. Vor dem Hintergrund des jeweiligen Lagebildes müssen die Gesundheitsämter allerdings den Aggregierungsgrad so wählen, dass die Rekonstruktion eines Personenbezugs ausgeschlossen ist.

4 Allgemeines Datenschutzrecht

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

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

— Im Februar 2020 erschien eine Orientierungshilfe **„Videoüberwachung durch bayerische öffentliche Stellen“**, welche die einschlägigen landesrechtlichen Vorschriften in Art. 24 BayDSG eingehend erläutert. Die Orientierungshilfe wird durch das Formular „Prüfbogen für eine Videoüberwachung durch eine bayerische öffentliche Stelle“ ergänzt. Dieses Formular bietet für die Anwendung der Norm ein „Prüfungsraster“ und ermöglicht zugleich eine Dokumentation technisch-organisatorischer Maßnahmen sowie des Eintrags im Verzeichnis der Verarbeitungstätigkeiten. Ein weiteres Formular „Vorfallsdokumentation für eine Videoüberwachung durch eine bayerische öffentliche Stelle“ soll den bayerischen öffentlichen Stellen dabei helfen, die für eine Videoüberwachung regelmäßig erforderliche Gefahrsituation adäquat darzustellen.

— Im Verlauf des Berichtszeitraums habe ich zudem mehrere Arbeitspapiere herausgebracht. So ergänzt das neue Arbeitspapier **„Informationspflichten bei der Rechnungsprüfung bayerischer öffentlicher Stellen“** (siehe Beitrag Nr. 4.4) meine Orientierungshilfe „Informationspflichten des Verantwortlichen“[19] für den sensiblen Bereich der öffentlichen Finanzkontrolle insbesondere im kommunalen Bereich. Die beiden Arbeitspapiere **„Transparenz bei Grundstücksverkäufen bayerischer Gemeinden“** (siehe Beitrag Nr. 13.1) sowie **„Datenschutz und Akteneinsichtsrechte im Gemeinderat“** behandeln Fragen des Informationszugangs auch unter datenschutzrechtlichen Gesichtspunkten.

— Ganz unterschiedlichen Themen waren die Aktuellen Kurz-Informationen 27 bis 34 gewidmet. Die Aktuelle Kurz-Information 33 **„Befreiung von der Maskenpflicht an bayerischen öffentlichen Schulen“** hat in der Abrufstatistik meiner Homepage innerhalb kurzer Zeit den mit weitem Abstand führenden Platz „erobert“; ich habe sie zwischenzeitlich mehrfach den sich schnell ändernden Rahmenbedingungen im Infektionsschutzrecht angepasst.

19 Bayerischer Landesbeauftragter für den Datenschutz, Informationspflichten des Verantwortliche, Stand 11/2018, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Informationspflichten“.

Auch ein „Papierprodukt“ ist im Berichtszeitraum erschienen. Das in einem neuen, handlichen Format gehaltene Büchlein **„Datenschutz für bayerische Gemeinderatsmitglieder“** war trotz einer beachtlichen Auflagenhöhe rasch vergriffen und liegt nun im Nachdruck vor. Es erläutert beispielhaft anhand von 25 typischen Situationen aus der Praxis datenschutzrechtliche Rahmenbedingungen der Gemeinderatsarbeit. Zur Sprache kommt etwa die Verschwiegenheitspflicht der Mandatsträger, die auch dem Schutz personenbezogener Daten dient. Die Nutzung von Smartphones bei der Gemeinderatsarbeit ist ebenso Thema wie der Einsatz von Ratsinformationssystemen. Weiterhin geht es beispielsweise um den Datenschutz bei Personalentscheidungen oder den Zugang zu Adressdaten von Bürgerinnen und Bürgern.

Um den Bezug dieser Broschüre wie auch aller anderen Printprodukte zu erleichtern, habe ich auf meiner Internetpräsenz https://www.datenschutz-bayern.de in der Rubrik „Broschürenbestellung“ ein **Online-Bestellformular** eingerichtet, das von öffentlichen Stellen wie auch von Privatpersonen lebhaft genutzt wird. Von der Freischaltung am 1. Oktober 2020 bis Jahresende gingen gut 700 Bestellungen ein.

Bayerische öffentliche Stellen, ihre Datenschutzbeauftragten wie auch alle anderen am Datenschutz Interessierten haben seit jeher die Möglichkeit, sich per **RSS-Feed** über Neuigkeiten auf meiner Internetpräsenz informieren zu lassen. Dieses Angebot ist eine datenschutzfreundliche Alternative zu einem Newsletter, weil es ohne eine Sammlung von Kontaktdaten auskommt. Seit Mitte 2020 wird für jede neue Publikation ein Hinweis mit einer kurzen Inhaltsangabe gepostet. Die Einbindung von RSS-Feeds in einen E-Mail-Client ist in der Regel nicht schwierig. Hinweise dazu sind auf https://www.datenschutz-bayern.de unter „RSS“ zu finden.

Für das **Jahr 2021** sind insbesondere wieder mehrere neue Orientierungshilfen und Arbeitspapiere sowie eine Fortführung der bewährten Reihe „Aktuelle Kurz-Informationen“ geplant.

4.2 Eine bayerische öffentliche Stelle – mehrere Datenschutzbeauftragte?

Behörden und sonstige bayerische öffentliche Stellen haben gemäß Art. 37 Abs. 1 Buchst. a DSGVO in Verbindung mit Art. 1 und 2 BayDSG in jedem Fall einen behördlichen Datenschutzbeauftragten zu benennen. In diesem Zusammenhang wurde die Frage an mich herangetragen, ob es zulässig sei, dass eine bayerische öffentliche Stelle mehrere Datenschutzbeauftragte mit jeweils klar abgegrenzter Zuständigkeit benenne. Meiner Auffassung nach ist diese Frage zu verneinen.

4.2.1 Ein Verantwortlicher – ein Datenschutzbeauftragter

Bereits der Wortlaut des Art. 37 Abs. 1 Buchst. a DSGVO legt nahe, dass ein Verantwortlicher in Erfüllung seiner gesetzlichen Verpflichtung jeweils nur einen Datenschutzbeauftragten benennen kann. Zwingend ausgeschlossen ist die Benennung mehrerer Datenschutzbeauftragter hierdurch gleichwohl nicht.

Gegen diese Möglichkeit sprechen aber insbesondere die institutionelle Einordnung sowie die Aufgaben des Datenschutzbeauftragten: Dieser soll unter anderem betroffenen Personen als Ansprechpartner (vgl. Art. 38 Abs. 4 DSGVO) und der Aufsichtsbehörde als Anlaufstelle (vgl. Art. 39 Abs. 1 Buchst. d und e DSGVO)

zur Verfügung stehen. Die Benennung mehrerer Datenschutzbeauftragter, die auch nach außen hin mit abgegrenzten Zuständigkeiten in Erscheinung treten, würde dieser Konzeption zuwiderlaufen. Weder betroffenen Personen noch der Aufsichtsbehörde kann zugemutet werden, die für sie zuständige Kontaktperson erst mittels einer „Vorprüfung" identifizieren zu müssen. Mit dem Datenschutzbeauftragten soll gerade dann jemand greifbar sein, wenn es um Datenschutzrechte geht und sich Funktionseinheiten des Verantwortlichen auf die eigene interne Unzuständigkeit berufen. Im Übrigen kann die Aufgabe des Datenschutzbeauftragten nur mit einem Gesamtüberblick über die Tätigkeit des Verantwortlichen effektiv wahrgenommen werden.

Unzulässig wäre es somit, wenn eine bayerische öffentliche Stelle als ein Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO in Verbindung mit Art. 3 Abs. 2 BayDSG mehrere Datenschutzbeauftragte benennt.

Demgegenüber benennen mehrere Verantwortliche in der Regel grundsätzlich auch dann jeweils für sich einen Datenschutzbeauftragten, wenn sie organisatorisch eng verbunden sind (wie etwa die Mitgliedsgemeinden einer Verwaltungsgemeinschaft). In solchen Fällen kann aber eine Kooperation angezeigt sein, indem ein gemeinsamer Datenschutzbeauftragter im Sinne von Art. 37 Abs. 3 DSGVO benannt wird oder alle verbundenen Stellen denselben Datenschutzbeauftragten benennen.

Zu beachten ist in diesem Zusammenhang ferner, dass auf Grundlage von Art. 4 Nr. 7 Halbsatz 2 DSGVO durch entsprechende gesetzliche Regelungen (ausnahmsweise, vgl. Art. 3 Abs. 2 Halbsatz 2 BayDSG) auch einzelnen Organisationseinheiten einer bayerischen öffentlichen Stelle für bestimmte Verarbeitungsvorgänge die Rolle des Verantwortlichen zugewiesen werden kann (vgl. etwa im Sozialrecht § 67 Abs. 4 Satz 2 Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz –).

4.2.2 Stellvertreter und Hilfskräfte des Datenschutzbeauftragten

Die dargestellte Auffassung steht der – rechtlich überdies gebotenen – Benennung eines stellvertretenden Datenschutzbeauftragten durch den Verantwortlichen nicht entgegen. Ein solcher tritt nämlich nur im Vertretungsfall, insbesondere bei Urlaub oder Erkrankung des „eigentlich" benannten Datenschutzbeauftragten an dessen Stelle – dann aber auch vollumfänglich. Nach außen hin erkennbare Unklarheiten oder Abgrenzungsfragen hinsichtlich der Zuständigkeiten sind hier nicht zu befürchten.

Ferner lässt es die dargestellte Auffassung zu, dass der benannte (interne oder externe) Datenschutzbeauftragte durch Hilfskräfte bei seiner Aufgabenerfüllung unterstützt wird. Ab einer bestimmten Größe des Verantwortlichen wird dies ohnehin unabdingbar sein; schließlich hat der Verantwortliche seinem Datenschutzbeauftragten gemäß Art. 38 Abs. 2 DSGVO die zur Aufgabenerfüllung erforderlichen – gegebenenfalls auch personellen – Ressourcen zur Verfügung zu stellen. Die interne Ausgestaltung bleibt dabei dem organisatorischen Ermessen des Verantwortlichen überlassen; in Betracht kommt etwa die Etablierung eines unterstützenden „Datenschutzteams" oder von „örtlichen Ansprechpartnern für den Datenschutz". In diesem Rahmen ist auch eine interne Festlegung dahingehend möglich, dass beispielsweise einzelnen Hilfskräften des Datenschutzbeauftragten bestimmte fachliche Schwerpunkte zugewiesen werden. Unberührt hiervon bleibt

freilich der Umstand, dass der Verantwortliche nur einen Datenschutzbeauftragten im Sinne der Art. 37 ff. DSGVO benennen kann. Bei diesem muss es sich im Übrigen um eine natürliche Person handeln, welche die Anforderungen des Art. 37 Abs. 5 DSGVO erfüllt.[20]

4.2.3 Fazit

Für eine bayerische öffentliche Stelle kann jeweils nur ein behördlicher Datenschutzbeauftragter benannt werden, der dann – seinen gesetzlichen Aufgaben entsprechend – einheitlich betroffenen Personen als Ansprechpartner und der Aufsichtsbehörde als Anlaufstelle zur Verfügung steht. Die Benennung mehrerer Datenschutzbeauftragter durch ein und denselben Verantwortlichen ist demgegenüber rechtlich nicht möglich, birgt ein solches Vorgehen doch die Gefahr, dass sich insbesondere betroffene Personen zunächst an die „falsche", weil für ihr jeweiliges Anliegen unzuständige Stelle wenden. Dies würde insbesondere eine effektive Durchsetzung von Betroffenenrechten erschweren.

Die rechtlich gebotene Benennung eines stellvertretenden Datenschutzbeauftragten bleibt freilich ebenso möglich wie die Zuweisung (weiterer) personeller Ressourcen an den Datenschutzbeauftragten.

4.3 Post für den behördlichen Datenschutzbeauftragten: Zuleitung nur ungeöffnet?

Der behördliche Datenschutzbeauftragte erhält auf analogen wie auf elektronischen Wegen alle möglichen Nachrichten. Darunter sind auch Zuschriften von Bürgerinnen und Bürgern sowie Anfragen von Kolleginnen und Kollegen. Gerade solche Zuschriften und Anfragen können einen vertraulichen Inhalt haben. An mich wurde bereits mehrfach die Frage gerichtet, wie im behördlichen Geschäftsgang mit analoger und elektronischer Post an den behördlichen Datenschutzbeauftragten umzugehen ist. Ich gebe dazu die folgenden datenschutzrechtlichen Hinweise:

4.3.1 Analoge Post

Die Behandlung von Eingängen ist in § 12 Allgemeine Geschäftsordnung für die Behörden des Freistaates Bayern (AGO) geregelt. Da es sich hierbei um eine von der Bayerischen Staatsregierung erlassene Verwaltungsvorschrift handelt, gelten die Vorschriften „von sich aus" nur für die bayerischen Staatsbehörden. Gleichwohl empfiehlt § 36 AGO insbesondere den kommunalen Trägern, die Vorschriften der Allgemeinen Geschäftsordnung ebenfalls anzuwenden. Zweckmäßig ist dabei der Erlass einer innerbehördlichen Regelung, welche dieses Regelwerk – gegebenenfalls mit einzelnen örtlichen Anpassungen – übernimmt. Das kommunale Selbstverwaltungsrecht lässt es aber auch zu, ein eigenständiges Gegenstück zur Allgemeinen Geschäftsordnung zu erlassen. § 12 AGO bestimmt:

[20] Vgl. ausführlich hierzu Bayerischer Landesbeauftragter für den Datenschutz, Der behördliche Datenschutzbeauftragte, Stand 5/2018, insbesondere Abschnitt II Nr. 3 Buchst. a, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Behördlicher Datenschutzbeauftragter".

„(1) [1]Es wird eine zentrale Eingangsstelle vorgehalten, die die an die Behörde gerichteten Sendungen (Eingänge) entgegennimmt. [2]Sie bearbeitet die Eingänge nach Maßgabe der folgenden Absätze und gibt sie in den Geschäftsgang.
[…]
(4) [1]Eingänge, die an Beschäftigte erkennbar persönlich gerichtet sind, sind diesen unmittelbar und ungeöffnet zuzuleiten. [2]Sind die Empfänger abwesend, können die Sendungen von der Vertretung geöffnet werden, wenn äußere Merkmale einen dienstlichen Inhalt erkennen lassen oder wenn sich die Empfänger mit dem Öffnen der Sendungen einverstanden erklärt haben. [3]Enthält der Eingang eine dienstliche Mitteilung, ist nach Absatz 6 zu verfahren. [4]Bei Eingängen mit der Behördenanschrift und dem Zusatz ‚zu Händen von' ist sicherzustellen, dass die bezeichneten Personen von ihnen Kenntnis erhalten. [5]Eingänge, die als Personalsache gekennzeichnet sind, dürfen nur von den zuständigen Personal verwaltenden Stellen geöffnet werden. [6]Sendungen an Personalvertretungen, Schwerbehindertenvertretungen und Gleichstellungsbeauftragte sind diesen ungeöffnet und unmittelbar zuzuleiten."

Eingehende Sendungen werden danach grundsätzlich von der Eingangsstelle (etwa einer Poststelle) geöffnet und – nach Anbringen des Eingangsstempels (vgl. § 12 Abs. 2 AGO) – in den Geschäftsgang gegeben; sie erreichen den zuständigen Bearbeiter oder die zuständige Bearbeiterin auf dem innerbehördlich vorgezeichneten Weg, an dem regelmäßig Vorgesetzte die entsprechenden Schriftstücke zur Kenntnis nehmen und/oder Bearbeitungsvermerke anbringen (können).

Die Zuleitung einer ungeöffneten Sendung unmittelbar an einen bestimmten Adressaten oder eine bestimmte Adressatin innerhalb der Behörde bildet den Ausnahmefall. Sie muss durch ein besonderes, rechtlich geschütztes Vertraulichkeitsinteresse gefordert sein. § 12 Abs. 4 AGO nennt mit der persönlichen Adressierung an einen Beschäftigten oder eine Beschäftigte (§ 12 Abs. 4 Satz 1 AGO; dazu ausführlich der Beitrag Nr. 19.2 „Postöffnung in Behörden" in meinem 22. Tätigkeitsbericht 2006), der Adressierung an Personalvertretungen, Schwerbehindertenvertretungen und Gleichstellungsbeauftragte (§ 12 Abs. 4 Satz 6 AGO) sowie der Kennzeichnung als Personalsache (§ 12 Abs. 4 Satz 5 AGO) einige dieser Ausnahmefälle.

Für Sendungen an behördliche Datenschutzbeauftragte enthält § 12 Abs. 4 AGO dagegen keine Regelung, die eine unmittelbare Zuleitung von ungeöffneten Sendungen anordnet. Eine solche Anordnung kann sich aber auch aus Vorschriften außerhalb der Allgemeinen Geschäftsordnung ergeben.

Art. 38 Abs. 3 DSGVO bestimmt zur Stellung des Datenschutzbeauftragten:

„Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. […] Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters."

Der behördliche Datenschutzbeauftragte ist in dieser Funktion weisungsfrei, selbst wenn er bei dem Verantwortlichen noch andere Aufgaben wahrnehmen und insofern weisungsgebunden sein sollte. Er wird – in Bezug auf eine von Art. 38 Abs. 3 Satz 1 DSGVO nicht ausgeschlossene Dienstaufsicht – grundsätzlich der Behördenleitung zugeordnet. In diesen Punkten unterscheidet er sich von den meisten (anderen) Beschäftigten der Behörde.

Soweit § 12 AGO einen Geschäftsgang regelt, den ein „Leben in der Hierarchie“ erfordert, werden die Bestimmungen der Funktion nicht gerecht, die der behördliche Datenschutzbeauftragte innehat:

— Die regelgemäße mittelbare Zuleitung geöffneter Sendungen verliefe an den behördlichen Datenschutzbeauftragten (zumindest) über die Behördenleitung. Diese könnte wegen der Weisungsfreiheit des behördlichen Datenschutzbeauftragten aber keine (von diesem zu beachtenden) Bearbeitungsvermerke anbringen.

— Die Behördenleitung dürfte den Inhalt der Sendungen oftmals auch gar nicht zur Kenntnis nehmen: Werden dem behördlichen Datenschutzbeauftragten in seiner Funktion nämlich Tatsachen anvertraut, ist er nach Maßgabe von Art. 38 Abs. 5 DSGVO in Verbindung mit Art. 12 Abs. 2 BayDSG zur Verschwiegenheit verpflichtet. Dies gilt auch und gerade gegenüber der Behördenleitung.

— Die Verschwiegenheitsverpflichtung sichert im Übrigen den grundsätzlich ungehinderten Zugang von Beschäftigten sowie von Bürgerinnen und Bürgern zum behördlichen Datenschutzbeauftragten ab.[21]

Vor diesem Hintergrund sind an den behördlichen Datenschutzbeauftragten gerichtete Sendungen diesem unmittelbar und ungeöffnet zuzuleiten. Eine Sendung ist an den behördlichen Datenschutzbeauftragten insbesondere dann gerichtet, wenn sie im Adressfeld diese Funktion nennt, oder wenn der Absender einen Versandvermerk wie etwa „Persönlich“ oder „Verschlossen“ verwendet hat.

4.3.2 Elektronische Post

Was die elektronische Kommunikation – insbesondere mittels E-Mail – betrifft, muss der Verantwortliche ebenfalls einen „unbeobachteten“ Zugang sicherstellen. Dies geschieht durch Bereitstellen einer (Funktions-)E-Mail-Adresse – etwa in der Form „datenschutzbeauftragter@[Bezeichnung der Behörde].de“. Für das entsprechende Postfach dürfen nur der behördliche Datenschutzbeauftragte und gegebenenfalls zur Vertretung oder Mitarbeit berufene Personen zugriffsberechtigt sein.

4.3.3 Sonderfälle

Manchmal erreichen einen behördlichen Datenschutzbeauftragten auch Eingänge, die „eigentlich“ durch den Verantwortlichen (insbesondere durch ein Fachsachgebiet) zu bearbeiten wären. Das geschieht etwa dann, wenn sich Bürgerinnen und Bürger über die Zuständigkeiten innerhalb der Behörde nicht im Klaren sind, wenn einzelne Bedienstete Kundinnen und Kunden bei Fragen mit datenschutzrechtlichem Bezug (vorschnell) an den behördlichen Datenschutzbeauf-

[21] Dazu ausführlich Bayerischer Landesbeauftragter für den Datenschutz, Dienstweg und Zugang zum behördlichen Datenschutzbeauftragten bei bayerischen öffentlichen Stellen, Aktuelle Kurz-Information 12, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Aktuelle Kurz-Informationen“.

tragten verweisen, oder auch dann, wenn an den behördlichen Datenschutzbeauftragten – ungeachtet der Frage, ob dies im Einzelfall zulässig ist – tatsächlich Aufgaben des Verantwortlichen delegiert worden sind.

Eine Öffnung aller an den behördlichen Datenschutzbeauftragten gerichteten Sendungen durch die Poststelle sowie eine Sichtung – etwa seitens der Behördenleitung – mit dem Ziel, Eingänge dieser Art „herauszufiltern", ist unstatthaft. Vielmehr hat allein der behördliche Datenschutzbeauftragte zu prüfen, welche der ihm unmittelbar und ungeöffnet zugeleiteten Sendungen durch ihn selbst und welche durch andere Stellen in der Behörde zu erledigen sind. „Fehlläufer" wird er unverzüglich an die Eingangsstelle zurückgeben.

4.3.4 Fazit

Auch wenn die Allgemeine Geschäftsordnung die Behandlung an den behördlichen Datenschutzbeauftragten gerichteter Sendung nicht näher regelt, sind die bayerischen öffentlichen Stellen gehalten, „unbeobachtete" Zugangswege zu gewährleisten. Analoge Post muss dem behördlichen Datenschutzbeauftragten in ungeöffnetem Zustand unmittelbar zugeleitet werden. Für eingehende E-Mails ist ein Postfach einzurichten, auf das grundsätzlich nur der behördliche Datenschutzbeauftragte Zugriff hat.

4.4 Informationspflichten bei der Rechnungsprüfung bayerischer öffentlicher Stellen

Die Tätigkeit der bayerischen Verwaltung unterliegt einer Finanzkontrolle. Dies gilt für die Behörden des Staates ebenso wie für die Träger der mittelbaren Staatsverwaltung, insbesondere die Gemeinden, Landkreise und Bezirke. Die Organe der Rechnungsprüfung nutzen dabei eine Vielzahl von Akten und Dateien. Solche Informationsbestände enthalten oftmals personenbezogene Daten von Bürgerinnen und Bürgern oder von Beschäftigten. Vor diesem Hintergrund stellt sich die Frage, ob die geprüften Stellen und/oder die Rechnungsprüfungsorgane gegenüber betroffenen Personen Informationspflichten nach Art. 13 und 14 DSGVO erfüllen müssen.

Die Informationspflichten nach Art. 13 und 14 DSGVO habe ich in meiner Orientierungshilfe „Informationspflichten des Verantwortlichen"[22] ausführlich erläutert. Der vorliegende Beitrag beruht auf diesen Erläuterungen. Er stellt einführend die im bayerischen öffentlichen Sektor vorgesehenen Rechnungsprüfungsorgane vor (Nr. 4.4.1) und zeigt den datenschutzrechtlichen Bezug ihrer Prüftätigkeit auf (Nr. 4.4.2). Auf dieser Grundlage erörtert er, ob eine geprüfte Stelle (Nr. 4.4.3) oder ein Rechnungsprüfungsorgan (Nr. 4.4.4) Informationspflichten nach Art. 13 und 14 DSGVO treffen.

4.4.1 Rechnungsprüfungsorgane im bayerischen öffentlichen Sektor

Die Finanzkontrolle wird in Bayern von verschiedenen Rechnungsprüfungsorganen wahrgenommen. Sie ist im **staatlichen Bereich** Aufgabe des **Bayerischen**

[22] Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Informationspflichten".

Obersten Rechnungshofs, dem fünf **Staatliche Rechnungsprüfungsämter** nachgeordnet sind. Kern dieser Aufgabe ist die Prüfung der Haushalts- und Wirtschaftsführung des Staates, seiner Betriebe und Sondervermögen (Art. 88 Abs. 1 Satz 1 Bayerische Haushaltsordnung – BayHO). Geprüft werden können aber etwa auch die Verwendung staatlicher Mittel durch nichtstaatliche Stellen (vgl. Art. 91 BayHO) oder Beteiligungen des Staates (vgl. Art. 92 BayHO).

Allerdings unterliegt der **Bayerische Oberste Rechnungshof** einer Datenschutzaufsicht durch den Bayerischen Landesbeauftragten für den Datenschutz nur, soweit er in Verwaltungsangelegenheiten tätig wird; bei seiner Prüftätigkeit ist er zwar an das materielle Datenschutzrecht gebunden, von der Datenschutzaufsicht aber freigestellt (vgl. Art. 1 Abs. 1 Satz 3 BayDSG).

Im **kommunalen Bereich** ist zwischen der vom kommunalen Träger selbst verantworteten örtlichen und einer überörtlichen Rechnungsprüfung zu unterscheiden, die eine externe Behörde durchführt. Die örtliche Rechnungsprüfung nimmt in kleineren Gemeinden mitunter der **Gemeinderat** selbst – gegebenenfalls unterstützt durch eine externe sachverständige Person – wahr. Größere Gemeinden bilden für diese Aufgabe einen **Rechnungsprüfungsausschuss** (vgl. Art. 103 Abs. 2 Halbsatz 1 Gemeindeordnung – GO). Sachverständige Unterstützung leistet in den meisten Großen Kreisstädten sowie – hier verpflichtend – in den kreisfreien Gemeinden ein (eigenes) **Rechnungsprüfungsamt** (auch „Revisionsamt", näher Art. 104 GO). Rechnungsprüfungsausschüsse und Rechnungsprüfungsämter gibt es auch bei den Landkreisen und Bezirken (vgl. Art. 89 Abs. 1, Art. 90 Landkreisordnung – LKrO, Art. 85 Abs. 1, Art. 86 Bezirksordnung – BezO). Überörtliche Prüfungen führt der **Bayerische Kommunale Prüfungsverband** bei den Landkreisen (Art. 91 Abs. 1 LKrO) und Bezirken (Art. 87 Abs. 1 Satz 1 BezO) sowie bei denjenigen Gemeinden durch, die zu seinen Mitgliedern zählen (Art. 105 Abs. 1 Var. 1 GO).[23] Für alle anderen Gemeinden sind die **Staatlichen Rechnungsprüfungsstellen** bei den Landratsämtern zuständig (Art. 105 Abs. 1 Var. 2 GO).

Soweit das bayerische Datenschutzrecht allgemein und ohne ausdrückliche Einschränkung den Begriff „Rechnungsprüfung" verwendet, wie dies etwa in Art. 6 Abs. 1 BayDSG und Art. 103 Satz 3 Bayerisches Beamtengesetz (BayBG) der Fall ist, erfasst es alle Rechnungsprüfungsorgane des staatlichen wie des staatsmittelbaren Bereichs.

4.4.2 Datenschutzrechtlicher Bezug der Prüftätigkeit

Die gesetzlichen Bestimmungen zur Finanzkontrolle sehen weitreichende **Auskunfts- und Vorlagerechte** der Rechnungsprüfungsorgane vor, so insbesondere Art. 95 BayHO im staatlichen sowie Art. 106 Abs. 6 GO, Art. 92 Abs. 6 LKrO und Art. 88 Abs. 6 BezO im kommunalen Bereich. In Art. 106 Abs. 6 GO heißt es etwa:

„[1]Die Organe der Rechnungsprüfung der Gemeinde und das für sie zuständige überörtliche Prüfungsorgan können verlangen, dass ihnen oder ihren beauftragten

[23] Zur Mitgliedschaft im Bayerischen Kommunalen Prüfungsverband siehe näher Art. 3 Prüfungsverbandsgesetz sowie Verwaltungsgericht Regensburg, Urteil vom 16. Oktober 2015, RO 3 K 14.1274, BeckRS 2015, 54495.

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."

Machen Rechnungsprüfungsorgane von solchen Auskunfts- und Vorlagerechten Gebrauch, gelangen sie oftmals an personenbezogene Daten. Solche Daten können „nebenbei" zur Kenntnis genommen werden, jedoch auch gerade Gegenstand einer Prüfung sein.

Beispiel 1: Der Bayerische Kommunale Prüfungsverband sichtet bei einem Landkreis im Rahmen der überörtlichen Rechnungsprüfung ausgewählte Akten über Vergabeverfahren zur Beschaffung von Bauleistungen. Er möchte feststellen, ob sich der Landkreis jeweils an die Vorgaben des Vergaberechts gehalten hat. Dabei erfährt der Prüfungsverband die Namen der für den Landkreis sowie für die Beteiligten handelnden Personen, denen bestimmte Verfahrenshandlungen zugeordnet werden können. Er gelangt so an personenbezogene Daten, auch wenn es für die Prüfung auf diese Daten nicht ankommt.

Beispiel 2: Das Rechnungsprüfungsamt einer Stadt möchte herausfinden, ob die von ihr betriebene Musikschule Beitragsermäßigungen bei Bedürftigkeit nur satzungsgemäß bewilligt hat. Es lässt sich zu diesem Zweck alle einschlägigen Vorgänge eines Haushaltsjahres vorlegen und überprüft, ob entsprechende Anträge vorliegen sowie über diese ordnungsgemäß entschieden wurde. Das Rechnungsprüfungsamt erlangt hier Informationen über die Identität der antragstellenden Personen und die von ihnen vorgebrachten, für eine Bedürftigkeit sprechenden Argumente. Das geschieht nicht „beiläufig"; es geht bei der Prüfung gerade darum, was die Verwaltung bei der Entscheidung über die Beitragsermäßigung aus diesen personenbezogenen Daten gemacht hat.

Das **Rechnungsprüfungsorgan** benötigt für die **Anforderung**, die **geprüfte Stelle** für eine entsprechende **Offenlegung** eine Verarbeitungsbefugnis. Unionsrechtlich ergibt sich das aus Art. 6 Abs. 1 DSGVO.

Was das **Rechnungsprüfungsorgan** betrifft, erfüllt Art. 106 Abs. 6 Satz 1 GO diese Funktion. Die Vorschrift ist zwar nicht spezifisch auf eine Anforderung von personenbezogenen Daten hin formuliert; indes verdeutlicht Art. 106 Abs. 6 Satz 3 GO, dass die Vorschrift auch diesen Anwendungsfall erfassen soll:[24]

„[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."

Gerade bei einer Anforderung (auch) von personenbezogenen Daten muss das Rechnungsprüfungsorgan darauf achten, dass das in seiner Befugnis enthaltene, in diesem Kontext datenschutzrechtlich „aufgeladene" Erforderlichkeitskriterium – Art. 106 Abs. 6 Satz 1 GO: „die [die Rechnungsprüfungsorgane] zur Erfül-

[24] Siehe auch Landtags-Drucksache 15/1063, S. 21: „In Anlehnung an die für den Obersten Rechnungshof in Art. 95 BayHO getroffenen Regelungen werden die Befugnisse der örtlichen und der überörtlichen Prüfungsorgane der Gemeinde gesetzlich klargestellt. Insbesondere haben diese ein Einsichtsrecht in Personal-, Sozial- und sonstige besonderen Einschränkungen unterliegenden Dateien oder Akten, soweit sie es zur Erfüllung ihrer Aufgaben für erforderlich halten".

lung ihrer Aufgaben für erforderlich halten“ – nicht verfehlt wird. Das Rechnungsprüfungsorgan muss sich dazu der Grenzen seines Aufgabenkreises bewusst sein; es ist grundsätzlich zur Finanzkontrolle, nicht zur allgemeinen Verwaltungskontrolle berufen (siehe etwa Art. 106 Abs. 1 GO: „Einhaltung der für die Wirtschaftsführung geltenden Vorschriften und Grundsätze“).

Die **geprüfte Stelle**, welche personenbezogene Daten im Rahmen einer Prüfung gegenüber dem Rechnungsprüfungsorgan offenlegen muss, kann einen solchen Datenumgang regelmäßig auf die für sie maßgeblichen Verarbeitungsbefugnisse stützen (beispielsweise auf Art. 4 und 5 BayDSG, jeweils in Verbindung mit Art. 6 Abs. 1 BayDSG). Das Fachrecht kann Sonderregelungen enthalten (so etwa Art. 103 Satz 3 BayBG für Personaldaten).

4.4.3 Informationspflicht der geprüften Stelle

Eine Informationspflicht gegenüber betroffenen Personen könnte zunächst die geprüfte Stelle treffen, wenn diese einem Rechnungsprüfungsorgan Informationen zur Verfügung stellt, die (auch) personenbezogene Daten enthalten. Maßgeblich sind insofern Art. 13 und 14 DSGVO.

4.4.3.1 Informationspflicht nach Art. 13 Abs. 1 DSGVO

Art. 13 Abs. 1 DSGVO regelt die Informationspflicht gegenüber der betroffenen Person, wenn der gemäß Art. 4 Nr. 7 DSGVO datenschutzrechtlich Verantwortliche bei dieser personenbezogene Daten erhebt. Legt die geprüfte Stelle personenbezogene Daten gegenüber dem Rechnungsprüfungsorgan offen, ist dies hinsichtlich der geprüften Stelle nicht als Erhebung zu werten. Art. 13 Abs. 1 DSGVO begründet deshalb insofern keine Informationspflicht. Das ist auch unbedenklich, weil die geprüfte Stelle meist bereits bei einer (früheren) Erhebung der Daten oder ihrer (sonstigen) Erlangung nach Art. 13 Abs. 1 oder Art. 14 Abs. 1 DSGVO informationspflichtig war, und weil Rechnungsprüfungsorgane zu den „planmäßigen“ Empfängern gehören, über die ohnehin nach Art. 13 Abs. 1 Buchst. e und Art. 14 Abs. 1 Buchst. e DSGVO zu informieren ist.

Beispiel 3: Die städtische Musikschule aus Beispiel 2 legt in ihren Datenschutzhinweisen dar, dass das Rechnungsprüfungsamt zu den Empfängern von personenbezogenen Daten gehört, die Benutzerinnen und Benutzer im Zusammenhang mit der Begründung und Durchführung eines Benutzungsverhältnisses zur Kenntnis bringen.

4.4.3.2 Informationspflicht nach Art. 13 Abs. 3 DSGVO

Demgegenüber normiert Art. 13 Abs. 3 DSGVO den Fall einer Weiterverarbeitung von personenbezogenen Daten, die nach Art. 13 Abs. 1 DSGVO erhoben sind. Hier entsteht eine Informationspflicht, wenn der Verantwortliche beabsichtigt, diese Daten für einen anderen Zweck als den Erhebungszweck weiterzuverarbeiten. Eine solche Weiterverarbeitung kann auch in der Offenlegung gegenüber einer anderen Stelle liegen.

Waren die Daten ursprünglich für einen bestimmten Verarbeitungszweck erhoben, werden sie im Rahmen der Rechnungsprüfung auf den ersten Blick für einen anderen Zweck verwendet.

Beispiel 4: In Beispiel 2 machen die antragstellenden Personen gegenüber der Musikschule auf einem dafür bereitgestellten Vordruck Angaben zu ihren wirtschaftlichen Verhältnissen, um eine Beitragsermäßigung zu erhalten. Zu diesem Zweck werden die Daten von der Musikschule auch verarbeitet. Nimmt nun das Rechnungsprüfungsamt Einsicht in diese Anträge, verfolgt es dagegen den Zweck, die Sparsamkeit und Wirtschaftlichkeit der Verwaltung sicherzustellen (vgl. Art. 106 Abs. 1 Nr. 3 GO)

Gleichwohl bestimmen Art. 6 Abs. 1 BayDSG im Allgemeinen und Art. 103 Satz 3 BayBG für Personaldaten im Speziellen, dass bayerische öffentliche Stellen, die personenbezogene Daten verarbeiten dürfen, dies unter anderem auch zur Rechnungsprüfung tun können. Der bayerische Gesetzgeber hat durch diese gesetzlichen Regelungen den ursprünglichen Zweck der Datenverarbeitung auf eine Datenverarbeitung im Rahmen der Rechnungsprüfung erweitert. Jedem beliebigen Verarbeitungszweck, den eine bayerische öffentliche Stelle verfolgt, ist dieser Zweck also gleichsam „angelagert". Man spricht hier auch von der Fiktion eines identischen Zwecks. Das hat zur Folge, dass die Weiterverarbeitung durch Offenlegung an ein Rechnungsprüfungsorgan nicht als zweckändernd anzusehen ist; auch Art. 13 Abs. 3 DSGVO begründet insofern keine Informationspflicht der geprüften Stelle.

4.4.3.3 Informationspflicht nach Art. 14 Abs. 1 DSGVO

Im Gegensatz zu Art. 13 Abs. 1 DSGVO sieht Art. 14 Abs. 1 DSGVO eine Informationspflicht vor, wenn personenbezogene Daten nicht bei der betroffenen Person erhoben werden, sondern die öffentliche Stelle die Daten auf anderem Wege erlangt. Hat die geprüfte Stelle die personenbezogenen Daten ursprünglich etwa bei einem Dritten erhoben, so wird sie regelmäßig nach Art. 14 Abs. 1 DSGVO informationspflichtig gewesen sein. Die Offenlegung gegenüber einem Rechnungsprüfungsorgan führt bei ihr aber nicht dazu, dass sie die Daten ein weiteres Mal erlangt, sodass Art. 14 Abs. 1 DSGVO keine Informationspflicht begründet.

4.4.3.4 Informationspflicht nach Art. 14 Abs. 4 DSGVO

Allerdings regelt Art. 14 Abs. 4 DSGVO eine Informationspflicht für den Fall, dass der Verantwortliche die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten beabsichtigt als den, für den er die personenbezogenen Daten erlangt hat. Einer Informationspflicht der geprüften Stelle nach Art. 14 Abs. 4 DSGVO für den Fall, dass die Daten nicht bei der betroffenen Person erhoben wurden, steht allerdings wie bei Art. 13 Abs. 3 DSGVO die Fiktion der Identität von ursprünglichem Verarbeitungszweck und Rechnungsprüfungszweck entgegen (siehe Nr. 4.4.3.2). Weil Art. 6 Abs. 1 BayDSG und Art. 103 Satz 3 BayBG den ursprünglichen Verarbeitungszweck und den Zweck „Rechnungsprüfung" verknüpfen, fehlt es an der von Art. 14 Abs. 4 DSGVO geforderten Zweckänderung.

4.4.4 Informationspflicht des Rechnungsprüfungsorgans

Die Frage, ob das Rechnungsprüfungsorgan Informationspflichten gegenüber betroffenen Personen erfüllen muss, ist ebenfalls anhand der Art. 13 und 14 DSGVO zu beantworten. Ansatzpunkt ist hier die Erhebung der Daten bei der geprüften Stelle und die Weiterverwendung im Rahmen der Prüfungstätigkeit.

4.4.4.1 Informationspflichten nach Art. 13 DSGVO

Wie die geprüfte Stelle trifft **grundsätzlich** auch das Rechnungsprüfungsorgan **keine Informationspflicht** nach Art. 13 Abs. 1 DSGVO. Es erhebt regelmäßig keine personenbezogenen Daten bei einer betroffenen Person, wenn es sich personenbezogene Daten von der geprüften Stelle offenlegen lässt oder sonst – etwa durch automatisierten Abruf – bei dieser auf personenbezogene Daten zugreift. Ebenso scheidet dann eine Informationspflicht des Rechnungsprüfungsorgans nach Art. 13 Abs. 3 DSGVO aus, weil es an einer „Ersterhebung" fehlt.

Gleichwohl kann es bei Prüfungshandlungen **ausnahmsweise** erforderlich werden, die **Informationspflicht** nach Art. 13 Abs. 1 DSGVO zu erfüllen. Zu denken ist hier insbesondere an die folgenden beiden Konstellationen:

— Das Rechnungsprüfungsorgan beschafft sich auf Grund eines entsprechenden Auskunftsrechts Informationen über die Verwendung öffentlicher Mittel außerhalb der „eigentlich" geprüften öffentlichen Stelle, insbesondere bei einem **Zuwendungsempfänger**.

Beispiel 5: Ein Landwirt hat für seine Tätigkeit eine Zuwendung aus einem öffentlichen Förderprogramm erhalten. Das Rechnungsprüfungsorgan möchte feststellen, ob diese Mittel auch dem Zweck entsprechend eingesetzt worden sind, zu welchem sie ausgereicht wurden. Es macht deshalb von der – gesetzlich (vgl. Art. 91 Abs. 1 Satz 1 Nr. 3, Abs. 2 BayHO) oder etwa in Förderbedingungen vorgesehenen – Möglichkeit Gebrauch, Informationen bei Zuwendungsempfängern einzuholen. Zuvor erteilt es dem Landwirt die Informationen nach Art. 13 Abs. 1 DSGVO.

— Das Rechnungsprüfungsorgan stößt im Zuge der Sachverhaltsermittlung bei einer geprüften öffentlichen Stelle auf eine **„Missstandszeugin"** oder einen **„Missstandszeugen"**. Zur Wahrnehmung seiner Prüfungsaufgaben ist jedes Rechnungsprüfungsorgan auf eine Vielzahl von Informationen angewiesen. Diese Informationen erhält es zu einem Gutteil in der Kommunikation mit Beschäftigten der geprüften öffentlichen Stelle. Im Regelfall wird dadurch nicht die Informationspflicht nach Art. 13 Abs. 1 DSGVO ausgelöst, weil die Beschäftigten „für" ihre öffentliche Stelle sprechen und nicht für sich selbst. Diese Rolle können die Beschäftigten im Einzelfall aber insbesondere dann verlassen, wenn sie – in Hinblick auf einen intern nicht abstellbaren Rechtsbruch – über persönliche Wahrnehmungen berichten oder persönliche Bewertungen abgeben, die mit der „offiziellen Linie" der geprüften Stelle nicht in Einklang stehen.

Beispiel 6: Das Rechnungsprüfungsorgan gewinnt im Zuge einer Prüfung Anhaltspunkte dafür, dass bei einer Vergabe von Bauleistungen nicht alles „mit rechten Dingen zugegangen" ist. Es identifiziert einen Beschäftigten, dessen Bedenken „beiseite geschoben" worden waren. Dem Rechnungsprüfungsorgan gelingt es, den Beschäftigten davon zu überzeugen, nicht in den Akten dokumentierte Informationen offenzulegen, die den „Anfangsverdacht" erhärten. – Eine Beschäftigte hat Manipulationen in einem anderen Vergabeverfahren beobachtet und zunächst für sich behalten, weil Vorgesetzte in den Sachverhalt verwickelt sind. Als das Vergabeverfahren Gegenstand der Rechnungsprüfung wird, gibt sie aus eigener Initiative eine persönliche Erklärung ab, welche von ihre bemerkte Manipulationen um-

fassend offenlegt. Das Rechnungsprüfungsorgan beabsichtigt, diese Informationen im Prüfungsbericht unter Namensnennung zu verwerten. – In beiden Fällen wird das Rechnungsprüfungsorgan die „Missstandszeugen" nach Art. 13 Abs. 1 DSGVO informieren.

4.4.4.2 Informationspflicht nach Art. 14 Abs. 1 DSGVO

Da das Rechnungsprüfungsorgan die personenbezogenen Daten nicht bei der betroffenen Person erhebt, sondern von der überprüften Stelle erhält, ist Art. 14 Abs. 1 DSGVO grundsätzlich einschlägig. Allerdings kann die Anwendung der Vorschrift gemäß Art. 14 Abs. 5 Buchst. a und b Satz 1 DSGVO ausgeschlossen sein. Dort ist bestimmt:

„Die Absätze 1 bis 4 finden keine Anwendung, wenn und soweit
a) die betroffene Person bereits über die Informationen verfügt,
b) die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde; dies gilt insbesondere für die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke vorbehaltlich der in Artikel 89 Absatz 1 genannten Bedingungen und Garantien oder soweit die in Absatz 1 des vorliegenden Artikels genannte Pflicht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, […]."

Ein Ausschluss nach **Art. 14 Abs. 5 Buchst. a DSGVO** kommt in Betracht, wenn eine betroffene Person bereits bei einer Erhebung nach Art. 13 Abs. 1 DSGVO oder im Zusammenhang mit einer (sonstigen) Erlangung nach Art. 14 Abs. 1 DSGVO informiert worden ist und dabei der Fall einer Verarbeitung zu Rechnungsprüfungszwecken umfassend berücksichtigt worden ist. Datenschutzhinweise können diesen nach Vorschriften wie Art. 6 Abs. 1 BayDSG oder Art. 103 Satz 3 BayBG privilegierten Zweck (siehe Nr. 4.4.3.2 und Nr. 4.4.3.4) insbesondere dann umfassend berücksichtigen, wenn es um die Tätigkeit der eigenen Rechnungsprüfungsorgane geht (etwa: Rechnungsprüfungsausschuss, kommunales Rechnungsprüfungsamt). Zu beachten ist hier allerdings, dass betroffene Personen in manchen Fällen noch nicht über alle nötigen Informationen verfügen (Art. 14 Abs. 5 DSGVO: „soweit"). In solchen Situationen müssen die noch fehlenden Informationen „nachgeschoben" werden. Das gilt im kommunalen Bereich etwa, wenn ursprünglich zwar über den Zweck „Rechnungsprüfung" informiert wurde, nicht jedoch hinsichtlich des überörtlichen Rechnungsprüfungsorgans als potentiellem Empfänger (vgl. Art. 13 Abs. 1 Buchst. e DSGVO oder Art. 14 Abs. 1 Buchst. e DSGVO).

Ein Ausschluss nach **Art. 14 Abs. 5 Buchst. b Satz 1 DSGVO** kann insbesondere mit der Fallgruppe des unverhältnismäßigen Aufwands eingreifen. Insofern ist anhand aller Umstände des Einzelfalls eine Abwägung vorzunehmen. Regelmäßig kann dabei der Informationswert des Wissens über die konkrete Verwendung bestimmter personenbezogener Daten durch Rechnungsprüfungsorgane im Hinblick auf Regelungen wie Art. 6 Abs. 1 BayDSG oder Art. 103 Satz 3 BayBG als eher gering eingeschätzt werden. Vor dem Hintergrund gesetzlicher Regelungen wie etwa Art. 6 Abs. 1 BayDSG oder Art. 103 Satz 3 BayBG muss die betroffene Person allgemein damit rechnen, dass ihre personenbezogenen Daten im Rahmen der öffentlichen Finanzkontrolle verarbeitet werden. Dies gilt für die ohnehin nicht informationspflichtige Weitergabe durch die geprüfte Stelle (siehe

Nr. 4.4.3.2 und Nr. 4.4.3.4), aber auch für die Tätigkeit des Rechnungsprüfungsorgans. Doch sind auch Konstellationen denkbar, in welchen dem Informationsinteresse betroffener Personen eine (atypisch) hohe Bedeutung zukommt. Dies ist beispielsweise der Fall, wenn das Rechnungsprüfungsorgan den Umgang mit besonderen Kategorien personenbezogener Daten in konkreten Einzelfällen nachprüft (so bei der Kontrolle der Bedürftigkeitsprüfung in Beispiel 2 oder von Beihilfeabrechnungen), und/oder wenn eine Prüfung darauf zielt, die geprüfte Stelle zu einer Rückforderung gewährter öffentlicher Leistungen zu veranlassen. Ein gesteigertes Informationsbedürfnis kommt zudem etwa dann in Betracht, wenn ein Rechnungsprüfungsorgan im Hinblick auf das Datenschutzgrundrecht gesteigert risikoträchtige Analysemethoden einsetzt.

Ergibt die Abwägung, dass die Erfüllung der Informationspflicht für das Rechnungsprüfungsorgan unverhältnismäßig ist, so bestimmt **Art. 14 Abs. 5 Buchst. b Satz 2 DSGVO**:

„In diesen Fällen ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit".

Eine **Veröffentlichung** der danach gebotenen Informationen kommt insbesondere dann in Betracht, wenn das Rechnungsprüfungsorgan Daten über eine Vielzahl betroffener Personen verarbeitet und eine individuelle Mitteilung nicht angezeigt ist. Hier können etwa besondere Datenschutzhinweise auf der Homepage des Rechnungsprüfungsorgans für die nötige Transparenz sorgen. Zweckmäßig kann es dabei sein, Kategorien von Prüfungen zu bilden. Das gilt insbesondere dann, wenn im Falle einer Information nach Art. 13 Abs. 1 DSGVO für einzelne „Prüfungstypen" unterschiedliche Informationen zu erteilen wären.

Weitere **Schutzvorkehrungen** können etwa sein:

— **Pseudonymisierungen** von Datenbeständen, wenn es auf die genaue Kenntnis des Personenbezugs im Rahmen der Rechnungsprüfung nicht ankommt;

— eine **Minimierung der Speicherfristen**;

— das Treffen geeigneter **technischer und organisatorischer Maßnahmen**, um ein hohes Schutzniveau zu gewährleisten.

Das Rechnungsprüfungsorgan sollte jedenfalls die Abwägungsentscheidung dokumentieren, die gemäß Art. 14 Abs. 5 Buchst. b Satz 1 DSGVO zu einem Ausschluss der Informationspflicht führt.

Nicht einschlägig ist der Ausschlusstatbestand des **Art. 14 Abs. 5 Buchst. c DSGVO** im Hinblick auf die Auskunfts- und Vorlagerechte der Rechnungsprüfungsorgane (siehe Nr. 4.4.2). Art. 14 Abs. 5 Buchst. c DSGVO lautet:

„Die Absätze 1 bis 4 finden keine Anwendung, wenn und soweit
[…]
c) die Erlangung oder Offenlegung durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist oder […]."

Art. 95 BayHO sowie Art. 106 Abs. 6 GO, Art. 92 Abs. 6 LKrO und Art. 88 Abs. 6 BezO regeln zwar einen Informationsfluss von der geprüften Stelle zu den Rechnungsprüfungsorganen im Allgemeinen, nicht jedoch speziell hinsichtlich personenbezogener Daten. Vor diesem Hintergrund lässt sich nicht sagen, dass die Erlangung oder Offenlegung personenbezogener Daten „ausdrücklich geregelt" sei. Die Vorschriften verhalten sich auch nicht zu „geeignete [n] Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Personen". Soweit personenbezogene Daten Gegenstand von Auskunft oder Vorlage sind, ist die Weitergabe im Wesentlichen durch den Erforderlichkeitsmaßstab begrenzt. Damit wird lediglich das Schutzniveau der allgemeinen Verarbeitungsbefugnisse in Art. 4 Abs. 1 und Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG erreicht. Das genügt nicht, um den Ausnahmetatbestand in Art. 14 Abs. 5 Buchst. c DSGVO zu begründen.

4.4.4.3 Informationspflicht nach Art. 14 Abs. 4 DSGVO

Eine Informationspflicht des Rechnungsprüfungsorgans kann nicht auf Art. 14 Abs. 4 DSGVO gestützt werden. Das Rechnungsprüfungsorgan erlangt die Daten zum Zweck der Rechnungsprüfung und verarbeitet sie auch zu diesem Zweck weiter. Infolgedessen fehlt es bereits an der von Art. 14 Abs. 4 DSGVO vorausgesetzten Zweckänderung.

4.4.5 Fazit

Im Rahmen der Rechnungsprüfung bei bayerischen öffentlichen Stellen entstehen anlässlich der Verarbeitung personenbezogener Daten **grundsätzlich keine Informationspflichten der geprüften Stelle** nach Art. 13 und 14 DSGVO.

Das **Rechnungsprüfungsorgan** wird sich **in vielen Fällen** auf den **Ausschluss der Informationspflicht** gemäß Art. 14 Abs. 5 Buchst. b DSGVO berufen können, ist aber dazu angehalten, entsprechende Schutzmaßnahmen sowie Dokumentationspflichten einzuhalten. Voraussetzung ist freilich immer, dass die Daten nur für den Zweck der Rechnungsprüfung verarbeitet werden. Ist eine (Weiter-) Verarbeitung zu anderen Zwecken beabsichtigt, müssen neben der Zulässigkeit der Weiterverarbeitung auch wieder etwaige Informationspflichten geprüft werden.

5 Polizei und Justiz

5.1 Programm „Polizei 2020“

Das Programm „Polizei 2020“ wirft zunehmend seine Schatten voraus. Mit diesem Großprojekt soll die polizeiliche Informationstechnologie in den 2020er Jahren eine weitreichende Erneuerung und vor allem Neuordnung erfahren. Wenn sich damit wie angekündigt „die deutsche Polizeiarbeit grundlegend ändern“[25] wird, betrifft dies natürlich auch die Bayerische Polizei und darüber hinaus alle Bürgerinnen und Bürger, die in polizeilichen Dateien gespeichert sind.

Das in politischer Hinsicht federführende Bundesministerium des Innern, für Bau und Heimat (BMI) beschreibt den dort erkannten „dringenden Handlungsbedarf“ wie folgt: „Bislang basiert die Informationsarchitektur der Polizei in Deutschland auf eine Vielzahl unterschiedlicher Datentöpfe[,] die kaum miteinander verbunden sind. Eine heterogene IT-Landschaft[,] die von Eigenentwicklungen, Sonderlösungen, Schnittstellen, unterschiedlichen Dateiformaten und Erhebungsregeln geprägt ist, genügt nicht mehr den Anforderungen an eine moderne Polizeiarbeit.“

Im Kern geht es beim Programm „Polizei 2020“ darum, „eine gemeinsame, moderne und einheitliche Informationsarchitektur für die deutschen Polizeien in Bund und Ländern zu schaffen. Im Ergebnis sollen die Polizistinnen und Polizisten jederzeit und überall Zugriff auf die Informationen haben, die sie benötigen, um ihre Aufgaben zu erfüllen“, so das BMI.

Leider ist es meine Erfahrung, dass bei großen EDV-Projekten oftmals die fachlichen und technischen Anforderungen im Fokus stehen, während die rechtlichen Rahmenbedingungen und vor allem der Datenschutz nur untergeordnete Rollen spielen. Um dem vorzubeugen, bin ich frühzeitig mit dem Bayerischen Staatsministerium des Innern, für Sport und Integration in Kontakt getreten und habe mir im Landeskriminalamt den dortigen Sachstand des bayerischen Teilprojekts darlegen lassen. Selbstverständlich begleiten auch meine Kolleginnen und Kollegen in den Datenschutz-Aufsichtsbehörden der anderen Bundesländer sowie beim Bund die dort anstehenden Teilprojekte.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat sich am 16. April 2020 in einer ihrer Entschließung wie folgt geäußert:

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 16. April 2020

Polizei 2020 – Risiken sehen, Chancen nutzen!

Mit dem von der Innenministerkonferenz beschlossenen Programm Polizei 2020 besteht die Chance, bisherige datenschutzrechtliche Defizite zu beseitigen und

[25] Zitate aus https://www.bmi.bund.de/DE/themen/sicherheit/nationale-und-internationale-zusammenarbeit/polizei-2020/polizei-2020-node.html.

den Datenschutz nachhaltig zu verbessern. Die Polizeibehörden in Bund und Ländern haben einen ersten „fachlichen Bebauungsplan" für das Programm Polizei 2020 vorgelegt. Dieser benennt den Datenschutz als eines der Kernziele. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder begrüßt dies ausdrücklich. Sie vermisst aber ausreichende Vorschläge, wie das Projekt den Datenschutz stärken will. Die Konferenz fordert deshalb, die Ziele und Meilensteine des Programms auch an datenschutzrechtlichen Kernforderungen auszurichten und die Datenschutzaufsicht in diesen Prozess einzubinden.

Aus Sicht der Datenschutzbehörden sind vorrangig folgende Ziele in den Blick zu nehmen:

1. Umfassende Bestandsaufnahme

Eine Projektanalyse umfasst bislang nur Fragen der technischen Machbarkeit. Sie hat insbesondere nicht die Ergebnisse aus den zahlreichen datenschutzrechtlichen Kontrollen und Beratungen der letzten Jahre einbezogen. Dies ist in einer unabhängigen Evaluierung nachzuholen.

2. Rechtliche Leitplanken

Mit dem neuen „Datenhaus" in Polizei 2020 schaffen die Sicherheitsbehörden eine technische Grundlage für umfassende computergestützte Analysen personenbezogener Daten. Diese greifen intensiv in Grundrechte ein und sind deshalb gesetzlich und technisch zu begrenzen. Sie lediglich auf Generalklauseln zu stützen, wird dem Grundrecht auf informationelle Selbstbestimmung nicht gerecht. Die verantwortlichen Stellen müssen die gesetzlich und verfassungsrechtlich implizierten roten Linien bestimmen. Dies ist zwingend erforderlich, bevor Haushaltsmittel in großem Umfang eingesetzt werden.

3. Zwecktrennung

Verarbeiten die Sicherheitsbehörden personenbezogene Daten, muss dafür immer ein konkreter Zweck festgelegt sein. Dies ist der Kern des Datenschutzrechts. Deshalb muss das neue System präzise zwischen den verschiedenen Verarbeitungszwecken Aufgabenerfüllung, Dokumentation und Vorsorge trennen. Insbesondere dürfen für eine konkrete Aufgabe oder zur Dokumentation gespeicherte Daten nicht pauschal in einen Datenvorrat überführt werden oder als Auswerte- und Rechercheplattform genutzt werden.

4. Verbesserung der Datenqualität

Wenn die Polizeibehörden die IT-Struktur neu aufstellen, müssen sie alle Chancen nutzen: Sie müssen vorhandene Datenbestände bereinigen, unnötige Daten aussondern und die Qualität der Daten sichern. Dies gilt auch, wenn alte Daten in die neuen Systeme übertragen werden. Datenschutzkontrollen haben aufgezeigt, dass dies erforderlich ist. Beispiel ist die Falldatei Rauschgift.

5. Datenschutzspezifische Basisdienste

Mit dem Programm Polizei 2020 besteht die Chance, neue technische Grundfunktionalitäten des Datenschutzes als „Basisdienste" zu implementieren. Notwendig sind z. B. ein „Basisdienst Zwecktrennung", ein „Basisdienst Datenqualität" und ein „Basisdienst Aufsicht und Kontrolle".

Ich habe das Bayerische Staatsministerium des Innern, für Sport und Integration über diese Entschließung informiert. Darüber hinaus habe ich erklärt, dass ich die weitere Entwicklung des Programms „Polizei 2020“ innerhalb der Bayerischen Polizei kritisch, aber auch mit der Hoffnung verfolgen werde, dass die in der Entschließung angesprochenen Chancen genutzt werden.

5.2 Polizeiliche Videoüberwachung im öffentlichen Raum

Unter den Voraussetzungen von Art. 33 Polizeiaufgabengesetz (PAG) kann die Polizei unter anderem zur Gefahrenabwehr (Art. 33 Abs. 2 Nr. 1 PAG), an Kriminalitätsschwerpunkten (Art. 33 Abs. 2 Nr. 2 und 3 PAG) oder besonders gefährdeten Objekten (Art. 33 Abs. 3 PAG) offen Bild- und Tonaufnahmen oder -aufzeichnungen von Personen anfertigen.

Obwohl ich die Zweckmäßigkeit der polizeilichen Videoüberwachung nicht grundlegend in Frage stelle, habe ich die qualitative und quantitative Entwicklung polizeilicher Videoüberwachungen in den letzten Jahren aber durchaus nicht ohne Bedenken verfolgt.

Die Prüfung der Zulässigkeit polizeilicher Videoüberwachungen im öffentlichen Raum gehört daher zu meinen Kernaufgaben und ist auch immer wieder Gegenstand von Vor-Ort-Kontrollen.

So habe ich beispielsweise die polizeiliche Videoüberwachung eines Stadtfestes zum Anlass genommen, eine vierwöchige Speicherdauer von Videoaufzeichnungen in Frage zu stellen. Aufgrund der Bedingungen vor Ort und aus den zurückliegenden Erfahrungen war bekannt, dass im Nachhinein entweder gar nicht oder erfolglos auf vorhandene Aufzeichnungen zugriffen würde. Erfreulicherweise konnte ich im Austausch mit dem Bayerischen Staatsministerium des Innern, für Sport und Integration erreichen, dass die Verbände der Bayerischen Polizei dahingehend sensibilisiert wurden, bei der polizeilichen Videoüberwachung die gesetzliche zulässige Höchstspeicherdauer von zwei Monaten (Art. 33 Abs. 8 Satz 1 PAG) im Grundsatz auf maximal 21 Tage zu begrenzen.

Dass Datenschutz und effektive polizeiliche Videoüberwachung keine unvereinbaren Gegensätze sein müssen, zeigt meine folgende Prüfung:

So prüfte ich im Februar 2020 vor Ort die polizeiliche Videoüberwachung des Polizeipräsidiums Oberpfalz im Bereich der Albertstraße, Ernst-Reuter-Platz und Bahnhofstraße/Bahnhofsvorplatz in Regensburg. In Regensburg bestand seit 2010 eine Kooperationsvereinbarung der Polizei mit den Regensburger Verkehrsbetrieben anlässlich der Videoüberwachung in den genannten Bereichen. Da sich im Laufe der Zusammenarbeit zeigte, dass die von den Verkehrsbetrieben verwendeten Kameras nicht uneingeschränkt für die polizeilichen Belange brauchbar waren (so etwa in Bezug auf die Detailschärfe zur Nachtzeit), entschloss sich das Polizeipräsidium Oberpfalz, die bestehenden Videokameras zu ertüchtigen und nunmehr **als alleiniger Verantwortlicher – unter Ausschluss der Verkehrsbetriebe –** zu betreiben.

Die Neukonzeption der polizeilichen Videoüberwachung des Polizeipräsidiums Oberpfalz in den genannten Bereichen gab aus datenschutzrechtlicher Sicht nicht nur keinen Anlass zur Kritik, sondern wurde geradezu vorbildmäßig ausgestaltet.

Die Videoüberwachung der überwachten Bereiche selbst stützte sich zulässigerweise auf Art. 33 Abs. 2 Nr. 2 PAG. Wie sich aus den polizeilichen Statistiken ergab, sind die betroffenen Bereiche **Kriminalitätsschwerpunkte**, vornehmlich im Bereich der Betäubungsmittelkriminalität und damit zusammenhängender Deliktsfelder. Die vom Polizeipräsidium Oberpfalz erstellte Gefahrenprognose gab insofern keinen Anlass, an der Erforderlichkeit der Videoüberwachung zu zweifeln. Die Videoüberwachung selbst ist dabei lediglich ein Baustein in einem Gesamtkonzept zur Kriminalitätsbekämpfung in Regensburg.

Bei der konkreten Umsetzung hat das Polizeipräsidium Oberpfalz sodann eine Reihe von Maßnahmen zum Schutze der Rechte der Bürgerinnen und Bürger ergriffen, welche die Videoüberwachung in der vorliegenden Ausgestaltung als verhältnismäßig erscheinen ließen. So war zunächst sehr erfreulich, dass mit der Ertüchtigung der Videokameras keine Ausweitung des überwachten Verkehrsraums verbunden war. Tonaufnahmen werden von vornherein nicht erstellt. Auch werden nicht-öffentliche Bereiche (sog. Privatzonen) konsequent und unwiderruflich zum Schutz der Privatsphäre verpixelt. Bei Versammlungen im Sinne des Bayerischen Versammlungsgesetzes werden die Kameras deaktiviert. Hierauf wird auch auf den insgesamt 22 von allen Zufahrtswegen gut erkennbaren Hinweisschildern hingewiesen. Die Speicherdauer beträgt 14 Tage und wird mittels eines Ringspeichers automatisiert überschrieben, soweit insbesondere keine Sicherung zum Zwecke der Strafverfolgung erfolgen darf. Sie bewegt sich damit deutlich unterhalb des gesetzlich vorgesehenen Maximalrahmens von zwei Monaten (Art. 33 Abs. 8 Satz 1 PAG) und nochmals unterhalb des von mir mit dem Innenministerium vereinbarten Regelhöchstspeicherzeitraums für polizeiliche Videoüberwachungen von 21 Tagen.

