33. Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz

gemäß Art. 59 Datenschutz-Grundverordnung

Berichtszeitraum: 1. Januar 2023 bis 31. Dezember 2023

Impressum

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

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

Inhaltsverzeichnis

Hinweis zu Abkürzungen

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

BayDSG	Bayerisches Datenschutzgesetz vom 15. Mai 2018 (GVBl. S.230), zuletzt geändert durch § 1 Abs. 26 Verordnung vom 4. Juni 2024 (GVBl. S. 98)
DSGVO	Datenschutz-Grundverordnung; die vollständige Bezeichnung lautet: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. L 119 vom 4. Mai 2016, S. 1, berichtigt ABl. L 314 vom 22. November 2016, S. 72, ABl. L 127 vom 23. Mai 2018, S. 2, und ABl. L 74 vom 4. März 2021, S. 35)
RLDSJ	Datenschutz-Richtlinie für Polizei und Strafjustiz; die vollständige Bezeichnung lautet: Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4. Mai 2016, S. 89, berichtigt ABl. L 127 vom 23. Mai 2018, S. 9, und ABl. L 74 vom 4. März 2021, S. 36)

1 Überblick

1.1 Digitalisierung und Datenschutz gehören zusammen wie zwei Seiten einer Medaille

Im Dezember 2018 veröffentlichte ein Hacker namens „Orbit“ in einer Art „Adventskalender“ bei Twitter täglich neue Daten über Politiker, Journalisten und anderen Prominente. Der Kalender enthielt Telefonnummern, Adressen, teilweise auch Ausweiskopien und private Fotos. Die Veröffentlichungen hatten erhebliche Auswirkungen auf die betroffenen Personen, insbesondere Politikerinnen und Politiker, die vielfachen Hetz- und Drohanrufen ausgesetzt waren. Nach Einschätzung der Strafverfolgungsbehörden hatte der später gefasste Täter keine besonderen technischen Fähigkeiten, sondern gelangte vor allem mit Fleiß und Ausprobieren an die personenbezogenen Daten seiner Opfer.[1]

Auch wenn „Orbit“ gefasst und gerichtlich verurteilt wurde, ist der Fall nach wie vor aktuell, wie zahlreiche Fälle externer Angriffe auf IT-Systeme bayerischer öffentlicher Stellen unterstreichen, von denen ich insbesondere durch Meldungen nach Art. 33 DSGVO erfahren habe. Der Fall zeigt: Digitalisierung geht nicht ohne ein Mindestmaß an Datenschutz. Gemeint sind damit allerdings nicht nur allgemeine Vorgaben der IT-Sicherheit, sondern auch der Schutz von Informationen über natürliche Personen.

Digitalisierungsdebatten sind gegenwärtig häufig von der Zielvorstellung „Datenschätze heben“ geprägt. Datenschutz und Datensicherheit werden mitunter als Innovationsbremsen wahrgenommen. Dabei schwingt die Wertung mit, dass die einschlägigen Anforderungen rigide zurückgeschnitten werden sollten, um endlich einer ungehemmten Nutzung auch personenbezogener Daten den Weg zu bahnen.

Aus datenschutzrechtlicher Sicht halte ich Ansätze dieser Art in vielerlei Hinsicht für problematisch. Bevor ich in den nachfolgenden Kapiteln über einzelne Bereiche meiner Tätigkeit berichten werde, möchte ich deshalb zunächst an einige zentrale datenschutzrechtliche Rahmenbedingungen der Digitalisierung erinnern:

1.1.1 Datenschutz ist nicht frei verfügbar

Wünsche nach dem Rückbau „lästiger“ Datenschutzbestimmungen übergehen allzu oft den Umstand, dass Datenschutz grundrechtlich fundiert und in der Verfassung des Freistaats Bayern, im Grundgesetz und in der Charta der Grundrechte der Europäischen Union fest verankert ist. Das nationale Grundrecht auf informationelle Selbstbestimmung ist ebenso wie das europäische Datenschutzgrundrecht ein integraler Bestandteil des (grund)rechtsstaatlichen Freiheitsversprechens. Sowohl im Hinblick auf öffentliche Interessen als auch im Hinblick auf öko-

[1] Vgl. etwa den Bericht „Bewährungsstrafe für jugendlichen Hacker wegen Ausspähens von Promidaten“ auf beck-aktuell, https://rsw.beck.de/aktuell/daily/meldung/detail/ag-alsfeld-bewaehrungsstrafe-fuer-jugendlichen-hacker-wegen-ausspaehens-von-promidaten.

nomische Interessen dürfen diese Grundrechte nicht beliebig, sondern nur entlang der verfassungsrechtlichen Vorgaben eingeschränkt werden. Dem dienen zuvorderst die Datenschutz-Grundverordnung und zahlreiche Datenschutzvorschriften des mitgliedstaatlichen Rechts. Der Gesetzgeber kann insbesondere die Verarbeitung personenbezogener Daten zu Gemeinwohlzwecken (nur) im Rahmen der Verhältnismäßigkeit gestatten. Die Grundrechte strukturieren ein Konzept der Digitalisierung und Datennutzung, bei dem das Individuum im Mittelpunkt steht – als mündige Bürgerin oder mündiger Bürger, die oder der souverän über die Verwendung der eigenen Daten entscheidet.

Und ja: Es gibt personenbezogene Daten, die einen Menschenwürdebezug haben und deshalb nach unserem Verfassungsrecht unantastbar sind. Solche personenbezogenen Daten darf selbst der Gesetzgeber nicht ohne oder gar gegen den Willen der betroffenen Personen für Verarbeitungen freigeben.

1.1.2 Paradigmenwechsel von der datenschutzrechtlichen Einwilligung zum Widerspruchsmodell

Was die datenschutzrechtliche Gestaltung digitalisierter Datennutzungen betrifft, ist gegenwärtig ein Paradigmenwechsel zu beobachten: Während bislang oft betroffene Personen mit ihren Einwilligungen Datennutzungen legitimierten, werden zunehmend „Widerspruchslösungen“ etabliert. Dabei erscheint die digitalisierte Datennutzung als „Normalfall“; von einer betroffenen Person, die etwas anderes möchte, wird „Aktivwerden“ erwartet. Die Begründung lautet meist, man wolle den bürokratischen Aufwand durch Einwilligungen vermeiden und damit – bei den Verantwortlichen – auch Kosten senken. Teilweise wird ohne näheren Nachweis behauptet, ohne solche „Widerspruchslösungen“ sei Digitalisierung nicht möglich.

Tatsächlich bedeutet der Paradigmenwechsel vom Einwilligungs- zum Widerspruchsmodell: Gerade als Patientin oder Patient, als Verbraucherin oder Verbraucher kann sich eine betroffene Person künftig bei digitalisierten Datennutzungen immer weniger darauf verlassen, noch gefragt zu werden – selbst wenn es um hochsensible Daten geht. Sie wird immer häufiger selbst die Initiative ergreifen müssen, um von einer ihr unerwünschten Verarbeitung personenbezogener Daten überhaupt zu erfahren und sie dann zu unterbinden. In manchen Fallkonstellationen mag ein solches Widerspruchsmodell sachgerecht sein, bei einem generellen Paradigmenwechsel droht aber eine Entwertung der Datenschutzgrundrechte. Das ist insbesondere dann problematisch, wenn ein Gesetzgeber legitime individuelle Vertraulichkeitsinteressen nicht angemessen berücksichtigt.

So befindet sich auf Unionsebene das Gesetzgebungsverfahren für eine Verordnung des Europäischen Parlaments und des Rates über den Europäischen Raum für Gesundheitsdaten (EHDS-Verordnung) in einem vorgerückten Stadium.[2] Die Regelung wird voraussichtlich das traditionsreiche Patientengeheimnis zugunsten der Sekundärnutzung von Gesundheitsdaten außerhalb des Behandlungsverhältnisses infrage stellen. Patientinnen und Patienten sollen künftig nicht mehr um ihre Einwilligung gefragt werden müssen, wenn es um die pseudonymisierte Sekundärnutzung ihrer Gesundheitsdaten geht. Selbst bei psychotherapeutischen Behandlungen könnten Behandlungsdaten beispielsweise auch für die Weiterent-

[2] Verfahrensstand und Materialien: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2022/0140(COD)&l=en.

wicklung von kommerziellen Gesundheitsdienstleistungen oder Medizinprodukten genutzt werden dürfen. Patientinnen und Patienten bliebe nur noch die Möglichkeit, gegen eine solche Nutzung zu intervenieren. Viele werden den Aufwand scheuen, auch aus der Befürchtung, ein Vertrauensverhältnis zur Behandlerin oder zum Behandler könnte Schaden nehmen. Bereits heute weisen Patientinnen und Patienten in Eingaben bei mir nicht selten darauf hin, dass sie beim Gebrauch von Datenschutzrechten im medizinischen Bereich Nachteile bei der Versorgungsqualität befürchten.

Nach meinen Eindrücken aus dem Gesetzgebungsverfahren hat sich die Bundesregierung nicht mit dem gebotenen Nachdruck für eine grundrechtsfreundlichere Lösung eingesetzt, obwohl solche Lösungen durchaus diskutiert wurden und hierfür auch eine geeignete IT-Unterstützung bereitstünde. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat bereits mit ihrer Stellungnahme vom 27. März 2023 auf das Problemfeld aufmerksam gemacht (ohne Hervorhebungen des Originaltextes):

Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 27. März 2023

Nutzung von Gesundheitsdaten braucht Vertrauen
Der Europäische Gesundheitsdatenraum darf das Datenschutzniveau der Datenschutz-Grundverordnung nicht aushöhlen

Die betroffenen Personen müssen darauf vertrauen dürfen, dass bei der Verarbeitung ihrer personenbezogenen Daten die Regelungen der europäischen Datenschutz- Grundverordnung (DS-GVO) und ihre Grundrechte nach Artikel 7, 8 der Charta der Grundrechte der Europäischen Union (GRCh) gewahrt bleiben, wie von der EU-Kommission in der Datenstrategie aus dem Jahr 2020[1] ausdrücklich zugesagt.

Auf Grundlage dieser Datenstrategie hat die EU-Kommission bisher mehrere Datengesetze initiiert, um zum gesamtgesellschaftlichen Vorteil einen Binnenmarkt für Daten zu schaffen. Zu einem ersten sektorenspezifischen Datenraum hat sie im Mai 2022 einen Verordnungsentwurf (EHDS-VO-E[2]) zur Schaffung und Regulierung eines Europäischen Gesundheitsdatenraums (European Health Data Space – EHDS) vorgestellt.

Der Entwurf der EHDS-Verordnung enthält Regelungen zur europaweiten Primärnutzung der elektronischen Gesundheitsdaten, um bei Gesundheitsversorgung auch auf Informationen aus den Systemen der anderen Mitgliedsstaaten zugreifen zu können. Von wesentlicher Bedeutung ist darüber hinaus die Regulierung der Sekundärnutzung von elektronischen Gesundheitsdaten, vor allem für Zwecke der Forschung, die u. a. eine zentrale Zugangsstelle vorsieht, die den Zugang zu den elektronischen Gesundheitsdaten vermittelt.

Diese Regelungen dürften als Blaupause für weitere Datenräume im Europäischen Raum dienen. Neben der Tatsache, dass im EHDS besonders sensible Daten verarbeitet werden, unterstreicht diese „Vorreiterrolle" die besondere Bedeutung der EHDS-VO.

Für die Errichtung des EHDS ist das Grundrecht auf Datenschutz bzw. auf informationelle Selbstbestimmung u. a. mit dem öffentlichen Interesse an wissenschaftlicher Forschung in einen angemessenen Ausgleich zu bringen.[3] Hier greift der Verordnungsentwurf allerdings deutlich zu kurz.

A. Grundsätzliche Erwägungen

Betroffenenrechte

Die DSK begrüßt das Regulierungsvorhaben, soweit es die Rechte der betroffenen Patientinnen und Patienten bei der Primärnutzung von elektronischen Gesundheitsdaten – insbesondere die Portabilität – aufwertet. Sie erkennt an, dass für die grenzüberschreitende Behandlung, für Forschungszwecke sowie für öffentliche Zwecke von hoher Bedeutung Datenzugangsrechte geschaffen werden sollen. Gleichzeitig gilt insbesondere im Rahmen der Sekundärnutzung: Der Mensch muss erkennbar im Mittelpunkt stehen. Daraus folgt, dass diejenigen, deren personenbezogene Daten den wissenschaftlichen und wirtschaftlichen Mehrwerten zugrunde liegen, eingebunden sein und ihre Rechte aus der DS-GVO auf einfache Weise und granular realisieren können müssen. Ausschlüsse oder Beschränkungen von Betroffenenrechten müssen mit den Grundrechten vereinbar sein. Die Betroffenenrechte der DS-GVO dürfen nicht verkürzt werden.

Die betroffenen Personen müssen eine effektive Kontrolle über die Verarbeitung ihrer personenbezogenen Daten behalten. Hierfür sind präzise und leicht verständliche Informationen der Verantwortlichen elementar. Sämtliche Übermittlungswege und Verarbeitungsprozesse müssen für die Betroffenen transparent sein.

Rechtsklare Regelungen

Es bedarf rechtsklarer Regelungen, die erkennen lassen, ob und in welchem Umfang die Verarbeitung personenbezogener Daten umfasst und zulässig ist. Die Regelungen müssen konform mit den Grundrechten sein, wonach wesentliche Festlegungen, insbesondere zu Umfang, Art und Zwecken der Datenverarbeitungen, in der Verordnung selbst zu treffen sind.

Technische und organisatorische Maßnahmen

Die Verarbeitung der Gesundheitsdaten unterliegt nach der DS-GVO einem hohen Schutzbedarf, der in den technischen und organisatorischen Maßnahmen umzusetzen ist. Dazu gehören auch die Ende-zu-Ende-Verschlüsselung, die Pseudonymisierung bzw. die Anonymisierung sowie ein wirksames Löschkonzept.

Der EHDS-VO-E lässt bisher jedoch offen, wie die Daten anonymisiert werden können. Eine rechtsklare Regelung der Anforderungen an Methoden und Wirkungen der Anonymisierung könnte die rechtssichere Datennutzung unterstützen.

Die betroffenen Personen haben ein Recht auf sichere und vertrauliche Verarbeitung ihrer Gesundheitsdaten. Da sich bei der Verarbeitung von Gesundheitsdaten Risiken nicht gänzlich ausschließen lassen, sind geeignete Garantien mit Transparenz und durch Anwendung von Methoden im Sinne von „Data Protection by Design“ und „Data Protection by Default“ vorzusehen. Beispielsweise muss es den betroffenen Personen mittels digitaler Management-Systeme möglich sein, ihre

elektronischen Gesundheitsdaten auch im EHDS unter angemessenen technischen und rechtlichen Bedingungen kontrollieren zu können.

B. Verhältnis zu anderen Rechtsakten, Begriffe und Datenkategorien

Gewährleistung des DS-GVO-Schutzniveaus

Die Vorgaben der DS-GVO zu Datenschutz und Datensicherheit dürfen durch die EHDS-VO nicht ausgehöhlt werden; sie sind Grundlage für das Vertrauen der betroffenen Personen. Die datenschutzrechtlichen Grundsätze, wie der Grundsatz der Datenminimierung, der Datenrichtigkeit, der Speicherbegrenzung, der Integrität und Vertraulichkeit und das Erforderlichkeitsprinzip müssen gewährleistet werden. Es ist klarzustellen, dass die EHDS-VO-E den Rechtsrahmen der DS-GVO respektiert, die dort vorgesehenen Regelungsräume also nutzt, aber nicht das Schutzniveau unterläuft.

Gerade bei besonders schützenswerten Gesundheitsdaten dürfen die grundrechtlich garantierten und in der DS-GVO vorgesehenen Betroffenenrechte nicht entwertet werden. Dies gilt auch für die Sekundärnutzung von elektronischen Gesundheitsdaten; hier ist bisher nicht erkennbar, ob und, wenn ja, inwieweit nach dem Regelungsentwurf den Betroffenen überhaupt Rechte zustehen sollen.

Verhältnis zu weiteren Rechtsakten

Zudem muss sich die EHDS-VO hinsichtlich der Begriffe und Definitionen sowie des Anwendungsbereichs kohärent und konsistent in das Regelungssystem der weiteren Rechtsakte wie des Data Governance Act, des Data Act und des Artificial Intelligence Act einfügen.

Im Bezug zur JI-Richtlinie[4] wird an die Problematik erinnert, die bei elektronischen Datensammlungen entsteht. Insbesondere dürfen den Strafverfolgungsbehörden durch die EHDS-VO keine Zugriffsrechte auf gesundheitsbezogene Daten ermöglicht werden. Dies ist durch eine klare Zweckbindungsregelung sicherzustellen.

Datenkategorien

Außerdem müssen die in Artikel 33 EHDS-VO-E genannten Datenkategorien begrenzt werden: Da die EHDS-Verordnung ermöglichen soll, elektronische Gesundheitsdaten für die Förderung der individuellen Gesundheit und der öffentlichen Gesundheit, insbesondere im Rahmen von Forschungsvorhaben, bereitzustellen, sollten auch nur hierfür geeignete personenbezogene Daten vom Anwendungsbereich der Verordnung umfasst sein. Die Datensätze insbesondere aus Wellness-Anwendungen sind aus dem Anwendungsbereich der EHDS-VO zu entfernen, da der Erkenntnisgewinn unklar bleibt. Diese Daten bieten voraussichtlich nicht die erforderliche Richtigkeitsgewähr und Qualität und können zugleich mit einer hohen Eingriffsintensität hinsichtlich des Verhaltens der betroffenen Personen verbunden sein. Die Aufnahme von Daten zu gesundheitsrelevanten Faktoren, einschließlich sozialer, umweltbedingter und verhaltensbezogener Gesundheitsfaktoren, Lebensstil, Wohlbefinden und Verhaltensdaten, ist ebenfalls kritisch zu sehen. Ihre Verarbeitung sollte nur für näher zu bestimmende Zwecke zugelassen werden. Die Regelung zur Bereitstellung von persönlichen Genomdaten greift in den intimsten Bereich der betroffenen Personen und ihrer Angehörigen ein und ist daher von Grundrechts wegen zu streichen.

C. Datenverarbeitung zum Primärzweck und Electronic Health Record (EHR)-Systeme

Primärzweck: Behandlung

Die Patientensouveränität darf durch die neuen europaweiten Regelungen nicht eingeschränkt werden. Die Datenverarbeitung für den Primärzweck, also der medizinischen Behandlung, ist nur mit der effektiven Kontrollmöglichkeit und einer aktiven Mitwirkung der betroffenen Personen, also der Patientinnen und Patienten zulässig. Es muss sichergestellt sein, dass sie über Verarbeitungsvorgänge und insbesondere – zur Wahrung des Patientengeheimnisses – über Übermittlungen an andere verantwortliche Stellen informiert und damit einverstanden sind.

EHR-Systeme

Electronic Health Record-Systeme (EHR-Systeme), d. h. Geräte oder Software, die vom Hersteller dazu bestimmt sind, elektronische Patientenakten zu speichern, zu vermitteln, zu importieren, zu exportieren, zu konvertieren, zu bearbeiten oder anzuzeigen, müssen von einer unabhängigen Stelle unter Beteiligung der Datenschutz-Aufsichtsbehörden zugelassen werden, bevor sie in Betrieb genommen werden, damit die nötigen hohen Anforderungen an die Sicherheit und die Ausgestaltung der Datenverarbeitung erfüllt sind. Sie müssen eine sichere Ende-zu-Ende-Verschlüsselung gewährleisten und Anonymisierungs- und Pseudonymisierungskomponenten enthalten. Technische und organisatorische Maßnahmen, wie die Authentifizierung, müssen ein hohes Sicherheitsniveau gewährleisten. Das Management des EHR-Systems muss effektiv und granular ausgestaltet sein und auch solchen betroffenen Personen zur Verfügung stehen, die keine vertieften Digitalkenntnisse oder keine mobilen Endgeräte haben. Insbesondere müssen die Patientinnen und Patienten Nutzungsbeschränkungen und Berechtigungen auf leichte Art und barrierefrei einrichten können.

Die Zugriffsstrukturen im EHR-System haben dem bei Gesundheitsdaten vermuteten hohen Risiko für die Rechte und Freiheiten natürlicher Personen Rechnung zu tragen, sodass das Risiko eines Missbrauchs, insbesondere mit zeitlich beschränkbaren Zugangsrechten je nach Erforderlichkeit kontinuierlich minimiert wird. Der Zugriff im Notfall muss auf einen definierten, strukturierten und begrenzten Datensatz erfolgen, um wirksam zu sein. Um den Zugriffschutz des restlichen EHR-Systems nicht zu unterlaufen, muss der Notfalldatensatz technisch getrennt vorgehalten werden.

D. Datenverarbeitung zu weiteren Zwecken (Sekundärnutzung)

Paradigmenwechsel und Patientensouveränität

Der EHDS-VO-E bedingt einen Wechsel der relevanten Grundlage für die Sekundärnutzung von erheblicher Tragweite. Es werden umfangreiche gesetzliche Nutzungsrechte vorgesehen, die in die Rechte der Betroffenen eingreifen. Um den Kernbereich der Grundrechte zu gewährleisten, sind daher die Betroffenen in geeigneter Weise einzubinden, auch dann, wenn auf eine aus datenschutzrechtlicher Sicht vorzuziehende Zustimmung (Opt-in) verzichtet wird, z. B. indem zumindest ein niederschwelliges Widerspruchsrecht (Opt-out) vorgesehen wird. Zur Verwaltung von Widerspruch oder Zustimmung zu bestimmten Datenverarbeitungen oder Zwecken sollten digitale Managementsysteme verwendet werden.[5]

Außerdem müssen zu den in Artikel 34 EHDS-VO-E genannten Zwecken entsprechende Garantien und Bedingungen im Sinne von Artikel 9 Abs. 2 DS-GVO festgelegt werden. Der Grundsatz der Verhältnismäßigkeit erfordert, dass, je sensibler persönliche Daten sind, umso strenger auch die Anforderungen an deren Verarbeitung sein müssen.

Der Zielsetzung des EHDS als Förderungsinstrument für die wissenschaftliche Forschung und die öffentlichen Interessen entsprechend muss die sekundäre Datennutzung stets dem Allgemeinwohlinteresse dienen. Die im EHDS-VO-E ausgewiesenen Zwecke müssen im Einklang mit den Vorgaben der DS-GVO für besonders zu schützende Daten stehen und durch entsprechende Garantien flankiert werden. Insbesondere muss die sachgerechte Prüfung der Anträge auf zulässige Zwecke und den erforderlichen Datenumfang sichergestellt sein; eine automatische Zulassung einer Datennutzung nach Ablauf der Antragsbearbeitungsfrist ist unzulässig.

Einwilligungsbasierte neben gesetzlich geregelter Forschung

Einwilligungsbasierte Forschung wie in klinischen Studien muss unabhängig von der EHDS-Verordnung bestehen bleiben. Die freiwillige datenschutzrechtliche Einwilligung als Grundlage für die Datennutzung kann dem hohen Gut des Rechts auf informationelle Selbstbestimmung unmittelbar Ausdruck verleihen.

Spezifische Dateninhaber

Der Begriff des Dateninhabers muss klargestellt und begrenzt werden. Dabei sind auch die Rechtsverhältnisse der Dateninhaber mit den jeweiligen betroffenen Personen und die sich aus entsprechenden Vertrauensverhältnissen ergebenden Schweigepflichten wie Arztgeheimnis, Berufsgeheimnis, Sozialgeheimnis, aber auch Geschäftsgeheimnisse zu berücksichtigen.

Dateninfrastruktur und Zugangsstelle für elektronische Gesundheitsdaten

Die Datenverarbeitungen in der Dateninfrastruktur und bei der Zugangsstelle für die elektronischen Gesundheitsdaten müssen den technischen und organisatorischen Maßgaben der DS-GVO entsprechend ein hohes Sicherheitsniveau umsetzen. Die Aufgaben und die Verfahren bei der Zugangsstelle müssen so konzipiert sein, dass insbesondere die Grundsätze der Datenminimierung und Erforderlichkeit gewahrt werden und die noch einzuräumenden Betroffenenrechte barrierefrei ausgeübt werden können. Die Aufgaben sollten daher auf verschiedene Verantwortliche aufgeteilt werden. So müssen unabhängige Vertrauensstellen die Aufgabe der Pseudonymisierung übernehmen, während die Zugangsstellen die Koordinierung und Verwaltung der Dateninfrastruktur und die Bearbeitung der Antragsverfahren übernehmen. Für die Bereitstellung der Daten in einer sicheren Verarbeitungsumgebung können auch unabhängige Treuhandplattformen eingerichtet werden.

Dabei sind die datenschutzrechtlichen Verantwortlichkeiten aller beteiligten Stellen lückenlos festzulegen, damit betroffene Personen ihre Datenschutzrechte wirksam ausüben können.

Die im Entwurf der Kommission vorgesehene zentrale Zusammenführung von Klardaten, also von Datensätzen mit identifizierenden Angaben, bei der Zugangs-

stelle birgt hohe Risiken und ist unzulässig. Die Daten sind vor der anlassbezogenen und temporären Zusammenführung zu pseudonymisieren oder zu anonymisieren.[6]

[1] *Europäische Kommission, Mitteilung COM(2020) 66: „Eine europäische Datenstrategie" vom 19. Februar 2020.*
[2] *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen europäischen Raum für Gesundheitsdaten vom 3. Mai 2022 (2022/0140).*
[3] *Vgl. hierzu auch: EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space vom 12. Juli 2022.*
[4] *Richtlinie EU 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016.*
[5] *Petersberger Erklärung der DSK zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung vom 24.11.2022, S. 7.*
[6] *Vgl. Seite 3 Ziffer 3 Satz 1 der Petersberger Erklärung der DSK zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung vom 24.11.2022.*

Nach Artikel 8 Abs. 2 Satz 1 Charta der Grundrechte der Europäischen Union dürfen personenbezogene Daten nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Nach diesem grundrechtlichen Konzept bringt die Einwilligung die informationelle Selbstbestimmung der betroffenen Person unmittelbar zur Geltung. Der Gesetzgeber kann andere Lösungen nur entwickeln, wenn er dabei das informationelle Selbstbestimmungsrecht der betroffenen Personen angemessen berücksichtigt. Personenbezogene Daten sind nicht frei verfügbar.

1.1.3 Datenschutz fördert und fordert Digitalisierung

An einer konsequenten Umsetzung datenschutzrechtlicher Vorgaben durch den Gesetzgeber und die Verwaltung führt aus grundrechtlicher Sicht kein Weg vorbei.

Eine durchdachte Implementierung von Datenschutz setzt gerade im Bereich der technisch-organisatorischen Maßnahmen voraus, dass die verantwortlichen Stellen bereits bei der Planung von Digitalisierungsvorhaben prüfen, wie sich Nutzerfreundlichkeit und Vertrauenswürdigkeit von digitalen Verwaltungsdienstleistungen verbinden lassen. Als Datenschutz-Aufsichtsbehörde verkenne ich nicht, dass guter Datenschutz eine Herausforderung bei der Digitalisierung ist. Der verbundene Aufwand lohnt aber. Nutzerinnen und Nutzer werden viel eher bereit sein, sich auf digitale Angebote öffentlicher Stellen einzulassen, wenn sie sicher sein können, dass ihre Daten dort in guten Händen sind und nicht irgendwann auf irgendeine Weise zu ihrem Nachteil verwendet werden.

Ohne die in der Datenschutz-Grundverordnung verankerten zentralen Datenschutzgrundsätze insbesondere der Rechtmäßigkeit, Transparenz, Zweckbindung, Integrität und Vertraulichkeit werden Digitalisierungsvorhaben auf nur wenig **Akzeptanz bei den Bürgerinnen und Bürgern** treffen. Zudem hat der öffentliche Sektor bei der Digitalisierung eine besondere Vorbildfunktion und steht deshalb mehr „unter Beobachtung" als manche Unternehmen. Die viel beschworene „Datensouveränität" der Menschen setzt voraus, dass sie sich im Verhältnis zur öffentlichen Hand stets als Subjekt fühlen können. Besonders vulnerable Bevölkerungsgruppen müssen zudem auch weiterhin einen besonders starken Schutz genießen.

1.2 Künstliche Intelligenz: Sind wir vorbereitet?

1.2.1 Was ist Künstliche Intelligenz (KI)?

Vereinfacht ausgedrückt meint KI eine Technik, die es Maschinen ermöglicht, ähnlich wie Menschen zu lernen und zu „denken". Bei KI-Systemen, die mit Verfahren des maschinellen Lernens arbeiten, geben Entwicklerinnen und Entwickler nur bestimmte Rahmenbedingungen vor, zum Beispiel eine konkrete Aufgabe. Das KI-System ermittelt daraufhin selbständig eine Lösung. Allerdings sind KI-Anwendungen auf unzählige Daten angewiesen, um daraus ihre Vorgehensweise abzuleiten.

Die sogenannte „schwache" KI ist längst im Alltag angekommen. Typische Internetfunktionalitäten wie etwa die Autokorrektur, personalisierte Empfehlungssysteme und Übersetzungsprogramme werden mittlerweile regelmäßig zumindest von KI-Anwendungen unterstützt. Auch Spam-Filter und sonstige Maßnahmen der IT-Sicherheit beruhen heute zum Teil auf KI-Methoden.

Im Berichtszeitraum hat auch die bayerische öffentliche Verwaltung zunehmend die **textgenerierende Künstliche Intelligenz** in den Blick genommen. So können Chatbots menschenähnliche Konversationen führen und sollen deshalb eingesetzt werden, um Bürgeranfragen in natürlicher, verständlicher Sprache zu beantworten. Dafür greifen Chatbots auf umfangreiche Textdatenbanken zu.

Von öffentlichen Stellen wohl noch nicht ganz so häufig genutzt wird bislang die **bildgenerierende KI**. Sie kann beispielsweise aus Textbeschreibungen Bilder, Grafiken oder Illustrationen erzeugen. Durch die Medienberichterstattung weithin bekannt geworden sind beispielsweise KI-generierte Abbildungen des Papstes in ungewohnten Rollen.

1.2.2 Künstliche Intelligenz: Viele Vorteile, aber auch Risiken

Der Einsatz von KI an sich ist wertneutral. KI-Technologien sind Werkzeuge, deren Auswirkungen davon abhängen, wie sie verwendet werden. Mit dem Einsatz von KI im Bereich der öffentlichen Verwaltung können vielfältige Vorteile und Chancen verbunden sein, etwa in der medizinischen Diagnostik oder bei der Unterstützung des individuellen Lernens in der Schule.

Nicht verkannt werden darf allerdings, dass der Einsatz neuer Technologien wie KI auch risikobehaftet ist und bei vielen Menschen zu Ängsten führt. Auf sehr abstrakter Ebene begründet der Einsatz von KI die Furcht vor einem Kontrollverlust, weil Maschinen den Menschen als Arbeitskraft überflüssig machen könnten. Eine Studie der Universität Oxford prognostiziert sogar das Risiko, eine künftige Generation der KI-Technologie könne imstande sein, die Menschheit auszurotten.[3]

Ohne dass ich diese Sorgen bewerten oder gar bagatellisieren will, erscheint mir aus datenschutzrechtlicher Sicht vor allem der Umstand als bedeutsam, dass KI-Systeme **unsere Wahrnehmung von Inhalten** und damit auch die Grundlage un-

[3] Cohen/Hutter/Osborne, Advanced artificial agents intervene in the provision of award, AI Magazine, Volume 43, Issue 3, September 2022, S. 282 ff.

serer **Meinungsbildung beeinflussen können**. Werden KI-Modelle mit fehlerhaften Trainings- und Testdaten trainiert, welche die Realität verzerrt wiedergeben („Bias"), wirkt sich dies auch auf die weitere Datenverarbeitung der KI-Modelle aus. KI-Modelle greifen dann auf erlernte Vorurteile zurück und leiten daraus diskriminierende Entscheidungsvorschläge ab. Überdies erzeugen text- und bildgenerierende KI-Systeme auch personenbezogene Daten, die nicht notwendig „richtig" sein müssen. Stimmen, Sprache, Bilder werden so nachgestellt, dass bisweilen selbst Expertinnen oder Experten auf dem ersten Blick getäuscht werden. Das Erscheinungsbild von Nachrichten kann mittlerweile so realistisch nachgeformt werden, dass News und Fake News kaum noch voneinander zu unterscheiden sind. KI ist zudem „kreativ" in dem Sinne, dass sie auf der Grundlage der von ihr rezipierten Datenquellen neue, eigene Inhalte schafft. Die Folge ist: Wer Suchmaschinen nutzt, wird mittelfristig zunehmend auf Inhalte stoßen, die KI-generiert sind.

Öffentliche Stellen sollten vor diesem Hintergrund noch sensibler mit personenbezogenen Daten umgehen. Soweit sie aus öffentlichen Quellen Informationen erheben, die auch personenbezogene Daten enthalten, steigt die Wahrscheinlichkeit, dass diese Informationen KI-generiert sind.

Setzen öffentliche Stellen ihrerseits KI-Systeme ein, müssen sie sicherstellen, dass dies innerhalb klarer Leitlinien erfolgt. Dazu gehört unter anderem ein hohes Maß an Transparenz und menschlicher Kontrolle. Namentlich beim Einsatz von bild- und textgenerierenden KI-Systemen gilt der Grundsatz „Human-in-the-Loop", also der **menschlichen Endkontrolle**, ob der jeweils KI-generierte Text sachlich richtig, rechtskonform und nichtdiskriminierend ist. Die datenschutzrechtliche Verantwortung verbleibt bei der öffentlichen Stelle, die das KI-System für eigene Zwecke nutzt.

1.2.3 KI-Verordnung: Wesentliche Inhalte

Bereits in meinem 32. Tätigkeitsbericht 2022 habe ich über die Diskussion zu einem europäischen Gesetz über Künstliche Intelligenz informiert (Nr. 1.1.1.4). Die KI-Verordnung[4] ist nach dem Berichtszeitraum in Kraft getreten, gilt aber noch nicht.

Die Einigung enthält unter anderem Vorschriften für KI-Systeme, die einem allgemeinen Verwendungszweck dienen und künftig systemische Risiken erzeugen können. Dazu stellt die Verordnung einen Governance-Rahmen zur Verfügung. Strafverfolgungsbehörden soll es nur im engen Rahmen erlaubt sein, im öffentlichen Raum KI-basierte biometrische Fernidentifizierungen einzusetzen. Betreiber von KI-Systemen werden verpflichtet, vor deren Inbetriebnahme eine Folgenabschätzung in Bezug auf die Grundrechte durchzuführen.

Soweit KI-Systeme personenbezogene Daten verarbeiten, gilt grundsätzlich die Datenschutz-Grundverordnung. Im Berichtszeitraum ist eine Entscheidung des

[4] Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L 2024/1689 vom 12. Juli 2024).

Europäischen Gerichtshofs zur Auslegung der automatisierten Einzelfallentscheidung nach Artikel 22 DSGVO ergangen, die im Zusammenhang mit dem Einsatz von KI-Systemen besonders relevant sein dürfte. Danach ist der Begriff der „automatisierten Entscheidung im Einzelfall" weit auszulegen. Sogar eine automatisiert erstellte Bewertung (Scorewert) kann hierfür genügen, wenn das Handeln des verantwortlichen Entscheiders maßgeblich von ihr geleitet wird.[5] Insbesondere sofern KI-Systeme zur Vorbereitung von Verwaltungsentscheidungen eingesetzt werden sollen, ist damit Art. 22 DSGVO besonders in den Blick zu nehmen.

Bei der Umsetzung der KI-Verordnung wird es zunächst darauf ankommen, dass die verantwortlichen Stellen einerseits die Risiken von KI-basierter Datenverarbeitung einhegen, andererseits die effektive Nutzung der Chancen gewährleistet bleibt, die mit einem Einsatz von KI-Systemen zu legitimen Zielen verbunden sind. Diesen Maßstab werde ich auch meiner künftigen Datenschutzaufsicht über KI-Systeme zugrunde legen.

1.3 Über diesen Tätigkeitsbericht

Der jährliche Tätigkeitsbericht steht in einem engen Verbund mit meinen rein digitalen **Veröffentlichungen**, darunter im Berichtsjahr zwei „große", in Bayern und über die Landesgrenzen hinaus rezipierte Orientierungshilfen (Beitrag Nr. 2.1). Schwerpunkte des Tätigkeitsberichts bilden traditionell die Beratung in Gesetzgebungsverfahren, Beiträge zu Anfragen bayerischer öffentlicher Stellen sowie Erkenntnisse, die ich bei der Bearbeitung von Bürgereingaben gewinnen konnte. Dabei gilt nicht der Grundsatz „ein Fall – ein Beitrag". Nur vergleichsweise wenige Arbeitsergebnisse „schaffen es" in den Tätigkeitsbericht – vorzugsweise solche, die prägend für meine Arbeit waren und über den Einzelfall hinaus für das Verständnis, auch die Beachtung datenschutzrechtlicher Rahmenbedingungen des Verwaltungshandelns hilfreich sein können.

Im **allgemeinen Datenschutzrecht** habe ich mich etwa mit der grundsätzlichen Frage des Personenbezugs sowie den Folgen des Angemessenheitsbeschlusses zum EU-U. S. Data Privacy Framework für Verantwortliche des bayerischen öffentlichen Sektors auseinandergesetzt (Beiträge Nr. 2.2 und 2.7). Hinweise zu Datenpannen bei der Excel-Nutzung, zum Umgang mit der Windows-Telemetriekomponente sowie mit der automatischen Rechtschreibkorrektur bei Webbrowsern sollen dabei unterstützen, den Büroalltag in bayerischen Verwaltungen datenschutzkonform zu gestalten (Beiträge Nr. 2.4 bis 2.6).

Im Bereich der **Polizei** habe ich mich intensiv mit Fragen der Löschung in der Vorgangsverwaltung IGVP sowie im Fallbearbeitungssystem EASy befasst, dies im Rahmen einer Stellungnahme gegenüber dem Untersuchungsausschuss „NSU II" des Bayerischen Landtags (Beiträge Nr. 3.1 und 3.2). Ich habe mehrere polizeiliche Videoüberwachungen überprüft (Beitrag Nr. 3.4) und konnte feststellen, dass die Postsicherstellung nach Art. 35 Polizeiaufgabengesetz in der Praxis erfreulich selten angeordnet wird (Beitrag Nr. 3.6). Bei der Anwendung der noch neuen Regelungen zu polizeilichen Zuverlässigkeitsüberprüfungen aus Anlass von Großveranstaltungen sowie der Bestimmungen zur Lichtbildanforderung nach Verkehrsordnungswidrigkeiten konnte ich auf eine grundrechtsschonende Handhabung hinwirken (Beiträge Nr. 3.7 und 3.8).

[5] Europäischer Gerichtshof, Urteil vom 7. Dezember 2023, C-634/21, Rn. 40 ff.

Was die **Allgemeine Innere Verwaltung** betrifft, habe ich die jüngste Kommunalrechtsnovelle kritisch begleitet. Bei den neuen Vorschriften für das Streaming von Bürgerversammlungen sowie von Gremiensitzungen konnte ich in konstruktiver Zusammenarbeit mit dem Bayerischen Staatsministerium des Innern, für Sport und Integration klare datenschutzrechtliche Verbesserungen erreichen (Beiträge Nr. 4.4.1 und 4.4.2). Dagegen ist es mir leider nicht gelungen, die Abschaffung der erst vor wenigen Jahren gefundenen, deutschlandweit vorbildlichen bayerischen Regelung zum Einsatz elektronischer Wasserzähler zu verhindern (Beitrag Nr. 4.4.4). Beschäftigt haben mich daneben viele kleinere datenschutzrechtliche Fragen wie etwa die automatisierte Kennzeichenerfassung beim Kameraparken (Beitrag Nr. 4.7) oder das öffentliche „Hinhängen" einer kritischen Bürgerin in einer Gemeinderatssitzung (Beitrag Nr. 4.3).

Da die Datenschutzaufsicht auch die Verarbeitung personenbezogener Daten in **öffentlichen Registern** erfasst, kann ich die Einhaltung zahlreicher Vorgaben des Melderechts sowie des Fahrzeugregisterrechts überprüfen. So habe ich nicht nur die Nutzung des Melderegisters für die Einladung zum Kinderfest einer politischen Partei förmlich beanstandet (Beitrag Nr. 5.1), sondern auch festgestellt, dass eine bayerische Metropole nicht berechtigt war, das Fahrzeugregister als „Adressquelle" zu verwenden, um Halter von Kraftfahrzeugen mit Dieselmotor über mögliche Fahrverbote zu informieren (Beitrag Nr. 5.2).

Im **Sozial- und Gesundheitsbereich** hatte mein Einsatz für ein uneingeschränktes Widerspruchsrecht von Patientinnen und Patienten gegen dauerhafte Speicherungen im Bayerischen Krebsregister endlich Erfolg (Beitrag Nr. 6.1). Der Prüfungs- und Beratungsalltag bot mir etwa Gelegenheit, einem wohl systemischen Mangel bei Einwilligungsformularen entgegenzuwirken (Beitrag Nr. 6.2) oder die Anforderung von Wundverlaufsprotokollen durch Krankenkassen kritisch zu würdigen (Beitrag Nr. 6.3). Im Zusammenhang mit der Masernimpfpflicht beschäftigten mich nochmals datenschutzrechtliche Fragen bei Kontraindikationsattesten (Beitrag Nr. 6.5).

Vielschichtig waren im Jahr 2023 die Fragestellungen, die ich im **Personaldatenschutz** zu bewältigen hatte. Bei der Begleitung von dienstrechtlichen Gesetzgebungsverfahren etwa hatten nun endlich meine Bemühungen Erfolg, ein Mitbestimmungsrecht des Personalrats bei der Benennung und Abberufung des behördlichen Datenschutzbeauftragten (Beitrag Nr. 7.9.1) sowie datenschutzgerechte Vorgaben für die Übermittlung von Untersuchungs- oder Beobachtungsbefunden im Rahmen der Unfallfürsorge (Beitrag Nr. 7.2.1) zu etablieren. Zu einer Art datenschutzrechtlichem Vexierspiel entwickelte sich das Störfallmanagement des 2023 eingeführten Dienstradprogramms „JobBike Bayern". Auch hier konnten schließlich praktikable, gleichwohl datenschutzkonforme Lösungen gefunden werden (Beitrag Nr. 7.8). Meine Prüfungs- und Beratungstätigkeit gab ferner Anlass, die Rahmenbedingungen für den Umgang mit den Kontaktdaten von Beschäftigten fortzuentwickeln (Beitrag Nr. 7.5). Bei der „Stufenvorweggewährung", einem tarifrechtlichen Instrument zur Bindung qualifizierter Fachkräfte, konnte die konsequente Anwendung von Datenschutzrecht sogar zu einer Verwaltungsvereinfachung beitragen (Beitrag Nr. 7.7).

Verbesserungen des Datenschutzes bei **Schulen und Hochschulen** konnte ich in gleich zwei Gesetzen erreichen: In das Bayerische Gesetz über das Erziehungs- und Unterrichtswesen fand ein voraussetzungsloses Widerspruchsrecht in Bezug auf Datenübermittlungen von Schulen an die Agenturen für Arbeit Aufnahme

(Beitrag Nr. 8.1.1), im Bayerischen Schulfinanzierungsgesetz wurde die Zweckbindung von Schülerdaten bei der Abrechnung von Gastschulbeiträgen gestärkt (Beitrag Nr. 8.1.2). Im Zusammenhang mit der Masernimpfpflicht beschäftigten mich mehrmals Beschwerden, die Weitergaben ärztlicher Atteste von Schulen an Gesundheitsämter betrafen (Beitrag Nr. 8.2). Bei der Datenschutzaufsicht gegenüber den Hochschulen war das Recht auf Kopie im Prüfungskontext ein wichtiges Thema (Beitrag Nr. 8.4). Eine eher originelle Eingabe legte einen datenschutzrechtlichen Anfängerfehler offen – begangen ausgerechnet vom Dozenten eines Datenschutzkurses (Beitrag Nr. 8.5).

Meine Prüfungs- und Beratungspraxis erfasst auch das im Bayerischen Datenschutzgesetz geregelte **Informationszugangsrecht** (Art. 39 BayDSG). Ich habe in einem Überblicksbeitrag einige Erkenntnisse aus Einzelfällen zusammengestellt, mit denen ich im Lauf des Berichtsjahres zu tun hatte (Beitrag Nr. 10.3). Recht arbeitsintensiv war ein Fall, in welchem ein privater Verein mit Hilfe von Art. 39 BayDSG eine Erhebung bei bayerischen Kommunen durchzuführen suchte. Eine Vielzahl von Gemeinden war hier nicht umfassend kooperationsbereit, und es bedurfte einiger Mühe, den Verein bei seinem Anliegen zu unterstützen (Beitrag Nr. 10.2).

Interessante Fragen des **technisch-organisatorischen Datenschutzes** stellten sich in der Folge eines ursprünglich zu Unterrichtszwecken durchgeführten Penetrationstests im pädagogischen Netzwerk einer bayerischen öffentlichen Schule. Hier hatte ein Schüler Sicherheitslücken entdeckt, war aber zunächst nur gemaßregelt worden. Im weiteren Verlauf nutze er das erworbene Wissen ohne pädagogische Aufsicht zu einem größer angelegten Angriff. Ich habe den bayerischen öffentlichen Stellen nun einige Hinweise zum proaktiven Umgang mit den Ergebnissen unerbetener Pentests gegeben (Beitrag Nr. 11.3). Weiterhin hatte ich mich beispielsweise mit der datenschutzgerechten Gestaltung von Bürgerbüros (Beitrag Nr. 11.7), mit der Nutzung nicht dienstlich administrierter E-Mail-Accounts im dienstlichen Kontext (Beitrag Nr. 11.1) oder mit dem Verlust einer Patientenakte (Beitrag Nr. 11.8) zu befassen. Ich habe zahlreiche Verantwortliche zu Datenschutz-Folgenabschätzungen beraten (Beitrag Nr. 11.4) und mich intensiv an der Gremienarbeit zur Anonymisierung und Pseudonymisierung sowie zum KI-Einsatz in der medizinischen Forschung beteiligt (Beitrag Nr. 11.12). Über den Berichtszeitraum gingen bei mir erwartungsgemäß wieder hunderte Meldungen von Datenpannen ein, denen nachzugehen war (Beitrag Nr. 11.9). Gegen ein bayerisches öffentliches Krankenhaus musste ich eine Anordnung nach Art. 58 Abs. 2 DSGVO mit dem Ziel erlassen, dort ein gesetzmäßiges Rollen- und Berechtigungskonzept zu implementieren (Beitrag Nr. 11.11).

Schließlich kann ich über einen recht grundsätzlichen Fall berichten, der das **Verhältnis von gesamtverantwortlichen Stellen und Datenschutz-Aufsichtsbehörde** betraf (Beitrag Nr. 4.2). In diesem Fall hatte ein Fachreferat eines Staatsministeriums in einem Förderbescheid versucht, die für ein IT-Projekt zu gewährenden Leistungen an eine Unbedenklichkeitsbescheinigung des Landesbeauftragten zu binden. Eine solche Vorgehensweise ist mit der völligen Unabhängigkeit der Datenschutz-Aufsichtsbehörden nicht in Einklang zu bringen. Auf meinen Widerstand hin hat die Behördenleitung des Staatsministeriums den Versuch einer ungesetzlichen Arbeitserleichterung ohne weitere Diskussion unterbunden. Die zügige und eindeutige Reaktion hat mein Vertrauen, dass die bayerische Verwaltung den datenschutzrechtlichen Handlungsrahmen insgesamt ernst nimmt, durchaus gestärkt.

2 Allgemeines Datenschutzrecht

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

Obwohl die Infothek „Datenschutzreform 2018“ auf meiner Internetpräsenz inzwischen recht umfangreich ist, konnte ich auch im Jahr 2023 einige neue Informationen bereitstellen; weitere bereits bewährte Papiere habe ich zudem erweitert und auf einen aktuellen Stand gebracht. Unter den neuen Beiträgen sind drei hervorzuheben:

– das schon im Januar erschienene Arbeitspapier **„Löschung oder Archivierung? Archivrechtliche Aufbewahrungs- und datenschutzrechtliche Löschungsregelungen im bayerischen öffentlichen Sektor“**. Dieses Papier habe ich gemeinsam mit der Generaldirektion der Staatlichen Archive Bayerns erarbeitet. Es erläutert das Verhältnis zwischen datenschutzrechtlicher Löschungs- und archivrechtlicher Anbietungspflicht, charakterisiert die Archivierung als Löschungssurrogat und geht – unter Berücksichtigung der je eigenen Perspektive von Datenschutz- und Archivrecht – auf die in der Praxis besonders wichtige Frage der Aufbewahrungsdauer ein. Ferner kommt mit der vorzeitigen Löschung personenbezogener Daten im Einzelfall ein besonderes Problem des Verhältnisses von Datenschutz- und Archivrecht zur Sprache. Schließlich werden die datenschutzrechtlichen Informationspflichten bei der Archivierung von Unterlagen erläutert.

  Das von mir als der Datenschutz-Aufsichtsbehörde für den bayerischen öffentlichen Sektor sowie der Generaldirektion als der zentralen staatlichen Fachbehörde für alle Fragen des Archivwesens entwickelte Papier gibt nach meiner Auffassung ein schönes Beispiel nicht nur für die Verzahnung, sondern auch für die einfühlsame Abstimmung von Fach- und Datenschutzrecht;

– die im April publizierte Orientierungshilfe **„Datenschutz als Kriterium im Vergabeverfahren“**. Viele Leistungen und Produkte, die bayerische öffentliche Stellen beschaffen, haben Bezüge zum Datenschutz und müssen einschlägigen rechtlichen Anforderungen sowie ergänzenden technisch-organisatorischen Standards entsprechen. Die Weichen zum (auch) datenschutzgerechten Produkt werden im Zuge des Beschaffungsprozesses gestellt. Die 43-seitige Orientierungshilfe, die mittlerweile in einer Version 2.0 vorliegt, zeigt unter Berücksichtigung der Spruchpraxis von Vergabekammern und Gerichten systematisch, welche „Einfallstore“ sich in Beschaffungsprozessen für datenschutzrechtliche Anforderungen öffnen und wie man sie zielführend nutzt. Sie befasst sich dabei unter anderem auch mit den Rechtmäßigkeitsvoraussetzungen der besonders praxisrelevanten Vergabe von Cloud-Leistungen. Datenschutzrecht und Vergaberecht sind dabei durchgängig im Verbund dargestellt;

— die im Mai veröffentlichte Orientierungshilfe **„Internationale Datentransfers“**. Das 60 Seiten starke Papier zeichnet den Stand der Rechtsentwicklung bei diesem recht „schnelllebigen“ Thema nach und entwickelt daraus Hinweise für die Verwaltungspraxis der bayerischen öffentlichen Stellen. Die nach der „Schrems II“-Entscheidung entstandenen Wegweisungen des Europäischen Datenschutzausschusses sind ebenso berücksichtigt wie einschlägige Verlautbarungen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder.