Die Nutzung der Anlage selbst unterliegt einem detaillierten Rollenkonzept mit abgestuften Berechtigungen. Als besonders sinnvoll erachte ich die vorgesehene, jährliche Evaluierung der Erforderlichkeit der Videoüberwachungsanlage, in einem Jahresbericht. Dies gewährleistet eine kontinuierliche Überprüfung der gesetzlichen Voraussetzungen der offenen Videoüberwachung und ruft die Eingriffsintensität stets aufs Neue zurück ins Bewusstsein. Insgesamt gab die Umsetzung der offenen polizeilichen Videoüberwachung in Regensburg aus datenschutzrechtlicher Sicht zu keinerlei Beanstandungen Anlass. Aufgrund der Abkehr von der bisher praktizierten „Mischnutzung“ der Videoüberwachung mit den Verkehrsbetrieben entfallen von vornherein einige datenschutzrechtliche Probleme (etwa bei der Verantwortlichkeit, der Erforderlichkeit, der Datensicherheit sowie dem Zugriffskonzept). Aber auch im Übrigen hat das Polizeipräsidium Oberpfalz einen verhältnismäßigen Ansatz gewählt, der einen gelungenen Ausgleich zwischen den Sicherheitsinteressen einerseits und dem Grundrecht der Bürger auf informationelle Selbstbestimmung andererseits gewährleistet.

Positiv ist mir im Berichtszeitraum zudem die organisatorische Vorgehensweise bei einer mobilen polizeiliche Videoüberwachung zweier Musikfestivals aufgefallen, da hier der datenschutzrechtliche Grundsatz der Erforderlichkeit und das polizeiliche Interesse an einer wirksamen Gefahrenabwehr auf einen gemeinsamen Nenner gebracht wurden:

Das Polizeipräsidium Mittelfranken hatte in erster Linie den Einsatz mobiler Videotechnik zur Anfertigung von Live-Übersichtsaufnahme vorgesehen, um die polizeiliche Einsatzführung zu unterstützen. Die Aufzeichnung von Videoaufnahmen war nur für den sogenannten „Alarmfall“ vorgesehen, das heißt nur im Einzelfall aufgrund eines konkreten Gefahrenereignisses.

Während des gesamten Einsatzzeitraums kam es bei beiden Festivals nicht zu einem solchen Alarmfall, so dass keinerlei Videoaufzeichnungen angefertigt wurden. Dem stehen in vergleichbaren Fällen oft mehrere Stunden Videomaterial gegenüber, die häufig nicht oder erfolglos ausgewertet werden und deren rechtzeitige Löschung technisch sichergestellt werden muss.

5.3 Automatisierte Kennzeichenerfassung zu Zwecken der Strafverfolgung

Im Berichtszeitraum setzte ich mich erneut mit dem Thema der automatisierten Kennzeichenerfassung auseinander. Im Rahmen eines Vermisstenfalls im Raum Berlin wurde bekannt, dass im Land Brandenburg die automatisierten Kennzeichenerfassungssysteme des Öfteren auch im sogenannten Aufzeichnungsmodus zu Zwecken der Strafverfolgung genutzt wurden. Bei diesem Aufzeichnungsmodus werden die erfassten KfZ-Kennzeichen – im Unterschied zum sogenannten Fahndungsmodus – nicht nur für einen sehr kurzen Augenblick zum Zwecke eines Datenabgleichs mit zur Fahndung ausgeschriebenen Nummernschildern, sondern über einen längeren Zeitraum gespeichert.

In diesem Zusammenhang ergab eine Nachfrage beim Bayerischen Staatsministerium des Innern, für Sport und Integration, dass die in Bayern vorhandenen automatisierten Kennzeichenerfassungsanlagen lediglich in sehr seltenen Einzelfällen zu Zwecken der Strafverfolgung eingesetzt werden. Die Anlagen würden im Regelbetrieb im sogenannten Fahndungsmodus lediglich zur Gefahrenabwehr eingesetzt. Eine Aktivierung des sogenannten Aufzeichnungsmodus zu Zwecken der Strafverfolgung erfolge nur in seltenen Ausnahmefällen und habe bisher maximal über eine Zeitspanne weniger Stunden angedauert.

Gleichwohl sehe ich den Einsatz von automatisierten Kennzeichnungserfassungssystemen zu repressiven Zwecken äußerst kritisch. Insbesondere die Erfassung und Speicherung von Kennzeichen sämtlicher passierender Kraftfahrzeuge über einen längeren Zeitraum hinweg stellt einen schwerwiegenden Grundrechtseingriff dar.

Die gegen diesen Einsatz automatisierter Kennzeichenerfassungssysteme bestehenden Bedenken hat auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 6. November 2019 zum Ausdruck gebracht:

Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 6. November 2019

Keine massenhafte automatisierte Aufzeichnung von Kfz-Kennzeichen für Strafverfolgungszwecke!

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) weist auf den Missstand hin, dass seit einiger Zeit eigentlich für Zwecke der polizeilichen Gefahrenabwehr eingerichtete automatisierte Kennzeichenerfassungssysteme auch für Zwecke der Strafverfolgung eingesetzt werden. Sie erfassen dabei massenhaft und teilweise längerfristig Kfz-Daten unabhängig von der Beschuldigteneigenschaft der betroffenen Personen.

Im Rahmen der Gefahrenabwehr fahndet die Polizei auf Grundlage des jeweiligen Landespolizeigesetzes nach einzelnen Kraftfahrzeugkennzeichen. Nur im Fall einer Übereinstimmung von Kennzeichen und gesuchtem Fahrzeug kommt es zu einer Speicherung des einzelnen Kraftfahrzeugkennzeichens. Kfz-Kennzeichen, nach denen nicht polizeilich gefahndet wird, werden nach ihrer Erfassung unverzüglich gelöscht.

Demgegenüber wird im Bereich der Strafverfolgung – gestützt auf gerichtliche Beschlüsse oder staatsanwaltliche Anordnungen – nicht nur nach einzelnen Kraftfahrzeugen punktuell gefahndet. Vielmehr werden teilweise zusätzlich die Kennzeichen sämtlicher Fahrzeuge, die eine Straße mit einem Erfassungsgerät passieren, über einen längeren Zeitraum hinweg unterschiedslos erfasst und langfristig gespeichert. Als Rechtsgrundlage für solche Strafverfolgungsmaßnahmen wird in der Regel § 100h der Strafprozessordnung (StPO) herangezogen. Dieser erlaubt zwar, zur Observation beschuldigter Personen bestimmte technische Mittel einzusetzen, sofern Gegenstand der Strafverfolgung eine Straftat von erheblicher Bedeutung ist. Gegen andere Personen sind solche Maßnahmen nur ausnahmsweise zulässig. Eine umfassende Datenverarbeitung, wie sie die Aufzeichnung der Kennzeichen aller ein Erfassungsgerät passierender Kraftfahrzeuge über einen längeren Zeitraum bedeutet, führt jedoch dazu, dass sämtliche Verkehrsteilnehmende im Erfassungsbereich Ziel von Ermittlungsmaßnahmen sind und insoweit Bewegungsprofile entstehen können. Eine Ausweitung des Betroffenenkreises in dieser Größenordnung ist durch keinerlei Tatsachen begründbar und nicht zu rechtfertigen. Sie kann deshalb insbesondere nicht auf § 100h StPO gestützt werden.

Angesichts einer fehlenden Rechtsgrundlage sieht die DSK in der geschilderten exzessiven Nutzung von Kennzeichenerfassungssystemen für die Zwecke der Strafverfolgung einen Verstoß gegen das Grundgesetz und eine Verletzung der Bürgerinnen und Bürger in ihrem Recht auf informationelle Selbstbestimmung. Die DSK fordert die Polizeibehörden und Staatsanwaltschaften auf, die umfassende und unterschiedslose Erfassung, Speicherung und Auswertung von Kraftfahrzeugen durch Kennzeichenerfassungssysteme für Zwecke der Strafverfolgung zu unterlassen und die rechtswidrig gespeicherten Daten zu löschen.

Die DSK lehnt Vorschläge ab, die auf die Schaffung einer neuen Rechtsgrundlage für derartige strafprozessuale Maßnahmen abzielen. Nach verfassungsgerichtlicher Rechtsprechung stellen bereits die automatisierten Kfz-Kennzeichen-Kontrollen zur Fahndung nach Personen oder Sachen einen Eingriff von erheblichem Gewicht dar, selbst wenn die Kfz-Kennzeichen unverzüglich spurenlos gelöscht werden. Eine längerfristige Aufzeichnung sämtlicher Kennzeichen begründet demgegenüber einen deutlich schwerwiegenderen Grundrechtseingriff.

5.4 Speicherung eines Auskunftsersuchens im Integrationsverfahren der Bayerischen Polizei

Im Berichtszeitraum wandte sich eine Bürgerin mit der Bitte an mich, Speicherungen zu ihrer Person im elektronischen Vorgangsverwaltungssystem der Polizei (Integrationsverfahren der Bayerischen Polizei – IGVP) zu überprüfen. Im Jahr 2018 hatte die Bürgerin bei der bayerischen Polizei einen Antrag auf Auskunft über die zu ihrer Person gespeicherten personenbezogenen Daten gestellt. Dem auf die Auskunftserteilung folgenden Löschungsersuchen der Bürgerin hatte die Polizei mit entsprechendem Bescheid sodann teilweise stattgegeben. Um die angekündigten Löschungen zu kontrollieren, stellte die Bürgerin ein paar Monate

nach Erhalt des Bescheids einen neuerlichen Auskunftsantrag. Laut der neuen Auskunft wurden die angekündigten Löschungen tatsächlich durchgeführt, jedoch fiel der Bürgerin auf, dass im IGVP nunmehr eine Eintragung „Auskunftsersuchen aus dem Jahr 2018“ existierte. Die Bürgerin befürchtete, nun allein wegen der Inanspruchnahme ihres gesetzlich normierten Auskunftsrechts nach Art. 65 Polizeiaufgabengesetz und ihres daran anknüpfenden Löschungsantrags eine weitere elektronische Speicherung im IGVP ausgelöst zu haben.

Meine daraufhin vorgenommene Prüfung bei der Polizei bestätigte diese Befürchtung. Ich teilte sodann sowohl dem zentral für Auskünfte und Löschungen zuständigen Bayerischen Landeskriminalamt als auch dem betreffenden Polizeipräsidium mit, dass eine derartige Speicherpraxis in datenschutzrechtlicher Hinsicht nicht hinnehmbar sei. Das Recht auf informationelle Selbstbestimmung von Personen, die dieses Recht mit einem Auskunfts-/Löschungsantrag aktiv in Anspruch nehmen, würde mit einer solchen polizeilichen Verfahrensweise ad absurdum geführt. Das Bayerische Landeskriminalamt bestätigte mir, dass diese Speicherungspraxis nicht der internen Regelungslage entspräche. Danach sind Auskunfts- und Löschungsanträge nicht im für viele Polizeibeamtinnen und Polizeibeamte elektronisch zugänglichen IGVP zu speichern, sondern nur nach dem Aktenplan der Bayerischen Polizei zu erfassen. Hierdurch ist der Zugriff auf die Information, dass eine Bürgerin oder ein Bürger einen Auskunfts- und/oder Löschantrag gestellt hat, stark eingeschränkt.

Ich konnte erreichen, dass die betroffene Polizeidienststelle vergleichbare Falscherfassungen recherchierte und sofort löschte. Meine Hinweise wurden außerdem zum Anlass genommen, die Sachbearbeiterinnen und Sachbearbeiter für die Zukunft entsprechend zu sensibilisieren.

5.5 Auswirkungen der sogenannten „Mitziehklausel“

Als eine meiner Kernaufgaben verstehe ich die Überprüfung von Datenspeicherungen bei der Bayerischen Polizei. Regelmäßig wenden sich Bürgerinnen und Bürger mit zahlreichen Fragen zu diesem Thema an mich. Neben umfangreichen Informationen auf meiner Homepage unter https://www.datenschutz-bayern.de nutze ich meinen Tätigkeitsbericht, um Beispiele zu dem komplexen Bereich der Speicherung von personenbezogenen Daten in polizeilichen Dateien darzustellen.

Art. 54 Abs. 2 Polizeiaufgabengesetz (PAG) gibt den Rahmen für die Dauer einer polizeilichen Speicherung vor. Die dort genannten „Prüfungstermine“ sind von verschiedenen Faktoren abhängig und gelten nicht absolut. Beispielsweise sind für Erwachsene andere Regelfristen vorgesehen als für Kinder und Jugendliche, auch kann es wegen der Schwere oder der Geringfügigkeit der jeweiligen Tat entweder Verlängerungen oder Verkürzungen der Speicherdauer geben.

Für die betroffenen Personen besonders nachteilig kann es sich auswirken, wenn mehr als ein Delikt im Kriminalaktennachweis (KAN) der Polizei gespeichert ist. In diesen Fällen wirkt sich die sogenannte „Mitziehklausel“ des Art. 54 Abs. 2 Satz 6 PAG aus, die oftmals zu einer erheblichen Verlängerung aller vorhandenen Speicherungen führt:

„Werden innerhalb der Frist [...] 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.“

Ich habe den Automatismus solcher „Mitziehungen“ bereits mehrfach kritisiert, zum Beispiel in meinem 28. Tätigkeitsbericht unter Nr. 4.4.3. Durch die Regelung des Art. 54 Abs. 2 Satz 6 PAG können etwa lange zurückliegende Verfehlungen von Jugendlichen oder Heranwachsenden zum Teil über Jahrzehnte gespeichert werden. Dies kann, insbesondere wenn es um die Speicherung von (auch geringfügigen) Drogendelikten geht, erhebliche Unannehmlichkeiten für betroffene Personen haben, beispielsweise im Rahmen von polizeilichen Kontrollen. Bürgerinnen und Bürger berichten mir regelmäßig, dass sie im Rahmen von Fahrzeugkontrollen immer noch Durchsuchungen ihrer Person und ihres Wagens über sich ergehen lassen müssen, obwohl das zugrunde liegende Delikt bereits 15 Jahre oder länger zurückliegt und sich ihre Lebensumstände erheblich verändert haben.

Vor diesem Hintergrund ist es, wenn mehrere KAN-Einträge vorliegen, wichtig, sich die jüngsten Speicherungen besonders genau anzusehen, wie die folgenden zwei Fälle zeigen:

Im ersten Fall ging es um einen geringfügigen Verstoß nach dem Betäubungsmittelgesetz, weil gegen die betroffene Person im Jahr 2002 wegen des Besitzes einer geringen Menge Cannabis ermittelt wurde. Weitere Ermittlungen folgten im Jahr 2009 wegen einer Körperverletzung und im Jahr 2019 wegen einer Beleidigung.

Wegen der Folgespeicherungen in den Jahren 2009 und 2019 wurde das Drogendelikt nie ausgesondert, sondern im Datenbestand des Kriminalaktennachweises immer wieder verlängert, also „mitgezogen“. Im konkreten Fall hätte dies eine Gesamtspeicherdauer von mehr als zwei Jahrzenten für ein einmaliges geringfügiges Vergehen wegen des Besitzes von Cannabis bedeutet, obwohl das zuständige Strafgericht im Jahr 2002 von einer Verfolgung der Tat abgesehen hatte.

Gegenüber der geringen Bedeutung, die diesem Fall seitens der Justiz beigemessen wurde, erschien mir eine polizeilich vorgesehene Speicherdauer von mehr als 20 Jahren unverhältnismäßig und mit dem Prinzip der Speicherbegrenzung (Art. 66 PAG in Verbindung mit Art. 28 Abs. 2 Satz 1 Nr. 2 BayDSG und Art. 5 Abs. 1 Satz 1, Buchst. e DSGVO) nicht vereinbar. Vor allem war für mich nicht ersichtlich, welchen Nutzen diese Speicherung für die polizeiliche Gefahrenabwehr nach so langer Zeit noch haben sollte, obwohl die betroffene Person nie wieder wegen eines Drogendelikts auffällig geworden war.

Ich habe daher das Bayerische Landeskriminalamt (BLKA) gebeten, die Dauer dieser Speicherung auf das erforderliche Maß zu beschränken. Im Ergebnis möchte ich positiv hervorheben, dass das BLKA eine Löschung der betreffenden Speicherung aus dem Kriminalaktennachweis durchsetzte, obwohl die ursprünglich ermittelnde und speichernde Polizeidienststelle eine Aussonderung immer noch als „problematisch“ erachtete.

Der zweite Fall betraf einen Petenten, der im Zeitraum von 1995 bis 2003 als Serientäter in mehreren Dutzend Fällen polizeilich auffällig war und letztlich auch mehrmals inhaftiert wurde. Seine zahlreichen Speicherungen im Kriminalaktennachweis, darunter vorrangig Eigentumsdelikte, waren zum damaligen Zeitpunkt sicherlich vertretbar.

Nach seiner letzten Haftentlassung wurde es polizeilich ruhiger um den Petenten. Er veränderte sich wohl und trat bis 2007 nur noch sporadisch in Erscheinung. In der Überzeugung, die „schiefe Bahn“ vor mehr als zehn Jahren verlassen zu haben,

stellte er schließlich gemäß Art. 65 PAG einen Auskunftsantrag bei der Polizei. Als er immer noch mit einer Vielzahl von Speicherungen ab Mitte der 1990er Jahre konfrontiert wurde, wandte er sich, ohne seine lange zurückliegenden Taten zu relativieren, an mich und bat um eine Überprüfung der Speicherungen.

In der von der Polizei erteilten Auskunft fiel sofort der „neueste" Eintrag, eine einzelne Speicherung aus dem Jahr 2012 wegen Betrugs und Unterschlagung, auf, die aufgrund der „Mitziehklausel" für die Aufrechterhaltung aller früheren Speicherungen sorgte. Der Petent verwies hierzu auf ein Missverständnis im Rahmen eines Beziehungsstreits und die Einstellung des Verfahrens nach § 170 Abs. 2 Strafprozessordnung (StPO). Auf meine Nachfrage zur Erforderlichkeit dieser einzelnen Speicherung wurde mir von der Polizei mitgeteilt, dass diese nicht mehr bejaht werde und eine Löschung dieses Eintrags im Kriminalaktennachweis erfolgt sei. Da man damit das für die Anwendung der „Mitziehklausel" entscheidende Delikt gelöscht hatte und alle früheren Ermittlungen mehr als zehn Jahre zurücklagen, führte dies schließlich zur vollständigen Löschung der gesamten Speicherungen im Kriminalaktennachweis.

5.6 Prüfung der Vergabe des ermittlungsunterstützenden Hinweises „Reisender Täter"

Im Informationssystem der Polizei (INPOL) besteht nach § 16 Abs. 6 Nr. 2 des **Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten** (Bundeskriminalamtgesetz – BKAG) die Möglichkeit, sogenannte ermittlungsunterstützende Hinweise (EHW) einzutragen. Die Polizei versteht hierunter im Wesentlichen Hinweise auf Besonderheiten einer natürlichen Person, die dazu geeignet sind, polizeiliches Handeln zielgerichteter zu steuern oder zu unterstützen. Um dieser Aufgabe gerecht zu werden, werden EHW auf Basis bestimmter Vergabekriterien entsprechend einem bundeseinheitlichen Leitfaden (EHW-Leitfaden) dokumentiert. Als EHW können nach den entsprechenden Kriterien im Zusammenhang mit einer Person zum Beispiel die Begriffe „Intensivtäter", „BtM-Handel", „Sexualtäter" oder „Reisender Täter" gespeichert werden.

Generell stehe ich den EHW kritisch gegenüber, weil die Vergabekriterien teilweise zu unbestimmt sind und ich die Gefahr einer Stigmatisierung der betroffenen Personen sehe. Aus diesem Grund habe ich deshalb die Vergabe des EHW „Reisender Täter" im Zuständigkeitsbereich eines Polizeipräsidiums geprüft. Nach entsprechender Vorauswahl und Anforderung legte mir das Polizeipräsidium vollständige INPOL-Auszüge zu mehreren Personen vor, für welche der EHW „Reisender Täter" eingetragen worden war. Ich habe diese im Hinblick auf ihre Vereinbarkeit mit den polizeilichen Vergabekriterien überprüft.

In etwa einem Drittel der vorgelegten Fälle habe ich das Polizeipräsidium um ergänzende Begründung der Vergabe des EHW „Reisender Täter" gebeten, da ich diese nicht ohne weiteres nachvollziehen konnte. Auf meine Nachfrage hin, wurden die Fälle von der Polizei sodann nochmals überprüft und bei der Hälfte dieser Fälle wurde der EHW erfreulicherweise sofort gelöscht.

Die vorgenommenen Stichproben haben gezeigt, dass der EHW „Reisender Täter" vielfach gespeichert wurde, obwohl die von der Polizei selbst festgelegten Kriterien nicht vorlagen.

Das betroffene Polizeipräsidium, das sich sehr kooperativ an der Prüfung beteiligte, habe ich daher gebeten, zukünftig mehr auf die Einhaltung der im EHW-Leitfaden festgesetzten Kriterien zu achten und die nachgeordneten Bereiche entsprechend zu sensibilisieren.

5.7 Präventive DNA-Speicherung durch die Polizei

Am 18. Mai 2018 hat der bayerische Gesetzgeber das Gesetz zur Neuordnung des bayerischen Polizeirechts (PAG-Neuordnungsgesetz) verabschiedet. Das Gesetz soll ausweislich der Gesetzesbegründung die Richtlinie (EU) 2016/680 umsetzen und die verfassungsrechtlichen Maßgaben aus der Entscheidung des Bundesverfassungsgerichts zum Bundeskriminalamtgesetz berücksichtigen. Zudem bedurfte es nach Einschätzung des Gesetzgebers „einer weiteren, dem Stand der Technik entsprechenden Ergänzung und noch effektiveren Ausgestaltung wichtiger polizeilicher Befugnisnormen."[26] Insoweit sieht das Polizeiaufgabengesetz (PAG) unter anderem erstmals die Durchführung molekulargenetischer Untersuchungen zur Feststellung von DNA-Identifizierungsmustern im Rahmen der erkennungsdienstlichen Maßnahmen (Art. 14 Abs. 3, 4 PAG) vor.

Art. 14 Abs. 3 und 4 PAG lauten:

„(3) [1]Die Polizei kann dem Betroffenen zudem Körperzellen entnehmen und diese zur Feststellung des DNA-Identifizierungsmusters molekulargenetisch untersuchen, wenn dies zur Abwehr einer Gefahr für ein bedeutendes Rechtsgut erforderlich ist und andere erkennungsdienstliche Maßnahmen nicht hinreichend sind. [2]Ein körperlicher Eingriff darf dabei nur von einem Arzt vorgenommen werden. [3]Die entnommenen Körperzellen sind unverzüglich nach der Untersuchung zu vernichten, soweit sie nicht nach anderen Rechtsvorschriften aufbewahrt werden dürfen. [4]Eine Maßnahme nach Satz 1 darf nur durch den Richter angeordnet werden, bei Gefahr im Verzug auch durch die in Art. 36 Abs. 4 Satz 2 und 3 genannten Personen.
(4) [1]Die molekulargenetische Untersuchung darf sich allein auf das DNA-Identifizierungsmuster erstrecken. [2]Anderweitige Untersuchungen oder anderweitige Feststellungen sind unzulässig."

Neben der vom Ministerrat mit Beschluss vom 12. Juni 2018 beauftragten Kommission zur unabhängigen Begleitung und Prüfung der Anwendung des Polizeiaufgabengesetzes (PAG-Kommission) habe ich den Vollzug der neu eingeführten Befugnis des Art. 14 Abs. 3 und 4 PAG ebenfalls – und über den Berichtszeitraum der PAG-Kommission hinaus – geprüft.

Insgesamt wurden mir auf meine Anfrage durch die Polizeipräsidien neben den neun Fällen, die bereits im Abschlussbericht der PAG-Kommission vom 30. August 2019 beschrieben sind, weitere vier Fälle aus dem präventivpolizeilichen Anwendungsbereich mitgeteilt. In insgesamt elf der 13 Fälle stützte die Polizei die Befugnis zur Entnahme der DNA auf eine Freiwilligkeits-/Einverständniserklärung. Die betreffenden Körperzellen wurden in allen 13 Fällen nach Übersendung an das Bayerische Landeskriminalamt und dortiger Auswertung vernichtet. Alle Polizeiverbände wiesen einstimmig darauf hin, dass Art. 14 Abs. 5 PAG keine feste Speicherdauer vorsehe, weswegen die verantwortlichen Polizeidienststellen je-

26 Landtags-Drucksache 17/20425, S. 1.

weils eine Einzelfallprüfung in Bezug auf eine etwaige Löschung betreffender Daten durchzuführen hätten, sobald die Voraussetzungen des Art. 14 Abs. 3 PAG nicht mehr vorlägen. Lediglich im Falle der präventiven DNA-Entnahme einer jugendlichen Ausreißerin wurde mir vom zuständigen Polizeipräsidium als Löschzeitpunkt die Vollendung des 18. Lebensjahres benannt.

Ausweislich der Gesetzesbegründung soll die Befugnis des Art. 14 Abs. 3 PAG das erkennungsdienstliche Instrumentarium ergänzen, wobei davon ausgegangen wurde, dass es sich dabei „nicht um ein regelhaftes präventiv-erkennungsdienstliches Instrument“[27] handele. Gerade bei Personen, „von denen ein erhebliches Gefährdungspotential“ ausgehe, könne eine entsprechende Befugnis aber zur sicheren, nachhaltigen Identifizierbarkeit erforderlich sein. Aufgrund der erhöhten Sanktionswahrscheinlichkeit könne hierdurch auch eine Spezialprävention erreicht werden. Wegen der Grundrechtsrelevanz der mit Art. 14 Abs. 3 PAG verbundenen Eingriffe sei aber eine ausdrückliche – unter Richtervorbehalt stehende – Regelung geboten.[28]

Nach meiner Einschätzung steht die bei meiner Prüfung festgestellte Vollzugspraxis hiermit nicht in Einklang:

So umgeht die überwiegend geübte Praxis des Rückgriffs auf Freiwilligkeitserklärungen den in Art. 14 Abs. 3 Satz 4 PAG geregelten Richtervorbehalt. Sie widerspricht zudem Erwägungsgrund 35 RLDSJ. Danach können die zuständigen Behörden bei der Wahrnehmung der ihnen übertragenen Aufgaben, Straftaten zu verhüten, zwar natürliche Personen auffordern oder anweisen, ihren Anordnungen nachzukommen. Kommt die betroffene Person dieser Anweisung nach, stellt eine solche Einwilligung aber keine rechtliche Grundlage für die Verarbeitung personenbezogener Daten dar. Denn wenn eine betroffene Person aufgefordert wird, einer rechtlichen Verpflichtung nachzukommen, hat sie keine echte Wahlfreiheit, weshalb ihre Reaktion nicht als freiwillig abgegebene Willensbekundung betrachtet werden kann.

Ich habe gegenüber dem Bayerischen Staatsministerium des Innern, für Sport und Integration daher folgende durch die PAG-Kommission bereits gestellte Forderung wiederholt: Zumindest in einer Vollzugsbekanntmachung muss klargestellt werden, dass der Richtervorbehalt nach Art. 14 Abs. 3 Satz 4 PAG nicht durch die Einholung eines wie auch immer gearteten Einverständnisses ersetzt werden darf.

Auch was die Erfüllung der materiellen Voraussetzungen des Art. 14 Abs. 3 PAG anbelangt, erscheinen die bekannten Anwendungsfälle zumindest als diskussionswürdig. So wiesen bei den von der PAG-Kommission geschilderten neun Fällen lediglich „zwei Fallkonstellationen ein hohe Plausibilität für die Rechtmäßigkeit auf. […] Alle anderen […] Fälle werfen durchaus berechtigte Zweifel auf.“ Zur näheren Begründung möchte ich auf die Einschätzung der PAG-Kommission verweisen.[29] Auch hier habe ich das Innenministerium aufgefordert, zumindest in einer Vollzugsbekanntmachung klarzustellen, dass es sich bei der DNA-Entnahme nach Art. 14 Abs. 3 PAG gerade nicht um ein regelhaftes präventiv-erkennungsdienstliches Instrument handelt und auf die Verhältnismäßigkeit der Maßnahme daher besonders zu achten ist. Auch sollte stärkeres Augenmerk auf die Tatsache gerichtet werden, dass eine präventive DNA-Entnahme nur bei Vorliegen einer

27 Landtags-Drucksache 17/20425, S. 41.
28 Landtags-Drucksache 17/20425, S. 41.
29 PAG-Kommission, Abschlussbericht, 2019, S. 41 f., Internet: https://www.pag.bayern.de.

konkreten Gefahr zulässig ist. Diese Voraussetzung darf nicht durch eine überdehnte Wahrscheinlichkeitsbetrachtung unterlaufen werden.

Ich hatte bereits bei der Beteiligung im Rahmen des PAG-Neuordnungsgesetzes des bayerischen Polizeirechts (erfolglos) darauf hingewiesen, dass angesichts des mit der molekulargenetischen Untersuchung einhergehenden erheblichen Eingriffs in das Recht auf informationelle Selbstbestimmung sowie der präventiven Natur der Maßnahme eine Regelung zur Speicherdauer erforderlich ist. Aufgrund meiner oben geschilderten Feststellungen zur Speicherdauer habe ich das Innenministerium gefragt, wie sichergestellt wird, dass eine regelmäßige Überprüfung der Speicherungsvoraussetzung stattfindet und ob entsprechende Aussonderungsprüffristen existieren. Hierauf wurde mir mitgeteilt, dass derzeit mindestens jährlich geprüft werde, ob die Speicherung eines DNA-Musters aufrechterhalten werden muss. Auch hier sollte zumindest im Rahmen einer Vollzugsbekanntmachung Rechtssicherheit geschaffen werden.

Zwischenzeitlich wurden unter anderem auch die Ergebnisse der PAG-Kommission zum Anlass genommen, eine Änderung des Polizeiaufgabengesetzes herbeizuführen. Nach Abschluss meiner Prüfung erreichte mich der Entwurf eines Gesetzes zur Änderung des Polizeiaufgabengesetzes (PAG-Änderungsgesetz). Im Rahmen dieses Gesetzgebungsverfahren habe ich, auch aufgrund der oben geschilderten Prüfungsergebnisse, dem Innenministerium dringend empfohlen, die Befugnis für eine Entnahme von Körperzellen zur Feststellung des DNA-Identifizierungsmusters in Art. 14 Abs. 3 PAG ersatzlos zu streichen.

5.8 Unzulässige Datenübermittlung mittels Strafzettel

Die Anlässe für polizeiliche Datenübermittlungen sind vielfältig. Solche Datenweitergaben können auf verschiedenen Rechtsgrundlagen beruhen, auf unterschiedlichen Wegen vonstattengehen und haben dennoch immer eines gemeinsam: Sie sind eine sensible Angelegenheit, sollten nicht unbedacht vorgenommen werden und sind stets am Grundsatz der Erforderlichkeit zu beurteilen.

In einem von mir zu prüfenden Fall wandte sich ein Hotelangestellter an mich. Er hatte die Polizei über ein verbotswidrig in der Hotelzufahrt abgestelltes Fahrzeug informiert. Die verständigte Streifenbesatzung fuhr zum Einsatzort, stellte eine Verkehrsordnungswidrigkeit fest und hinterließ am Wagen des Falschparkers einen sogenannten Strafzettel (Verwarnung mit Zahlungsaufforderung). Kurz nachdem der Hotelangestellte seine Schicht beendet hatte, erschien der Fahrzeugführer im Hotel, nannte den Namen des Hotelangestellten und wollte diesen zur Rede stellen.

Wie sich zeigte, hatte die Streifenbesatzung der Polizei den Namen des Hotelangestellten als „Mitteiler“ in das Formularfeld „Tatbestandskonkretisierung“ des Strafzettels eingetragen. Dies hatte zur Folge, dass der Name auf dem rosafarbenen Durchschlag des Strafzettels, der wie üblich an der Windschutzscheibe des Fahrzeugs angebracht wurde, ebenfalls zu lesen war. Insofern fand hier eine – wenn auch etwas ungewöhnliche und wohl auch unbeabsichtigte – Datenübermittlung statt. Diese Datenübermittlung war unzulässig. Der Datenfluss zum Betroffen ist durch § 56 OWiG und die Richtlinie für die Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten, hier Anlage 2, geregelt. Der Name des Mitteilers wird dabei nicht offengelegt.

Das betroffene Polizeipräsidium räumte auf meine Anfrage hin ein, dass die namentliche Nennung des Mitteilers auf dem Strafzettel in datenschutzrechtlicher Hinsicht nicht zulässig war. Insbesondere war den Polizeibeamten durch eine eigene Inaugenscheinnahme der Situation vor Ort möglich, die Verkehrsbehinderung wahrzunehmen, selbst zu bewerten und letztendlich zu ahnden. Es war zwar in Ordnung, dass die Polizeibeamten den Namen des Hotelangestellten als Mitteiler und Zeugen erhoben hatten, um gegebenenfalls in einem späteren gerichtlichen Verfahren auf diesen zurückzukommen zu können. Dieses Verfahrensstadium war aber noch nicht erreicht.

Positiv hervorzuheben ist in diesem Fall, dass der Vorfall von der Polizei sorgfältig aufgearbeitet und auch in Dienstunterrichten erörtert wurde, um die Einsatzkräfte zu sensibilisieren und entsprechende Wiederholungen zu vermeiden.

5.9 Zugangskontrolle bei Gerichten

Bereits in meinem 26. Tätigkeitsbericht 2014 unter Nr. 5.2.2 beschäftigte ich mich mit Zugangskontrollen bei Gerichten. Auch im Berichtszeitraum hat mich eine Beschwerde zu diesem Thema erreicht.

An den Eingängen von Dienstgebäuden der ordentlichen Gerichtsbarkeit wie auch der Fachgerichtsbarkeiten werden regelmäßig allgemeine Zugangskontrollen durchgeführt. Diese Zugangskontrollen beruhen nach gefestigter Rechtsprechung auf dem Hausrecht des jeweiligen Gerichtsvorstands. Das Hausrecht gestattet zur Gewährleistung eines ordnungsgemäßen Dienstbetriebes Maßnahmen zur Aufrechterhaltung der Sicherheit und Ordnung im Gerichtsgebäude, wie beispielsweise die Anordnung, einen Metalldetektorrahmen zu passieren sowie damit verbundene Begleitanordnungen. Die Maßnahmen müssen dem Verhältnismäßigkeitsgebot genügen.

Die Maßnahmen, die im Rahmen der Zugangskontrolle auf der Grundlage des Hausrechts getroffen wurden, waren im konkreten Fall datenschutzrechtlich nicht zu beanstanden. Es stellte sich jedoch heraus, dass das Gericht für den Fall, dass bei einem Betreten des Gebäudes nicht erlaubte Gegenstände beim Sicherheitsdienst zu hinterlegen waren, vorsah, die Personalien der betroffenen Person zu erheben und im Wachbuch des kontrollierenden Sicherheitsdienstes aufzuzeichnen. Dies geschah, obwohl der betroffenen Person zudem eine Nummernkarte ausgegeben wurde, die sich auf eine Kiste mit entsprechender Nummer mit dem zu hinterlegenden Gegenstand bezog. Diese Nummer wurde ebenfalls zu den erhobenen Personalien notiert. Bei Verlassen des Gebäudes konnte die betroffene Person die Nummernkarte abgeben und unter zusätzlicher Angabe der Personalien den hinterlegten Gegenstand wieder herausverlangen.

In diesem Zusammenhang habe ich es für kritisch erachtet, dass trotz Ausgabe der Nummernkarte noch ergänzend eine Erhebung der Personalien und eine Eintragung dieser Daten in die Wachbücher des Sicherheitsdienstes erfolgte. Da die Erhebung dieser Daten nicht zur Aufgabenerfüllung erforderlich war, waren die Voraussetzungen des Art. 4 Abs. 1 BayDSG nicht erfüllt. Meine Bedenken habe ich dem betroffenen Gericht mitgeteilt, worauf das Gericht entschied, auf die Erhebung und Eintragung der Personalien in die Wachbücher des Sicherheitsdienstes künftig zu verzichten. Man werde die hinterlegten Gegenstände allein nach Vorzeigen und Abgabe der entsprechenden Nummernkarte wieder herausgeben, ohne sich mittels Personalien zusätzlich legitimieren zu müssen.

Die neu gewonnene Haltung des betroffenen Gerichts begrüße ich ausdrücklich, weil sie datensparsamer ist und somit den datenschutzrechtlichen Belangen der betroffenen Personen nunmehr in höherem Maße gerecht wird.

6 Allgemeine Innere Verwaltung

6.1 Factoring bei ÖPNV-Leistungen durch Stadtwerke

Die moderne Verwaltung greift bei der Erfüllung ihrer öffentlichen Aufgaben immer häufiger auf (rechtliche) Instrumente der Privatwirtschaft zurück. Eines dieser Instrumente ist das Factoring. Hierbei verkauft der Gläubiger eine (künftige) Forderung gegenüber seinem Schuldner an einen Finanzdienstleister, den Factor. Für den Gläubiger hat dies zwei wesentliche Vorteile: eine Verbesserung der Liquidität durch schnelle Realisierung der Forderung bei gleichzeitiger Entledigung vom Forderungsinkasso. Trägt der Factor das wirtschaftliche Ausfallrisiko der Forderung, so spricht man von einem echten Factoring. Allerdings müssen öffentliche Stellen die für sie geltenden Vorgaben des Datenschutzrechts auch dann beachten, wenn sie von Gestaltungsmöglichkeiten Gebrauch machen, die im Zivilrecht bereits seit langem anerkannt sind. Speziell in Bezug auf ein echtes Factoring beim Online-Ticketverkauf durch in Rechtsform einer privatrechtlichen GmbH organisierte Stadtwerke für den Öffentlichen Personennahverkehr (ÖPNV) habe ich dies im Berichtszeitraum überprüft.

Meiner Prüfung lag im Wesentlichen folgender Sachverhalt zugrunde: Wenn eine Kundin oder ein Kunde in der entsprechenden Mobile App der Stadtwerke elektronisch ein ÖPNV-Ticket kaufen will und durch Auswahl des gewünschten Tickets ein Angebot zum Abschuss eines Kaufvertrags abgibt, fragen die Stadtwerke zunächst beim Zahlungsdienstleister an, ob dieser bereit ist, die (potenzielle) Forderung aufzukaufen. In diesem Rahmen werden personenbezogene Daten der (potentiellen) Kundin oder des (potentiellen) Kunden an den Zahlungsdienstleister übermittelt. Der Zahlungsdienstleister führt sodann anhand dieser Daten eine Bonitätsprüfung durch. Bei positiver Prüfung übermittelt der Zahlungsdienstleister an die Stadtwerke eine Zusage, dass er die Forderung kaufen werde. Entsprechendes gilt bei einer Kaufablehnung. Nur im positiven Fall nehmen die Stadtwerke das Kundenangebot an und schließen den elektronischen Ticketkauf ab. Die hierbei entstehende Forderung wird dann von den Stadtwerken an den Zahlungsdienstleister abgetreten. Andernfalls lehnen die Stadtwerke das Kundenangebot ab und der Online-Kauf scheitert. Datenschutzrechtlich habe ich dies wie folgt bewertet:

6.1.1 Keine Auftragsverarbeitung

Die Datenumgänge zwischen den Stadtwerken und dem Zahlungsdienstleister im Rahmen des Factorings sind schon mangels Weisungsgebundenheit des Factors keine Verarbeitung im Auftrag gemäß Art. 4 Nr. 8, Art. 28 DSGVO. Vielmehr handeln beide jeweils als eigene Verantwortliche gemäß Art. 4 Nr. 7 DSGVO.

6.1.2 Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO als Rechtsgrundlage

Rechtliche Konsequenz der Ablehnung einer Auftragsverarbeitung ist, dass die Stadtwerke als öffentliche Stelle gemäß Art. 1 Abs. 2 BayDSG (Gesellschafter waren im konkreten Fall mehrere öffentliche Stellen nach Art. 1 Abs. 1 BayDSG, und

der ÖPNV ist eine Aufgabe der öffentlichen Verwaltung nach Art. 1 Abs. 2 Satz 1 BayDSG) für die beschriebenen Datenumgänge eine Rechtsgrundlage benötigen. Hierbei konnten sich die Stadtwerke erfolgreich auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO in Verbindung mit Art. 1 Abs. 3 BayDSG stützen. Im Einzelnen:

Zwar unterfallen die Stadtwerke grundsätzlich dem Ausschlusstatbestand des Art. 6 Abs. 1 UAbs. 2 DSGVO. Danach gilt Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO nicht für Behörden, wenn diese Daten in Erfüllung ihrer Aufgaben verarbeiten, wobei nach meiner derzeitigen Rechtsauffassung auch öffentliche Stellen nach Art. 1 Abs. 2 BayDSG Behörden im Sinne des Art. 6 Abs. 1 UAbs. 2 DSGVO sind.

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

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

Gleichwohl konnten sich hier die Stadtwerke erfolgreich auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO berufen. Denn beim ÖPNV liegt eine Wettbewerbsteilnahme im Sinne des Art. 1 Abs. 3 BayDSG vor. Dies erstreckt sich kraft Sachzusammenhangs auch auf den Vertragsabschluss und die Geltendmachung entsprechender Forderungen. Mithin sind für diese Datenverarbeitungen die Vorschriften für nicht-öffentliche Stellen anzuwenden, also auch Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO.

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 nicht öffentliche Stellen. [2]Die Zuständigkeit des Landesbeauftragten für den Datenschutz (Landesbeauftragter) nach Art. 15 bleibt hiervon unberührt.
[…]

Das erforderliche berechtigte Interesse der Stadtwerke bestand in der Auslagerung des Forderungsmanagements. Die Übertragung personenbezogener Daten potentieller Kundinnen und Kunden an den Factor und die Entgegennahme der positiven oder negativen Information des Factors (Zusage oder Ablehnung des

Ankaufs der zukünftigen Forderung) sind auch erforderlich, um den Forderungsverkauf zu erfüllen. Der Factor wiederum benötigt die personenbezogenen Daten seiner potentiellen Schuldner, um deren Bonität zu prüfen.

6.1.3 Informationen nach Art. 13 und Art. 14 DSGVO

Art. 13 DSGVO verpflichtet den Verantwortlichen dazu, betroffenen Personen verschiedene Informationen zur Datenverarbeitung zu geben, sobald der Verantwortliche personenbezogene Daten erhebt. Art. 14 DSGVO sieht eine solche Informationspflicht vor, wenn der Verantwortliche die Daten nicht bei den betroffenen Personen, sondern bei Dritten erhebt. Diese Informationen sind in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln (Art. 12 Abs. 1 DSGVO).

Beim oben beschriebenen Factoring unterfallen die Stadtwerke zum einen der Informationspflicht nach Art. 13 Abs. 1 und 2 DSGVO, wenn sie personenbezogene Daten der (potentiellen) Kundin oder des (potentiellen) Kunden im Rahmen der Entgegennahme von deren oder dessen Angebot eines Online-Ticketkaufs erheben. Zum anderen müssen die Stadtwerke der (potentiellen) Kundin oder dem (potentiellen) Kunden auch die Informationen nach Art. 14 Abs. 1 DSGVO geben, wenn sie Daten vom potentiellen Factor als Dritten erheben. Da sich die Informationen für beide Erhebungsvorgänge inhaltlich überschneiden, genügt insoweit eine einmalige Information (vgl. Art. 13 Abs. 4 beziehungsweise Art. 14 Abs. 5 Buchst. a DSGVO).

Beim Factoring erhebt auch der Zahlungsdienstleister personenbezogene Daten der (potentiellen) Kundinnen und Kunden. Da jedoch im Stadium der Vertragsanbahnung nur die Stadtwerke, nicht aber der Zahlungsdienstleister unmittelbaren Kontakt mit den betroffenen (potentiellen) Kundinnen und Kunden haben, hatte der Zahlungsdienstleister die Stadtwerke verpflichtet, entsprechende Informationen des Zahlungsdienstleisters gleichsam als dessen Bote zur Verfügung zu stellen. Auch wenn die Erfüllung der Informationspflichten des Zahlungsdienstleisters von mir mangels Zuständigkeit nicht unmittelbar zu bewerten ist, erwarte ich doch von öffentlichen Stellen, dass diese bei der Wahl ihrer Vertragspartner darauf achten, dass diese Partner die Vorgaben des Datenschutzes – darunter fallen auch die Informationspflichten nach Art. 13 f. DSGVO – einhalten.

6.1.4 Automatisierte Entscheidungsfindung/besondere Transparenzanforderungen

Greifen öffentliche Stellen im Rahmen des Art. 1 Abs. 3 BayDSG auf rechtliche Instrumente wie das Factoring zurück, so haben sie besonderes Augenmerk auf die Sicherstellung einer hinreichenden Transparenz gemäß Art. 5 Abs. 1 Buchst. a DSGVO zu richten. Da derartige zivilrechtliche Instrumente wohl noch nicht zum „Standard-Kanon“ verwaltungsüblicher Handlungsformen zählen, rechnen die Bürgerinnen und Bürger nicht schon vornherein mit entsprechenden Datenverarbeitungen. Daher habe ich unabhängig davon, ob im Einzelfall bereits eine Informationspflicht wegen automatisierter Entscheidungsfindung nach Art. 13 Abs. 2 Buchst. f beziehungsweise Art. 14 Abs. 2 Buchst. g DSGVO besteht, die Beachtung nachstehender Transparenzvorgaben gefordert: Verarbeitet eine bayerische öffentliche Stelle bei der Teilnahme als Unternehmen am Wettbewerb personenbezogene Daten im Rahmen eines (echten) Factorings, so hat sie diesen Prozess

nachvollziehbar (transparent) darzustellen. Dies bedingt zumindest, dass die öffentliche Stelle in ihren Datenschutzhinweisen darlegt, dass der Kauf eines Online-Tickets durch Kundinnen und Kunden davon abhängt, dass der Factor die Forderung kaufen wird. Mit anderen Worten: Das Zustandekommen des Online-Ticketkaufs hängt von der Entscheidung des Zahlungsdienstleisters ab. Hierbei ist auch darzustellen, welche Folgen eine negative Entscheidung des Zahlungsdienstleisters für den Kaufprozess der Kundin oder des Kunden hat.

6.2 Datenschutz bei elektronischen Wasserzählern mit Funkmodul

Zuletzt hatte ich mich in meinem 28. Tätigkeitsbericht 2018 unter Nr. 7.3 mit dem Thema Datenschutz bei elektronischen Wasserzählern mit Funkmodul befasst. Anlass war der im damaligen Berichtszeitraum in Kraft getretene Art. 24 Abs. 4 Gemeindeordnung (GO). Diese Norm enthält nicht nur die von mir stets geforderte gesetzliche Rechtsgrundlage für Einbau und Betrieb elektronischer Wasserzähler mit Funkmodul, sondern gewährt in Art. 24 Abs. 4 Satz 5 bis 7 GO auch das von mir geforderte voraussetzungslose Widerspruchsrecht gegen die Verwendung des Funkmoduls. Zudem regeln Art. 24 Abs. 4 Satz 2 bis Satz 4 GO unmittelbar geltende Anforderungen an die Datenverarbeitung in einem elektronischen Wasserzähler. Über die seither erreichten datenschutzrechtlichen Verbesserungen möchte ich im Folgenden berichten.

6.2.1 Änderung des Musters für eine gemeindliche Wasserabgabesatzung

Mittels Bekanntmachung vom 20. Februar 2019[30] hat das Bayerische Staatsministerium des Innern, für Sport und Integration seine Bekanntmachung über das Muster für eine gemeindliche Wasserabgabesatzung vom 13. Juli 1989[31] (im Folgenden WAS-Bekanntmachung) unter meiner Beteiligung geändert. Hervorheben möchte ich in diesem Zusammenhang folgende Punkte:

— Zunächst sieht § 19a Abs. 2 Satz 1 Satzungsmuster eine Regelung in allgemeiner Form vor, dass die gespeicherten oder ausgelesenen personenbezogenen Daten zu löschen sind, soweit sie für die dort genannten Zwecke nicht mehr benötigt werden. Dies dient der Umsetzung des datenschutzrechtlichen Grundsatzes der Speicherbegrenzung (Art. 5 Abs. 1 Buchst. f DSGVO) und dem Recht auf Löschen (Art. 17 Abs. 1 Buchst. a DSGVO). § 19a Abs. 2 Satz 2 Satzungsmuster enthält darüber hinaus pauschale Höchstfristen. Grund hierfür sind die in meiner Prüfpraxis festgestellten Schwierigkeiten bei der Handhabung abstrakter Löschregelungen. Konkret definierte Löschfristen, welche absolute Höchstspeicherdauern ausbuchstabieren, setzen der Speicherung dagegen sichere, in der Verwaltungspraxis leicht handhabbare Grenzen. Danach sind die im Wasserzähler vor Ort gespeicherten personenbezogenen Daten spätestens nach zwei Jahren zu löschen, die ausgelesenen personenbezogenen Daten spätestens nach fünf Jahren. Auf diese Weise wird verhindert, dass elektronische Wasserzähler zu dauerhaften Datenlagern mutieren.

30 BayMBl. Nr. 98.
31 AllMBl. S. 579.

— Der Grundsatz der Datenminimierung wurde in Nr. 10.3 der Anlage 2 zum Satzungsmuster konkretisiert. So wird insbesondere ausdrücklich klargestellt, dass für die Erstellung der Abrechnung ein periodisches autonomes Funken von Daten über das Jahr hinweg nicht erforderlich ist und für die Abrechnung primär nur Zählernummer und Zählerstand notwendig sind. Die Abwehr einer Gefahr für den ordnungsgemäßen Betrieb der Wasserversorgungseinrichtung und die Aufklärung von Störungen im Wasserversorgungsnetz, etwa die Lokalisierung von Leckagen kann es freilich voraussetzen, weitere Daten – wie etwa Durchflusswerte oder Alarmcodes – auch in kurzen Intervallen automatisch zu senden. Dies verlangt jedoch einen konkreten Anlass im Einzelfall, also einen Hinweis auf eine solche Gefahr oder Störung. Für die technische Umsetzung dieser Anlassbezogenheit werden zwei Wege aufgezeigt: zum einen die Sendung eines Alarmcodes, sobald der Zähler eine solche Gefahr oder Störung registriert, zum anderen die Aktivierung der engmaschigen Alarmsendefrequenz durch Funk von außen, falls in einem bestimmten Versorgungsgebiet ein besonderes Vorkommnis (zum Beispiel eine Leckage) festgestellt wird.

— Für Altfälle, also Funkwasserzähler, die zum Zeitpunkt des Inkrafttretens der Änderung des Art. 24 Abs. 4 GO am 25. Mai 2018 bereits verbaut waren und die Daten teils – wie vorstehend erläutert datenschutzrechtlich problematisch – in relativ kurzen Zeitintervallen senden, ist vorgesehen, dass einem nachträglichen Widerspruch gegen den Einsatz eines Funkwasserzählers unter Verwendung des Funkmoduls unabhängig von der Frist nach Art. 24 Abs. 4 Satz 5 GO grundsätzlich abgeholfen und das Funkmodul deaktiviert wird.

6.2.2 Datenverarbeitung mittels Einwilligung begrenzt erweiterbar

Da derzeit noch viele elektronische Wasserzähler im Einsatz sind, die den soeben erläuterten Konflikten mit den Grundsätzen der Speicherbegrenzung und der Datenminimierung nicht genügen, wurde ich um Beratung gebeten, ob und inwieweit deren Einbau und Betrieb auf Basis von Einwilligungen rechtssicher möglich ist. Hierbei habe ich Wert darauf gelegt, die zentralen datenschutzrechtlichen Wertungen des Art. 24 Abs. 4 GO vor einer Umgehung zu schützen und die datenschutzrechtliche Autonomie der Betroffenen zu wahren. Die den Kommunen vom Innenministerium insoweit gegebenen Hinweise sehen daher insbesondere vor, dass etwaige Einwilligungen freiwillig (Art. 4 Nr. 11, Art. 7 Abs. 3 Satz 3 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) erteilt sein müssen. Daneben sehen die Hinweise vor, dass auch auf Grund einer Einwilligung die in einem elektronischen Wasserzähler gespeicherten Daten nur für die in Art. 24 Abs. 4 Satz 2 GO genannten Zwecke übermittelt werden dürfen und betonen, dass das gesendete Datenpaket möglichst klein sein sollte (grundsätzlich nur Zählernummer, Zählerstand, Alarm-/Fehlercode). Außerdem sprechen sich die Hinweise dafür aus, bidirektionalen Verfahren (welche erst auf Anforderung Daten senden) gegenüber unidirektionalen Verfahren (welche Daten ohne Anforderung senden) den Vorzug einzuräumen, soweit diese verfügbar sind.

6.2.3 Bericht aus der Beratungspraxis

Im Berichtszeitraum haben sich erneut viele Bürgerinnen und Bürger an mich mit Fragen zur zulässigen Datenverarbeitung beim Einsatz und Betrieb elektronischer Wasserzähler mit Funkmodul gewandt. Folgende Fragen sind dabei immer wieder aufgetaucht:

6.2.3.1 Kein Anspruch auf mechanischen Wasserzähler

Oftmals konnte ich Eingaben entnehmen, dass Betroffene anstelle des elektronischen Wasserzählers einen mechanischen, also analogen Wasserzähler beibehalten oder wieder eingebaut bekommen möchten. Diesen Wunsch musste ich jedoch aus datenschutzrechtlicher Sicht enttäuschen. Art. 24 Abs. 4 Satz 1 GO stellt die gesetzliche Rechtsgrundlage für die Kommunen dar, den Einbau und Betrieb elektronischer Wasserzähler (mit oder ohne Funkmodul) in einer Satzung vorzuschreiben. Auch das Widerspruchsrecht aus Art. 24 Abs. 4 Satz 5 bis 7 GO vermittelt keinen Anspruch darauf, dass ein herkömmlicher mechanischer Wasserzähler (wieder) eingebaut wird. Vielmehr dürfen gleichwohl elektronische Wasserzähler ohne Funkmodul oder mit deaktiviertem Funkmodul eingebaut und betrieben werden.

6.2.3.2 Kein Widerspruchsrecht bei Wasserzählern für mehrere Hausparteien

Misst ein elektronischer Wasserzähler mit Funkmodul nicht nur den Wasserverbrauch einer Wohnung, sondern noch von mindestens einer weiteren Wohnung steht den Betroffenen kein Widerspruchsrecht aus Art. 24 Abs. 4 Satz 5 und 6 GO zu. Denn das Widerspruchsrecht nach Art. 24 Abs. 4 Satz 5 und Satz 6 GO ist nicht anwendbar, soweit in einem versorgten Objekt mehrere Einheiten einen gemeinsamen Wasserzähler haben (Art. 24 Abs. 4 Satz 7 GO). Datenschutzrechtlicher Hintergrund ist, dass in diesem Fall typischerweise keine personenbezogenen Daten nach Art. 4 Nr. 1 DSGVO vorliegen. Bei mehreren Einheiten kann der gemessene Verbrauch in der Regel – ohne zusätzliches Sonderwissen, über das der Wasserversorger jedoch grundsätzlich nicht verfügt – nicht mehr konkreten identifizierbaren Personen zugeordnet werden.

6.2.3.3 Keine Gebühr für die Ausübung des Widerspruchsrechts

Das vom Gesetzgeber voraussetzungslos gewährte Widerspruchsrecht nach Art. 24 Abs. 4 Satz 5 bis 7 GO stellt dessen Reaktion auf die Betroffenheit von Grundrechtspositionen, nämlich dem Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz (GG) und dem Recht auf Unverletzlichkeit der Wohnung gemäß Art. 13 Abs. 1 GG dar. Die Erhebung einer Gebühr oder eines Kostenersatzes für die Ausübung dieses datenschutzrechtlichen Rechts, welches auch grundrechtlich radiziert ist, käme einer Maßregelung gleich. Ohne Rechtsgrundlage ist es aber einer öffentlichen Stelle untersagt, ihre Bürgerinnen und Bürger für die Ausübung von Rechten zu bestrafen. Zudem widerspricht ein solches Handeln dem auch datenschutzrechtlich relevanten Grundsatz von Treu und Glauben (Art. 5 Abs. 1 Buchst. a DSGVO). Daneben kann ich aus Datenschutzsicht auch nicht erkennen, dass die Ausübung dieses gesetzlichen Rechts einen Sondervorteil für die Betroffenen darstellen würde. Flankierend hat mir das Innenministerium auf Nachfrage bestätigt, dass es auch kommunalabgabenrechtlich keine Grundlage für die Erhebung von Gebühren oder Ähnlichem wegen Ausübung des Widerspruchsrechts sieht. Daher werde ich darauf achten, dass die Ausübung dieses datenschutzrechtlichen Rechts nicht

zu finanziellen Belastungen für die Betroffenen führt. Unabhängig von beziehungsweise neben eigenen aufsichtsrechtlichen Maßnahmen werde ich soweit notwendig insoweit auch die Kommunalaufsicht einschalten.

6.3 Öffentliche Gemeinderatssitzung: Behandlung einer Privatinsolvenz

Auch im aktuellen Berichtszeitraum war ich wieder des Öfteren mit dem Problem über das erforderliche Maß hinausgehender Datenverarbeitungen bei Beratung und Beschlussfassung im Gemeinderat befasst. Folgenden besonders prägnanten Fall greife ich exemplarisch heraus: Eine Gemeinde stellte im Vorfeld der geplanten Beauftragung eines Unternehmens mit der Durchführung einer Veranstaltung Recherchen zum potentiellen Vertragspartner an. Hierbei stieß die Gemeinde auf das Vorliegen einer Insolvenz in der Vergangenheit. Jedoch war hiervon nicht das Unternehmen als potentieller Vertragspartner betroffen, sondern eine für das Unternehmen als Projektleiter bei der geplanten Veranstaltung tätige Privatperson. Das Rechercheergebnis – Vorliegen einer Privatinsolvenz des Projektleiters – wurde in öffentlicher Sitzung beraten und so der Bürgerschaft offengelegt. Ich habe daher einen Verstoß gegen datenschutzrechtliche Vorgaben festgestellt:

Die Information, dass über das Privatvermögen einer bestimmten oder bestimmbaren natürlichen Person ein Insolvenzverfahren eröffnet wurde, ist ein personenbezogenes Datum gemäß Art. 4 Nr. 1 DSGVO. Wird diese Information im Rahmen einer öffentlichen Gemeinderatssitzung behandelt und so an die anwesenden Gemeindebürger bekanntgegeben, werden personenbezogene Daten verarbeitet (Art. 4 Nr. 2 DSGVO). Die Verarbeitung personenbezogener Daten bedarf einer Befugnis (Art. 6 Abs. 1 DSGVO). Bayerische öffentliche Stellen stützen sich hierbei regelmäßig auf gesetzliche Verarbeitungsbefugnisse des nationalen Rechts (Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 UAbs. 1 Buchst. b DSGVO).

6.3.1.1 Datenverarbeitung wohl schon nicht zur Sitzungsvorbereitung erforderlich

Nach Art. 46 Abs. 2 Satz 1 Gemeindeordnung (GO) bereitet der erste Bürgermeister die Beratungsgegenstände des Gemeinderats vor. Eine gesetzliche Verpflichtung zur Beifügung von Unterlagen mit der Ladung zur Sitzung des Gemeinderats besteht jedoch nicht. Die Vorbereitungspflicht aus Art. 46 Abs. 2 Satz 1 GO korrespondiert allerdings mit dem Informationsrecht des Gemeinderats beziehungsweise des beschließenden Ausschusses. Danach hat der Gemeinderat oder der beschließende Ausschuss ein Recht auf die Informationen, die für seine Aufgabenerfüllung erforderlich sind, also insbesondere für die Beratung und für den Beschluss von Entscheidungen in seinem Zuständigkeitsbereich. Mangels anderweitiger gesetzlicher Regelung in der Gemeindeordnung steht die Entscheidung, wie die erste Bürgermeisterin oder der erste Bürgermeister den Gemeinderat respektive die beschließenden Ausschüsse über die zu behandelnden Beratungsgegenstände vorbereitend informiert, in ihrem oder seinem pflichtgemäßen Ermessen. Dieses Ermessen wird jedoch durch die Belange des grundrechtlich fundierten Datenschutzes begrenzt. Der Umfang der Befugnis zur Offenlegung personenbezogener Daten ergibt sich insoweit primär aus den einschlägigen fachgesetzlichen Verarbeitungsbefugnissen, nachrangig aus den allgemeinen Verarbeitungsbefugnissen in Art. 4 und 5 BayDSG.

Mangels einschlägiger Fachgesetze waren im konkreten Fall die Regelungen des Bayerischen Datenschutzgesetzes maßgeblich. Die (internen!) Sitzungsvorlagen

der Verwaltung für den Gemeinderat durften daher **personenbezogene Daten** enthalten, **soweit dies für dessen Aufgabenerfüllung erforderlich war**. Vorliegend ergaben sich jedoch bereits insoweit **Zweifel an der Erheblichkeit** der Privatinsolvenz des Projektleiters für Beratung und Beschlussfassung im Gemeinderat. So war schon nicht hinreichend bestimmbar, inwieweit die private Bonität einer für das potentiell zu beauftragende Unternehmen tätigen Privatperson (Haftungs-)Risiken für die Gemeinde barg. Nach Mitteilung der Gemeinde waren für die Nichtberücksichtigung des Unternehmens dann letztlich auch **andere Kriterien kausal**.

6.3.1.2 Jedenfalls Behandlung und Bekanntgabe in öffentlicher Sitzung unzulässig

Der Gemeinderat berät und beschließt gemäß Art. 52 Abs. 2 Satz 1 GO grundsätzlich in öffentlicher Sitzung, soweit nicht Rücksichten auf das Wohl der Allgemeinheit oder auf berechtigte Ansprüche einzelner entgegenstehen. Die Norm ist keine Rechtsgrundlage im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 UAbs. 1 Buchst. b DSGVO für eine Verarbeitung personenbezogener Daten, da ihr der erforderliche datenschutzbezogene Regelungsgehalt fehlt (siehe auch meine Ausführungen im 29. Tätigkeitsbericht 2019 unter Nr. 5.1.1.1). Soweit nicht fachgesetzliche Besonderheiten bestehen, können bayerische Gemeinden insoweit aber regelmäßig auf Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG als allgemeine Rechtsgrundlage für Datenübermittlungen zurückzugreifen. Daher duften bei der Behandlung der Angelegenheit in öffentlicher Gemeinderatssitzung auch personenbezogene Daten offengelegt werden, **wenn und soweit** dies **zur Aufgabenerfüllung** der Gemeinde **erforderlich** war.

Hieran **fehlte e**s im konkreten Fall aber schon deswegen, da nach Art. 52 Abs. 2 Satz 1 GO die Behandlung der Privatinsolvenz des Projektleiters wegen berechtigter Ansprüche Einzelner von vornherein **in nicht-öffentlicher Sitzung hätte erfolgen müssen.** Solche berechtigten Ansprüche Einzelner sind nicht erst Rechtsansprüche, sondern schon **Interessen einzelner Personen** oder Personengesellschaften, die eine Beratung und Beschlussfassung in geheimer Sitzung erfordern. Angelegenheiten, die sich auf die wirtschaftlichen und finanziellen Verhältnisse, auf die familiären und beruflichen Verhältnisse, aber auch auf die individuellen persönlichen Verhältnisse einer oder eines Einzelnen beziehen und Rückschlüsse auf ihre oder seine Person zulassen, sind regelmäßig in nicht-öffentlicher Sitzung zu behandeln.[32] Hinsichtlich der Information, dass über das Vermögen einer Privatperson ein Insolvenzverfahren eröffnet wurde, hätte die Gemeinde das schutzwürdige Interesse der betroffenen Person im Sinne des Art. 52 Abs. 2 Satz 1 GO erkennen müssen.