  Nach Wirksamwerden des bereits berücksichtigten Angemessenheitsbeschlusses für das EU-U. S. Data Privacy Framework habe ich die neue Orientierungshilfe noch um ein speziell auf diese Transferbeziehung zugeschnittenes Papier ergänzt (siehe Beitrag Nr. 2.7).

In der Reihe der **Aktuellen Kurz-Informationen** fallen die Nummern 45 bis 52 in das Berichtsjahr. Zudem haben die seit 2018 auf meiner Homepage stets „abrufstarken“ Beiträge „Versand von Newslettern durch bayerische öffentliche Stellen“ sowie „Melderegisterdaten und Gratulationen“ den Stand von 2023 erhalten. Vom beliebten zweisprachigen (deutsch/englisch) Newsletter **„Privacy in Bavaria“** erschienen in diesem Jahr neun Ausgaben.

Zusammengefasst und überarbeitet habe ich schließlich mein **Informationsangebot zum Schuldatenschutz**. Es ist nun in den beiden Arbeitspapieren „Foto- und Videoaufnahmen in der Schule, insbesondere im Schulunterricht“ und „Datenschutz bei Schülerunterlagen“ sowie einem FAQ-Papier „Datenschutz an bayerischen öffentlichen Schulen – Fragen und Antworten“ gebündelt.

Für das Jahr 2024 sind weitere Veröffentlichungen geplant. Verantwortliche des bayerischen öffentlichen Sektors, ihre behördlichen Datenschutzbeauftragten und alle anderen am Datenschutz Interessierten erfahren auf meinem **Mastodon-Kanal** https://social.bund.de/@BayLfD tagesaktuell, was es an Neuem gibt.

2.2 Wann ist eine natürliche Person identifizierbar?

Ohne die Verarbeitung personenbezogener Daten gibt es weder funktionsfähige öffentliche Verwaltungen noch erfolgreiche private Unternehmen. Soweit und solange verarbeitete Daten personenbezogen sind, müssen Datenverarbeiter allerdings datenschutzrechtliche Vorgaben beachten. Die Antwort auf die Frage, ob Daten einen Personenbezug aufweisen, ist daher von grundlegender Bedeutung. Vielfach wird das einfach zu beurteilen sein; in anderen Fällen jedoch bereitet die Weichenstellung in das Datenschutzrecht erhebliches Kopfzerbrechen. Schwierigkeiten ergeben sich insbesondere bei der Feststellung, ob eine Person im datenschutzrechtlichen Sinn „identifizierbar“ ist.

Wann eine „Identifizierbarkeit“ natürlicher Personen und in der Folge eine Verarbeitung personenbezogener Daten anzunehmen ist, hat jüngst auch den Europäischen Gerichtshof (abermals) beschäftigt.[6] Aus diesem Anlass möchte der vorliegende Beitrag den bayerischen öffentlichen Stellen die rechtlichen Hintergründe auf Basis der bisherigen unionsgerichtlichen Rechtsprechung zusammenfassend erläutern und einige Empfehlungen mit auf den Weg zu geben.

[6] Europäischer Gerichtshof, Urteil vom 9. November 2023, C-319/22.

2.2.1 Rechtlicher Hintergrund

Nach Art. 4 Nr. 1 Halbsatz 1 DSGVO sind personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person“ (die sogenannte „betroffene Person“) beziehen. Ein Personenbezug liegt also nicht erst dann vor, wenn sich die Identität einer betroffenen Person unmittelbar aus den verarbeiteten Daten ergibt, die Person mithin bereits identifiziert ist. Ausreichend ist vielmehr, dass die Daten die Identifizierung einer natürlichen Person „direkt oder indirekt“ (vgl. Art. 4 Nr. 1 Halbsatz 2 DSGVO) ermöglichen. Eine solche Identifizierbarkeit setzt (mindestens) einen „Zwischenschritt“ voraus, nämlich den Einsatz von (Identifizierungs-)Mitteln (insbesondere in Form von „Zusatzwissen“), mit deren Hilfe eine Beziehung zwischen dem Informationsgehalt der verarbeiteten Daten und einer Person – und damit ein Personenbezug – hergestellt werden kann.[7]

Damit stellt sich die Frage, auf wessen Mittel es ankommen soll, um die Identifizierbarkeit einer Person und damit einen Personenbezug im Sinne von Art. 4 Nr. 1 DSGVO annehmen zu können. Sind hier nur die Mittel des Verantwortlichen selbst oder auch – und gegebenenfalls in welchem Umfang – Erkenntnisse oder Erkenntnismöglichkeiten Dritter zu berücksichtigen?

Die praktische Bedeutung dieser Frage ist nicht zu unterschätzen: Relevant wird sie etwa in Fällen der Übermittlung pseudonymisierter Daten. Bei einer Pseudonymisierung werden personenbezogene Daten so verarbeitet, dass eine Zuordnung dieser Daten zu einer natürlichen Person nur mittels gesondert aufbewahrter und gesicherter „zusätzlicher Informationen“ erfolgen kann. Für die übermittelnde Stelle, welche über diese Zusatzinformationen verfügt, bleiben diese Daten jedenfalls personenbezogen, vgl. Art. 4 Nr. 5 DSGVO. Doch wie ist der Personenbezug zu bewerten, wenn der Empfänger von pseudonymisierten Daten über diese Zusatzinformationen nicht verfügt und auch keine (legale) Möglichkeit hat, auf diese Informationen zuzugreifen?

2.2.2 „Relatives“ und „absolutes“ Verständnis des Personenbezugs

Die Diskussion zur Identifizierbarkeit natürlicher Personen und zum Personenbezug von Daten reicht in der (deutschen) Datenschutz-Fachwelt noch bis deutlich vor den Geltungsbeginn der Datenschutz-Grundverordnung zurück. Die Ergebnisse dieser Diskussion lassen sich wie folgt zusammenfassen: Nach einem sogenannten „relativen“ oder „subjektiven“ Verständnis des Personenbezugs sind allein die Mittel – insbesondere das „Zusatzwissen“ – des Verantwortlichen maßgebend. Für das „absolute“ oder „objektive“ Verständnis genügt demgegenüber, dass eine beliebige Stelle, nicht zwingend der Verantwortliche selbst, einen Personenbezug herstellen kann. Überspitzt gesagt, nimmt das absolute Verständnis das „Weltwissen“ in den Blick. Zwischen diesen Extrempositionen gruppieren sich zahlreiche vermittelnde, differenzierende oder anderweit kompromissorientierte Meinungen.[8]

[7] Vgl. Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 DSGVO Rn. 57.

[8] Ausführlich hierzu Klar/Kühling, in: Kühling/Buchner, DS-GVO/BDSG, 4. Aufl. 2024, Art. 4 Nr. 1 DSGVO Rn. 25 ff.; Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 DSGVO Rn. 58 ff.

2.2.3 Wie verhält sich die Datenschutz-Grundverordnung hierzu?

Die Legaldefinition in Art. 4 Nr. 1 DSGVO erhellt nicht, auf wessen Mittel es zur Identifizierbarkeit einer Person ankommen soll. Aussagen dazu bringt allerdings EG 26 Satz 3 DSGVO: Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten danach „alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren [...]". Offenbar sollen also nicht allein die Mittel des Verantwortlichen, die dieser zur Identifizierung einer Person nutzen kann, sondern auch entsprechende Mittel anderer Stellen in den Blick genommen werden. Dabei kommt es dem Wortlaut nach allein auf das „Nutzungspotential" an; ob bestehende Identifizierungsmöglichkeiten vom Verantwortlichen oder von Dritten dann tatsächlich auch ausgeschöpft werden, soll wohl nicht entscheidend sein.[9]

Dieser im Ausgangspunkt weitreichende Ansatz wird zugleich dahin eingeschränkt, dass nur Mittel berücksichtigt werden sollen, die Verantwortliche oder andere Stellen nach allgemeinem Ermessen wahrscheinlich zu Identifizierungszwecken nutzen. Wann das der Fall ist, bestimmt sich nach EG 26 Satz 4 DSGVO anhand „objektiver Faktoren". Daraus folgt, dass subjektive Absichtserklärungen von Verantwortlichen oder anderen Stellen, auf bestimmte Identifizierungsmittel verzichten zu wollen, im Rahmen dieser Wahrscheinlichkeitsbeurteilung für sich genommen unerheblich sind.[10] Zu berücksichtigen sind hingegen stets „die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen" (EG 26 Satz 4 DSGVO am Ende). Dies trägt dem Umstand Rechnung, dass die fortschreitende technologische Entwicklung zunehmend mehr Möglichkeiten der (Re-)Identifizierung von Personen bietet. Demnach können sich auch vormals anonyme oder als anonymisiert angesehene Daten – Daten also, die vermeintlich keinen Personenbezug (mehr) aufweisen –, allein aufgrund technologischer Entwicklungen als noch oder wieder personenbezogen herausstellen.[11]

Zusammenfassend verdeutlicht EG 26 DSGVO, dass es bei der Frage der Identifizierbarkeit einer Person sowohl auf die Mittel des Verantwortlichen als auch anderer Stellen ankommen kann. Umgekehrt wird jedoch nicht auf ein gegebenenfalls nur rein theoretisch abrufbares „Weltwissen" abgestellt – verfügbare Mittel müssen vielmehr nach allgemeinem Ermessen wahrscheinlich eingesetzt werden. Dabei spielen auch zunehmend technologische Möglichkeiten zur (Re-)Identifizierung betroffener Personen eine Rolle; sie können dazu führen, dass eine vormalige Einstufung von Daten als „nicht personenbezogen" im Nachgang revidiert werden muss.

Übertragen auf deutsche Begrifflichkeiten vereint EG 26 DSGVO damit Elemente sowohl des absoluten als auch des relativen Personenbezugs. Auf diesem Weg bietet die Datenschutz-Grundverordnung bereits eine wertvolle Orientierung bei der Beurteilung, ob personenbezogene Daten vorliegen oder nicht. Die Ausführungen bleiben soweit noch abstrakt – insbesondere bedarf die Anforderung, dass

9 Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 DSGVO Rn. 62.

10 Für eine Berücksichtigung subjektiver Faktoren im Rahmen des objektiven Maßstabs nach EG 26 Satz 4 DSGVO Klar/Kühling, in: Kühling/Buchner, DS-GVO/BDSG, 4. Aufl. 2024, Art. 4 Nr. 1 DSGVO Rn. 23.

11 Vgl. Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 DSGVO Rn. 63.

lediglich hinreichend „wahrscheinlich“ eingesetzte Mittel zu berücksichtigen sind, einer Konkretisierung. Abgesehen von gesetzlichen Ergänzungen oder Klarstellungen ist dies Aufgabe der Rechtsprechung – insbesondere des Europäischen Gerichtshofs –, jedoch auch der Datenschutz-Aufsichtsbehörden in den Mitgliedstaaten.

2.2.4 Die unionsgerichtliche Rechtsprechung zur Identifizierbarkeit einer natürlichen Person

Im Folgenden werden drei Entscheidungen der Unionsgerichte vorgestellt, die sich (auch) mit der Frage der Identifizierbarkeit einer natürlichen Person und so mit den Anforderungen an den Personenbezug von Daten befasst haben. Zwei dieser Entscheidungen stammen vom Europäischen Gerichtshof, eine vom Gericht der Europäischen Union.[12] Ziel der Darstellung ist keine vertiefte wissenschaftliche Auseinandersetzung mit den einzelnen Urteilen, sondern das Herausarbeiten und eine Kurzbewertung ihrer wesentlichen Aussagen. Dabei ist stets im Blick zu behalten, dass der Europäische Gerichtshof dem Begriff der „personenbezogenen Daten“ generell eine weite Bedeutung beimisst.[13]

2.2.4.1 Das Urteil des Europäischen Gerichtshofs zu dynamischen IP-Adressen

Als durchaus wegweisend kann das sogenannte „Breyer-Urteil“ des Europäischen Gerichtshofs bezeichnet werden.[14] Diese Entscheidung ist zwar noch zur „alten“ Datenschutzrichtlinie[15] ergangen; die insoweit maßgeblichen rechtlichen Vorgaben finden sich jedoch im Wesentlichen – mit geringfügigen sprachlichen Abweichungen[16] – auch in der Datenschutz-Grundverordnung. Die Erwägungen des Gerichtshofs im Breyer-Urteil können daher auch unter Geltung der Datenschutz-Grundverordnung nutzbar gemacht werden (siehe hierzu näher Nr. 2.2.4.3).

Dem Breyer-Urteil lag unter anderem die Vorlagefrage zugrunde, ob – verkürzt gesagt – dynamische IP-Adressen, die ein Anbieter von Online-Mediendiensten von Besucherinnen und Besuchern der Internetpräsenz gespeichert hat, für diesen Anbieter personenbezogene Daten darstellen. Prämisse war dabei, dass zwar nicht der Anbieter selbst, aber ein Dritter (hier: der Internetzugangsanbieter) über

[12] Art. 19 Abs. 1 Satz 1 Vertrag über die Europäische Union (EUV) fasst unter der Dachbezeichnung „Gerichtshof der Europäischen Union“ den Europäischen Gerichtshof, das Gericht der Europäischen Union sowie Fachgerichte zusammen. Das Gericht der Europäischen Union entscheidet in erster Instanz über bestimmte Klagen gegen Maßnahmen der Union, vgl. Art. 256 EUV.

[13] Vgl. nur Europäischer Gerichtshof, Urteil vom 4. Mai 2023, C-478/21, Rn. 23.

[14] Europäischer Gerichtshof, Urteil vom 19. Oktober 2016, C-582/14, BeckRS 2016, 82520.

[15] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

[16] So stellt etwa EG 26 Satz 2 der Richtlinie 95/46/EG im vorliegenden Zusammenhang auf Mittel ab, die „vernünftigerweise“ eingesetzt werden können, während EG 26 Satz 3 DSGVO von Mitteln spricht, die „nach allgemeinem Ermessen wahrscheinlich genutzt werden.“ Die englischen Sprachfassungen sind an diesen Stellen „näher beieinander“ und nennen einmal „all the means likely reasonably to be used“ beziehungsweise „all the means reasonably likely to be used“. Es ist daher davon auszugehen, dass der europäische Gesetzgeber sowohl in der Datenschutz-Richtlinie als auch in der Datenschutz-Grundverordnung insoweit das Gleiche gemeint hat.

das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt.[17]

Der Gerichtshof hat diese Frage anhand der ihm vorliegenden Informationen im Ergebnis bejaht:[18] Für die Einstufung eines Datums als „personenbezogenes Datum" sei es nicht erforderlich, „dass sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befinden."[19] Damit erteilte der Gerichtshof unter Bezugnahme auf EG 26 Satz 2 Richtlinie 95/46/EG jedenfalls dem streng relativen Verständnis des Personenbezugs im oben dargestellten Sinn eine Absage.

Zu berücksichtigen seien allerdings nur Mittel, die „vernünftigerweise zur Bestimmung der betroffenen Person eingesetzt werden" können. Letzteres sei nicht der Fall, wenn die Identifizierung der betroffenen Person gesetzlich verboten oder praktisch – etwa wegen eines unverhältnismäßigen Aufwands an Zeit und Kosten – nicht durchführbar wäre, sodass „das Risiko einer Identifizierung de facto vernachlässigbar" erscheine.[20] Der Gerichtshof konkretisiert die „vernünftigerweise" oder – in der Formulierung der Datenschutz-Grundverordnung – „nach allgemeinem Ermessen wahrscheinlich" genutzten Mittel somit durch eine „Negativabgrenzung" – wobei im Einzelnen allerdings offen bleibt, wann die Schwelle zum „unverhältnismäßigen Aufwand" überschritten ist. Der Gerichtshof verlangt jedenfalls nicht, dass die Identifizierung einer Person in jedem Falle mit Sicherheit ausgeschlossen sein muss, sondern akzeptiert ein gegebenenfalls verbleibendes Identifizierungs(rest-)risiko, sofern dieses „de facto vernachlässigbar" ist.

Mit Blick auf die Vorlagefrage stellt der Gerichtshof im Weiteren auf Mittel ab, die dem Anbieter von Online-Mediendiensten zur Verfügung stehen. Vernünftigerweise einsetzbar seien dabei „rechtliche Mittel", die es diesem erlauben, gegebenenfalls mittels eines „Umwegs" über die zuständige Behörde die betroffene Person bestimmen zu lassen.[21]

2.2.4.2 Das Europäische Gericht und die Übermittlung pseudonymisierter Daten

Regelmäßig steht die Rechtsprechung des Europäischen Gerichtshofs im Fokus der datenschutzfachlichen Aufmerksamkeit. In jüngerer Zeit hat jedoch auch eine Entscheidung des Gerichts der Europäischen Union, die sich mit Fragen der Identifizierbarkeit natürlicher Personen und dem Personenbezug von Daten befasste, in Fachkreisen für Aufsehen gesorgt.[22] Im konkreten Fall war zwar nicht die Datenschutz-Grundverordnung maßgebend, sondern die Verordnung (EU)

17 Europäischer Gerichtshof, Urteil vom 19. Oktober 2016, C-582/14, BeckRS 2016, 82520, Rn. 37.

18 Europäischer Gerichtshof, Urteil vom 19. Oktober 2016, C-582/14, BeckRS 2016, 82520, Rn. 49.

19 Europäischer Gerichtshof, Urteil vom 19. Oktober 2016, C-582/14, BeckRS 2016, 82520, Rn. 43.

20 Europäischer Gerichtshof, Urteil vom 19. Oktober 2016, C-582/14, BeckRS 2016, 82520, Rn. 45 f.

21 Europäischer Gerichtshof, Urteil vom 19. Oktober 2016, C-582/14, BeckRS 2016, 82520, Rn. 47 ff.

22 Gericht der Europäischen Union, Urteil vom 26. April 2023, T-557/20 = ZD 2023, 399 mit Anmerkung Baumgartner.

2018/1725. Dieses Gesetz enthält datenschutzrechtliche Vorgaben für Verarbeitungen durch Stellen der Europäischen Union.[23] Was den Begriff der „personenbezogenen Daten“ angeht, sind die einschlägigen Bestimmungen in diesen Verordnungen jedoch inhaltlich deckungsgleich;[24] das Urteil des Gerichts ist daher auch in der Welt der Datenschutz-Grundverordnung von Bedeutung.

Der im Einzelnen durchaus komplexe Sachverhalt lässt sich vereinfacht wie folgt zusammenfassen: Eine Stelle, hier der „Einheitliche Abwicklungsausschuss“, erhob im Rahmen eines Anhörungsverfahrens Stellungnahmen natürlicher Personen. Die eingegangenen Stellungnahmen wurden mit einem alphanumerischen Code versehen, sodass die Inhalte der Stellungnahmen von den persönlichen Daten der einreichenden Personen getrennt waren. Die Identitätsdaten der Beteiligten hielt der Einheitliche Abwicklungsausschuss in einer eigenen Datenbank vor, zu der nur einige seiner Beschäftigten Zugang hatten. Ein Teil der so „codierten“ Stellungnahmen wurde im Anschluss an ein externes Beratungsunternehmen zur Bewertung übermittelt. Der Einheitliche Abwicklungsausschuss konnte anhand des verwendeten Codes und der vorgehaltenen Identitätsdaten die einzelnen Stellungnahmen bestimmten Personen zuordnen. Das Beratungsunternehmen hatte dagegen keinen Zugang zu der Datenbank mit den Identitätsdaten der Beteiligten.[25]

Nach Auffassung des Europäischen Datenschutzbeauftragten – des Beklagten in diesem Verfahren – hat der Einheitliche Abwicklungsausschuss pseudonymisierte und damit personenbezogene Daten an das Beratungsunternehmen übermittelt; schließlich sei aufgrund der noch vorhandenen Identitätsdaten eine (Re-)Identifizierung der betroffenen Personen „hinter“ den codierten Stellungnahmen weiterhin möglich.[26] Der Einheitliche Abwicklungsausschuss war demgegenüber der Ansicht, die übermittelten Daten seien für das Beratungsunternehmen anonymisiert worden; er habe weder die für eine Reidentifizierung notwendigen Zusatzinformationen mit dem Beratungsunternehmen geteilt, noch habe dieses ein entsprechendes Zugangsrecht.[27]

Das Gericht nimmt in seiner Entscheidung zunächst ausführlich Bezug auf das oben dargestellte Breyer-Urteil des Europäischen Gerichtshofs.[28] Auf dieser Grundlage vergleicht es sodann die Situation des Beratungsunternehmens mit derjenigen des Anbieters von Online-Mediendiensten im Breyer-Urteil: Für die Bewertung, ob es sich bei den übermittelten Informationen um personenbezogene Daten handle, sei darauf abzustellen, ob sich diese Informationen nach dem

[23] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG.

[24] Vgl. nur die mit Art. 4 Nr. 1 DSGVO identische Begriffsbestimmung in Art. 3 Nr. 1 Verordnung (EU) 2018/1725.

[25] Vgl. im Einzelnen Gericht der Europäischen Union, Urteil vom 26. April 2023, T-557/20, Rn. 2 ff., insbesondere Rn. 14 ff. und Rn. 24.

[26] Vgl. Gericht der Europäischen Union, Urteil vom 26. April 2023, T-557/20, Rn. 32, 79 ff.

[27] Gericht der Europäischen Union, Urteil vom 26. April 2023, T-557/20, Rn. 76 ff.

[28] Gericht der Europäischen Union, Urteil vom 26. April 2023, T-557/20, Rn. 88 ff.

Verständnis des Beratungsunternehmens auf „identifizierbare Personen“ bezogen hätten.[29] Demgegenüber habe sich die Prüfung des Europäischen Datenschutzbeauftragten auf die Perspektive des Einheitlichen Abwicklungsausschusses und damit (nur) des Datenübermittlers beschränkt.[30]

Bemerkenswert ist dieses Urteil unter anderem[31] deshalb, weil es bei der Frage, ob die Übermittlung pseudonymisierter Daten datenschutzrechtlich relevant ist, dem „Empfängerhorizont“ entscheidende Bedeutung beimisst. Damit eröffnet das Gericht Raum für eine im Einzelfall mögliche „anonymisierende Wirkung“ einer Pseudonymisierung: Eine solche Pseudonymisierung ändert zwar für den Verantwortlichen, der die für eine (Re-)Identifizierung der betroffenen Personen erforderlichen Zusatzinformationen vorhält, grundsätzlich nichts am Personenbezug (vgl. Art. 4 Nr. 15 DSGVO). Folgt man der Auffassung des Gerichts, kann eine Übermittlung von pseudonymisierten Daten unter Umständen gleichwohl zu einer auf die konkrete Übermittlung beschränkten Aufhebung des Personenbezugs dieser Daten führen, nämlich dann, wenn der Empfänger über keine vernünftigerweise einsetzbaren Identifizierungsmöglichkeiten verfügt. Ob Letzteres im konkreten Fall tatsächlich zutraf, hat das Gericht nicht entschieden, sondern die insoweit unterbliebene Prüfung der Aufsichtsbehörde moniert.[32]

Das Urteil des Gerichts ist noch nicht rechtskräftig;[33] eine Entscheidung des Europäischen Gerichtshofs in dieser Sache bleibt abzuwarten.

2.2.4.3 Der Europäische Gerichtshof und die Fahrzeug-Identifizierungsnummer

Etwas mehr als ein halbes Jahr nach der Entscheidung des Gerichts hatte nun der Europäische Gerichtshof in einem anderen Verfahren Anlass, sich zum Personenbezug von Daten und der Identifizierbarkeit natürlicher Personen zu äußern. Seine neueste Entscheidung[34] betrifft zwar im Schwerpunkt keine ausgesprochen datenschutzrechtliche Streitsache, behandelt gleichwohl aber die Frage, ob Fahrzeughersteller im Sinne von Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO verpflichtet sind, sogenannten „unabhängigen Wirtschaftsakteuren“ (wie etwa unabhängigen Werkstätten oder Ersatzteilhändlerinnen und Ersatzteilhändlern) die Fahrzeugidentifizierungsnummern (FIN) der produzierten Fahrzeuge bereitzustellen. Die Anwendbarkeit von Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO – und der Datenschutz-Grundverordnung insgesamt – hängt hier davon ab, ob es sich bei der FIN um eine Information über eine identifizierbare natürliche Person und damit um ein personenbezogenes Datum im Sinne von Art. 4 Nr. 1 DSGVO handelt.

Unter Bezugnahme auf sein Breyer-Urteil macht der Gerichtshof eingangs darauf aufmerksam, dass zur Beantwortung dieser Frage alle Mittel berücksichtigt werden sollten, die vernünftigerweise entweder von dem Verantwortlichen oder von einem Dritten eingesetzt werden könnten, um die betroffene Person zu bestimmen. Dabei sei es nicht erforderlich, dass sich alle zur Identifizierung dieser Person

[29] Gericht der Europäischen Union, Urteil vom 26. April 2023, T-557/20, Rn. 97.
[30] Gericht der Europäischen Union, Urteil vom 26. April 2023, T-557/20, Rn. 103.
[31] Die weiteren Ausführungen des Gerichts beschäftigen sich im Schwerpunkt mit der Frage, ob die Stellungnahmen überhaupt Informationen enthielten, die sich inhaltlich auf natürliche Personen beziehen, vgl. Gericht der Europäischen Union, Urteil vom 26. April 2023, T-557/20, Rn. 64 ff.
[32] Gericht der Europäischen Union, Urteil vom 26. April 2023, T-557/20, Rn. 104 f.
[33] Vgl. Rechtsmittel des Europäischen Datenschutzbeauftragten, ABl. C Nr. 296 vom 21. August 2023, S. 26.
[34] Europäischer Gerichtshof, Urteil vom 9. November 2023, C-319/22.

notwendigen Informationen in den Händen einer einzigen Einrichtung befinden.[35] Damit wiederholt der Gerichtshof Kernaussagen des Breyer-Urteils – erstaunlicherweise ohne EG 26 Satz 3 und 4 DSGVO zu erwähnen. Der Gerichtshof sieht die Grundsätze aus dem Breyer-Urteil also auch unter der Datenschutz-Grundverordnung weiter als maßgebend an.

Da die FIN unmittelbar nur die Identifizierung eines Fahrzeugs ermöglicht, stellt sie nach Ansicht des Gerichtshofs „als solche" zwar kein personenbezogenes Datum dar. Verfügt eine Stelle allerdings „bei vernünftiger Betrachtung" über Mittel, die es ihr ermöglichen, „Daten wie die FIN" einer bestimmten Person zuzuordnen, werden diese Daten zu personenbezogenen Daten.[36] Noch deutlicher als im Breyer-Urteil lässt der Gerichthof damit ein relatives Grundverständnis des Personenbezugs erkennen: Ein „eigentlich" nicht personenbezogenes Datum kann in bestimmten Verwendungszusammenhängen zu einem personenbezogenen Datum werden.

Als „Zuordnungsmittel" kam im vorliegenden Fall insbesondere die Zulassungsbescheinigung in Betracht, die neben der FIN auch Namen und Anschrift des Inhabers enthält.[37] Ob die FIN danach ein personenbezogenes Datum darstellt, hat der Gerichtshof nicht abschließend entschieden, sondern der Prüfung durch das vorlegende Gericht überlassen. Sollte die FIN für die unabhängigen Wirtschaftsakteure nach den oben genannten Kriterien ein personenbezogenes Datum sein, gilt dies nach Auffassung des Gerichtshofs allerdings „mittelbar" auch für die Fahrzeughersteller, welche die FIN bereitstellen.[38] Ähnlich wie das Gericht der Europäischen Union in dem unter Nr. 2.2.4.2 behandelten Urteil stellt der Gerichtshof bei der Beurteilung des Personenbezugs von (in diesem Fall durch Bereitstellung) offengelegten Daten auf den „Empfängerhorizont" ab – dies freilich unter „geänderten Vorzeichen": Während das Gericht den Personenbezug der übermittelten Daten mit der unter Nr. 2.2.4.2 dargelegten Argumentation hinterfragte, zieht der Gerichtshof diese gerade heran, um einen Personenbezug einzelfallabhängig begründen zu können.

2.2.5 Was folgt daraus für bayerische öffentliche Stellen?

Die Entscheidungen zeigen, dass die Frage der Identifizierbarkeit natürlicher Personen und damit des Personenzugs von Daten zwar in ihren Grundzügen, nicht jedoch in allen Einzelheiten geklärt ist. Dies betrifft insbesondere den Umfang, in welchem Wissen und Möglichkeiten Dritter bei der Beurteilung des Personenbezugs zu berücksichtigen sind, sowie die Bedeutung, die dem „Empfängerhorizont" bei der Offenlegung von Daten insoweit zukommt. Weitere Konkretisierungen durch die unionsgerichtliche Rechtsprechung sind zu erwarten.

Bayerische öffentliche Stellen sind daher gut beraten, die Rechtsprechung aufmerksam zu verfolgen; es empfiehlt sich, zu diesem Zweck den Newsletter „Privacy in Bavaria" per RSS-Feed oder Mastodon-Account zu beziehen.[39]

35 Europäischer Gerichtshof, Urteil vom 9. November 2023, C-319/22, Rn. 45.
36 Europäischer Gerichtshof, Urteil vom 9. November 2023, C-319/22, Rn. 46.
37 Europäischer Gerichtshof, Urteil vom 9. November 2023, C-319/22, Rn. 47 f.
38 Europäischer Gerichtshof, Urteil vom 9. November 2023, C-319/22, Rn. 49.
39 Internet: https://www.datenschutz-bayern.de/static/rss-main.html und https://www.datenschutz-bayern.de/mastodon.

Deutlich geworden ist aus den bisherigen Entscheidungen bereits: Ob und inwieweit sich Daten auf eine identifizierbare Person beziehen, erfordert in der Regel eine Einzelfallbetrachtung. Deutlich zu kurz gegriffen wäre es dabei, wenn eine öffentliche Stelle nur ihre eigenen Identifizierungsmöglichkeiten in den Blick nehmen würde. Nicht nur, aber gerade bei der Offenlegung von Daten können die Mittel Dritter dazu führen, dass ein Personenbezug von Daten erst hergestellt wird. Aus EG 26 Satz 4 DSGVO ergibt sich ferner, dass der Begriff der „personenbezogenen Daten" nicht statisch ist. Technologische Entwicklungen können dazu führen, dass Daten, bei denen ein Personenbezug zunächst verneint worden ist, einen solchen mit fortschreitender Entwicklung dann doch erhalten.

In Zweifelsfällen sollten bayerische öffentliche Stellen einen Personenbezug annehmen und – gegebenenfalls „überobligatorisch" – datenschutzrechtliche Vorgaben beachten.

2.2.6 Fazit

Die Frage, welche Mittel für die Identifizierbarkeit natürlicher Personen zu berücksichtigen sind, ist für den Begriff der „personenbezogenen Daten" und damit für die Anwendbarkeit des Datenschutzrechts von erheblicher Bedeutung. Sowohl die Datenschutz-Grundverordnung als auch die Rechtsprechung des Europäischen Gerichtshofs verweisen darauf, dass es hier nicht nur auf die Mittel des Verantwortlichen, sondern auch auf Mittel Dritter ankommen kann. Solche Mittel werden dem Verantwortlichen nicht schrankenlos zugerechnet; begrenzend wirkt insbesondere die Prüfung, ob der Einsatz eines Mittels zur Identifizierung natürlicher Personen hinreichend wahrscheinlich oder vernünftigerweise zu erwarten ist. In Fällen der Datenoffenlegung scheint die jüngere unionsgerichtliche Rechtsprechung dabei den Mitteln des Datenempfängers maßgebende Bedeutung beizumessen.

Klar ist aber auch: Das letzte Wort ist zu diesen Fragen noch nicht gesprochen.

2.3 Frühjahrsputz im Verarbeitungsverzeichnis

Sie erinnern sich noch, was Sie Anfang 2018 gemacht haben? Sie haben als behördliche Datenschutzbeauftragte oder behördlicher Datenschutzbeauftragter bei einer bayerischen öffentlichen Stelle an der erstmaligen Erstellung des Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 DSGVO mitgewirkt? Dann war Ihre öffentliche Stelle damals schneller als viele andere.

Allerdings ist die mühsam erarbeitete Dokumentation nun schon (fast) fünf Jahre alt. Da ist es allerhöchste Zeit, die Texte einmal hervorzuholen, um zu kontrollieren ob noch alles auf dem aktuellen Stand ist. Das sollte nämlich so sein. Das Verzeichnis der Verarbeitungstätigkeiten (im Folgenden kurz: Verarbeitungsverzeichnis) will regelmäßig gepflegt werden. Das vorliegende Papier zeigt auf, worauf dabei zu achten ist. Zur Beruhigung: Man muss meist nicht alles neu machen.

2.3.1 Organisation

Das Verarbeitungsverzeichnis zu führen ist nach Art. 30 Abs. 1 Satz 1 DSGVO Aufgabe des Verantwortlichen oder seines Vertreters (zu dieser Rolle vgl. Art. 27

DSGVO). Das Verarbeitungsverzeichnis zu führen ist also nicht Sache der oder des (behördlichen) Datenschutzbeauftragten; ihr oder ihm kommen insoweit Beratungs- und Überwachungsaufgaben zu (vgl. Art. 39 Abs. 1 Buchst. a und b DSGVO).

Verantwortliche können ihren Datenschutzbeauftragten zwar die zentrale Verwaltung des Verarbeitungsverzeichnisses zur Aufgabe machen, also das reine „Befüllen" der Felder eines – analog oder digital – vorgehaltenen Formulars (im Folgenden: das Verarbeitungsverzeichnis führende Datenschutzbeauftragte). Die Inhalte muss der Verantwortliche aber selbst erarbeiten (lassen). Die oder der behördliche Datenschutzbeauftragte im Nebenamt sollte übrigens auch im Hauptamt keine Verzeichniseinträge verfassen, weil es andernfalls leicht zu Interessenkonflikten kommen kann.

Vor diesem Hintergrund sollte die Führung des Verarbeitungsverzeichnisses mit Bedacht geregelt sein. Interne Vorgaben des Verantwortlichen – etwa in einer Datenschutz-Geschäftsordnung[40] – sollten insbesondere die folgenden Regelungsfragen beantworten:

— Welche Stelle verwaltet das Verarbeitungsverzeichnis (Verwalten: Dokumentieren, Sammeln, Vorhalten)?

— Welche Stelle (zentral) oder welche Stellen (dezentral) erarbeiten die Verzeichniseinträge?

— Wie ist gewährleistet, dass neue Verarbeitungstätigkeiten erkannt sowie entsprechende Einträge erstellt werden?

— Wie ist gewährleistet, dass Änderungen bei Verarbeitungstätigkeiten erkannt sowie entsprechende Einträge angepasst werden?

— Wie ist gewährleistet, dass auslaufende Verarbeitungstätigkeiten erkannt sowie entsprechende Einträge angepasst oder gelöscht werden?

— Wie ist sichergestellt, dass die das Verzeichnis führende Stelle von solchen Änderungen erfährt?

— Wie ist sichergestellt, dass nötige Änderungen auch tatsächlich umgesetzt werden?

Was zu tun ist:

Prüfen Sie die internen Regelungen Ihrer öffentlichen Stelle. Finden Sie heraus, ob die vorstehenden Regelungsfragen beantwortet sind und in der Praxis auch gelebt werden.

Ist das nicht der Fall, können Sie als behördliche Datenschutzbeauftragte oder behördlicher Datenschutzbeauftragter

[40] Muster in Bayerisches Staatsministerium des Innern, für Sport und Integration, Arbeitshilfen zur praktischen Umsetzung der Datenschutz-Grundverordnung, der Richtlinie (EU) 2016/680 (Richtlinie zum Datenschutz bei Polizei und Justiz) und des Bayerischen Datenschutzgesetzes für bayerische öffentliche Stellen, Stand 3/2022, S. 21 ff.

- Ihre Ansprechperson beim Verantwortlichen auf festgestellte Defizite hinweisen,

- Regelungsvorschläge machen,

- insbesondere bei einem „Vollzugsdefizit“: datenschutzverantwortliche Führungskräfte für ihre Aufgaben in Bezug auf das Verarbeitungsverzeichnis sensibilisieren (in Absprache mit der Leitung der öffentlichen Stelle).

Wenn Sie beim Verantwortlichen für die Gestaltung der Datenschutz-Geschäftsordnung zuständig sind, sollten Sie aktiv werden – möglichst, bevor die oder der behördliche Datenschutzbeauftragte Sie dazu auffordert.

Was behördliche Datenschutzbeauftragte nicht tun sollten:

Wenn Sie behördliche Datenschutzbeauftragte oder behördlicher Datenschutzbeauftragter sind, sollten Sie sich vom Verantwortlichen nicht dazu überreden lassen, eine fällige Überarbeitung des Verarbeitungsverzeichnisses allein zu stemmen – und zwar auch dann nicht, wenn Sie sich das grundsätzlich zutrauen. Ausgenommen ist eine zentrale Berichtigung der Informationen nach Art. 30 Abs. 1 Satz 2 Buchst. a DSGVO, die oftmals für alle Verarbeitungstätigkeiten identisch sind.

2.3.2 Einzelne Verzeichniseinträge

2.3.2.1 Neue, geänderte oder auslaufende Verarbeitungstätigkeiten (Art. 30 Abs. 1 Satz 1 DSGVO)

Der Bestand an Verarbeitungstätigkeiten ist bei vielen bayerischen öffentlichen Stellen Schwankungen unterworfen. Dabei kann es sich um **quantitative Schwankungen** handeln (neue und auslaufende Verarbeitungstätigkeiten).

Neue Verarbeitungstätigkeiten können sich insbesondere durch **Änderungen Aufgaben zuweisender Rechtsnormen** ergeben (Beispiel: Regelung in einem Gesetz oder einer Verordnung, dass bestimmte staatliche Behörden das Bewilligungsverfahren für eine neue Leistung durchführen sollen). Im Bereich der Gemeinden ist bei **Übernahme einer zusätzlichen freiwilligen Aufgabe** (vgl. Art. 6 Abs. 1 Satz 1, Art. 7 Abs. 1 Gemeindeordnung – GO) stets zu fragen, ob sich Auswirkungen auf das Verzeichnis der Verarbeitungstätigkeiten ergeben. Gleiches gilt bei **Aufgabenübertragungen von einem anderen Rechtsträger** (Beispiele: Übertragung durch Zweckvereinbarung, Art. 7 Abs. 2 Gesetz über die kommunale Zusammenarbeit – KommZG; Übertragung an einen Zweckverband, Art. 17 Abs. 1 KommZG; Übertragung an ein Kommunalunternehmen, Art. 89 Abs. 2 Satz 1 GO, oder an ein Beteiligungsunternehmen, vgl. Art. 87 Abs. 1 Satz 1 Nr. 3 GO, jeweils aus Sicht des Übertragungsempfängers).

Auslaufende Verarbeitungstätigkeiten kommen insbesondere dann vor, wenn eine öffentliche Stelle eine Aufgabe überträgt (siehe die oben aus Sicht des Übertragungsempfängers gebildeten Beispiele), eine freiwillige Aufgabe nicht mehr wahrnimmt oder der Gesetzgeber eine Aufgabe abschafft. In diesen Fällen ist der Eintrag im Verarbeitungsverzeichnis nicht sofort zu löschen, sondern den geänderten Verhältnissen anzupassen. Aus ihm muss zumindest ersichtlich werden,

dass der Verantwortliche die auslaufende Aufgabe ab einem bestimmten Zeitpunkt nicht mehr wahrnimmt. Zudem kann es insbesondere erforderlich sein, eine vorgeschriebene oder zumindest erlaubte Speicherung von personenbezogenen Daten abzubilden, die bisher bei der Verarbeitungstätigkeit angefallen sind (Beispiel: Eine Gemeinde hat die bisher selbst wahrgenommene Aufgabe, Ordnungswidrigkeiten im ruhenden Verkehr zu verfolgen, auf einen Zweckverband übertragen; aus dem Eintrag im Verarbeitungsverzeichnis sollte hervorgehen, ab welchem Zeitpunkt die Gemeinde diese Aufgabe nicht mehr wahrnimmt und unter welchen Bedingungen alte „Knöllchen-Vorgänge" bei der Gemeinde gespeichert bleiben.)

Sie sollten jedoch auch an **qualitative Schwankungen** denken, die mitunter gar nicht so leicht zu erkennen sind. Gerade wenn ein Verantwortlicher bei der Beschreibung von Verarbeitungstätigkeiten eine eher globale Betrachtung gewählt hat (Beispiel: Bildung einer Verarbeitungstätigkeit „Führung des Melderegisters" anstelle gesonderter Verarbeitungstätigkeiten für einzelne Verwaltungsprodukte der Meldebehörde), sollten Änderungen im rechtlichen Rahmen für die Verarbeitungstätigkeit routinemäßig darauf überprüft werden, ob sie für das Verarbeitungsverzeichnis relevant werden (Beispiel: Einführung eines neuen Übermittlungstatbestandes in der Meldedatenverordnung, der sich im Verarbeitungsverzeichnis bei den nach Art. 30 Abs. 1 Satz 2 Buchst. d DSGVO zu dokumentierenden Kategorien von Empfängern auswirkt).

Was zu tun ist:

Wenn die nötigen organisatorischen Vorkehrungen getroffen sind (siehe Nr. 2.3.1), Ihr Verarbeitungsverzeichnis aber dennoch seit der erstmaligen Erstellung eingestaubt (Akte) oder ungeöffnet ist (Datei), können Sie in der Rolle einer oder eines das Verarbeitungsverzeichnis führenden behördlichen Datenschutzbeauftragten

— die datenschutzverantwortlichen Führungskräfte um die selbstständige Überprüfung der jeweils „eigenen" Einträge bitten; zu diesem Zweck stellen Sie jeweils einen (vermeintlich) aktuellen Auszug aus dem Verarbeitungsverzeichnis zur Verfügung (in Absprache mit der Leitung der öffentlichen Stelle);

— Ihre Ansprechperson beim Verantwortlichen bitten, bei der Behördenleitung verfügbare Informationen über Änderungen im Aufgabenbestand zur Verfügung zu stellen;

— im kommunalen Bereich proaktiv die Tätigkeit des Selbstverwaltungsgremiums beobachten, die solche Änderungen oftmals erkennen lässt (Beispiel: Übernahme neuer freiwilliger Aufgaben);

— einzelne (insbesondere „änderungsverdächtige") Einträge initiativ prüfen und bei Feststellung von Defiziten nachdrücklich auf eine Verbesserung der Zuarbeit durch die datenschutzverantwortlichen Führungskräfte hinwirken;

— in einem Tätigkeitsbericht (soweit nach den internen Regelungen vorgesehen) auf (wiederholt festgestellte) Defizite aufmerksam machen.

In der Rolle einer datenschutzverantwortlichen Führungskraft sollten Sie der oder dem behördlichen Datenschutzbeauftragten unaufgefordert zuarbeiten.

2.3.2.2 Namen und Kontaktdaten (Art. 30 Abs. 1 Satz 2 Buchst. a DSGVO)

Namen von Verantwortlichen können sich ebenso ändern wie Namen von behördlichen Datenschutzbeauftragten – die Gründe dafür sind vielfältig. Im Verarbeitungsverzeichnis muss die Änderung des Namens einer Gemeinde ebenso umgesetzt werden wie der Umzug einer Staatsbehörde an einen anderen Standort oder ein Wechsel im Amt der oder des behördlichen Datenschutzbeauftragten.

Was zu tun ist:

Viele Änderungen bei Namen und Kontaktdaten wird eine behördliche Datenschutzbeauftragte oder ein behördlicher Datenschutzbeauftragter auch ohne die Unterstützung des Verantwortlichen mitbekommen. Wenn sie oder er das Verarbeitungsverzeichnis verwalten, kann sie oder er solche Änderungen gleich umsetzen. Datenschutzverantwortliche Führungskräfte sollten sich gleichwohl nicht auf einen solchen „Automatismus" verlassen, sondern die nötigen Informationen zeitnah weitergeben.

2.3.2.3 Verarbeitungszwecke (Art. 30 Abs. 1 Satz 2 Buchst. b DSGVO) sowie Kategorien betroffener Personen und personenbezogener Daten (Art. 30 Abs. 1 Satz 2 Buchst. c DSGVO)

Personenbezogene Daten dürfen bekanntlich nur für einen bestimmten **Zweck** oder mehrere davon verarbeitet werden. Diese Zwecke müssen im Verarbeitungsverzeichnis abgebildet sein. Nun können sich Zwecke im Lauf der Zeit ändern. Das ist bei der zweckändernden Weiterverarbeitung der Fall, bei der das personenbezogene Datum allerdings (meist) in eine andere Verarbeitungstätigkeit „übergeht", im Verarbeitungsverzeichnis also „den Eintrag wechselt". Gerade im öffentlichen Sektor sind die Verarbeitungszwecke allerdings recht weitgehend durch Gesetz oder sonstige normative Vorgaben festgelegt. Dieser Rahmen kann sich verändern, insbesondere kann der zuständige Normgeber für bereits vorhandene wie auch für neu hinzukommende Datensätze bisherige Zwecke aufgeben (seltener) oder zusätzliche festlegen (häufiger). Im Melderecht beispielsweise ist jede Einführung weiterer regelmäßiger Datenübermittlungen grundsätzlich geeignet, die Zweckbestimmung des Meldedatensatzes zu erweitern.

Auch die von einer Verarbeitungstätigkeit **betroffenen Personen** sowie erfassten **personenbezogenen Daten** können Änderungen unterworfen sein. Im öffentlichen Sektor folgt auch dies meist aus einer Fortentwicklung des normativen Rahmens. Im Melderecht beispielsweise würden weitere Kategorien betroffener Personen in eine Verarbeitungstätigkeit einbezogen, wenn eine Meldepflicht für einen Personenkreis neu begründet wird, der bislang nicht von einer solchen Pflicht erfasst war; bei Einführung eines einzigen neuen Merkmals im gesetzlich festgelegten Meldedatensatz wäre die Verarbeitungstätigkeit um eine weitere Kategorie personenbezogener Daten erweitert.

Was zu tun ist:

Die für eine zeitgerechte Abbildung neuer, geänderter oder auslaufender Verarbeitungstätigkeiten empfohlenen Maßnahmen (Nr. 2.3.2.1) sollten mögliche Änderungen durch zuständige Normgeber bei den Zwecken, den Kategorien betroffener Personen oder den erfassten personenbezogenen Daten einschließen.

In der Rolle einer oder eines das Verarbeitungsverzeichnis führenden behördlichen Datenschutzbeauftragten sollten Sie datenschutzverantwortliche Führungskräfte auch dafür sensibilisieren, insofern für das Verarbeitungsverzeichnis relevante Änderungen frühzeitig zu erkennen und mitzuteilen.

In der Rolle einer datenschutzverantwortlichen Führungskraft sollten Sie die oder den behördlichen Datenschutzbeauftragten gegebenenfalls vorausschauend unterstützen.

2.3.2.4 Kategorien von Empfängern (Art. 30 Abs. 1 Satz 2 Buchst. d DSGVO)

Im Verarbeitungsverzeichnis sind Kategorien von Empfängern zu dokumentieren; dabei gelten die Hinweise unter Nr. 2.3.2.3 entsprechend. Zu bedenken ist, dass der Rechtsprechung zufolge bei einer Auskunft nach Art. 15 Abs. 1 DSGVO auf Wunsch der betroffenen Person anstelle der Empfängerkategorie grundsätzlich die (bereits) bekannten konkreten Empfänger anzugeben sind.[41] Da eine Funktion des Verarbeitungsverzeichnisses darin besteht, Auskünfte nach Art. 15 Abs. 1 DSGVO vorzubereiten,[42] kann es sinnvoll sein, konkrete Empfänger mit ihrem Bekanntwerden auch an dieser Stelle festzuhalten. Der Verpflichtung nach Art. 30 Abs. 1 Satz 2 Buchst. d DSGVO kann auch auf diese Weise genügt werden.

2.3.2.5 Übermittlungen an ein Drittland (Art. 30 Abs. 1 Satz 2 Buchst. e DSGVO)

Ist das Verarbeitungsverzeichnis unter dem Gesichtspunkt von Art. 30 Abs. 1 Satz 2 Buchst. e DSGVO gut gepflegt, wird nicht nur erkennbar, in welchem Umfang der Verantwortliche Drittlandtransfers veranlasst oder (insbesondere durch Auftragsverarbeiter) zugelassen hat. Möglich werden auch Rückschlüsse, in welchen Drittländern sich bei welchen Verarbeitern Datenbestände aufbauen, die jedenfalls im Geltungsbereich der Datenschutz-Grundverordnung nicht ohne weiteres verknüpft werden dürfen. Für betroffene Personen, denen unter Zuhilfenahme des Verarbeitungsverzeichnisses Auskunft erteilt wird, sind solche Angaben bedeutsam, weil Drittlandtransfers „von außen“ nicht ohne weiteres zu erkennen sind und oftmals mit Risiken einhergehen, denen der Verantwortliche mit kompensatorischen Maßnahmen begegnen muss.[43]

Bei Verarbeitungstätigkeiten „im Bestand“ können Drittlandtransfers nicht nur in dem einfach erkennbaren Fall erstmals auftreten, dass der Verantwortliche ein „transferfreies“ Betriebsmittel gegen ein „transferbelastetes“ austauscht. Leichter zu übersehen sind Konstellationen, in welchen Auftragsverarbeiter eine ihnen rechtlich nicht verschlossene Option nutzen, Unterauftragsverarbeiter in einem Drittland zu beauftragen. Auch in solchen Fällen ergeben sich Konsequenzen für die Angaben zu der betreffenden Verarbeitungstätigkeit im Verarbeitungsverzeichnis.

41 Europäischer Gerichtshof, Urteil vom 12. Januar 2023, C-154/21, Rn. 28 ff.

42 Ausführlich mit tabellarischer Übersicht der Synergien Bayerischer Landesbeauftragter für den Datenschutz, Das Recht auf Auskunft nach der Datenschutz-Grundverordnung, Orientierungshilfe, Stand 12/2019, Rn. 97, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018“.