6.4 Niederschriften über Gemeinderatssitzungen: Abwesenheitsgrund von Ratsmitgliedern nicht detailliert angeben

Gemäß Art. 54 Abs. 1 Satz 2 Gemeindeordnung (GO) müssen die Niederschriften über Verhandlungen des Gemeinderats neben weiteren Pflichtangaben auch die Namen der anwesenden Gemeinderatsmitglieder und die der abwesenden unter

[32] Hölzl/Hien/Huber, Gemeindeordnung mit Verwaltungsgemeinschaftsordnung, Landkreisordnung und Bezirksordnung für den Freistaat Bayern, Stand Juni 2020, Art. 52 GO Erl. 4.

Angabe ihres Abwesenheitsgrundes enthalten. Die Einsicht in die Niederschriften über öffentliche Sitzungen des Gemeinderats steht nach Art. 54 Abs. 3 Satz 2 Halbsatz 1 GO allen Gemeindebürgern offen.

Art. 54
Niederschrift
(1) [1]Die Verhandlungen des Gemeinderats sind niederzuschreiben. [2]Die Niederschrift muß Tag und Ort der Sitzung, die Namen der anwesenden Gemeinderatsmitglieder und die der abwesenden unter Angabe ihres Abwesenheitsgrundes, die behandelten Gegenstände, die Beschlüsse und das Abstimmungsergebnis ersehen lassen. [3]Jedes Mitglied kann verlangen, daß in der Niederschrift festgehalten wird, wie es abgestimmt hat.
[…]
(3) [1]Die Gemeinderatsmitglieder können jederzeit die Niederschrift einsehen und sich Abschriften der in öffentlicher Sitzung gefaßten Beschlüsse erteilen lassen. [2]Die Einsicht in die Niederschriften über öffentliche Sitzungen steht allen Gemeindebürgern frei; dasselbe gilt für auswärts wohnende Personen hinsichtlich ihres Grundbesitzes oder ihrer gewerblichen Niederlassungen im Gemeindegebiet.

Im Berichtszeitraum war ich mit der Frage befasst, ob insoweit die Angabe von Krankheit als Abwesenheitsgrund zulässig ist. Meine Prüfung hat insoweit Folgendes ergeben:

Nimmt eine Gemeinde in die Niederschrift über eine Sitzung des Gemeinderats hinsichtlich namentlich benannter Gemeinderatsmitglieder die Information „abwesend wegen Krankheit" auf, so verarbeitet sie ein Gesundheitsdatum im Sinne von Art. 4 Nr. 15 DSGVO. Hieran stellt die Datenschutz-Grundverordnung in deren Art. 9 aber besondere Anforderungen. So ist die Verarbeitung von Gesundheitsdaten gem. Art. 9 Abs. 1 DSGVO grundsätzlich untersagt, sofern nicht eine Ausnahme nach Abs. 2 greift.

Art. 9 DSGVO
Verarbeitung besonderer Kategorien personenbezogener Daten
(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.
[…]

Art. 54 GO erfüllt jedoch nicht die in Art. 9 Abs. 2 DSGVO genannten Anforderungen an eine Rechtsgrundlage zur Verarbeitung von Gesundheitsdaten. Verschärfend kommt für öffentliche Sitzungen des Gemeinderats die voraussetzungslose Offenlegung der entsprechenden Informationen im Rahmen des Einsichtsrechts nach Art. 54 Abs. 3 Satz 2 GO hinzu.

Ich bin daher an das für die Kommunalaufsicht zuständige Bayerische Staatsministerium des Innern, für Sport und Integration herangetreten und habe vor dem Hintergrund des Anwendungsvorrangs des Europarechts gebeten, zukünftig anstelle der Angabe „abwesend wegen Krankheit" in die Niederschriften lediglich den Hinweis „entschuldigt/unentschuldigt fehlend" aufzunehmen und dies auf alle

Abwesenheitsgründe zu erweitern. Denn eine Veränderung nur bezüglich Krankheit als Abwesenheitsgrund würde weiterhin Rückschlüsse auf den Gesundheitszustand von Ratsmitgliedern zulassen.

Das Innenministerium hat meine Anregung aufgegriffen und die Gemeinden gebeten, in Niederschriften über Verhandlungen des Gemeinderats **generell nur noch die Angabe „entschuldigt" oder „unentschuldigt" für jede Form der Abwesenheit aufzunehmen.**

6.5 Gemeinde- und Landkreiswahlen: Unterschriften auf Unterstützungslisten zukünftig besser geschützt

Bei Gemeinde- und Landkreiswahlen müssen neue Wahlvorschlagsträger nach dem Gemeinde- und Landkreiswahlgesetz (GLKrWG) grundsätzlich von einer ausreichenden Zahl weiterer Wahlberechtigter unterstützt werden. Hierfür werden von den Kommunen Unterstützungslisten aufgelegt, in welche sich Wahlberechtigte, die einen Wahlvorschlag unterstützen wollen, eintragen können. Anlässlich der im Berichtszeitraum stattfindenden Gemeinde- und Landkreiswahlen bin ich durch Eingaben besorgter Bürgerinnen und Bürger darauf aufmerksam geworden, dass dabei die **bereits geleisteten Unterschriften durch nachfolgende Unterzeichnende eingesehen werden können.** Meine datenschutzrechtliche Überprüfung hat insoweit Folgendes ergeben:

6.5.1 Besserer Schutz von Unterschriften bei Eintragungslisten für Volksbegehren

Art. 37 Abs. 5 Gemeinde- und Landkreiswahlordnung (GLKrWO) bestimmt:

„[1]Auskünfte über die Zahl der Eintragungen können bereits vor Abschluss der Unterstützungslisten erteilt werden; im Übrigen dürfen aus den Unterstützungslisten keine Auskünfte erteilt und keine Aufzeichnungen zugelassen werden. [2]Zur Eintragung darf nur die laufende Seite vorgelegt werden."

Eine vergleichbare Regelung findet sich für die Eintragungslisten von Volksbegehren inhaltsgleich in den Sonderbestimmungen für Volksbegehren nach der Landeswahlordnung (LWO):

„[1]Die Gemeinde kann bereits vor Abschluss der Eintragungslisten Auskünfte über die Zahl der Eintragungen erteilen; im Übrigen dürfen aus den Eintragungslisten keine Auskünfte erteilt und keine Aufzeichnungen zugelassen werden. [2]Den Stimmberechtigten darf nur die laufende Liste vorgelegt werden."

Die Eintragungslisten für **Volksbegehren** sind entsprechend dem Muster der Anlage 20 zur LWO zu erstellen. In diesem Muster findet sich folgender, über den unmittelbaren Wortlaut des § 80 Abs. 7 LWO hinausgehender Hinweis:

„Aus Datenschutzgründen werden bereits geleistete Eintragungen abgedeckt (vgl. § 80 Abs. 7 LWO)".

In den maßgeblichen Vorschriften für die Durchführung von **Gemeinde- und Landkreiswahlen**, also dem Gemeinde- und Landkreiswahlgesetz, der Ge-

meinde- und Landkreiswahlordnung sowie der Gemeinde- und Landkreiswahlbekanntmachung[33] hier insbesondere bei der sachlich einschlägigen Nr. 42 und dem Muster für die Eintragung in Unterstützungslisten gemäß Anlage 10 zu Nr. 42 GLKrWBek – findet sich ein solcher Hinweis dagegen **nicht.**

6.5.2 Anhebung des Schutzniveaus für Unterschriften auf Unterstützungslisten

Ich bin daher an das für das Wahlrecht in Bayern zuständige Bayerische Staatsministerium des Innern, für Sport und Integration herangetreten und habe darauf hingewiesen, dass eine im Herrschaftsbereich der Kommune erfolgende, von dieser geduldete Offenlegung bereits geleisteter Unterstützungsunterschriften an nachfolgende Unterzeichnende eine **Übermittlung personenbezogener Daten seitens der die Liste auslegenden Gemeinde an die jeweils unterschreibenden Personen darstellt.** Übermittelt werden dabei neben Namen und Adressen anderer Unterzeichnender auch Informationen zu deren politischer Überzeugung. Gerade letztere Information steht sogar unter dem besonderen Schutz des Art. 9 Abs. 1 DSGVO. Aber auch unabhängig von den besonderen Anforderungen des Art. 9 DSGVO konnte ich für die gerade erläuterte Datenübermittlung durch die Kommunen mangels Erforderlichkeit bereits **keine den allgemeinen Anforderungen in Art. 6 DSGVO genügende Rechtsgrundlage** erkennen. Hinzu kommt der Grundsatz der Datenminimierung (vgl. Art. 5 Abs. 1 Buchst. c DSGVO). Ich habe daher gefordert, zukünftig auch bei Gemeinde- und Landkreiswahlen bereits geleistete Unterstützungsunterschriften abzudecken.

Erfreulicherweise hat das **Innenministerium zugesagt**, meinen **Vorschlag** zur Ergänzung der Anlage 10 zu Nr. 42 GLKrWBek um einen datenschutzrechtlichen Hinweis zur Abdeckung bereits geleisteter Unterschriften nach dem Vorbild der Anlage 20 zur LWO im Rahmen der Evaluierung der Gemeinde- und Landkreiswahlen 2020 **aufzugreifen**.

6.6 Beweissicherung bei gemeindlichen Straßenbaumaßnahmen per Foto

Die Gemeinden sind gemäß Art. 47 Abs. 1 Bayerisches Straßen- und Wegegesetz (BayStrWG) Träger der Straßenbaulast für die erforderlichen Gemeindestraßen innerhalb des Gemeindegebiets.

Bei der Erweiterung vorhandener Baugebiete kann es im Vorfeld gemeindlicher Straßenbaumaßnahmen sinnvoll sein, zwecks Beweissicherung den Zustand vorhandener Gebäude fotografisch zu erfassen. Straßenbaumaßnahmen können mit der Gefahr verbunden sein, dass bereits vorhandene Gebäude Schaden nehmen, etwa wenn durch Erschütterungen Risse in Wänden auftreten. Für eventuelle Rechtsstreitigkeiten wegen (angeblichen) Beschädigungen durch eine Straßenbaumaßnahme kann eine vorsorglich angefertigte Fotodokumentation des Gebäudezustands ein wertvolles Beweisstück sein, welches hilft, Streit zu vermeiden und gegebenenfalls Steuergelder zu sparen.

Im Berichtszeitraum war ich insoweit mehrfach mit der Frage befasst, welche datenschutzrechtlichen Anforderungen zu beachten sind, wenn solche Fotoaufnahmen angefertigt werden sollen. Insoweit habe ich folgende Hinweise gegeben:

[33] Vom 7. Mai 2019 (BayMBl. Nr. 188).

6.6.1 Zustand der Außen- und Innenwände privater Wohngebäude ist ein personenbezogenes Datum

Der zur Beweissicherung gemeindlicherseits dokumentierte Zustand von Außen- als auch von Innenwänden privater Wohngebäude stellt regelmäßig ein personenbezogenes Datum gemäß Art. 4 Nr. 1 DSGVO dar, da die angefertigten Dokumentationen schon von ihrer eingangs erläuterten Zwecksetzung her sinnvollerweise nur unter Hinzufügung von Adresse des Ortes, an dem sich die abgelichteten Objekte befinden und Namen von Betroffenen (Bewohnern oder Eigentümern) in der Gemeindeverwaltung oder bei einem beauftragten Dienstleister veraktet oder elektronisch abgelegt werden. Anders könnte der mit ihnen verfolgte Zweck auch gar nicht erreicht werden. Damit handelt es sich um Informationen, die sich auf identifizierte oder identifizierbare natürliche („betroffene") Personen beziehen. Werden derartige Fotoaufnahmen, welche zumindest mittels Standortdaten (Adressen) sowie den gerade erläuterten Zusatzinformationen natürlichen Personen zugeordnet werden können, erstellt, gespeichert und gegebenenfalls zu Beweiszwecken verwendet, liegt eine Verarbeitung im Sinne von Art. 4 Nr. 2 DSGVO vor.

6.6.2 Allenfalls Ablichtung jederzeit einsehbarer Außenwände auf Basis gesetzlicher Befugnis zulässig, im Übrigen nur mit Einwilligung

Für die genannten Datenumgänge brauchen Gemeinden gemäß Art. 6 Abs. 1 DSGVO eine Rechtsgrundlage. Das Bayerische Straßen- und Wegegesetz stellt eine solche Rechtsgrundlage nicht zur Verfügung. Auf Art. 4 Abs. 1 BayDSG kann eine Erstellung und Speicherung von Gebäudeaufnahmen nur begrenzt gestützt werden.

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.
[…]

Diese Norm hat nämlich die Funktion eines „Auffangtatbestands", um öffentlichen Stellen bei Fehlen einer fachgesetzlichen Verarbeitungsbefugnis die zur Erfüllung ihrer vielgestaltigen Aufgaben nötigen Datenumgänge zu ermöglichen. Unter Berücksichtigung der unterschiedlichen Intensität der mit den erläuterten Datenumgängen einhergehenden Eingriffe in die Grundrechte der Betroffenen ist daher zu **unterscheiden**, ob Gegenstand der Datenverarbeitungen Fotografien von **Außenfassaden** oder von **Innenräumen** sind.

Insoweit lässt sich allenfalls die Erstellung von Fotografien von **Außenfassaden** und deren weitere Verarbeitung auf **Art. 4 Abs. 1 BayDSG** in Verbindung mit der Aufgabe aus Art. 47 Abs. 1 BayStrWG stützen. Voraussetzung hierfür ist insbesondere aber, dass die betroffenen Wände jederzeit unschwer von der Straße aus, also auch **ohne etwaiges einvernehmliches Betreten von Nachbargrundstücken von öffentlichen Straßen aus einsehbar sind**. Die insoweit angefertigten Dokumentationen sind dann nämlich nur von sehr geringer Eingriffsintensität, da sie nicht über das hinausgehen, was sowieso jedermann im Vorbeigehen an dem Grundstück von öffentlichen Straßengrund aus unschwer wahrnehmen kann.

Mit Fotoaufnahmen der Innenräume von Wohnungen wird demgegenüber regelmäßig in das Grundrecht auf Unverletzlichkeit der Wohnung eingegriffen (Art. 13 Abs. 1 Grundgesetz). Da die Wohnung einer Person ihrer Privatsphäre zuzuordnen ist, wird mit der Aufnahme, Speicherung und Verwendung derartiger Fotografien das Persönlichkeitsrecht auf besondere Weise beeinträchtigt. Daher können die geschilderten Datenumgänge im Wohnungs**innenbereich** gerade **nicht** mehr auf die Auffangnorm des **Art. 4 Abs. 1 BayDSG** gestützt werden kann. Vielmehr sind Bildaufnahmen im Innenbereich von Wohnungen und weitere Datenumgänge im oben skizzierte Sinne nur auf Grundlage rechtswirksamer **Einwilligungen** der hiervon betroffenen Person nach Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 4 Nr. 11 und Art. 7 DSGVO zulässig.[34]

6.6.3 Auftragsverarbeitung

Soweit die Gemeinde als Verantwortliche (vgl. Art. 4 Nr. 7 DSGVO) die Fotografien nicht selbst erstellt, sondern damit – sowie gegebenenfalls der Speicherung der Aufnahmen – Externe wie etwa ein (Ingenieur-)Büro beauftragt, ist grundsätzlich eine **Auftragsverarbeitungsvereinbarung** zu schließen (Art. 28 DSGVO).[35]

6.7 Datenschutz bei Jagdgenossenschaften

Datenschutzrechtliche Fragestellungen aus dem Bereich der Jagdgenossenschaften haben mich im Berichtszeitraum wiederholt beschäftigt. Auf Folgendes möchte ich besonders hinweisen:

6.7.1 Anwendbarkeit des Bayerischen Datenschutzgesetzes

Jagdgenossenschaften sind in Bayern gemäß Art. 11 Abs. 1 Satz 1, 2 Bayerisches Jagdgesetz (BayJG) Körperschaften des öffentlichen Rechts unter staatlicher Aufsicht. Damit fallen sie als öffentliche Stellen unter das Bayerische Datenschutzgesetz (Art. 1 Abs. 1 Satz 1 BayDSG).

6.7.2 Benennung von Datenschutzbeauftragten

Oftmals waren sich Jagdgenossenschaften nicht bewusst, dass sie – unabhängig von ihrer Größe – nach Art. 37 Abs. 1 Satz 1 Buchst. a DSGVO **zur Benennung von Datenschutzbeauftragten verpflichtet** sind. Ich konnte insbesondere zu Aufgaben und Qualifikation auf meine Orientierungshilfe „Der behördliche Datenschutzbeauftragte“[36] verweisen. Konkretisierend habe ich insoweit darauf aufmerksam gemacht, dass regelmäßig ein **Interessenkonflikt** im Sinne des Art. 38

34 Vgl. allgemein Bayerischer Landesbeauftragter für den Datenschutz, Die Einwilligung nach der Datenschutz-Grundverordnung, Stand 10/2018, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Einwilligung“.

35 Dazu Bayerischer Landesbeauftragter für den Datenschutz, Auftragsverarbeitung, Orientierungshilfe, Stand 4/2019, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Auftragsverarbeitung“.

36 Bayerischer Landesbeauftragter für den Datenschutz, Der behördliche Datenschutzbeauftragte, Stand 5/2018, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Behördlicher Datenschutzbeauftragter“.

Abs. 6 DSGVO zu befürchten ist, wenn Datenschutzbeauftragte zugleich Mitglieder der Vorstandschaft sind. Der Grund hierfür liegt darin, dass die Vorstandschaft als Vertretung der Jagdgenossenschaft nach außen die Aufgaben wahrnimmt, welche die Datenschutz-Grundverordnung dem Verantwortlichen zuweist.

Da nach meinem Eindruck gerade bei kleineren Jagdgenossenschaften die Benennung von geeigneten Datenschutzbeauftragten nicht unerhebliche Probleme bereitet, habe ich auf die den Jagdgenossenschaften offenstehenden Kooperationsmöglichkeiten hingewiesen. Beispielsweise könnte nach Art. 37 Abs. 6 DSGVO etwa eine Jagdgenossin oder ein Jagdgenosse mit datenschutzrechtlichen Kenntnissen die Funktion als Datenschutzbeauftragter für mehrere Jagdgenossenschaften übernehmen.

6.7.3 Führung eines Verarbeitungsverzeichnisses

Auch Jagdgenossenschaften müssen gemäß Art. 30 DSGVO ein **Verarbeitungsverzeichnis führen**. Als Verarbeitungstätigkeit aufzunehmen ist zumindest die Führung des Jagdkatasters. Zu denken ist auch an die Verarbeitung weiterer Daten von Mitgliedern (wie beispielsweise Telefonnummern oder Bankverbindungen) oder von Dritten, wie beispielsweise Jagdpächterinnen und Jagdpächtern oder Begehungsscheininhaberinnen und Begehungsscheininhabern.

6.7.4 Zugang zum Jagdkataster

Auch der datenschutzkonforme Umgang hinsichtlich des Jagdkatasters hat mich mehrfach beschäftigt. Rechtsgrundlage für dessen Führung ist Art. 11 Abs. 1 Satz 1 BayJG in Verbindung mit § 5 Abs. 1 Verordnung zur Ausführung des Bayerischen Jagdgesetzes (AVBayJG). Danach haben Jagdgenossenschaften eine Satzung mit den in Anlage 1 zur AVBayJG genannten Bestimmungen zu beschließen. Nach § 3 Abs. 2 Satz 1 Mustersatzung führt die Jagdgenossenschaft ein Jagdkataster, in dem die Eigentümer oder Nutznießer der zum Gebiet der Jagdgenossenschaft gehörenden Grundflächen und deren Größe ausgewiesen werden.

Dieses Jagdkataster liegt nach § 3 Abs. 2 Satz 4 Mustersatzung für die Jagdgenossen und deren schriftlich Bevollmächtigte zur Einsicht offen. Damit hat der bayerische Gesetzgeber die Entscheidung getroffen, den Jagdgenossinnen und Jagdgenossen zu den Informationen aus dem Jagdkataster **voraussetzungslos Zugang** zu gewähren. Diese weite Fassung des Einsichtsrechts, welches nicht nur die eigenen personenbezogenen Daten der Einsicht nehmenden Person, sondern auch der übrigen Jagdgenossinnen und Jagdgenossen umfasst, wird dann nachvollziehbar, wenn man die in § 9 Abs. 3 Bundesjagdgesetz (BJagdG) enthaltene Regelung über die erforderliche Mehrheit für die Beschlussfassung in den Sitzungen der Jagdgenossenschaft berücksichtigt. Ein Beschluss bedarf danach nämlich nicht nur einer Mehrheit der anwesenden Personen, sondern auch einer Mehrheit der vertretenen Flächen. Die im Jagdkataster niedergelegten Informationen bilden somit die Grundlage für eine ordnungsgemäße Beschlussfassung. Damit die Jagdgenossinnen und Jagdgenossen dies im Bedarfsfall überprüfen können, müssen ihnen die Daten zugänglich sein.

6.7.5 Datenschutzkonforme Mitgliederversammlungen

Zur datenschutzgerechten Gestaltung von Mitgliederversammlungen habe ich folgende Hinweise gegeben:

6.7.5.1 Umgang mit gestellten Anträgen in öffentlichen Einladungen zur Sitzung

Auch wenn es sich bei dem bloßen Hinweis, dass Jagdgenossinnen oder Jagdgenossen Anträge gestellt haben, welche in der Versammlung behandelt werden sollen, regelmäßig nicht um besonders sensible personenbezogene Informationen handelt, benötigt die Jagdgenossenschaft doch eine Rechtsgrundlage, wenn sie Antragstellerinnen und Antragsteller namentlich in öffentlichen Einladungen zu der nicht öffentlichen Versammlung der Jagdgenossen nennt. Derartige Einladungen ergehen nach § 7 Abs. 1 und Abs. 3 sowie § 15 Mustersatzung durch Bekanntmachung und müssen unter anderem die Tagesordnung enthalten. Jedoch ist regelmäßig **keine Erforderlichkeit** erkennbar, **in öffentlichen Einladungen zu einer nicht öffentlichen Versammlung die Antragsteller namentlich zu nennen**. Insoweit war zu berücksichtigen, dass die veröffentlichte Information eben nicht nur den Jagdgenossinnen und Jagdgenossen, sondern auch Nichtmitgliedern zur Kenntnis gebracht wurde.

6.7.5.2 Namentliche Bekanntgabe des ausgezahlten Jagdzinses in der Versammlung

Nach § 13 Abs. 2 Satz 1 Mustersatzung ist zum Ende des Geschäftsjahres eine Jahresrechnung (Kassenbericht) zu erstellen, die den Rechnungsprüfern zur Prüfung und der Versammlung der Jagdgenossen zur Entlastung des Jagdvorstandes und des Kassenführers vorzulegen ist. Einige Jagdgenossenschaften **nennen** in diesem Rahmen **namentlich diejenigen Mitglieder, welche eine Auszahlung des Jagdzinses nach § 10 Abs. 3 BJagdG beantragt haben**, und zwar **mitsamt den jeweiligen Auszahlungsbeträgen.** Soweit den Jagdgenossinnen und Jagdgenossen aus § 13 Abs. 2 Satz 1 der Mustersatzung ein generelles Prüfungs- und Einsichtsrecht in den vorzulegenden Kassenbericht sowie in die zugehörigen Belege zukommt, um die Überprüfung auch konkreter Rechnungspositionen zu ermöglichen, ist die Kenntnisnahme im Kassenbericht verarbeiteter personenbezogener Daten aus datenschutzrechtlicher Sicht **grundsätzlich nicht zu beanstanden**. Jedenfalls ist aber speziell im Hinblick auf die Auszahlung des Jagdzinses zu berücksichtigen, dass die Höhe des Auszahlungsbetrages sich gemäß § 10 Abs. 3 BJagdG aus dem Reinertrag der Jagdnutzung sowie der vertretenen Fläche berechnet. Dabei handelt es sich aber um Informationen, die den Jagdgenossinnen und Jagdgenossen entweder ohnehin bekannt oder jedenfalls über das Jagdkataster zugänglich sind.

Ich habe insoweit allerdings angeregt, zunächst als datenschutzfreundlichere Möglichkeit eine Zusammenfassung der Auszahlungssummen in Betracht zu ziehen und den gesamten Kassenbericht (insbesondere hinsichtlich personenbezogener Rechnungspositionen) im Rahmen der Versammlung erst dann bekannt zu geben, wenn dies von den Jagdgenossinnen und Jagdgenossen zu Prüfungszwecken gewünscht wird.

6.8 Dienstausweise der Naturschutzwacht datenschutzkonform ausgestaltet

Seit Geltungsbeginn der Datenschutz-Grundverordnung am 25. Mai 2018 bestand schon mehrfach Veranlassung, gerade auch die Datenschutzkonformität von mittlerweile „in die Jahre gekommenen" Vorschriften zu überprüfen. Dies möchte ich an folgendem Beispiel erläutern:

Ein aufmerksamer Bürger hat mich darauf hingewiesen, dass die Ausweise der Naturschutzwacht eine Vielzahl personenbezogener Daten enthalten. Bei meiner Überprüfung habe ich festgestellt, dass die inhaltlich seit Inkrafttreten der Verordnung über die Naturschutzwacht (NatSchWV) im Jahr 1975 unveränderte Anlage 1 „Dienstausweis der Angehörigen der Naturschutzwacht" ein verbindliches Ausweismuster vorsah. Der Ausweis enthielt folgende Informationen: die Ausstellungsbehörde, ein Lichtbild der Ausweisinhaberin oder des Ausweisinhabers, ihr oder sein Vor- und Familienname, das Geburtsdatum, der Geburtsort, eine Amtsbezeichnung oder ein Beruf, die Wohnanschrift sowie eine Unterschrift. Aus § 11 Abs. 1 NatSchWV ergab sich zudem, dass Mitglieder der Naturschutzwacht den Dienstausweis bei der Ausübung des Dienstes mitzuführen und bei Vornahme einer Amtshandlung auf Verlangen vorzuzeigen haben.

Der umfangreiche Datensatz führte dazu, dass ehrenamtliche Mitglieder der Naturschutzwacht, welche Naturschutzbehörden und Polizei unterstützen, bei Amtshandlungen eventuell eine **Vielzahl privater Informationen offenbaren müssen**. Insoweit stellte sich aus datenschutzrechtlicher Sicht die Frage, wofür eine derart weitreichende Verpflichtung zur Offenbarung personenbezogener Daten erforderlich sein soll. Regelmäßig erfolgt die Vorlage von Dienstausweisen an von Maßnahmen Betroffene nur, um diesen die Überprüfung zu ermöglichen, ob es sich bei der handelnden Person tatsächlich um eine Amtsperson handelt und diese innerhalb der Zuständigkeit agiert. Zieht man vor diesem Hintergrund den **Vergleich zu anderen amtlichen bayerischen Dienstausweisen**, wie beispielsweise denen, die auf der Grundlage der Allgemeinen Geschäftsordnung für die Behörden des Freistaats Bayern (AGO) ausgestellt werden, wird deutlich, dass diese nach § 35 Abs. 2 AGO mit einem **weit geringeren Datensatz** auskommen, der lediglich Lichtbild, Vor- und Familienname, Beschäftigungsbehörde mit Anschrift und Unterschrift umfasst.

Daher habe ich mich an das fachlich zuständige Bayerische Staatsministerium für Umwelt und Verbraucherschutz gewandt und darauf hingewiesen, dass der umfangreiche Datensatz der Naturschutzwachtdienstausweise vor dem Hintergrund des Grundsatzes der Datenminimierung (vgl. Art. 5 Abs. 1 Satz 1 Buchst. c DSGVO) erheblichen Zweifeln begegnet. Das Umweltministerium hat meinen **Hinweis umgehend aufgegriffen** und im Rahmen einer grundlegenden – über meine datenschutzrechtlichen Hinweise deutlich hinausgehenden – Neustrukturierung der gemachten rechtlichen Vorgaben auch den Inhalt der Dienstausweise der Naturschutzwacht angepasst. Anlage 3 der Bekanntmachung des bayerischen Staatsministeriums für Umwelt und Verbraucherschutz über die Bildung einer Naturschutzwacht[37] sieht nunmehr ein Ausweismuster vor, welches neben Informationen zur Ausstellungsbehörde nur noch ein **Lichtbild** sowie **Vor- und Zunamen** und **Unterschrift** der Ausweisinhaberin/des Ausweisinhabers umfasst.

37 Vom 8. Juni 2020 (BayMBl. Nr. 395).

7 E-Government und öffentliche Register

7.1 Gesetz über die Digitalisierung im Freistaat Bayern

Auch im aktuellen Berichtszeitraum war ich wieder intensiv mit datenschutzrechtlichen Fragen der Verwaltungsmodernisierung, insbesondere aus dem Bereich E-Government befasst. Neben der Erarbeitung eines Leitfadens zum Outsourcing kommunaler IT (siehe hierzu unter Nr. 7.2) war ich insbesondere auch beteiligt beim Erlass eines Gesetzes über die Digitalisierung im Freistaat Bayern (Bayerisches Digitalgesetz – DigitalG).

Mit dem Bayerischen Digitalgesetz will der Freistaat Bayern über seine bisherigen Maßnahmen zur Förderung und Gestaltung der Digitalisierung hinausgehen und einen umfassenden allgemeinen Rechtsrahmen für die Digitalisierung von Gesellschaft und Wirtschaft, Staat und Verwaltung schaffen. Dieser neue Rechtsrahmen soll das in wesentlichen Teilen am 30. Dezember 2015 in Kraft getretene Gesetz über die elektronische Verwaltung in Bayern (siehe hierzu meinen 27. Tätigkeitsbericht 2016 unter Nr. 12.1) ersetzen und grundlegend weiterentwickeln. Neben der Verwirklichung grundsätzlicher Ziele wie etwa der Gewährleistung von digitaler Souveränität im Freistaat Bayern sowie einer Begründung digitaler Rechte der Bürgerinnen und Bürger soll das Bayerische Digitalgesetz aber auch ganz konkret der Umsetzung des Bundesgesetzes zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz) vom 14. August 2017 dienen. Mit letzterem Punkt verbunden sind Aufbau und Betrieb eines Portalverbunds von Bund und Ländern. Insbesondere soll durch das Bayerische Digitalgesetz ein Bayerischer Portalverbund mit einem zentralen Bürger-Nutzerkonto zur Inanspruchnahme digitaler Verwaltungsleistungen implementiert werden. An diesem aktuell noch laufenden Gesetzgebungsverfahren wurde ich vom federführenden Staatsministerium für Digitales beteiligt und habe in meinen Stellungnahmen insbesondere folgende für die Bürgerinnen und Bürger zentralen Datenschutzforderungen erhoben:

7.1.1 Verarbeitung von Meldedaten begrenzen

Zwar habe ich es begrüßt, dass bereits nach den ersten mir vorgelegten Entwürfen zum Bayerischen Digitalgesetz die Verwendung der gerade erwähnten Bürger-Nutzerkonten freiwillig sein sollte. Jedoch fehlte mir aus datenschutzrechtlicher Sicht die maßgebliche Klarstellung, dass diese Freiwilligkeit auch bereits für deren Einrichtung gilt. Eine im Laufe der Erarbeitung des Bayerischen Digitalgesetzes zwischenzeitlich vorgesehene Änderung der Verordnung zur Übermittlung von Meldedaten (Meldedatenverordnung) ließ insoweit nämlich vermuten, dass diese Konten pauschal für alle Bürgerinnen und Bürger gleichsam auf Vorrat erstellt werden sollen, unabhängig davon, ob diese jemals einen Antrag auf Einrichtung eines solchen Bürger-Nutzerkontos stellen. Konkret war insoweit vorgesehen, dass die Meldebehörden zwecks Bereitstellung von Nutzerkonten an dessen technischen Betreiber grundsätzlich folgende Meldedaten übermitteln: Familienname, Vornamen, Doktorgrad, Geburtsdatum und Geburtsort sowie bei Geburt im

Ausland auch den Staat, derzeitige Anschriften (Haupt- und Nebenwohnung), Familienstand, bei Verheirateten oder Personen, die eine Lebenspartnerschaft führen, zusätzlich Datum der Eheschließung oder der Begründung der Lebenspartnerschaft, Sterbedatum, Ordens- und Künstlername sowie Geschlecht. Die pauschale Übermittlung eines solch umfangreichen Meldedatenkranzes aller Bürgerinnen und Bürger – letztlich auf Vorrat – habe ich gerade vor dem Hintergrund der das Datenschutzrecht durchziehenden Grundsätze der Erforderlichkeit (vgl. Art. 6 Abs. 1 UAbs. 1 DSGVO) und der Datenminimierung (vgl. Art. 5 Abs. 1 Buchst. c DSGVO) sehr kritisch gesehen. Daher habe ich insoweit gefordert, jedenfalls derart umfangreiche Meldedatenflüsse zur Einrichtung von Nutzerkonten davon abhängig zu machen, dass vorher entsprechende Einwilligungen der Betroffenen vorliegen.

Wichtig war mir insoweit aber auch, dass die Einrichtung von Nutzerkonten beim technischen Betreiber nicht – letztlich von den Bürgerinnen und Bürgern unbemerkt – zur Entstehung eines weiteren umfassenden Bürgerbasisdatenbestands neben dem meldebehördlichen Melderegister führt. Genau dies war aber zwischenzeitlich zu befürchten, da die schon angesprochene, im Laufe der Diskussionen vorgesehene Änderung der Meldedatenverordnung insoweit vorsah, dass bei Aktivierung des Nutzerkontos die vollständigen Meldedatensätze abgerufen werden dürfen. Die Möglichkeit eines solchen vollständigen Meldedatenabrufs würde aber nicht nur systematisch einen Fremdkörper in der Meldedatenverordnung darstellen, welche bislang – feingranular nach der jeweiligen Aufgabenstellung der Datenempfänger ausdifferenziert – nur die Übermittlung enumerativ aufgezählter Meldedaten zulässt, sondern auch inhaltlich höchst sensible Daten umfassen, wie beispielsweise einen Ausschluss von der Wahlberechtigung beziehungsweise Wählbarkeit oder das Vorliegen von Passversagungsgründen (vgl. § 3 Abs. 2 Nr. 1 Buchst. a und Nr. 4 Bundesmeldegesetz). Daher habe ich insoweit gefordert, den Datenfluss nach Aktivierung der Nutzerkonten für die Bürgerinnen und Bürger transparent zu gestalten und vor allem auf das (jeweils) konkret erforderliche Ausmaß zu begrenzen.

7.1.2 Transparente Regelung der Verantwortlichkeiten

Wichtig ist mir aber auch, dass die Verantwortlichkeiten bei der Verarbeitung von personenbezogenen Daten der Bürgerinnen und Bürger transparent und nachvollziehbar sind. Angesichts der Komplexität der vorgesehenen ineinandergreifenden Datenverarbeitungsvorgänge im Zusammenhang mit dem Aufbau des oben angesprochenen Bayerischen Portalverbunds mit seinem zentralen Bürger-Nutzerkonto zur Inanspruchnahme digitaler Verwaltungsleistungen ist dies eine nicht leicht zu bewerkstelligende Aufgabe. Konkret aufeinander abzustimmen sind insoweit nämlich vor allem die geplante Schaffung einer digitalen Identität, welche jeder natürlichen Person das Recht auf staatliche Bereitstellung digitaler Dienste einräumen soll, die Schaffung des Portalverbunds Bayern mit seinen Unterportalen BayernPortal und Organisationsportal Bayern sowie das ebenfalls vorgesehene Nutzerkonto mit seinen Unterformen Bürgerkonto und Organisationskonto. Ansatzpunkt meiner noch andauernden Bemühungen um die Herstellung von mehr Klarheit hinsichtlich der Frage, welche öffentliche Stelle datenschutzrechtlicher Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO für welchen (Teil-)Datenverarbeitungsvorgang innerhalb des Gesamtsystems sein soll, stellt eine im aktuellsten mir bekannten Entwurf enthaltene Regelung dar, welche zwischen Basisdiensten (Verantwortung der nutzenden Behörde) und zentralen Diensten (Verantwortung

des bereitstellenden Ressorts) unterscheidet. Was mir an dieser Stelle aus datenschutzrechtlicher Sicht bislang jedoch fehlt, ist eine klare Zuordnung der einzelnen Infrastrukturelemente (Portalverbund Bayern, BayernPortal, Organisationsportal Bayern, Nutzerkonto und digitale Identität) zu den Begrifflichkeiten „Basisdienst" oder „zentraler Dienst", um so eine „Brücke" zu den Verantwortlichkeiten zu bauen. Mir ist an dieser Stelle eine transparente, bürgerfreundliche Regelung besonders wichtig, denn die Betroffenen sollen im Falle eines datenschutzrechtlichen Missstands den Verantwortlichen schnell ermitteln können. Mittlerweile zeichnet sich erfreulicherweise eine Lösung der Problematik über ein „Regel-Ausnahme-Verhältnis" ab, wonach alle Dienste als Basisdienste gelten sollen, außer in den Fällen einer ausdrücklichen Festlegung als zentraler Dienst. Den weiteren Prozess der Erarbeitung des Bayerischen Digitalgesetzes werde ich gerade auch insoweit unverändert aufmerksam begleiten.

7.1.3 Transparenz bei der Beauftragung staatlicher Rechenzentren

In der öffentlichen Verwaltung werden IT-Verfahren zunehmend nicht mehr lokal, sondern stattdessen zentral gebündelt in großen staatlichen Rechenzentren für viele bayerische Behörden betrieben. Den rechtlichen Rahmen hierfür stellen seit dem 25. Mai 2018 die Regelungen zur Auftragsverarbeitung gemäß Art. 28 ff. DSGVO bereit. Vor diesem Zeitpunkt war in Bayern Art. 6 BayDSG in der bis zum 24. Mai 2018 geltenden Fassung maßgeblich. Auf Basis dieser Vorschrift kamen Auftragsverarbeitungen mittels Abschluss entsprechender Verträge zustande. Diese genießen jedoch keinen Bestandsschutz. Auch bestehende Verträge müssen daher an die Anforderungen der Datenschutz-Grundverordnung angepasst werden. Für die im Zuge der Digitalisierung immer wichtiger werdenden staatlichen Rechenzentren bedeutet diese Anpassung jedoch einen nicht unerheblichen Aufwand.

Dieser Aufwand hätte ursprünglich durch den Erlass einer **Rechtsverordnung zur Regelung der öffentlich-rechtlichen Auftragsverarbeitungsverhältnisse** (siehe hierzu meinen 28. Tätigkeitsbericht 2018 unter Nr. 7.2) verringert werden sollen. Beabsichtigt war insoweit, von der in Art. 28 Abs. 3 Satz 1 Var. 2 DSGVO erstmals enthaltenen Möglichkeit zur Begründung von Auftragsverarbeitungsverhältnissen auf Grundlage eines **„anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten"** Gebrauch zu machen. Hiergegen habe ich im Rahmen meiner Beteiligung am Normsetzungsprozess zwar keine grundsätzlichen Bedenken erhoben, jedoch insbesondere gefordert, dass die inhaltlichen Vorgaben des Art. 28 Abs. 3 DSGVO sich in der geplanten Rechtsverordnung wiederfinden. Wichtig war mir aber auch die Sicherstellung der erforderlichen Transparenz. Insoweit kam es mir zusammengefasst darauf an, dass die Beteiligten im Hinblick auf die in Art. 5 Abs. 2 DSGVO geregelte Rechenschaftspflicht zu jedem Zeitpunkt in der Lage sind, darüber Auskunft zu geben, ob und seit wann, für welche Bereiche und mit welchem Inhalt Auftragsverarbeitungsverhältnisse zwischen ihnen bestehen.

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.

Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

In der Folgezeit wurden die Überlegungen zum Erlass einer Rechtsverordnung zur Regelung der öffentlich-rechtlichen Auftragsverarbeitungsverhältnisse jedoch von der Staatsregierung nicht weiter verfolgt und – ohne weitere Abstimmung mit mir – nur für den Bereich des Staatsministeriums der Finanzen und für Heimat in **§ 3a Verordnung über Organisation und Zuständigkeiten in der Bayerischen Steuerverwaltung** (Steuer-Zuständigkeitsverordnung – ZustVSt) eine partielle Regelung für Behörden der Finanzverwaltung sowie Steuerverwaltungstätigkeiten geschaffen. Dieses „andere Rechtsinstrument" enthält in Absatz 1 Satz 3 und Absatz 3 klare Regelungen zur Beendigung bestehender sowie Begründung neuer Auftragsverarbeitungen und greift insoweit meine damaligen Forderungen zur Rechtsverordnung zur Regelung der öffentlich-rechtlichen Auftragsverarbeitungsverhältnisse auf.

§ 3a ZustVSt
Auftragsverarbeitung durch staatliche Rechenzentren
(1) […] [3]Bereits bestehende Auftragsverarbeitungsverhältnisse werden zum 1. Mai 2019 für ungültig erklärt.
[…]
(3) [1]Zur Begründung eines Auftragsverarbeitungsverhältnisses teilt der Verantwortliche dem Auftragsverarbeiter in Textform mit
1. Gegenstand und Dauer der Verarbeitung,
2. Art und Zweck der Verarbeitung,
3. die Art der personenbezogenen Daten und
4. die Kategorien betroffener Personen.
[2]Satz 1 gilt auch, wenn sich die mitzuteilenden Angaben wesentlich ändern. [3]Der Auftragsverarbeiter führt ein Verzeichnis sämtlicher Verarbeitungstätigkeiten, die er als Auftragsverarbeiter ausführt und aus dem sich die Angaben aus Satz 1 ergeben.

Wohl als neuen Anlauf, die oben geschilderte Problematik bei den staatlichen Rechenzentren nun umfassend zu lösen, sah das Bayerische Digitalgesetz zunächst eine Regelung vor, die sich wie folgt zusammenfassen lässt: Durch die **tatsächliche Inanspruchnahme** einer Auftragsverarbeitung kommt ein „Rechtsverhältnis" zustande, in welches die in Form einer Bekanntmachung der Staatsregierung veröffentlichten Allgemeinen Nutzungsbedingungen zur Verarbeitung personenbezogener Daten im Auftrag in der Verwaltung (Allgemeine Nutzungsbedingungen Auftragsverarbeitungsverhältnis) grundsätzlich automatisch einbezogen werden. Hiergegen habe ich jedoch schwerwiegende datenschutzrechtliche Einwände erhoben. Insbesondere habe ich gefordert, dass die Formerfordernisse des Art. 28 Abs. 9 DSGVO an die Begründung von Auftragsverarbeitungsverhältnissen – schriftliche Abfassung, was auch in einem elektronischen Format möglich ist – nicht durch die Konstruktion eines „Rechtsverhältnisses", hinter dem sich wohl ein formloser konkludenter Vertrag verbergen sollte, umgangen werden dürfen. Besonders wichtig war mir insoweit aber auch wiederum der Hinweis, dass es nicht möglich ist, mittels Abstellen auf eine bloß tatsächliche Inanspruchnahme hinreichend transparent gemäß Art. 5 Abs. 2 DSGVO zu belegen, seit wann, inwieweit und für wie lange die jeweilige Auftragsverarbeitung tatsächlich mit Wissen und Wollen der Beteiligten im Einzelfall besteht.

In der Folgezeit wurde dieser Ansatz dann erfreulicherweise nicht weiter verfolgt. Stattdessen ist nun eine Regelung vorgesehen, welche ausdrücklich klarstellt, dass Auftragsverarbeitungsverhältnisse im staatlichen Bereich grundsätzlich weiterhin auf Basis **explizit geschlossener „klassischer" Verträge** erfolgen, soweit nicht vorrangige gesetzliche Regelungen (wie etwa der bereits erwähnte § 3a ZustVSt) exisitieren. Zwar halte ich die sich damit abzeichnende Divergenz zwischen der Auftragsverarbeitung in der Steuerverwaltung auf Basis des § 3a ZustVSt als „anderen Rechtsinstruments" und der im Übrigen vertraglichen Abwicklung nicht für besonders glücklich, da ein und derselbe Sachverhalt – Inanspruchnahme von IT-Dienstleistungen durch öffentliche Stellen – dann auf zwei grundverschiedenen Wegen gelöst wird. Diese Grundsatzfrage war von mir aber in spezifisch datenschutzrechtlicher Hinsicht letztlich nicht zu hinterfragen. Gefordert habe ich dagegen aber sehr wohl, Regelungen zu treffen, welche Beginn und Inhalt abgeschlossener Auftragsverarbeitungsverhältnisse transparent und rechtssicher ausgestalten sowie das Schicksal bereits bestehender Auftragsverarbeitungen festlegen. Dem in diesem Zusammenhang weiter verfolgten pragmatischen Ansatz, die Rechte und Pflichten der Parteien zukünftig regelmäßig mittels

(dynamischer) Allgemeiner Nutzungsbedingungen Auftragsverarbeitungsverhältnis zu regeln, bin ich nicht grundsätzlich entgegengetreten. Wichtig war mir insoweit aber, dass die inhaltlichen Anforderungen des Art. 28 DSGVO an Verträge über Auftragsverarbeitungen im Ergebnis vollumfänglich erfüllt werden. Da die Erarbeitung der Allgemeinen Nutzungsbedingungen Auftragsverarbeitungsverhältnis noch nicht abgeschlossen ist, werde ich gerade auch diesen Prozess in datenschutzrechtlicher Hinsicht weiterhin aufmerksam begleiten.

7.1.4 Zustimmung ist keine Einwilligung im Sinne der Datenschutz-Grundverordnung

Eine rechtmäßige Verarbeitung personenbezogener Daten ist gemäß Art. 6 Abs. 1 DSGVO nur auf Basis von an dieser Stelle enumerativ aufgezählten Rechtsgrundlagen möglich. Die Einwilligung stellt gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO eine solche Rechtsgrundlage dar. Die Einwilligung ist in Art. 4 Nr. 11 DSGVO legal definiert und in Art. 7 DSGVO inhaltlich weiter ausgeformt. Eine solche Einwilligung ist daher insbesondere nur wirksam, wenn sie freiwillig, informiert und unmissverständlich abgegeben wird. Wird der Begriff Einwilligung in einem Gesetz im datenschutzrechtlichen Sinne verwendet, müssen daher zunächst einmal die gerade erläuterten inhaltlichen Anforderungen erfüllt sein. Ergänzend legt Erwägungsgrund 43 DSGVO aber ganz generell eine zurückhaltende Verwendung der Einwilligung als Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch öffentliche Stellen nahe. Zudem ist die Möglichkeit öffentlicher Stellen, sich für ihr Verwaltungshandeln in zentralen Punkten ihrer Aufgabenerfüllung auf Einwilligungen von Bürgerinnen und Bürgern zu berufen, auch verfassungsrechtlich aus Gewaltenteilungsgründen stark eingeschränkt. Vielmehr müssen sich öffentliche Stellen für die Verarbeitung personenbezogener Daten in der Regel auf gesetzliche Befugnisse stützen können.

Ursprünglich hatte das Bayerische Digitalgesetz insoweit aber in großem Umfang die Einholung von Einwilligungen vorgesehen. Insoweit habe ich nachdrücklich auf die gerade eben erläuterten datenschutzrechtlichen Implikationen aufmerksam gemacht. Zwar habe ich durchaus Verständnis, wenn aus Transparenzgedanken beziehungsweise um die Freiwilligkeit für die Bürgerinnen und Bürger zu unterstreichen, eine positive Willensbekundung erwünscht ist. Jedoch sollte diese Willensbekundung aber anders benannt werden, um Verwechslungen mit der datenschutzrechtlichen Einwilligung von vornherein zu vermeiden. Derzeit zeichnet sich die Verwendung des Begriffs Zustimmung ab. Hiergegen habe ich keine Einwände erhoben, denn damit wird hinreichend klargestellt, dass es nicht um die Einholung von Einwilligungen als eigenständige Rechtsgrundlage für Datenverarbeitungen geht, sondern nur um eine zustimmende Willensbekundung von Bürgerinnen und Bürgern als Tatbestandsmerkmal beziehungsweise Voraussetzung einer Datenverarbeitung auf gesetzlicher Grundlage.

Das Gesetzgebungsverfahren zum Bayerischen Digitalgesetz werde ich auch insoweit weiterhin aufmerksam begleiten.

7.2 Leitfaden zum Outsourcing kommunaler IT

Das Thema IT-Outsourcing bei öffentlichen Stellen, das heißt die Auslagerung von Aufgaben und Verantwortung aus der eigenen IT-Abteilung an einen externen Dienstleister gegen Entgelt, beschäftigt mich seit geraumer Zeit, gerade auch im

kommunalen Bereich. Da ich aufgrund der Vielzahl an diesbezüglichen Anfragen und Beratungsbitten davon ausgegangen bin, dass Überlegungen hinsichtlich des Ob und Wie eines solchen IT-Outsourcings nicht nur einzelne Kommunen betreffen, sondern – wenn auch sicher graduell unterschiedlich – bayernweit von immer mehr Kommunen angestellt werden, habe ich einen übergreifenden Abstimmungsprozess zu Grenzen und Voraussetzungen des IT-Outsourings im kommunalen Bereich angestoßen (siehe hierzu bereits meinen 29. Tätigkeitsbericht 2019 unter Nr. 6.3). Die hierzu eingerichtete Arbeitsgruppe beim Bayerischen Staatsministerium des Innern, für Sport und Integration, an der neben mir auch der Bayerische Kommunale Prüfungsverband, das Bayerische Landesamt für Sicherheit in der Informationstechnik, der Bayerische Städtetag und der Bayerische Gemeindetag beteiligt waren, hat inzwischen einen detaillierten Leitfaden erarbeitet, welcher den Kommunen bei der Entscheidung helfen soll, ob und inwieweit ein IT-Outsourcing für sie in Frage kommt und was sie dabei beachten müssen. Dieser Leitfaden steht auf meiner Webseite https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Auftragsverarbeitung“ als PDF-Datei kostenfrei zum Download bereit.

7.2.1 Rechtliche Einbettung

Dieser Leitfaden ist in rechtlicher Hinsicht zunächst einmal vor dem Hintergrund zu sehen, dass die Kommunen im Rahmen des Art. 28 DSGVO Auftragsverarbeiter einschalten dürfen. Rechtmäßige Auftragsverarbeitungen sind rechtlich privilegiert: Für die Weitergabe personenbezogener Daten an den Auftragsverarbeiter sowie für die Verarbeitung durch diesen ist regelmäßig keine weitere Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO erforderlich als diejenige, auf die der Verantwortliche selbst die Verarbeitung stützt. Die Einholung von Einwilligungen betroffener Bürgerinnen und Bürger in eine Auftragsverarbeitung ist daher grundsätzlich nicht erforderlich, denn die Auftragsverarbeitung entspricht rechtlich dem Einsatz von eigenem Personal des Verantwortlichen. Ein Auftragsverarbeiter ist gerade kein Dritter gemäß Art. 4 Nr. 10 DSGVO. Jedoch müssen die Kommunen insbesondere auf eine sorgfältige Auswahl der Dienstleister achten. Nach Art. 28 Abs. 1 DSGVO darf nämlich nur ein Auftragsverarbeiter ausgewählt werden, der hinreichende Garantien für eine DSGVO-konforme Verarbeitung bietet.

Die von der Datenschutz-Grundverordnung bereitgestellte Auftragsverarbeitung ist jedoch nur ein abstraktes und damit neutrales rechtliches Modell. Auf die losgelöst hiervon zu beantwortende Rechtsfrage, ob und inwieweit von diesem Modell gerade auch für ein IT-Outsourcing im kommunalen Bereich Gebrauch gemacht werden darf, gibt Art. 28 DSGVO keine Antwort. Diese Antwort ist vielmehr außerhalb des Art. 28 DSGVO – in anderen Bestimmungen der Datenschutz-Grundverordnung sowie im nationalen Recht – zu suchen. Maßgeblich zu berücksichtigen ist hierbei, dass die Kommunen aufgrund ihrer breit gefächerten Zuständigkeiten Daten aus den verschiedensten fachlichen Bereichen verarbeiten – teilweise besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO oder Daten, die speziellen fachgesetzlichen Regelungen unterliegen, wie beispielsweise solche aus den Bereichen Meldewesen, Steuern, Personal-, Gesundheits- oder Sozialwesen. Sofern solche bereichsspezifischen Anforderungen bestehen, müssen diese auch im Rahmen der Auftragsverarbeitung beachtet werden. Zur Beurteilung der Frage, ob und inwieweit ein IT-Outsourcing im kommunalen Bereich zulässig ist, sind daher zunächst einmal die Wertungen des nationalen Fachrechts heranzuziehen. Daneben sind aber auch die in Art. 24, 25 und 32 DSGVO enthal-

tenen Pflichten des Verantwortlichen zu beachten, geeignete technisch-organisatorische Maßnahmen umzusetzen, um eine datenschutzkonforme Verarbeitung zu gewährleisten. Von maßgeblicher Bedeutung ist zudem die Wertung des Art. 33 Abs. 4 Grundgesetz, wonach die Ausübung hoheitsrechtlicher Befugnisse als ständige Aufgabe in der Regel Angehörigen des öffentlichen Dienstes zu übertragen ist, die in einem öffentlich-rechtlichen Dienst- und Treueverhältnis stehen.

Exemplarisch erläutern möchte ich dies anhand des Meldewesens: Im Hinblick auf das Führen des Melderegisters ergeben sich die Grenzen des IT-Outsourcings aus den melderechtlichen Vorgaben. Nach § 2 Abs. 2 Bundesmeldegesetz (BMG) in Verbindung mit Art. 1 Abs. 1 Satz 1 Bayerisches Gesetz zur Ausführung des Bundesmeldegesetzes (BayAGBMG) führen die Gemeinden als Meldebehörden zur Erfüllung ihrer Aufgaben das Melderegister.

§ 2 BMG
Aufgaben und Befugnisse der Meldebehörden
[…]
(2) Die Meldebehörden führen zur Erfüllung ihrer Aufgaben Melderegister. Diese enthalten Daten, die bei der betroffenen Person erhoben, von öffentlichen Stellen übermittelt oder sonst amtlich bekannt werden.
[…]

Art. 1 BayAGBMG
Meldebehörden
(1) [1]Meldebehörden sind die Gemeinden. 2Sie nehmen diese Aufgabe im übertragenen Wirkungskreis wahr. [2][…]

Das „Führen“ setzt dabei vom Ausgangspunkt her voraus, dass diese Aufgabe in der durch nichts eingeschränkten rechtlichen und faktischen Herrschaft der Meldebehörde erfüllt wird oder aber eine gemäß Art. 3 Abs. 1 BayAGBMG zulässige Übertragung von Aufgaben, die über eine Auftragsverarbeitung hinausgeht, vorliegt. Unterhalb der Schwelle der Aufgabenübertragung nach Art. 3 BayAGBMG besteht die Möglichkeit der Auftragsverarbeitung gemäß Art. 2 Abs. 1 BayAGBMG.

Art. 2 BayAGBMG
Auftragsverarbeitung
(1) [1]Verarbeitet ein Auftragsverarbeiter Meldedaten eines Einwohners für mehrere Meldebehörden, so kann er die Daten eines Einwohners in einem Datensatz speichern. [2]Dabei muss sichergestellt sein, dass die Meldebehörden auf diesen Datensatz nur im Rahmen ihrer Zuständigkeit zugreifen können.
[…]

Art. 3 BayAGBMG
Übertragung von Aufgaben der Datenverarbeitung
(1) Die Meldebehörden können Aufgaben der Meldedatenverarbeitung, die über eine Auftragsverarbeitung nach Art. 2 hinausgehen, auf andere Meldebehörden, auf Zweckverbände und gemeinsame Kommunalunternehmen oder auf die Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) übertragen.
[…]

Diese Vorschrift lässt darauf schließen, dass eine Auftragsverarbeitung auch bei Meldedaten die Speicherung der Daten von Einwohnerinnen und Einwohnern umfassen kann. Insoweit bestätigend legt die Allgemeine Verwaltungsvorschrift

zur Durchführung des Bundesmeldegesetzes (BMGVwV) in Nr. 2.2.1. unter anderem fest, dass zum Melderegister auch Einwohnerdatenbestände gehören, welche die Meldebehörden bei anderen Stellen im Rahmen der Auftragsdatenverarbeitung führen lassen. Da es sich hierbei um sensible Basisdaten insbesondere zur Identität und zu den Wohnungen von Einwohnerinnen und Einwohnern handelt, hat die für die Datenverarbeitung verantwortliche Gemeinde gerade auch im Falle einer Auslagerung des kompletten Datenbestandes diesem Umstand bei der Festlegung angemessener Sicherheitserfordernisse im Sinne der Art. 24, 25, 32 DSGVO sowie des Art. 28 DSGVO besonders Rechnung zu tragen. Sofern die Daten daher nicht in den Räumen der zuständigen Gemeinde verarbeitet und keine eigenen Speicherressourcen eingesetzt werden, ist besonderes Augenmerk auf die Datensicherheit zu legen.

Bei Erarbeitung des Leitfadens galt es, für die erläuterten abstrakten Gesichtspunkte bei den vielgestaltigen Facetten des kommunalen IT-Outsourcings eine in der Praxis handhabbare konkrete Form zu finden.

7.2.2 Erläuterung zentraler technisch-organisatorischer Kriterien

Im Folgenden sollen in komprimierter Form einige zentrale technisch-organisatorische Anforderung an Planung, Vergabe und Umsetzung eines kommunalen IT-Outsourcings dargestellt werden. Dabei wird zunächst eine mögliche Vorgehensweise vorgestellt, danach werden wichtige technische Aspekte betrachtet. Im Anschluss wird auf die speziellen Herausforderungen gerade für kleinere Kommunen eingegangen, die oftmals wegen nicht ausreichender personeller Ressourcen weiterer Unterstützung bedürfen. Abschließend finden sich Arbeitserleichterungen, wenn von Auftragsverarbeitern Sicherheitszertifikate oder Testate vorgelegt werden können.

7.2.2.1 Vorgehensweise

Vor Ausschreibung und Beauftragung eines IT-Outsourcings sind regelmäßig folgende Schritte durchzuführen, um den Pflichten eines Verantwortlichen adäquat nachzukommen:

— Schritt 1: Benennung technisch versierter Ansprechpartnerinnen und Ansprechpartner

  Zunächst bedarf es auf Seiten der öffentlichen Stelle technisch versierter Ansprechpartnerinnen und Ansprechpartner, welche die Planung und die Beauftragung beim IT-Outsourcing unterstützen, sowie idealerweise später als Ansprechpartnerinnen und Ansprechpartner für den Auftragsverarbeiter dienen.

— Schritt 2: Szenario

  Zur Planung der Auslagerung muss nun zunächst das Auslagerungsszenario so konkret wie möglich festgehalten werden. Dabei sind sowohl Art und Umfang der Auslagerung festzulegen, wie auch zu bestimmen, welche Datenkategorien davon betroffen sein sollen.

  Gängige IT-Outsourcing-Varianten sind beispielsweise:

1. Webhosting,

2. Betreuung der lokalen IT-Infrastruktur,

3. Rechenzentrumsbetrieb,

4. Betrieb Fachanwendungen (auch als Webanwendung).

Bis auf Variante 2 sind diese IT-Outsourcing-Varianten auch als Cloud-Auslagerungsszenarien denkbar. Allerdings entstehen mit der Auslagerung in die Cloud unter Umständen weitere Herausforderungen durch Cloud-spezifische Aspekte. Hierzu zählen beispielsweise die Verteilung auf mehrere Rechenzentren, deren Standorte und Beschäftigte unter Umständen weltweit verteilt sein können, oder der Betrieb durch eine Firma außerhalb des Geltungsbereichs der Datenschutz-Grundverordnung. Hierdurch ergeben sich weitere rechtliche und technische Herausforderungen. Diese sind nicht Gegenstand der aktuellen Fassung des Leitfadens. Dies schließt eine Cloud – Nutzung beim IT-Outsourcing nicht aus, erfordert allerdings zusätzlichen Aufwand auf Seiten der Kommune, um die Cloud – spezifischen Aspekte ebenfalls zu berücksichtigen. Die neuen Leitlinien des Europäischen Datenschutzausschusses (EDSA) zu Schrems II und neue Standarddatenschutzklauseln,[38] können bei diesen Cloud-spezifischen Herausforderungen unterstützen.

— Schritt 3: Schutzbedarf

Anhand der Daten, die ausgelagert werden sollen, muss der Schutzbedarf nach dem Maximalprinzip festgelegt werden. Somit ist, falls für eine Datenkategorie der Schutzbedarf als hoch ermittelt worden ist, der Schutzbedarf insgesamt, für alle damit zusammenhängenden Daten und/oder Verarbeitungsvorgänge, als hoch zu bewerten. Datenkategorien mit einem hohen Schutzbedarf sind aus der Sicht des Datenschutzes beispielsweise Daten nach Art. 9 DSGVO oder Daten, die spezialgesetzlichen Anforderungen unterliegen.

— Schritt 4: Datenschutz-Folgenabschätzung.

Da durch eine Auslagerung zu einem IT-Dienstleister die technischen Gegebenheiten verändert werden, muss anhand einer Erforderlichkeitsprüfung festgestellt werden, ob diese neuen Aspekte dazu führen, dass eine Datenschutz-Folgenabschätzung für die auszulagernden Verarbeitungen erforderlich wird.

— Schritt 5: Sorgfältige Auswahl des IT-Dienstleisters.

Für die sorgfältige Auswahl des Auftragsverarbeiters können mehrere Kriterien hilfreich sein. Unerlässlich ist ein ausführliches Sicherheitskonzept, das der Kommune vorgelegt werden muss. Hierbei hat die Kommune zu prüfen, ob die anzuwendenden Punkte des Anforderungskonzepts adäquat umgesetzt sind. Für gegebenenfalls fehlende Aspekte können vertragliche

[38] Internet: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en.

Zusatzvereinbarungen getroffen werden. Eine vorhandene Sicherheitszertifizierung, ein aktueller Bericht beziehungsweise ein Testat zu einem Sicherheitsaudit können zusätzlich bei der Auswahl unterstützen. Zukünftig können derzeit noch nicht vorhandene Zertifizierungen nach Art. 42 DSGVO oder genehmigte Verhaltensregeln nach Art. 41 DSGVO hilfreiche Werkzeuge darstellen.

7.2.2.2 Besonders hervorzuhebende technisch-organisatorische Aspekte

Der Anforderungskatalog listet neben den rechtlichen Gegebenheiten auch technische und organisatorische Maßnahmen auf, die bei der Beauftragung eines IT-Outsourcings zur Erreichung der IT-Sicherheitsziele von Vertraulichkeit, Verfügbarkeit und Integrität durch den Auftragnehmer zu ergreifen sind. Des Weiteren listet er Anforderungen auf, die erforderlich sind, um die notwendigen Rechenschaftspflichten zu erfüllen. Die dort gelisteten technischen Anforderungen stellen keinen abschließenden Prüfkatalog für die Prüfung der durch den Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen dar, sondern heben vielmehr die Anforderungen hervor, die auf Grund kommunaler Besonderheiten besondere Berücksichtigung bei einer (Teil-)Auslagerung der IT finden müssen.

Die Anforderungen beziehen sich hauptsächlich – aber nicht ausschließlich – auf das Szenario eines externen Rechenzentrumsbetriebs für Kommunen. Für andere Szenarien können Anforderungen nicht relevant sein oder auch weitere hinzukommen (etwa für die Auslagerung in die Cloud).

Die Anforderungen wurden zusammengestellt im Hinblick auf die Verarbeitung sensibler Bürgerdaten durch die Kommune, die jederzeit die Vertraulichkeit, aber auch den notwenigen Zugriff auf diese Daten sicherstellen muss. Im Katalog finden sich konkrete Anforderungen an die Technik, die dort kurz beschrieben sind. Es finden sich Anforderungen für einen normalen Schutzbedarf, aber auch Anforderungen, falls Daten mit hohem Schutzbedarf ausgelagert werden sollen. Die Anforderungen sind im Katalog dementsprechend gekennzeichnet. Zu jeder relevanten Anforderung muss der Dienstleister konkrete technische Maßnahmen vorweisen können. Gegebenenfalls ist es sinnvoll, dem Anbieter die Anforderungen vorzulegen, so dass dieser seine Maßnahmen hierzu erläutern kann.

Zu folgenden Aspekten finden sich Hinweise im Anforderungskatalog:

- Verfügbarkeit: Hierzu gehören unter anderem physischer Schutz der Gebäude, Räume und Rechner und Zugangssicherung zur Sicherstellung der Verfügbarkeit; Wiederherstellbarkeit und Ausfallsicherheit; Patchmanagement;

- Vertraulichkeit: Insbesondere Trennung der IT-Dienstleistungen; Datenverschlüsselung; Sicherstellung der Vertraulichkeit bei Backup und Datenarchivierung; Zugänge und Berechtigungen; Fremd- und Fernwartung;

- Integrität: beispielweise Protokollierung von Änderungen;

- Rechenschaftspflichten: unter anderem Zertifizierungen; Dokumentation IT-Sicherheits- und Datenschutzvorfälle, Audits/Kontrollen/Zugang, Penetrationstests.

Da es für IT-Dienstleister eher unüblich ist, Maßnahmen für den Fall der eigenen Insolvenz anzubieten, wird dieser Aspekt hier gesondert aufgegriffen: Die Kommune muss jederzeit sicherstellen können, dass sie auf die eigenen Daten Zugriff hat. Hierzu sind neben den üblichen Maßnahmen zum Ausfall von Servern oder auch der Kommunikationsleitung zum Anbieter die Aspekte einer möglichen Insolvenz zu berücksichtigen. Zur Absicherung für den Insolvenzfall gibt es mehrere Möglichkeiten, beispielsweise die Spiegelung der Daten der Gemeinde auf einem im Eigentum der Gemeinde befindlichen Server, der beispielsweise im Rechenzentrum des Anbieters, eines anderen Anbieters oder einem geeigneten Raums bei der Gemeinde untergebracht ist.

7.2.2.3 Unterstützung für kleinere Kommunen

Kleinere Kommunen fühlen sich eventuell auf Grund mangelnder personeller Ressourcen von den im IT-Outsourcing-Leitfaden formulierten Anforderungen auf den ersten Blick überfordert. Auf Grund der rechtlich normierten Verpflichtungen durch die Datenschutz-Grundverordnung und die oben genannten weiteren rechtlichen Regelungen, können kleinere Kommunen allerdings nicht völlig aus diesen Verpflichtungen entlassen werden. Um die notwendigen Schritte für ein IT-Outsourcing trotzdem durchführen zu können, sei auf die Möglichkeiten der kommunalen Zusammenarbeit wie beispielsweise der Zusammenschluss mehrerer Kommunen zur Gründung eines eigenen IT-Dienstleisters (etwa im Rahmen eines Zweckverbands oder gemeinsamen Kommunalunternehmens), auf die Nutzung eines bereits bestehenden kommunalen Rechenzentrums oder IT-Dienstleisters hingewiesen sowie auf die mögliche Zusammenarbeit mehrerer Kommunen, die denselben Dienstleister beauftragen wollen. Zudem sollten die Arbeitserleichterungen, die im folgenden Abschnitt erläutert werden, möglichst genutzt werden.

7.2.2.4 Arbeitserleichterungen

Soll ein IT-Dienstleister beauftragt werden, der nach der Norm ISO 27001[39] zertifiziert ist, so kann die Kommune dadurch den Aufwand, der sich durch die jährlich notwendige Kontrolle des Dienstleisters ergibt, deutlich reduzieren. Zu beachten ist allerdings, dass eine Zertifizierung nach dieser Norm zwar die Kontrollpflicht beim Auftraggeber reduziert, nicht aber von der sorgfältigen Auswahl des Dienstleisters befreit. Hierzu gehört nicht nur die Überprüfung, ob der Untersuchungsgegenstand der Zertifizierung anwendbar ist, sondern auch, dass gegebenenfalls weitere technische Anforderungen aus diesem Anforderungskatalog vertraglich zu vereinbaren sind.

Auf die Kontrollen der vom Dienstleister ergriffenen technisch-organisatorischen Maßnahmen selbst kann in diesem Fall verzichtet werden. Dies ist dadurch begründet, dass ein akkreditierter Auditor das Erstaudit sowie nach drei Jahren ein Rezertifizierungsaudit und zusätzlich jährliche Überwachungsaudits durchführt. Im Erstaudit überprüft der Auditor den Dienstleister zunächst im Rahmen einer Dokumentenprüfung formale und inhaltliche Aspekte des Informationssicherheitsmanagements (ISMS), danach erfolgt vor Ort die Prüfung der Umsetzung der in den Dokumenten niedergelegten Maßnahmen. Bei erfolgreicher Prüfung erfolgt die Ausstellung des Zertifikats. Im Rahmen des ersten und zweiten Überwachungsaudits wird im Wesentlichen auf Basis der Kenntnisse aus dem Erstaudit die Weiterentwicklung des ISMS geprüft. Hiermit soll sichergestellt werden, dass

[39] DIN EN ISO/IEC 27001:2017–06, erhältlich über https://www.beuth.de/de/norm/din-en-iso-iec-27001/269670716.

das ISMS wie dokumentiert während der gesamten Gültigkeitsdauert des Zertifikats betrieben wird. Nach drei Jahren erfolgt üblicherweise eine umfangreiche Rezertifizierung Im Rahmen der Rezertifizierung wird das Audit mit dem gleichen Vorgehen wie bei der Erstzertifizierung durchgeführt., der Auditor überprüft hierbei üblicherweise die Dokumente und die Umsetzung erneut, ohne dabei auf Wissen aus dem Erstaudit zurückzugreifen. Die Kommune muss damit bei einem nach dieser Norm zertifizierten Dienstleister lediglich überprüfen, ob eine Rezertifizierung durchgeführt wird. Entfällt die Rezertifizierung ist die Kommune wieder kontrollpflichtig.

Als weitere Arbeitserleichterung für die Auswahl des Dienstleisters wurde im Anhang des Anforderungskatalogs dargestellt, wie sich eine Zertifizierung des Dienstleisters nach ISO 27001 auf Basis von IT-Grundschutz und ein Testat eines Prüfers über die Einhaltung der BSI Cloud Computing Compliance Criteria Catalogue[40] (kurz: BSI C5)[41] arbeitserleichternd auf die Überprüfung der technischen Anforderungen auswirken kann. Hierbei wird dargestellt, ob Anforderungen zur Gänze, teilweise oder nicht erfüllt sind, wenn eine Zertifizierung nach ISO 27001 (mit IT-Grundschutz) oder ein Testat nach BSI C5 vorliegt. Die Anforderung „physischer Schutz der Gebäude, Räume und Rechner und Zugangssicherung zur Sicherstellung der Verfügbarkeit" ist beispielsweise bei beiden Standards zur Gänze erfüllt, wohingegen bei der Anforderung „Wiederherstellbarkeit und Ausfallsicherheit" weitere Betrachtungen der Anforderung notwendig sind. Der Anhang gibt hier konkrete noch offene Anforderungen an.

Für den Fall der Zertifizierung des IT-Dienstleisters nach ISO 27001 ist die Anwendung dieser Arbeitserleichterung jedoch nur möglich, falls der Untersuchungsgegenstand der Zertifizierung das geplante Auslagerungsszenario vollumfänglich – also auch mit dem notwendigen Schutzbedarf – umfasst. Dieser Untersuchungsgegenstand wird bei der Veröffentlichung des Zertifikats auf den Web-Seiten der jeweiligen Zertifizierungsstelle angegeben und ist dort nachlesbar.

7.3 Datenschutz im Standesamt: Unzulässigkeit einer regelhaften Anfertigung von Personalausweis- und Reisepasskopien bei der Anmeldung von Eheschließungen

In einem Standesamt fertigten Bedienstete regelmäßig Kopien der amtlichen Ausweisdokumente (Personalausweis, Reisepass) von Bürgerinnen und Bürgern, die dort wegen einer Eheschließung vorstellig wurden. Dadurch sollte bei einem Sachbearbeiterwechsel eine unproblematische Weiterarbeit erleichtert werden. Aus datenschutzrechtlicher Sicht habe ich diese Praxis wie folgt bewertet:

40 Siehe Bundesamt für Sicherheit in der Informationstechnik, Kriterienkatalog Cloud Computing C5, C5:2020, https://www.bsi.bund.de/c5.

41 Zur BSI C5 ist anzumerken, dass zwar die besonderen Herausforderungen der Cloud-Nutzung im Anforderungskatalog nicht berücksichtigt sind, der BSI C5 Standard aber viele Aspekte vorweist, die bei einer Auslagerung an sich relevant sind. Gibt es Cloud-Anbieter, die ausschließlich im Geltungsbereich der DSGVO agieren und ein BSI C5-Testat vorlegen können, so sind die wichtigsten Herausforderungen der Cloud-Nutzung gemeistert.

7.3.1 Fehlen einer gesetzlichen Befugnis für die Datenverarbeitung

Die Anfertigung und Speicherung von Kopien amtlicher Ausweise ist eine Verarbeitung personenbezogener Daten (vgl. Art. 4 Nr. 2 DSGVO), für deren Rechtmäßigkeit eine Rechtsgrundlage notwendig ist (vgl. Art. 6 Abs. 1 DSGVO). Öffentliche Stellen stützen sich bei ihren Datenverarbeitungen regelmäßig auf eine gesetzliche Verarbeitungsbefugnis. Nach Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 UAbs. 1 Buchst. b DSGVO werden solche Befugnisse im nationalen Recht geregelt. Da für die Datenverarbeitung keine (vorrangige) bereichsspezifische Rechtsgrundlage ersichtlich war (vgl. Art. 1 Abs. 5 BayDSG), kam als Verarbeitungsbefugnis allein **Art. 4 Abs. 1 BayDSG** in Betracht. Insoweit fehlte es aber an der **Erforderlichkeit** zur Aufgabenerfüllung.

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.
[…]

Das Standesamt hat nach dem Personenstandsgesetz (PStG) und der Verordnung zur Ausführung des Personenstandsgesetzes (PStV) die Aufgabe, die Eheschließung vorzubereiten, vorzunehmen und zu beurkunden. Welche Nachweise Eheschließende bei der Anmeldung der Eheschließung mittels öffentlicher Urkunden zu erbringen haben legt § 12 Abs. 2 PStG fest.

§ 12 PStG
Anmeldung der Eheschließung
[…]
(2) Die Eheschließenden haben bei der Anmeldung der Eheschließung durch öffentliche Urkunden nachzuweisen
1. ihren Personenstand,
2. ihren Wohnsitz oder gewöhnlichen Aufenthalt,
3. ihre Staatsangehörigkeit,
4. wenn sie schon verheiratet waren oder eine Lebenspartnerschaft begründet hatten, die letzte Eheschließung oder Begründung der Lebenspartnerschaft sowie die Auflösung dieser Ehe oder Lebenspartnerschaft. Ist die letzte Ehe oder Lebenspartnerschaft nicht bei einem deutschen Standesamt geschlossen worden, so ist auch die Auflösung etwaiger weiterer Vorehen oder Lebenspartnerschaften nachzuweisen, wenn eine entsprechende Prüfung nicht bereits von einem deutschen Standesamt bei einer früheren Eheschließung oder Begründung einer Lebenspartnerschaft durchgeführt worden ist.
[…]

Nr. 12.4.1 Allgemeine Verwaltungsvorschrift zum Personenstandsgesetz (PStG-VwV) sieht insoweit konkretisierend vor, dass insbesondere ein Reisepass oder Personalausweis oder ein sonstiger mit Lichtbild versehener amtlicher Ausweis zur Prüfung der Ehevoraussetzungen dienen kann. Korrespondierend bestimmt § 8 Abs. 1 Satz 1 PStV, dass zur Prüfung der deutschen Staatsangehörigkeit der Personalausweis oder der Reisepass oder eine erweiterte Bescheinigung der Meldebehörde, aus der sich die Staatsangehörigkeit ergibt, **vorzulegen** ist.

§ 8 PStV
Prüfung der Staatsangehörigkeit
(1) Zur Prüfung der deutschen Staatsangehörigkeit ist Folgendes vorzulegen:
1. der Personalausweis oder der Reisepass oder
2. eine erweiterte Bescheinigung der Meldebehörde, aus der sich die Staatsangehörigkeit ergibt.
Bestehen danach Zweifel an der deutschen Staatsangehörigkeit, ist eine Staatsangehörigkeitsurkunde vorzulegen.
[…]

Zur Prüfung des Vorliegens der Ehevoraussetzungen genügt jedoch die **Einsichtnahme** in den Personalausweis oder Reisepass und die Anfertigung eines Aktenvermerks hierüber oder die entsprechende Dokumentation in der Niederschrift über die Anmeldung der Eheschließung (vgl. Nr. 12.5.1 PStG-VwV). Dies korrespondiert mit den Vorgaben des § 4 Abs. 1 PStV.

§ 4 PStV
Rückgabe von Urkunden
(1) Von den Beteiligten vorgelegte Urkunden, die nicht ausdrücklich zur Vorlage beim Standesamt ausgestellt worden sind, sollen ihnen zurückgegeben werden. Von Urkunden, die nicht jederzeit wieder beschafft werden können, soll das Standesamt eine Abschrift oder Ablichtung zurückbehalten, die zu beglaubigen ist; bei Übertragung in ein elektronisches Dokument genügt ein Vermerk, der angibt, wann und durch wen die Übertragung vorgenommen worden ist.
[…]

Insbesondere kann auch § 4 Abs. 1 Satz 2 Halbsatz 1 PStV die regelmäßige Anfertigung von Kopien von Ausweisdokumenten **nicht** legitimieren, denn Personalausweis und Reisepass sind **keine Urkunden, die nicht jederzeit wieder beschafft werden können**. Das Standesamt kann sich im Bedarfsfall vielmehr **das jeweilige Ausweisdokument jederzeit wieder vorlegen** lassen.

7.3.2 Auch Einwilligung kein Mittel zur beliebigen Erweiterung der Datenerhebungsbefugnis

Soweit der mit einer Datenverarbeitung verbundene Eingriff im gesetzlich festgelegten Aufgabenbereich einer öffentlichen Stelle liegt, scheidet die Einholung von Einwilligungen der Antragstellerinnen und Antragsteller (vgl. Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO) zur Erweiterung gesetzlich beschränkter Befugnisse aus. Vielmehr müssen angesichts des verfassungsrechtlichen Gesetzesvorbehalts wesentliche Eingriffe in die Grundrechte der Bürgerinnen und Bürger vom (Parlaments-)Gesetzgeber geregelt werden. Bayerische öffentliche Stellen können daher personenbezogene Daten auf der Grundlage von **Einwilligungen nur in Ausnahmefällen** verarbeiten. Die Einwilligung stellt gerade kein Mittel dar, um öffentlichen Stellen pauschal die Möglichkeit zu geben, auch außerhalb ihrer gesetzlich festgelegten Befugnisse grundrechtsrelevant tätig zu werden. Dass dies gerade auch für die regelhafte Einholung von Einwilligungen in eine Anfertigung von Kopien amtlicher Ausweisdokumente gilt, habe ich bereits in meinem 29. Tätigkeitsbericht 2020 unter Nr. 5.6 ausführlich dargelegt.

7.3.3 Ergebnis

Die **regelmäßige Anfertigung von Kopien amtlicher Ausweisdokumente** durch Standesämter bei der Anmeldung von Eheschließungen ist auch bei Vorliegen entsprechender Einwilligungen der Betroffenen datenschutzrechtlich **nicht zulässig**.

7.4 Datenschutz im Standesamt: Unzulässigkeit einer regelhaften Betreuerinformation über die Anmeldung betreuter Personen zur Eheschließung

Ein Betreuerausweis legt offen, dass für den Betroffenen eine Betreuerin beziehungsweise ein Betreuer bestellt ist. Dem Betreuerausweis ist dagegen nicht zu entnehmen, ob und inwieweit die Betreffenden geschäftsunfähig sind. Der Gesetzgeber hat vielmehr die Betreuung in ihren Voraussetzungen bewusst von der Frage der Geschäftsunfähigkeit gelöst, so dass die Bestellung eines Betreuers auch für geschäftsfähige Personen in Frage kommt[42]. Durch eine bei mir eingereichte Beschwerde bin ich nun darauf aufmerksam geworden, dass Bedienstete eines Standesamts bei Kenntnis von der Existenz eines Betreuungsausweises regelmäßig die Betreuer von der Heiratsabsicht der Betreuten in Kenntnis gesetzt haben. Aus datenschutzrechtlicher Sicht habe ich dies wie folgt bewertet:

Die Mitteilung der Heiratsabsicht einer betreuten Person durch die Gemeinde an deren Betreuerin oder Betreuer stellt eine Übermittlung personenbezogener Daten an eine nichtöffentliche Stelle dar, für welche die Gemeinde eine Rechtsgrundlage benötigt (vgl. Art. 6 Abs. 1 DSGVO). Öffentliche Stellen sollen sich bei ihren Datenverarbeitungen grundsätzlich auf eine gesetzliche Verarbeitungsbefugnis stützen. Nach Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 UAbs. 1 Buchst. b DSGVO haben die Mitgliedstaaten die Möglichkeit, nationale Rechtsgrundlagen für die Verarbeitung personenbezogener Daten zu schaffen. Da für die geschilderte Datenverarbeitung keine (vorrangige) bereichsspezifische Rechtsgrundlage vorhanden war (vgl. Art. 1 Abs. 5 BayDSG), kam als Übermittlungsbefugnis allein **Art. 5 Abs. 1 BayDSG** in Betracht. Insoweit **fehlte** es allerdings an der **Erforderlichkeit** einer **regelmäßigen Datenübermittlung** an die Betreuer zur Aufgabenerfüllung des Standesamts (Art. 5 Abs. 1 Satz 1 Nr. 1 Var. 1 BayDSG). Auch die Voraussetzungen des Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG lagen schon deshalb nicht vor, da diese Norm nicht auf eine eigeninitiativ erfolgende pauschale regelhafte Übermittlung von Daten durch eine öffentliche Stelle an eine nichtöffentliche Stelle zugeschnitten ist. Die Norm setzt vielmehr zunächst voraus, dass die nicht-öffentliche Stelle zunächst ein berechtigtes Interesse glaubhaft macht. Bereits daran fehlte es.

Art. 5 BayDSG
Übermittlung
(1) [1]Eine Übermittlung personenbezogener Daten ist zulässig, wenn
1. sie zur Erfüllung einer der übermittelnden oder der empfangenden öffentlichen Stelle obliegenden Aufgabe erforderlich ist oder
2. der Empfänger eine nicht öffentliche Stelle ist, diese Stelle ein berechtigtes Interesse an ihrer Kenntnis glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat; dies gilt auch, soweit die Daten zu anderen Zwecken als denjenigen, zu denen sie erhoben wurden, übermittelt werden.

[42] Vgl. Müller-Engels, in: Hau/Poseck, BeckOK BGB, Stand 11/2020, § 1896 BGB Rn. 19 mit Hinweis auf Bundestags-Drucksache 11/4528, S. 60.

[2]Bei einer Übermittlung nach Satz 1 Nr. 2 darf der Empfänger die übermittelten Daten nur für den Zweck verarbeiten, zu dem sie ihm übermittelt wurden.

Das Standesamt hat nach dem Personenstandsgesetz (PStG) und der Verordnung zur Ausführung des Personenstandsgesetzes (PStV) die Aufgabe, die Eheschließung vorzubereiten, vorzunehmen und zu beurkunden. Hierbei hat das Standesamt zu prüfen, ob der Eheschließung ein Hindernis entgegensteht (vgl. § 13 Abs. 1 Satz 1 PStG). Zur Ehefähigkeit gehört auch die Geschäftsfähigkeit (vgl. §§ 1304, 104 Bürgerliches Gesetzbuch – BGB). **Jedoch begründet wie bereits eingangs dargestellt, die Bestellung eines Betreuers nicht notwendig die Geschäftsunfähigkeit der oder des Betreuten**. Dementsprechend bestimmt Nr. 13.2.4 Satz 1 Allgemeine Verwaltungsvorschrift zum Personenstandsgesetz (PStG-VwV), dass ein Volljähriger, für den ein Betreuer bestellt ist, die Ehe schließen kann, wenn er geschäftsfähig ist. Für die Willenserklärung zur Eingehung der Ehe **bedarf** er **nicht** der **Einwilligung des Betreuers** (vgl. Nr. 13.2.4 Satz 2 PStG-VwV).

Gleichwohl kann die Tatsache der Betreuung aber durchaus ein Indiz für das Fehlen der Geschäftsfähigkeit darstellen und daher **im Zusammenspiel mit hinzukommenden Auffälligkeiten** weitere eigene Ermittlungen des Standesamts rechtfertigen.[43] Vor diesem Hintergrund ist **bei weiteren Auffälligkeiten** auch eine **Anfrage** bei der Betreuerin oder dem Betreuer mit dem Zweck denkbar zu erfragen, ob dieser **Informationen im Hinblick auf eine etwaige Geschäftsunfähigkeit** der betreuten Person hat. Die bloße Kenntnis von der Betreuung einer sich zur Eheschließung anmeldenden Person berechtigt das Standesamt dagegen nicht, die Betreuerin oder den Betreuer regelhaft und ohne Vorliegen weiterer Auffälligkeiten über eine Anmeldung zur Eheschließung zu unterrichten.

7.5 Datenschutz im Standesamt: Verfahren bei Zweifeln an der Echtheit vorgelegter Urkunden

Im Berichtszeitraum wurde ich bei folgender Frage um datenschutzrechtliche Beratung gebeten: Darf sich das Standesamt bei seiner Beurkundungstätigkeit nach dem Personenstandsgesetz in Fällen, in denen Dokumente aus Herkunftsländern mit unsicherem Urkundswesen vorgelegt werden, hilfesuchend an das Ausländeramt wenden und gestützt auf die allgemeine Vorschrift des Art. 4 BayDSG Kopien der dort zu den betreffenden Personen vorhandenen ausländerrechtlichen Dokumente und Urkunden erheben? Hierzu habe ich aus datenschutzrechtlicher Sicht folgende Hinweise gegeben:

Welche Nachweise von Betroffenen für die Beurkundungstätigkeit des Standesamts vorzulegen sind, ist abschließend in den bereichsspezifischen Bestimmungen der §§ 9 ff. Personenstandsgesetz (PStG) geregelt. Exemplarisch ist hinsichtlich der Beurkundung von Eheschließungen auf §§ 12 Abs. 2, 13 Abs. 1 und 2 PStG und hinsichtlich des Erwerbs der deutschen Staatsangehörigkeit von Kindern ausländischer Eltern auf § 34 Abs. 1 und 2 Personenstandsverordnung (PStV) hinzuweisen.

43 Vgl. Gaaz, in: Gaaz/Bornhofen/Lammers, Personenstandsgesetz, 5. Aufl. 2020, § 13 Rn. 7.

§ 12 PStG
Anmeldung der Eheschließung
(1) Die Eheschließenden haben die beabsichtigte Eheschließung mündlich oder schriftlich bei einem Standesamt, in dessen Zuständigkeitsbereich einer der Eheschließenden seinen Wohnsitz oder seinen gewöhnlichen Aufenthalt hat, anzumelden. Hat keiner der Eheschließenden Wohnsitz oder gewöhnlichen Aufenthalt im Inland, so ist das Standesamt, vor dem die Ehe geschlossen werden soll, für die Entgegennahme der Anmeldung zuständig.
(2) Die Eheschließenden haben bei der Anmeldung der Eheschließung durch öffentliche Urkunden nachzuweisen

1. *ihren Personenstand,*
2. *ihren Wohnsitz oder gewöhnlichen Aufenthalt,*
3. *ihre Staatsangehörigkeit,*
4. *wenn sie schon verheiratet waren oder eine Lebenspartnerschaft begründet hatten, die letzte Eheschließung oder Begründung der Lebenspartnerschaft sowie die Auflösung dieser Ehe oder Lebenspartnerschaft. Ist die letzte Ehe oder Lebenspartnerschaft nicht bei einem deutschen Standesamt geschlossen worden, so ist auch die Auflösung etwaiger weiterer Vorehen oder Lebenspartnerschaften nachzuweisen, wenn eine entsprechende Prüfung nicht bereits von einem deutschen Standesamt bei einer früheren Eheschließung oder Begründung einer Lebenspartnerschaft durchgeführt worden ist.*

§ 13 PStG
Prüfung der Ehevoraussetzungen
(1) Das Standesamt, bei dem die Eheschließung angemeldet ist, hat zu prüfen, ob der Eheschließung ein Hindernis entgegensteht. Reichen die nach § 12 Abs. 2 vorgelegten Urkunden nicht aus, so haben die Eheschließenden weitere Urkunden oder sonstige Nachweise vorzulegen.
(2) Bestehen konkrete Anhaltspunkte dafür, dass die zu schließende Ehe nach § 1314 Abs. 2 des Bürgerlichen Gesetzbuchs aufhebbar wäre, so können die Eheschließenden in dem hierzu erforderlichen Umfang einzeln oder gemeinsam befragt werden; zum Beleg der Angaben kann ihnen die Beibringung geeigneter Nachweise aufgegeben werden. Wenn diese Mittel nicht zur Aufklärung des Sachverhalts führen, so kann auch eine Versicherung an Eides statt über Tatsachen verlangt werden, die für das Vorliegen oder Nichtvorliegen von Aufhebungsgründen von Bedeutung sind.

§ 34 PStG
Eheschließungen im Ausland oder vor ermächtigten Personen im Inland
(1) Hat ein Deutscher im Ausland die Ehe geschlossen, so kann die Eheschließung auf Antrag im Eheregister beurkundet werden; für den Besitz der deutschen Staatsangehörigkeit ist der Zeitpunkt der Antragstellung maßgebend. Die §§ 3 bis 7, 9, 10, 15 und 16 gelten entsprechend. Gleiches gilt für Staatenlose, heimatlose Ausländer und ausländische Flüchtlinge im Sinne des Abkommens über die Rechtsstellung der Flüchtlinge vom 28. Juli 1951 (BGBl. 1953 II S. 559) mit gewöhnlichem Aufenthalt im Inland. Antragsberechtigt sind die Ehegatten, sind beide verstorben, deren Eltern und Kinder.
(2) Die Beurkundung der Eheschließung nach Absatz 1 erfolgt auch dann, wenn die Ehe im Inland zwischen Eheschließenden, von denen keiner Deutscher ist, vor einer von der Regierung des Staates, dem einer der Eheschließenden angehört, ordnungsgemäß ermächtigten Person in der nach dem Recht dieses Staates vorgeschriebenen Form geschlossen worden ist.

In den in § 9 Abs. 2 PStG genannten Fällen kann das Standesamt zum Nachweis von für die Beurkundung erheblichen tatsächlichen Behauptungen der Betroffenen von diesen oder anderen Personen die Abnahme einer **Versicherung an Eides statt** verlangen.

§ 9 PStG
Beurkundungsgrundlagen
(1) Eintragungen in den Personenstandsregistern werden auf Grund von Anzeigen, Anordnungen, Erklärungen, Mitteilungen und eigenen Ermittlungen des Standesamts sowie von Einträgen in anderen Personenstandsregistern, Personenstandsurkunden oder sonstigen öffentlichen Urkunden vorgenommen.
(2) Ist den zur Beibringung von Nachweisen Verpflichteten die Beschaffung öffentlicher Urkunden nicht oder nur mit erheblichen Schwierigkeiten oder unverhältnismäßig hohen Kosten möglich, so können auch andere Urkunden als Beurkundungsgrundlage dienen. Sind auch diese nicht einfacher zu beschaffen als die erforderlichen öffentlichen Urkunden oder können die für die Beurkundung erheblichen tatsächlichen Behauptungen der Betroffenen weder durch öffentliche noch durch andere Urkunden nachgewiesen werden, so kann der Standesbeamte zum Nachweis dieser Tatsachen Versicherungen an Eides statt der Betroffenen oder anderer Personen verlangen und abnehmen.

Daneben können die bayerischen Standesämter gemäß § 22 Meldedatenverordnung (MeldDV**)** zur Erfüllung ihrer Aufgaben nach dem Personenstandsgesetz und der Personenstandsverordnung auch die dort aufgezählten Daten aus dem nach Art. 7 Abs. 1 Bayerisches Gesetz zur Ausführung des Bundesmeldegesetzes geschaffenen **zentralen Meldedatenbestand abrufen** (zum Umfang des Meldedatensatzes vgl. § 3 Bundesmeldegesetz).

§ 22 PStG
Datenübermittlungen an die Standesämter
Zur Erfüllung ihrer Aufgaben nach dem Personenstandsgesetz (PStG) und der Personenstandsverordnung (PStV) können die bayerischen Standesämter aus dem nach Art. 7 Abs. 1 BayAGBMG geschaffenen zentralen Meldedatenbestand folgende Daten automatisiert abrufen:

		Datenblätter:
1.	*Familienname*	*0101 bis 0106,*
2.	*frühere Namen*	*0201 bis 0206,*
3.	*Vornamen*	*0301, 0302,*
4.	*Doktorgrad*	*0401,*
5.	*Geburtsdatum und Geburtsort sowie bei Geburt im Ausland auch den Staat*	*0601 bis 0606,*
6.	*Geschlecht*	*0701,*
7.	*gesetzliche Vertreter*	
	a) Familienname	*0902 bis 0903,*
	b) Vornamen	*0904,*
	c) Doktorgrad	*0905,*
	d) Anschrift	*1200 bis 1212, 0907a,*
8.	*derzeitige Staatsangehörigkeiten*	*1001,*
9.	*derzeitige und frühere Anschriften (Haupt- und Nebenwohnung)*	*1200 bis 1213a,*
10.	*Einzugsdatum und Auszugsdatum*	*1301, 1306,*
11.	*Familienstand, bei Verheirateten oder Personen, die eine Lebenspartnerschaft führen, zusätzlich Datum*	*1401 bis 1409,*

	und Ort der Eheschließung oder der Begründung der Lebenspartnerschaft sowie bei Eheschließung oder Begründung der Lebenspartnerschaft im Ausland auch den Staat sowie bei einer Scheidung, Nichtigerklärung oder Aufhebung einer Ehe oder bei einer Aufhebung der Lebenspartnerschaft Datum und Grund der Beendigung der Ehe oder der Lebenspartnerschaft	
12.	*Ehegatte oder Lebenspartner*	
	a) Familienname	*1501 bis 1502, 1517 bis 1518,*
	b) Vornamen	*1503, 1519,*
	c) Doktorgrad	*1504, 1520,*
	d) derzeitige Anschrift (Hauptwohnung) im oder außerhalb des Zuständigkeitsbereichs der Meldebehörde	*1200 bis 1213a, 1508, 1524,*
	e) Geburtsdatum	*1505, 1521,*
	f) Sterbedatum	*1516, 1532,*
13.	*minderjährige Kinder*	
	a) Familienname	*1601 bis 1602,*
	b) Vornamen	*1603,*
	c) Geburtsdatum	*1604,*
	d) Sterbedatum	*1605,*
14.	*Sterbedatum und Sterbeort*	*1901, 1904, 1905.*

Alternativ können Standesämter in solchen Fällen, in denen sie die Echtheit vorgelegter ausländischer Urkunden bezweifeln, diese Frage in eigener Zuständigkeit und von Amts wegen **von den jeweiligen Auslandsvertretungen überprüfen lassen**.

Angesichts dieses spezialgesetzlich vorgezeichneten Umfangs zulässiger Datenumgänge bei der Beurkundungstätigkeit von Standesämtern besteht **kein Raum, Datenerhebungen durch das Standesamt beim Ausländeramt auf die Auffangnormen des Bayerischen Datenschutzgesetzes zu stützen.**

7.6 Nochmals: unberechtigte Zugriffe auf Meldedaten

Bereits in meinem 28. Tätigkeitsbericht 2018 unter Nr. 7.1 habe ich erläutert, wie dienstlich nicht veranlassten Meldedatenabfragen im Bayerischen Behördeninformationssystem (BayBIS) entgegengewirkt werden kann. Im Berichtszeitraum musste ich nun öffentliche Stellen mehrmals darauf hinweisen, dass Beschäftigte auch auf die behördeninternen Meldedatensätze nur insoweit zugreifen dürfen, wie es im Einzelfall für die Erfüllung der ihnen obliegenden Aufgaben erforderlich ist. Insoweit habe ich ausdrücklich darauf aufmerksam gemacht, dass die für das BayBIS bereits erläuterten Vorgaben zur Sicherstellung des Datenschutzes auch bei behördeninternen Zugriffen auf Meldedaten zu beachten sind. Diese Vorgaben erläutere ich nochmals wie folgt:

1. Der **Zugriff** auf Meldedaten durch Bedienstete ist im Rahmen eines Rechte- und Rollenkonzepts durch die jeweilige öffentliche Stelle zu **protokollieren**.

2. **Beschäftigte** mit Zugriff auf Meldedaten 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 Zugriffe protokolliert und unberechtigte Meldedatenabfragen insbesondere durch Stichproben (dazu nachfolgend 3.) entdeckt werden können. 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 hinsichtlich der Meldedaten an diese Rahmenbedingungen erinnert werden. Idealerweise geschieht dies im Rahmen einer **auffrischenden Schulung**. Alternativ kann aber auch ein Rundschreiben oder dergleichen verschickt werden. Die präventiven Maßnahmen sind zu dokumentieren (siehe Art. 5 Abs. 2 DSGVO).

3. In regelmäßigen Abständen (mindestens jährlich) sollten nicht angekündigte **Stichproben** erfolgen. Dabei sollte insbesondere auf ungewöhnlich häufige Meldedatenabfragen zu bestimmten Personen geachtet werden. Mit dieser Aufgabe können insbesondere Fachvorgesetzte oder behördliche Datenschutzbeauftragte betraut werden. Der Umfang hängt von der Zahl der Beschäftigten mit Zugang zu Meldedaten ab; er sollte gewährleisten, dass im Missbrauchsfall ein hinreichendes Entdeckungsrisiko besteht. Wenn sich zeigt, dass eine effektive Verhinderung von missbräuchlichen Abrufen nicht erreicht wird, sollten häufigere Stichproben durchgeführt werden.

Ich werde im Rahmen der Datenschutzaufsicht weiterhin darauf achten, dass bayerische öffentliche Stellen wirksame Maßnahmen zur Verhütung von „Neugierabfragen“ eigener Beschäftigter im Melderegister treffen.

7.7 Nochmals: Meldedatenübermittlung für Wahlwerbezwecke

Die im Berichtszeitraum stattfindenden bayerischen Kommunalwahlen führten erneut dazu, dass sich eine Reihe von öffentlichen Stellen, jedoch auch Bürgerinnen und Bürger wegen der Zulässigkeit einer Meldedatenübermittlung für Wahlwerbezwecke an mich wandten. Insoweit konnte ich regelmäßig auf meine anlässlich des Geltungsbeginns der Datenschutz-Grundverordnung aktualisierten Hinweise in meinem 28. Tätigkeitsbericht 2018 unter Nr. 7.8.1 verweisen. Dort hatte ich die gesetzliche Regelung des § 50 Abs. 1 Bundesmeldegesetz (BMG) zur Übermittlung von Meldedaten an politische Parteien zum Zwecke der Wahlwerbung erläutert. Dabei habe ich zudem die Möglichkeit dargestellt, wie Betroffene dieser Datenverarbeitung widersprechen können. Zusätzlich hatte ich zu diesem Thema rechtzeitig vor der Wahl eine Aktuelle Kurz-Information[44] veröffentlicht. Obwohl die Rechtslage damit an sich klar war, musste ich im Berichtszeitraum folgenden gravierenden Verstoß feststellen.

[44] Bayerischer Landesbeauftragter für den Datenschutz, Auskunft aus dem Melderegister an politische Parteien vor Wahlen, Aktuelle Kurz-Information 28, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Aktuelle Kurz-Informationen“.

Im Februar 2020 hatte eine politische Partei zu Wahlwerbungszwecken bei einer kreisfreien bayerischen Stadt beantragt, ihr ein Verzeichnis **aller** in der Stadt wahlberechtigten **Bürgerinnen und Bürger anderer Mitgliedstaaten der Europäischen Union nebst Staatsbürgerschaft** zu übersenden. In der Folge wurde die Wahlwerbung als Briefsendung vom damaligen Oberbürgermeister als Kandidat dieser Partei und einem weiteren Kandidaten dieser Partei – dem (damaligen) stellvertretenden Vorsitzenden des Migrations- und Integrationsbeirats – an über 3.000 EU-Ausländer, die in der Wahlwerbung namentlich angesprochen wurden, versandt. Die Wahlwerbung war dabei in sieben verschiedenen europäischen Sprachen verfasst. Anlässlich einer Beschwerde von betroffenen Personen bei mir habe ich die Stadt um Stellungnahme gebeten. Die Stadt teilte mir insoweit mit, eine Übermittlung der Staatsbürgerschaft im Rahmen des § 50 Abs. 1 BMG sei nach der gesetzlichen Formulierung „Gruppen von Wahlberechtigten" für zulässig erachtet worden. Dies sei vor dem Hintergrund der COVID-19-Pandemie nicht weiter hinterfragt worden.

Diesen Sachverhalt habe ich in datenschutzrechtlicher Hinsicht wie folgt bewertet:

Öffentliche Stellen benötigen für die Verarbeitung personenbezogener Daten eine Rechtsgrundlage (vgl. Art. 6 Abs. 1 DSGVO) und sollen Verarbeitungen bei der Erfüllung ihrer öffentlichen Aufgaben grundsätzlich auf ihre gesetzlichen Verarbeitungsbefugnisse stützen. **Melderegisterdaten sind dabei nach den spezialgesetzlichen Vorgaben des Bundesmeldegesetzes zu verarbeiten**.

Gemäß § 50 Abs. 1 Satz 1 BMG darf die Meldebehörde Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit Wahlen und Abstimmungen auf staatlicher und kommunaler Ebene in den sechs der Wahl oder Abstimmung vorangehenden Monaten **Auskunft** aus dem Melderegister **über die in § 44 Abs. 1 Satz 1 BMG bezeichneten Daten** von **Gruppen von Wahlberechtigten** erteilen, soweit für deren **Zusammensetzung das Lebensalter bestimmend** ist. Die Geburtsdaten der Wahlberechtigten dürfen dabei nicht mitgeteilt werden (§ 50 Abs. 1 Satz 2 BMG). In § 44 Abs. 1 Satz 1 BMG ist der Umfang der sog. einfachen Melderegisterauskunft geregelt:

§ 44 Abs. 1 Satz 1 BMG
Einfache Melderegisterauskunft
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.*

Für die erteilte Gruppenauskunft stand der Stadt danach **insgesamt** keine Rechtsgrundlage zur Verfügung. Der an sich in Betracht kommende § 50 Abs. 1 Satz 1 in Verbindung mit § 44 Abs. 1 Satz 1 BMG war **aus zwei Gründen** nicht einschlägig. Zum einen wurden die **Gruppen von Wahlberechtigten nicht anhand des Kriteriums „Lebensalter" gebildet**, sondern anhand der **Staatsangehörigkeit.** Daher fehlte bereits eine zentrale Voraussetzung für die Erteilung der Gruppenauskunft. Zum anderen gehört die **Staatsangehörigkeit** gerade **nicht** zu dem von § 44 Abs. 1 Satz 1 BMG umschriebenen **Auskunftsumfang**. Auch auf einen nach

dem Lebensalter der Wahlberechtigten gestellten Auskunftsantrag hin hätte dieses Merkmal daher nicht mitgeteilt werden dürfen.

Insgesamt war ein **Datenschutzverstoß** festzustellen**.** Diesem Verstoß kam auch ein **besonderes Gewicht zu**. Erstens war davon eine große Zahl von Personen betroffen. Zweitens hat die Stadt durch ihr datenschutzwidriges Handeln dem Empfänger im Ergebnis eine umfassende „EU-Ausländer-Kartei" zu ihrer Bewohnerschaft übermittelt. Ich habe daher gegenüber der Stadt einen Verstoß gegen datenschutzrechtliche Vorgaben **beanstandet** (Art. 16 Abs. 4 Satz 1 BayDSG).

8 Soziales und Gesundheit

8.1 Verhängung eines Bußgeldes gegenüber Sozialbehörden

Im Zusammenhang mit der Verhängung eines Bußgeldes gegen eine nicht in Bayern ansässige gesetzliche Krankenkasse durch eine Datenschutz-Aufsichtsbehörde ist an mich die Frage herangetragen worden, ob ich gegenüber einer meiner Zuständigkeit unterliegenden Krankenkasse bereits ebenfalls eine solche Sanktion ausgesprochen habe. Das habe ich aus folgenden Gründen verneint.

Gemäß § 85a Abs. 3 Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X) werden gegen Behörden und sonstige öffentliche Stellen keine Geldbußen bei Verstößen gegen die Datenschutz-Grundverordnung verhängt. Hiermit wurde von der Öffnungsklausel des Art. 83 Abs. 7 DSGVO Gebrauch gemacht, national zu regeln, ob und in welchem Umfang gegen Behörden und sonstige öffentliche Stellen Geldbußen verhängt werden können.[45] Folglich kann im Anwendungsbereich des Sozialgesetzbuches kein Bußgeld gegenüber den oben genannten Stellen verhängt werden.

Die in einem ersten Referentenentwurf für ein Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU[46] noch vorgesehenen Regelungen, wonach Kranken- und Pflegekassen – abweichend von § 85a Abs. 3 SGB X – jeweils mit Bußgeldern bei Verstößen gegen die Datenschutz-Grundverordnung hätten belegt werden können, sind im Laufe des Gesetzgebungsverfahrens wieder gestrichen worden.

Die Verhängung eines Bußgeldes gegenüber Sozialbehörden wäre allenfalls ausnahmsweise denkbar, und zwar für den Fall, dass sie keine Sozialdaten im Sinne von § 67 Abs. 2 Satz 1 SGB X verarbeiten, also außerhalb ihres gesetzlich vorgesehenen Aufgabenbereichs tätig werden würden; in diesem Fall käme § 85a Abs. 3 SGB X nicht zur Anwendung.[47] Für bayerische öffentliche Stellen würde dann Art. 22 BayDSG gelten.[48]

45 Siehe Begründung des Entwurfs eines Gesetzes zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften, Bundestags-Drucksache 18/12611, S. 123.

46 Siehe das Zweite Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680“ vom 20. November 2019, BGBl. I S. 1626.

47 So wohl Begründung der Entscheidung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg bezüglich der Verhängung eines Bußgeldes gegenüber der AOK Baden-Württemberg, siehe Pressemitteilung vom 30. Juni 2020, Internet: https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-bussgeld-gegen-aok-baden-wuerttemberg-wirksamer-datenschutz-erfordert-regelmaessige-kontrolle-und-anpassung.

48 Siehe vertiefend hierzu Bayerischer Landesbeauftragter für den Datenschutz, Geldbußen nach Art. 83 Datenschutz-Grundverordnung gegen bayerische öffentliche Stellen, Aktuelle Kurz-Information 17, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Aktuelle-Kurzinformationen“.

8.2 Einbeziehung Dritter in den Patientendatenbegriff

Aufgrund einer Eingabe habe ich mich mit der Frage befasst, inwiefern personenbezogene Daten Dritter in den Patientendatenbegriff miteinzubeziehen und wie sie datenschutzrechtlich zu behandeln sind.

Die betroffene Person, die sich an mich gewandt hat, begleitete einen Angehörigen zu einem Arztgespräch in einem Krankenhaus und nahm an dieser Besprechung teil. Im Rahmen des Gesprächs wurden nicht nur personenbezogene Daten des Patienten erhoben, sondern auch die Begleitperson machte Angaben zu ihrer Person und Gesundheit. Der Arzt verarbeitete die personenbezogenen Daten der Begleitperson im Rahmen eines Arztbriefes betreffend den Patienten, da es sich aus seiner medizinisch-fachlichen Sicht um für die Behandlung des Patienten relevante Angaben handelte. Der Arztbrief wurde einschließlich der personenbezogenen Daten der Begleitperson an die weiterbehandelnden Ärzte des Patienten verschickt.

Art. 27 Abs. 1 Satz 1 Bayerische Krankenhausgesetz (BayKrG) definiert den Begriff der Patientendaten. Danach sind Patientendaten alle Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Patienten aus dem Bereich der Krankenhäuser. Davon mitumfasst sind auch personenbezogene Daten von Angehörigen und anderen Bezugspersonen der Patientin oder des Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden.[49] Als Spezialvorschrift für den Krankenhausbereich weicht Art. 27 BayKrG insoweit von dem allgemeinen datenschutzrechtlichen Grundsatz ab, dass jede Person datenschutzrechtlich getrennt zu betrachten ist.

Eine Offenbarung von Patientendaten an Vor-, Mit- oder Nachbehandelnde ist zulässig, soweit das Einverständnis der Patienten anzunehmen ist, Art. 27 Abs. 5 Satz 2 BayKrG. Das BayKrG stellt insoweit bewusst auf den Patienten und nicht auf etwaig sonstige datenschutzrechtlich betroffene Personen ab.

Da der Patient in die Übermittlung seiner Behandlungsdaten und Befunde an die weiterbehandelnden Ärzte schriftlich eingewilligt hatte, stellte die Übersendung des Arztbriefes einschließlich der personenbezogenen Daten der Begleitperson keinen Datenschutzverstoß dar. Einer Einwilligung der Begleitperson bedurfte es dabei nicht.

Die Klinik hatte es jedoch versäumt, bei der Erhebung der personenbezogenen Daten der Begleitperson ihrer Informationspflicht nach Art. 13 DSGVO nachzukommen. Ich habe sie daher darauf hingewiesen, dass Art. 13 DSGVO bei anwesenden Bezugspersonen der Patientinnen und Patienten zu beachten ist und dass Begleitpersonen entsprechend über ihre Einbeziehung in die Anamnese zu informieren sind.

Da Art. 27 BayKrG bislang keine ausdrückliche Regelung zur Einbeziehung personenbezogener Daten Dritter in den Patientendatenbegriff enthält, sondern dies nur im Wege der Gesetzesauslegung erfolgt, erscheint eine entsprechende Klarstellung im Gesetzestext aus datenschutzrechtlicher Sicht als wünschenswert.

[49] Vgl. Landtags-Drucksache 10/9742, S. 23.

9 Personalverwaltung

9.1 Personalaktenrecht: Neuerungen für vertraglich Beschäftigte im bayerischen öffentlichen Dienst

Mit dem „Gesetz zur besseren Vereinbarkeit von Familie und Beruf sowie zur Änderung weiterer dienstrechtlicher Vorschriften“[50] hat der bayerische Gesetzgeber unter anderem das im Bayerischen Beamtengesetz (BayBG) geregelte **Personalaktenrecht** weiter modernisiert. Damit knüpft er an die Anpassungen an die Datenschutz-Grundverordnung durch das „Gesetz zur Änderung personalaktenrechtlicher und weiterer dienstrechtlicher Vorschriften“[51] an. Die aus datenschutzrechtlicher Sicht bedeutsamste Neuregelung enthält Art. 145 Abs. 2 BayBG, der das Personalaktenrecht für vertraglich Beschäftigte im bayerischen öffentlichen Dienst auf eine neue Grundlage stellt. Die Vorschrift lautet:

Art. 145 BayBG
Vertraglich Beschäftigte im öffentlichen Dienst
[…]
(2) Für Personen, die auf Grund eines Vertrages im Dienst einer der in Art. 1 Abs. 1 genannten juristischen Personen des öffentlichen Rechts stehen, gelten vorbehaltlich einer Regelung durch Tarifvertrag § 50 BeamtStG und Art. 103 bis 111 entsprechend; Art. 110 gilt mit der Maßgabe entsprechend, dass nicht durch Gesetz oder Tarifvertrag längere Fristen vorgesehen sind.

Die genannten § 50 Beamtenstatusgesetz (BeamtStG) und Art. 103 ff. BayBG betreffen in erster Linie das Personalaktenrecht der Beamtinnen und Beamten. Sie regeln neben Inhalt und Aufbau der Personalakten insbesondere auch Auskunftsrechte der Beschäftigten und enthalten Vorgaben zur Aufbewahrung und Vernichtung von Unterlagen. Die Geltung dieser detaillierten Vorschriften bedeutet für vertraglich Beschäftigte einen wesentlich transparenteren Datenschutz als bislang. Anders als das Beamtenrecht enthalten die Tarifverträge für den öffentlichen Dienst – über punktuelle Regelungen hinaus[52] – regelmäßig nämlich keine (ausdrückliche) Pflicht, Personalakten überhaupt zu führen, und deshalb auch keine (umfassenden) Vorgaben zu deren Inhalt, Gliederung oder Gestaltung, zur Aufnahme oder Entfernung von Vorgängen, zur Dauer der Aufbewahrung von Unterlagen oder zur elektronischen Aktenführung. Der Umgang mit diesen Fragen lag mangels gesetzlicher Grundlage daher grundsätzlich im Organisationsermessen des Arbeitgebers. Jetzt dagegen muss – entsprechend § 50 BeamtStG – auch für alle vertraglich im öffentlichen Dienst Beschäftigten zwingend eine vertraulich zu behandelnde Personalakte geführt werden, zu der alle Unterlagen gehören, die mit dem Beschäftigungsverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten). Wie bei den Beamtinnen und den Beamten kann die Personalakte nach sachlichen Gesichtspunkten in Grundakte und Teilakten gegliedert werden (vgl. Art. 104 Abs. 1 Satz 1 BayBG).

50 Vom 23. Dezember 2019 (GVBl. S. 724)

51 Vom 18. Mai 2018 (GVBl. S. 286), vgl. dazu meine Ausführungen im 28. Tätigkeitsbericht 2018 unter Nr. 12.1.

52 Beispielsweise in § 3 Abs. 6 Tarifvertrag für den öffentlichen Dienst der Länder.

Wichtig ist, dass Art. 145 Abs. 2 BayBG nicht nur das Personalaktenrecht der Beamtinnen und Beamten für anwendbar erklärt. Der für vertraglich Beschäftigte entsprechend geltende Art. 103 BayBG stellt generell die Verarbeitung personenbezogener Daten durch den Dienstherrn unter den Vorbehalt, dass sie zur Durchführung organisatorischer, personeller oder sozialer Maßnahmen erforderlich ist oder zu Rechnungsprüfungszwecken erfolgt. Dementsprechend gewährt Art. 107 Abs. 1 Satz 1 BayBG ein Auskunftsrecht nicht nur hinsichtlich der Personalakte, sondern allgemein für Akten, die personenbezogene Daten der Beschäftigten enthalten und für das Dienstverhältnis verarbeitet werden. Für die Verarbeitung personenbezogener Daten **im Tarifbeschäftigtenverhältnis gelten damit grundsätzlich die gleichen Bedingungen wie für Beamtinnen und Beamte**.

Allerdings können § 50 BeamtStG und Art. 103 ff. BayBG auf vertraglich Beschäftigte nicht unbesehen übertragen werden, da sich die Beschäftigungsverhältnisse von Beamtinnen und Beamten einerseits und vertraglich Beschäftigten andererseits in mancherlei Hinsicht grundlegend unterscheiden. Eine entsprechende Anwendung setzt jedoch eine vergleichbare Interessenlage der Beschäftigtengruppen voraus. Deshalb ist jeweils zu prüfen, ob und wie eine der beamtenrechtlichen Regelungen „entsprechend" für vertraglich Beschäftigte anzuwenden ist. Je ähnlicher die Lage von vertraglich beschäftigten Personen mit der Situation von Beamtinnen oder Beamten ist, desto eher ist eine beamtenrechtliche Regelung auf vertraglich Beschäftigte anwendbar. Soweit sich Beamten- und Tarifbeschäftigtenverhältnis dagegen wesentlich unterscheiden, können die beamtenrechtlichen Vorschriften nicht übertragen werden. Das ist offensichtlich bei den personalaktenrechtlichen Beihilferegeln (vgl. Art. 105 BayBG), da vertraglich Beschäftigte in der Regel keine Beihilfe erhalten. Die entsprechenden Regelungen können auf vertraglich Beschäftigte daher nur dann angewendet werden, wenn sie ausnahmsweise beihilfeberechtigt sind. Ebenso gelten im Tarifbeschäftigtenbereich mitunter längere als die beamtenrechtlichen Aufbewahrungsfristen. Dementsprechend ordnet Art. 145 Abs. 2 BayBG ausdrücklich an, dass Art. 110 BayBG, der Fristen für die Aufbewahrung der Personalakten von Beamtinnen und Beamten regelt, nur mit der Maßgabe entsprechend gilt, dass nicht durch Gesetz oder Tarifvertrag längere Fristen vorgesehen sind. Das betrifft vor allem Unterlagen zu Ansprüchen auf Altersversorgung im öffentlichen Dienst bei der Versorgungsanstalt des Bundes und der Länder, die erst nach 30 Jahren verjähren (vgl. § 18a Betriebsrentengesetz – BetrAVG).

In anderen Konstellationen ist es dagegen nicht so einfach zu beurteilen, ob und wie die beamtenrechtlichen Regelungen für vertraglich Beschäftigte passen. Auch wenn ich Art. 145 Abs. 2 BayBG die klare Tendenz entnehme, die beamtenrechtlichen Regeln anzuwenden, bin ich in der Beratungspraxis auf die nachstehend behandelten Fragen gestoßen, die eine nähere Betrachtung fordern.

9.1.1 Betroffener Personenkreis

Art. 145 Abs. 2 BayBG erstreckt den beamtenrechtlichen Beschäftigtendatenschutz auf „Personen, die auf Grund eines Vertrages im Dienst einer der in Art. 1 Abs. 1 [BayBG] genannten juristischen Personen des öffentlichen Rechts stehen". Das betrifft Beschäftigte des Staates, der Gemeinden, der Gemeindeverbände und der sonstigen unter der Aufsicht des Staates stehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts und damit die **vertraglich im öffentlichen Dienst Beschäftigten** (vgl. auch die Definition des öffentlichen

Diensts in § 130 Betriebsverfassungsgesetz). Erfasst werden dabei nicht nur Personen, die auf arbeitsvertraglicher Grundlage tätig werden, denn auch sogenannte Honorarkräfte (**freie Mitarbeiter**) werden auf Grundlage eines (Dienst-) Vertrags tätig und können somit „auf Grund eines Vertrages" im Dienst einer der in Art. 1 Abs. 1 BayBG genannten Stellen stehen. Auch sie umfasst Art. 145 Abs. 2 BayBG. Für den ganz überwiegenden Teil der bei bayerischen öffentlichen Stellen Beschäftigten gilt deshalb – nunmehr ausdrücklich – ein weitgehend einheitlicher Beschäftigtendatenschutz.

Gleichwohl erfasst Art. 145 Abs. 2 BayBG nicht alle Beschäftigten im öffentlichen Umfeld. Da die Vorschrift nur für den in Art. 1 Abs. 1 BayBG angesprochenen öffentlichen Dienst gilt, betrifft sie **nicht Beschäftigte bei privatrechtlich organisierten Unternehmen**, etwa einer kommunalen GmbH. Nicht unter die Neuregelung fallen auch **ehrenamtliche Mitarbeiterinnen und Mitarbeiter** des als Körperschaft des öffentlichen Rechts organisierten Bayerischen Roten Kreuzes, da diese nicht auf Grundlage eines Dienst- oder Arbeitsvertrags tätig sind.

Auch **Bewerberinnen und Bewerber** für ein Dienstverhältnis sind (noch) nicht auf der Grundlage eines Vertrags tätig. Fraglich ist daher, ob ebenso wie bei Bewerberinnen für Beamtinnenstellen und Bewerbern für Beamtenstellen die Art. 103 ff. BayBG für Bewerberinnen und Bewerber auf Tarifbeschäftigtenstellen entsprechend gelten. Nach meiner Einschätzung strebt der Gesetzgeber bei vergleichbarer Interessenlage einen weitgehenden Gleichlauf der datenschutzrechtlichen Regelungen der Beamtinnen, Beamten und vertraglich Beschäftigten an. Deshalb gehe ich davon aus, dass im Ergebnis die gleichen datenschutzrechtlichen Anforderungen für den Umgang mit Daten von Bewerberinnen und Bewerbern gelten sollen, gleich ob sie sich für eine Einstellung im Beamten- oder im Tarifbeschäftigtenverhältnis bewerben.

9.1.2 Recht auf Einsicht in die Personalakte, insbesondere auf Kopien

Unterschiede zwischen den Beschäftigtengruppen im öffentlichen Dienst können – jedenfalls bei strenger Auslegung der tariflichen Vereinbarungen – beim Recht auf Einsicht in die Personalakte bestehen. Hintergrund ist, dass Art. 145 Abs. 2 BayBG die beamtenrechtlichen Rechte für vertraglich Beschäftigte unter den Vorbehalt sonstiger Regelungen stellt. Anders als das Beamtenrecht, das den Beamtinnen und Beamten ein sehr weitgehendes Recht auf Einsicht in die Personalakte und grundsätzlich auch auf Überlassung einer vollständigen Kopie gewährt (vgl. Art. 107 Abs. 4 BayBG), räumen tarifvertragliche Regelungen den Beschäftigten neben dem Einsichtsrecht regelmäßig nur das Recht ein, Auszüge oder Kopien „aus" ihren Personalakten zu verlangen (vgl. etwa § 3 Abs. 6 Satz 1 bis 3 Tarifvertrag für den öffentlichen Dienst der Länder – TV-L). Dieses Recht wird vielfach so verstanden, dass die vertraglich Beschäftigten nur Kopien einzelner Unterlagen, aber nicht der gesamten Personalakte fordern können.

Derartige Unterschiede zwischen den Beschäftigtengruppen werden durch die Neuregelung nicht beseitigt. Der Gesetzgeber will – wie der Vorbehalt für tarifvertragliche Regelungen zeigt – mit Art. 145 Abs. 2 BayBG die tariflichen Vereinbarungen nicht auf das beamtenrechtliche Niveau anheben. Dafür spricht auch die Gesetzesbegründung, der zufolge die Anwendung der beamtenrechtlichen Regeln in erster Linie den übertariflich bezahlten Beschäftigten im öffentlichen

Dienst diene,[53] die sich auf tarifvertragliche Regelungen grundsätzlich nicht berufen können (vgl. etwa § 1 Abs. 2 TV-L).

Wenn der Gesetzgeber für diese Gruppe von Beschäftigten aber die Anwendung der im Einzelfall gegenüber tariflichen Regelungen weitergehenden beamtenrechtlichen Regeln festlegen möchte, kann ich aus Datenschutzsicht keinen nachvollziehbaren Grund dafür erkennen, die übertariflich Bezahlten etwa mit Blick auf das Recht auf Überlassung einer Kopie der Personalakte gegenüber den Tarifbeschäftigten zu bevorzugen und nur ihnen das gleiche Einsichtsrecht einschließlich Kopie-Anspruch wie den Beamtinnen und den Beamten zuzugestehen. Ein Ausweg könnte darin liegen, dass die bayerischen öffentlichen Stellen die tarifvertraglichen und sonstigen Regeln über die Einsichtsrechte nicht eng auslegen und das Recht auf Auszüge oder Kopien nicht auf Teile der Personalakte beschränken, sondern sich – unabhängig vom jeweiligen Beschäftigtenstatus – zu Gunsten aller vertraglich Beschäftigten an den beamtenrechtlichen Maßstäben orientieren.

9.1.3 Entfernung nachteiliger Unterlagen, insbesondere von Abmahnungen, aus der Personalakte

Gewisse Unklarheiten der Neuregelung haben sich im Zusammenhang mit der Entfernung und Vernichtung nachteiliger Unterlagen aus der Personalakte gezeigt. Für Beamtinnen und Beamte regelt diese Fragen primär Art. 109 BayBG. Gemäß Art. 109 Abs. 1 Satz 1 Nr. 1 BayBG gilt der Grundsatz, dass unzutreffende Unterlagen über Beschwerden, Behauptungen und Bewertungen mit Zustimmung des Beamten oder der Beamtin unverzüglich aus der Personalakte entfernt und vernichtet werden. Treffen die Beschwerden, Behauptungen oder Bewertungen dagegen zu, können die Unterlagen erst nach zwei Jahren entfernt und vernichtet werden (vgl. Art. 109 Abs. 1 Satz 1 Nr. 2 BayBG). Das steht jedoch unter dem Vorbehalt, dass nicht – wegen der Schwere der Verfehlung – vorrangig die Vorschriften des Disziplinarrechts anzuwenden sind. Unterlagen über Disziplinarverfahren werden bis zum Ablauf der in § 17 Abs. 1 und 3 Bayerisches Disziplinargesetz (BayDG) genannten Fristen in der Personalakte aufbewahrt; die Aufbewahrungsfrist richtet sich nach der konkret verhängten Disziplinarmaßnahme und beträgt zwischen drei und sieben Jahren. Praktisch bedeutet dies, dass bei Beamtinnen und Beamten die Unterlagen über schwerere, nämlich disziplinarrechtlich relevante, Verfehlungen länger aufbewahrt werden als Unterlagen über weniger schwere Vorfälle.

Da für vertraglich Beschäftigte das Disziplinarrecht von vornherein nicht gilt (vgl. Art. 1 Abs. 1 BayDG), kann sich der in Art. 109 BayBG geregelte Vorbehalt zugunsten der längeren Aufbewahrungsfristen des Disziplinarrechts nicht realisieren. Unterlagen über Verfehlungen der vertraglich Beschäftigten wären daher – unabhängig von deren Schwere – bei wortlautgetreuer Anwendung von Art. 109 Abs. 1 Satz 1 Nr. 2 BayBG auf vertraglich Beschäftigte immer nach zwei Jahren aus der Personalakte zu entfernen und zu vernichten. Das wäre bei schwereren Verfehlungen zum einen eine Besserstellung gegenüber Beamtinnen und Beamten in vergleichbaren Fällen. Darüber hinaus bedeutete dieses Verständnis eine erhebliche Verbesserung gegenüber der bislang in der Rechtsprechung vorherrschenden Meinung, dass etwa Abmahnungen von Beschäftigten nach arbeitsrechtlichen Grundsätze regelmäßig erst dann aus der Personalakte entfernt werden

[53] Vgl. Landtags-Drucksache 18/3922, S. 28.

müssen, wenn sie in jeder Hinsicht, etwa zur Beurteilung der charakterlichen Eignung für eine Beförderung, bedeutungslos geworden sind, wobei dieser Zeitraum deutlich mehr als zwei Jahre dauern kann.[54]

Diese Thematik kann insbesondere im Zusammenhang mit der Stellensuche bedeutsam werden, wenn der neue öffentliche Arbeitgeber – wie weithin auch bei Tarifbeschäftigten üblich – Einsicht in die Personalakte erbittet. Die nicht hinterfragte Anwendung von Art. 109 BayBG könnte auch bei schweren Verfehlungen, die gerade noch nicht zur Kündigung ausreichen, dazu führen, dass entsprechende Unterlagen nach relativ kurzer Zeit aus der Personalakte zu entfernen wären. Aus der Gesetzesbegründung ergibt sich jedenfalls nicht, dass der Gesetzgeber diese Konsequenz beabsichtigt hat und die vertraglich Beschäftigten hinsichtlich der Aufbewahrung von Abmahnungen und ähnlichen Unterlagen gegenüber der bisherigen Rechtslage deutlich besser stellen wollte.