43 Dazu näher Bayerischer Landesbeauftragter für den Datenschutz, Office-Anwendungen aus Drittstaaten bei bayerischen öffentlichen Stellen, Aktuelle Kurz-Information 39, Stand 12/2021, Rn. 16 ff., Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018“.

Was zu tun ist:

Drittlandtransfers fordern die volle Aufmerksamkeit behördlicher Datenschutzbeauftragter wie auch des Verantwortlichen. Eine Einbindung der oder des behördlichen Datenschutzbeauftragten frühzeitig vor der Beschaffung eines Betriebsmittels, das mit einem solchen Transfer verbunden sein kann, und vor Begründung eines Auftragsverarbeitungsverhältnisses, das Drittlandtransfers vorsieht oder zulässt, sollte für bayerische öffentliche Stellen eine Selbstverständlichkeit sein. Dann kann die oder der behördliche Datenschutzbeauftragte den Punkt „Fortschreibung des Verarbeitungsverzeichnisses" auch insofern gleich bei der Beratung berücksichtigen.

Im Übrigen sollten Beschwerden betroffener Personen, Kontakte mit der Datenschutz-Aufsichtsbehörde und sonstige Erkenntnisse zu Drittlandtransfers für behördliche Datenschutzbeauftragte stets Anlass sein, den Eintrag im Verarbeitungsverzeichnis für die betroffene Verarbeitungstätigkeit kritisch zu überprüfen und – soweit erforderlich – bei dem Verantwortlichen auf eine Anpassung hinzuwirken.

Hilfreich kann es für behördliche Datenschutzbeauftragte auch sein, einen aktuellen Stand zum Umfang von Drittlandtransfers in einen nach der örtlichen Datenschutz-Geschäftsordnung etwa zu erstattenden eigenen Tätigkeitsbericht aufzunehmen und insofern – gegebenenfalls auch für die Öffentlichkeit – Transparenz zu schaffen.

2.3.2.6 Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 Satz 2 Buchst. f DSGVO)

Die im Verarbeitungsverzeichnis „wenn möglich" anzugebenden Fristen für die Löschung der verschiedenen Datenkategorien lassen sich beim Ersteintrag manchmal nach gesetzlichen Vorgaben, mitunter nach fachlichen Standards wie dem Einheitsaktenplan,[44] manchmal aber auch gar nicht angeben – einfach, weil bei Aufnahme einer Verarbeitungstätigkeit noch nicht klar ist, wie lange eine Verarbeitung erforderlich sein wird (vgl. Art. 5 Abs. 1 Buchst. e DSGVO), oder noch auf ausstehende Vorgaben der zuständigen Normgeber gewartet werden muss. In solchen Fällen darf das „wenn möglich" des Gesetzes durchaus als „sobald möglich" verstanden werden.

Was zu tun ist:

Das Verarbeitungsverzeichnis führende behördliche Datenschutzbeauftragte sowie datenschutzverantwortliche Führungskräfte sollten zunächst die Hinweise aus Nr. 2.3.2.1 entsprechend berücksichtigen. Behördlichen Datenschutzbeauftragten sei zudem empfohlen:

— Identifizieren Sie Einträge im Verarbeitungsverzeichnis, die bei diesem Punkt von vornherein defizitär sind. Legen Sie für sich eine Frist für wiederkehrende Kontrollen fest und fragen Sie dann jeweils bei den datenschutzverantwortlichen Führungskräften, ob fehlende normative Vorgaben

[44] Bayerischer Gemeindetag/Bayerischer Städtetag/Bayerischer Landkreistag/Generaldirektion der Staatlichen Archive Bayerns, Einheitsaktenplan für die bayerischen Gemeinden und Landratsämter mit Verzeichnis der Aufbewahrungsfristen, Stand 4/2011, Internet: https://www.gda.bayern.de/publikationen/einheitsaktenplan.

„nachgeliefert“ wurden und/oder die Verwaltungspraxis mittlerweile gezeigt hat, wie lange die betreffenden Kategorien personenbezogener Daten typischerweise benötigt werden. Beraten Sie im Bedarfsfall zu einer internen Festlegung von Löschungsfristen, wenn Vorgaben von außen weiterhin fehlen.

— Halten Sie sich außerdem über die Fortschreibung des Einheitsaktenplans auf dem Laufenden, soweit dieser in Ihrer öffentlichen Stelle anzuwenden ist. Nutzen Sie auch Ihre Beteiligung bei der Erstellung von Löschkonzepten, Anpassungen des Verarbeitungsverzeichnisses anzuregen, und wirken Sie auf die Erstellung solcher Konzepte hin, wenn Ihr Verantwortlicher diese Aufgabe vernachlässigt.

2.3.2.7 Allgemeine Beschreibung der gemäß Art. 32 Abs. 1 DSGVO zu treffenden technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 Satz 2 Buchst. g DSGVO)

Auch die allgemeine Beschreibung der gemäß Art. 32 Abs. 1 DSGVO zu treffenden technischen und organisatorischen Maßnahmen ist bei einschlägigen Änderungen nachzuführen. Können die von Art. 30 Abs. 1 Satz 2 Buchst. g DSGVO geforderten Angaben oftmals durch einen Verweis auf ein nach Art. 43 Abs. 1 Bayerisches Digitalgesetz zu erstellendes Informationssicherheitskonzept in das Verarbeitungsverzeichnis eingeführt werden,[45] ist die Aktualität des Verarbeitungsverzeichnisses sichergestellt, wenn der Verweis dynamisch gestaltet ist und das Informationssicherheitskonzept durch die zuständige Organisationseinheit sukzessive dem Stand der Technik angepasst wird.

2.3.3 Synergien

Bedenken Sie immer: das Aktuell-Halten des Verarbeitungsverzeichnisses ist weder für das Verarbeitungsverzeichnis führende behördliche Datenschutzbeauftragte noch für datenschutzverantwortliche Führungskräfte eine sinnbefreite Arbeitsbeschaffungsmaßnahme. Entsteht ein anderer Eindruck, ist die Datenschutzorganisation bei dem betreffenden Verantwortlichen noch nicht ausreichend optimiert. Das Verarbeitungsverzeichnis nimmt für die Erfüllung der Informationspflichten (Art. 13 und 14 DSGVO) wie auch für die Erteilung von Auskünften über die Metainformationen zu einer Datenverarbeitung (Art. 15 Abs. 1 Halbsatz 2 Buchst. a bis h DSGVO) eine Schlüsselfunktion ein: Wer das Verarbeitungsverzeichnis aktuell hält, hat einige dazu nötige Vorarbeiten bereits geleistet. Dann muss nur noch organisatorisch sichergestellt sein, dass diese Vorarbeiten bei der Erfüllung der Informationspflichten und der Erteilung von Auskünften über die Metainformationen auch genutzt werden können. Die Orientierungshilfe zum Recht auf Auskunft enthält eine tabellarische Übersicht, welche Informationen aus dem Verarbeitungsverzeichnis in den Kontexten „Datenschutzhinweise/Informationspflichten“ und „Auskunftsrecht“ relevant werden.[46]

[45] Arbeitshilfen (Fn. 40), S. 56, Internet: https://www.stmi.bayern.de/sus/datensicherheit/datenschutz/reform_arbeitshilfen/index.php.

[46] Bayerischer Landesbeauftragter für den Datenschutz, Das Recht auf Auskunft nach der Datenschutz-Grundverordnung, Orientierungshilfe, Stand 12/2019, Rn. 97, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018“.

Was zu tun ist:

Prüfen Sie als behördliche Datenschutzbeauftragte, behördlicher Datenschutzbeauftragter oder datenschutzverantwortliche Führungskraft in Ihrer öffentlichen Stelle einmal nach, wie die Informationen im Verarbeitungsverzeichnis, in den Datenschutzhinweisen und bei der Auskunfterteilung untereinander vernetzt sind. Sind alle Synergien genutzt? Wird „Doppelarbeit" vermieden? Sind gar Widersprüche durch eine getrennte „Bewirtschaftung" von Informationsbeständen begünstigt? Wie könnte eine für Ihre öffentliche Stelle effiziente Organisation der Angaben in Verarbeitungsverzeichnis, Datenschutzhinweisen und erteilten Auskünften erreicht werden? Die Fragen verlangen örtliche Antworten – da sind Sie gefordert!

2.3.4 Folgen fehlender Aktualität

Eine öffentliche Stelle, die ihr Verarbeitungsverzeichnis nicht aktuell hält, missachtet zunächst einmal ihre Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO. Wird der Informationsbestand genutzt, können auch Datenschutzhinweise mit der Zeit veralten oder Informationen nach Art. 15 Abs. 1 Halbsatz 2 Buchst. a bis h DSGVO nicht mehr stimmen. Mögliche Folgen sind nicht nur datenschutzaufsichtliche Maßnahmen, sondern auch Rechtsbehelfe betroffener Personen.

Abschließender Hinweis:

Auch wenn im Titel dieses Beitrags von einem **Frühjahrsputz** die Rede ist – eine Pflege des Verarbeitungsverzeichnisses ist natürlich auch zu anderen Jahreszeiten angezeigt: Hauptsache, sie findet statt, und zwar regelmäßig.

2.4 Datenschutz bei Rechtschreibkorrektur im Webbrowser

Im Zuge der Digitalisierung ist die Nutzung von Webbrowsern bei bayerischen öffentlichen Stellen eine Selbstverständlichkeit. Bei Webbrowsern denkt man vorrangig an die Informationsrecherche im World Wide Web – jedoch ist das Einsatzspektrum viel breiter: Immer mehr Desktopanwendungen werden durch Webanwendungen ersetzt, die nur in einem Browser zu nutzen sind. Das gilt etwa für elektronische Akten, cloudbasierte Office-Lösungen und Online-Formulare. Kommen personenbezogene Daten ins Spiel, können Webbrowser schnell zum datenschutzrechtlichen Stolperstein werden, wenn sie eingegebene Daten – unbemerkt – an Dritte übermitteln.

So enthalten moderne Webbrowser in der Regel Funktionen zur Rechtschreib- und Grammatikkorrektur sowie zur Autovervollständigung einzelner Wörter. Solche Funktionen sind datenschutzrechtlich nicht besonders bedenklich, solange die Eingaben lediglich auf dem Gerät (lokal) geprüft oder mit einem lokal vorgehaltenen Wörterbuch abgeglichen werden. Mit der Einbindung cloudbasierter Künstlicher Intelligenz (KI), die für optimierte Korrekturleistungen Texteingaben an Dritte übermittelt, ändert sich aber die datenschutzrechtliche Bewertung.

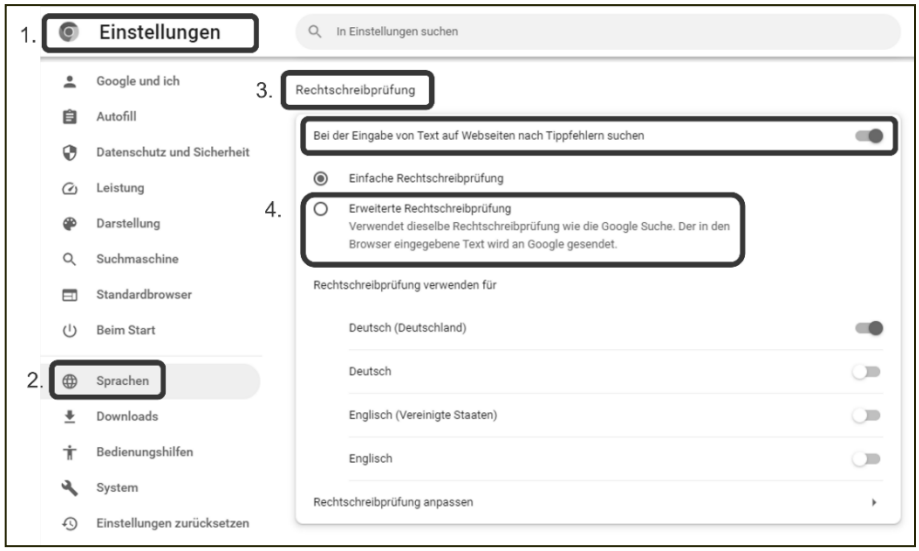
2.4.1 KI-Unterstützung bei Webbrowser-Funktionen

Durch den Einsatz von KI und Maschinellem Lernen (ML) können auf Basis von Sprachmodellen fließende, grammatisch vertretbare Sätze und sogar ganze Satzgefüge generiert werden. Sprachmodelle nutzen dazu statistische Eigenschaften von Texten, wie die Häufigkeit von Wörtern und Wortfolgen (Phrasen). Die Funktionalität von Sprachmodellen entwickelte sich mit Anwendungen der jüngsten Generation – wie beispielsweise ChatGPT – sprunghaft weiter, so dass Sprachmodelle in kurzer Zeit erheblich an Relevanz gewannen. Das Interesse der Anwendungsanbieter ist hoch, die Texteingabe durch **KI-Unterstützung** zu erleichtern und die Qualität von Korrekturvorschlägen zu verbessern. Allerdings wird die zugehörige KI-Anwendung nicht mehr lokal auf dem Gerät des Nutzenden installiert; die Datenverarbeitung erfolgt vielmehr regelmäßig mittels eines Web- oder Cloud-Diensts. Dazu werden die eingegebenen Daten zum Generieren von Korrekturvorschlägen mithilfe des Webbrowsers **an den Anwendungsanbieter, also einen Dritten, übermittelt**. Insbesondere die dazugehörige Formulierung in den Einstellungen von Google Chrome – „Bei der Eingabe von Text auf Webseiten nach Tippfehlern suchen" – mag den Verantwortlichen zu der Annahme verleiten, die Rechtschreibkorrektur-Funktion betreffe lediglich klassische Webseiten „draußen" im World Wide Web und nicht auch Fachanwendungen wie die elektronische Akte:

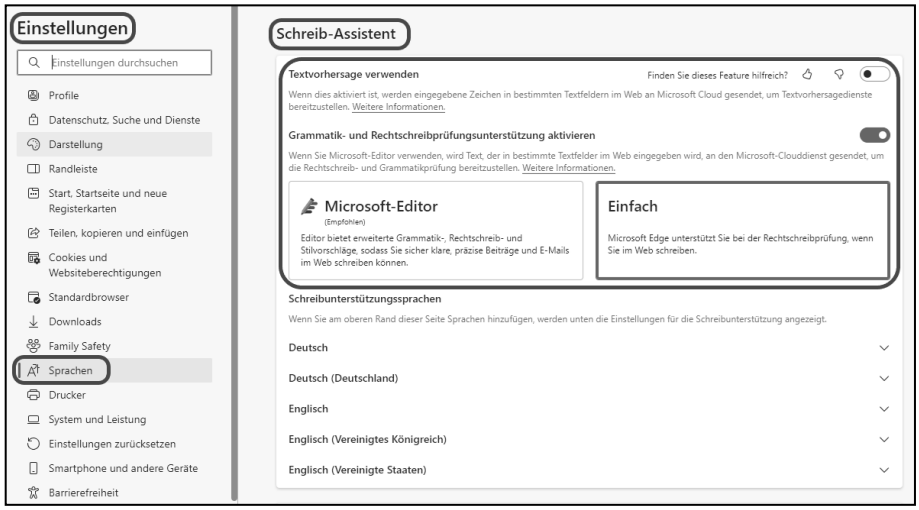
Der Browser kennt diese Unterscheidung allerdings grundsätzlich nicht: Für ihn ist jeder Inhalt eine „Webseite". Wenn also eine ausschließlich zur internen Nutzung gedachte Webanwendung einen Texteditor oder Formularfelder zur Texteingabe enthält, kommt die Rechtschreibkorrektur hierfür in der Regel ebenso zur Anwendung wie bei irgendeinem im Internet frei zugänglichen Webformular. Die Korrektur findet dabei möglicherweise bereits ganz unauffällig im Hintergrund während der Eingabe statt, also ohne Anzeige eines expliziten Hinweises im Webbrowser und ohne bewussten Aufruf einer entsprechenden Funktion durch den Nutzenden.

2.4.2 Einstellungen bei verbreiteten Webbrowsern

Eine „Erweiterte Rechtschreibprüfung" bietet beispielsweise der Webbrowser „Google Chrome": „Der in den Browser eingegebene Text wird an Google gesendet", heißt es in einem separaten Hinweis in den Browser-Einstellungen in der Rubrik „Sprachen" zu dieser Option für die Rechtschreibprüfung. Die „Erweiterte Rechtschreibprüfung" mit der damit einhergehenden Übermittlung von Daten an Google ist jedoch in den Spracheinstellungen nicht standardmäßig aktiviert; stattdessen stellt die „Einfache Rechtschreibprüfung" die Standardeinstellung dar:



Anders verhält es sich beim Webbrowser „Microsoft Edge“: Im Rahmen eines Updates wurde hier die als „Schreib-Assistent“ bezeichnete Schreibhilfe durch eine cloudbasierte KI-Unterstützung namens „Microsoft Editor“ ergänzt. Dieser bietet eine erweiterte Rechtschreibprüfung, eine Grammatikprüfung und Textvorhersagen. So sollen Nutzende schneller und mit weniger Fehlern schreiben können – sie sind sich aber eventuell nicht der Tatsache bewusst, dass Microsoft Edge den eingegebenen Text im Hintergrund an einen Microsoft-Clouddienst sendet, der den Text verarbeitet, um Rechtschreib- und Grammatikfehler zu erkennen. Sofern die Funktion „Textvorhersage verwenden“ aktiviert ist, werden eingegebene Zeichen und Textvorhersagen nach Angabe von Microsoft sogar bis zu 30 Tage lang zwischengespeichert, um die Dienstqualität und Leistung zu verbessern. Entsprechende Hinweise finden sich erst im „Kleingedruckten“ beziehungsweise unter „Weitere Informationen“ zu diesen Funktionen.



Ist der Microsoft-Editor aktiviert, werden Eingaben im Browser (etwa in Formularfeldern) zu Zwecken dieser erweiterten Rechtschreibunterstützung **an Microsoft übermittelt**. Es gibt Hinweise darauf, dass davon sogar Passwörter betroffen sein könnten.[47] Microsoft kennzeichnet den Microsoft Editor nicht nur als empfohlene

47 Otto-JS Research Team, „Chrome & Edge Enhanced Spellcheck Features Expose PII, Even Your Passwords“, 16. September 2022, Internet: https://www.otto-js.com/news/article/chrome-and-edge-enhanced-spellcheck-features-expose-pii-even-your-passwords.

Einstellung beim Verwenden der Schreibunterstützung, **sondern hat ihn automatisch im Zuge eines Updates aktiviert**: Mit der Version 104.0.1293.47 (Stable-Release vom 5. August 2022; Beta-Version: 104.0.1293.14 vom 7. Juli 2022) wurde die intern offenbar als „Text Prediction" bezeichnete Funktionalität, die nach der Dokumentation[48] einen „Microsoft Turing service" genannten Dienst nutzt, per Richtlinie **standardmäßig** aktiviert.[49] So werden die Daten nach diesem Update automatisch im Hintergrund an Microsoft übermittelt. Dies geschieht möglicherweise ohne Wissen und Zutun des Nutzenden und damit **ohne vorherige informierte Einwilligung des Nutzenden oder anderer Betroffener**.

2.4.3 Datenschutzrechtliche Anforderungen

Die Datenübermittlung an einen Browseranbieter wie Google oder Microsoft bedarf einer Rechtsgrundlage, wenn sich eine bayerische öffentliche Stelle bei der Verarbeitung personenbezogener Daten dieser Funktionen zur Rechtschreib- und Grammatikkorrektur bedient (vgl. Art. 6 Abs. 1 DSGVO). Die bayerische öffentliche Stelle handelt hier als Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO, da sie durch die Nutzung der KI-unterstützten Browserfunktion über die Mittel und Zwecke der Datenverarbeitung (jedenfalls: mit-)entscheidet.

Da ein Rückgriff auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO für Behörden bei Erfüllung ihrer Aufgaben wegen Art. 6 Abs. 1 UAbs. 2 DSGVO nicht möglich ist, kommt zunächst als Rechtsgrundlage die Einwilligung in Betracht (Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO). Diese wird allerdings zum Zeitpunkt der Datenverarbeitung regelmäßig nicht vorliegen, da sich die bayerische öffentliche Stelle – wie oben aufgezeigt – der Übermittlung wahrscheinlich nicht bewusst ist und daher hierfür keine Einwilligungsroutine besteht. Eine rückwirkende Genehmigung einer rechtsgrundlosen Datenverarbeitung ist unzulässig. Die Datenübermittlung auf eine – rechtzeitig eingeholte – Einwilligung zu stützen erscheint jedoch auch aus einem anderen Grund fragwürdig: Es ist nicht Aufgabe der Bürgerinnen und Bürger, den Behörden auf diesem Wege den Einsatz eines „bequemeren" Betriebsmittels zu ermöglichen.

Stattdessen könnte als Rechtsgrundlage für die Übermittlung personenbezogener Daten durch eine bayerische öffentliche Stelle – sofern keine spezialgesetzliche Regelung existiert – Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO in Verbindung mit Art. 5 Abs. 1 Satz 1 Nr. 1 Bayerisches Datenschutzgesetz herangezogen werden, wonach die Übermittlung zulässig ist, wenn sie zur Erfüllung einer der übermittelnden oder der empfangenden öffentlichen Stelle obliegenden Aufgabe erforderlich ist. Daran fehlt es.

Der Begriff der Erforderlichkeit ist als Bestandteil von Verarbeitungsbefugnissen, die auf Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO gestützt sind, unionsrechtlich zu verstehen. Er ist im Lichte des unionalen Verhältnismäßigkeitsprinzips zu interpretieren. Geboten ist danach eine Abwägung zwischen den Grundrechten der be-

[48] Referenzdokumentation von Microsoft Edge, Internet: https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-policies#textpredictionenabled.

[49] Versionshinweise zu Microsoft Edge Version 104.0.1293.47 vom 5. August 2022, Internet: https://learn.microsoft.com/de-de/deployedge/microsoft-edge-relnote-archive-stable-channel#version-1040129347-august-5.

troffenen Person einerseits und dem gegenläufigen öffentlichen Interesse andererseits.[50] Eine Verarbeitung personenbezogener Daten ist nicht schon deshalb generell zulässig, weil sie für die Aufgabenerfüllung einer öffentlichen Stelle generell förderlich ist.[51] Eine KI-gestützte Rechtschreibkorrektur mag eine willkommene Hilfe sein; allerdings wird es schlechthin keine öffentliche Aufgabe geben, bei der sich das Interesse an ihrem Einsatz gegen das unionale Datenschutzgrundrecht wie auch das nationale Grundrecht betroffener Personen auf informationelle Selbstbestimmung durchsetzen kann. Dies gilt umso mehr, als eingegebener Text mit der oben erwähnten „Einfachen Rechtschreibprüfung" lokal geprüft werden kann, mithin eine übermittlungsfreie Handlungsalternative zur Verfügung steht. Bequemlichkeit macht keine Erforderlichkeit.

Dass bei einem Browseranbieter aus dem Nicht-EU-Ausland darüber hinaus die Vorgaben zu Datenübermittlungen in Drittstaaten gemäß Art. 44 ff. DSGVO beachtet werden müssen, die infolge des „Schrems II-Urteils"[52] mit nur schwer zu erfüllenden Anforderungen verbunden sind, spielt in Anbetracht der bereits fehlenden Rechtsgrundlage letztlich keine entscheidende Rolle mehr.

2.4.4 Fazit

KI-gestützte Korrekturfunktionen moderner Webbrowser wie Google Chrome und Microsoft Edge mögen für die Erstellung von Texten zwar nützlich sein; bayerische öffentliche Stellen werden für ihren Einsatz aber keine Rechtsgrundlage finden, sobald personenbezogene Daten betroffen sind. Von der Verwendung solcher Funktionen ist daher abzuraten.

Da die betreffende Funktion zumindest im Fall von Microsoft Edge mittels Updates standardmäßig aktiviert wurde, sollten bayerische öffentliche Stellen, die diesen Browser nutzen, die Konfiguration zeitnah überprüfen und gegebenenfalls datenschutzgerecht anpassen.

2.5 Datenpannen mit Microsoft Excel verursachen und vermeiden

Das Tabellenkalkulationsprogramm Microsoft Excel erfreut sich auf Grund seines weiten Funktionsumfangs großer Beliebtheit in Unternehmen und Verwaltungen; auch bei bayerischen öffentlichen Stellen ist es vielfach im Einsatz. Nicht selten begegnen Nutzerinnen und Nutzer dem Programm eher intuitiv; entgegen der primären Zweckbestimmung wird Excel oftmals schon dann eingesetzt, wenn die Spaltenzahl in Word nicht ausreicht. Befinden sich personenbezogene Daten in einer Excel-Arbeitsmappe, kann der nicht sachgerechte Umgang mit der Anwendung allerdings leicht eine Datenpanne auslösen.