9.1.4 Bewertung und Ausblick

Da die Interessen von Beamtinnen, Beamten und Tarifbeschäftigten an einer datenschutzkonformen Personalaktenführung weitestgehend gleich gerichtet sind, habe ich schon lange nachdrücklich die Auffassung vertreten, dass – vorbehaltlich tarifvertraglicher und sonstiger Sonderregeln – die beamtenrechtlichen Vorschriften über die Personalaktenführung als allgemein gültige Schutzvorschriften für alle öffentlichen Bediensteten grundsätzlich auch im Tarifbereich zu beachten sind.[55] Nunmehr hat der bayerische Gesetzgeber ausdrücklich anerkannt, dass die entsprechende Anwendung der beamtenrechtlichen Personalaktenvorschriften für vertraglich Beschäftigte im öffentlichen Dienst „unumgänglich“ ist.[56] Ich sehe die Neuregelung daher auch als Ergebnis meines langen Beharrens.

Auch wenn die nun geschaffene Regelung, wie gezeigt, einige Fragen noch nicht abschließend klärt, bis ich sicher, dass diese in der Praxis – wie bislang auch –datenschutzrechtskonform und sachgerecht gelöst werden können. Nichtsdestotrotz würde ich es begrüßen, wenn der Gesetzgeber bei nächster Gelegenheit nachjustieren und die aufgeworfenen Fragen klarstellen würde.

Noch nicht durchdringen konnte ich mit meinem Anliegen, den Beschäftigtendatenschutz mit einem **Mitbestimmungsrecht des Personalrats bei der Benennung des behördlichen Datenschutzbeauftragten** weiter zu stärken. Dieser wird bislang allein durch den Verantwortlichen, regelmäßig die Leiterin oder den Leiter der Dienststelle, benannt. Der Datenschutzbeauftragte soll jedoch gerade auch für die Beschäftigten ein unabhängiger Ansprechpartner in datenschutzrechtlichen Fragen sein, vor allem bei datenschutzrechtlichen Konflikten mit dem Dienstherrn. Eine Einbindung des Personalrats in das Verfahren der Benennung des behördlichen Datenschutzbeauftragten könnte dessen Legitimation und das ihm von den betroffenen Beschäftigten entgegengebrachte Vertrauen maßgeblich steigern, da der Eindruck vermindert würde, er stünde einseitig im Lager der Dienststellenleitung. Für eine entsprechende Neuregelung werde ich mich in meinen Gesprächen mit dem Gesetzgeber und der Staatsregierung weiterhin einsetzen.

54 Vgl. Bundesarbeitsgericht, Urteil vom 19. Juli 2012, 2 AZR 782/11, BeckRS 2012, 76055.

55 Regelmäßig seit meinem 18. Tätigkeitsbericht 1998 unter Nr. 12.2.

56 Vgl. Landtags-Drucksache 18/3922, S. 28.

9.2 Beschäftigten-Geburtstagslisten bei bayerischen öffentlichen Stellen

Geburtstage von Beschäftigten geben in vielen bayerischen öffentlichen Stellen immer wieder Anlass zu einer Gratulation, zum Mitbringen eines Geburtstagskuchens oder zur Entgegennahme eines angemessen großen Stücks davon. Geburtstage werden wahrgenommen – von Kolleginnen und Kollegen, Vorgesetzten, Mitarbeiterinnen und Mitarbeitern. Sie sind Gegenstand sozialer Erwartungen.

Oftmals entstehen in den Dienststellen Geburtstagslisten, die von allen Beschäftigten in einer Organisationseinheit eingesehen werden können und so für das als notwendig empfundene Maß an Transparenz sorgen. Solche Geburtstaglisten enthalten für jede eingetragene Person außer dem Namen zumindest das Datum, häufig auch das Jahr des Geburtstags. Aus datenschutzrechtlicher Sicht ist insofern zu bemerken:

9.2.1 Verantwortlichkeit

Verantwortlicher ist nach Art. 4 Nr. 7 Halbsatz 1 DSGVO die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Eine Beschäftigten-Geburtstagsliste wird entweder auf dienstliche Veranlassung oder in „Eigenregie“ durch die Mitarbeiterinnen und Mitarbeiter geführt.

Die Verantwortlichkeit einer bayerischen öffentlichen Stelle für eine dort vorgehaltene Beschäftigten-Geburtstagsliste ist jedenfalls begründet, wenn

— Vorgesetzte die Liste führen oder dies veranlassen,

— Vorgesetzte auf eine Eintragung in der Liste hinwirken oder sonst Eintragungsanreize schaffen oder

— die Liste von der Personalstelle mit den nötigen Daten beschickt wird.

Die nachfolgenden Hinweise betreffen Beschäftigten-Geburtstagslisten, die von einer bayerischen öffentlichen Stelle als Verantwortlichem geführt werden.

9.2.2 Beschäftigten-Geburtstagsliste und Personaldatenschutz

Die Führung einer Beschäftigten-Geburtstagsliste, die Beschäftigten außerhalb der personalverwaltenden Stelle zugänglich ist, findet keine Rechtfertigung in Art. 103 Satz 1 Nr. 1 Bayerisches Beamtengesetz (BayBG). Diese Vorschrift fungiert als grundlegende Verarbeitungsbefugnis für den Bereich der Personalstellen; sie ist Rechtsgrundlage im Sinne von Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 UAbs. 1 Buchst. b DSGVO und gilt nicht nur für die Beamtinnen und Beamten, sondern gemäß Art. 145 Abs. 2 BayBG grundsätzlich auch entsprechend für Tarifbeschäftigte bei bayerischen staatlichen Behörden und staatsmittelbaren Rechtsträgern.

Nach Art. 103 Satz 1 Nr. 1 BayBG darf der Dienstherr Personaldaten verarbeiten, soweit dies zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere zu Zwecken der Personalverwaltung oder Personalwirtschaft erforderlich ist.

Die Führung von Beschäftigten-Geburtstagslisten, die innerhalb einer „behördeninternen Öffentlichkeit" eingesehen werden können, ermöglicht die Gratulation in der jeweiligen Organisationseinheit und gegebenenfalls ein anlassbezogenes Gemeinschaftserlebnis. Bei alldem handelt es sich um Akte der kollegialen Beziehungspflege, nicht aber um vom Dienstherrn zu veranlassende organisatorische, personelle oder soziale Maßnahmen.

9.2.3 Einwilligung als Rechtsgrundlage

Vor diesem Hintergrund kommt als Rechtsgrundlage für Verarbeitungen im Zusammenhang mit Beschäftigten-Geburtstagslisten nur die Einwilligung (Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO) in Betracht. Unter dem Aspekt der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) sollte die „Neuaufnahme" in eine Liste grundsätzlich auf Tag und Monat beschränkt, auf die – von nicht wenigen Menschen als sensibler empfundene – Angabe des Geburtsjahres hingegen verzichtet werden.

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".[57]

Eine 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).

Die öffentliche Stelle muss die Einwilligung im Rahmen ihrer Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) nachweisen können (Art. 7 Abs. 1 DSGVO).

9.2.4 Verzeichnis der Verarbeitungstätigkeiten

Eine Verarbeitungstätigkeit mit dem Zweck „Führen von Beschäftigten-Geburtstagslisten" gehört auch in das Verzeichnis der Verarbeitungstätigkeiten. Rechtsgrundlage für diese Verarbeitungstätigkeit ist Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO. Betroffene Personen sind die Beschäftigten, die ihre Geburtsdaten in die Liste einpflegen oder einpflegen lassen. Zu den Kategorien personenbezogener Daten zählen regelmäßig der Name und der Vorname sowie das Geburtsdatum. Kategorien (dritter) Empfänger können bei einer internen Liste außer Betracht bleiben. Die Löschfrist ist an die Zugehörigkeit der betroffenen Person zu der Organisationseinheit gekoppelt, für welche die Beschäftigten-Geburtstagsliste ge-

[57] Bayerischer Landesbeauftragter für den Datenschutz, Die Einwilligung nach der Datenschutz-Grundverordnung, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Einwilligung".

führt wird. Ein Eintrag ist zu löschen, wenn die betroffene Person diese Funktionseinheit – auch durch Umsetzung innerhalb einer Behörde – verlässt oder die Einwilligung widerruft. Der Verzeichniseintrag sollte so gefasst werden, dass er alle bei der öffentlichen Stelle geführten Beschäftigten-Geburtstagslisten abdeckt.

9.2.5 Informationspflichten

Die in einer Beschäftigten-Geburtstagsliste typischerweise enthaltenen Daten befinden sich regelmäßig bereits in der Sphäre des Verantwortlichen, weil sie zum Grundbestand an Beschäftigtendaten gehören. Die Nutzung von Name und Geburtsdatum im Rahmen einer Beschäftigten-Geburtstagsliste lässt sich als eine Weiterverwendung deuten, welche die Informationspflicht nach Art. 13 Abs. 3 DSGVO auslöst.

Im Regelfall werden die erforderlichen Informationen bereits durch die zu Beginn eines Beschäftigungsverhältnisses angezeigten Datenschutzhinweise erteilt sein, die eingeführte Beschäftigten-Geburtstagslisten möglichst berücksichtigen sollten. Vor der Einwilligung sollte der betroffenen Person der zusätzliche Verarbeitungszweck deutlich gemacht werden; unmissverständlich ist auf das Widerrufsrecht hinzuweisen (Art. 13 Abs. 2 Buchst. c, Art. 7 Abs. 3 Satz 3 DSGVO). Ist dies gewährleistet, kann meist ein Kenntnisstand angenommen werden, der eine gesonderte Information entbehrlich macht (vgl. Art. 13 Abs. 4 DSGVO).

9.2.6 Fazit

Die Führung von Beschäftigten-Geburtstagslisten durch bayerische öffentliche Stellen ist auch in der Welt der Datenschutz-Grundverordnung kein unlösbares Problem. Stets sollte aber insbesondere darauf geachtet werden, dass

- eine Verantwortlichkeit der öffentlichen Stelle organisatorisch klar geregelt ist,
- der Verarbeitung wirksame Einwilligungen zugrunde liegen,
- das Verzeichnis der Verarbeitungstätigkeiten eine entsprechende Position enthält sowie
- am Beginn eines Dienst- oder Arbeitsverhältnisses gegebene Datenschutzhinweise auch Informationspflichten hinsichtlich Beschäftigten-Geburtstagslisten mit abdecken.

9.3 Auskunft an Beschäftigte bayerischer öffentlicher Stellen aus Unterlagen des Personalrats

Das Bayerische Personalvertretungsgesetz (BayPVG) regelt in Art. 10 Abs. 1 Satz 1 BayPVG eine besondere Schweigepflicht vor allem für Mitglieder der Personalvertretung. Dementsprechend steht Beschäftigten bayerischer öffentlicher Stellen **grundsätzlich kein Recht auf Einsicht in Personalratsunterlagen** zu. Sie können allerdings ihr Auskunftsrecht gemäß Art. 15 DSGVO auch im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten durch den Personalrat geltend machen. Es stellt sich dann die Frage, ob und gegebenenfalls in welchem

Umfang die Schweigepflicht des Personalrats das Recht der Beschäftigten auf Auskunft einschränkt.

9.3.1 Anspruchsinhalt

Das Auskunftsrecht nach Art. 15 Abs. 1 DSGVO umfasst zunächst die Bestätigung, ob überhaupt personenbezogene Daten der Auskunft suchenden Beschäftigten verarbeitet werden (Art. 15 Abs. 1 Halbsatz 1 DSGVO). Ist dies der Fall, haben die Beschäftigten ein Recht auf Auskunft über diese Daten (Art. 15 Abs. 1 Halbsatz 2 Var. 1 DSGVO) sowie über bestimmte „Metainformationen", etwa zu den Verarbeitungszwecken (Art. 15 Abs. 1 Halbsatz 2 Var. 2 DSGVO). Beschäftigte können zudem eine Kopie ihrer verarbeiteten Daten verlangen, Art. 15 Abs. 3 DSGVO.[58]

9.3.2 Anspruchsverpflichteter

Die Rechte nach Art. 15 DSGVO richten sich gegen den Verantwortlichen. Zwar ist der Personalrat nach meiner derzeitigen Auffassung nicht als eigenständiger Verantwortlicher im Sinn von Art. 4 Nr. 7 DSGVO anzusehen; dies ist vielmehr die jeweilige bayerische öffentliche Stelle, bei welcher er gebildet ist. Der besonderen Stellung des Personalrats ist allerdings – insbesondere im Hinblick auf die Schweigepflicht nach Art. 10 Abs. 1 Satz 1 BayPVG – organisatorisch gleichwohl Rechnung zu tragen. Dies hat unter anderem zur Folge, dass der Personalrat Auskunftsersuchen Beschäftigter bezüglich seiner eigenen Datenverarbeitungen selbstständig zu bearbeiten hat.[59]

9.3.3 Die Schweigepflicht des Personalrats als Anspruchshindernis?

Gemäß Art. 10 Abs. 2 Nr. 3 BayDSG unterbleibt die Auskunft unter anderem, soweit „personenbezogene Daten oder die Tatsache ihrer Speicherung [...] wegen der überwiegenden berechtigten Interessen Dritter geheim gehalten werden müssen". Die Vorschrift schränkt die Rechte nach Art. 15 DSGVO insgesamt ein, sowohl hinsichtlich des „eigentlichen" Auskunftsanspruchs nach Art. 15 Abs. 1 DSGVO als auch hinsichtlich des Rechts auf Kopie nach Art. 15 Abs. 3 DSGVO. Der bayerische Gesetzgeber hat mit dieser Regelung von der Beschränkungsmöglichkeit des Art. 23 DSGVO Gebrauch gemacht. Bei Auskunftsbegehren im Hinblick auf (mögliche) Datenverarbeitungen des Personalrats findet das in Art. 10 Abs. 2 Nr. 3 BayDSG allgemein umschriebene Geheimhaltungsinteresse seine spezialgesetzliche Ausprägung in Art. 10 Abs. 1 Satz 1 BayPVG, der eine besondere Schweigepflicht für Mitglieder der Personalvertretung normiert.

58 Vgl. ausführlich zum Anspruchsinhalt von Art. 15 DSGVO Bayerischer Landesbeauftragter für den Datenschutz, Das Recht auf Auskunft nach der Datenschutz-Grundverordnung, Stand 12/2019, Rn. 90 ff., Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Recht auf Auskunft über die eigenen personenbezogenen Daten".

59 Vgl. zum Ganzen Bayerischer Landesbeauftragter für den Datenschutz, Der Personalrat – Verantwortlicher im Sinne des Datenschutzrechts?, Aktuelle Kurz-Information 23, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Aktuelle Kurz-Informationen".

Deutlich zu kurz gegriffen wäre es allerdings, wenn der Personalrat Auskunftsersuchen Beschäftigter pauschal mit einem Verweis auf Art. 10 Abs. 1 Satz 1 BayPVG ablehnen könnte. Vielmehr ist zu differenzieren:

— Soweit eine Schweigepflicht allein dem Schutz der betroffenen Person dient, kann diese Pflicht dem Recht der betroffenen Person auf Auskunft und auf Erhalt einer Kopie nicht entgegengehalten werden. Denn dann würde sich eine Vorschrift, die der Stärkung der Rechtsposition der betroffenen Person dienen soll, ihren Auswirkungen nach ins Gegenteil verkehren.

— Auskunftsbeschränkende Wirkung kann die Schweigepflicht daher nur entfalten, soweit sie (zumindest auch) die Interessen Dritter schützt. Dies ist im Hinblick auf die Zweckrichtung der jeweils einschlägigen Schweigepflicht im Einzelfall zu beurteilen. Die Schweigepflicht nach Art. 10 Abs. 1 Satz 1 BayPVG dient zum einen zwar dem Vertraulichkeitsinteresse der Beschäftigten, zum anderen aber auch dem Zweck, die Funktionsfähigkeit des Personalrats sowie die vertrauensvolle Zusammenarbeit mit der Dienststellenleitung (vgl. Art. 2 Abs. 1 BayPVG) zu gewährleisten.[60]

Der Anspruch nach Art. 15 Abs. 1 DSGVO ist somit auch im Beschäftigungsverhältnis kein „Alles-oder-Nichts"-Anspruch: Die Schweigepflicht steht ihm nur so weit entgegen, wie sie im konkreten Fall reicht. Es kommt auch eine Teilerfüllung dergestalt in Betracht, dass der Personalrat diejenigen Informationen bereitstellt, die nicht von dem Anspruchshindernis erfasst sind. Eine solche Teilerfüllung ist sowohl hinsichtlich der vom Personalrat verarbeiteten Daten der betroffenen Person als auch bezüglich der zu erteilenden Metainformationen nach Art. 15 Abs. 1 Halbsatz 2 Var. 2 DSGVO denkbar.

Bei der Prüfung, ob und gegebenenfalls in welchem Umfang die Schweigepflicht nach Art. 10 Abs. 1 Satz 1 BayPVG das Auskunftsrecht nach Art. 15 Abs. 1 DSGVO beschränkt, sollte der Personalrat insbesondere Folgendes beachten:

— Im Hinblick auf die eigenen personenbezogenen Daten der betroffenen Person wird die Schweigepflicht des Personalrats den Anspruch nach Art. 15 Abs. 1 DSGVO nur in Fällen einschränken können, in denen diese Pflicht zugunsten des Personalrats selbst oder zugunsten Dritter, insbesondere der Dienststellenleitung, besteht. In Betracht hierfür kommen etwa Konstellationen, in denen die Dienststellenleitung dem Personalrat bestimmte personenbezogene Daten einer beschäftigten Person im Rahmen einer beabsichtigten Personalmaßnahme (etwa einer vorgesehenen Versetzung) „vorab" zur Verfügung stellt, die beschäftigte Person von der geplanten Maßnahme jedoch noch keine Kenntnis hat. Hier soll die Schweigepflicht nicht allein das Vertraulichkeitsinteresse der betroffenen Person schützen, sondern auch die vertrauensvolle Zusammenarbeit mit der Dienststelle gewährleisten.

[60] Vgl. Ballerstedt/Schleicher/Faber, Bayerisches Personalvertretungsgesetz, Stand 8/2018, Art. 10 BayPVG Rn. 1b f. mit weiteren Nachweisen.

— Die Schweigepflicht nach Art. 10 Abs. 1 Satz 1 BayPVG bezieht sich insbesondere auch auf die Meinungsäußerungen und das Abstimmungsverhalten der Personalratsmitglieder in den Sitzungen.[61] Diese werden in aller Regel keine personenbezogenen Daten der betroffenen Person, deren Angelegenheit Gegenstand der Beratung ist, darstellen und sind insoweit von Rechten nach Art. 15 DSGVO (einschließlich des Rechts auf Kopie) ohnehin nicht erfasst. Sofern der betroffenen Person bezüglich ihrer personenbezogenen Daten Auskunft in Form von (Teil-)Ablichtungen von Personalratsdokumenten erteilt werden kann, ist dementsprechend in besonderem Maße darauf zu achten, dass Dokumententeile, die Rückschlüsse auf Meinungsäußerungen und das Abstimmungsverhalten einzelner Personalratsmitglieder enthalten, zuvor – etwa durch Schwärzung – unkenntlich gemacht werden.

— Auch hinsichtlich der in Art. 15 Abs. 1 Halbsatz 2 Var. 2 DSGVO aufgelisteten Metainformationen ist jeweils gesondert zu prüfen, ob die Schweigepflicht nach Art. 10 Abs. 1 Satz 1 BayPVG ein Anspruchshindernis darstellt. In Betracht kommt dies insbesondere hinsichtlich der Informationen über die Herkunft der Daten nach Art. 15 Abs. 1 Buchst. g DSGVO, so in dem Fall, dass der Personalrat personenbezogene Daten anlässlich einer Beschwerde eines anderen Beschäftigten verarbeitet.

9.3.4 Ergänzende Hinweise

Neben der Schweigepflicht des Personalrats können im Einzelfall auch andere Anspruchshindernisse – insbesondere nach Art. 10 Abs. 2 Nr. 1 und 2 sowie Nr. 3 Var. 1 BayDSG – in Betracht kommen. Bezüglich des Rechts auf Kopie nach Art. 15 Abs. 3 DSGVO sieht Art. 15 Abs. 4 DSGVO ferner ein spezifisches Anspruchshindernis vor. Diesem dürfte angesichts der Schweigepflicht der Personalratsmitglieder allerdings keine weitergehende Bedeutung zukommen: Denn soweit das Recht auf Kopie der eigenen personenbezogenen Daten ausnahmsweise die Rechte und Freiheiten anderer Personen beeinträchtigen würde (vgl. Art. 15 Abs. 4 DSGVO), wird bereits die Schweigepflicht nach Art. 10 Abs. 1 Satz 1 BayPVG dem Auskunftsanspruch entgegenstehen.

Sowohl Dienststelle als auch Personalrat haben durch organisatorische Vorkehrungen sicherzustellen, dass Auskunftsersuchen, welche (auch) die Verarbeitung personenbezogener Daten durch den Personalrat betreffen, ordnungsgemäß und insbesondere innerhalb der Frist(en) des Art. 12 Abs. 3 DSGVO bearbeitet werden. Dabei kann auch der Personalrat den behördlichen Datenschutzbeauftragten – möglichst ohne die Nutzung personenbezogener Beschäftigtendaten – zu Rate ziehen (vgl. Art. 39 Abs. 1 Buchst. a DSGVO). Weitere Hilfestellung diesbezüglich bietet hier meine Orientierungshilfe, „Das Recht auf Auskunft nach der Datenschutz-Grundverordnung“.[62]

[61] Vgl. Bayerischer Verwaltungsgerichtshof, Beschluss vom 2. November 2009, 17 P 08.2325, BeckRS 2011, 46028, Rn. 25.

[62] Bayerischer Landesbeauftragter für den Datenschutz, Das Recht auf Auskunft nach der Datenschutz-Grundverordnung, Stand 12/2019, Rn. 138 ff., Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Recht auf Auskunft über die eigenen personenbezogenen Daten“.

9.3.5 Fazit

Zwar ist der Personalrat nicht selbst Verantwortlicher im datenschutzrechtlichen Sinn. Aufgrund seiner besonderen Stellung hat er allerdings Ersuchen nach Art. 15 DSGVO – soweit diese Datenverarbeitungen des Personalrats betreffen – eigenständig zu bearbeiten. Dabei kann er ein solches Ersuchen nicht pauschal mit einem Hinweis auf eine bestehende Schweigepflicht zurückweisen. Vielmehr hat er im Hinblick auf das jeweilige, konkrete Ersuchen – gegebenenfalls mit Unterstützung durch den behördlichen Datenschutzbeauftragten – sorgfältig zu prüfen, ob und gegebenenfalls in welchem Umfang die Schweigepflicht nach Art. 10 Abs. 1 Satz 1 BayPVG Rechte der betroffenen Person nach Art. 15 DSGVO einschränkt.

10 Schulen und Hochschulen

10.1 Beratung bei der Änderung von Vorschriften

Im Berichtszeitraum wurden mehrere Gesetze in den Bereichen Schulen und Hochschulen geändert, bei denen ich das Bayerische Staatministerium für Unterricht und Kultus sowie das Bayerische Staatsministerium für Wissenschaft und Kunst datenschutzrechtlich beraten habe.

10.1.1 Gesundheitsdienst- und Verbraucherschutzgesetz

Im Berichtszeitraum wurde Art. 14 Gesundheitsdienst- und Verbraucherschutzgesetz (GDVG) geändert. Die Neuregelung betrifft die Übermittlung von Erkenntnissen aus Untersuchungen im Rahmen der Schulgesundheitspflege (vergleiche auch Art. 80 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen – BayEUG) durch die unteren Behörden für Gesundheit, Veterinärwesen und Verbraucherschutz an die Schulen.

Art. 14 GDVG
Schutz der Gesundheit von Kindern und Jugendlichen
[. . .]
(5) [1]Die unteren Behörden für Gesundheit, Veterinärwesen und Verbraucherschutz nehmen in Zusammenarbeit mit der Schule und den Personensorgeberechtigten die Schulgesundheitspflege wahr. [2]Diese hat insbesondere das Ziel, entwicklungsbedingten oder gesundheitlichen Beeinträchtigungen und Entwicklungsverzögerungen vorzubeugen, sie frühzeitig zu erkennen und den Personensorgeberechtigten Wege für deren Behebung aufzuzeigen sowie diese präventiv und mit Blick auf einen möglichen Förderbedarf gesundheitlich zu beraten. [3]Die unteren Behörden für Gesundheit, Veterinärwesen und Verbraucherschutz informieren nach Anhörung der Personensorgeberechtigten die Schulleitung der Schule, an der die Schulpflicht erfüllt wird oder voraussichtlich zu erfüllen ist, schriftlich

1. *unmittelbar nach der Sprachstandserhebung, wenn der Besuch eines Vorkurses Deutsch notwendig ist,*
2. *frühestens ab Beginn des Jahres, in dem das Kind bis zum 30. September sechs Jahre alt oder nach Art. 37 Abs. 1 Satz 2 oder 3 des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen (BayEUG) schulpflichtig wird,*
   a) *ob gesundheitliche Beeinträchtigungen, Entwicklungsverzögerungen oder Behinderungen festgestellt wurden, wenn dies im Einzelfall für die Beschulung, insbesondere für die individuelle Förderung, erforderlich ist,*
   b) *über Erkrankungen, die gegebenenfalls ein unmittelbares medizinisches Eingreifen oder medizinische Maßnahmen an der Schule erfordern.*

[4]Die Personensorgeberechtigten haben ihr Kind zur Schuleingangsuntersuchung nach Art. 80 Satz 1 BayEUG den unteren Behörden für Gesundheit, Veterinärwesen und Verbraucherschutz vorzustellen und den Nachweis über die Teilnahme an

der für das Kind im Zeitpunkt der Schuleingangsuntersuchung altersentsprechenden Früherkennungsuntersuchung vorzulegen. [5]Wird dieser Nachweis nicht erbracht oder ist eine schulärztliche Untersuchung aufgrund einer Verordnung gemäß Art. 34 Abs. 3 Satz 1 Nr. 6 indiziert, haben die betroffenen Kinder an der schulärztlichen Untersuchung teilzunehmen. [6]Wird ein Teil der Schuleingangsuntersuchung verweigert, erfolgt eine Mitteilung an das zuständige Jugendamt. [7]Die Jugendämter haben unter Heranziehung der Personensorgeberechtigten oder der Erziehungsberechtigten festzustellen, ob gewichtige Anhaltspunkte für eine Kindeswohlgefährdung im Sinn des § 8a des Achten Buches Sozialgesetzbuch bestehen. [8]Bei der Schuleingangsuntersuchung nach Satz 4 und bei weiteren schulischen Impfberatungen sind vorhandene Impfausweise und Impfbescheinigungen (§ 22 IfSG) der Kinder durch die Personensorgeberechtigten vorzulegen. [9]Einzelheiten werden in einer Rechtsverordnung der beteiligten Staatsministerien nach Art. 34 Abs. 3 Satz 1 Nr. 6 geregelt.
[…]

Dabei werden von den unteren Behörden für Gesundheit, Veterinärwesen und Verbraucherschutz Gesundheitsdaten der Vorschulkinder an die Schulleitung der Schule übermittelt, an der die Schulpflicht erfüllt wird oder voraussichtlich zu erfüllen ist. Nach dem im Datenschutzrecht relevanten sogenannten Doppeltürmodell benötigt jedoch nicht nur die übermittelnde Behörde (hier die untere Behörde für Gesundheit, Veterinärwesen und Verbraucherschutz) eine Rechtsgrundlage für die Datenverarbeitung (diese liegt im neuen Art. 14 Abs. 5 Satz 3 GDVG), sondern auch die empfangende Behörde, hier also die Schule. Denn für diese stellt der Vorgang eine Datenverarbeitung der übermittelten Daten dar. In diesem Bereich habe ich bei meiner Beratung des Kultusministeriums Defizite in Bezug auf die gesetzlichen Verarbeitungsbefugnisse der Schulen festgestellt. Die bisherigen Rechtsgrundlagen, insbesondere Art. 85 Abs. 1 BayEUG und die Regelungen über die Schülerunterlagen in der Bayerischen Schulordnung (BaySchO), §§ 37 ff. BaySchO, haben insbesondere die durch die Neuregelung des Art. 14 Abs. 5 GDVG veranlasste Datenverarbeitung zum Teil nur unzureichend abgebildet.

Zum einen vermisste ich eine gesetzliche Aufgabenzuweisung an die Schulen in Bezug auf die Verarbeitung von Daten im Zusammenhang mit den Vorkursen zur Förderung der deutschen Sprachkenntnisse. Eine solche wurde nun in Art. 37 Abs. 5 BayEUG geschaffen:

Art. 37 BayEUG
Vollzeitschulpflicht.
[…]
(5) Die zuständige Grundschule führt einen Vorkurs Deutsch gemeinsam mit den Kindertageseinrichtungen in ihrem Sprengel durch.

Somit wurde die Verarbeitung der Daten, die die Schule gemäß Art. 14 Abs. 5 Satz 3 Nr. 1 GDVG erhält, auf eine sichere normative Basis gestützt, nämlich auf Art. 85 Abs. 1 Satz 1 BayEUG in Verbindung mit Art. 37 Abs. 5 BayEUG.

Zum anderen sah ich es kritisch, die hier in Rede stehenden Daten von Vorschulkindern, also Kindern, die noch nicht den Status von Schülerinnen und Schülern haben (vergleiche Art. 56 Abs. 1 Satz 1 BayEUG), unter die Vorschriften der Schülerunterlagen nach §§ 37 ff. BaySchO zu fassen. Um diese Auslegungsunsicherheit zu beseitigen, hat daher das Kultusministerium auf meine Bitte die Regelung

der Schülerunterlagen insoweit präzisiert und speziell für die Daten, die die Schulgesundheitspflege betreffen, eine eigenständige Regelung in § 37 Satz 2 Nr. 1 Buchst. o BaySchO aufgenommen:

§ 37 BaySchO
Schülerunterlagen
[1]Die Schülerunterlagen umfassen die für das Schulverhältnis jeder Schülerin und jedes Schülers wesentlichen Unterlagen. 2Zu den Schülerunterlagen gehören
[…]
o) Unterlagen, die die Schulgesundheitspflege gemäß Art. 80 BayEUG betreffen,
[…].

Dies stellt einen wichtigen Baustein für den Schuldatenschutz dar. Denn damit unterfallen diese Daten aus den Schulgesundheitsuntersuchungen nun klar dem (datenschutzrechtlichen) Regime der §§ 37 ff. BaySchO. Dies führt dazu, dass die Schulen normative Leitlinien zum Umgang mit diesen Daten haben und bewirkt einen erheblichen Gewinn an Rechtssicherheit in der Praxis.

10.1.2 Bayerische Schulordnung

Das vergangene Jahr war geprägt von der COVID-19-Pandemie. Insbesondere aufgrund von Kontaktbeschränkungen und Quarantäneanordnungen wurde auch das Schulleben vor bislang nicht gekannte Herausforderungen gestellt. Über große Zeiträume wurde der Schulunterricht weg aus der Schule, dem Klassenzimmer, hinein in die häusliche Sphäre verlegt. Der sogenannte Distanzunterricht war geboren, der in räumlicher Trennung von Lehrkräften und Schülerinnen und Schülern stattfindet. Dies bringt den verstärkten Einsatz von digitalen Lernformen, insbesondere mit modernen Kommunikations- und Kollaborationswerkzeugen, mit sich. Während der ersten Welle der COVID-19-Pandemie im Frühjahr 2020 wurde der Einsatz von solchen Kommunikations- und Kollaborationswerkzeugen mangels spezifischer gesetzlicher Rechtsgrundlagen regelmäßig auf die datenschutzrechtliche Einwilligung der betroffenen Schülerinnen und Schüler oder von deren Erziehungsberechtigten gestützt. Eine wirksame Einwilligung setzt unter anderem eine freiwillige Entscheidung voraus. Eine solche liegt grundsätzlich nur vor, wenn es adäquate Alternativen gibt.

Öffentliche Stellen – wie dies auch die bayerischen öffentlichen Schulen sind – sollen sich bei der Datenverarbeitung zur Erfüllung öffentlicher Aufgaben, etwa der Erfüllung des staatlichen Erziehungs- und Bildungsauftrags, vornehmlich auf gesetzliche Rechtsgrundlagen stützen. Dies entspricht zum einen dem verfassungsrechtlichen Grundsatz des Vorbehaltes des Gesetzes. Zum anderen kann der (Distanz-)Unterricht auf der Grundlage und damit in Abhängigkeit von Einwilligungen der Betroffenen faktisch oftmals nur unzureichend abgebildet werden.

Vor diesem Hintergrund habe ich es begrüßt, dass das Kultusministerium den Distanzunterricht in § 19 Abs. 4 BaySchO vor Beginn des Unterrichts im Schuljahr 2020/2021 gesetzlich geregelt hat:

§ 19 BaySchO
Stundenplan, Unterrichtszeit, Unterrichtsform
[…]

(4) [1]Distanzunterricht ist Unterricht, der in räumlicher Trennung von Lehrkräften und Schülerinnen und Schülern stattfindet. [2]Dieser wird grundsätzlich durch elektronische Datenkommunikation unterstützt. [3]Die Durchführung von Distanzunterricht an einer Schule oder in einzelnen Klassen oder Kursen der Schule ist nur zulässig,

1. wenn die zuständigen Behörden zum Schutz von Leben oder Gesundheit
   a) die Schulschließung oder den Ausschluss einzelner Klassen oder Kurse anordnen und das Einvernehmen der Schulaufsicht vorliegt oder
   b) den Ausschluss einzelner Personen anordnen oder genehmigen,
2. soweit auf Grund außergewöhnlicher witterungsbedingter Ereignisse der Präsenzunterricht an Schulen ausfällt oder
3. sofern einzelne Schulordnungen dies vorsehen.

[4]Bei Distanzunterricht nach Satz 1 ist sicherzustellen, dass eine gleichwertige Teilnahmemöglichkeit aller Schülerinnen und Schüler besteht. [5]Die Schule legt die im Rahmen des Distanzunterrichts eingesetzten elektronischen Verfahren fest, die nach Zweck, Umfang und Art den in Anlage 2 Abschnitt 4 und 7 geregelten Vorgaben entsprechen müssen.

Soweit diese Regelung zum Distanzunterricht den Datenschutz betrifft, habe ich das Kultusministerium intensiv beraten. In diesem Zusammenhang ist der zusammen mit § 19 Abs. 4 BaySchO geschaffene Abschnitt 7 der Anlage 2 zur BaySchO hervorzuheben. Dieser Abschnitt stellt in Verbindung mit § 46 BaySchO die gesetzliche Befugnis zur Datenverarbeitung durch die Schule beim Einsatz von digitalen Kommunikations- und Kollaborationswerkzeugen zum Zweck der Durchführung von Distanzunterricht unter den Voraussetzungen von § 19 Abs. 4 BaySchO dar.

Des Weiteren steckt Abschnitt 7 der Anlage 2 zur BaySchO in Verbindung mit § 46 BaySchO den datenschutzrechtlichen Rahmen bei der Beratung und Beschlussfassung schulischer Gremien mit digitalen Hilfsmitteln unter den Voraussetzungen des – ebenfalls neu geschaffenen – § 18a BaySchO ab. Mit Einwilligung der betroffenen Personen oder ihrer Erziehungsberechtigten können Daten durch digitale Kommunikations- und Kollaborationswerkzeuge auch zu den weiteren Zwecken der Unterstützung der Schulentwicklung, der Ergänzung der pädagogischen Arbeit durch virtuelle Klassenräume, des ortsunabhängigen Arbeitens mit digitalen Unterrichtswerkzeugen sowie der Innen- und Außenkommunikation der Schule in dem in der Anlage genannten Umfang genutzt werden.

Bei der Neuaufnahme von Abschnitt 7 der Anlage 2 zur BaySchO war es mir wichtig, dafür Sorge zu tragen, dass keine Verschlechterung des Datenschutzniveaus eintritt. Daher habe ich die Erweiterung der Datenverarbeitungsbefugnisse durch Abschnitt 7 der Anlage 2 zur BaySchO kritisch hinterfragt, insbesondere ob diese unter dem Blickwinkel des Datenschutzes – auch in Zeiten der besonderen Herausforderungen, die der Schule durch die Pandemie aufgezwungen werden – erforderlich und gerechtfertigt ist. Durch mein Einwirken konnte ich zahlreiche Verbesserungen für den Datenschutz erreichen. Deren einzelteilige Darstellung würde jedoch den Rahmen des Tätigkeitsberichts überschreiten, so dass ich hier nur einige Punkte herausgreife:

— So habe ich erreicht, dass die im Rahmen der Kategorie „Sichtbare Profilinformationen“ (Nr. 3.1.2) erfassten Daten genau aufgeführt werden, so dass der zulässige Rahmen klar definiert ist.

- Auf meine Anregung hin wurde in § 19 Abs. 4 Satz 5 BaySchO auch der Verweis auf Abschnitt 4 der Anlage 2 zur BaySchO (passwortgeschützte Lernplattform) aufgenommen, so dass für die Datenverarbeitung im Rahmen der passwortschützten Lernplattform im Fall des Distanzunterrichts nach § 19 Abs. 4 BaySchO nun mit § 46 Abs. 1 BaySchO ebenfalls eine gesetzliche Rechtsgrundlage vorliegt.

- Ich habe erreicht, dass durch die Aufnahme einer „Negativ-Kategorie" die Verarbeitung besonders sensibler Daten (etwa von Gesundheitsdaten) grundsätzlich ausgeschlossen ist (Nr. 3.4). Eine Ausnahme gilt nur dann, wenn sie durch Bekanntmachung des Kultusministeriums zugelassen wird, die die jeweiligen Anforderungen an die Datensicherheit festlegt.

- Meine Anregung, dass nicht nur die Bild-, sondern auch die Tonübertragung vom Nutzer unterbrochen werden kann, wurde ebenfalls übernommen (Nr. 6).

Nicht durchsetzen konnte ich mich bislang mit der Forderung, dass die Bestimmung zur Datenverarbeitung im Distanzunterricht eine formell-gesetzliche Grundlage erhält. Auch aufgrund der Eingriffsintensität der Regelungen halte ich eine Entscheidung des Parlamentsgesetzgebers für geboten. Das Kultusministerium hat mir immerhin in Aussicht gestellt, eine formell-gesetzliche Regelung nachzuholen.

10.1.3 Weitere Fachschulordnungen und Qualifikationsverordnung für Fachlehrerinnen und Fachlehrer verschiedener Ausbildungsrichtungen an beruflichen Schulen und an Landesfeuerwehrschulen

Neben der eben dargestellten Änderung der Bayerischen Schulordnung hat das Kultusministerium noch in diversen (Berufsfach-)Schulordnungen eine Regelung aufgenommen, nach der Distanzunterricht möglich ist. Diese (Berufsfach-) Schulordnungen enthalten nun jeweils folgende Bestimmung:

„(3) [1]Mit Genehmigung der Schulaufsichtsbehörde kann in organisatorisch oder pädagogisch begründeten Fällen der Unterricht in einzelnen Fächern in begrenztem Umfang als Distanzunterricht nach § 19 Abs. 4 der Bayerischen Schulordnung abgehalten werden. [2]Die Lehrerkonferenz und das Schulforum sind vorher anzuhören."

Nicht durchdringen konnte ich mit meiner Kritik, dass die tatbestandlichen Voraussetzungen dieser Regelung, nämlich ein Vorliegen eines organisatorisch oder pädagogisch begründeten Falles, zu unbestimmt seien. Ich konnte allerdings erreichen, dass diese Bestimmungen – wie übrigens auch die anderen Regelungen zum Distanzunterricht – jeweils nur zeitlich befristet gelten.

Des Weiteren habe ich das Kultusministerium auch bei der Einfügung einer Regelung zum Distanzunterricht in der Krankenhausschulordnung, der Hausunterrichtsverordnung und der Berufsschulordnung sowie in der Qualifikationsverordnung für Fachlehrerinnen und Fachlehrer verschiedener Ausbildungsrichtungen an beruflichen Schulen und an Landesfeuerwehrschulen beraten. Soweit diese Normen unspezifisch auf § 19 Abs. 4 BaySchO verweisen, habe ich – leider vergeblich – eine Präzisierung der Verweisung angeraten, insbesondere im Hinblick auf die Frage, ob hier eine Rechtsgrund- oder Rechtsfolgenverweisung erfolgen

soll. Jedenfalls solange noch keine formell-gesetzliche Rechtsgrundlage für den Distanzunterricht vorliegt, hätte ich mir bei den diversen (Berufsfach/Fach)-Schulordnungen und in der Qualifikationsverordnung konkretere, die Anwendungsfälle des Distanzunterrichts normativ einschränkende Tatbestandsmerkmale gewünscht.

10.1.4 Fernprüfungen an Hochschulen

Nicht nur die Schulen, sondern auch die Hochschulen sahen sich im Frühjahr 2020 durch die Pandemie vor erhebliche Probleme gestellt. Die Pandemie und die infektionsschutzrechtlichen Vorgaben in Bezug auf Kontaktvermeidung und Abstand brachten es mit sich, dass einige bayerische Hochschulen keine Präsenz-, sondern digitale Fernprüfungen durchführen wollten und mussten.

In diesem Zusammenhang habe ich das Wissenschaftsministerium intensiv beraten. Dabei war die Rechtslage sehr komplex. Denn die denkbare Bandbreite der technischen Unterstützung einer elektronischen Fernprüfung, die eine Hochschule als datenschutzrechtlich Verantwortlicher durchführt, ist sehr breit und reicht von einem Telefonat bis hin zu einem technisch – eventuell auch unter Einsatz von KI-Systemen – vollüberwachten IT-Arbeitsplatz im privaten häuslichen Umfeld. Dementsprechend stellen sich vielfältige rechtlich gewichtige Datenschutzfragen, auch solche technisch-organisatorischer Art. Vor allem ist bei der Durchführung von elektronischen Fernprüfungen eine Vielzahl an Grundrechten betroffen. Zu nennen sind zuvorderst das Grundrecht auf informationelle Selbstbestimmung (Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz – GG) sowie das Grundrecht auf Datenschutz nach Art. 8 Charta der Grundrechte der Europäischen Union. Soweit der betroffene Prüfling über eine Kamera erfasst wird, ist insbesondere das Recht am eigenen Bild berührt. Wenn dabei auch die Wohnung der betroffenen Person aufgezeichnet wird, steht ferner das Grundrecht auf die Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG im Raum. Auch die Chancengleichheit (Art. 3 Abs. 1 GG) der Prüflinge steht in Rede. Diese verfassungsrechtliche Spannungslage, die durch die Durchführung von elektronischen Fernprüfungen erzeugt wird, war bislang im Hochschulrecht in Bezug auf die Rechtsgrundlagen zur Datenverarbeitung nur unzureichend abgebildet gewesen. Daher habe ich vom Wissenschaftsministerium unter Verweis auf die verfassungsrechtliche Wesentlichkeitstheorie gefordert, dass eine spezifische Rechtsgrundlage, mithin eine Regelung für die Durchführung von elektronischen Fernprüfungen geschaffen wird. Nach der Wesentlichkeitstheorie hat das Parlament unter anderem alle grundrechtswesentlichen Entscheidungen selbst zu treffen. Zudem habe ich darauf bestanden, dass das Wissenschaftsministerium flankierend zur formell-gesetzlichen Regelung in einer Rechtsverordnung den Einsatz von Fernprüfungen konkretisiert und den zulässigen rechtlichen Rahmen für die Durchführung von elektronischen Fernprüfungen bayernweit absteckt. Hierbei hatte ich Erfolg.

So wurde mit Art. 61 Abs. 10 Bayerisches Hochschulgesetz (BayHSchG) eine neue Regelung zur Erprobung neuer oder effizienterer Prüfungsmodelle, einschließlich elektronischer Fernprüfungen, geschaffen.

Art. 61 BayHSchG
Prüfungen, Prüfungsordnungen
[…]
(10) [1]Zur Erprobung neuer oder effizienterer Prüfungsmodelle kann das Staatsministerium durch Rechtsverordnung vorsehen, dass Prüfungen, die ihrer Natur

nach dafür geeignet sind, in elektronischer Form und ohne die Verpflichtung durchgeführt werden können, persönlich in einem vorgegebenen Prüfungsraum anwesend sein zu müssen. [2]In der Rechtsverordnung sind insbesondere Bestimmungen zu treffen

1. zur Sicherung des Datenschutzes,
2. zur Sicherung persönlicher Leistungserbringung durch den zu Prüfenden während der gesamten Prüfungsdauer,
3. zur eindeutigen Authentifizierung des zu Prüfenden,
4. zur Verhinderung von Täuschungshandlungen,
5. zum Umgang mit technischen Problemen.

[3]Im Übrigen bleiben Art. 12 Abs. 3 Nr. 6 und Art. 61 Abs. 3 Nr. 8 unberührt. 4Das Staatsministerium evaluiert diese Bestimmung sowie die darauf aufbauenden Prüfungsregelungen spätestens zum Jahresende 2024 und berichtet hierzu dem Landtag.

Auf diese Weise hat der demokratisch unmittelbar legitimierte Gesetzgeber die wichtige Entscheidung über die grundsätzliche Zulässigkeit der probeweisen Einführung von elektronischen Fernprüfungen getroffen. Auch sieht diese Regelung vor, dass eine Rechtsverordnung des Wissenschaftsministeriums, die solche elektronischen Fernprüfungen zulässt, unter anderem Regelungen zur Sicherung des Datenschutzes enthalten muss. Wichtig war mir, dass diese neue Regelung zu elektronischen Fernprüfungen zunächst nur zeitlich befristet ist. Auch insoweit konnte ich mein Anliegen durchsetzen. Art. 61 Abs. 10 BayHSchG tritt mit Ablauf des 31. Dezember 2024 außer Kraft.

Von der gesetzlichen Ermächtigung in Art. 61 Abs. 10 BayHSchG hat das Wissenschaftsministerium Gebrauch gemacht und die Bayerische Fernprüfungserprobungsverordnung (BayFEV) erlassen. Auch hierbei habe ich das Wissenschaftsministerium intensiv beraten und konnte zahlreiche Verbesserungen für den Datenschutz erwirken. Diese im Einzelnen aufzuzählen, würde den Rahmen des Tätigkeitsberichts jedoch überschreiten. Daher will ich hier nur auf folgende Punkte eingehen, die mir besonders wichtig waren:

— Mir war es ein hervorgehobenes Anliegen, dass die Teilnahme an elektronischen Fernprüfungen weitestgehend am Freiwilligkeitsprinzip ausgerichtet ist. Die Teilnahme erfolgt nun grundsätzlich auf freiwilliger Basis mit einer termingleichen Präsenzprüfung als Alternative (§ 8 Abs. 1 BayFEV). Ist dies im Pandemiefall (§ 1 Abs. 2 BayFEV) nicht möglich, so dürfen den Studierenden jedenfalls keine prüfungsrechtlichen Nachteile entstehen (§ 8 Abs. 2 Satz 2 und 3 BayFEV).

§ 8 BayFEV
Wahlrecht
(1) [1]Die Teilnahme an elektronischen Fernprüfungen erfolgt auf freiwilliger Basis. [2]Die Freiwilligkeit der Teilnahme ist grundsätzlich auch dadurch sicherzustellen, dass eine termingleiche Präsenzprüfung als Alternative angeboten wird. [3]Termingleich sind Prüfungen, die innerhalb desselben Prüfungszeitraums unter strenger Beachtung der Grundsätze der Chancengleichheit stattfinden.
(2) [1]Soll die elektronische Fernprüfung nach § 1 Abs. 2 Satz 2 angeboten werden, stellen die Hochschulen fest, ob und für wie viele Studierende eine Präsenzprüfung unter Beachtung der jeweils geltenden infektionsschutzrechtlichen Vorgaben und Empfehlungen angeboten werden kann. [2]Kann eine Präsenzprüfung nicht durchgeführt werden oder melden sich zu viele

Studierende für die Alternative der Präsenzprüfung an, können die Hochschulen Studierende auf den voraussichtlich nächstmöglichen Präsenzprüfungstermin verweisen.[3] Prüfungsrechtliche Nachteile dürfen dadurch nicht entstehen.[4] Hierzu legen die Hochschulen Kriterien fest, wobei die Auswahl vorrangig nach dem Studienfortschritt erfolgen soll.[5] Den betroffenen Studierenden muss ein Wechsel zur elektronischen Fernprüfung ermöglicht werden.

– Des Weiteren habe ich darauf geachtet, dass die Authentifizierung möglichst datensparsam und auf vergleichsweise „konventionellem" Weg möglich ist (§ 5 BayFEV). So können sich die Studierenden mit gültigem Lichtbildausweis authentifizieren. Alternative Authentifizierungsmethoden können die Hochschulen nur als zusätzliches Verfahren – im Sinne eines freiwilligen Angebots – vorsehen.

§ 5 BayFEV
Authentifizierung
(1) [1] Vor Beginn einer elektronischen Fernprüfung erfolgt die Authentifizierung mit Hilfe eines gültigen Lichtbildausweises, der nach Aufforderung vorzuzeigen ist. [2] Die Hochschulen können weitere, gleich geeignete Authentifizierungsverfahren durch Satzung festlegen, die sie neben der Authentifizierung nach Satz 1 zusätzlich anbieten.
(2) [1] Eine Speicherung der im Zusammenhang mit der Authentifizierung verarbeiteten Daten über eine technisch notwendige Zwischenspeicherung hinaus ist unzulässig. [2] Personenbezogene Daten aus der Zwischenspeicherung sind unverzüglich zu löschen.

Art. 61 Abs. 10 BayHSchG und die Bayerische Fernprüfungserprobungsverordnung sind rückwirkend zum 20. April 2020 in Kraft getreten.

Dadurch wird die Datenverarbeitung durch Hochschulen bei elektronischen Fernprüfungen auf eine spezielle rechtliche Grundlage gestützt. Dies dient nicht nur der Rechtssicherheit, sondern auch dem Datenschutz.

10.1.5 Elektronische Hochschulwahlen

Das Wissenschaftsministerium hat im Zusammenhang mit der erwähnten Änderung des Bayerischen Hochschulgesetzes auch beabsichtigt, das Recht der Hochschulwahlen zu liberalisieren und mehr in die Verantwortung der Hochschulen zu geben. Dabei sollte den Hochschulen auch die Möglichkeit gegeben werden, diese elektronisch durchzuführen. Aufgrund der meines Erachtens vorliegenden Gewichtigkeit dieser Entscheidung war es mir aber wichtig, dass der parlamentarische Gesetzgeber diese Möglichkeit der elektronischen Wahl explizit im Gesetzestext klarstellt und somit die Letztverantwortung trägt. Dies konnte ich erreichen. Die neue Vorschrift Art. 38 Abs. 2 BayHSchG lautet nun:

Art. 38
Wahlen
[…]
(2) [1] Die Hochschule regelt die nach diesem Gesetz durchzuführenden Wahlen durch Satzung, in der auch die Amtszeiten festzulegen sind. [2] In der Satzung kann vorgesehen werden, dass die Wahlen ganz oder teilweise elektronisch durchgeführt werden. [3] Solange und soweit keine Regelung durch Satzung vorliegt, gelten

die Wahlbestimmungen, die in der Grundordnung oder vom Staatsministerium durch Rechtsverordnung getroffen werden.

10.2 Aus der Prüfungs- und Beratungspraxis

Auch in diesem Berichtszeitraum hatte ich mich mit zahlreichen Vorgängen zu Datenverarbeitungen von Schulen und Hochschulen zu befassen. Neben Beratungsanfragen von betroffenen Personen, von deren Eltern, von Verbänden, von den datenverarbeitenden Stellen selbst und von Staatsministerien waren auch vermehrt Beschwerden zu bearbeiten. Im Zusammenhang mit der COVID-19-Pandemie sind zahlreiche neue Fragen entstanden. Nur beispielhaft seien Datenverarbeitungen durch Schulen im Zusammenhang mit Ausnahmen von der Maskenpflicht (siehe vor Nr. 3.1), der Distanzunterricht (siehe Nr. 10.1.2) und der Einsatz von Videokonferenzsystemen (siehe Nr. 12.4) genannt. Unabhängig davon möchte ich hier auch über andere Konstellationen berichten.

10.2.1 Umsetzung des Masernschutzgesetzes an Schulen

Mit dem weitgehenden Inkrafttreten des Masernschutzgesetzes[63] zum 1. März 2020 enthalten nunmehr insbesondere § 20 Abs. 8 bis 14 Infektionsschutzgesetz (IfSG) Regelungen zum verpflichtenden Nachweis eines ausreichenden Impfschutzes oder einer Immunität gegen Masern.

Im Berichtszeitraum war ich daher häufig mit datenschutzrechtlichen Fragen im Zusammenhang mit der Umsetzung des Masernschutzgesetzes an bayerischen öffentlichen Schulen befasst. Neben vereinzelten Beschwerden hatte ich zahlreiche Beratungsanfragen von betroffenen Schülerinnen und Schülern und vor allem von deren Erziehungsberechtigten, jedoch auch von Lehrkräften und Schulen zu bearbeiten. Sie betrafen vorwiegend die Prüfung und Dokumentation des Nachweises eines ausreichenden Masernimpfschutzes durch Schulen sowie die Zulässigkeit von Mitteilungen an Gesundheitsämter.

10.2.1.1 Informationen und Empfehlungen zur Umsetzung des Masernschutzgesetzes durch das Bayerische Staatsministerium für Unterricht und Kultus

Um den bayerischen Schulen die Umsetzung des Masernschutzgesetzes zu erleichtern, hat das Bayerische Staatsministerium für Unterricht und Kultus auf seiner Internetseite Informationen und Empfehlungen hierzu zur Verfügung gestellt.[64] Diese Informationen umfassen auch eine „Dokumentationshilfe für Einrichtungen beziehungsweise Übermittlungsbogen an das zuständige Gesundheitsamt – Nachweis über einen ausreichenden Masernschutz gemäß § 20 Absatz 9 Infektionsschutzgesetz (IfSG)“.

63 Vom 10. Februar 2020 (BGBl. I S. 148).

64 Internet: https://www.km.bayern.de/allgemein/meldung/6891/so-setzen-schulen-das-masernschutzgesetz-richtig-um.html.

10.2.1.2 Nachweispflicht

Im Hinblick auf die Pflicht zum Nachweis eines ausreichenden Masernschutzes an bayerischen öffentlichen Schulen gilt – ohne nachfolgend alle Einzelheiten abbilden zu wollen – Folgendes:

— Personen, die nach dem 31. Dezember 1970 geboren sind und in Schulen oder sonstigen Ausbildungseinrichtungen gemäß § 33 Nr. 3 IfSG betreut werden, müssen laut § 20 Abs. 8 Satz 1 IfSG einen entsprechenden Impfschutz oder eine Immunität gegen Masern aufweisen.

— Der Leitung der jeweiligen Einrichtung müssen Personen, die dort betreut/beschult werden sollen, gemäß § 20 Absatz 9 Satz 1 IfSG vor Beginn ihrer Betreuung hierzu bestimmte Nachweise vorlegen. Bei minderjährigen Personen haben gemäß § 20 Abs. 13 IfSG die sorgeberechtigten Personen für die Einhaltung der Nachweisverpflichtung zu sorgen.

— Schülerinnen und Schüler, die am 1. März 2020 bereits eine bestimmte Schule besuchen, müssen die entsprechenden Nachweise gemäß § 20 Abs. 10 IfSG bis Ablauf des 31. Juli 2021 erbringen.

10.2.1.3 Nachweisdokumente

Die zum Nachweis geeigneten Dokumente – beispielsweise eine Impfdokumentation (Impfausweis oder Impfbescheinigung) oder ein ärztliches Zeugnis darüber, dass eine Immunität gegen Masern vorliegt oder die betroffene Person aufgrund einer medizinischen Kontraindikation nicht geimpft werden kann – werden in § 20 Abs. 9 Satz 1 IfSG aufgelistet.

10.2.1.4 Vorlage, Prüfung, Dokumentation

Grundsätzlich müssen die entsprechenden Nachweise gemäß § 20 Abs. 9 IfSG bei der Leitung der betroffenen Gemeinschaftseinrichtung (Schulleitung) vorgelegt werden. Diese nimmt die entsprechende Prüfung vor.

Entsprechend den Empfehlungen des Bayerischen Staatsministeriums für Unterricht und Kultus (vergleiche Nr. 10.2.1.1) wird der Nachweis über einen ausreichenden Masernschutz lediglich im erforderlichen Umfang (Erfüllung oder Nichterfüllung der Voraussetzungen des § 20 Abs. 9 IfSG und Begründung hierfür) in der Dokumentationshilfe festgehalten. Bei Schülerinnen und Schülern wird die Dokumentationshilfe Bestandteil der Schülerakte (§§ 37 ff. Schulordnung für schulartübergreifende Regelungen an Schulen in Bayern).

Es ist nicht vorgesehen, dass auch die für den Nachweis bei der Schule vorgelegten Dokumente (beispielsweise Impfpässe oder ärztliche Bescheinigungen) Eingang in die jeweilige Schülerakte finden. Die entsprechenden Unterlagen sind vielmehr nur zur Prüfung der Voraussetzungen notwendig und verbleiben nach Abschluss dieser Prüfung nicht bei der Schule (auch nicht in Kopie).

10.2.1.5 Mitteilungspflicht an das Gesundheitsamt

Wird der entsprechende Nachweis nicht fristgerecht vorgelegt oder ergibt sich, dass ein Impfschutz gegen Masern erst zu einem späteren Zeitpunkt möglich ist

oder vervollständigt werden kann, darf eine schulpflichtige Person zwar die jeweilige Schule besuchen (vergleiche § 20 Abs. 9 Satz 9 IfSG), jedoch hat die Schulleitung gemäß § 20 Abs. 9 Satz 4 IfSG unverzüglich das Gesundheitsamt, in dessen Bezirk sich die Einrichtung befindet, darüber zu benachrichtigen und diesem personenbezogene Angaben dazu zu übermitteln.

Zu den personenbezogenen Angaben gehören dabei gemäß § 2 Nr. 16 IfSG Name und Vorname, Geschlecht, Geburtsdatum, Anschrift der Hauptwohnung oder des gewöhnlichen Aufenthaltsortes und (falls abweichend), Anschrift des derzeitigen Aufenthaltsortes der betroffenen Person, Telefonnummer (soweit vorliegend) und E-Mail-Adresse (soweit vorliegend). Nicht umfasst wird insoweit also die Übermittlung der vorgelegten Nachweisdokumente. Das Gesundheitsamt kann die entsprechenden Nachweise nach Maßgabe von § 20 Abs. 12 IfSG jedoch gegebenenfalls selbst bei der betroffenen Person anfordern.

10.2.2 Datenübermittlung sensibler Daten per einfacher E-Mail durch eine bayerische öffentliche Schule

An einer bayerischen öffentlichen Schule wurde vom Sekretariat der Schulleitung per einfacher E-Mail eine Nachricht der Schulpsychologin an alle Eltern mit Schulkindern verschickt, die an Legasthenie leiden. Die Nachricht der Schulpsychologin informierte über eine Neuregelung im Bereich des Notenschutzes bei Legasthenie. Die jeweiligen Empfänger konnten dabei alle anderen Empfänger mit deren Vor- und Zunamen erkennen. Auf diese Weise hat jeder Empfänger davon Kenntnis erlangt, welche (anderen) Schulkinder ebenfalls an Legasthenie leiden.

Das Vorgehen der Schule war in mehrfacher Hinsicht datenschutzrechtlich unzulässig. Für die Verarbeitung personenbezogener Daten benötigen Schulen eine Befugnis (vgl. Art. 6 Abs. 1 UAbs. 1 DSGVO). Im Schulbereich stellt Art. 85 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG) eine zentrale Befugnisnorm dar (vgl. Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2, Abs. 3 UAbs. 1 Buchst. b DSGVO). Im Übrigen gelten Art. 5 Abs. 1 Satz 2, Abs. 2 und 4 BayDSG.

Die Schule hat auf meine Aufforderung zur Stellungnahme unmittelbar eingeräumt, dass die Voraussetzungen des Art. 85 BayEUG und auch eine andere Rechtsgrundlage nicht vorliegen und sie die Legasthenie der jeweils betroffenen Schulkinder nicht an alle anderen Eltern mit betroffenen Schulkindern hätte weitergeben dürfen.

Auch die Weitergabe einer personalisierten E-Mail-Adresse durch eine öffentliche Stelle durch Versendung mittels der cc-Funktion an andere Empfänger eines E-Mail-Verteilers ist eine Verarbeitung von personenbezogenen Daten durch Übermittlung (Art. 4 Nr. 2 DSGVO), für die eine Befugnis benötigt wird (Art. 6 Abs. 1 UAbs. 1 DSGVO). Meine Auffassung hierzu habe ich bereits in meinem 27. Tätigkeitsbericht 2016 unter Nr. 2.1.3 dargelegt. An dieser halte ich weiterhin fest.

Darüber hinaus ist der Versand sensibler personenbezogener Daten per einfacher E-Mail grundsätzlich nicht zulässig (vgl. Art. 32 DSGVO sowie Nr. 6.1 Buchst. c Bekanntmachung über erläuternde Hinweise zum Vollzug der datenschutzrechtlichen Bestimmungen für die Schulen).[65] Das Vorliegen einer Legasthenie ist ein

[65] Vom 11. Januar 2013 (KWMBl. S. 27, ber. S. 72).

sensibles personenbezogenes Datum. Gleichwohl wurde die E-Mail unverschlüsselt versandt. Daher habe ich jeweils einen Verstoß der Schule gegen datenschutzrechtliche Bestimmungen festgestellt. Von einer förmlichen Beanstandung habe ich hier vor allem deshalb abgesehen, weil die Schule die Fehler unmittelbar eingeräumt und bereits Maßnahmen zur zukünftigen Vermeidung vergleichbarer Fehler ergriffen hat sowie die Bereitschaft zur Einhaltung der datenschutzrechtlichen Vorgaben deutlich erkennbar war.

10.2.3 Nachteilsausgleich – Weitergabe von Gesundheitsdaten eines Studenten innerhalb einer Hochschule

Ein Student stellte bei dem Vorsitzenden des Prüfungsausschusses eines Studiengangs an einer Hochschule schriftlich einen Antrag auf Nachteilsausgleich für eine Prüfung. Bei Bewilligung eines Nachteilsausgleichs kann die jeweilige Prüfungssituation modifiziert werden, beispielsweise durch eine Zeitverlängerung. Der Antrag enthielt ein (nerven-)ärztliches Attest mit Diagnosen zum Krankheitsbild des Petenten. In dem Antrag hat der Petent ausdrücklich darum gebeten, den Nachteilsausgleich vertraulich und diskret zu bearbeiten.

Der Vorsitzende des Prüfungsausschusses lehnte den Antrag gegenüber dem Studenten per Bescheid ab. Dies geschah mittels einer nicht ausreichend verschlüsselten E-Mail, die auch den Antrag des Studenten und dessen Attest als gescannte PDF-Datei als Anhang enthalten hat. Diese E-Mail samt Anhang ist mittels der sogenannten cc-Funktion auch an Prüfungsausschussmitglieder sowie einen anderen Lehrstuhl versendet worden. Gemäß der von mir angeforderten Stellungnahme der Hochschule hätten an dem anderen Lehrstuhl ausschließlich der Lehrstuhlinhaber und dessen Sekretariat Zugriff auf die Funktions-E-Mail-Adresse des Lehrstuhls gehabt.