Excel bietet auf Grund seiner zahlreichen Funktionen auch viele Möglichkeiten, Datenpannen zu verursachen. Der vorliegende Beitrag kann diesen „Reichtum" nicht ansatzweise abbilden. Er greift lediglich einige wenige Programmfeatures

[50] Vgl. Bayerisches Oberstes Landesgericht, Beschluss vom 6. August 2020, 1 VA 33/20, BeckRS 2020, 18859, Rn. 59.
[51] Vgl. Bayerisches Oberstes Landesgericht, Beschluss vom 6. August 2020, 1 VA 33/20, BeckRS 2020, 18859, Rn. 60.
[52] Europäischer Gerichtshof, Urteil vom 16. Juli 2020, C-311/18.

heraus, die in der Praxis des Bayerischen Landesbeauftragten für den Datenschutz bereits im Zusammenhang mit Datenpannen in Erscheinung getreten sind. Dabei geht es nicht etwa um Schwächen des Programms, sondern um Aspekte, die in der Hektik des Büroalltags hin und wieder schlicht übersehen werden. An allen beschriebenen „Problemstellen" kann es zu einer unbeabsichtigten Offenlegung von personenbezogenen Daten kommen. Excel enthält selbst Sicherheitsvorkehrungen, die allerdings auch genutzt werden müssen. Im Übrigen kann der Verantwortliche für die Sicherheit der bei ihm mit Excel verarbeiteten personenbezogenen Daten einiges tun – damit Datenpannen vermieden werden und nicht zu meldepflichtigen Datensicherheitsverletzungen führen.

2.5.1 Eine Arbeitsmappe – mehrere Arbeitsblätter

Um welches Programmfeature geht es? Beim Aufruf einer Excel-Datei öffnet sich eine Arbeitsmappe, die jedenfalls ein sichtbares Arbeitsblatt enthält; weitere Arbeitsblätter können hinzukommen. Wie viele Arbeitsblätter es sind, zeigen grundsätzlich die Reiter am unteren Rand des Fensters an, die der Navigation zwischen den einzelnen Arbeitsblättern dienen.

Wie kann ich eine Datenpanne verursachen? Sie haben von Ihrer Vorgängerin oder Ihrem Vorgänger mit der Sachgebietsleitung auch eine Excel-Datei mit den dienstlichen Kontaktdaten Ihrer Mitarbeiterinnen und Mitarbeiter übernommen. Diese Datei – genaugenommen: das zuletzt geänderte Arbeitsblatt – befindet sich auf dem Bildschirm gerade vor Ihnen. Es ist die Kontaktliste. Sie tragen Ihre eigenen Daten ein und löschen die Ihrer Vorgängerin oder Ihres Vorgängers. Dann leiten Sie die Datei den Beschäftigten im Sachgebiet per E-Mail zu. Leider hatte sich Ihre Vorgängerin oder Ihr Vorgänger auf dem zweiten, gerade nicht sichtbaren Arbeitsblatt zu allen „Kontakten" Notizen für die nächste dienstliche Beurteilung gemacht. Weil Sie das zweite Arbeitsblatt übersehen haben, sind diese Notizen jetzt im Sachgebiet öffentlich.[53]

Wie kann ich eine solche Datenpanne vermeiden? Machen Sie sich bewusst, dass Excel-Arbeitsmappen mehrere Arbeitsblätter umfassen können (die Anzahl ist nach Angaben von Microsoft übrigens nur durch den verfügbaren Arbeitsspeicher begrenzt[54]) – auch wenn Sie selbst nicht regelmäßig mit solchen „mehrblättrigen" Arbeitsmappen arbeiten.

— Prüfen Sie also vor der Weitergabe einer personenbezogene Daten enthaltenden Excel-Arbeitsmappe an andere, insbesondere vor dem Anhängen an eine E-Mail, ob mehr als ein Arbeitsblatt enthalten ist und wirklich alles weitergegeben werden soll.

— Überlegen Sie außerdem, ob die Datei bei einer Empfängerin oder einem Empfänger noch weiterbearbeitet werden soll – andernfalls ist die Zuleitung einer PDF-Version vorzugswürdig, die sich vor dem Versand leicht auf versteckte Daten kontrollieren lässt.

[53] Vgl. den Fall in Bayerischer Landesbeauftragter für den Datenschutz, 29. Tätigkeitsbericht 2019, Nr. 12.8.2, Internet: https://www.datenschutz-bayern.de, Rubrik „Tätigkeitsberichte".

[54] Microsoft, Spezifikationen und Beschränkungen in Excel, Internet: https://support.microsoft.com/de-de/office/spezifikationen-und-beschränkungen-in-excel-1672b34d-7043-467e-8e27-269d656771c3.

– Seien Sie bei Excel-Dateien, die andere erstellt haben, besonders vorsichtig.

– Löschen Sie aus bestehenden Excel-Arbeitsmappen nach Möglichkeit konsequent die nicht (mehr) benötigten Arbeitsblätter.

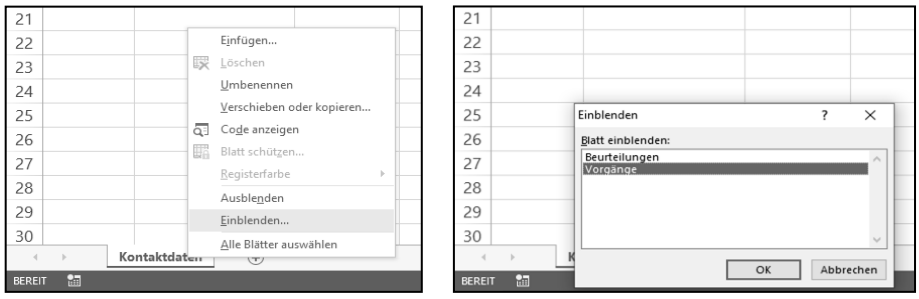
– Überlegen Sie vor der Neuanlage einer Arbeitsmappe mit mehreren Arbeitsblättern, ob Sie die Aufgabe auch mit mehreren Ein-Arbeitsblatt-Arbeitsmappen erledigen können.

– Überlegen Sie außerdem, ob Sie für die zu erledigende Aufgabe Excel benötigen oder ein „schlichteres" Betriebsmittel (etwa ein Textverarbeitungsprogramm) ausreicht.

2.5.2 Sichtbare Arbeitsblätter – unsichtbare Arbeitsblätter

Um welches Programmfeature geht es? Zum Funktionsumfang von Excel gehört das Verstecken von Arbeitsblättern. Dazu klickt man mit der rechten Maustaste den zum Arbeitsblatt gehörenden Reiter an und wählt „Ausblenden".

Wie kann ich eine Datenpanne verursachen? Auf dem gleichen Weg wie unter Nr. 2.5.1 beschrieben. Es ist nur noch weniger Unachtsamkeit erforderlich: Seien Sie ehrlich – wer denkt bei Excel-Arbeitsmappen, die jemand anderes erstellt hat, schon daran, dass verborgene Arbeitsblätter enthalten sein könnten? Das Wieder-Sichtbar-Machen geht übrigens so: Sie klicken mit der rechten Maustaste auf ein sichtbares Arbeitsblatt (eines ist immer da), wählen „Einblenden" (links) und suchen dann die Sie interessierenden Arbeitsblätter aus (rechts; vorausgesetzt, das Datenschutzrecht steht dem nicht entgegen).



Wie kann ich eine solche Datenpanne vermeiden? Merken Sie sich, dass Excel-Arbeitsmappen auch unsichtbare Arbeitsblätter enthalten können. Wenden Sie die Empfehlungen aus Nr. 2.5.1 entsprechend an.

2.5.3 Daten „auf weiter Flur“

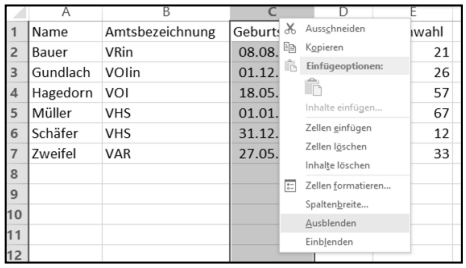
Um welches Programmfeature geht es? Die Leistungsfähigkeit von Excel hängt nicht zuletzt damit zusammen, dass in ein Arbeitsblatt ziemlich viele Daten hineinpassen. Möglich sind in aktuellen Versionen 1.048.576 Zeilen und 16.384 Spalten,[55] also maximal 17.179.869.184 (gut 17 Milliarden) Zellen pro Arbeitsblatt. Und in einer Arbeitsmappe können ja noch mehrere Arbeitsblätter sein …

Wie kann ich eine Datenpanne verursachen? Stellen Sie sich eine Abwandlung des in Nr. 2.5.1 geschilderten Falls vor: Sie haben eine Arbeitsmappe mit tatsächlich nur einem Arbeitsblatt vor sich; in der fünfspaltigen Tabelle sind Ihre 15 Mitarbeiterinnen und Mitarbeiter und Sie selbst aufgeführt. Sie leiten die Datei an alle weiter. Nicht beachtet haben Sie, dass Ihre Vorgängerin oder Ihr Vorgänger in Spalte A bis E ab Zeile 201 eine Kontaktliste für die Schulklasse von Tochter oder Sohn geführt hat und in Spalte AA bis AE, dort ab Zeile 101, eine Kontaktliste für einen Verein, in dem sie oder er Mitglied ist.

Wie kann ich eine solche Datenpanne vermeiden? Sie sollen sich bewusst sein, dass Excel-Arbeitsblätter nicht „auf einen Blick“ überschaubar sein müssen. Ob in der Weite eines Arbeitsblatts noch irgendwo etwas ist, stellen Sie unkompliziert fest, indem Sie bei geöffnetem Arbeitsblatt die Tastenkombination Strg+Ende eingeben. Aktiv ist dann dessen letzte Zelle. Diese Zelle bildet die rechte untere Ecke eines Tabellenrechtecks, in dem sich „irgendwo“ Werte befinden können. Gelangen Sie so im geschilderten Fall zur Zelle AE 290, wissen Sie, dass in den Spalten von A bis AE und in den Zeilen von 1 bis 290 Daten sein können. Sie müssen jetzt nicht alles absuchen. Häufig dürfte es am einfachsten sein, den tatsächlich benutzten Bereich in eine neue Tabelle zu kopieren und mit dieser diszipliniert weiterzuarbeiten.

2.5.4 Ausgeblendete Spalten, Zeilen oder Zellen

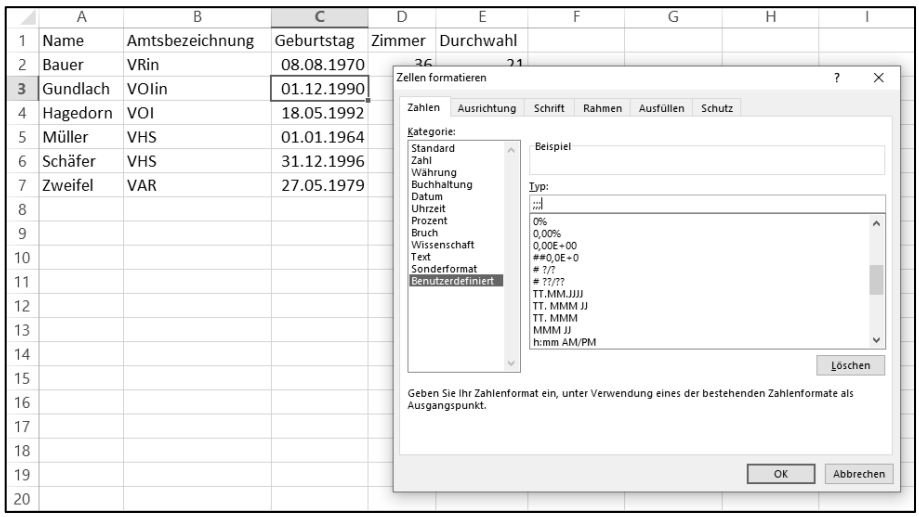
Um welche Programmfeatures geht es? Excel-User haben die Möglichkeit, Spalten, Zeilen oder sogar einzelne Zellen so weit unsichtbar zu machen, dass jedenfalls auf den ersten Blick Daten übersehen werden können. Das Verbergen geht bei **Spalten** oder **Zeilen** so: Sie klicken mit der rechten Maustaste auf den Spaltenbuchstaben oder die Zeilennummer und wählen „Ausblenden“ (links). Dass „etwas da war“, erkennen Sie (nur noch) daran, dass Spaltenbuchstabe oder Zeilennummer ausgespart bleiben (rechts).



[55] Siehe Fn. 54.

Sie können das „Ausblenden“ rückgängig machen, indem Sie die beiden benachbarten Spalten oder Zeilen markieren und mit Hilfe der rechten Maustaste den Befehl „Einblenden“ aufrufen.

Eine vergleichbare Funktion gibt es auch, um einzelne **Zellen** ein Stück weit „unsichtbar“ zu machen. Dazu markieren Sie die betreffenden Zellen, wählen aus dem Menü „Zellen formatieren“ (erreichbar mit der Tastenkombination Strg+1) die Kategorie „Benutzerdefiniert“ und geben als Typ drei Strichpunkte ein.



	A	B	C	D	E
1	Name	Amtsbezeichnung	Geburtstag	Zimmer	Durchwahl
2	Bauer	VRin	08.08.1970	36	21
3	Gundlach	VOIin	01.12.1990		
4	Hagedorn	VOI	18.05.1992		
5	Müller	VHS	01.01.1964		
6	Schäfer	VHS	31.12.1996		
7	Zweifel	VAR	27.05.1979		

Die Werte in den Zellen sind dann ausgeblendet, bleiben aber zumindest in der Formelzeile noch sichtbar (das Datum hier als 33.208. Tag vom 1. Januar 1900 aus gerechnet).

C3 | 33208

	A	B	C	D	E
1	Name	Amtsbezeichnung	Geburtstag	Zimmer	Durchwahl
2	Bauer	VRin	08.08.1970	36	21
3	Gundlach	VOIin		30	26
4	Hagedorn	VOI	18.05.1992	39	57
5	Müller	VHS	01.01.1964	37	67
6	Schäfer	VHS	31.12.1996	35	12
7	Zweifel	VAR	27.05.1979	32	33

Revidiert wird das „Unsichtbarmachen“ durch Zurückändern der Formatierung, hier sinnvollerweise auf einen Typ aus der Kategorie „Datum“.

Wie kann ich eine Datenpanne verursachen? Auch im Fall ausgeblendeter Spalten, Zeilen oder Zellen gilt: aus Versehen ziemlich leicht. Im Arbeitsblatt steht auf den ersten Blick das, was man sieht. Und bevor auffällt, dass da noch mehr ist, befindet sich die Datei bereits bei einem Dritten …

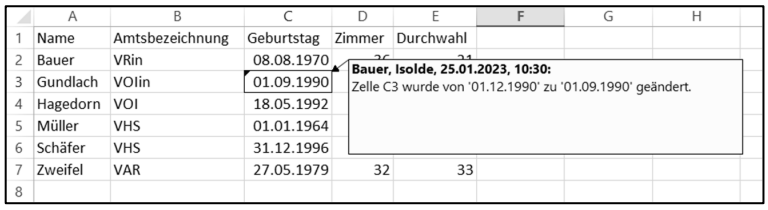
Wie kann ich eine solche Datenpanne vermeiden? Ebenfalls durch Kenntnis der betreffenden Funktionen und etwas Aufmerksamkeit. Insbesondere bei nicht selbst angelegten Arbeitsmappen ist es besser, zweimal hinzuschauen: Ist bei den Spaltenbuchstaben oder den Zeilennummern irgendwo eine Lücke? Oder weist ein Arbeitsblatt scheinbar unerklärliche weiße Stellen auf? Dann sollten Sie zunächst prüfen, ob hier jemand etwas versteckt hat.

Leer kann übrigens auch eine schlecht befüllte Zelle wirken – dann nämlich, wenn beispielsweise beim schlampigen „Herüberkopieren“ von irgendwoher so viele

Leerzeichen „mitgekommen“ sind, dass sie die Tabellenzelle in ganzer Breite ausfüllen.

2.5.5 Metadaten

Personenbezogene Daten können in einer Excel-Datei auch in der Rolle von Metadaten übersehen werden. Das gilt nicht nur für entsprechende Angaben in den Dateieigenschaften (einzusehen unter „Datei – Informationen“; hier ist nicht nur auf „Relevante Personen“ zu achten, sondern auch auf die Freitextfelder unter „Eigenschaften“). Im Menü „Überprüfen“ gibt es mit dem Punkt „Änderungen nachverfolgen – Änderungen hervorheben“ vielmehr auch eine Funktion, die für ausgewählte Zellen eine Protokollierung von Änderungen ermöglicht. Die entsprechenden Zellen erhalten zwar eine Markierung; die Protokollierungsinformationen werden aber nur angezeigt, wenn eine solche Zelle aktiv ist oder der Mauszeiger darüber streicht.



	A	B	C	D	E	F	G	H
1	Name	Amtsbezeichnung	Geburtstag	Zimmer	Durchwahl			
2	Bauer	VRin	08.08.1970					
3	Gundlach	VOIin	01.09.1990					
4	Hagedorn	VOI	18.05.1992					
5	Müller	VHS	01.01.1964					
6	Schäfer	VHS	31.12.1996					
7	Zweifel	VAR	27.05.1979	32	33			
8								

Beachten Sie im Übrigen: Schon ein „sprechender“ Dateiname kann personenbezogene Daten enthalten, die „eigentlich“ gar nicht mitgeteilt werden sollen – etwa das Kürzel der letzten bearbeitenden Person, mit dem diese „ihr Werk“ unverwechselbar machen wollte.

2.5.6 Funktion „Dokumentprüfung“

Einige der angesprochenen „Problemstellen“ von Excel-Dateien lassen sich mit dem Programmfeature „Dokumentprüfung“ leicht erkennen; dies gilt insbesondere für ausgeblendete Spalten oder Zeilen sowie etwa noch vorhandene Metadaten. Auch eine automatische Entfernung ist mit diesem Instrument möglich. Die Dokumentprüfung kann unter „Datei – Informationen“ mit der Schaltfläche „Auf Probleme überprüfen – Dokument prüfen“ angestoßen werden; dabei lassen sich einzelne Punkte des Prüfprogramms zu- oder abwählen. Der Hersteller hat zu dieser Funktion Hinweise veröffentlicht.[56] Die Dokumentprüfung kann übrigens auch bei einigen anderen Microsoft-Produkten wie etwa Word hilfreich sein.

[56] Microsoft, Entfernen von ausgeblendeten Daten und persönlichen Informationen durch Überprüfen von Dokumenten, Präsentationen oder Arbeitsmappen, Internet: https://support.microsoft.com/de-de/office/entfernen-von-ausgeblendeten-daten-und-persönlichen-informationen-durch-überprüfenen-von-dokumenten-päsentationen-oder-arbeitsmappen-356b7b5d-77af-44fe-a07f-9aa4d085966f#ID0EBBF=Excel.

2.5.7 Was der Verantwortliche tun sollte

Der Verantwortliche muss gewährleisten, dass personenbezogene Daten beim Einsatz von Excel sicher verarbeitet werden. Grundlage dafür ist eine **sachgerechte Konfiguration und Administration** der Anwendung. Dabei können Abweichungen von den „Werkseinstellungen" angezeigt sein.[57]

Was die ab Nr. 2.5.1 beschriebenen „Problemstellen" betrifft, sollte der Verantwortliche zum einen **Excel nutzende Beschäftigte ausreichend sensibilisieren**. Das kann im Rahmen von Datenschutzschulungen geschehen. Außerdem sollte der Verantwortliche in einer geeigneten Form (bei bayerischen öffentlichen Stellen etwa in einer Dienstanweisung) **organisatorische Vorkehrungen** treffen, die das Risiko einer unbeabsichtigten Offenlegung personenbezogener Daten durch „Übersehen" scheinbar verborgener Teile von Excel-Arbeitsmappen minimieren. Der vorliegende Beitrag bietet dazu Anregungen. Zu erwägen sind insbesondere Vorgaben, dass

— Excel-Dateien für einen (E-Mail-)Versand grundsätzlich in das PDF-Format umzuwandeln und dann (nochmals) zu kontrollieren sind;

— Excel-Dateien vor einem (E-Mail-)Versand im Ursprungsformat neu anzulegen und/oder standardmäßig mit der Dokumentprüfung, erforderlichenfalls nach einer zusätzlichen Prüfroutine zu prüfen sind.

Auch **„Betriebsmittelkritik"** ist (wie gar nicht selten) sinnvoll: Nicht jede Arbeit mit einer Tabelle muss in Excel erledigt werden, und auch nicht jeder PC-Arbeitsplatz muss mit dieser Anwendung ausgestattet sein.

Eine Excel-Datenpanne kann die **Meldepflicht** nach Art. 33 DSGVO und die **Benachrichtigungspflicht** nach Art. 34 DSGVO auslösen.[58] Das setzt voraus, dass sich die Datenpanne als „Verletzung des Schutzes personenbezogener Daten" im Sinne von Art. 4 Nr. 12 DSGVO darstellt. Nach Auffassung des Bayerischen Landesbeauftragten für den Datenschutz muss dazu ein Verletzungserfolg vorliegen, der auf einem Verletzungsverhalten beruht. Als Verletzungserfolg wird meist eine unbefugte Offenlegung festzustellen sein; daran kann es allenfalls einmal fehlen, wenn die „versehentlich" weitergegebenen Daten dem Empfänger etwa auf Grund einer Einwilligung der betroffenen Person ohnehin mitgeteilt werden durften. Das Verletzungsverhalten kann sich als organisatorisches Fehlverhalten des Verantwortlichen zeigen, wenn etwa der Verantwortliche seine Beschäftigten ohne eine Sensibilisierung für risikoträchtige Programmfunktionen, wie sie in Schulungen oder Dienstanweisungen geleistet werden kann, auf das Betriebsmittel Excel „loslässt" (Ausfallen organisatorischer Standards); das Verletzungsverhalten kann aber auch darin bestehen, dass sich die Beschäftigten eines „sorgfältigen" Verantwortlichen nicht an die ihnen aufgegebenen Vorsichtsmaßnahmen halten (Verfehlen gesetzter organisatorischer Standards im Betrieb). Liegt eine

[57] Bundesamt für Sicherheit in der Informationstechnik (BSI), Sichere Konfiguration von Microsoft Excel, Internet: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_136.html.

[58] Zu den Voraussetzungen sowie zur Erfüllung der Melde- und der Benachrichtigungspflicht ausführlich Bayerischer Landesbeauftragter für den Datenschutz, Meldepflicht und Benachrichtigungspflicht des Verantwortlichen, Stand 6/2019, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018".

Datensicherheitsverletzung vor, richtet sich das Eingreifen von Melde- und Benachrichtigungspflicht nach der dann vorzunehmenden Risikobeurteilung.

Hinweis:

Die Abbildungen in diesem Beitrag dienen nur der Veranschaulichung. Die Frage, was insbesondere aus Sicht des Personaldatenschutzes unter welchen Voraussetzungen zulässig ist (oder niemals zulässig sein kann), ist nicht Thema dieses Beitrags.

2.6 Bayerische öffentliche Stellen und die Windows-Telemetriekomponente

Windows ist ein sehr beliebtes Betriebssystem. Das gilt vor allem für die Versionen 10 und 11, die wohl von weit mehr als einer Milliarde Menschen weltweit genutzt werden. Auch aus der IT-Landschaft bayerischer öffentlicher Stellen ist Windows nicht wegzudenken. Dabei ist für IT-Verantwortliche und Administratoren klar, dass die Sicherheit von Windows-Installationen nicht herstellergegeben ist, sondern – mitunter mühsam – erarbeitet werden muss: Insbesondere funktionierende Firewalls, regelmäßige Updates und eine zielführende, möglicherweise durchaus von den Standardeinstellungen abweichende Konfiguration sind erforderlich, um gegen Angriffe geschützt zu sein.

Bei der üblichen Priorisierung von Maßnahmen gegen Angriffe von außen sind sich vielleicht nicht alle IT-Verantwortlichen und Administratoren bei bayerischen öffentlichen Stellen bewusst, dass Windows selbst – je nach Version, Edition und Einstellungen – unbemerkt und auch unerwünscht Daten an den Hersteller übermitteln kann. Dass Microsoft für solche Datenströme harmlos-technisch klingende Bezeichnungen wie etwa „Telemetrie“, „Diagnosedaten“ oder „Feedback“ wählt, ändert dabei nichts an der Tatsache, dass auch personenbezogene Daten umfasst sein können. Eine Übermittlung personenbezogener Daten „per Telemetrie“ muss genauso rechtmäßig sein wie jede andere Datenübermittlung – im Fall eines Drittlandtransfers nach Maßgabe der dafür zusätzlich zu beachtenden Vorgaben. Die Erfüllung der Rechenschaftspflicht (Art. 5 Abs. 2 Datenschutz-Grundverordnung) ist insofern zumindest anspruchsvoll. Eine im Grundansatz vergleichsweise einfache Alternative liegt darin, die Übermittlung von Telemetriedaten durch geeignete Einstellungen zu unterbinden.

2.6.1 Ausgangslage

Moderne Betriebssysteme wie Windows 10 und 11 bestehen aus einer Vielzahl von Komponenten, Subsystemen, Treibern, Diensten und Dienstprogrammen, die verschiedene Funktionen erfüllen und vielfältig voneinander abhängen. Im konkreten Kontext des Einsatzes bei einer bestimmten bayerischen öffentlichen Stelle sind manche Systembestandteile essenziell, manche jedoch weniger oder gar nicht relevant für die aufgabenbezogene Funktionalität des spezifischen Systems. Allerdings können einzelne Dienste und Funktionen notwendig darauf angewiesen sein, Informationen nach außen zu kommunizieren oder von dort zu erhalten. Das ist etwa bei der Lizenzverwaltung, bei Malwaredefinitionen, Updates oder Zertifikatswiderrufen der Fall. Dazu treten diese Dienste mit bestimmten „Endpunkten“ in Kontakt, die in der Regel durch Microsoft betrieben werden.