Öffentliche Stellen wie Hochschulen benötigen für die Verarbeitung personenbezogener Daten eine Befugnis (vgl. Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2, Abs. 3 UAbs. 1 Buchst. b DSGVO). Nach Art. 42 Abs. 4 Satz 1 Bayerisches Hochschulgesetz bestimmt sich die Verarbeitung von personenbezogenen Daten der Studierenden und Gaststudierenden nach den jeweils geltenden Vorschriften über den Schutz personenbezogener Daten. Nach Art. 4 Abs. 1 BayDSG ist die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle unbeschadet sonstiger Bestimmungen zulässig, wenn sie zur Erfüllung einer ihr obliegenden Aufgabe erforderlich ist. Das als Anlage versendete ärztliche Attest über den Petenten enthält überdies Gesundheitsdaten im Sinne des Art. 9 Abs. 1 DSGVO. Die Verarbeitung von Gesundheitsdaten ist nach Art. 9 Abs. 1 DSGVO untersagt, wenn nicht die Voraussetzungen des Art. 9 Abs. 2 DSGVO vorliegen.

Für die hier in Rede stehenden Datenverarbeitungen konnte die Hochschule keine Befugnisnorm darlegen.

In Betracht gekommen wäre allenfalls Art. 9 Abs. 2 Buchst. g DSGVO in Verbindung mit Art. 4 Abs. 1 BayDSG in Verbindung mit der Allgemeinen Prüfungsordnung der Hochschule. Dann hätte die beschriebene Versendung des ärztlichen Attestes allerdings zur Durchführung des Nachteilsausgleichsverfahrens erforderlich sein müssen. Dies war jedoch nicht der Fall. Dabei ist auch der Grundsatz der Datenminimierung zu beachten (Art. 5 Abs. 1 Buchst. c DSGVO).

10.2.3.1 Versendung an die weiteren Mitglieder des Prüfungsausschusses

Die Versendung des Attestes an die weiteren Mitglieder des Prüfungsausschusses rechtfertigte die Hochschule damit, dass diese stimmberechtigte Mitglieder des Prüfungsausschusses seien. Sie würden an den Entscheidungen mitwirken und würden auf diesem Weg über den erfolgten Bescheiderlass in Kenntnis gesetzt.

Zur Information über den erfolgten Bescheid ist es allerdings nicht erforderlich, den Mitgliedern das Attest per E-Mail zu übersenden. Hierfür genügt eine Nachricht, dessen Informationsgehalt sich darauf beschränkt, dass der Antrag des Antragstellers mit Bescheid von einem bestimmten Datum abgelehnt worden ist. Daraus folgt auch, dass die Übersendung des Bescheids an die Mitglieder in Kopie ebenfalls nicht erforderlich war.

10.2.3.2 Versendung an einen anderen Lehrstuhl

Die Versendung an einen anderen Lehrstuhl hat die Hochschule damit begründet, dass es sich bei der in Rede stehenden Prüfung um eine nicht zentral vom Prüfungsamt, sondern vom Lehrstuhl organisierte Prüfung gehandelt habe. Gegenüber dem Prüfungsausschuss habe ein Mitarbeiter des Lehrstuhls zu erkennen gegeben, dass der Lehrstuhl über den Antrag des Studenten auf Nachteilsausgleich informiert gewesen wäre. Daher sei es notwendig gewesen, den Lehrstuhl über die negative Entscheidung des Prüfungsausschusses in Kenntnis zu setzen.

Diese Begründung trägt jedoch nicht. Für die Organisation der Prüfung wäre es für den Lehrstuhl allenfalls nötig zu erfahren, dass der Antrag abgelehnt wurde und für den Petenten bei der Durchführung der Prüfung daher kein Nachteilsausgleich zu organisieren ist. Hierfür war es weder erforderlich, dem Lehrstuhl den ablehnenden Bescheid in Kopie noch das ärztliche Attest zu übersenden. Es hätte jedenfalls genügt, wenn der Prüfungsausschuss dem Lehrstuhl nur die Information mitgeteilt hätte, dass der Antrag ablehnt worden sei.

Ich habe daher mehrere Verstöße gegen datenschutzrechtliche Bestimmungen bei der Hochschule beanstandet. Dies war unter Ausübung meines Ermessens auch angezeigt, weil die Hochschule lediglich in Bezug auf die Übermittlung an den anderen Lehrstuhl (ansatzweise) einen Fehler eingeräumt hat und zudem hier besonders sensible Gesundheitsdaten betroffen waren. Hinzu kommt, dass der Petent ausdrücklich um Vertraulichkeit gebeten hatte. Dennoch hatte dies den Vorsitzenden des Prüfungsausschusses offensichtlich nicht zu einem datenschutzrechtlich sensibleren Umgang veranlasst. Des Weiteren habe ich bei der Hochschule veranlasst, dass alle von dem Vorgang betroffenen Personen der Hochschule das dort ohne Rechtsgrundlage verarbeitete Attest aus ihrem E-Mail-Programm und Computer löschen (Art. 17 Abs. 1 Buchst. d DSGVO).

10.2.4 Datenschutzerklärung auf der Schulhomepage

Kontakte mit Schulen im Rahmen meiner Aufsichtstätigkeit habe ich regelmäßig zum Anlass genommen, die Erfüllung der Informationspflichten nach Art. 13 DSGVO auf deren Webseiten zu überprüfen. Hierbei habe ich leider öfter feststellen müssen, dass die jeweilige Datenschutzerklärung nicht den gesetzlichen Anforderungen entsprach. In diesen Fällen war selten nahezu keine Datenschutzer-

klärung vorhanden, teils haben zentrale Informationen gefehlt, teils waren nur kleinere Mängel zu finden. Dabei hat das Bayerische Staatsministerium für Unterricht und Kultus ein mit mir abgestimmtes Muster für Datenschutzhinweise für Schulen samt Anwendungsvorgaben auf seiner Webseite veröffentlicht. Immerhin habe ich bei den betroffenen Schulen nach meinem Hinweis auf den Missstand stets die unmittelbare Bereitschaft zur Anpassung ihrer Datenschutzerklärung an das Muster feststellen können. Ich werde auch in Zukunft bei einem Kontakt mit einer Schule regelmäßig die Einhaltung der Informationspflichten nach Art. 13 DSGVO, insbesondere auf der Schulwebseite, überprüfen.

11 Weitere rechtliche Themen

11.1 Telemedienrecht: Webseiten bayerischer öffentlicher Stellen und Nutzung von Cookies

Häufiges Thema meiner Beratungstätigkeit waren auch in diesem Berichtszeitraum die Vorgaben für den Einsatz von Cookies auf den Webseiten bayerischer öffentlicher Stellen. Konkret ging es oft darum, in welchen Fällen das Einholen einer Einwilligung der Webseitennutzenden erforderlich ist und wie entsprechende Erklärungen gegebenenfalls zu gestalten sind.

Ausgangspunkt war dabei häufig der Wunsch der öffentlichen Stellen, Informationen darüber zu erhalten, wie ihre Webseiten genutzt werden, beispielsweise, welche Inhalte am häufigsten aufgerufen werden, um ihr Informationsangebot bedarfsgerecht am Informationsinteresse der Bürgerinnen und Bürger ausrichten zu können. Um entsprechende Seitenaufrufe auswerten zu können, wird oft auf Analysetools zurückgegriffen, die mit Cookies arbeiten, die auf dem jeweiligen Endgerät der Webseitennutzenden gespeichert werden.

In der von ihr am 29. März 2019 veröffentlichten „Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien“,[66] analysierte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) die Rechtslage insbesondere zur Reichweitenmessung und zum Tracking auf Webseiten, jedoch beschränkt auf die Internetauftritte nicht öffentlicher Stellen. Sie ging dabei davon aus, dass insbesondere § 15 Telemediengesetz (TMG) nach Inkrafttreten der Datenschutz-Grundverordnung nicht mehr anzuwenden ist; eine europarechtskonforme Auslegung von § 15 Abs. 3 TMG im Sinne des Art. 5 Abs. 3 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation; nichtamtlich: ePrivacy-Richtlinie) scheide aus. Anzuwenden sei vielmehr die Datenschutz-Grundverordnung. Im Ergebnis wird aber auch bei Anwendung der Datenschutz-Grundverordnung häufig das Einholen einer Einwilligung erforderlich sein.

§ 15 TMG
Nutzungsdaten
[…]
(3) Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.
[…]

66 Internet: https://www.datenschutz-konferenz-online.de/orientierungshilfen.html.

Art. 5 Datenschutzrichtlinie für elektronische Kommunikation
Vertraulichkeit der Kommunikation
[…]
(3) Die Mitgliedstaaten stellen sicher, dass die Benutzung elektronischer Kommunikationsnetze für die Speicherung von Informationen oder den Zugriff auf Informationen, die im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur unter der Bedingung gestattet ist, dass der betreffende Teilnehmer oder Nutzer gemäß der Richtlinie 95/46/EG klare und umfassende Informationen insbesondere über die Zwecke der Verarbeitung erhält und durch den für diese Verarbeitung Verantwortlichen auf das Recht hingewiesen wird, diese Verarbeitung zu verweigern. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung oder Erleichterung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder, soweit dies unbedingt erforderlich ist, um einen vom Teilnehmer oder Nutzer ausdrücklich gewünschten Dienst der Informationsgesellschaft zur Verfügung zu stellen.

11.1.1 Rechtsprechung des Europäischen Gerichtshofes sowie des Bundesgerichtshofes

Bereits in einer Entscheidung aus dem Jahr 2019[67] hatte der Europäische Gerichtshof Aussagen zu den Voraussetzungen einer wirksamen Einwilligung bei Verwendung von Cookies im Internet getroffen. Er entschied, dass keine wirksame Einwilligung vorliege, wenn die Speicherung von oder der Zugriff auf Informationen, die bereits im Endgerät des Nutzers einer Webseite gespeichert sind, mittels Cookies durch ein voreingestelltes Ankreuzkästchen erlaubt wird, das der Nutzer zur Verweigerung seiner Einwilligung abwählen muss. Dabei komme es nicht darauf an, ob es sich bei den im Endgerät des Nutzers einer Webseite gespeicherten oder abgerufenen Informationen um personenbezogene Daten handele oder nicht.

Zudem wies das Gericht darauf hin, dass Art. 5 Abs. 3 Datenschutzrichtlinie für elektronische Kommunikation die Mitgliedstaaten dazu verpflichte, sicherzustellen, dass die Speicherung oder der Zugriff auf Informationen, die bereits im Endgerät eines Nutzers gespeichert sind, nur gestattet sei, wenn der betreffende Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er über die Zwecke der Verarbeitung erhält, seine Einwilligung hierzu gegeben habe.

Auf Grundlage dieses Urteils entschied der Bundesgerichtshof 2020,[68] dass § 15 Abs. 3 Satz 1 TMG mit Blick auf Art. 5 Abs. 3 Satz 1 der Datenschutzrichtlinie für elektronische Kommunikation dahingehend richtlinienkonform auszulegen sei, dass der Diensteanbieter Cookies zur Erstellung von Nutzungsprofilen für Zwecke der Werbung oder Marktforschung nur mit Einwilligung des Nutzers einsetzen darf.

Der richtlinienkonformen Auslegung des § 15 Abs. 3 Satz 1 TMG stehe nicht entgegen, dass der deutsche Gesetzgeber bisher keinen Umsetzungsakt vorgenommen habe. Es sei anzunehmen, dass der Gesetzgeber die bestehende Rechtslage in Deutschland für richtlinienkonform erachtete. Mit dem Wortlaut des § 15 Abs. 3 Satz 1 TMG sei eine entsprechende richtlinienkonforme Auslegung noch verein-

67 Europäischer Gerichtshof, Urteil vom 1. Oktober 2019, C-673/17.
68 Bundesgerichtshof, Urteil vom 28. Mai 2020, I ZR 7/16, NJW 2020, S. 2540 ff.

bar. Im Fehlen einer (wirksamen) Einwilligung könne mit Blick darauf, dass der Gesetzgeber mit § 15 Abs. 3 Satz 1 TMG das unionsrechtliche Einwilligungserfordernis umgesetzt sah, der nach dieser Vorschrift der Zulässigkeit der Erstellung von Nutzungsprofilen entgegenstehende Widerspruch gesehen werden.

11.1.2 Reaktion der deutschen Datenschutzaufsichtsbehörden

Vor dem Hintergrund, dass der Bundesgerichtshof von der Möglichkeit einer europarechtskonformen Auslegung des § 15 Abs. 3 TMG ausgeht, forderte die Datenschutzkonferenz in ihrer Entschließung vom 25. November 2020 vom Bundesgesetzgeber, Rechtssicherheit bezüglich der Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation zu schaffen:

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 25. November 2020

Betreiber von Webseiten benötigen Rechtssicherheit
Bundesgesetzgeber muss europarechtliche Verpflichtungen der „ePrivacyRichtlinie" endlich erfüllen

Der Gesetzgeber ist verpflichtet, die EU-Richtlinie über den europäischen Kodex für die elektronische Kommunikation vom 11. Dezember 2018 (RL 2018/1972/EU) bis zum 20. Dezember 2020 umzusetzen.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) fordert den Gesetzgeber auf, endlich Regelungen zu erlassen, um die ePrivacy-Richtlinie vollständig und im Einklang mit der Datenschutz-Grundverordnung (DSGVO) umzusetzen.

Die DSK hat in der Vergangenheit wiederholt kritisch darauf hingewiesen, dass der Gesetzgeber Art. 5 Abs. 3 ePrivacy-Richtlinie nicht oder nicht ordnungsgemäß umgesetzt hat. Das Urteil des Bundesgerichtshofs (BGH) vom 28. Mai 2020 (I ZR 7/16 – „Planet49") verstärkt nach Auffassung der DSK den seit langem bestehenden, dringenden Handlungsbedarf.

Die DSK hat bereits im April 2018 in der Positionsbestimmung „Zur Anwendbarkeit des TMG für nichtöffentliche Stellen ab dem 25. Mai 2018" den Standpunkt vertreten, dass die Datenschutzvorschriften des Telemediengesetzes neben der Datenschutz-Grundverordnung (DSGVO) nicht mehr anwendbar sind. Eine ausführliche Begründung zu dieser Rechtsauffassung wurde von der DSK in der Orientierungshilfe für Anbieter von Telemedien im März 2019 veröffentlicht.

Der BGH hatte im Planet49-Verfahren einen Streit zu entscheiden, in dem das beklagte Unternehmen personenbezogene Daten über das Nutzungsverhalten von Verbrauchern mittels Cookies zu pseudonymisierten Nutzungsprofilen verarbeitete und diese für personalisierte Werbung nutzte. Nach dem Wortlaut des § 15 Abs. 3 Telemediengesetz (TMG) wäre ein solches Vorgehen dann zulässig, wenn die Personen entsprechend informiert wurden und nicht widersprochen haben (sogenannte Widerspruchslösung). Mit Blick auf Art. 5 Abs. 3 ePrivacy-Richtlinie legt der BGH § 15 Abs. 3 TMG dahingehend aus, schon in dem Fehlen einer wirksamen Einwilligung könne ein solcher Widerspruch gesehen werden, weshalb eine aktive Einwilligung erforderlich sei. Unter Zugrundelegung dieser Auslegung von § 15 Abs. 3 TMG wendet er diese Vorschrift neben der DSGVO an. Letztlich ist der

BGH der Vorabentscheidung des Europäischen Gerichtshofes gefolgt und bestätigt das grundsätzliche Erfordernis einer wirksamen Einwilligung für das Setzen von Cookies.

Schon die Tatsache, dass die DSK und der BGH bei einer sehr praxisrelevanten Rechtsfrage zwar im Ergebnis darin übereinstimmen, dass eine Verarbeitung, wie sie den Gerichten zur Entscheidung vorlag, einwilligungsbedürftig ist, jedoch bei der Herleitung dieses Ergebnisses voneinander abweichende Auffassungen vertreten, verdeutlicht das Ausmaß der Rechtsunklarheit.

Mit der Entscheidung wird die Abgrenzung der Regelungsbereiche zwischen ePrivacyRichtlinie, DSGVO und den Datenschutzvorschriften des TMG deutlich erschwert. Der BGH stellt ausdrücklich heraus, dass ePrivacy-Richtlinie und DSGVO unterschiedliche Schutzrichtungen verfolgen. Die Vorschriften in den §§ 12 bis 15 TMG knüpfen ausdrücklich an den Begriff der Verarbeitung personenbezogener Daten an. Diese Materie ist auf europäischer Ebene weitgehend abschließend durch die Datenschutz-Grundverordnung geregelt. Art. 5 Abs. 3 ePrivacy-Richtlinie hat hingegen auch Informationen ohne Personenbezug zum Regelungsgegenstand. Es bleibt daher offen, ob § 15 Abs. 3 TMG – entgegen des Wortlautes – auch dann eine Umsetzung des Art. 5 Abs. 3 ePrivacy-Richtlinie darstellen soll, wenn die Informationen, die im Endgerät eines Teilnehmers gespeichert werden oder auf die zugegriffen wird, keinen Personenbezug haben.

§ 15 Abs. 3 TMG bezieht sich ausdrücklich und ausschließlich auf die Erstellung von pseudonymen Nutzungsprofilen für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien. Die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, kann jedoch auch zu anderen Zwecken erfolgen und ist nicht auf die in § 15 Abs. 3 TMG genannten Zwecke beschränkt.

Schließlich fordert Art. 5 Abs. 3 ePrivacy-Richtlinie grundsätzlich ohne Berücksichtigung konkreter Zwecke eine Einwilligung. Lediglich in Art. 5 Abs. 3 Satz 2 ePrivacy-Richtlinie finden sich Ausnahmen von diesem Grundsatz. Dieses Regel-Ausnahme-Prinzip findet sich im TMG nicht wieder.

Webseitenbetreiber und andere Akteure, die ihre Dienste u. a. in Bezug auf „Cookies" rechtskonform gestalten müssen, brauchen Rechtsklarheit. Der Gesetzgeber ist deshalb aufgefordert, bestehende Rechtsunsicherheiten umgehend durch eine klare und europarechtskonforme Gesetzgebung zu beseitigen."

Gegen Ende des Beurteilungszeitraums verdichteten sich nun tatsächlich die Anzeichen, dass der Bundesgesetzgeber vorhat, diesen Appell aufzugreifen und eine Neuregelung zur Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation plant. Ob, wann und welche Regelungen schließlich getroffen werden, konnte ich zum Redaktionsschluss dieses Berichts jedoch noch nicht einschätzen.

11.1.3 Ausblick

Unabhängig vom möglichen Ergebnis eines solchen Gesetzgebungsverfahrens auf Bundesebene habe ich für meinen Zuständigkeitsbereich die genannte Entscheidung des Bundesgerichtshofes jedoch bereits zum Anlass genommen, auf die federführenden Ressorts der Bayerischen Staatsregierung zuzugehen, damit

diese unter meiner Beteiligung die Verwendung von Cookies sowie die Ausgestaltung erforderlicher Einwilligungserklärungen auf staatlichen Webseiten in den Blick nehmen und vorhandene Muster für die Datenschutzhinweise auf staatlichen Webseiten überarbeiten. Zum Ende des Berichtszeitraums konnte dieser Anpassungsprozess noch nicht abgeschlossen werden. Ich bin allerdings zuversichtlich, dass dies zeitnah gelingt.

Die bayerischen öffentlichen Stellen sollten für die Zukunft jedoch ebenso wie ich im Blick behalten, dass an sich geplant ist, die rechtlichen Vorgaben auch zur Verwendung von Cookies auf europäischer Ebene durch eine Verordnung neu zu regeln. Bereits seit Januar 2017 (!) läuft dort ein Gesetzgebungsverfahren, das darauf gerichtet ist, die Datenschutzrichtlinie für elektronische Kommunikation durch eine Verordnung über Privatsphäre und elektronische Kommunikation (nichtamtlich: ePrivacy-Verordnung) abzulösen, welche dann unmittelbare Geltung in den Mitgliedstaaten beanspruchen würde. Mit der geplanten ePrivacy-Verordnung habe ich mich bereits in meinem 28. Tätigkeitsbericht unter Nr. 13.2 beschäftigt.

Ob, wann und mit welchem Inhalt dieses europäische Gesetzgebungsverfahren seinen Abschluss finden wird, bleibt derzeit offen. Ich werde mich allerdings dafür einsetzen, dass das Datenschutzniveau bei einer europäischen Neuregelung nicht abgesenkt wird.

11.2 Internationaler Datenverkehr: Übermittlung personenbezogener Daten in Drittländer, insbesondere in die Vereinigten Staaten von Amerika

Bayerische öffentliche Stellen nutzen zur Erfüllung ihrer gesetzlichen Aufgaben häufig (Software-)Anwendungen und sonstige Dienstleistungen von Unternehmen, die ihren Hauptsitz in den Vereinigten Staaten von Amerika (USA) haben. Auch bei Vertragsbeziehungen mit hiesigen Niederlassungen US-amerikanischer Unternehmen oder Einschaltung anderer Dienstleister kann es dazu kommen, dass personenbezogene Daten, die von den öffentlichen Stellen in solchen Anwendungen oder im Zusammenhang mit diesen Dienstleistungen verarbeitet werden, in die USA übermittelt werden.

11.2.1 Aktuelle Rechtsprechung

Solche Datenübermittlungen erfolgten bislang in vielen Fällen auf Grundlage des Durchführungsbeschlusses (EU) 2016/1250 der Europäischen Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes (Privacy Shield), einem Angemessenheitsbeschluss im Sinne von Art. 45 DSGVO. Zum Privacy Shield habe ich mich bereits in meinem 27. Tätigkeitsbericht 2016 unter Nr. 13.2 und in meinem 28. Tätigkeitsbericht 2018 unter Nr. 14.1 geäußert.

In seinem Urteil vom 16. Juli 2020[69] hat der Europäische Gerichtshof diesen Durchführungsbeschluss nunmehr für ungültig erklärt. Datenübermittlungen in

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

die USA können hierauf somit nicht mehr gestützt werden. Zugleich hat er festgestellt, dass die Entscheidung 2010/87/EG der Kommission über Standardvertragsklauseln grundsätzlich weiterhin gültig ist.

Soll eine Übermittlung personenbezogener Daten auf der Grundlage von Garantien in Standarddatenschutzklauseln (Art. 46 Abs. 2 Satz 1 Buchst. c DSGVO) erfolgen, müssen Verantwortliche jedoch prüfen, ob den betroffenen Personen, deren personenbezogene Daten in ein Drittland übermittelt werden, ein Schutzniveau gewährt wird, das dem Schutzniveau in der Europäischen Union im Wesentlichen gleichwertig ist.

Bei konsequenter Auslegung des Urteils hielt das Gericht die Übermittlung personenbezogener Daten in die USA auf Grundlage der Standardvertragsklauseln ohne zusätzliche Schutzmaßnahmen grundsätzlich nicht für ausreichend.

11.2.2 Reaktion der deutschen und europäischen Datenschutzaufsichtsbehörden

Um den Interessenträgern erste Erläuterungen und vorläufige Anhaltspunkte zur Verwendung von Rechtsinstrumenten zur Übermittlung personenbezogener Daten an Drittländer, einschließlich der USA, zur Verfügung zu stellen, veröffentlichte der Europäische Datenschutzausschuss bereits am 23. Juli 2020 das Dokument „Häufig gestellte Fragen“[70] als Hilfestellung im Zusammenhang mit der Umsetzung des Urteils.

In ihrer Pressemitteilung vom 28. Juli 2020,[71] die ich in einer eigenen Pressemitteilung vom 29. Juli 2020[72] aufgegriffen habe, äußerte sich auch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) zu der dargestellten Entscheidung und wies darauf hin, dass diese den Datenschutz für EU-Bürgerinnen und -Bürger stärke. In diesem Zusammenhang stellte die Datenschutzkonferenz auch ihre erste Einschätzung zu den Auswirkungen des Urteils dar (nachfolgend in Auszügen):

Pressemitteilung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 28. Juli 2020

Urteil des Europäischen Gerichtshofs zur Übermittlung personenbezogener Daten in Drittländer („Schrems II“) stärkt den Datenschutz für EU-Bürgerinnen und Bürger

[…]

Für die Übermittlung personenbezogener Daten in die USA und andere Drittländer hat das Urteil nach einer ersten Einschätzung der DSK folgende Auswirkungen:

1. *Die Übermittlung personenbezogener Daten in die USA auf der Grundlage des Privacy Shield ist unzulässig und muss unverzüglich eingestellt werden. Der EuGH hat das Privacy Shield für ungültig erklärt, weil das durch den*

70 Internet: https://edpb.europa.eu/our-work-tools/our-documents/ohrajn/frequently-asked-questions-judgment-court-justice-european-union_de.

71 Internet: https://www.datenschutzkonferenz-online.de/media/pm/20200616_pm_schrems2.pdf.

72 Internet: https://www.datenschutz-bayern.de/presse/20200729_PMEuGH1.html.

EuGH bewertete US-Recht kein Schutzniveau bietet, das dem in der EU im Wesentlichen gleichwertig ist. […]

2. *Für eine Übermittlung personenbezogener Daten in die USA und andere Drittländer können die bestehenden Standardvertragsklauseln der Europäischen Kommission zwar grundsätzlich weiter genutzt werden. Der EuGH betonte jedoch die Verantwortung des Verantwortlichen und des Empfängers, zu bewerten, ob die Rechte der betroffenen Personen im Drittland ein gleichwertiges Schutzniveau wie in der Union genießen. Nur dann kann entschieden werden, ob die Garantien aus den Standardvertragsklauseln in der Praxis verwirklicht werden können. Wenn das nicht der Fall ist, sollte geprüft werden, welche zusätzlichen Maßnahmen zur Sicherstellung eines dem Schutzniveau in der EU im Wesentlichen gleichwertigen Schutzniveaus ergriffen werden können. Das Recht des Drittlandes darf diese zusätzlichen Schutzmaßnahmen jedoch nicht in einer Weise beeinträchtigen, die ihre tatsächliche Wirkung vereitelt. Nach dem Urteil des EuGH reichen bei Datenübermittlungen in die USA Standardvertragsklauseln ohne zusätzliche Maßnahmen grundsätzlich nicht aus.*

   […]

5. *Verantwortliche, die weiterhin personenbezogene Daten in die USA oder andere Drittländer übermitteln möchten, müssen unverzüglich überprüfen, ob sie dies unter den genannten Bedingungen tun können. Der EuGH hat keine Übergangs- bzw. Schonfrist eingeräumt.*

Inzwischen hat zudem der Europäische Datenschutzausschuss Empfehlungen zu ergänzenden Maßnahmen für Übertragungsinstrumente zur Gewährleistung des EU-Schutzniveaus[73] sowie Empfehlungen zu den grundlegenden europäischen Garantien für Überwachungsmaßnahmen[74] veröffentlicht.[75]

Ziel dieser Ausarbeitungen ist es, die Verantwortlichen (und Auftragsverarbeiter), die als Datenexporteure tätig sind, bei ihrer Pflicht, geeignete ergänzende Maßnahmen aufzufinden und umzusetzen, zu unterstützen und Hilfestellung bei der Bewertung zu geben, ob der rechtliche Rahmen im Drittland, der den Zugang von Behörden zu Daten für Überwachungszwecke regelt, die Garantien des Übertragungsinstruments nach Art. 46 DSGVO beeinträchtigt.

Zu den genannten Empfehlungen zu ergänzenden Maßnahmen hat der Europäische Datenschutzausschuss auch ein öffentliches Konsultationsverfahren eingeleitet.

73 Internet: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

74 Internet: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf.

75 Vgl. hierzu die Pressemitteilung des Europäischen Datenschutzausschusses vom 11. November 2020: EDPB adopts recommendations on supplementary measures following Schrems II, https://edpb.europa.eu/news/news/2020/european-data-protection-board-41st-plenary-session-edpb-adopts-recommendations_de.

11.2.3 Ausblick und Handlungsbedarf der bayerischen öffentlichen Stellen

Die Entscheidung des Europäischen Gerichtshofs wird für eine Vielzahl bayerischer öffentlicher Stellen erhebliche Auswirkungen auf deren Verarbeitungs- und Übermittlungsabläufe haben. In vielen Fällen wird dies Fragen der grundsätzlichen Vertragsgestaltung mit den jeweiligen Anbietern betreffen. Denn können nicht in einem ausreichenden Maße zusätzliche Maßnahmen zur Sicherstellung eines mit der Europäischen Union vergleichbaren Datenschutzniveaus getroffen werden, so wird häufig nur noch der Einsatz von solchen Systemen in Betracht kommen, bei denen die Problematik eines Datentransfers in die USA von vornherein nicht besteht oder aber der Abschluss einer Vereinbarung, wonach ein solcher Datentransfer effektiv ausgeschlossen wird. Die Problematik kann sich auch für Datenübermittlungen in andere Drittländer stellen, abhängig insbesondere von der Rechtslage im jeweiligen Drittland.

Vor diesem Hintergrund habe ich mich bereits Anfang August 2020 unter anderem an die Amtschefinnen und Amtschefs der Bayerischen Staatskanzlei und der bayerischen Staatsministerien gewandt. Dabei habe ich auf die sich aus dem Urteil ergebenden datenschutzrechtlichen Probleme und den daraus resultierenden unmittelbaren Handlungsbedarf mit Blick auf die jeweiligen Geschäftsbereiche hingewiesen. Auch die Vielzahl von Beratungsanfragen, die bayerische öffentliche Stellen im Nachgang der Entscheidung an mich gerichtet haben, lässt einen erheblichen Anpassungsbedarf in der bayerischen Verwaltung erkennen. Ich gehe davon aus, dass die Aufarbeitung der durch das Urteil für die bayerischen öffentlichen Stellen aufgeworfenen Fragen von einer bayernweiten Koordinierung profitieren würde. Die Staatsregierung hat mich hierzu auch bereits kontaktiert. Bei allem Verständnis für die Komplexität der hier für die bayerische Verwaltung entstehenden Herausforderungen werde ich darauf achten, dass sie aus datenschutzrechtlicher Sicht zufriedenstellend gelöst werden.

12 Technik und Organisation

12.1 Das digitale Bürgerkonto

Das bayerische digitale Bürgerkonto stellt Bürgerinnen und Bürgern insbesondere Möglichkeiten zur Online-Kommunikation mit Behörden zur Verfügung. Es ist integriert in das BayernPortal, dessen Weiterentwicklung ich seit mehreren Jahren immer wieder beratend begleite (siehe 27. Tätigkeitsbericht unter Nr. 12.2). Mittels des digitalen Bürgerkontos kann eine elektronische Identität (BayernID) und ein Servicekonto online eingerichtet werden.

Folgende Registrierungsarten sind derzeit möglich:

- Registrierung anhand der eID-Funktion des Personalausweises beziehungsweise elektronischen Aufenthaltstitels;
- Registrierung anhand des Softwarezertifikats authega;
- Registrierung mit Benutzername/Passwort.

Mit dem digitalen Bürgerpostfach stehen je nach Registrierungsart folgende wichtige Funktionen zur Verfügung:

- Postfach mit bidirektional verschlüsselter elektronische Kommunikation;
- optional Identifikation (Prüfung der Identität) und Authentifizierung (Nachweis der Identität);
- optional Schriftformersatz (digitale Unterschrift).

Allein das Merkmal der verschlüsselten elektronischen Kommunikation stellt bereits einen deutlichen Mehrwert gegenüber der unverschlüsselten E-Mail dar. Kann sich die Behörde über die Identität des elektronischen Gegenübers zu jeder Zeit auf Grund einer sicheren Identifikation und Authentifizierung sicher sein, besteht die Möglichkeit der verschlüsselten elektronischen Antwort durch die Behörde sogar im Erstkontakt, auch wenn hierbei sensible personenbezogene Daten übermittelt werden.

Aus diesem Grund habe ich in meinem 27. Tätigkeitsbericht unter Nr. 8.3.7 insbesondere Sozialbehörden auf die Nutzung dieses Portals zur Kommunikation mit Bürgerinnen und Bürgern hingewiesen.

Basierend auf den unterschiedlichen Registrierungsarten komme ich zu folgender Bewertung für die Kommunikation unter Zuhilfenahme des BayernPortals:

Registrierungsart eID-Funktion des Personalausweises oder elektronischen Aufenthaltstitels:

- **Schriftformersatz** (digitale Unterschrift) ist möglich.

- **Identifikation und Authentifizierung:** Die Identifikation und die Freischaltung der eID-Funktion erfolgt bei Ausstellung des Personalausweises beziehungsweise des elektronischen Aufenthaltstitels. Die elektronische Identität ist somit zuverlässig der echten Identität zugeordnet und damit auch nicht abstreitbar. Zudem ist davon auszugehen, dass die Person, die über den Personalausweis verfügt (physischer Besitz) und die zugehörige PIN kennt (Wissen), zu jeder Zeit im Verfahren empfangsberechtigt ist. Somit ist auch die korrekte Authentifizierung beim Anmeldeprozess sichergestellt.

- **Einsatz des Postfachs:** Die Behörde kann über das Postfach des BayernPortals antworten, auch wenn dabei personenbezogene Daten übermittelt werden.

Registrierungsart Softwarezertifikat authega:

- **Schriftformersatz** (digitale Unterschrift): Die Möglichkeit der digitalen Unterschrift hängt von den gesetzlichen Vorgaben ab. In Bayern wurde das Softwarezertifikat authega gemäß Zertifizierungsbekanntmachung-authega[76] als schriftformersetzend zertifiziert. Für Verwaltungsvorgänge, die auf Bundesgesetzgebung basieren, ist eine derartige Zertifizierung bisher noch nicht erfolgt.

- **Identifikation und Authentifizierung:** Die Authentifikation erfolgt bei Ausstellung des Zertifikates. Durch den Prozess der Ausstellung ist sichergestellt, dass die korrekte Person das Softwarezertifikat sowie das zugehörige Passwort erhält. Allerdings ist nicht abzustreiten, dass es Konstellationen geben kann, in denen sowohl Softwarezertifikat wie auch Passwort von unbefugten Personen verwendet werden können. So ist üblicherweise ein Softwarezertifikat auf einem Rechner gespeichert, wenn nicht sogar im Browser installiert. Somit kann es für Personen mit Zugriff auf den Rechner (Familienmitglieder oder andere Mitbewohner) sowie für Angreifer (etwa durch Hacking) verfügbar sein. Das zugehörige Passwort kann unsicher sein, unbemerkt abgegriffen („gephisht“) werden oder im Browser ungesichert gespeichert sein. Alle diese Faktoren liegen nicht im Einflussbereich der Behörde, sind aber dennoch bei der Bewertung der Sicherheit der Authentifizierung zu berücksichtigen.

- **Einsatz des Postfachs:** Möchte eine Behörde Verfahren betreiben, bei denen eine Rückmeldung mit personenbezogenen Daten erfolgen soll, so sind in jeden Fall bei der Anmeldung zum Fachverfahren Sicherheitshinweise zu geben, so dass das notwendige Wissen vermittelt wird, um sicherzustellen, dass keine unberechtigte Person auf die Rückmeldung der Behörde zugreifen kann.

76 Vom 24. März 2017 (FMBl. S. 254).

Registrierungsart Benutzername/Passwort:

- **Schriftformersatz** (digitale Unterschrift) ist nicht möglich.

- **Identifikation und Authentifizierung:** Die Registrierung mit Benutzername/Passwort erfolgt durch Angabe von einigen persönlichen Daten inklusive E-Mailadresse und Passwort. Eine Authentifikation erfolgt hierbei nicht, es wird lediglich die Existenz einer E-Mailadresse überprüft. Die Behörde kann also zu keiner Zeit sicher davon ausgehen, mit einem identifizierten Gegenüber zu kommunizieren.

- **Einsatz des Postfachs:** Eine Antwort der Behörde mit personenbezogenen Daten ist nicht möglich. Folgende Szenarien sind unter anderem dennoch denkbar: Die Kommunikation zu allgemeinen Fragen ohne Übermittlung personenbezogener Daten seitens der Behörde; Anfrage des Bürgers, auch mit personenbezogenen Daten, die aber eine postalische Rückantwort an eine der Behörde bereits auf einem anderen Weg bekannte Adresse erfordert.

Im Berichtszeitraum besonders erfreulich zeigen sich Aktivitäten des Zentrum Bayern Familie und Soziales (ZBFS) zur Anbindung von Fachverfahren an die BayernID. So wurde das Fachverfahren zur Feststellung einer Schwerbehinderung an die BayernID angebunden. Damit kann das ZBFS nun auch elektronische Rückmeldung geben, falls Antragsteller über ein Konto mit eID-Registrierung verfügen. Des Weiteren können nun in einigen Fällen Anfragen über das Kontaktformular mit Nutzung der BayernID gestellt werden. Eine elektronische Antwort wird nur für Konten, die über eID registriert wurden, verschickt, anderenfalls wird die Antwort postalisch versandt.

Begrüßenswert ist, dass in dem zugrundeliegenden Projekt eine Architektur geschaffen wurde, um weitere Fachverfahren und Anwendungsfälle an die BayernID anzuschließen. Ich werte dies als eine deutliche Verbesserung bezüglich der Sicherheit der elektronischen Kommunikation und würde eine sichere Anbindung weiterer geeigneter Fachverfahren begrüßen.

12.2 Leitfaden zum Outsourcing kommunaler IT

IT-Outsourcing, also die Auslagerung von Aufgaben der eigenen IT-Abteilung an einen externen Dienstleister, wird heutzutage auch vermehrt von öffentlichen Stellen in Betracht gezogen. Auch Kommunen ziehen diese Möglichkeit immer häufiger in Erwägung. Da Kommunen auf Grund der Vielfalt der Tätigkeitsfelder auch eine Vielzahl an rechtlichen Regelungen zu beachten haben, habe ich mich dieses Themas angenommen und sowohl die rechtliche Einbettung wie daraus resultierende Anforderungen an den Auftragnehmer in Zusammenarbeit mit einer hierfür durch das Bayerischen Staatsministerium des Innern, für Sport und Integration eingerichteten Arbeitsgruppe erarbeitet. Sowohl rechtliche wie auch die technisch-organisatorische Details finden sich im Beitrag Nr. 7.2 dieses Tätigkeitsberichts. Die Veröffentlichung des vollständigen Kriterienkatalog auf meiner Webseite stand zum Redaktionsschluss dieses Tätigkeitsberichts kurz bevor.

12.3 Räumliche, personelle, technische und organisatorische Trennung zwischen Beauftragten der Staatsregierung und Staatsministerien

Die Bayerische Staatsregierung hat auf der Grundlage von Art. 1 Abs. 1 Satz 1 Bayerisches Beauftragtengesetz (BayBeauftrG) und Art. 15 Abs. 1 Bayerisches Integrationsgesetz für verschiedene Politikbereiche insgesamt acht Beauftragte ernannt, die für Themen wie Integrations-, Asyl- und Migrationspolitik, Patienten und Pflege oder die Belange von Menschen mit Behinderungen zuständig sind. Der nach Art. 33a Verfassung des Freistaates Bayern (im Folgenden: BV) vom Bayerischen Landtag zu wählende Bayerische Landesbeauftragte für den Datenschutz gehört nicht zu diesem Kreis von Beauftragten.

Die Beauftragten sind Beraterinnen und Berater der Staatsregierung, gehören ihr aber nicht an. Sie sollen die Staatsregierung unterstützen, indem sie in ihrem fachlichen Bereich Verbesserungsvorschläge erarbeiten, und Ansprechpartner für die Bürgerinnen und Bürger sein, die sich unbeschadet des verfassungsrechtlich verbürgten Petitionsrechts mit ihren Anliegen an die Beauftragten wenden können. Rechtlich und fachlich verantwortlich bleiben im jeweiligen Ressort aber die Staatsministerien (vgl. Art. 51 Abs.1, Art. 55 Nr. 5 bis 7 BV).

Zur Erfüllung der Aufgaben verfügt jede und jeder Beauftragte über eine gemäß Art. 3 Abs. 2 BayBeauftrG „auf das Notwendige beschränkte Geschäftsstelle“, die in der Regel bei dem fachlich zuständigen Staatsministerium angesiedelt ist und die dort vorhandenen Ressourcen nutzt. Angesichts dieser organisatorischen Vorgaben sind ausschließlich in der Geschäftsstelle eingesetzte Beschäftigte die Ausnahme. Regelmäßig sind die Beschäftigten der Geschäftsstelle zugleich in einem entsprechenden Fachreferat des Staatsministeriums tätig.

Diesbezüglich erhielt ich eine Beschwerde hinsichtlich der Trennung von Aktenführung, IT-Systemen und insbesondere hinsichtlich der Tatsache möglicher Interessenkonflikte bei Beschäftigten, die nicht ausschließlich für die Beauftragte oder den Beauftragten tätig sind. Aus Datenschutzsicht waren folgende Hinweise veranlasst:

Gemäß Art. 1 Abs. 3 Satz 1 BayBeauftrG sind die Beauftragten trotz ihrer „Zuordnung“ zu einem Staatsministerium eigenständige öffentliche Stellen im Sinne des Bayerischen Datenschutzgesetzes. Die Beschäftigten ihrer Geschäftsstellen sind in dieser Rolle den Beauftragten unterstellte Personen im Sinne von Art. 29 DSGVO. Als öffentliche Stellen dürfen die Beauftragten zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten (vgl. Art. 4 Abs. 1 BayDSG). Im Gegenzug sind sie für die Einhaltung der datenschutzrechtlichen Vorschriften selbst verantwortlich (vgl. Art. 3 Abs. 2 BayDSG).

Als datenschutzrechtlich Verantwortliche müssen die Beauftragten insbesondere eine eigene behördliche Datenschutzbeauftragte oder einen eigenen behördlichen Datenschutzbeauftragten benennen (dies kann auch die oder der behördliche Datenschutzbeauftragte des jeweiligen Staatsministeriums sein, vgl. Art. 37 Abs. 3 DSGVO) sowie für die Einhaltung der Anforderungen des technisch-organisatorischen Datenschutzes und der Vertraulichkeit personenbezogener Daten auch gegenüber dem Staatsministerium sorgen.

12.3.1 Allgemeine Vorgaben zur Vertraulichkeit personenbezogener Daten

Der Sicherung der Vertraulichkeit personenbezogener Daten dient vor allem Art. 1 Abs. 3 Satz 1 BayBeauftrG, der die Beauftragten selbst zur Verschwiegenheit verpflichtet.

Die Beauftragten müssen die Vertraulichkeit auch mit Blick auf ihre Geschäftsstellen gewährleisten. Insofern gilt zunächst, dass die den Beauftragten unterstellten Personen personenbezogene Daten nur nach deren Weisung verarbeiten dürfen (vgl. Art. 29, 32 Abs. 4 DSGVO). Die notwendigen Weisungen zum Umgang mit Vorgängen sollten die Beauftragten schon deshalb schriftlich erteilen, um der in Art. 5 Abs. 2 DSGVO geregelten Rechenschaftspflicht zu genügen, die Einhaltung datenschutzrechtlicher Vorgaben jederzeit nachweisen zu können.

Die Beschäftigten der Geschäftsstelle unterwirft Art. 11 BayDSG darüber hinaus dem Datengeheimnis, das auch nach dem Ende der Tätigkeit fortbesteht. Das Datengeheimnis verbietet es den Beschäftigten einer öffentlichen Stelle, personenbezogene Daten unbefugt zu verarbeiten. Der Begriff der Verarbeitung schließt insbesondere die Offenlegung personenbezogener Daten durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung ein (vgl. Art. 4 Nr. 2 DSGVO). Die Beschäftigten sollten über ihre datenschutzrechtlichen Verpflichtungen aufgeklärt werden (siehe auch mein 28. Tätigkeitsbericht 2018 unter Nr. 12.2). Dabei sollte insbesondere darauf hingewiesen werden, dass die Geschäftsstelle datenschutzrechtlich eine eigenständige öffentliche Stelle ist und das Datengeheimnis deshalb auch im Verhältnis zur sonstigen Tätigkeit im Staatsministerium gilt.

12.3.2 Technisch-organisatorische Maßnahmen der Beauftragten

Insbesondere zur Umsetzung der Vertraulichkeitsanforderungen sollten die Beauftragen in technisch-organisatorischer Hinsicht Folgendes berücksichtigen (Empfehlungen für Maßnahmen nach Art. 24 und 32 DSGVO):

12.3.2.1 Räumliche Trennung der Beauftragten innerhalb des Ministeriums

Den Beschäftigten des Beauftragten sollten während dieser Tätigkeit idealerweise eigene Räumlichkeiten zur Verfügung gestellt werden. Diese sollten beispielsweise durch eine eigene Schließanlage abgesichert werden.

12.3.2.2 Getrennte Papieraktenführung

Die Verwaltung und insbesondere Aufbewahrung der Papierakten von Personen, die sich an den Beauftragten gewandt haben, muss getrennt von den sonstigen Akten des Staatsministeriums, etwa in gesonderten, verschließbaren Schränken, erfolgen. Die Akten dürfen nur den Beschäftigten der Geschäftsstelle des Beauftragten zugänglich sein.

12.3.2.3 IT-Systeme

Sollen IT-Systeme wie beispielsweise die E-Akte des jeweiligen Staatsministeriums mitbenutzt werden, so ist eine Mandantentrennung oder die Umsetzung äquivalenter Schutzmaßnahmen erforderlich. Der technische Begriff „Mandant“ und, eng damit verbunden, der Begriff der „Mandantenfähigkeit“ eines IT-Systems

kommt zum Tragen, wenn es Organisationen ermöglicht werden soll, Daten logisch beziehungsweise physikalisch zu trennen und zu verwalten. Der abgeschlossene Datenhaltungs- und Verarbeitungskontext einer im datenschutzrechtlichen Sinne verantwortlichen Stelle wird nachfolgend als **Mandant** bezeichnet, die getrennte Speicherung und Verarbeitung als **Mandantentrennung**. Ein Verfahren ist **mandantenfähig**, wenn es eine Mandantentrennung umsetzen kann.

In der Praxis sollte die Mandantentrennung zwischen fest definierten Organisationseinheiten oder Rollen vollzogen werden, wie beispielsweise Abteilungen oder bestimmten Personengruppen. Personenbezogene Daten, die von unterschiedlichen Verantwortlichen oder zu unterschiedlichen Zwecken erhoben und verarbeitet werden, sollten grundsätzlich getrennt verarbeitet werden, wie dies in Art. 5 Abs. 1 Buchst. b DSGVO gefordert ist. Die getrennte Verarbeitung betrifft sowohl die Speicherung als auch die Verarbeitungsfunktionen wie etwa Datenbanktransaktionen und Datensatzbuchungen.

Aus wirtschaftlichen oder organisatorischen Gründen kann es in begründeten Fällen sinnvoll sein, Ressourcen wie Hard- und Software für verschiedene Datenbestände gemeinsam zu nutzen. Voraussetzung hierfür ist, dass die Daten mandantenbezogen geführt und die Verarbeitungsfunktionen, die Zugriffsberechtigungen und die Konfigurationseinstellungen eigenständig je Mandant festgelegt werden können.

Aus technischer Sicht existieren unterschiedliche Ansätze zur Umsetzung der Mandantentrennung, beispielswiese:

- **Trennung in der Datenhaltung:** In den eingesetzten Datenspeichersystemen werden die Daten der Mandanten getrennt voneinander vorgehalten. Der Zugriff sollte über mandantenspezifische Benutzerzugänge beziehungsweise Accounts erfolgen. Diese Trennung gilt ebenso für schriftlich geführte Akten. Außerdem muss auch die Datensicherung und Erstellung von Backups mandantenfähig umgesetzt werden. Idealerweise werden die Dienste für verschiedene Mandaten in logisch getrennten Bereichen gehalten.

- **Trennung der Umgebungen:** Die Dienste gegenüber den Mandanten werden auf verschiedenen virtuellen oder physischen Systemen angeboten. Dabei müssen auch Berechtigungskonzepte zur Regelung des Zugriffs von personenbezogenen Daten erarbeitet werden.

- **Mandantenspezifische Verschlüsselung:** Um einen unbefugten mandatenübergreifenden Zugriff zu verhindern, kommen kryptografische Verfahren mit individuellen Schlüsseln für verschiedene Mandanten zum Einsatz.

- **Applikationsseitige Trennung:** Es wird auf Programmebene entschieden, welche Daten erhoben werden und für wen diese zugänglich sind. Den Benutzern werden jeweils nur die Daten angezeigt, die ihren Berechtigungen entsprechen.

Nicht alle Ansätze bieten das gleiche Maß an Sicherheit bezüglich der Datentrennung an. Bei einer rein applikationsseitigen Trennung kann beispielsweise eine Fehlkonfiguration von Berechtigungen leichter zu unbefugten Zugriffsmöglichkeiten führen als bei einer Trennung der Datenhaltung beziehungsweise der Umgebungen. Es ist daher vor der Umsetzung der Mandantentrennung zu prüfen,

welche Variante dem Schutzbedarf der verarbeitenden Daten (insbesondere Gesundheits- und Sozialdaten) gerecht wird.

In jedem Fall sollte eine Trennung von Entwicklungs-, Test- und Produktivsystem erfolgen. Es sollten nur anonymisierte oder pseudonymisierte Testdaten für Software-Tests verwendet werden. Andernfalls sind für die Test- und Entwicklungsumgebungen die gleichen Schutzmaßnahmen anzuwenden wie für die Produktivsysteme.

12.4 Einsatz von Videokonferenzsystemen

Die Nutzung von Videokonferenzsystemen ist während der COVID-19-Pandemie auch im öffentlichen Bereich nicht mehr wegzudenken. Dabei können die Grundanforderungen an ein Videokonferenzsystem ganz unterschiedlich sein. Bei Online-Großveranstaltungen, wie etwa Vorlesungen an Hochschulen oder Webseminaren, müssen insbesondere viele teilnehmende Endgeräte performant und in bestimmten Funktionen zentral steuerbar (etwa bei der Deaktivierung der Mikrofone) vom Videokonferenzsystem verwaltet werden. In anderen Konstellationen hingegen sollen personenbezogene Daten mit einem besonderen Schutzbedarf, beispielsweise sensible Gesundheitsdaten bei einer Videokonferenz zwischen Ärztin oder Arzt und Patientin oder Patient oder nur unter medizinischem Personal und mit einer damit einhergehenden hohen Verfügbarkeitserwartung mittels Videokonferenz ausgetauscht werden.

Solche unterschiedlichen Einsatzbereiche haben nicht nur Auswirkung auf die technische Ausprägung von Videokonferenzsystemen, sondern auch auf datenschutzrechtliche Aspekte. Wie jede der 17 anderen deutschen Datenschutzaufsichtsbehörden werde auch ich in der alltäglichen Beratungspraxis mit unterschiedlichen Videokonferenzlösungen und Fragen zu deren datenschutzrechtlichen Zulässigkeit konfrontiert. In diesem Zusammenhang möchte ich insbesondere auf die Empfehlungen hinweisen, welche die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder in ihrer „Orientierungshilfe Videokonferenzsysteme“ gibt.[77]

Die Auswahl eines bestimmten Videokonferenz-Produkts führt nicht schon zur datenschutzrechtlichen Zulässigkeit von Verarbeitungsvorgängen, die das Videokonferenzsystem als Betriebsmittel nutzen. Vor dem Hintergrund, dass eine bestimmte Videokonferenzlösung unterschiedlich betrieben, konfiguriert, gehandhabt und ganz unterschiedliche Kategorien von personenbezogenen Daten verarbeiten kann, ist nochmals hervorzuheben, dass der Einklang mit der Datenschutz-Grundverordnung nur mit dem datenschutzrechtlichen Dreiklang rechtmäßiger Zweck, tragfähige Rechtsgrundlage sowie rechtmäßige Art und Weise der Verarbeitung nachgewiesen werden kann.

Mit Blick auf die Rechtsgrundlage für eine Datenübermittlung ist besonders erwähnenswert, dass bei Datenübermittlungen in die USA oder andere Drittstaaten die Anforderungen des Kapitels V der DSGVO einzuhalten sind. Der Europäische Gerichtshof hat den Angemessenheitsbeschluss zum EU-US Privacy Shield für ungültig erklärt (siehe Beitrag Nr. 11.2.1). Dieser Regelungsrahmen steht daher

77 Internet: https://www.datenschutzkonferenz-online.de/orientierungshilfen.html.

als Instrument für die Sicherstellung eines angemessenen Schutzes in die USA übermittelter Daten nicht mehr zur Verfügung.

Aus diesem Grund empfehle ich derzeit die Nutzung von Videokonferenzprodukten US-amerikanischer Anbieter sorgfältig zu prüfen. Dies gilt auch, wenn Vertragspartnerin eine europäische Tochtergesellschaft ist.

Im Fall, dass ein Videokonferenzsystem durch einen Auftragsverarbeiter betrieben wird, ist mit ihm ein Auftragsverarbeitungsvertrag abzuschließen, der die Anforderungen des Art. 28 DSGVO erfüllt. Unklarheiten im Auftragsverarbeitungsvertrag sind daher regelmäßig Ausschlusskriterium für die Nutzung des jeweiligen Anbieters.

Ob die Art und Weise der Verarbeitung mit Hilfe eines Videokonferenzsystems in einer betrachteten Konstellation rechtskonform erfolgt, kann erst nach Erstellung einer datenschutzrechtlichen Risikoanalyse beurteilt werden.

Wie ich bereits anhand der Risikoanalyse im Kontext der Datenschutz-Folgenabschätzung dargelegt habe (siehe Beitrag Nr. 12.8), besteht eine Risikoanalyse mindestens aus den Bestandteilen Schwachstelle, Risikoquelle, Risikoszenario, technisch und organisatorische Maßnahmen sowie die Bewertung des Ausgangs- und des Restrisikos.

Generell hat bei der Bereitstellung von Kommunikationsmitteln die jeweils einsetzende bayerische öffentliche Stelle darauf zu achten, dass der Einsatz datenschutzkonform erfolgt. Denn öffentliche Stellen sind in besonderem Maße Recht und Gesetz verpflichtet. Daher sollten sie ein Vorhaben nicht nur bei allgemein erwiesener Unzulässigkeit unterlassen, sondern bereits bei offenen datenschutzrechtlichen Fragen, die sie selbst nicht rechtssicher ausräumen können.

12.5 Löschung von Datenkopien aus Backup-Systemen

Nach Art. 17 Abs. 1 Buchst. a DSGVO sind personenbezogene Daten zu löschen, wenn sie für den ursprünglichen Verarbeitungszweck nicht mehr notwendig sind. Zum Thema Löschung von personenbezogenen Daten habe ich mich in meinen Tätigkeitsberichten bereits mehrfach im Hinblick auf unterschiedliche fachliche Zusammenhängen geäußert (siehe 29. Tätigkeitsbericht 2019 unter Nr. 3.2 und 18. Tätigkeitsbericht 1998 unter Nr. 3.3.3, Nr. 7.2.1.1, Nr. 7.2.4 sowie Nr. 8.1). Diese Thematik wurde nun durch die Fragestellung erweitert, wie die Löschung von Datenkopien, die in Backup-Systemen ausschließlich der Datensicherung dienen, in zeitlicher Hinsicht erfolgen muss.

Der Begriff „Löschung“ wird in der Datenschutz-Grundverordnung nicht näher definiert. Das bisherige deutsche Datenschutzrecht verstand darunter das „Unkenntlichmachen gespeicherter Daten“ (vgl. § 3 Abs. 4 Nr. 5 Bundesdatenschutzgesetz in der bis zum 24. Mai 2018 geltenden Fassung). Somit hat ein datenschutzrechtlicher Löschvorgang eines bestimmten personenbezogenen Datums die Folge, dass dieses nach der Löschung in den Dateisystemen, die dem betroffenen Verantwortlichen zurechenbar sind, weder vorhanden ist noch wiederhergestellt werden kann. Diese Anforderung trifft folglich nicht nur den aktiven produktiven Datenbestand, sondern auch die Datenkopien, die in Backup-Systemen aus Verfügbarkeitsgründen (vgl. Wiederherstellungsanforderung in Art. 32 Abs. 1 Buchst. c

DSGVO) verarbeitet werden. Da eine zeitgleiche Löschung des aktiven personenbezogenen Datums und seiner im Backup-System gespeicherten Kopie oftmals insbesondere aus technischen Gründen nicht zeitgleich, sondern nur zeitversetzt möglich ist, stellt sich die Frage, wie die datenschutzrechtliche Forderung mit dem derzeit technisch sowie organisatorisch Möglichen in Einklang gebracht werden kann.

Nach Erwägungsgrund 26 DSGVO dürfen gelöschte personenbezogene Daten nicht oder nach allgemeinem Ermessen nur mit geringer Wahrscheinlichkeit wiederherstellbar sein. Das bedeutet in der betrachteten Konstellation, dass nach der datenschutzrechtlichen Löschung von Daten im Primärsystemen diese nun nicht mehr vorhandenen personenbezogenen Daten nur mit geringer Wahrscheinlichkeit durch eine Kopie aus dem Backup-System (Reliktdaten) im gerade genannten Sinn wiederherstellbar sein dürfen. Idealerweise sollte daher bei der Neukonzeption von IT-Systemen die Anforderungen einer zeitgleichen Löschung von Daten aus dem Backup mit berücksichtigt werden.

Sollte eine zeitgleiche Löschung trotz Berücksichtigung aller relevanten Schutzmaßnahmen nach Art. 32 DSGVO, also insbesondere nach dem aktuellen Stand der Technik und Organisation nicht möglich sein, ist dies entsprechend zu begründen. Diese dokumentierte Begründung muss auch die umgesetzten Schutzmaßnahmen enthalten oder auf diese verweisen, die ergriffen wurden, damit eine zeitlich verzögerte Löschung der Reliktdaten nur mit geringer Wahrscheinlichkeit zur Reproduzierbarkeit der aus dem Primärsystem gelöschten Daten führen kann.

Im Ergebnis darf die Löschung der Datensicherungskopie nur bei kumulativer Erfüllung folgender Anforderungen zeitlich verzögert von der Löschung des entsprechenden personenbezogenen Datums im Primärsystem erfolgen:

— **Technische Unmöglichkeit oder Unzumutbarkeit:** Bei dem betroffenen Backup-System ist aus Sicht eines verständigen Betrachters oder einer verständigen Betrachterin nachvollziehbar die gleichzeitige Löschung der Datensicherungskopie technisch nicht möglich oder im Hinblick auf den vorliegenden Schutzbedarf der personenbezogenen Daten unverhältnismäßig aufwändig.

— **Löschfrequenz im Backup-System:** Die Wiederholungsfrequenz der allgemeinen Löschung sowie gegebenenfalls außerordentliche Löschungen nicht mehr benötigter Datensicherungskopien richtet sich im Backup-System nach dem Schutzbedarf der betroffenen personenbezogenen Daten. Die umgesetzte Löschstrategie für die Datensicherungskopien im Backupsystem wird in Form eines Datensicherungskonzeptes nachgewiesen. Dieses Konzept enthält insbesondere auch wichtige Aspekte zum datenschutzrechtlichen Grundsatz der Erforderlichkeit, wie etwa das zum Einsatz kommende Sicherungsverfahren (zum Beispiel vollständig, differenziell, inkrementell, Spiegelung) und das gegebenenfalls verwendete Generationenprinzip. Erläuterungen hierzu und weitergehende Informationen sind etwa in den „Umsetzungshinweisen zum Baustein CON.3 Datensicherungskonzept“ des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu finden.[78]

78 Bundesamt für Sicherheit in der Informationstechnik, Umsetzungshinweise zum Baustein

- **Verfügbarkeit nur mittels Wiederherstellung:** Es ist hinreichend sichergestellt, dass die Datensicherungskopien ausschließlich über die vorgesehene Wiederherstellungsfunktionalität aus dem Backup-System ausgelesen werden können. Zur Absicherung der ausschließlichen Verwendung dieser Wiederherstellungsfunktion sind geeignete Schutzmaßnahmen umzusetzen, wie insbesondere der Einsatz kryptografischer Verfahren für die Datensicherungskopien im Backup-System (vgl. Art. 32 Abs. 1 Buchst. a DSGVO und den Punkt „CON.3.A13 Einsatz kryptografischer Verfahren bei der Datensicherung“ aus dem IT-Grundschutz-Baustein „CON.3 Datensicherungskonzept“ des Bundesamts für Sicherheit in der Informationstechnik).[79]

- **Löschung bei Wiederherstellung:** Bei jeder Wiederherstellung von Daten aus dem Backup-System muss gewährleistet sein, dass alle Daten, die im Primärsystem aus Datenschutzgründen bereits gelöscht wurden (Reliktdaten), nicht wiederhergestellt oder – falls technisch nicht anders möglich – so nach der Wiederherstellung wieder gelöscht werden, so dass ihre rechtswidrige Verarbeitung ausgeschlossen ist.

- **Dokumentation und Umsetzungsnachweis**: Der Verarbeitungsvorgang „Backup-System verwenden“ ist geeignet zu dokumentieren und dessen wirksame Umsetzung nachzuweisen. Dabei ist insbesondere darauf zu achten, dass jede Wiederherstellung von Daten unter Angabe des Wiederherstellungsgrundes und der gegebenenfalls rechtzeitig durchgeführten Löschung von Reliktdaten dokumentiert wird.

12.6 Altsysteme und veraltete Softwarearchitekturen

Viele in öffentlichen Stellen genutzte Fachverfahren haben eine sehr lange Einsatz- und Lebensdauer, nicht zuletzt aufgrund des großen Aufwands für die Einführung neuer Software sowohl für den Anbieter als auch für die Nutzerinnen und Nutzer. Dies führt dazu, dass in der Zwischenzeit veraltete Programmiersprachen, Softwarekomponenten und -architekturen zum Einsatz kommen, die Sicherheitslücken bezüglich aktueller Angriffsszenarien aufweisen. Zudem stellt insbesondere für die Fehlerbehebung und Wartung die Rekrutierung geeigneter Beschäftigter ein Problem dar.

Im aktuellen Prüfzeitraum wurde mir ein Angriffsszenario auf Software für Fachverfahren gemeldet, die noch auf einer Zwei-Schichten-Architektur (klassische Client-Server-Architektur) basiert. Bei dieser Architektur übernimmt der Client sowohl die Darstellung der Benutzerschnittstelle als auch die Logik der Anwendung, das heißt unter anderem die Steuerung des Datenbankzugriffs. Dadurch entsteht das Risiko, dass clientseitig Sicherheitsmaßnahmen wie beispielsweise das Berechtigungskonzept umgangen und Seitenkanäle geöffnet werden können. Bei Drei-Schichten-Architekturen übernimmt diese Funktion eine eigene Logik-

CON.3 Datensicherungskonzept, Internet: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Umsetzungshinweise/umsetzungshinweise_node.html.

79 Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Baustein CON.3 Datensicherungskonzept, Internet: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/03_CON_Konzepte_und_Vorgehensweisen/CON_3_Datensicherungskonzept_Edition_2021.html.

Schicht (Middleware), so dass eine Umgehung der Sicherheitsmaßnahmen durch den Client nicht mehr möglich ist, sondern alle Zugriffe nur noch über die Middleware als zentrale Stelle gesteuert werden.

Letztendlich sollten die betroffenen Fachverfahren vom Anbieter zeitnah auf eine Drei-Schichten-Architektur gehoben werden. Der Aufwand für derartige Umstellungen ist hierbei nicht unerheblich. In dem oben erwähnten konkreten Fall musste nicht nur von Seiten des Herstellers die Software angepasst werden, für den Übergangszeitraum mussten auch zahlreichen Hilfsmaßnahmen entwickelt, umgesetzt und an die Nutzer der Software kommuniziert werden, so dass hierdurch umfangreich Ressourcen gebunden wurden. Zudem muss sichergestellt sein, dass die nutzenden Stellen entsprechende Updates auch zeitnah einspielen, um die Sicherheitslücken auch vor Ort zu schließen.

Im Baustein OPS.1.1.3 „Patch- und Änderungsmanagement" des IT-Grundschutzkompendiums des Bundesamts für Sicherheit in der Informationstechnik[80] wird bereits in der Einleitung dargestellt, wie wichtig es ist, die Komponenten der Informationstechnik aktuell zu halten. Dies begründet das BSI mit der immer schneller werdenden Entwicklung in der Informationstechnik. Der Baustein beschränkt sich zwar auf Systeme und Anwendungen, zu denen Patches und Änderungen von Herstellern bereitgestellt werden. Die schnelle Fortentwicklung der Informationstechnik begründet aber auch, dass Systeme oder Anwendungen, die angepasst an den eigenen Bedarf oder den einer Kundengruppe entwickelt werden, ebenfalls regelmäßig darauf überprüft werden müssen, ob die eingesetzten Technologien noch auf dem Stand der Technik sind.

Wie bereits erwähnt, können im Verlauf des Nutzungszeitraums der Software Angriffsmöglichkeiten bekannt geworden sein, so dass nachträglich Sicherheitsmechanismen installiert werden müssen, die den Angriffsvektor schließen. Ob dies vollumfänglich möglich ist, hängt von vielen Faktoren ab, die unter Umständen vom Nutzer nicht zu beeinflussen sind.

Neben der Sicherheit stellt aber auch die Umsetzung neuer Anforderungen an Systeme eine Herausforderung dar. So entstanden beispielsweise im Zuge der Datenschutzreform zusätzliche Anforderungen bezüglich der Betroffenenrechte oder der Rechenschaftspflichten von Seiten des Verantwortlichen.

In diesem Zusammenhang empfehle ich sowohl den Herstellern von Fachverfahren als auch öffentlichen Stellen, die selbst Software entwickeln oder auch im Auftrag entwickeln lassen, regelmäßig zu prüfen, ob die eingesetzten Technologien noch dem Stand der Technik entsprechen. Zudem sollte eine rechtzeitige Auseinandersetzung mit der Notwendigkeit einer Neu- oder Weiterentwicklung erfolgen.

Zusätzlich sollten insbesondere Altsysteme und -anwendungen, die noch nicht aktualisiert oder ausgetauscht werden konnten, im besonderen Fokus von regelmäßigen Penetrationstests stehen, um neu entstandene Angriffsszenarien schnellstmöglich erkennen und Gegenmaßnahmen einleiten zu können. Desweiteren muss regelmäßig geprüft werden, ob im Rahmen des Betriebs des Altverfahrens

[80] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_1_1_3_Patch_und_Aenderungsmanagement_Edition_2021.pdf.

zusätzliche Sicherheitsmaßnahmen ergriffen werden können, die die bestehenden Risiken und Gefährdungen abschwächen können („Workaround“). Hierfür bietet sich beispielsweise die Virtualisierung von Arbeitsplätzen an.

12.7 Sicherheitslücken in Lernplattform

Bezüglich der Lernplattform „mebis“ wurde ich von einem Bürger auf mehrere möglicherweise sicherheitskritische Schwachstellen der Webanwendung hingewiesen. Er gab an, diese bereits vor einiger Zeit an den Verantwortlichen gemeldet zu haben, eine Behebung sei aber noch nicht erfolgt. Durch eigene Tests konnte das Bestehen der Lücken bestätigt werden.

Um die Schwachstellen möglichst zeitnah zu beheben, informierte ich das Landesamt für Sicherheit in der Informationstechnik, das umgehend Sicherheitsmaßnahmen zur Abmilderung der Lücken ergriff. Zeitnah wurden dann auch vom Bayerischen Staatsministerium für Unterricht und Kultus die Sicherheitslücken schrittweise behoben.

Dies zeigt erneut, wie wichtig es ist, dass Verantwortliche insbesondere auch schon länger im Betrieb befindliche Webanwendungen in regelmäßigen Abständen auf Sicherheitslücken prüfen, damit diese möglichst gefunden und behoben werden können, bevor potentielle Angreifer sie ausnutzen. Auch sollte Hinweisen auf mögliche sicherheitsrelevante Schwachstellen eine hohe Priorität eingeräumt werden.

12.8 Umsetzung einer Datenschutz-Folgenabschätzung (DSFA)

Immer mehr bayerische öffentliche Stellen führen eine Datenschutz-Folgenabschätzung (DSFA) in den für sie relevanten Verarbeitungsbereichen durch. Die in Art. 35 DSGVO geregelte Datenschutz-Folgenabschätzung (dazu bereits mein 28. Tätigkeitsbericht 2018 unter Nr. 3.1.3 sowie mein 29. Tätigkeitsbericht 2019 unter Nr. 12.2) ist ein Verfahren, in welchem Risiken aus Blick des Datenschutzes strukturiert ermittelt und bewertet sowie risikoreduzierende Gegenmaßnahmen festgelegt und wirksam umgesetzt werden.

Die Datenschutz-Grundverordnung selbst gibt mit den relativ abstrakt formulierten Anforderungen an die DSFA keine Antworten auf wichtige Methodenfragen und konkrete Vorgehensschritte. Die Entscheidung für eine bestimmte DSFA-Methode, die dann auch praxisgerecht durchführbar ist, ist für den einen oder anderen Verantwortlichen noch mit Schwierigkeiten verbunden. Zwar finden sich in der Literatur immer häufiger Fundstellen hierzu. Aus Praxissicht sind diese Hinweise aber oft noch sehr theorielastig und bieten keine anschaulichen Beispiele.

Da eine veröffentlichte DSFA oder auch nur veröffentlichte Ausschnitte einer DSFA immer noch recht schwer zu finden sind, werden die von mir publizierten Arbeitshilfen, die einzelne DSFA-Arbeitsschritte anhand von konkreten Beispielen veranschaulichen und erleichtern, als Arbeitsgrundlage von bayerischen öffentlichen Stellen und weiteren Einrichtungen gerne angenommen. Dabei hilft die darin enthaltene Fokussierung auf das Wesentliche und die Konkretisierung der Mindestanforderungen an eine DSFA.

Die von mir empfohlene Methode, die auf bereits Bestehendes und Anerkanntes Bezug nimmt und dieses kombiniert, erscheint in der Praxis als ausreichend verständlich, flexibel und skalierbar. So dienen meine Empfehlungen bereits als Basis für die DSFA von einfacheren und komplexeren folgenabschätzungspflichtigen Verarbeitungsvorgängen sowie als Grundlage für eine gesetzliche DSFA nach Art. 14 Abs. 1 Nr. 2 BayDSG.

Auf entsprechende Nachfragen hin habe ich diesen „Werkzeugkasten" nun um ein weiteres Formular ergänzt, mit dessen Hilfe die Durchführung einer DSFA-Erforderlichkeitsprüfung dokumentiert und nachgewiesen werden kann.[81] Die DSFA-Erforderlichkeitsprüfung ist eine notwendige Vorprüfung, die nicht mit der eigentlichen Durchführung einer DSFA verwechselt werden darf.

Wie in der Orientierungshilfe „Datenschutz-Folgenabschätzung"[82] ausführlich dargestellt, muss das Ergebnis dieser Erforderlichkeitsprüfung insbesondere auch dann dokumentiert werden, wenn der Verantwortliche zu der Auffassung gelangt, dass ein Verarbeitungsvorgang nicht folgenabschätzungspflichtig ist.

Die Bereitstellung von Arbeitshilfen ist eine Möglichkeit, die Durchführung einer DSFA zu erleichtern. Weitere Synergiepotenziale könnten genutzt werden, wenn durchgeführte DSFA-Beispiele in geeigneter Art und Weise durch den jeweiligen Verantwortlichen publiziert werden würden. Denn ist eine DSFA erforderlich, kann eine weitere DSFA-Durchführung im Einzelfall insbesondere dann unterbleiben, falls eine DSFA für einen ähnlichen Verarbeitungsvorgang mit ähnlich hohen Risiken bereits vorhanden ist (Art. 35 Abs. 1 Satz 2 DSGVO). Der Verantwortliche hat diese Voraussetzungen zu prüfen. Das Ergebnis der Prüfung, einschließlich einer Begründung für den Verzicht auf die Durchführung einer weiteren DSFA, ist zu dokumentieren. Ist die Voraussetzung des Art. 35 Abs. 1 Satz 2 DSGVO erfüllt, kann der Verantwortliche die vorhandene, bereits durchgeführte DSFA auch für seinen geplanten Verarbeitungsvorgang mit gegebenenfalls unwesentlichen Anpassungen übernehmen.

Zudem kann nach Art. 14 BayDSG die Durchführung einer weiteren DSFA durch den Verantwortlichen unterbleiben, soweit

— eine solche für den Verarbeitungsvorgang bereits vom fachlich zuständigen Staatsministerium oder einer von diesem ermächtigten öffentlichen Stelle durchgeführt wurde und dieser Verarbeitungsvorgang im Wesentlichen unverändert übernommen wird (Art. 14 Abs. 1 Nr. 1 BayDSG),

— ein automatisiertes Verfahren, das zum Einsatz durch öffentliche Stellen bestimmt ist, durch eine öffentliche Stelle (zum Beispiel die Anstalt für Kommunale Datenverarbeitung in Bayern – AKDB) entwickelt wurde, die entwickelnde Stelle eine DSFA durchgeführt hat und das Verfahren im Wesentlichen unverändert übernommen wird (Art. 14 Abs. 2 BayDSG), oder

— der konkrete Verarbeitungsvorgang in einer Rechtsvorschrift geregelt ist und im Rechtsetzungsverfahren bereits eine DSFA erfolgt ist, es sei denn,

81 Vgl. das Modul 2 „DSFA-Erforderlichkeitsprüfung", Internet: https://www.datenschutz-bayern.de, Rubrik „DSFA".

82 Vgl. Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz-Folgenabschätzung, Orientierungshilfe, Internet: https://www.datenschutz-bayern.de, Rubrik „DSFA".

dass in der Rechtsvorschrift etwas anderes bestimmt ist (Art. 14 Abs. 1 Nr. 2 BayDSG).

Durch die Regelungen des Art. 14 BayDSG und Art. 35 Abs. 1 Satz 2 DSGVO entfällt also nicht das Erfordernis einer DSFA als solches. Vielmehr wurde diese bereits im Gesetzgebungsverfahren (Art. 14 Abs. 1 Nr. 2 BayDSG) beziehungsweise durch eine andere Stelle (Art. 14 Abs. 1 Nr. 1, Abs. 2 BayDSG) durchgeführt, oder es kann eine DSFA für einen ähnlichen Verarbeitungsvorgang mit ähnlich hohen Risiken verwendet werden (Art. 35 Abs. 1 Satz 2 DSGVO). Eine weitere DSFA durch den Verantwortlichen kann somit unterbleiben, wenn dieser eine bereits entsprechend durchgeführte DSFA „als eigene" übernimmt.

12.9 Best-Practice-Prüfkriterien zur Cybersicherheit für medizinische Einrichtungen

Auch in diesem Berichtszeitraum nahm die Zahl der Angriffe mit Schadsoftware auf öffentliche Stellen weiter zu. Gerade Angriffe auf Gesundheitseinrichtungen in Zeiten der Pandemie zeigen, wie wichtig es ist, hier ausreichende technische und organisatorische Sicherheitsmaßnahmen umzusetzen. Grundlegendes hierzu habe ich bereits meinem 29. Tätigkeitsbericht unter Nr. 12.3 dargestellt.

Zudem haben der Bayerische Landesbeauftragte für den Datenschutz und das Bayerische Landesamt für Datenschutzaufsicht gemeinsam eine Checkliste mit Best-Practice-Maßnahmen zur Sicherstellung der Verfügbarkeit bezüglich Cyberattacken in medizinischen Einrichtungen erstellt. Diese ist auf meiner Homepage abrufbar.[83]

Diese Handreichung ermöglicht einen Überblick über einige Praxismaßnahmen zur Cybersicherheit für medizinische Einrichtungen – inklusive eines Themenblocks speziell für Labore – entsprechend den geltenden gesetzlichen Datenschutzvorgaben. Im Sinne einer gezielten Prävention soll damit eine gesteigerte Sensibilisierung für sicherheitsrelevante Themen erreicht und aktiv ein störungsfreier Betrieb dieser Einrichtungen unterstützt werden. Der Fokus des Dokuments liegt auf der Verfügbarkeit der Daten und Dienste bezüglich Angriffen aus dem Internet und weniger auf deren Vertraulichkeit und Integrität, die aus Datenschutzsicht jedoch ebenfalls zu beachten sind. Die aufgeführten Maßnahmen sind nicht als abschließend zu betrachten, sondern stellen einen Best-Practice-Ansatz dar, der einen effektiven Schutz gegen aktuelle Cybersicherheitsbedrohungen unterstützen kann.

12.10 Meldungen von Verletzungen des Schutzes personenbezogener Daten

Die Zahl der Meldungen nach Art. 33 DSGVO ist auch in diesem Berichtszeitraum weiterhin steigend und zeigt, dass die bayerischen öffentlichen Stellen die gesetzlichen Pflichten dahingehend ernst nehmen. Erfreulich ist zudem, dass diese beinahe ausschließlich über das Online-Formular auf meiner Homepage unter

[83] Der Bayerische Landesbeauftragte für den Datenschutz/Bayerisches Landesamt für Datenschutzaufsicht, Cybersicherheit für medizinische Einrichtungen, Stand 5/2020, Internet: https://www.datenschutz-bayern.de, Rubrik „Corona-Pandemie – Cybersicherheit für medizinische Einrichtungen".

https://www.datenschutz-bayern.de abgegeben wurden und lediglich eine geringe Zahl an Meldungen über einen anderen Weg einging.

Ein großer Anteil von Meldungen lässt sich auch dieses Mal wieder auf Bereiche zurückführen, in denen sensible medizinische Daten oder Sozialdaten verarbeitet werden. Bedauerlicherweise handelt es sich zum Großteil um die gleichen Probleme, die ich schon in meinem letzten Tätigkeitsbericht dargestellt habe:

Datenfehlübermittlungen

Die Hauptlast der gemeldeten Datenpannen betraf die Thematik, dass Daten oder Unterlagen per Postversand oder auch elektronisch unbeabsichtigt an unberechtigte Empfänger übermittelt wurden.

Papierversand

Diesen Vorfällen lagen meist eine unkorrekte Adressierung und eine fehlerhafte Zusammenstellung oder falsche Kuvertierung von Unterlagen zugrunde, sowohl durch fehlerhafte Konfiguration von Kuvertiermaschinen als auch bei der händischen Zusammenstellung. Dies fiel insbesondere häufiger in Krankenhäusern auf, wenn den Patientinnen oder Patienten Unterlagen mitgegeben wurden.

Falscheingabe der Telefaxnummer

Zu meinem Leidwesen nahmen in diesem Berichtszeitraum Meldungen eines unsachgemäßen Versands von vertraulichen Unterlagen an unberechtigte Empfängerinnen und Empfänger über Telefax nicht ab. An dieser Stelle möchte ich weiterhin betonen, dass gerade für die Übermittlung sensibler Daten wie Gesundheits- oder Sozialdaten der Telefaxversand lediglich in Ausnahmefällen, und wenn, dann exakt und kontrolliert, genutzt werden sollte. Ferner sollte stets geprüft werden, ob nicht auch ein alternatives Kommunikationsmedium zur Verfügung steht und eine verschlüsselte elektronische Übersendung der Daten möglich ist.

(Unverschlüsselte) E-Mails an falsche Adressaten

Ebenso blieb die fehlerhafte Adressierung von E-Mail ein leidiges Thema. Hierbei trat häufiger das Problem auf, dass bei der Eingabe der E-Mail-Adresse nicht ausreichend überprüft wurde, ob es sich tatsächlich um die gewünschte Empfängerin oder den gewünschten Empfänger handelte (beispielsweise „Autovervollständigen“). Dadurch wurden die E-Mails an falsche Empfängerinnen und Empfänger versandt. Hinzu kommt die Problematik, dass E-Mails mit sensiblen Inhalten unverschlüsselt über das Internet verschickt wurden, wenn die eigentlich vorgesehene Empfängerin oder der eigentlich vorgesehene Empfänger eine andere Beschäftigte oder ein anderer Beschäftigter der öffentlichen Stelle war.

„cc“ statt „bcc“

Obwohl schon vielfach darauf hingewiesen, kommt es auch weiterhin beim elektronischen Versand von Unterlagen an mehrere Adressatinnen und Adressaten zu einem Versand per „cc“, so dass jeweils alle Empfängerinnen und Empfänger Kenntnis der E-Mail-Adressen aller vom Verteiler umfassten Personen erhalten haben. Dies ist insbesondere kritisch zu sehen, wenn es sich dabei nicht um dienstliche E-Mail-Adressen handelt. Wie zuletzt in meinem 27. Tätigkeitsbericht unter

Nr. 2.1.3 hinreichend erläutert, lässt sich diesem Umstand ohne zusätzlichen Aufwand dadurch begegnen, dass bei der Eingabe in den Header der E-Mail das „bcc“-Feld anstelle des „cc“-Feldes verwendet wird.

Hackerangriffe, Schadsoftware oder Systemausfälle

Zu meinem Bedauern blieben auch weiterhin Behörden, Kliniken, Universitäten und andere öffentliche Stellen von Hackerangriffen, Schadsoftware oder Systemausfällen nicht verschont. Gerade kleinere öffentliche Stellen wie Gemeinden oder freiwillige Feuerwehren sind zunehmend von Schadsoftware betroffen. Wie die Meldungen auch zeigen, sind die Ausfall- und Bereinigungszeiten bei einem Schadcodebefall sehr unterschiedlich.

Dass manche öffentliche Stellen gegenüber dem Angriff durch die feindliche Schadsoftware besser aufgestellt waren als andere und nur wenig bis gar keine Ausfallzeiten hatten, beruhte hauptsächlich auf zwei Gründen: Zum einen standen ihnen geschulte und sicherheitsbewusste Mitarbeiterinnen und Mitarbeitern zur Verfügung, die E-Mail-Eingänge bei Unklarheiten durch Nachfrage bei einer (angeblichen) Absenderin oder einem (angeblichen) Absender auf deren Korrektheit überprüften und keine ausführbaren Anhänge ohne Verifikation öffneten. Zum anderen verfügten sie über eine funktionstüchtige Basis-IT, in deren Sicherheit investiert wurde. Wie bereits in meinem 29. Tätigkeitbericht 2019 unter Nr. 12.3 dargestellt, sollte in jedem Fall die Verwendung von aktuellen Betriebssystemversionen, das Einspielen von Sicherheitsupdates sowie der Einsatz von aktueller Virenschutzsoftware sichergestellt sein und eine Netzwerksegmentierung unterstützt werden, um gefährdete Bereiche abzuschotten. Zudem müssen Maßnahmen hinsichtlich des Umgangs mit E-Mails und der Internet-Nutzung ergriffen werden.

Um gegenüber Verschlüsselungstrojanern gut aufgestellt zu sein, sind eine gut funktionierende Back-Up-Lösung und Notfallpläne zwingend notwendig.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat zum Thema Cyber-Sicherheit einen umfassenden und regelmäßig aktualisierten Themenkatalog auf seiner Homepage veröffentlicht.[84]

Bei einem Befall mit Schadsoftware rate ich dringend, das Bayerische Landeskriminalamt für weitere Ermittlungen einzuschalten. Ebenso empfiehlt es sich, das Bayerische Landesamt für Sicherheit in der Informationstechnik von den Vorfällen in Kenntnis zu setzen.

„Neugierzugriffe“

Eine weitere Problematik trat durch die COVID-19-Pandemie verschärft hervor, nämlich sogenannte **Neugierzugriffe** durch Beschäftigte in Krankenhäusern auf Patientenakten, insbesondere von Verwandten und anderen Personen aus dem sozialen Umfeld. Im Berichtszeitraum ging eine erhöhte Zahl von Meldungen solcher Datenschutzverstöße bei mir ein. Die Bandbreite dieser Verstöße reichte von Meldungen über Beschäftigte, die unberechtigt über das Krankenhausinformationssystem auf Daten von Kolleginnen oder Kollegen zugegriffen hatten, bis hin zu

[84] Internet: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/oeffentliche-verwaltung_node.html.

Meldungen über Beschäftigte, die aus Sorge um Angehörigen handelten, die Patientinnen oder Patienten in ihrer Einrichtung waren.

Auch wenn ich die Sorgen und Absichten der Beschäftigten verstehe, möchte ich dennoch darauf hinweisen, **dass Datenzugriffe durch Personal in Krankenhäusern nur dann erfolgen dürfen, wenn dies für dienstliche Zwecke wie beispielsweise im Rahmen einer Heilbehandlung erforderlich ist.** Ein Zugriff aus familiären oder freundschaftlichen Gründen fällt nicht hierunter, selbst wenn die „ausgeforschte" Person (im Nachhinein) ihre Zustimmung zu gegeben hat. In allen Fällen wurden dienstliche Verwarnungen oder Abmahnungen an die betreffenden Beschäftigten ausgesprochen.

Gerade in Krisenzeiten wird offenkundig, ob das Personal im Vorfeld genügend für den Datenschutz sensibilisiert worden ist und die Datenschutzthemen auch im täglichen Berufsalltag umsetzt. Deshalb sind Datenschutzschulungen und ein funktionstüchtiges Datenschutzmanagement die Basis für eine funktionierende Zusammenarbeit innerhalb der Organisation.

12.11 Beanstandungen wegen technisch-organisatorischer Mängel

12.11.1 Beanstandung nach unbeabsichtigtem Versand einer Bewerberdatei

Eine Beanstandung betraf den Versand von Bewerberdaten. Mittels E-Mail mit unverschlüsseltem Dateianhang wurden personenbezogene Daten von mehr als tausend Bewerbern für die Warteliste der Gymnasiallehrkräfte an hunderte unbefugte Empfängerinnen und Empfänger übermittelt.

Bei dem Dateianhang handelte es sich um ein Excel-Dokument, das unter anderem die jeweils unterrichteten Fächerkombinationen der Bewerberinnen und Bewerber enthielt. Diese Liste sollte im Hinblick auf die Vergabe von weiteren Beschäftigungsmöglichkeiten zur internen Verwendung genutzt werden.

Beabsichtigt war, die auf der Warteliste stehenden Personen über die noch bestehenden Personallücken und die Möglichkeit der Anstellung mit einem Aushilfsvertrag an einer Förderschule zu informieren. Tatsächlich wurde die Liste dabei dann versehentlich als Anhang mit versandt.

Der Versand erfolgte blockweise für jeweils 50–150 Empfängeradressen ohne Verwendung der „bcc"-Funktion.

Insbesondere da das Anhängen der Excel-Datei versehentlich erfolgte, wurde dementsprechend keine Verschlüsselung der E-Mails vorgenommen.

Es handelte sich aus technisch-organisatorischer Sicht unter mehreren Gesichtspunkten um einen Datenschutzverstoß:

— Durch den Versand mittels mit „cc" anstatt „bcc" wurden alle Empfängeradressen der E-Mail den anderen Empfängern bekannt.

— Durch den unbeabsichtigten Anhang der Excel-Datei erfolgte ein Versand von Daten an unberechtigte Empfänger.

— Durch den unverschlüsselten Versand hätte deren Inhalt grundsätzlich von allen technisch zwischen Sender und Empfänger liegenden Zwischenstationen des E-Mail-Versandes eingesehen werden können.

— Zudem hätten vom Empfänger genutzte Dienstanbieter möglicherweise die Daten einsehen oder auswerten können.

Von Seiten der verantwortlichen Stelle wurden insbesondere der Grundsatz der Vertraulichkeit der Kommunikation Art. 5 Abs. 1 Buchst. f in Verbindung mit Art. 32 Abs. 1 Buchst. b DSGVO nicht beachtet.

Zugleich verstieß der Versand gegen die besonderen beamtenrechtlichen Datenschutzregeln. Gemäß Art. 103 Satz 1 Nr. 1 Bayerisches Beamtengesetz (BayBG) darf der Dienstherr personenbezogene Daten über Bewerber und Bewerberinnen sowie aktive und ehemalige Beamte und Beamtinnen nur verarbeiten, soweit dies zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere zu Zwecken der Personalverwaltung oder Personalwirtschaft erforderlich ist. Sollen die Daten für andere Zwecke verarbeitet werden, erfordert dies regelmäßig eine Einwilligung der betroffenen Person (vgl. § 50 Satz 4 Beamtenstatusgesetz – BeamtStG). Dieser Maßstab gilt auch für vertraglich beschäftigte Personen im öffentlichen Dienst (vgl. Art. 145 Abs. 2 BayBG).

Der Versand der Tabelle erfüllt die Voraussetzungen einer Verarbeitung im Sinne des Art. 103 BayBG, da als Verarbeitung jede Form der Verbreitung oder Bereitstellung personenbezogener Daten gilt (vgl. Art. 4 Nr. 2 DSGVO). Diese Datenverarbeitungen waren aber nicht zu einem der in Art. 103 Satz 1 Nr. 1 BayBG genannten Zwecke erforderlich, insbesondere nicht für die Personalverwaltung oder die Personalwirtschaft, und damit unzulässig. Im Übrigen fehlte es an einer Einwilligung im Sinne des § 50 Satz 4 BeamtStG.

Da auch die Fächerkombination der Lehrkräfte enthalten war, könnten im Falle von Religionslehrerinnen und Religionslehrern auch religiöse Überzeugungen betroffen sein. Diese gehören nach Art. 9 Abs. 1 DSGVO zu besonderen Kategorien personenbezogener Daten, deren Verarbeitung besonderen Schutzes bedarf.

Weiterhin war festzustellen, dass zwar eine Meldung der Datenschutzverletzung an mich erfolgte, allerdings nicht innerhalb der nach Art. 33 Abs. 1 DSGVO vorgegebenen 72 Stunden nach Bekanntwerden. Ein Grund für die Verzögerung wurde mir nicht dargelegt.

Den Verstoß gegen datenschutzrechtliche Vorschriften habe ich daher förmlich beanstandet (Art. 16 Abs. 4 Satz 1 BayDSG).

12.11.2 Beanstandung eines Landratsamts wegen des Verlusts von Festplatten

Beim Kauf einer gebrauchten Festplatte auf ebay musste der Käufer feststellen, dass darauf in großem Umfang personenbezogene Daten eines Landratsamts gespeichert und ohne technische Hindernisse auslesbar waren. Unter den Daten fanden sich unter anderem eine Vielzahl von Unterlagen der Zulassungsstelle, aber auch E-Mails des Jugendamts sowie erstmalige Zugangsdaten für neue Benutzer zu verschiedenen Online-Diensten.

Das betroffene Landratsamt war bis zu diesem Vorfall davon ausgegangen, dass auf den Festplatten der Arbeitsplatz-PCs keine personenbezogenen Daten gespeichert würden, sondern diese nur in den jeweiligen Fachverfahren, im Dokument-Management-System oder auf zentralen Fileservern abgelegt seien. Daher wurde aufgrund befürchteter praktischer Probleme bis zu diesem Vorfall auf eine Verschlüsselung der Festplatten verzichtet.

Ursache des Vorfalls war, dass das Landratsamt Leasing-PCs für seine Arbeitsplätze einsetzte, bei denen Festplattendefekte auftraten. Aufgrund dieser Defekte mussten mehrere Festplatten ausgetauscht werden. Entgegen dem eigentlich üblichen Vorgehen, wurden diese Festplatten nicht vor der Rückgabe an den Leasingdienstleister im Landratsamt datenschutzgerecht gelöscht. Die Löschung sollte stattdessen durch den Lieferanten der PCs erfolgen.

Allerdings musste im Nachgang des Kaufs der Festplatte auf ebay festgestellt werden, dass zwischen dem Landratsamt und dem Dienstleister vertraglich keine Zerstörung der Festplatten vereinbart worden war, wenn diese bei einem Austausch an den Hersteller zurück gesandt wurde. Somit gingen die Festplatten wieder in das Eigentum des Herstellers über, der sie dementsprechend auch weiterverkaufen durfte. Wurden die Festplatten zuvor etwa auf Grund von Defekten nicht vollständig gelöscht, so waren die darauf befindlichen Daten weiterhin gespeichert.

Es handelt sich bei diesem Vorfall um einen gravierenden Datenschutzverstoß insbesondere gegen die Anforderungen an die Vertraulichkeit gemäß Art. 5 DSGVO. Erschwerend kommt hinzu, dass es sich zumindest im Falle der Daten des Jugendamtes um besonders schützenswerte Sozial- und Gesundheitsdaten handelt.

Insgesamt wurden somit keine ausreichenden technischen und organisatorischen Maßnahmen gemäß Art. 25 und 32 DSGVO umgesetzt, da die ausgetauschten Festplatten weder verschlüsselt waren noch im Landratsamt vorab gelöscht wurden. Zudem ist das Landratsamt seinen Pflichten als Verantwortlicher gemäß Art. 24 DSGVO nicht nachgekommen, da zusätzlich zu den technischen Mängeln auch kein Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO vorhanden war.

Daher habe ich das Landratsamt förmlich gemäß Art. 16 Abs. 4 Satz 1 BayDSG beanstandet. Zudem habe ich das Landratsamt aufgefordert, Maßnahmen zu ergreifen, um eine Wiederholung derartiger Probleme zu verhindern und die Betroffenen über den Vorfall gemäß Art. 34 DSGVO zu informieren. Dem ist das Landratsamt nachgekommen.

12.11.3 Beanstandung nach dem Verlust einer Personalratsakte

Ein Personalratsmitglied einer bayerischen Gemeinde hat nach einer Personalratssitzung seinen Aktenordner, der die vom Personalratsmitglied selbst zusammengestellten Unterlagen für die Personalratssitzung enthielt, auf dem Rückweg in sein Büro an einem unbekannten Ort verloren. Trotz intensiver Suche konnte der Aktenordner nicht wieder gefunden werden.

Nach den Erinnerungen des Personalratsmitglieds konnte der Inhalt des verlorenen Aktenordners rekonstruiert werden. Die Begutachtung dieser Unterlagen ergab, dass im Hinblick auf den Datenschutz insgesamt über 30 Personen vom Verlust der verlorenen Unterlagen betroffen waren. Die gemeindliche Risikoeinschätzung führte zum Ergebnis, dass der Ordnerverlust für über zehn betroffene

Personen voraussichtlich ein hohes oder sehr hohes Risiko zur Folge hatte. Nach der gemeindlichen Information der Personen, die von diesem Verlust betroffen waren, reichte eine der betroffenen Personen Beschwerde bei mir ein, die aufgrund organisatorischer Defizite zu einer datenschutzrechtlichen Beanstandung der betroffenen Gemeinde führte.

Das in diesem Fall eingetretene datenschutzrechtliche Risiko zeigt, dass der Personalrat auf die wirksame Umsetzung technischer und organisatorischer Schutzmaßnahmen genau achten muss. Insbesondere der Transport von Papierunterlagen mit sensiblen Personalratsangelegenheiten birgt ein Verlustrisiko, das unter anderem durch folgende Maßnahmen deutlich reduziert werden kann:

- **Risikoanalyse durchführen:** Das Risiko, sensible Personalratsunterlagen zu verlieren, ist eines von mehreren Risikoszenarien, das bei der entsprechend durchzuführenden datenschutzrechtlichen Risikoanalyse zu betrachten ist. In aller Regel sind nach der Bewertung des Ausgangsrisikos geeignete Schutzmaßnahmen wirksam umzusetzen, um dieses Risiko auf ein vertretbares Niveau zu reduzieren.

- **Transport vermeiden:** Bestehende Potenziale, sensible Personalratsunterlagen nicht unnötig zu transportieren, sind zu realisieren. Dabei können digitale Hilfsmittel, beispielsweise eine zentrale digitale Ablage mit geeignetem Zugriffsschutz und weiteren Sicherheitsvorkehrungen, von Nutzen sein.

- **Transport absichern:** Sensible Personalratsunterlagen, bei denen ein Transport unverzichtbar ist, müssen geeignet abgesichert transportiert werden. Je nach Risikolage ist etwa bei Papierunterlagen auf verschlossene Sicherheitstransportbehälter und bei Digitalunterlagen auf geeignete Verschlüsselung zu achten.

- **Konsequent löschen:** Sobald Personalratsunterlagen für den ursprünglichen Verarbeitungszweck nicht mehr notwendig sind, sind diese zu löschen oder zu anonymisieren.

  Dieser Anforderung folgend hat etwa der Personalrat der vom Verlust betroffenen Gemeinde einen Aktenvernichter in dem Raum, in dem die Personalratssitzungen stattfinden, aufstellen lassen. Unmittelbar nach jeder Personalratssitzung werden nun die relevanten Papierunterlagen sofort vernichtet.

  Digitale Personalratsunterlagen müssen entsprechend organisiert gelöscht werden.

Bei dieser Angelegenheit ersuchte eine vom Verlust besonders betroffene Person zudem um Auskunft gegenüber dem Personalrat. Die dabei aufgeworfenen datenschutzrechtlichen Fragestellungen behandle ich ebenfalls in diesem Tätigkeitsbericht (siehe Nr. 9.3).

12.11.4 Beanstandung einer Klinik wegen Weitergabe von Gesundheitsdaten an den Arbeitgeber eines Patienten

Die beanstandete Klink hat ein Gutachten über einen Arbeitnehmer erstellt, das von dessen Arbeitgeber in Auftrag gegeben wurde. Auftragsgemäß wurde dieses Gutachten anschließend an das zuständige Gesundheitsamt übermittelt.

Gleichzeitig wurde das Gutachten zusammen mit der Kostenrechnung an den Arbeitgeber versandt. Dadurch war es dem Arbeitgeber möglich, detaillierte Gesundheitsdaten der betroffenen Person zur Kenntnis zu nehmen. Dieser Vorfall ist aufgrund besonderer Umstände des Einzelfalls geeignet, die Ehre der betroffenen Person empfindlich zu verletzen, seinen Ruf zu schädigen sowie ihn nicht nur beruflich, sondern auch sozial und gesellschaftlich in Misskredit zu bringen.

Hierbei spielte es keine Rolle, ob der Arbeitgeber des Betroffenen nach Übermittlung des Gutachtens tatsächlich den Inhalt des Gutachtens zur Kenntnis nahm. Allein die Möglichkeit, dass höchst sensible Daten der betroffenen Person für den Arbeitgeber, der vorliegend nicht unmittelbarer Adressat des Gutachtens war, verfügbar waren und dadurch sowohl privat als auch insbesondere beruflich Nachteile entstehen können, genügte im vorliegenden Fall, um eine erhebliche Datenschutzverletzung anzunehmen.

Die Klinik hat gemäß Art. 5 Abs. 1 Buchst. f, 24 Abs. 1, 25 Abs. 1, 32 Abs. 1 Buchst. a und b DSGVO technisch-organisatorische Maßnahmen festzulegen, um den Schutz vor unbefugter und unrechtmäßiger Verarbeitung zu gewährleisten und im vorliegenden Fall insbesondere hochsensible Gesundheitsdaten des Betroffenen im Sinne des Art 9 Abs. 1 vor unbefugter Kenntnisnahme zu schützen.

Gerade auch bei einem Postversand von Unterlagen sollte durch geeignete organisatorische Maßnahmen wie beispielsweise ein Vier-Augen-Prinzip, bei der Kuvertierung und Adressierung der Unterlagen sichergestellt werden, dass das erstellte Gutachten nur an die befugte Stelle (Gesundheitsamt) gelangt. Da dies versäumt worden war, habe ich die Klinik gemäß Art. 16 Abs. 4 Satz 1 BayDSG förmlich beanstandet.

12.11.5 Beanstandung einer Stadt wegen unterlassener Pseudonymisierung

Im Vorfeld einer von der Volkshochschule einer bayerischen Stadt geplanten Buchvorstellung hatte die für diese Veranstaltung eingeladene Autorin eines autobiografischen Werkes darum gebeten, dass statt ihres Namens ausschließlich ein Pseudonym verwendet und bekannt werden sollte. Der Grund hierfür war, dass die Autorin im Laufe der Buchvorstellung über eine bei ihr diagnostizierte Schizophrenie berichten wollte, die sie noch nicht vollständig überwunden hatte. Ein Bekanntwerden des „echten“ Namens und die damit logischerweise verbundene Möglichkeit von Rückschlüssen auf die gesundheitliche Disposition der Autorin konnten in der Gesamtschau sowohl im privaten als auch beruflichen Umfeld der Autorin negative Folgen nach sich ziehen, die es aus Sicht der Betroffenen unbedingt zu vermeiden galt.

Gemäß Art. 5 Abs. 1 Buchst. f, 24 Abs. 1, 25 Abs. 1, 32 Abs. 1 Buchst. a und b DSGVO hatte die Stadt technisch-organisatorische Maßnahmen festzulegen, um den Schutz vor unbefugter und unrechtmäßiger Verarbeitung zu gewährleisten

und insbesondere personenbezogene Daten vor unbefugter Kenntnisnahme zu schützen.

Dem Wunsch der Autorin entsprechend wurde bei der Drucklegung des Programmheftes nur das Pseudonym als Datensatz abgespeichert, verwendet und abgedruckt. Allerdings musste dieser Datensatz im Zusammenhang mit der Erstellung und dem Ausdruck des Honorarvertrages auf deren amtlichen Namen geändert werden. Nach Vertragsdruck wurde von Seiten der Stadt vergessen, den amtlichen Namen der Autorin wieder zu löschen und lediglich das Pseudonym zu belassen. Hierbei sowie in ähnlichen oder gleichgelagerten Fällen ist durch entsprechende technische und organisatorische Maßnahmen sicherzustellen (zum Beispiel Anlage von zwei Datensätzen – „Pseudonym“ und „amtlicher Name“, Erstellung des Honorarvertrages ohne Zugriff auf einen vorhandenen Datensatz), dass die Persönlichkeitsrechte gewährleistet sind.

Da der in der Verwaltungssoftware gespeicherte Datensatz auch die Grundlage für die Homepage der Volkshochschule bildet, wurde neben dem Pseudonym ab diesem Zeitpunkt auch der amtliche Namen der Autorin im Zusammenhang mit dem geplanten Vortrag auf der Homepage der Volkshochschule angezeigt. Der Fehler wurde erst nach einer Woche bekannt und der Datensatz unmittelbar korrigiert.

Zwar war nun auf der Homepage der Volkshochschule wieder lediglich das Pseudonym der Autorin sichtbar, allerdings wurde nicht bemerkt, dass bei einer Suchmaschinenrecherche im Internet noch immer auch der „echte“ Name der Autorin zu finden war. Die betroffene Autorin hat dies etwa sieben Wochen nach der Veranstaltung selbst bemerkt und bei der Volkshochschule reklamiert, woraufhin umgehend die Löschung des entsprechenden Links beim Suchmaschinenanbieter beantragt wurde.

Bei der Preisgabe des Namens der Autorin durch die Versäumnísse bei der Anlage der Datensätze handelt es sich um einen erheblichen Datenschutzverstoß, da es jeder Person, die im Internet nach dem Pseudonym der Autorin gesucht hätte, möglich gewesen wäre, die wahre Identität der Autorin zu erfahren, was unbedingt vermieden werden sollte.

In der Gesamtschau spielte es keine Rolle, ob sich tatsächlich jemand per Suchmaschinenrecherche den „echten“ Namen der Autorin anhand ihres Pseudonyms verschaffte.

Aus diesen Gründen habe ich diesen Verstoß gegen datenschutzrechtliche Vorschriften förmlich gemäß Art. 16 Abs. 4 Satz 1 BayDSG beanstandet.

13 Informationsfreiheit

13.1 Transparenz bei Grundstücksverkäufen bayerischer Gemeinden

Viele bayerische Gemeinden gehören als Eigentümer von Bauland, land- oder forstwirtschaftlichen Flächen zu den bedeutenden Grundeigentümern. Manchmal veräußern sie im Rahmen ihrer Aufgaben der kommunalen Bodenpolitik Grundstücke, die sie für Verwaltungszwecke nicht mehr benötigen.

So schrieb etwa eine Gemeinde ein in ihrem Eigentum befindliches bebautes Grundstück gegen Höchstgebot öffentlich zum Verkauf aus. Der Gemeinderat entschied sich in nichtöffentlicher Sitzung für eines von drei Geboten. Die Gemeinde schloss mit dem Bieter einen Kaufvertrag und übereignete ihm das Grundstück. Ein in der Gemeinde ansässiger kommunalpolitisch interessierter Bürger wollte nun wissen, wem die Gemeinde für welchen Betrag den Zuschlag erteilt hatte und welche Höhe die unterlegenen Gebote erreicht hatten. Er stellte daher bei der Gemeinde einen Auskunftsantrag. Die Gemeinde war nicht bereit, die Informationen herauszugeben. Daraufhin wandte sich der Bürger an mich.

Aus datenschutzrechtlicher Sicht ist in Fällen dieser Art zu beachten:

13.1.1 Ablauf kommunaler Grundstücksgeschäfte

Nicht jedes kommunale Grundstückgeschäft gleicht dem anderen, auch folgt nicht jedes denselben rechtlichen Regeln wie ein anderes. Das vorliegende Arbeitspapier behandelt allein Transparenzfragen beim **„einfachen“ Verkauf mit anschließender Eigentumsübertragung zur grundsätzlich freien Verfügung**. Außer Betracht bleiben dagegen Grundstücksgeschäfte, die mit öffentlichen Bauaufträgen oder Baukonzessionen verknüpft sind.

Bei einem Grundstücksverkauf muss die Gemeinde Art. 75 Abs. 1 Gemeindeordnung (GO) beachten. Dort heißt es:

„[1]Die Gemeinde darf Vermögensgegenstände, die sie zur Erfüllung ihrer Aufgaben nicht braucht, veräußern. [2]Vermögensgegenstände dürfen in der Regel nur zu ihrem vollen Wert veräußert werden.“

Ein bewährter – wenngleich nicht der einzig zulässige – Weg, die Vorgabe in Art. 75 Abs. 1 Satz 2 GO umzusetzen, ist eine **öffentliche Ausschreibung**. Typischerweise erarbeitet die gemeindliche Liegenschaftsverwaltung dafür einen Ausschreibungstext, der das Grundstück vorstellt sowie die Zuschlagskriterien, die Anforderungen an die Angebote und das Verfahren im Übrigen erläutert, zudem gegebenenfalls ein Mindestgebot und die vom Üblichen abweichenden Vertragsbedingungen (wie etwa eine Aufzahlungsklausel oder eine Regelung für den Fall eines Altlastenfunds) nennt. Fällt die Erteilung des Zuschlags – wie dies bei bebauten oder bebaubaren Grundstücken meist der Fall ist – in die Zuständigkeit des

Gemeinderats,[85] kann dieser mit dem Grundsatzbeschluss, der den „Verkaufswillen“ zum Ausdruck bringt, auch bereits den Ausschreibungstext billigen. Im Anschluss daran veröffentlicht die Gemeinde die Ausschreibung, etwa auf ihrer Homepage, in regionalen Zeitungen oder auf einem Immobilienportal im Internet.

Sind Angebote eingegangen, werden diese von der Liegenschaftsverwaltung ausgewertet und gereiht; die entsprechende Sitzungsvorlage für den Gemeinderat enthält den Beschlussvorschlag, das Grundstück an eine konkret benannte Bieterin oder einen konkret benannten Bieter zu einem bestimmten Gebot zu vergeben. Der Gemeinderat fasst darüber – regelmäßig in nichtöffentlicher Sitzung[86] – Beschluss. Im weiteren Verlauf schließt die Gemeinde mit der erfolgreichen Bieterin oder dem erfolgreichen Bieter einen Kaufvertrag und übereignet das Grundstück.

13.1.2 Transparenz nach kommunalrechtlichen Vorgaben

In den soeben skizzierten Ablauf ist die interessierte Öffentlichkeit bereits zu einem frühen Zeitpunkt eingebunden. Auch wenn der Gemeinderat über die grundsätzliche Bereitschaft zum Verkauf sowie die Fassung eines Ausschreibungstextes unter Ausschluss der Öffentlichkeit beraten und entschieden haben sollte, erfährt die Allgemeinheit jedenfalls mit der Ausschreibung, dass und zu welchen Bedingungen ein gemeindliches Grundstück verkauft wird.

Den Augen der Öffentlichkeit entzogen sind dagegen die eingehenden Gebote und ihre Auswertung wie auch eine Beratung und Entscheidung des Gemeinderats über den Zuschlag in nichtöffentlicher Sitzung. Das so entstehende „Transparenzdefizit“ muss durch die von Art. 52 Abs. 3 GO geforderte **Bekanntgabe des Beschlusses** wieder ausgeglichen werden. Diese Vorschrift lautet:

„Die in nichtöffentlicher Sitzung gefaßten Beschlüsse sind der Öffentlichkeit bekanntzugeben, sobald die Gründe für die Geheimhaltung weggefallen sind.“

Wie gut der Ausgleich des „Transparenzdefizits“ gelingt, hängt maßgeblich davon ab, wie der Beschlusstenor gefasst ist und zu welchem Zeitpunkt informiert wird. In der Kommunalpraxis ist manchmal zu beobachten, dass der Beschlusstenor wenig aussagekräftig gehalten und die Erfüllung der Pflicht aus Art. 52 Abs. 3 GO über Gebühr hinausgeschoben wird.

13.1.2.1 Formulierung des Beschlusstenors

Transparenzfreundlich ist eine Formulierung des Beschlusstenors, die den Namen der Erwerberin oder des Erwerbers sowie den erzielten Preis ausdrücklich nennt. Mit der Bekanntgabe nach Art. 52 Abs. 3 GO werden diese Angaben offengelegt. Soweit es sich bei der Bieterin oder dem Bieter um eine natürliche Person handelt, ist dagegen aus datenschutzrechtlicher Sicht grundsätzlich nichts einzuwenden, weil die kommunalrechtliche Bekanntgabepflicht eine Rechtsgrundlage

[85] Zur Verteilung der Zuständigkeiten zwischen dem ersten Bürgermeister und dem Gemeinderat bei Grundstücksgeschäften vgl. die Regelungsvorschläge des Bayerischen Gemeindetags in § 8 Abs. 2 Nr. 2 Buchst. d Muster einer Geschäftsordnung des Gemeinderats (kleinere Gemeinden) und § 13 Abs. 2 Nr. 2 Buchst. d Muster einer Geschäftsordnung des Gemeinderats (größere Gemeinden), BayGT 2020, S. 121 ff., mit Erläuterungen auf S. 167, Internet: https://bay-gemeindetag.de, Rubrik „Verbandszeitschrift“.

[86] § 17 Abs. 1 Satz 1 Nr. 2 und § 22 Abs. 1 Satz 1 Nr. 2 der vorstehenden Muster.

für die mit ihrer Erfüllung verbundene Datenverarbeitung vermittelt (Art. 6 Abs. 1 UAbs. 1 Buchst. c Datenschutz-Grundverordnung).

Ist der Ausschluss der Öffentlichkeit bei der Beratung und Entscheidung des Gemeinderats über den Zuschlag (auch) auf „berechtigte Ansprüche einzelner" gestützt (Art. 52 Abs. 2 Satz 1 GO), können diese **ausnahmsweise** einen längerfristigen oder gar dauerhaften **Ausschluss des Erwerbernamens von der Bekanntgabe** nach Art. 52 Abs. 3 GO tragen. Dann muss die Gemeinde aber Gründe vorbringen können, welche die Erwerberin oder den Erwerber als (atypisch) schutzwürdig erscheinen lassen. Das kann insbesondere dann der Fall sein,

— wenn die Mitteilung des erzielten Preises den Rückschluss auf (weit) überdurchschnittliche finanzielle Spielräume der Erwerberin oder des Erwerbers zulässt,

— wenn die Erwerberin oder der Erwerber bei Offenlegung ihrer oder seiner Identität im Hinblick auf die Vorgeschichte des Erwerbsvorgangs unzumutbare Anfeindungen befürchten müsste oder

— wenn die Erwerberin oder der Erwerber das Grundstück für sich zu Wohnzwecken nutzen will und für sie oder ihn im Melderegister eine Auskunftssperre (§ 51 Bundesmeldegesetz) eingetragen ist oder die Voraussetzungen dafür erfüllt sind.

Beispiel 1: Eine Gemeinde verkauft ein gewöhnliches, 1000 m^2 großes Baugrundstück zu einem moderaten marktüblichen Preis an A., der dort ein Einfamilienhaus errichten möchte. – Der Erwerber muss eine Namensnennung bei der Bekanntgabe des Vergabebeschlusses hinnehmen.

Beispiel 2: Eine an einem oberbayerischen See gelegene Gemeinde verkauft ein 1000 m^2 großes bebaubares Grundstück mit Seezugang zu einem Liebhaberpreis von 5 Mio. Euro. Zahlreiche Bürgerinnen und Bürger wollen die dort befindliche wilde Badestelle nicht verlieren. Die örtliche Bauträgerin B., der ein Interesse an dem Grundstück zugeschrieben wird, erreichten bereits mehrere Morddrohungen für den Fall des Erwerbs. Gleichwohl möchte B. auf dem Grundstück ein exklusives Mehrfamilienhaus errichten. Sie reicht daher ein Gebot ein, das kein Konkurrent übertrifft. – B. kann verlangen, dass der Vergabebeschluss jedenfalls vorerst ohne Nennung ihres Namens bekanntgegeben wird.

13.1.2.2 Zeitpunkt der Bekanntgabe

Der Zeitpunkt für die Bekanntgabe ist gekommen, „sobald die Gründe für die Geheimhaltung weggefallen sind" (Art. 52 Abs. 3 GO). Die vertrauliche Behandlung von Grundstücksgeschäften im Gemeinderat bezweckt in der Regel zum einen den Schutz fiskalischer Belange der Gemeinde als Teilnehmerin am Grundstücksverkehr (das „Sich-nicht-in-die-Karten-schauen-Lassen" bei der Anbahnung des Geschäfts), zum anderen den Schutz der personenbezogenen Daten der unterlegenen Bieterinnen und Bieter. Der letztgenannte Belang ist für die Bekanntgabe des Vergabebeschlusses ohne Bedeutung, weil dort allenfalls die Erwerberin oder der Erwerber genannt wird, während der erstgenannte Belang spätestens mit dem Vertragsschluss seine Schutzbedürftigkeit einbüßt. Daher ist hinsichtlich des Vergabebeschlusses grundsätzlich dann die im Einzelfall gebotene Transparenz herzustellen, wenn der Kaufvertrag geschlossen ist.

13.1.3 Zusätzliche Transparenz durch das allgemeine Recht auf Auskunft

Das in Art. 39 Abs. 1 Satz 1 BayDSG geregelte allgemeine Recht auf Auskunft ergänzt die in den kommunalrechtlichen Vorgaben bereits angelegte Transparenz. Dies gilt insbesondere dann, wenn die Gemeinde den bekanntzugebenden Vergabebeschluss so formuliert hat, dass die Erwerberin oder der Erwerber und/oder der erzielte Kaufpreis nicht ersichtlich sind. Art. 39 Abs. 1 Satz 1 BayDSG lautet:

„Jeder hat das Recht auf Auskunft über den Inhalt von Dateien und Akten öffentlicher Stellen, soweit ein berechtigtes, nicht auf eine entgeltliche Weiterverwendung gerichtetes Interesse glaubhaft dargelegt wird und

1. *bei personenbezogenen Daten eine Übermittlung an nicht öffentliche Stellen zulässig ist und*
2. *Belange der öffentlichen Sicherheit und Ordnung nicht beeinträchtigt werden."*

Der Zugangsanspruch kann – wie im eingangs erwähnten Beispiel – die Identität der „Bestbieterin", des „Bestbieters" oder unterlegener Bieterinnen und Bieter, aber auch den Kaufpreis oder die Höhe der nicht erfolgreichen Gebote in den Blick nehmen, ferner etwa den Inhalt des geschlossenen Kaufvertrags. Alle diese Informationen werden regelmäßig in Dateien oder Akten der Gemeinde zu finden sein. Ein berechtigtes Interesse in Bezug auf solche Informationen glaubhaft darzulegen, ist meist nicht schwierig, wenn es um die Transparenz kommunaler Grundstücksgeschäfte geht. Es genügt hier grundsätzlich, dass ein Zugangsinteressent ein kommunalpolitisches Interesse zum Ausdruck bringt, die für einen Verkauf getroffene Entscheidung bewerten zu können.

Soweit der Zugangsanspruch auch in Bezug auf **personenbezogene Daten** geltend gemacht wird – die Zugangsinteressentin oder der Zugangsinteressent insbesondere die Namen von Bieterinnen oder Bietern erfahren möchte –, ist **Art. 39 Abs. 1 Satz 1 Nr. 1 BayDSG** zu beachten, der auf die allgemeine Übermittlungsvorschrift in Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG verweist und so das Informationszugangs- mit dem Datenschutzrecht verzahnt. Eine Übermittlung ist danach zulässig, wenn die Empfängerin oder der Empfänger ein berechtigtes Interesse an der Kenntnis des personenbezogenen Datums glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an einem Ausschluss der Übermittlung hat.

Bei der **erfolgreichen Bieterin** oder dem **erfolgreichen Bieter** ist ein solches schutzwürdiges Interesse regelmäßig nicht gegeben: Die Gemeinde ist als öffentlicher Träger gesetzlichen Transparenzpflichten unterworfen. Dies gilt – wie Art. 52 GO zeigt – insbesondere für die Tätigkeit des Gemeinderats, die sich „unter den Augen der Öffentlichkeit" abspielt. Wer ein gemeindliches Grundstück erwirbt, hat einen institutionellen Vertragspartner, der nicht Anteilseignerinnen und Anteilseignern, sondern der Öffentlichkeit Rechenschaft schuldet. Wie viel „Geheimheit" möglich ist, bestimmen hier das Kommunal- und das Datenschutzrecht. Die kommunalrechtlichen Wertungen nachzeichnend, ist im Rahmen von Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG ein schutzwürdiges Interesse der Erwerberin oder des Erwerbers nur ausnahmsweise anzuerkennen (siehe oben Nr. 13.1.2.1 mit möglichen Fallkonstellationen).

Das Vertraulichkeitsinteresse **unterlegener Bieterinnen und Bieter** ist demgegenüber stets als schutzwürdig zu werten. Ihre Identität spielt in aller Regel für die Verwirklichung des Zugangsinteresses keine Rolle. Soweit die nicht erfolgreichen Gebote daher anonym bleiben können, steht Art. 39 Abs. 1 Satz 1 Nr. 1 BayDSG

einer Mitteilung ihrer Höhe an eine Zugangsinteressentin oder einen Zugangsinteressenten nicht entgegen.

Auch der Schutz von **Betriebs- und Geschäftsgeheimnissen** einer Erwerberin oder eines Erwerbers kann einen Informationszugang ausschließen. Das Gesetz sieht einen entsprechenden Tatbestand in **Art. 39 Abs. 3 Nr. 3 BayDSG** ausdrücklich vor. Ein Betriebs- oder Geschäftsgeheimnis zeichnet sich durch **Wettbewerbsrelevanz** aus. Dass es sich um eine Information handelt, die ein Unternehmen aus anderen als wettbewerblichen Gründen für sich behalten möchte, genügt nicht. Das Bundesverwaltungsgericht hat ausgeführt:[87]

„Als Betriebs- und Geschäftsgeheimnisse werden […] allgemein alle auf ein Unternehmen bezogenen Tatsachen, Umstände und Vorgänge verstanden, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat. Ein berechtigtes Geheimhaltungsinteresse ist anzuerkennen, wenn die Offenlegung der Information geeignet ist, den Konkurrenten exklusives technisches oder kaufmännisches Wissen zugänglich zu machen und so die Wettbewerbsposition des Unternehmens nachhaltig zu beeinflussen (Wettbewerbsrelevanz). Hierfür muss die prognostische Einschätzung nachteiliger Auswirkungen im Falle des Bekanntwerdens der Information nachvollziehbar und plausibel dargelegt werden […].“

Die **Angabe des Kaufpreises** ist regelmäßig nicht als Geschäftsgeheimnis zu werten. Eine andere Würdigung kann jedoch etwa in Betracht kommen, wenn bei seinem Bekanntwerden auf „Vorsprungswissen“ geschlossen werden könnte oder Nachteile bei einer Weiterveräußerung zu erwarten wären.[88]

Beispiel 3: Die Gemeinde G. schreibt im Zentrum (baurechtlich: nicht beplanter Innenbereich) ein 1000 m^2 großes bebautes Grundstück zum Verkauf aus. C. ist Bauträger und hat Interesse. Er möchte den vorhandenen Altbestand abbrechen und ein modernes Wohn- und Geschäftshaus errichten. Auf Grund seiner Marktkenntnis gibt er ein Gebot ab, das die Gebote der anderen Bieter knapp übersteigt. – Gründe für eine Geheimhaltung von Erwerber und Kaufpreis über den Vertragsschluss hinaus sind hier nicht ersichtlich: Wer diese Informationen erlangt, der erfährt über C. und seine Geschäfte nichts wesentlich Neues.

Beispiel 4: Die Stadt S. verkauft eine ungenutzte Kiesgrube, in der – bislang unerkannt – seltene Erden lagern. Zwei örtliche Bauunternehmer geben von der Stadt erwartete Gebote ab; ein alle Erwartungen weit übersteigendes Gebot kommt von einem internationalen Rohstoffkonzern, der den Wert der Kiesgrube auf Grund seiner geologischen Expertise zutreffend einschätzt. – Hier manifestiert sich im Höchstgebot ein Wissensvorsprung, den die Bekanntgabe des Bieters wie auch des Kaufpreises implizit offenlegen würde. Spräche sich der Erwerb in den Verkehrskreisen herum, könnte der Konzern seinen Wissensvorsprung insbesondere nicht mehr zum günstigen Erwerb benachbarter Grundstücke nutzen. Dies legt einen Ausschluss des Zugangsanspruchs nach Art. 39 Abs. 3 Nr. 3 BayDSG nahe.

87 Bundesverwaltungsgericht, Urteil vom 17. März 2016, 7 C 2.15, BeckRS 2016, 46247, Rn. 35.

88 Vgl. auch Oberverwaltungsgericht Berlin-Brandenburg, Urteil vom 6. März 2014, OVG 12 B 19.12, BeckRS 2014, 49566.

Einem Zugangsanspruch kann zudem ein öffentliches Interesse entgegenstehen. Der gemäß **Art. 39 Abs. 1 Satz 2 Nr. 1 BayDSG** ein „Versagungsermessen“[89] eröffnende Ausschlussgrund wird allerdings nicht durch das Anliegen der Gemeinde ausgefüllt, Grundstücksgeschäfte „im Verborgenen zu halten“. Dies hindert bereits die in Art. 52 Abs. 3 GO enthaltene Wertung, welche grundsätzlich Transparenz fordert. Mit der Offenlegung des Kaufpreises wird im Übrigen regelmäßig nicht ein hinreichend konkretes Risiko verbunden sein, dass die Gemeinde bei zukünftigen Grundstücksgeschäften ihre Verhandlungsposition verschlechtert.[90]

Art. 39 Abs. 1 Satz 1 BayDSG kann grundsätzlich auch Zugang zum **Inhalt von Verträgen** verschaffen. Hier bedarf es aber im Einzelfall einer differenzierten, einzelne Vertragsklauseln berücksichtigenden Prüfung. Grundstückskaufverträge können neben den üblichen formularmäßigen Bestimmungen Regelungen enthalten, die auf Besonderheiten der jeweiligen Situation reagieren. An solchen Regelungen können unterschiedliche Vertraulichkeitsinteressen bestehen, die dann rechtlich zu bewerten sind. Generelle Leitlinien lassen sich auf Grund der Vielgestaltigkeit denkbarer Sachverhalte nicht aufstellen.

13.1.4 Verfahrensbezogene Hinweise

Das **Verfahren auf Erteilung einer Auskunft** nach Art. 39 Abs. 1 Satz 1 BayDSG ist ein Verwaltungsverfahren im Sinne von Art. 9 Bayerisches Verwaltungsverfahrensgesetz.[91] Dessen Durchführung ist an anderer Stelle erläutert.[92] In diesem Rahmen sind auch Dritte anzuhören, deren Vertraulichkeitsinteressen bei einer Erteilung der begehrten Auskunft betroffen sein könnten. Verwaltungsverfahren über Auskunftsanträge im Zusammenhang mit kommunalen Grundstücksgeschäften sollten – auch wegen der regelmäßigen Beteiligung der Erwerberin oder des Erwerbers – grundsätzlich durch Bescheid abgeschlossen werden.

Um „unliebsame“ Überraschungen bei Erwerberinnen und Erwerbern von vornherein zu vermeiden, sollte in einem **Verfahren zum Verkauf eines Grundstücks** frühzeitig, etwa mit der Ausschreibung, darauf hingewiesen werden, dass die Gemeinde eine kommunalrechtliche Transparenzpflicht trifft, und dass sie weiterhin Zugangsansprüche nach Art. 39 Abs. 1 Satz 1 BayDSG zu erfüllen haben kann. Diese Pflichten können durch vertragliche „Verschwiegenheitsklauseln“ oder entsprechende vorvertragliche Vereinbarungen zwischen der Gemeinde und (potenziellen) Erwerberinnen oder Erwerbern grundsätzlich nicht ausgeschlossen werden.[93]

89 Zur Wirkungsweise dieses Ausschlussgrundes näher Engelbrecht, Das allgemeine Recht auf Auskunft im Bayerischen Datenschutzgesetz, 2017, Teil 1 Rn. 136 ff., Internet: https://www.datenschutz-bayern.de, Rubrik „Auskunftsanspruch“.

90 Vgl. näher Oberverwaltungsgericht für das Land Nordrhein-Westfalen, Urteil vom 19. März 2013, 8 A 1172/11, BeckRS 2013, 51675.

91 Vgl. Bayerischer Verwaltungsgerichtshof Urteil vom 13. Mai 2019, 4 B 18.1515, BeckRS 2019, 17760, Rn. 27.

92 Engelbrecht, Das allgemeine Recht auf Auskunft im Bayerischen Datenschutzgesetz, 2017, Teil 1 Rn. 181 ff.

93 Vgl. näher Schoch, Informationsfreiheitsgesetz, 2. Aufl. 2016, § 3 Rn. 323 f.

13.1.5 Fazit

Das Kommunalrecht gewährleistet grundsätzlich, dass sich Grundstücksgeschäfte in den Gemeinden nicht unter Ausschluss der Öffentlichkeit abspielen. Die Bekanntgabe des Beschlusses über einen Verkauf sollte regelmäßig über den erzielten Kaufpreis und die Identität der Erwerberin oder des Erwerbers informieren. Sieht die Gemeinde von einer Bekanntgabe des Beschlusses ab oder hält sie ihn in der Formulierung unspezifisch, können interessierte Bürgerinnen und Bürger diese Informationen mit Hilfe von Art. 39 Abs. 1 Satz 1 BayDSG erfragen; die Gemeinde muss dann insbesondere prüfen, ob dem rechtlich geschützte Vertraulichkeitsinteressen entgegenstehen. Häufig ist dies nicht der Fall. Zudem kann Art. 39 Abs. 1 Satz 1 BayDSG dabei helfen, unterlegene Gebote aus einem Bieterverfahren transparent zu machen. Je nach Lage des Einzelfalls ist sogar ein Zugang zum Inhalt eines geschlossenen Grundstückskaufvertrags möglich.