Mit der Übermittlung von Telemetriedaten („Fernmessdaten“) „telefoniert“ das Betriebssystem des Arbeitsplatzes gleichsam „nach Hause“. Telemetrie ermöglicht dem Hersteller, Informationen über die Nutzung und die Leistung des Betriebssystems zu sammeln, aber auch zu Kompatibilitäten (etwa bei Treibern) und Systemabstürzen. Schließlich fallen sogar Informationen an, die strategische Relevanz haben können, so etwa zur Ausbreitung neuer Malware.

Telemetrie hat also grundsätzlich eine sachliche Berechtigung, oft auch einen wenigstens für den Hersteller sinnvollen Zweck – und kann den Datenschutzzielen „Sicherheit“ und „Verfügbarkeit“ dadurch zumindest indirekt dienlich sein. Für den Hersteller ist potenziell eine Vielzahl an Daten relevant. Sein Interesse, möglichst aussagekräftige Daten zu erhalten, ist im Grundsatz nachvollziehbar. Gleichwohl ist aufgrund der „Blackbox“-Eigenschaft und der Komplexität des Betriebssystems grundsätzlich schwer einzuschätzen, welche Daten nun genau übermittelt werden. Verantwortliche Stellen können nicht ohne weiteres feststellen, welche Daten geteilt werden, ob sich personenbezogene Daten darunter befinden, und, wenn ja, welche. Fraglich bleibt zudem, ob der Empfänger die Telemetriedaten auch zu einem anderen Zweck als zur Optimierung des „sendenden“ Betriebssystems nutzt (etwa für das eigene Marketing oder eine eigene Suchmaschine) oder sie gar an Dritte weitergibt, etwa als Trainingsdaten für KI-Produkte.

2.6.2 Editionen und Optionen

In Windows 11 können Sie unter „Einstellungen - Diagnose & Feedback“ auswählen, in welchem Umfang Diagnose- und Nutzungsinformationen an Microsoft gesendet werden sollen:

Abb.: Einstellungsdialog „Diagnose & Feedback“ in Windows 11.

Die Dokumentation zu Windows 11 [59] nennt drei Einstellungsmöglichkeiten für die Sammlung von Diagnosedaten unter Windows 11:

- Diagnosedaten aus (Sicherheit),
- Erforderliche Diagnosedaten senden (Standard),
- Optionale Diagnosedaten senden (Vollständig).

[59] Siehe: https://learn.microsoft.com/de-de/windows/privacy/configure-windows-diagnostic-data-in-your-organization#diagnostic-data-settings.

Die Einstellung „Sicherheit“ lässt sich nicht über die grafische Oberfläche einstellen. Unter Windows 10 gibt es noch die Einstellung „Erweitert“, deren Umfang zwischen „Standard“ und „Vollständig“ liegt.

Bei der Option „Diagnosedaten aus (Sicherheit)“ werden keine Windows-Diagnosedaten vom Gerät gesendet. Diese ist somit die aus Datenschutzsicht empfehlenswerte Option. Die Option „Diagnosedaten aus“ ist jedoch nur für die Windows-Editionen „Enterprise“ und „Education“ verfügbar und kann nur über eine Gruppenrichtlinie oder die Registry gewählt werden, nicht jedoch über das Graphical User Interface (GUI): Wie aus der folgenden Abbildung ersichtlich, wird dort eine Option „Sicherheit“ nicht angeboten.

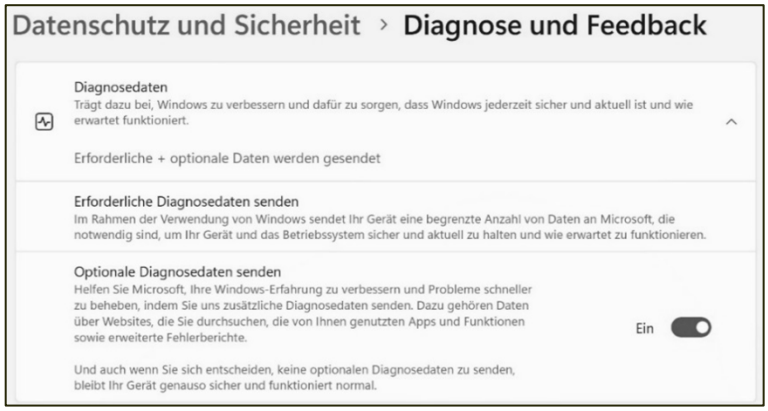


Abb.: Das Windows 11-GUI kann nur „optionale“ Diagnosedaten deaktivieren.

Auf die Gründe für das Weglassen der Option „Sicherheit“ bei den **„Pro“- und „Home“-Editionen** kann an dieser Stelle nicht vertieft eingegangen werden. Jedenfalls kann die Tatsache, dass die Option in diesen Editionen nicht verfügbar ist, für bayerische öffentliche Stellen kleiner und mittlerer Größe relevant sein, da sich die „Pro“-Edition explizit an kleine und mittlere Unternehmen richtet und auch von der öffentlichen Hand eingesetzt wird. Verantwortliche sollten deshalb ihre Möglichkeiten für die Nutzung der „Enterprise“- oder „Education“-Editon ausloten. Die Eigenschaften der „Home“-Edition können eine Rolle spielen, wenn Beschäftigte bayerischer öffentlicher Stellen Privatgeräte dienstlich nutzen (etwa unter bestimmten Voraussetzungen bei Lehrkräften).

2.6.3 Viele Wege führen zum Ziel

Eine **Gruppenrichtlinie** lässt sich mit Hilfe der Gruppenrichtlinien-Verwaltungskonsole einrichten. Die gewünschte Einstellung (vollständige Deaktivierung der Diagnosedaten) kann dort unter „Computerkonfiguration – Administrative Vorlagen – Windows-Komponenten – Datensammlung und Vorabversionen – Diagnosedaten zulassen“ (nächste Abbildung links) ausgewählt werden. Ein wenig irreführend ist, dass zuerst die Gruppenrichtlinie „Diagnosedaten zulassen“ aktiviert werden muss, damit die Option „Diagnosedaten deaktiviert (nicht empfohlen)“ ausgewählt werden kann (nächste Abbildung rechts). Als langjährige Windows-Nutzer wissen Sie aber: Der „Aus“-Button kann sich unter „Start“ verstecken.

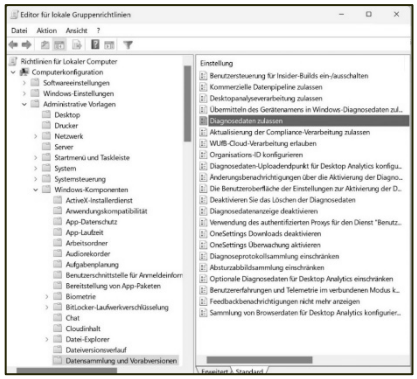


Abb. links: Gruppenrichtlinie für Diagnosedatensammlung
Abb. rechts: Deaktivierung der Diagnosedatensammlung

Alternativ kann die Anpassung auch mittels eines Eintrags in der **Registry** vorgenommen werden: Ändern oder erstellen Sie dazu die REG_DWORD-Registrierungseinstellung namens „AllowTelemetry“ mit dem Wert „0 (Null)“ unter dem Registrierungspfad „Computer\\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\DataCollection“.

2.6.4 Weitere Einschränkungsmöglichkeiten

Die unter Nr. 2.6.2 und 2.6.3 behandelten Windows-Diagnosedaten sind ein prominentes Beispiel für einen eingebauten Datenversand durch Windows. Die erläuterten Einstellungen gelten allerdings nur für Systemelemente, die Windows als eigene ansieht. Windows-Systemkomponenten können im Einzelfall weitere Informationen an Microsoft schicken, die keine Diagnosedaten sind. Zudem sind auch andere Microsoft-Anwendungen (wie etwa Office) gegenüber dem Hersteller nicht völlig schweigsam.

Aus diesen Erwägungen ist zu empfehlen, (vor-)installierte Apps und (standardmäßig) aktivierte Systemdienste systematisch zu prüfen und erforderlichenfalls zu deinstallieren oder zu deaktivieren. Dieses Vorgehen ähnelt dem „Härten“ in der IT-Sicherheit und reduziert die Angriffsfläche. Der radikale Ansatz, schlicht alle Systemdienste, die eine Netzwerkverbindung zu Microsoft aufbauen, ohne weitere Prüfung zu deaktivieren, ist dagegen nicht uneingeschränkt zu empfehlen: Manche Dienste benötigen für den ordnungsgemäßen Betrieb eine Verbindung oder hängen auf eine Art und Weise voneinander ab, dass eine Deaktivierung der Gesamtfunktionalität schaden kann: So könnten etwa nützliche Windows-Updates blockiert werden.

Die Windows-Dokumentation enthält neben Ausführungen zur Deaktivierung von Diagnosedaten eine ganze Reihe **„Hinweise zum Verwalten von Verbindungen zu Microsoft-Diensten“**[60] mit entsprechenden Einstelloptionen. Den Administratoren der „Education“- und „Enterprise“-Editionen gibt Microsoft praktischerweise das **„Windows Restricted Traffic Limited Functionality Baseline“**-Paket[61] (RTLFB) an die Hand, um die durchaus zahlreichen Einstellungen zügig vornehmen zu können. In der Praxis sollten Sie für die entsprechende Windows 11-

[60] Abrufbar unter: https://learn.microsoft.com/de-de/windows/privacy/manage-connections-from-windows-operating-system-components-to-microsoft-services.

[61] Download-Link: https://download.microsoft.com/download/D/9/0/D905766D-FEDA-43E5-86ED-8987CEBD8D89/WindowsRTLFB.zip.

Version die Baseline als Grundlage nutzen und um Anpassungen ergänzen, die auf Ihre Anforderungen und Ihre Systemumgebung zugeschnitten sind.

Vor dem Einsatz müssen alle Auswirkungen genau geprüft und abgewogen werden, da diese Baseline beispielsweise auch die Zeitsynchronisation (sogar innerhalb des eigenen Netzwerks) deaktiviert. Die „Windows Restricted Traffic Limited Functionality Baseline" kann somit insbesondere zu Sicherheits- und damit auch zu Datenschutzmängeln führen, wenn sie unbedacht eingesetzt wird.

Nach eingehender Prüfung bezüglich der Auswirkungen können Sie die **„Windows Restricted Traffic Limited Functionality Baseline"** so anwenden:

— Laden Sie das Windows Restricted Traffic Limited Functionality Baseline-Paket.

— Extrahieren Sie die Datei WindowsRTLFB.zip.

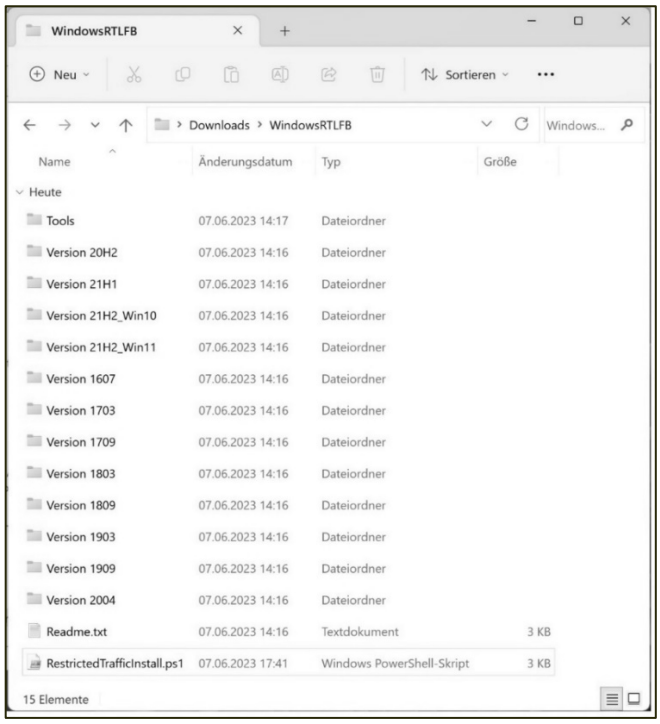


Abb.: Entpacktes Windows RTLFB-Paket

— Nehmen Sie hier eventuell notwendige, behördenspezifische Anpassungen vor. Eine Hilfestellung dazu finden Sie in der Microsoft Dokumentation.[2]

— Laden Sie das „Local Group Policy Object Utility" (LGPO) herunter, welches Teil des Microsoft Security Compliance Toolkits 1.0 ist.

— Extrahieren Sie nun das soeben heruntergeladene Archiv „LGPO.zip" in das Verzeichnis „WindowsRTLFB\Tools\".

— Prüfen Sie, ob das Verzeichnis „WindowsRTLFB" Ihre Windows Version enthält (wie in der Abbildung oben etwa „21H2").

– Führen Sie nun das PowerShell-Skript „RestrictedTrafficInstall.ps1“, das sich im WindowsRTLFB-Verzeichnis befindet, mit Administratorrechten aus (die Systemrechte für das Ausführen von Skripten müssen erforderlichenfalls erteilt werden).

– Starten Sie abschließend Windows neu.

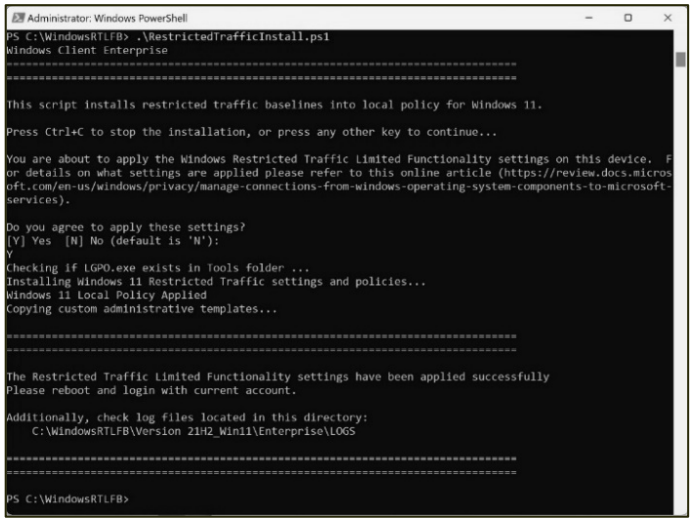


Abb.: Beispielhafte Ausgabe des RestrictedTrafficInstall-Skripts

Sie können die **„Windows Restricted Traffic Limited Functionality Baseline“** in Ihren bestehenden Softwareverteilungsprozess einfügen und die nötigen spezifischen Anpassungen über die Gruppenrichtlinie vornehmen.

Eine Antiviruslösung, die Verfügbarkeit von Updates und die Überprüfbarkeit von Lizenzen sind zwingende Voraussetzungen für den ordnungsgemäßen Betrieb von Windows. Verbindungen zu Microsoft lassen sich somit nicht ohne Weiteres vollständig vermeiden.

Ergänzt man die dargestellten Maßnahmen um eine Antivirus-Lösung eines Drittanbieters, einen Server für die Verteilung von Windows Updates (Windows Server Update Services, WSUS) und ein Windows Key Management Service (KMS), lässt sich damit die Anzahl der Verbindungen zu Microsoft signifikant weiter reduzieren, wenn nicht sogar ganz vermeiden. Diese zusätzlichen Schritte empfehlen sich grundsätzlich für bayerische öffentliche Stellen, die über das dazu erforderliche technische Know-How verfügen, insbesondere aber für Netzwerkumgebungen mit erhöhten Sicherheitsanforderungen (etwa bei der Verarbeitung von personenbezogenen Daten mit erhöhtem Schutzbedarf wie beispielsweise Gesundheitsdaten). Trotzdem ist es insbesondere hier unerlässlich, mögliche Auswirkungen auf den Betrieb und die Sicherheit vorab eigenständig und eigenverantwortlich zu prüfen.

2.6.5 Fazit

Privacy-by-Design und Privacy-by-Default sind Datenschutzziele, die Hersteller möglicherweise anders bewerten und umsetzen als Verantwortliche des öffentlichen Sektors sowie Datenschutz-Aufsichtsbehörden. So sind bayerische öffentli-

che Stellen, die Microsoft Windows in den Versionen 10 und 11 auf ihren Arbeitsplätzen im Einsatz haben, gehalten, ihre Konfiguration zu prüfen und gegebenenfalls nachzubessern.

Immerhin hat Microsoft eine ausführliche und verständliche Dokumentation zu den verschiedenen Diensten und Programmen zur Verfügung gestellt, die eine Verbindung zum Hersteller aufbauen, und darin erläutert, wie eine Telemetriedaten-Übermittlung zum Zweck von Diagnose und Feedback abgestellt werden kann – wenngleich das außerhalb der „Enterprise"- und „Education"-Editionen nicht ganz einfach ist.

Für bayerische öffentliche Stellen wird das bereits angekündigte Supportende von Windows 10 am 14. Oktober 2025 und ein damit verbundener Umstieg auf Windows 11 eine gute Gelegenheit sein, sich auch mit dem Thema „Telemetriedaten-Übermittlung" zielführend auseinanderzusetzen.

2.7 Erste Hilfe zum Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework

Am 10. Juli 2023 hat die Europäische Kommission einen **Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework** (deutsch: Datenschutzrahmen EU-USA, im Folgenden: Angemessenheitsbeschluss) erlassen.[62] Damit attestiert sie den Vereinigten Staaten von Amerika (USA) ein **angemessenes Schutzniveau** für personenbezogene Daten, die innerhalb dieses Rahmens aus der Europäischen Union (EU) an US-Unternehmen als Datenimporteure übermittelt werden. Der Angemessenheitsbeschluss ist ein Durchführungsrechtsakt (Art. 291 Abs. 2 Vertrag über die Arbeitsweise der Europäischen Union – AEUV) in der Form eines an die Mitgliedstaaten gerichteten Beschlusses (Art. 288 Abs. 4 AEUV); ihm ist ein besonders geregeltes Verfahren vorangegangen.[63]

Der Erlass des Angemessenheitsbeschlusses beendet eine lange Wartezeit für Verantwortliche in der EU, hatte doch der Europäische Gerichtshof mit seinem „Schrems II"-Urteil[64] den Vorgänger des EU-U.S. Data Privacy Framework, das „EU-U.S. Privacy Shield", beanstandet und so Datenübermittlungen in die USA auf den in der Praxis eher „steinigen" Weg der geeigneten Garantien gemäß Art. 46 DSGVO verwiesen.

Zu internationalen Datentransfers hat der Bayerische Landesbeauftragte für Datenschutz im Mai 2023 eine umfassende Orientierungshilfe[65] veröffentlicht. Die-

62 Commission Implementing Decision of 10. Juli 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, Internet: https://commission.europa.eu/document/download/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en?filename=Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf.

63 Einzelheiten dazu bei Ehmann, Der Weg zum Angemessenheitsbeschluss für das Transatlantic Data Privacy Framework (TDPF), Stand 5/2023, Internet: https://www.rehm-verlag.de/verwaltung/aktuelle-beitraege-datenschutz/datentransfer-in-die-usa-bedeutsam-auch-fuer-die-verwaltung/.

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

65 Vgl. Bayerischer Landesbeauftragter für den Datenschutz, Internationale Datentransfers, Stand 5/2023, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018".

ser Beitrag konzentriert sich daher auf die Erläuterung der Eckpunkte des Angemessenheitsbeschlusses und auf die Darstellung der Folgen für den bayerischen öffentlichen Sektor.

2.7.1 Was ist die Ausgangslage?

Vor dem neuen Angemessenheitsbeschluss wurde die Übermittlung personenbezogener Daten in die USA in erster Linie auf **geeignete Garantien gemäß Art. 46 Abs. 1 DSGVO** gestützt, die der Datenexporteur (der Verantwortliche oder der Auftragsverarbeiter) vorzusehen hat, wobei den betroffenen Personen zugleich durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen müssen.

Diese Garantien können nach Art. 46 Abs. 2 Buchst. c DSGVO insbesondere in sogenannten **Standarddatenschutzklauseln**[66] bestehen, vorausgesetzt, dass die vereinbarten Klauseln tatsächlich auch wirksam sind, ihre Wirksamkeit also nicht durch Rechtsvorschriften oder behördliche Praktiken in den USA beeinträchtigt wird. Eine solche Beeinträchtigung hatte der Europäische Gerichtshof vor allem für Datenübermittlungen angenommen, die etwa in den Anwendungsbereich von Section 702 Foreign Intelligence Surveillance Act of 1978 („FISA")[67] oder von Executive Order 12.333[68] fallen.[69]

Daher mussten Datenexporteure speziell in solchen Fällen **zusätzliche Maßnahmen („supplementary measures")** auswählen, um für die übermittelten Daten ein Schutzniveau zu erreichen, das dem unionsrechtlichen Standard gleichwertig war. In der Regel wurden zusätzliche technische Maßnahmen – wie eine Verschlüsselung oder Pseudonymisierung – benötigt, deren Implementierung für Datenexporteure mit erheblichem Aufwand verbunden war. Schließlich mussten Datenexporteure den Nachweis erbringen, dass eine Aufhebung der Verschlüsselung und/oder Pseudonymisierung durch US-Behörden bei dem jeweiligen US-Vertragspartner ausgeschlossen werden konnte. Sofern im Einzelfall keine effektiven zusätzlichen Maßnahmen implementiert werden konnten, durfte die Übermittlung nicht auf Art. 46 DSGVO gestützt werden.

2.7.2 Wie schafft der Angemessenheitsbeschluss Erleichterung?

Soweit die EU-Kommission durch ihren Angemessenheitsbeschluss bereits festgestellt hat, dass die USA ein angemessenes Schutzniveau für personenbezogene Daten bieten, entfallen für einen Datenexporteur die oben dargestellten (Prüf-) Schritte. Vorausgesetzt ist dabei, dass er die personenbezogenen Daten an ein für

66 Vgl. insbesondere Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, C/2021/3972 (ABl. L 199 vom 7. Juni 2021, S. 31).

67 Zugleich 50 United States Code §§ 1881, 1881a; eingeführt durch FISA Amendments Act of 2008 vom 10. Juli 2008, H.R. 6304, Publ. L. No. 110–261, 122 Stat. 2437; Internet: https://www.govinfo.gov/content/pkg/STATUTE-122/pdf/STATUTE-122-Pg2436.pdf. Zuletzt verlängert bis 31. Dezember 2023 durch FISA Amendments Reauthorization Act of 2017 vom 18. Januar 2018, Publ. L. No. 115–118, 132 Stat. 3; Internet: https://www.congress.gov/115/plaws/publ118/PLAW-115publ118.pdf.

68 Internet: https://www.archives.gov/federal-register/codification/executive-order/12333.html.

69 Europäischer Gerichtshof, Urteil vom 16. Juli 2020, C-311/18, Rn. 171 ff.

das EU-U.S. Data Privacy Framework zertifiziertes US-Unternehmen übermittelt. Der Angemessenheitsbeschluss gilt folglich – wie bereits der vorangegangene Angemessenheitsbeschluss für das EU-U.S. Privacy Shield – **nur partiell** und nicht für alle in den USA ansässigen Datenimporteure. Seine Geltung ist gemäß Art. 45 Abs. 1 Satz 1 DSGVO sachlich auf „spezifische Sektoren" beschränkt (auch sog. sektoraler Angemessenheitsbeschluss). Ist das US-Unternehmen für das EU-U.S. Data Privacy Framework zertifiziert, entfaltet der Angemessenheitsbeschluss dann **unmittelbare Wirkung**; die Datenübermittlung bedarf weder **einer aufsichtsbehördlichen Genehmigung** (vgl. Art. 45 Abs. 1 Satz 2 DSGVO) **noch besonderer Schutzmaßnahmen**.

Da ein Angemessenheitsbeschluss seine Wirksamkeit verlieren kann (vgl. Nr. 2.7.7), sollte ein Datenexporteur stets zunächst die **aktuelle Liste der Angemessenheitsbeschlüsse** der EU-Kommission konsultieren.[70] Sofern der Datenexporteur das Fortbestehen des Angemessenheitsbeschlusses für das EU-U.S. Data Privacy Framework positiv festgestellt hat, können die Daten dann ohne weitere Prüfung bezüglich Kapitel V DSGVO übermittelt werden.

2.7.3 Welche Datenübermittlungen betrifft dies?

Vom EU-U.S. Data Privacy Framework erfasst werden nahezu alle Übermittlungen personenbezogener Daten an US-Unternehmen, die sich im Rahmen eines **Zertifizierungsmechanismus** zur Einhaltung von bestimmten Datenschutzgrundsätzen verpflichtet haben. Voraussetzung für eine Zertifizierung ist, dass das betreffende US-Unternehmen **der Aufsicht der U.S. Federal Trade Commission[71] oder des U.S. Department of Transportation[72]** unterliegt; bei Unternehmen mit mehreren Sparten ist daher denkbar, dass nicht alle Unternehmensbereiche erfasst sind.

Ausgenommen vom Anwendungsbereich des EU-U.S. Data Privacy Framework sind **personenbezogene Daten**, die **im Rahmen journalistischer Aktivitäten** zu Zwecken der öffentlichen Kommunikation gesammelt werden, sowie Informationen aus früher veröffentlichtem Material, das aus Medienarchiven stammt. Solche Daten können somit nicht auf der Grundlage des Angemessenheitsbeschlusses übermittelt werden.