13.2 Zugang zu Niederschriften der Sitzungen kollegialer Selbstverwaltungsorgane in bayerischen Gemeinden und Landkreisen

Über die Sitzungen der Gemeinderäte, der Kreistage und ihrer beschließenden Ausschüsse sind nach Art. 54 Abs. 1 Satz 1, Art. 45 Abs. 2 Satz 2 Gemeindeordnung (GO) sowie Art. 48 Abs. 1 Satz 1, Art. 40 Abs. 2 Satz 2 Landkreisordnung (LKrO) Niederschriften zu fertigen. Die Geschäftsordnungen enthalten hierzu regelmäßig nähere Regelungen; in diesem Rahmen kann die Protokollierungspflicht auch auf vorberatende Ausschüsse erstreckt werden.[94] Die Niederschriften haben nicht nur für die Mitglieder des Gemeinderats und die Gemeindeverwaltung Bedeutung; auch Bürgerinnen und Bürger möchten sich mitunter im Nachhinein vergewissern, was in den Beratungen gesagt und am Ende beschlossen wurde. Das Landesrecht gewährt ihnen vor diesem Hintergrund Zugangsansprüche. Aus Datenschutzsicht ist insofern zu bemerken:

13.2.1 Kommunalrechtliche Zugangsansprüche

Das Kommunalrecht kennt bereits seit langem Ansprüche auf Zugang zu Niederschriften, auch zugunsten von Bürgerinnen und Bürgern. So heißt es in Art. 54 Abs. 3 Satz 2 GO:

„Die Einsicht in die Niederschriften über öffentliche Sitzungen steht allen Gemeindebürgern frei; dasselbe gilt für auswärts wohnende Personen hinsichtlich ihres Grundbesitzes oder ihrer gewerblichen Niederlassungen im Gemeindegebiet."

Art. 48 Abs. 2 Satz 2 LKrO bestimmt:

„Die Einsicht in die Niederschriften über öffentliche Sitzungen steht allen Kreisbürgern frei."

Beide Vorschriften begründen keine „Jedermannsrechte". **Anspruchsberechtigt** sind im Fall von Art. 54 Abs. 3 Satz 2 Halbsatz 1 GO die **Gemeindebürger** – das

94 So etwa das vom Bayerischen Gemeindetag herausgegebene Muster einer Geschäftsordnung für den Gemeinderat (größere Gemeinden), BayGT 2020, S. 121 ff. in § 36 Abs. 1 Satz 1 und § 34 Abs. 1 Satz 1. – Siehe auch § 77 Abs. 1 Geschäftsordnung des Stadtrats der Landeshauptstadt München (Stadtrecht Nr. A 19).

sind die Gemeindeangehörigen, die in ihrer Gemeinde das Recht besitzen, an den Gemeindewahlen teilzunehmen (Art. 15 Abs. 2 GO) –, im Fall von 48 Abs. 2 Satz 2 LKrO die **Kreisbürger**, also die Kreisangehörigen, die das Wahlrecht für die Kreiswahlen besitzen (Art. 11 Abs. 2 LKrO).

Eine **Anspruchsberechtigung für** die sog. **Forensen** gibt es **nur auf Gemeindeebene** (vgl. Art. 54 Abs. 3 Satz 2 Halbsatz 2 GO); sie ist nicht – wie bei den Gemeindebürgern – umfassend, sondern auf das Grundstück oder Gewerbe bezogen („hinsichtlich"). Das Einsichtsrecht bezieht sich insofern also lediglich auf Tagesordnungspunkte, die einen entsprechenden Bezug aufweisen.[95]

Anders als der in Art. 39 Abs. 1 Satz 1 BayDSG geregelte Zugangsanspruch verlangen Art. 54 Abs. 3 Satz 2 GO und Art. 48 Abs. 2 Satz 2 LKrO nicht, dass die Zugangsinteressentin oder der Zugangsinteressent ein berechtigtes Interesse glaubhaft darlegt. Wer nach diesen Bestimmungen Niederschriften einsehen möchte, kann sich über die Beweggründe also ausschweigen.

Gegenstand der Zugangsansprüche nach Art. 54 Abs. 3 Satz 2 GO und Art. 48 Abs. 2 Satz 2 LKrO sind die gemäß Art. 54 Abs. 1 Satz 1 oder Art. 48 Abs. 1 Satz 1 LKrO gefertigten, **unterzeichneten Niederschriften**. Im Anwendungsbereich der Gemeindeordnung muss zudem die **Genehmigung** durch das jeweilige Gremium vorliegen (vgl. Art. 54 Abs. 2 GO).[96] „Vorprodukte" – wie etwa zur Unterstützung der protokollführenden Person gefertigte Tonbandmitschnitte – sind nicht erfasst.

Die Zugangsansprüche sind im Übrigen auf „Niederschriften über öffentliche Sitzungen" begrenzt. Dies bedeutet, dass **Niederschriften über nichtöffentliche Sitzungen nicht erfasst** sind. Dies gilt auch dann, wenn sich die Sachlage hinsichtlich der Vertraulichkeit nachträglich ändert.[97] Die Gesetze sehen zwar eine Bekanntgabe von Beschlüssen vor, sobald die Gründe für die Geheimhaltung weggefallen sind (Art. 52 Abs. 3 GO, Art. 46 Abs. 3 LKrO). Daraus ist aber nicht zu folgern, dass auch die Niederschriften offenzulegen wären: Gründe der Geheimhaltung können für einen Beschluss wegfallen, für den Inhalt der Beratung, eine mögliche namentliche Abstimmung sowie eine darüber gefertigte Niederschrift aber fortbestehen. Die Gemeinde oder der Landkreis schuldet nach Art. 54 Abs. 3 GO oder Art. 46 Abs. 3 LKrO nur eine Prüfung, ob Beschlüsse bekanntzugeben sind, nicht dagegen, ob auch Niederschriften öffentlich gemacht werden können.

Anspruchsinhalt ist bei Art. 54 Abs. 3 Satz 2 GO und Art. 48 Abs. 2 Satz 2 LKrO die **Einsicht** in das jeweilige Dokument, also in das Beschlussbuch oder in Auszüge daraus.

95 Vgl. Verwaltungsgericht Würzburg, Beschluss vom 19. April 2005, W 5 E 05.307, BeckRS 2008, 36286, Rn. 6.

96 Glaser, in: Widtmann/Grasser/Glaser, Bayerische Gemeindeordnung, Stand 12/2015, Art. 54 GO Rn. 14.

97 So auch Jung, in: Dietlein/Suerbaum, BeckOK Kommunalrecht Bayern, Stand 6/2020, Art. 54 GO Rn. 25, sowie – für das baden-württembergische Landesrecht – Verwaltungsgerichtshof Baden-Württemberg, Urteil vom 4. Februar 2020, 10 S 1229/19, BeckRS 2020, 2371, Rn. 9. Anderer Auffassung Prandl/Zimmermann/Büchner/Pahlke, Kommunalrecht in Bayern, Stand 9/2015, Art. 54 GO Erl. 8.

Begehrt eine anspruchsberechtigte Person statt Einsicht eine **Auskunft**, bestehen keine Bedenken, wenn die Gemeinde oder der Landkreis den Anspruch auf diese Art erfüllt.

Meinungsverschiedenheiten entstehen mitunter, wenn die **Bereitstellung von Kopien** aus den Niederschriften verlangt wird. Manche Kommunen sind nämlich der Auffassung, auf derartige „Sonderwünsche" überhaupt nicht eingehen zu müssen. Mit dieser Haltung haben sie zwar den Normtext auf ihrer Seite, der von „Einsicht" spricht. Allerdings ist daraus nicht abzuleiten, dass der Informationszugang nicht in einer anderen Form – so sie gewünscht wird – gewährt werden darf.[98]

Der Kommune kommt vielmehr ein **Ermessen** zu: Beantragt eine anspruchsberechtigte Person eine Bereitstellung von Kopien, muss die Kommune nach pflichtgemäßem Ermessen entscheiden, ob sie diesem Anliegen entspricht oder auf den Zugang durch Einsicht verweist. Im Rahmen der Ermessensentscheidung ist auch das vom Gesetz geschützte Zugangsinteresse mit den von der Kommune im Einzelfall geltend gemachten Belangen (etwa: Vermeidung von Personal- und Sachaufwand bei der Herstellung von Kopien) in Ausgleich zu bringen. Eine Ermessensentscheidung zugunsten der anspruchsberechtigten Person kommt insbesondere dann in Betracht, wenn sich das Zugangsgesuch auf Tagesordnungspunkte bezieht, zu welchen die Niederschrift umfangreiche, komplexe oder sonst im begrenzten zeitlichen Rahmen einer Einsicht nicht erfassbare Informationen enthält, oder wenn sich die anspruchsberechtigte Person mit einer Kostenerstattung nach dem Kostengesetz einverstanden erklärt.[99]

Eine **vollständige Ermessensreduzierung** soll einer Rechtsprechung aus der Zeit vor Einführung des allgemeinen Rechts auf Auskunft zufolge allerdings (wohl nur) dann eintreten, wenn eine anspruchsberechtigte Person durch Verweis auf eine Einsicht schlechter gestellt würde als andere Zugangsinteressenten.[100] Das kann nicht nur bei Zugangsgesuchen etwa sehbehinderter Personen der Fall sein, sondern auch dann, wenn eine Kommune in ständiger Verwaltungspraxis Kopien aus Niederschriften überlässt, eine bestimmte Bürgerin oder einen bestimmten Bürger aber auf die Einsicht verweisen möchte.

13.2.2 Allgemeines Recht auf Auskunft (Art. 39 BayDSG)

Ende 2015 hat der bayerische Gesetzgeber ein **allgemeines Recht auf Auskunft** eingeführt, das seit der Datenschutzreform 2018 in Art. 39 Abs. 1 Satz 1 BayDSG geregelt ist. Die Vorschrift lautet:

„Jeder hat das Recht auf Auskunft über den Inhalt von Dateien und Akten öffentlicher Stellen, soweit ein berechtigtes, nicht auf eine entgeltliche Weiterverwendung gerichtetes Interesse glaubhaft dargelegt wird und

1. bei personenbezogenen Daten eine Übermittlung an nicht öffentliche Stellen zulässig ist und

98 Ähnlich Bayerischer Verwaltungsgerichtshof, Urteil vom 4. März 2008, 4 BV 07.1329, BeckRS 2009, 31911, Rn. 14 ff.

99 Zur Erhebung von Kosten bei Auskünften nach Art. 39 Abs. 1 Satz 1 BayDSG Engelbrecht, Das allgemeine Recht auf Auskunft im Bayerischen Datenschutzgesetz, 2017, Teil 1 Rn. 152 f.

100 Dazu näher Bayerischer Verwaltungsgerichtshof, Urteil vom 4. März 2008, 4 BV 07.1329, BeckRS 2009, 31911, Rn. 20.

2. Belange der öffentlichen Sicherheit und Ordnung nicht beeinträchtigt werden."

Da die Niederschriften der Sitzungen kollegialer Selbstverwaltungsorgane üblicherweise in Akten vorgehalten werden und die bayerischen Gemeinden und Landkreise öffentliche Stellen im Sinne von Art. 1 Abs. 1 Satz 1 BayDSG sind, fragt sich, ob Art. 39 Abs. 1 Satz 1 BayDSG neben Art. 54 Abs. 3 Satz 2 GO und Art. 48 Abs. 2 Satz 2 LKrO angewendet werden kann.

Das Verhältnis des allgemeinen Rechts auf Auskunft zu anderen Informationszugangsrechten wird maßgeblich von **Art. 39 Abs. 2 BayDSG** bestimmt:

„Abs. 1 findet keine Anwendung auf Auskunftsbegehren, die Gegenstand einer Regelung in anderen Rechtsvorschriften sind."

Bei einem Vergleich von Art. 39 Abs. 1 Satz 1 BayDSG auf der einen sowie Art. 54 Abs. 3 Satz 2 GO und Art. 48 Abs. 2 Satz 2 LKrO auf der anderen Seite ist festzustellen, dass Art. 39 Abs. 1 Satz 1 BayDSG ein Jedermannsrecht ist, dass die Regelung vor den Informationszugang die glaubhafte Darlegung eines berechtigten Interesses stellt, und dass die Vorschrift primär auf Auskunft gerichtet ist, nach Ermessen der auskunftspflichtigen Stelle aber auch die Gewährung von Einsicht oder die Bereitstellung von Kopien zulässt. Demgegenüber berechtigt Art. 54 Abs. 3 Satz 2 GO nur Gemeindebürger und Forensen, Art. 48 Abs. 2 Satz 2 LKrO nur Kreisbürger; beide Vorschriften setzen kein berechtigtes Interesse voraus, zielen primär auf Einsicht, wobei nach Ermessen auch Auskunft erteilt werden kann oder Kopien bereitgestellt werden können.

Würden Art. 39 Abs. 1 Satz1 BayDSG sowie Art. 54 Abs. 3 Satz 2 GO und Art. 48 Abs. 2 Satz 2 LKrO nebeneinander angewendet, käme den beiden letztgenannten Vorschriften lediglich die Funktion einer Privilegierung zu: Anders als alle anderen Zugangsinteressentinnen und Zugangsinteressenten müssten Gemeindebürgerinnen und Gemeindebürger – im Fall von Art. 54 Abs. 3 Satz 2 GO – sowie Kreisbürgerinnen und Kreisbürger – im Fall von Art. 48 Abs. 2 Satz 2 LKrO – ein berechtigtes Interesse nicht darlegen, wenn sie Einsicht in die Niederschriften öffentlicher Sitzungen nehmen wollten. Der Zugang zu den Niederschriften nichtöffentlicher Sitzungen richtete sich für alle Zugangsinteressentinnen und Zugangsinteressenten nach Art. 39 Abs. 1 Satz 1 BayDSG. Auf diese Weise würde das tradierte Zugangsregime der Gemeindeordnung erheblich umgebaut.

Werden dagegen Art. 54 Abs. 3 Satz 2 GO und Art. 48 Abs. 2 Satz 2 LKrO als „Regelung[en] in anderen Rechtsvorschriften" im Sinne von Art. 39 Abs. 2 BayDSG angesehen, bleibt der Informationszugang auf den durch diese Bestimmungen gesetzten Rahmen begrenzt; andere als die dort genannten Personen können Zugang zu Niederschriften nicht erlangen, und die Niederschriften nichtöffentlicher Sitzungen bleiben gänzlich von Zugangsansprüchen ausgenommen.

Vor der Einführung von Art. 39 Abs. 1 Satz 1 BayDSG bildeten Art. 54 Abs. 3 Satz 2 GO und Art. 48 Abs. 2 Satz 2 LKrO eine „Transparenzinsel" in einem Verwaltungsbereich, der allenfalls punktuelle Informationszugangsrechte kannte, so etwa im Umweltinformationsrecht. Der Gesetzgeber hat die Regelung eines allgemeinen Rechts auf Auskunft nicht zum Anlass genommen, die bestehenden kommunalrechtlichen Regelungen anzupassen, wobei eine insgesamt spannungsfreie Regelungslage am einfachsten durch Aufhebung von Art. 54 Abs. 3 Satz 2 GO und

Art. 48 Abs. 2 Satz 2 LKrO hätte erreicht werden können. Dies spricht für die Annahme, dass für die Sitzungsniederschriften der kommunalen Selbstverwaltungsgremien das hergebrachte Zugangsregime erhalten werden sollte,[101] die beiden beibehaltenen besonderen Zugangsansprüche mithin „Regelung[en] in anderen Rechtsvorschriften" im Sinne von Art. 39 Abs. 2 BayDSG darstellen. Nach Einführung von Art. 39 Abs. 1 Satz 1 BayDSG hat das allerdings die Konsequenz, dass das „Transparenzniveau" bei den Sitzungsniederschriften hinsichtlich der Anspruchsberechtigung und des Anspruchsgegenstands niedriger ausfällt als in dem von Art. 39 Abs. 1 Satz 1 BayDSG „abgedeckten" Bereich. Gleichwohl griffe die Annahme zu kurz, dass eine ursprünglich als „Transparenzinsel" konzipierte Regelung nun in Anbetracht eines geänderten Regelungsumfelds als „Intransparenzinsel" zu beschreiben wäre: Immerhin wird den in Art. 54 Abs. 3 Satz 2 GO und Art. 48 Abs. 2 Satz 2 LKrO berechtigten Personengruppen für Niederschriften öffentlicher Sitzungen der Zugang durch Verzicht auf die glaubhafte Darlegung eines berechtigten Interesses erleichtert. Für eine Anwendung von Art. 39 Abs. 2 BayDSG auf Art. 54 Abs. 3 Satz 2 GO und Art. 48 Abs. 2 Satz 2 LKrO sprechen daher insgesamt wohl die besseren Argumente.[102]

Die in Art. 39 Abs. 1 Satz 1 BayDSG zum Ausdruck gebrachte Grundentscheidung für eine transparente Verwaltung sollte geichwohl berücksichtigt werden, wenn sich Zugangsanträge nach Art. 54 Abs. 3 Satz 2 GO und Art. 48 Abs. 2 Satz 2 LKrO auf eine **Bereitstellung von Kopien** richten. Wird einem solchen Anliegen insbesondere entsprochen, wenn eine Niederschrift umfangreiche, komplexe oder sonst im begrenzten zeitlichen Rahmen einer Einsicht nicht erfassbare Informationen enthält, oder wenn sich eine anspruchsberechtigte Person mit einer Kostenerstattung nach dem Kostengesetz einverstanden erklärt, so wirkt dies auch auf eine Harmonisierung der besonderen kommunalrechtlichen Zugangsrechte mit Art. 39 Abs. 1 Satz 1 BayDSG hin.

13.2.3 Optionen zur Verbesserung der Transparenz

Soweit Kommunen das durch Art. 54 Abs. 3 Satz 2 GO und Art. 48 Abs. 2 Satz 2 LKrO gewährleistete Maß an Transparenz verbessern möchten, stehen verschiedene Handlungsoptionen zur Verfügung:

— Zunächst sind Kommunen nicht gehindert, im Rahmen von Art. 54 Abs. 3 Satz 2 GO und Art. 48 Abs. 2 Satz 2 LKrO auch **Zugangsanträgen** zu entsprechen, die nicht **von anspruchsberechtigten Personen** gestellt sind. Das Gesetz räumt zwar insofern keinen Anspruch ein, verbietet die Zugangsgewährung aber auch nicht.

— Was **Zugangsanträge** betrifft, **die auf** eine Bereitstellung von Sitzungsniederschriften in **Kopie zielen**, können sich Kommunen im Rahmen von

101 In diese Richtung auch die das Kommunalrecht ausdrücklich erwähnende Gesetzesbegründung, siehe Landtags-Drucksache 17/7537, S. 50.

102 Siehe auch Engelbrecht, Das allgemeine Recht auf Auskunft im Bayerischen Datenschutzgesetz, 2017, Teil 1 Rn. 167, sowie die Antwort des (damaligen) Bayerischen Staatsministeriums des Innern und für Integration auf eine Anfrage zum Plenum des Bayerischen Landtags in Landtags-Drucksache 17/23287, S. 17. – Im Ergebnis wie hier für das Verhältnis von § 38 Abs. 2 Satz 4 GemO BW zu § 1 Abs. 2 LIFG BW auch Verwaltungsgerichtshof Baden-Württemberg, Urteil vom 4. Februar 2020, 10 S 1229/19, BeckRS 2020, 2371, Rn. 20 ff.

Art. 54 Abs. 3 Satz 2 GO und Art. 48 Abs. 2 Satz 2 LKrO für eine Verwaltungspraxis entscheiden, die dem Anliegen der jeweils zugangsinteressierten Person grundsätzlich entspricht: Werden Kopien beantragt, wird der Zugang im Regelfall in dieser Form gewährt.

— Soweit die Kommune den rechtlich gebotenen Schutz von Vertraulichkeitsinteressen sicherstellt, kann sie in einer **Informationsfreiheitssatzung** Regelungen treffen, welche die in Art. 54 Abs. 3 Satz 2 GO und Art. 48 Abs. 2 Satz 2 LKrO genannten Niederschriften erfassen.[103]

— Unter Beachtung des rechtlich gebotenen Schutzes von Vertraulichkeitsinteressen kann sich die Kommune zudem dafür entscheiden, Niederschriften der in Art. 54 Abs. 3 Satz 2 GO und Art. 48 Abs. 2 Satz 2 LKrO genannten Art auf der **Homepage**, in einem elektronischen **Bürgerinformationssystem** oder einem – durch Informationsfreiheitssatzung eingerichteten[104] – **örtlichen Transparenzportal** zu veröffentlichen. Welche Vorkehrungen im Hinblick auf den rechtlich gebotenen Schutz von Vertraulichkeitsinteressen zu treffen sind, ist für den Bereich des Datenschutzes an anderer Stelle dargelegt.[105]

Aus Datenschutzsicht dürfen Kommunen allerdings nicht die in Art. 54 Abs. 3 Satz 2 GO und Art. 48 Abs. 2 Satz 2 LKrO zum Ausdruck kommende **Entscheidung des Gesetzgebers** relativieren, die **Niederschriften nichtöffentlicher Sitzungen unter Verschluss** zu halten. An dieser Vorgabe wären auf eine „Aufweichung" zielende örtliche Regelungen – insbesondere in Informationsfreiheitssatzungen – sowie eine entsprechende Verwaltungspraxis zu messen.

Gemeinderatsmitglieder, die Wünsche aus der Bürgerschaft nach mehr Transparenz bei den Niederschriften öffentlicher Sitzungen der kollegialen Selbstverwaltungsorgane unterstützen möchten, können dazu insbesondere ihr **Antragsrecht** nutzen. **Bürgerinnen und Bürgern** stehen entsprechend die Instrumente des **Bürgerantrags** (Art. 18b GO, Art. 12b LKrO) sowie des **Bürgerbegehrens** (Art. 18a GO, Art. 12a LKrO) zur Verfügung.

13.2.4 Fazit

Art. 54 Abs. 3 Satz 2 GO und Art. 48 Abs. 2 Satz 2 LKrO gewähren Gemeindebürgern und Forensen sowie Kreisbürgern voraussetzungslose Zugangsansprüche zu Sitzungsniederschriften der kollegialen Selbstverwaltungsorgane. Die Ansprüche sind primär auf Einsicht gerichtet, können jedoch auch in anderer Form erfüllt werden. Das Verhältnis dieser Zugangsansprüche zu Art. 39 Abs. 1 Satz 1 BayDSG ist durch Art. 39 Abs. 2 BayDSG mit der Folge reguliert, dass sich der Zugang zu den Sitzungsniederschriften auch weiterhin nach dem kommunalrechtlichen Sonderregime richtet. Ob das noch zeitgemäß ist, hat der Gesetzgeber zu beurteilen. Solange dieses Sonderregime fortbesteht, können die Kommunen immerhin einige Spielräume nutzen, um die Transparenz ihrer Verwaltungstätigkeit auch in

103 Dazu näher Engelbrecht, Die gemeindliche Informationsfreiheitssatzung und der Schutz personenbezogener Daten, KommP BY 2017, S. 397 ff.
104 Vgl. Engelbrecht, KommP BY 2017, S. 397 (399 f.).
105 Bayerischer Landesbeauftragter für den Datenschutz, FSt. BY 2018, Nr. 42.

Bezug auf die Niederschriften der öffentlichen Sitzungen ihrer kollegialen Selbstverwaltungsorgane zu erhöhen.

13.3 Zugang zu Ministerialschreiben

Im Rahmen meiner Aufsichtstätigkeit erreichen mich regelmäßig Anfragen von Bürgern, die um Informationszugang bei öffentlichen Stellen mithilfe des allgemeinen Auskunftsanspruchs nach Art. 39 Abs. 1 Satz 1 BayDSG nachsuchen. So begehrte im Berichtszeitraum ein Bürger die Kopie eines Rundschreibens eines Staatsministeriums, weil enthaltene Informationen zur Einschätzung der Rechtslage im Rahmen eines anderweitigen Rechtsstreits relevant waren.

Derartige Rundschreiben – nach verfassendem Staatsministerium etwa IMS (für Schreiben des Bayerischen Staatsministeriums des Innern, für Sport und Integration) oder KMS (für Schreiben des Bayerischen Staatsministeriums für Unterricht und Kultus) genannt – sind regelmäßig an die dem jeweiligen Fachministerium nachgeordneten Dienststellen gerichtet und enthalten Anwendungs- und Auslegungshilfen (Vollzugshinweise) zu Rechtsvorschriften des jeweiligen Ressorts oder Hinweise zum Umgang mit Rechtsänderungen. Auf diese Weise soll eine landesweit einheitliche Rechtsanwendung bei den Fachbehörden erleichtert werden. Derartige Schreiben werden zum Teil vom jeweiligen Fachministerium veröffentlicht, zum Teil handelt es sich aber auch um behördeninterne Informationen.

Das allgemeine Recht auf Auskunft in Art. 39 Abs. 1 Satz 1 BayDSG fordert, dass die auskunftsbegehrende Person ein berechtigtes Interesse glaubhaft darlegt. Ein berechtigtes Interesse kann dabei grundsätzlich jedes rechtliche, wirtschaftliche oder ideelle Interesse darstellen. Vorliegend konnte der Bürger erklären, dass er das betreffendem, nicht veröffentlichte Ministerialschreiben benötigte, um die Rechtslage in einem ihn betreffenden anderweitigen Verfahren und somit die Erfolgsaussichten etwaiger Rechtsbehelfe abschließend einschätzen zu können.

Das betreffende Staatsministerium lehnte zunächst das Auskunftsersuchen des Bürgers mit der Begründung ab, dass das Rundschreiben allein an Behörden adressiert sei und es sich um einen verwaltungsinternen Vorgang handele. Auch würde das Staatsministerium insoweit in Wahrnehmung einer Aufsichtsaufgabe handeln, die der Auskunftserteilung entgegenstehe.

Ich habe das Staatsministerium dahingehend beraten, dass der bloßen Adressierung eines Schreibens keine Bedeutung zukommt. Denn der Sinn des in Art. 39 Abs. 1 Satz 1 BayDSG geregelten allgemeinen Informationszugangsanspruchs liegt gerade darin, Nichtadressaten die grundsätzliche Möglichkeit einer Kenntnisnahme zu verschaffen. Der verwaltungsinterne Verwendungszweck des Schreibens vermag Auskunftsanspruch ebenfalls nicht auszuschließen. Vielmehr sind die Gründe, die zu einer Ablehnung des Auskunftsbegehrens führen können, allein in Art. 39 BayDSG aufgeführt; diese Gründe sind von der die Auskunft ablehnenden öffentlichen Stelle zu prüfen und vorzubringen.

Soweit das Staatsministerium mit der Wahrnehmung von Aufsichtsaufgaben gegenüber nachgeordneten Dienststellen argumentierte, berief es sich auf den Versagungsgrund des Art. 39 Abs. 1 Satz 2 Nr. 1 1. Var. BayDSG.

Art. 39 BayDSG
Allgemeines Auskunftsrecht
(1) [1][…] [2]Die Auskunft kann verweigert werden, soweit
1. Kontroll- und Aufsichtsaufgaben oder sonstige öffentliche oder private Interessen entgegenstehen,
[…].

Zwar ist das Staatsministerium gegenüber den nachgeordneten Dienststellen, an die das ministerielle Rundschreiben gerichtet war, die oberste Aufsichtsbehörde. Die Erstellung und der Versand des Schreibens kann mithin als Aufsichtsaufgabe angesehen werden. Gleichwohl war nicht ersichtlich, weshalb die Aufsichtsaufgabe der Auskunftserteilung entgegenstehen sollte. Es wurde nicht dargelegt, inwiefern die Aufsichtsaufgaben des Staatsministeriums durch die Offenlegung des Schreibens beeinträchtigt werden konnten.

Im Ergebnis hat das Staatsministerium aufgrund meiner Beratung dem Bürger Zugang zu dem betreffenden Schreiben gewährt.

14 Datenschutzkommission

Der Datenschutzkommission beim Bayerischen Landtag gehörten am Ende des Berichtszeitraums folgende Mitglieder und stellvertretende Mitglieder an:

Aus dem Landtag:

Mitglieder:

Peter Tomaschko, CSU
Benjamin Adjei, BÜNDNIS 90/DIE GRÜNEN
Alfred Grob, CSU
Martin Hagen, FDP
Gerd Mannes, AfD
Gerald Pittner, FREIE WÄHLER
Florian Ritter, SPD

Stellvertretende Mitglieder:

Tanja Schorer-Dremel, CSU
Verena Osgyan, BÜNDNIS 90/DIE GRÜNEN
Andreas Jäckel, CSU
Matthias Fischbach, FDP
Roland Magerl, AfD
Wolfgang Hauber, FREIE WÄHLER
Christian Flisek, SPD

Auf Vorschlag der Staatsregierung:

Mitglied:

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

Stellvertretendes Mitglied:

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

Auf Vorschlag der kommunalen Spitzenverbände in Bayern:

Mitglied:

Rudolf Schleyer, Vorstandsvorsitzender der Anstalt für Kommunale Datenverarbeitung in Bayern

Stellvertretendes Mitglied:

Gudrun Aschenbrenner, Mitglied des Vorstands der Anstalt für Kommunale Datenverarbeitung in Bayern

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

Mitglied:

Werner Krempl, Erster Direktor und Vorsitzender der Geschäftsführung der Deutschen Rentenversicherung Nordbayern

Stellvertretendes Mitglied:

Dr. Irmgard Stippler, Vorstandsvorsitzende der AOK Bayern – Die Gesundheitskasse

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

Mitglied:

Dr. Till Schemmann, Notar

Stellvertretendes Mitglied:

Dr. Thomas Kuhn, Rechtsanwalt

Herr Peter Tomaschko, MdL, führte den Vorsitz in der Datenschutzkommission; stellvertretender Vorsitzender war Herr Benjamin Adjei, MdL.

Die Datenschutzkommission beim Bayerischen Landtag tagte im Berichtszeitraum drei Mal.

15 Anlagen

Anlage 1: Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 3. April 2020: Datenschutz-Grundsätze bei der Bewältigung der Corona-Pandemie

Die Corona-Pandemie stellt eine der größten Bewährungsproben für die europäischen Gesellschaften seit Jahrzehnten dar. Alle Mitgliedstaaten der Europäischen Union haben gegenwärtig extreme Herausforderungen zu bewältigen, um die Gesundheit ihrer Bevölkerung zu gewährleisten. Angesichts der bereits getroffenen Maßnahmen wird gleichzeitig der Wert der Freiheitsrechte erlebbar, zu denen auch das Grundrecht auf informationelle Selbstbestimmung gehört.

Für die Stabilität von Staat und Gesellschaft ist es in dieser Lage unverzichtbar, dass sich die Bürgerinnen und Bürger darauf verlassen können, dass Freiheitsrechte wie das Grundrecht auf informationelle Selbstbestimmung nur so weit und so lange eingeschränkt werden, wie es zwingend erforderlich und angemessen ist, um die Gesundheit der Bevölkerung wirksam zu schützen. Einschneidende Regelungen müssen umkehrbar und eng befristet sein und von den Gesetzgebern und nicht allein durch die Exekutive verantwortet werden.

Was die Rechtfertigung der Verarbeitung personenbezogener Daten nach Maßgabe der europäischen Datenschutz-Grundverordnung anbelangt, stellt sie insbesondere in ihrem Artikel 5 **europaweit einheitliche Grundsätze** bereit, die als Leitfaden für staatliches Handeln auch gerade in Krisenzeiten dienen können, einer effektiven Bekämpfung der Corona-Pandemie nicht entgegenstehen und zugleich einen grundrechtsschonenden Umgang mit personenbezogenen Daten gewährleisten.

Im Zusammenhang mit der Bewältigung der Corona-Krise weist die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder daher auf **folgende wesentliche Rechtmäßigkeitsvoraussetzungen für die Verarbeitung personenbezogener Daten** hin:

— Krisenzeiten ändern nichts daran, dass die **Verarbeitung** personenbezogener Daten stets auf einer **gesetzlichen Grundlage** zu erfolgen hat. Das bedingt insbesondere, dass die mit einer Verarbeitung verfolgten Zwecke möglichst genau bezeichnet werden.

— Die **geplanten Maßnahmen** müssen zudem kritisch auf ihre **Eignung** überprüft werden, um etwa Infektionen zu erfassen, infizierte Personen zu behandeln oder Neuinfektionen zu verhindern. So kann es in Notfalllagen beispielsweise eine geeignete Maßnahme sein, Hilfsorganisationen zu verpflichten, medizinisch ausgebildetes Personal an die für die Gesundheitsversorgung zuständigen Behörden zu melden. Hingegen bestehen erhebliche Zweifel an der Eignung etwa von Maßnahmen, die allein mithilfe von Telekommunikationsverkehrsdaten individuelle Infektionswege nachvollziehen sollen.

- Die geplanten Maßnahmen müssen erforderlich sein. Stehen **ebenfalls geeignete Maßnahmen zur Zweckerreichung** zur Verfügung, die **weniger**, oder – wie eine vorherige Anonymisierung – sogar gar nicht in die Rechte der Menschen eingreifen, müssen diese vorrangig umgesetzt werden. Zudem darf die Verarbeitung der personenbezogenen Daten **nicht** – wie die präventive Überwachung ausnahmslos der gesamten Bevölkerung – **außer Verhältnis zum angestrebten legitimen Zweck** stehen. Daraus folgt, dass besonders stark freiheitseinschränkende Maßnahmen auch an besondere Voraussetzungen geknüpft werden müssen – etwa an die formelle Feststellung einer Gesundheitsnotlage, wie sie nach dem Infektionsschutzrecht in einigen Ländern bereits erfolgt ist.

- Zur verhältnismäßigen Ausgestaltung der Verarbeitung von sensiblen Daten gehört es schließlich, dass die speziell zur Bewältigung der Corona-Pandemie getroffenen Maßnahmen umkehrbar in dem Sinne gestaltet werden, dass sie nach Krisenende wieder zurückgenommen werden können und, wenn sie dann unverhältnismäßig sind, sogar müssen. So sind **nicht mehr für die benannten Zwecke benötigte** personenbezogene Daten **unverzüglich** zu **löschen**. Generell sollten zudem **alle Maßnahmen befristet** werden. Dies gilt insbesondere für solche gesetzlichen Maßnahmen, die in besonderem Maße in die Grundrechte der betroffenen Personen eingreifen.

- Technisch-organisatorische Maßnahmen zum Schutz der Integrität und Vertraulichkeit von Gesundheitsdaten sind nicht nur **rechtlich geboten**, sondern auch **notwendig**, um eine missbräuchliche Verwendung von Daten zu verhindern und Fehlern in der Verarbeitung entgegenzuwirken. Wichtig ist es auch, im Sinne des Datenschutz-Grundsatzes der Transparenz die betroffenen Personen in verständlicher Weise über die Verarbeitung ihrer Daten zu informieren.

Datenschutz-Grundsätze bieten gerade auch in Krisenzeiten hinreichende Gestaltungsmöglichkeiten für eine rechtskonforme Verarbeitung personenbezogener Daten. Ihre Einhaltung leistet einen Beitrag zur Wahrung der Freiheit in der demokratischen Gesellschaft.

Anlage 2: Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 26. August 2020: Registermodernisierung verfassungskonform umsetzen!

Mit dem Gesetz zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung (enthalten im Registermodernisierungsgesetz - RegMoG) plant die Bundesregierung eine Modernisierung der in der Verwaltung geführten Register. Hierzu soll u.a. eine Identifikationsnummer (ID-Nr.) für natürliche Personen als registerübergreifendes Ordnungsmerkmal in alle für die Umsetzung des Onlinezugangsgesetzes relevanten Register von Bund und Ländern eingeführt werden.

Als übergreifendes Ordnungsmerkmal soll die Steuer-Identifikationsnummer (Steuer-ID) dienen, vor deren fortschreitend ausgedehnter Nutzung die Datenschutzbeauftragten des Bundes und der Länder mehrfach deutlich gewarnt hatten. Die nun geplante ausgedehnte Verwendung der Steuer-ID als einheitliches

Personenkennzeichen löst sich vollständig von ihrer ursprünglichen Zweckbestimmung für rein steuerliche Sachverhalte, obwohl sie nur deswegen bislang als verfassungskonform angesehen werden kann.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) wies bereits in ihrer Entschließung vom 12.09.2019 darauf hin, dass die Schaffung solcher einheitlichen und verwaltungsübergreifenden Personenkennzeichen bzw. Identifikatoren (auch in Verbindung mit einer entsprechenden Infrastruktur zum Datenaustausch) die Gefahr birgt, dass personenbezogene Daten in großem Maße leicht verknüpft und zu einem umfassenden Persönlichkeitsprofil vervollständigt werden können.

Das Bundesverfassungsgericht hat der Einführung derartiger Personenkennzeichen seit jeher enge Schranken auferlegt, die hier missachtet werden. Der Blick auf den Anwendungsumfang der geplanten Regelung zeigt das Potential der möglichen missbräuchlichen Verwendung.

So verknüpft der Gesetzentwurf bei mehr als 50 Registern die Steuer-ID als zusätzliches Ordnungsmerkmal. Auf diese Weise könnten Daten etwa aus dem Melderegister mit Daten aus dem Versichertenverzeichnis der Krankenkassen sowie dem Register für ergänzende Hilfe zum Lebensunterhalt oder dem Schuldnerverzeichnis abgeglichen und zu einem Persönlichkeitsprofil zusammengefasst werden. Die im Gesetzentwurf vorgesehenen technischen und organisatorischen Sicherungen genügen nicht, um eine solche Profilbildung wirksam zu verhindern. Diese stellen zwar sicher, dass nur autorisierte Behörden die erforderlichen Daten Ende-zu-Ende verschlüsselt übermitteln. Sie bieten aber keinen ausreichenden Schutz gegen die missbräuchliche Zusammenführung der Daten zu einer Person, die aus unterschiedlichen Registern stammen, übrigens auch nicht bei Datenlecks. Zudem ist damit zu rechnen, dass die neue ID-Nr. auch im Wirtschaftsleben weite Verbreitung finden wird, was das Missbrauchsrisiko weiter erhöht.

Die Datenschutzkonferenz hatte demgegenüber „sektorspezifische“ Personenkennziffern gefordert, die datenschutzgerecht und zugleich praxisgeeignet sind, weil sie einerseits einen einseitigen staatlichen Abgleich deutlich erschweren und andererseits eine natürliche Person eindeutig identifizieren.

Obwohl ein solches Modell in der Republik Österreich seit vielen Jahren erfolgreich praktiziert wird, hat die Bundesregierung dies nie ernsthaft erwogen und ohne überzeugende Begründung mit dem pauschalen Verweis auf „rechtliche, technische und organisatorische Komplexität“ abgelehnt.

Auch wenn die Corona-Pandemie zeigt, wie notwendig eine Beschleunigung der Digitalisierung ist, darf dies nicht als Argument dafür benutzt werden, verfassungsrechtlich notwendige Nachbesserungen unter Hinweis auf den „Eilbedarf“ unter den Tisch fallen zu lassen.

Die Datenschutzkonferenz weist daher nochmals darauf hin, dass die dem Gesetzentwurf zugrundeliegende Architektur im Widerspruch zu verfassungsrechtlichen Regelungen steht. Sie fordert deshalb die Bundesregierung dazu auf, einen Entwurf vorzulegen, der den verfassungsrechtlichen Anforderungen genügt, bevor sie durch Entscheidung des Bundesverfassungsgerichts dazu verpflichtet wird.

Anlage 3: Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 1. September 2020: Patientendaten-Schutz-Gesetz: Ohne Nachbesserungen beim Datenschutz für die Versicherten europarechtswidrig!

Der Deutsche Bundestag hat am 3. Juli 2020 das Patientendaten-Schutz-Gesetz (PDSG) entgegen der von den unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder geäußerten Kritik beschlossen. Die Kritik richtet sich insbesondere gegen das nur grobgranular ausgestaltete Zugriffsmanagement, die Authentifizierung für die elektronische Patientenakte (EPA) und die Vertreterlösung für Versicherte, die nicht über ein geeignetes Endgerät verfügen.

Das PDSG soll am 18. September 2020 im Bundesrat abschließend beraten werden. Zentrale Gesetzesregelungen stehen in Widerspruch zu elementaren Vorgaben der EU-Datenschutz-Grundverordnung (DSGVO). Entgegen des derzeitigen Entwurfs müssen die Versicherten bereits zum Zeitpunkt der Einführung der EPA am 1. Januar 2021 die volle Hoheit über ihre Daten erhalten. Dies entspricht auch den im PDSG vom Gesetzgeber selbst formulierten Vorgaben, die Patientensouveränität über die versichertengeführten EPA grundsätzlich ohne Einschränkungen zu wahren und die Nutzung der EPA für alle Versicherten datenschutzgerecht auszugestalten.

Diese Ziele werden mit dem Gesetzentwurf nicht erreicht. Zum Start der EPA werden alle Nutzerinnen und Nutzer in Bezug auf die von den Leistungserbringern (Ärzten etc.) in der elektronischen Patientenakte gespeicherten Daten zu einem „alles oder nichts“ gezwungen, da im Jahr 2021 keine Steuerung auf Dokumentenebene für diese Daten vorgesehen ist. Das bedeutet, dass diejenigen, denen die Versicherten Einsicht in ihre Daten gewähren, alle dort enthaltenen Informationen einsehen können, auch wenn dies in der konkreten Behandlungssituation nicht erforderlich ist.

Erst ein Jahr nach dem Start der EPA, d.h. ab dem 1. Januar 2022, können lediglich Versicherte, die für den Zugriff auf ihre EPA geeignete Endgeräte (Smartphone, Tablet etc.) nutzen, eigenständig eine dokumentengenaue Kontrolle und Rechtevergabe in Bezug auf diese Dokumente durchführen.

Alle anderen Versicherten, die keine geeigneten Endgeräte besitzen oder diese aus Sicherheitsgründen zum Schutz ihrer sensiblen Gesundheitsdaten nicht nutzen möchten (d. h. sogenannte Nicht-Frontend-Nutzer), erhalten auch über den Stichtag 1. Januar 2022 hinaus nicht diese Rechte. Ab dem 1. Januar 2022 ermöglicht das PDSG insoweit den Nicht-Frontend-Nutzern lediglich eine Vertreterlösung. Danach können diese mittels eines Vertreters und dessen mobilem Endgerät ihre Rechte ausüben. Im Vertretungsfall müssten die Versicherten jedoch ihrem Vertreter den vollständigen Zugriff auf ihre Gesundheitsdaten einräumen.

Ein weiterer Kritikpunkt ist das Authentifizierungsverfahren für die EPA und die „Gewährleistung des erforderlichen hohen datenschutzrechtlichen Schutzniveaus“. Da es sich bei den fraglichen Daten um Gesundheitsdaten und damit um höchst sensible persönliche Informationen handelt, muss nach den Vorgaben der DSGVO die Authentifizierung ein höchstmögliches Sicherheitsniveau nach dem Stand der Technik gewährleisten. Dies gilt insbesondere für Authentifizierungsverfahren ohne Einsatz der elektronischen Gesundheitskarte. Wenn dabei alternative Authentifizierungsverfahren genutzt werden, die diesen hohen Standard nicht erfüllen, liegt ein Verstoß gegen die DSGVO vor.

Der Bundesrat hat in seiner Stellungnahme zum PDSG vom 15. Mai 2020 (BR-Drs. 164/1/20, s. Ziffer 21. zu Artikel 1 Nummer 31 [§§ 334 ff. SGB V-E9]) die Bundesregierung auf erhebliche Bedenken im Hinblick auf die DSGVO-Konformität des PDSG hingewiesen. Seine Kritik bezieht sich im Wesentlichen auf das zum Start der EPA fehlende feingranulare Zugriffsmanagement und die daraus resultierende Einschränkung der Datensouveränität der Versicherten. Er hat die Bundesregierung aufgefordert, im weiteren Gesetzgebungsverfahren insbesondere den Regelungsvorschlag zum Angebot und zur Einrichtung der EPA (§ 342 SGB V) umfassend bezüglich datenschutzrechtlicher Bedenken zu prüfen.

Auch im Lichte dessen fordern die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder den Bundesrat auf, anlässlich seiner für den 18. September 2020 anberaumten Beratung den Vermittlungsausschuss anzurufen, um notwendige datenschutzrechtliche Verbesserungen des PDSG noch im Gesetzgebungsverfahren zu erwirken.

Anlage 4: Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 22.September 2020: Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen

Der Begriff „Digitale Souveränität“ wird in der öffentlichen Debatte in verschiedenen Bedeutungen verwendet. Nach der Definition des Kompetenzzentrums Öffentliche IT[1] ist in einem umfassenden Sinne Digitale Souveränität die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rollen in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.

Die Rolle der öffentlichen Verwaltung ist die gesetzesgebundene Erfüllung der Staatsaufgaben. Aus der Sicht der Verantwortlichen in der öffentlichen Verwaltung bedeutet Digitale Souveränität insbesondere, eigenständig entscheiden zu können, wie die in Art. 1 Datenschutz-Grundverordnung (DS-GVO) formulierten Ziele im Einklang mit den in Art. 5 DS-GVO festgelegten Grundsätzen für die Verarbeitung personenbezogener Daten, wie Rechtmäßigkeit, Transparenz, Zweckbindung und Sicherheit der Verarbeitung, umzusetzen sind. Dies erfordert nach Ansicht der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) Wahlfreiheit und vollständige Kontrolle der Verantwortlichen über die eingesetzten Mittel und Verfahren bei der digitalen Verarbeitung von personenbezogenen Daten, gegebenenfalls unter Hinzuziehung des jeweiligen Auftragsverarbeiters.

Die Digitale Souveränität der öffentlichen Verwaltung ist jedoch nach einer für den Beauftragten der Bundesregierung für Informationstechnik durchgeführten „Strategischen Marktanalyse“[2] beeinträchtigt, „da die Geschäftsbeziehungen der öffentlichen Verwaltung mit externen, meist privaten IT-Anbietern erhebliche Ab-

1 Kompetenzzentrum Öffentliche IT (Hrsg.), Gabriele Goldacker, Digitale Souveränität, erhältlich unter https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souver%C3%A4nit%C3%A4t.

2 PwC Strategy& (Germany) GmbH, Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern, erhältlich unter https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.pdf?__blob=publicationFile.

hängigkeiten verursachen. Danach resultieren diese Abhängigkeiten aus der technischen Beschaffenheit der IT-Landschaft, aus den stark auf Software ausgerichteten Prozessen, aus dem Umstand, dass sich die Beschäftigten an die eingesetzte Software gewöhnt haben, aus Vertragsklauseln sowie aus den bestehenden Marktgegebenheiten." Sie bringen Kontrollverlust und eine eingeschränkte Verfügbarkeit, Vertraulichkeit und Integrität der verarbeiteten personenbezogenen Daten mit sich. Auch vor diesem Hintergrund hat sich der IT-Planungsrat zum Ziel gesetzt, die digitale Souveränität der öffentlichen Verwaltung in ihren Rollen als Nutzer, Bereitsteller und Auftraggeber von digitalen Technologien kontinuierlich zu stärken.

Die Datenschutzkonferenz teilt die Einschätzung des IT-Planungsrats, dass die Digitale Souveränität der öffentlichen Verwaltung beeinträchtigt ist und sieht deren Gewährleistung als ein vordringliches Handlungsfeld an. Aus ihrer Sicht sind datenschutzrechtliche Vorgaben für große Softwareanbieter, die in der „Strategischen Marktanalyse" empfohlene Diversifizierung durch den Einsatz alternativer Softwareprodukte sowie die Nutzung von Open Source Software besonders erfolgversprechende Handlungsoptionen. Durch den Einsatz von Open Source Software kann die Unabhängigkeit der öffentlichen Verwaltung von marktbeherrschenden Softwareanbietern dauerhaft sichergestellt werden. Konkret fordert die Datenschutzkonferenz Bund, Länder und Kommunen dazu auf, langfristig nur solche Hard- und Software einzusetzen,

- die den Verantwortlichen die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik belässt, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Zustimmung der Verantwortlichen im Einzelfall erfolgen,

- bei der alle zur Verfügung stehenden Sicherheitsfunktionen für Verantwortliche transparent sind und

- die eine Nutzung der Hard- und Software sowie den Zugriff auf personenbezogene Daten ermöglicht, ohne dass Unbefugte davon Kenntnis erhalten und ohne dass unzulässige Nutzungsprofile angelegt werden können.

Kurzfristig erfordert die Stärkung der Digitalen Souveränität der öffentlichen Verwaltung in Bund, Ländern und Kommunen zur Einhaltung der datenschutzrechtlichen Anforderungen insbesondere:

1. Verbesserte Möglichkeiten der datenschutzrechtlichen Beurteilung von Produkten und Dienstleistungen – sowohl bei der Auswahl als auch im laufenden Betrieb:

    - Zertifizierungen können Verantwortlichen die Prüfung und Kontrolle erleichtern, wenn sie sich nicht eigenständig ein valides Bild über die komplexe Funktionsweise von Informationstechnik machen können.

    - Die Ministerialebene sollte in die Pflicht genommen werden, Vorgaben für die öffentliche Verwaltung zu machen.

    - Zudem sollten Behörden stärker kooperieren, um die erforderliche Expertise selbst bereitstellen zu können.

2. Berücksichtigung der Ziele und Kriterien der Digitalen Souveränität bei der Vergabe und Beschaffung von Hardware, Software, Informations- und Kommunikationstechnik sowie IT-Dienstleistungen:

   — Für die Vergabe und Beschaffung von Hardware, Software, Informations- und Kommunikationstechnik sowie IT-Dienstleistungen sollten im Einklang mit dem europäischen Vergaberecht Ausschreibungskriterien entwickelt werden, um bei der Vergabe solche Anbieter bevorzugt auswählen zu können, welche Digitale Souveränität ermöglichen.

3. Nutzung von offenen Standards durch die Produktentwickler, damit die Verantwortlichen auch tatsächlich in die Lage versetzt werden, Anbieter und Produkte zu wechseln, wenn sie mit deren Produkten und Dienstleistungen die Datenschutzanforderungen nicht (mehr) oder nur ungenügend umsetzen können:

   — Die Nutzung von offenen Standards kann durch deren inhärente Transparenz dazu beitragen, die Überprüfbarkeit zu sichern und eine Kontrolle zu erleichtern. Dies betrifft Systemsoftware und insbesondere Datenformate, aber auch Datenbanken und Anwendungssoftware, die auf Software-Plattformen aufsetzen. Offene Standards sind zudem geeignet, unerwünschte Lock-in-Effekte zu vermeiden. Insbesondere können hierbei über die Einrichtung von Bund-/Länder-/Kommunen-übergreifenden Entwicklungsverbünden Aufwände verteilt und Skaleneffekte gehoben werden. Daher sollten Verantwortliche den Einsatz von Produkten und Dienstleistungen bevorzugen, die offene Standards verwenden.

4. Veröffentlichung des Quellcodes und der Spezifikationen öffentlich finanzierter digitaler Entwicklungen:

   — Wenn Software oder Hardwarestandards unter finanzieller Beteiligung der öffentlichen Hand entwickelt werden, sollten diese standardmäßig so veröffentlicht werden, dass diese nachvollzogen werden können.

   — Standardmäßig sollten diese so ausgestaltet werden, dass eine öffentliche Weiterentwicklung möglich ist (Open Source Lizenzen).

5. Möglichkeiten zur Steuerung des Zugriffs auf Daten, der Konfiguration von Systemen und der Gestaltung von Prozessen:

   — Verantwortliche müssen über tatsächliche Steuerungsmöglichkeiten verfügen, insbesondere, um ihre Pflichten nach Art. 25 DS-GVO erfüllen zu können. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen muss elementarer Bestandteil von Dienstleistungen und Produkten sein, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Verantwortliche sollten nur solche Produkte und Dienstleistungen beschaffen und nutzen, die diese Prinzipien beachten. Organisationen mit verteilter Verantwortung (etwa Kommunen, Bundesländer oder auch beteiligte Dienstleister wie Konzerne) müssen auch bei zentral beschafften oder betriebenen Komponenten wie Hardware,

Software und Dienstleistungen die erforderlichen Einstellungen vornehmen können, um einen rechtskonformen Betrieb der Verfahren zu gewährleisten. Bei zentral bereitgestellten Anwendungen, etwa in einer derzeit im IT-Planungsrat diskutierten „Verwaltungscloud", ist es eine notwendige Voraussetzung, dass die jeweiligen datenschutzrechtlichen Vorgaben der Verantwortlichen für Betrieb und Konfiguration individuell umgesetzt werden können. Das ist bei der Konzeption zu berücksichtigen.

Die Datenschutzkonferenz ist der Ansicht, dass die Stärkung der Digitalen Souveränität große strategische Bedeutung für die öffentliche Verwaltung hat und gemeinsam und kontinuierlich vorangetrieben werden muss. Sie fordert Bund, Länder und Kommunen dazu auf, die in der Entschließung aufgeführten Kriterien für eine Stärkung der Digitalen Souveränität der öffentlichen Verwaltung in den Bereichen IT-Beschaffung sowie System- und Fachverfahrensentwicklung zu berücksichtigen.

Anlage 5: Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 25.November 2020: Für den Schutz vertraulicher Kommunikation durch eine sichere Ende-zu-Ende-Verschlüsselung – Vorschläge des Rates der Europäischen Union stoppen

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) tritt Forderungen der Regierungen der Mitgliedstaaten der Europäischen Union entgegen, Sicherheitsbehörden und Geheimdiensten die Möglichkeit zu eröffnen, auf Inhalte verschlüsselter Kommunikation zuzugreifen. Als Reaktion auf jüngste Terroranschläge soll diesen Behörden und Diensten der Zugriff auf die verschlüsselte Kommunikation ermöglicht werden. Dies umfasst insbesondere auch Messenger-Dienste wie WhatsApp, Threema oder Signal. Nach dem Resolutionsentwurf „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung" des Rates der Europäischen Union (Nr. 12143/1/20 vom 6. November 2020) sollen entsprechende Möglichkeiten in Zusammenarbeit mit den Anbietern von Online-Diensten entwickelt werden.

Eine sichere und vertrauenswürdige Verschlüsselung ist essentielle Voraussetzung für eine widerstandsfähige Digitalisierung in Wirtschaft und Verwaltung. Unternehmen müssen sich vor Wirtschaftsspionage schützen können. Eine Schwächung der Verschlüsselungsverfahren könnte jedoch europäische Unternehmen im globalen Markt benachteiligen. Bürgerinnen und Bürger müssen auf eine sichere und integre Nutzung digitaler Verwaltungsleistungen vertrauen können und benötigen hierbei Schutz vor umfassender Überwachung und Datenmissbrauch. Auch die Ziele des Onlinezugangsgesetzes, Verwaltungsleistungen elektronisch über Verwaltungsportale anzubieten, würden konterkariert, wenn Nutzerinnen und Nutzer dieser Portale sich der Vertraulichkeit der elektronischen Kommunikation nicht sicher sein könnten.

Verschlüsselung ist ebenso ein zentrales Mittel für die Datenübermittlung in Drittländer gemäß den Empfehlungen zu ergänzenden Maßnahmen für Übertragungsinstrumente zur Gewährleistung des EU-Schutzniveaus des Europäischen Datenschutzausschusses als Reaktion auf das „Schrems II"-Urteil des Europäischen Gerichtshofs.

Würden die Vorschläge des Rates der Europäischen Union umgesetzt, würde eine sichere Ende-zu-Ende-Verschlüsselung untergraben und notwendiges Vertrauen zerstört, ohne dass das angestrebte Ziel, die Ermittlungsmöglichkeiten von Sicherheitsbehörden zu verbessern, nachhaltig und effektiv erreicht wird. Hintertüren in Verschlüsselungsverfahren stellen die Sicherheit und Wirksamkeit dieser gänzlich in Frage. Die Aushöhlung von Verschlüsselungslösungen würde zudem unweigerlich zu einem Ausweichen auf Umgehungstechniken führen, derer sich sowohl Kriminelle und Terroristen als auch technisch versierte Bürgerinnen und Bürger bedienen könnten. Gleichzeitig würde der Einsatz wirksamer Ende-zu-Ende-Verschlüsselung für technisch weniger versierte Bürgerinnen und Bürger faktisch unmöglich gemacht.

Aus gutem Grund hat sich die Bundesregierung bereits im Jahr 1999 in den Leitlinien deutscher Kryptopolitik zum Einsatz kryptographischer Verfahren bekannt. In Europa wird die Vertraulichkeit der Kommunikation durch das individuelle Recht auf Achtung der Kommunikation in Art. 7 GRCh geschützt. Ergänzend greift für gespeicherte Kommunikationsinhalte das in Art. 8 GRCh garantierte Recht auf Schutz personenbezogener Daten. In Deutschland wird der Grundrechtsschutz beim Einsatz von Kommunikationsdiensten durch das Fernmeldegeheimnis in Art. 10 GG und ergänzend durch das Recht auf informationelle Selbstbestimmung sowie das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme gewährleistet. Folgerichtig befürwortete die Bundesregierung im Jahr 2015 erneut den Einsatz von Kryptographie in der Charta zur Stärkung der vertrauenswürdigen Kommunikation.

Die Datenschutzkonferenz sieht keine Veranlassung, dass der Rat der Europäischen Union von diesen grundrechtswahrenden Positionen abweicht, zumal weitere, massiv in die Privatsphäre der Nutzerinnen und Nutzer eingreifende Befugnisse auch nicht erforderlich sind. Der effektive Kampf gegen Terror ist zwar ein legitimes Anliegen, aber den Sicherheitsbehörden stehen für die verfolgten Ziele bereits umfangreiche und sehr eingriffsintensive Instrumente zur Verfügung.

Die Datenschutzkonferenz hat sich wiederholt für den Einsatz sicherer und integrer Verschlüsselung eingesetzt und auf die Unverzichtbarkeit vertrauenswürdiger und integrer Kommunikationsmöglichkeiten hingewiesen. Sie fordert erneut die Bundesregierung und die deutsche EU-Ratspräsidentschaft auf, den Einsatz dem Stand der Technik entsprechender Verschlüsselungslösungen zu fördern und dem Bestreben, solche Lösungen zu schwächen, entschieden entgegenzutreten. Sichere Ende-zu-Ende-Verschlüsselung muss die Regel werden, um gerade im Zeitalter der Digitalisierung eine sichere, vertrauenswürdige und integre Kommunikation in Verwaltung, Wirtschaft, Zivilgesellschaft und Politik zu gewährleisten.

Anlage 6: Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 25. November 2020: Auskunftsverfahren für Sicherheitsbehörden und Nachrichtendienste verfassungskonform ausgestalten

Bei der Einrichtung des manuellen Auskunftsverfahrens von Bestandsdaten von Telekommunikationskunden hat der Gesetzgeber wichtige verfassungsrechtliche Vorgaben außer Acht gelassen. Die bisherigen Zugriffsbefugnisse der Sicher-

heitsbehörden sind zu weitreichend. Die Datenschutzaufsichtsbehörden des Bundes und der Länder haben bereits seit Jahren auf die Unverhältnismäßigkeit entsprechender Regelungen hingewiesen.

Mit Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 und 1 BvR 2618/13 – („Bestandsdatenauskunft II“) hat das Bundesverfassungsgericht erneut verfassungsrechtliche Vorgaben für die Ausgestaltung des manuellen Bestandsdatenauskunftsverfahrens gemacht. Das Gericht bekräftigte, dass sowohl die Übermittlung von Daten durch Telekommunikationsdiensteanbieter als auch der Abruf durch berechtigte Stellen jeweils einer verhältnismäßigen und normenklaren Rechtsgrundlage bedürfen. Die Übermittlungs- und Abrufregelungen müssen – so das Gericht – die Verwendungszwecke hinreichend begrenzen, mithin die Datenverwendung an bestimmte Zwecke, tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz binden (1. Leitsatz). Hierzu gehört, dass für den Einsatz zur Gefahrabwehr und die Tätigkeit der Nachrichtendienste grundsätzlich im Einzelfall eine konkrete Gefahr und für die Strafverfolgung ein Anfangsverdacht vorliegen müssen. Die Zuordnung dynamischer IP-Adressen muss darüber hinaus dem Schutz oder der Bewehrung von Rechtsgütern von hervorgehobenem Gewicht dienen (4. Leitsatz). Die Übermittlungsvorschrift des § 113 Telekommunikationsgesetz sowie eine Reihe mit ihm korrespondierender fachgesetzlicher Abrufregelungen wurden im Hinblick hierauf für mit dem Grundgesetz unvereinbar erklärt.

Zwar bleiben die bisherigen Vorschriften bis zur Neuregelung, längstens jedoch bis 31. Dezember 2021, nach Maßgabe der Entscheidungsgründe weiter anwendbar. Im Interesse der Rechtssicherheit appelliert die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) jedoch an die politisch Verantwortlichen, diese Frist nicht auszureizen, sondern das manuelle Auskunftsverfahren möglichst zeitnah verfassungskonform auszugestalten.

Die DSK hält es zudem für geboten, dass Bundes- und Landesgesetzgeber im Zuge der Umsetzung der Entscheidung nicht nur die unmittelbar von der Entscheidung betroffenen Vorschriften anpassen, sondern alle vergleichbaren Vorschriften, die Grundlage für die Übermittlung und den Abruf von personenbezogenen Daten sein können, im Lichte der Entscheidung des Bundesverfassungsgerichts überprüfen und gegebenenfalls verfassungskonform ausgestalten. Dies betrifft insbesondere Regelungen der Polizei- und Verfassungsschutzgesetze der Länder, die die Erteilung von Auskünften über Daten lediglich an die Erfüllung der Aufgaben der berechtigten Stelle knüpfen. Solche Regelungen sind mit der Gefahr unbegrenzter Verwendungen von Daten verbunden und damit unverhältnismäßig (vgl. BVerfG, o. g. Beschluss vom 27. Mai 2020, Rn. 154, 197). Datenabfragen dürfen nicht länger aufgrund derart unbestimmter Rechtsgrundlagen erfolgen.

Abkürzungsverzeichnis

ABl.	Amtsblatt der Europäischen Union
Abs.	Absatz
AfD	Alternative für Deutschland
App	Application, Anwendungsprogramm auf Smartphone
Art.	Artikel
BayDSG	Bayerisches Datenschutzgesetz
BayMBl.	Bayerisches Ministerialblatt
BeckOK	Beck'scher Online-Kommentar
BeckRS	Beck-Rechtsprechung
BDSG	Bundesdatenschutzgesetz
BGBl.	Bundesgesetzblatt
Buchst.	Buchstabe
CSU	Christlich-Soziale Union in Bayern
DNA	Desoxyribonuclein Acid, Träger der Erbinformation
DSFA	Datenschutzfolgenabschätzung
DSGVO	Datenschutz-Grundverordnung
EDV	Elektronische Datenverarbeitung
EU	Europäische Union
EuGH	Europäischer Gerichtshof
FDP	Freie Demokratische Partei
ff.	(nach)folgende
GVBl.	Bayerisches Gesetz- und Verordnungsblatt
https	Hyper Text Transfer Protocol Secure
IP	Internet Protocol
IT	Informationstechnik
lit.	Buchstabe
MdL	Mitglied des Landtages
m. w. N.	mit weiteren Nachweisen
Nr.	Nummer
PC	Personalcomputer
RLDSJ	Datenschutz-Richtlinie für Polizei und Strafjustiz
Rn.	Randnummer
sog.	sogenannt
SPD	Sozialdemokratische Partei Deutschlands
SSL	Secure Socket Layer
u. a.	unter anderem/und andere
UAbs.	Unterabsatz
vgl.	vergleiche
www	World Wide Web
z. B.	zum Beispiel

Stichwortverzeichnis