Auch die Übermittlung von **Personaldaten („HR Data")**, die im Rahmen eines Beschäftigungsverhältnisses erhoben werden, ist **nicht automatisch** vom EU-U.S. Data Privacy Framework erfasst; vielmehr muss das US-Unternehmen bei seiner Zertifizierung explizit angeben, dass sich diese auch auf die Übermittlung von Personaldaten beziehen soll. Damit geht insbesondere die Verpflichtung einher, mit den nationalen EU-Datenschutz-Aufsichtsbehörden zusammenzuarbeiten.

Datenexporteure müssen daher prüfen, ob ihre geplanten Datenübermittlungen in den Anwendungsbereich des Angemessenheitsbeschlusses fallen. Aus Gründen der Rechtssicherheit unterhält und pflegt das U.S. Department of Commerce eine Liste, die die US-Unternehmen enthält, die sich gemäß dem EU-U.S. Data

[70] Internet: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de.

[71] Vgl. zur Zuständigkeit insbesondere Annex IV des Angemessenheitsbeschlusses (Fn. 62).

[72] Vgl. zur Zuständigkeit insbesondere Annex V des Angemessenheitsbeschlusses (Fn. 62).

Privacy Framework zertifiziert haben (**„Data Privacy Framework List“**). Dieser Liste kann auch entnommen werden, welche Gesellschaften einer Unternehmensgruppe zertifiziert sind („covered entities“) sowie welche Kategorien personenbezogener Daten („covered data“) beziehungsweise welche Wirtschaftszweige („industries“) umfasst werden. Die Liste sowie weitere Informationen von US-Seite zum EU-U.S. Data Privacy Framework stehen seit dem 17. Juli 2023 auf der Website https://www.dataprivacyframework.gov zur Verfügung.

Zusammengefasst ergeben sich daraus für Datenexporteure des bayerischen öffentlichen Sektors folgende Prüfschritte, die zusätzlich zu den allgemeinen Rechtmäßigkeitsvoraussetzungen zu beachten sind (siehe hierzu Nr. 2.7.5):

- **1. Prüfschritt:** Ist der Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework noch in Kraft?
- **2. Prüfschritt:** Enthält die Data Privacy Framework List den gewünschten Datenimporteur?
- **3. Prüfschritt:** Ist die betreffende Unternehmenssparte des Datenimporteurs von der Zertifizierung umfasst?
- **4. Prüfschritt:** Ist die gewünschte Datenkategorie von der Zertifizierung umfasst?
- **Falls ja:** Drittlandtransfer ist nach Art. 45 DSGVO zulässig.

Datenübermittlungen an US-Unternehmen, die **nicht oder nicht für die gewünschte Übermittlung zertifiziert** sind, müssen (weiterhin) auf **eines der anderen in Art. 44 ff. DSGVO vorgesehenen Übermittlungsinstrumente** gestützt werden.

Dabei gelten allerdings nach Mitteilung der EU-Kommission alle von der US-Regierung **im Bereich der nationalen Sicherheit implementierten Schutzmaßnahmen** unabhängig von den verwendeten Übermittlungsinstrumenten **für alle Datenübermittlungen** im Rahmen der Datenschutz-Grundverordnung an US-Unternehmen. Deshalb können Datenexporteure im Rahmen der Datenübermittlung mithilfe geeigneter Garantien (Art. 46 DSGVO) die von der EU-Kommission im Angemessenheitsbeschluss ausgeführten Bewertungen bei der Prüfung der Wirksamkeit des gewählten Übermittlungsinstruments („Transfer Impact Assessment“) berücksichtigen.[73]

2.7.4 Ab welchem Zeitpunkt können Daten mit Hilfe des EU-U.S. Data Privacy Framework in die USA übermittelt werden?

Personenbezogene Daten können auf Grundlage des EU-U.S. Data Privacy Framework an zertifizierte Unternehmen **von dem Zeitpunkt an** übermittelt werden, zu dem diese vom U.S. Department of Commerce **auf die Data Privacy Framework List** (vgl. Nr. 2.7.3) **gesetzt** wurden. Um weiterhin am EU-U.S. Data

[73] Vgl. EU-Kommission, Fragen und Antworten: Datenschutzrahmen EU-USA, 10. Juli 2023, Internet: https://ec.europa.eu/commission/presscorner/api/files/document/print/de/qanda_23_3752/QANDA_23_3752_DE.pdf; zum Transfer Impact Assessment vgl. Bayerischer Landesbeauftragter für den Datenschutz, Internationale Datentransfers (Fn. 65), Rn. 62 ff..

Privacy Framework teilnehmen zu können, müssen die Unternehmen ihre **Zertifizierung jährlich erneuern**. Sofern ein Unternehmen – aus welchem Grund auch immer – aus dem EU-U.S. Data Privacy Framework ausscheidet, muss es alle Angaben entfernen, die darauf hindeuten, dass es weiterhin am EU-U.S. Data Privacy Framework teilnimmt. Eine regelmäßige Überprüfung der Data Privacy Framework List, die das U.S. Department of Commerce aktuell halten wird, ist Verantwortlichen dringend zu empfehlen, da ohne eine (fort-)bestehende Zertifizierung die Übermittlung nicht weiter auf den Angemessenheitsbeschluss gestützt werden kann.

Das U.S. Department of Commerce wird außerdem ein Verzeichnis der Unternehmen führen, die von der Data Privacy Framework List gestrichen wurden, und der Öffentlichkeit zugänglich machen, wobei auch der Grund für die Streichung angegeben wird.

2.7.5 Was ist dennoch zu tun?

Die Rechtmäßigkeit der Übermittlung personenbezogener Daten in Drittländer bemisst sich nicht allein nach den Art. 44 ff. DSGVO. Stets zu beachten sind auch die **allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 ff. DSGVO. Dazu zählt insbesondere das Erfordernis einer Rechtsgrundlage.** Vor diesem Hintergrund befreit der Angemessenheitsbeschluss die bayerischen öffentlichen Stellen nicht von allen Sorgen – insbesondere bleibt etwa die Prüfung notwendig, ob Verarbeitungsbefugnisse im Fachrecht oder im allgemeinen Datenschutzrecht eine Übermittlung zulassen und erforderlichenfalls die Voraussetzungen für eine Zweckänderung vorliegen. Ist die Übermittlung auf eine Einwilligung gestützt, muss diese auch wirksam sein. Gefordert ist also immer eine „Zwei-Stufen-Prüfung“:[74] zur Rechtsgrundlage (und allen weiteren Anforderungen der Datenschutz-Grundverordnung an die Rechtmäßigkeit) einer Verarbeitung personenbezogener Daten als erster Stufe tritt das Übermittlungsinstrument – im Fall von Art. 45 DSGVO der Angemessenheitsbeschluss – als zweite Stufe.

Vor einer solchen Prüfung sollten bayerische öffentliche Stellen wie bisher auf Grundlage eines Datenschutz-Sicherheitskonzepts die potentiellen Drittlandübermittlungen präzise erfassen (**„know your transfers“**).[75] Dabei ist vor allem auch auf **Weiterübermittlungen** zu achten, wenn zum Beispiel die für den Datenexporteur tätigen US-Auftragsverarbeiter die personenbezogenen Daten an einen Unterauftragsverarbeiter in einem anderen Drittland übermitteln. Schließlich gilt der Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework für solche Weiterübermittlungen nicht.

Um die **Rechenschaftspflicht** gemäß Art. 5 Abs. 2 DSGVO zu erfüllen, müssen bayerische öffentliche Stellen die Zwei-Stufen-Prüfung **dokumentieren**. Aus die-

[74] Zur Zwei-Stufen-Prüfung näher Bayerischer Landesbeauftragter für den Datenschutz, Internationale Datentransfers (Fn. 65), Rn. 10 ff.

[75] Vgl. Europäischen Datenschutzausschuss, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, Version 2.0, Stand 6/2021, Rn. 8 ff., Internet: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de.

sem Grund empfiehlt es sich, gegebenenfalls die Wahl des Übermittlungsinstruments im Verarbeitungsverzeichnis zu aktualisieren beziehungsweise erstmalig zu dokumentieren. Dies geht zwar über die in Art. 30 Abs. 1 Satz 2 Buchst. e DSGVO geforderten Mindestangaben hinaus; die Angabe dient jedoch dem Nachweis, dass die Frage geprüft wurde.

Außerdem müssen bayerische öffentliche Stellen ihre **Datenschutzhinweise** aktualisieren, sofern Datenübermittlungen in die USA nun auf das EU-U.S. Data Privacy Framework gestützt werden sollen, da der Hinweis auf einen Angemessenheitsbeschluss bei Drittlandübermittlungen zu den Pflichtangaben in einer Datenschutzerklärung gehört (vgl. Art. 13 Abs. 1 Buchst. f DSGVO).

2.7.6 Facebook, Microsoft, Google – ab jetzt kein Problem, oder?

Der Erlass des Angemessenheitsbeschlusses für das EU-U.S. Data Privacy Framework bringt auch für bayerische öffentliche Stellen manche Erleichterung mit sich. Allerdings erfassen die Art. 44 ff. DSGVO nur einen Teilaspekt grenzüberschreitender Datenverarbeitungen.

So sind beispielsweise die sich aus dem Urteil des Europäischen Gerichtshofs zum Betrieb einer **Facebook-Fanpage** ergebenden Konsequenzen zu beachten, wonach in der Regel eine **gemeinsame Verantwortlichkeit** des Fanpage-Betreibers zusammen mit Facebook vorliegen wird.[76] Sofern Facebook dem mitverantwortlichen Seitenbetreiber nicht die notwendigen Informationen zur Verfügung stellt, kann dieser seine datenschutzrechtlichen Pflichten, beispielsweise hinsichtlich der Transparenz und der Rechtmäßigkeit der Datenverarbeitung, aber auch die Informationspflichten gemäß Art. 13 DSGVO nicht erfüllen; seiner Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO kann er ebenfalls nicht nachkommen. Daran ändert der neue Angemessenheitsbeschluss nichts.

Ferner ist zu berücksichtigen, dass viele Social Media-Anbieter **Daten auch für eigene Zwecke** erheben, um damit umfangreiche Nutzerprofile zu erstellen und diese kommerziell zu nutzen, insbesondere zur Vermarktung zielgruppenorientierter Werbung. Welche personenbezogenen Daten in welcher Art und Weise konkret verarbeitet werden, bleibt allerdings weitgehend unklar. Der **Vorwurf mangelnder Transparenz** im Hinblick auf die Verarbeitung personenbezogener Daten zu eigenen Zwecken gilt gleichermaßen für Microsoft 365. Bayerische öffentliche Stellen erwarten hier zumindest erhebliche Schwierigkeiten, jederzeit den Rechenschaftspflichten nach Art. 5 Abs. 2 DSGVO nachkommen zu können, da Microsoft beispielsweise nicht vollumfänglich offenlegt, welche Verarbeitungen im Einzelnen stattfinden.[77] Auch insofern bietet der neue Angemessenheitsbeschluss keinen problemlösenden „Generalschlüssel".

Bayerischen öffentlichen Stellen ist folglich weiterhin zu empfehlen, solche Aspekte bei der Wahl ihrer Betriebsmittel zu berücksichtigen.

[76] Europäischer Gerichtshof, Urteil vom 5. Juni 2018, Az. C-210/16.

[77] Vgl. Zusammenfassung des Berichts der Arbeitsgruppe DSK „Microsoft-Onlinedienste" und Abschlussbericht der Arbeitsgruppe DSK „Microsoft-Onlinedienste", Internet: https://www.datenschutz-bayern.de/inhalte/dsk_ent_t.htm.

2.7.7 Ausblick

Ein Jahr nach Bekanntgabe des Angemessenheitsbeschlusses an die Mitgliedstaaten wird die EU-Kommission eine **erste Überprüfung** vornehmen, ob die neuen Mechanismen im US-Recht, die Voraussetzung für den Erlass des Angemessenheitsbeschlusses waren, vollständig umgesetzt wurden und in der Praxis wirksam funktionieren. Je nach Ausgang dieser Überprüfung wird die EU-Kommission insbesondere in enger Abstimmung mit dem Europäischen Datenschutzausschuss über die Häufigkeit künftiger Überprüfungen entscheiden. Gemäß Art. 45 Abs. 3 DSGVO müssen diese **mindestens alle vier Jahre** stattfinden.

Falls die EU-Kommission feststellen sollte, dass für personenbezogene Daten, die auf Grundlage von Angemessenheitsbeschlüssen an Drittländer übermittelt werden, kein angemessenes Schutzniveau mehr besteht, kann sie den betreffenden Angemessenheitsbeschluss widerrufen, abändern oder aussetzen (vgl. Art. 45 Abs. 5 DSGVO). Daneben können Angemessenheitsbeschlüsse vom Europäischen Gerichtshof überprüft und gegebenenfalls für ungültig erklärt werden.

2.8 Datenschutzaufsicht und Kommunalaufsicht

Der Bayerische Landesbeauftragte für den Datenschutz nimmt die Datenschutzaufsicht bei den bayerischen öffentlichen Stellen wahr (vgl. Art. 15 Abs. 1 Satz1 Bayerisches Datenschutzgesetz – BayDSG). Dazu zählen auch öffentliche Stellen des kommunalen Bereichs, insbesondere auf Gemeindeebene. Die Gemeinden sind zugleich einer allgemeinen staatlichen Aufsicht unterworfen, die je nach Aufgabenkreis die Gestalt einer Rechtsaufsicht oder einer Fachaufsicht annimmt. Ungeachtet der Unterschiede im Detail zielen beide Formen der Aufsicht jedenfalls auch darauf ab, dass die beaufsichtigten Stellen hinsichtlich der Rechtmäßigkeit ihres Handelns überwacht und – soweit erforderlich – „auf den rechten Weg gewiesen“ werden.

Dieses Ziel verfolgt die Datenschutzaufsicht für ihren Bereich ebenfalls. Vor diesem Hintergrund wundert es nicht, dass aufsichtführende Stellen gelegentlich Bürgerinnen und Bürgern oder dem Landesbeauftragten gegenüber die Auffassung vertreten, die Ausübung der Rechts- oder Fachaufsicht sei unstatthaft, wenn es um die korrekte Anwendung von Datenschutzrecht gehe. Diese Position mag zwar auf den ersten Blick eine „Doppelbefassung“ vermeiden helfen und so dem Wunsch nach einem „schlanken Staat“ entsprechen; mit dem geltenden Recht steht sie aber nicht in Einklang. Illustriert sei dies am Beispiel der Aufsicht über die Gemeinden.

2.8.1 Verhältnis von Datenschutzaufsicht und Kommunalaufsicht

Die Gemeinden unterliegen in ihrem eigenen Wirkungskreis der Rechtsaufsicht, die bei kreisangehörigen Gemeinden vom Landratsamt, bei kreisfreien Gemeinden von der Regierung wahrgenommen wird. Art. 110 Abs. 1 Satz 1 Gemeindeordnung (GO) bestimmt zum Inhalt der Rechtsaufsicht:

„In den Angelegenheiten des eigenen Wirkungskreises […] beschränkt sich die staatliche Aufsicht darauf, die Erfüllung der gesetzlich festgelegten und übernommenen öffentlich-rechtlichen Aufgaben und Verpflichtungen der Gemeinden und die Gesetzmäßigkeit ihrer Verwaltungstätigkeit zu überwachen (Rechtsaufsicht).“

Soweit „die Gesetzmäßigkeit [der] Verwaltungstätigkeit“ Gegenstand der Rechtsaufsicht ist, bestehen keine inhaltlichen Eingrenzungen dahin, dass bestimmte Rechtsgebiete ausgenommen wären. Auch aus dem Datenschutzrecht lassen sich solche Eingrenzungen nicht ableiten. Normen, welche die Überwachung datenschutzrechtlicher Vorgaben explizit von der Rechtsaufsicht ausnehmen, kennt weder die Datenschutz-Grundverordnung noch das bayerische Landesrecht.

Indem Art. 77 Abs. 1 DSGVO das Recht auf Beschwerde bei einer Aufsichtsbehörde „unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs“ gewährt, erkennt der Normgeber nicht nur an, dass der Rechtsschutz durch die Datenschutz-Aufsichtsbehörde neben den gerichtlichen Rechtsschutz tritt; er macht auch deutlich, dass national bestehende Instrumente der administrativen Selbstkontrolle („verwaltungsrechtliche[r] […] Rechtsbehelf[.]“) in der „Welt der Datenschutz-Grundverordnung“ einen Platz haben oder behalten können. Dem im deutschen Recht als Instrument dieser Art etablierten Antrag auf Einschreiten einer allgemeinen Aufsichtsbehörde stehen die Regelungen zum Beschwerderecht nicht entgegen. Die Wahrnehmung der Rechtsaufsicht erfährt auf verfahrensrechtlicher Ebene mithin ebenfalls keine Eingrenzung.

In die gleiche Richtung weist die in Art. 3 Abs. 1 BayDSG getroffene Regelung. In dieser Vorschrift heißt es:

„Die […] Staatsministerien und […] die Gemeinden […] haben für ihren Bereich die Ausführung der DSGVO, dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen.“

Aus dieser Norm folgt zwar nicht, dass das Bayerische Staatsministerium des Innern, für Sport und Integration als datenschutzrechtlich gesamtverantwortliche Stelle für sämtliche bayerische Kommunen fungiert – dies wäre mit der Gewährleistung der kommunalen Selbstverwaltung (Art. 28 Abs. 2 Satz 1 Grundgesetz, Art. 11 Abs. 2 Satz 2 Verfassung des Freistaates Bayern) kaum zu vereinbaren –; vielmehr nehmen die Kommunen diese Aufgabe je für sich wahr.

Was den Umfang der Rechtsaufsicht betrifft, die nach Art. 110 Abs. 1 Satz 1, 2 GO eine staatliche Aufgabe ist, steht jedoch Art. 3 Abs. 1 BayDSG einer „Ausgrenzung“ der Gesetzmäßigkeitskontrolle im Bereich des Datenschutzrechts entgegen. Nur ein solches Verständnis der Vorschrift stellt sicher, dass die in der Praxis essentielle Regelung zum Beanstandungsrecht des Landesbeauftragten (Art. 16 Abs. 4 BayDSG), das (eben auch) die Rechtsaufsichtsbehörde für eine Korrektur datenschutzwidrigen Verhaltens beaufsichtigter Stellen in Anspruch nimmt, nicht ins Leere läuft.

Für die Fachaufsicht, die jedenfalls auch die Gesetzmäßigkeit der Verwaltungstätigkeit beaufsichtigter Stellen erfasst (Art. 110 Abs. 2 Satz 1 GO: „auch“), gelten diese Überlegungen entsprechend; zu berücksichtigen sind hier allerdings fachspezifische Vorgaben für die Bestimmung der aufsichtführenden Stellen (vgl. Art. 115 Abs. 1 GO).

Insgesamt ist festzuhalten, dass sich Datenschutzaufsicht und Kommunalaufsicht nicht wechselseitig begrenzen, sondern ergänzen; die allgemeine Aufsicht ist durch die fachspezifische Datenschutzaufsicht verstärkt.

2.8.2 Hinweise für die Verwaltungspraxis

Für die Verwaltungspraxis der zur Rechts- und Fachaufsicht im kommunalen Bereich berufenen Stellen gibt der Landesbeauftragte die folgenden Hinweise:

— Kommunalaufsichtsbehörden haben bei der Wahrnehmung der Rechtsaufsicht auf die Gesetzmäßigkeit der Verwaltungstätigkeit im Bereich des Datenschutzrechts genauso Bedacht zu nehmen wie bezüglich jeder anderen einschlägigen Rechtsmaterie.

  Entsprechendes gilt für die zuständigen Aufsichtsbehörden, wenn im Rahmen der Fachaufsicht unter dem Gesichtspunkt des – auch: bereichsspezifischen – Datenschutzrechts die Gesetzmäßigkeit der Verwaltungstätigkeit in Frage steht.

— Die oberen Rechtsaufsichtsbehörden, die oberste Rechtsaufsichtsbehörde sowie vorgesetzte Fachaufsichtsbehörden müssen bei ihrer Tätigkeit ebenfalls dem Umstand Rechnung tragen, dass die Kommunalaufsicht durch ihnen nachgeordnete Stellen die Gesetzmäßigkeit der Verwaltungstätigkeit auch im Bereich des Datenschutzrechts im Blick haben muss.

— Hat eine bayerische Gemeinde möglicherweise Datenschutzrecht nicht beachtet, steht einer betroffenen Person neben dem Beschwerderecht beim Landesbeauftragten und einem eventuellen gerichtlichen Rechtsbehelf auch die Möglichkeit offen, bei der zuständigen Rechts- oder Fachaufsichtsbehörde um allgemein-aufsichtliches Einschreiten nachzusuchen.

  Die betroffene Person kann in diesem Rahmen zwar in der Regel lediglich verlangen, dass die zuständige allgemeine Aufsichtsbehörde nach Ermessen darüber entscheidet, ob und gegebenenfalls auf welche Weise sie von ihren aufsichtlichen Handlungsmöglichkeiten Gebrauch macht.

  Die allgemeine Aufsichtsbehörde darf einen solchen Antrag aber grundsätzlich nicht mit der Erwägung zurückweisen, zur aufsichtlichen Behandlung datenschutzrechtlicher Fragen sei ausschließlich der Landesbeauftragte berufen. Hat eine betroffene Person mit Kenntnis der allgemeinen Aufsichtsbehörde zugleich eine Beschwerde nach Art. 77 Abs. 1 DSGVO erhoben, kann es in Betracht kommen, eine Entscheidung über den Antrag auf aufsichtliches Einschreiten bis zum Abschluss des Beschwerdeverfahrens durch den Landesbeauftragten zurückzustellen.

— Eine Datenschutzbeschwerde beim Landesbeauftragten, ein gerichtlicher Rechtsbehelf gegen die Gemeinde sowie ein Antrag auf Einschreiten bei der Rechts- oder Fachaufsichtsbehörde können grundsätzlich nebeneinander eingelegt oder gestellt werden. Allerdings sollte eine diese Instrumente kumulativ nutzende Person allen für ihr Anliegen in Anspruch genommenen Stellen gegenüber deutlich machen, dass weitere Stellen einbezogen sind. Auf diese Weise kann sie dazu beitragen, eine divergierende Beurteilung desselben Sachverhalts insbesondere durch die Kommunalaufsichtsbehörden und den Landesbeauftragten zu vermeiden.

— Allgemeine Aufsichtsbehörden, die über datenschutzbezogene Anträge auf Einschreiten gegen eine Gemeinde zu entscheiden haben, steht die

Möglichkeit offen, bei dem Landesbeauftragten unter Vortrag von Sachverhalt und eigener Einschätzung um fachliche Unterstützung nachzusuchen. Auch auf diesem Weg kann die bei dem Landesbeauftragten vorhandene Sachkunde für eine zielführende Wahrnehmung der Kommunalaufsicht genutzt werden, wenn es etwa um die Rechtmäßigkeit der Verarbeitung personenbezogener Daten oder die ordnungsgemäße Erfüllung von Betroffenenrechten geht.

2.8.3 Fazit

Wie am Beispiel der Rechts- und Fachaufsicht über bayerische Gemeinden erläutert, begrenzt die Datenschutzaufsicht nicht die allgemeine Aufsicht. Vielmehr liegen hier zwei gangbare Wege, bei den beaufsichtigten Stellen auf die Gesetzmäßigkeit der Verwaltungstätigkeit hinzuwirken, nebeneinander. Je nach Lage des Einzelfalls kann einmal die Datenschutzaufsicht durch die allgemeine Aufsicht, ein anderes Mal die allgemeine Aufsicht durch die Datenschutzaufsicht effektiviert werden. Mit den gebotenen Modifikationen lassen sich die dargestellten Grundsätze auch auf andere Aufsichtsverhältnisse übertragen, nicht nur auf die Bereiche der Landkreise und Bezirke, sondern auch, was andere Körperschaften sowie Anstalten und Stiftungen des öffentlichen Rechts betrifft.

3 Polizei, Justiz, Verfassungsschutz

3.1 Stellungnahme gegenüber dem Bayerischen Landtag zu Datenlöschungen bei der Bayerischen Polizei

Nach Art. 15 Abs. 3 BayDSG können mich der Landtag oder die Staatsregierung unbeschadet meiner Unabhängigkeit ersuchen, zu bestimmten Vorgängen aus meinem Aufgabenbereich Stellung zu nehmen. Im Jahr 2011 war dies beispielsweise im Zusammenhang mit dem sogenannten „Staatstrojaner" der Fall, als mich der Bayerische Staatsminister des Innern bat, die technische Umsetzung der Maßnahmen zur sog. Quellen-TKÜ sowie die Einhaltung der rechtlichen Vorgaben zu überprüfen. Der damalige Prüfbericht ist nach wie vor auf meiner Homepage abrufbar.[78]

Im Herbst 2022 hat mich der Zweite Untersuchungsausschuss des Landtags zur weiteren Aufklärung des NSU-Komplexes[79] (UA „NSU II") um eine Stellungnahme ersucht. Meine Stellungnahme sollte ich dem Ersuchen zufolge „im Rahmen der schon laufenden datenschutzrechtlichen Überprüfung" erstatten.

Anlass für diese bereits initiierte Prüfung waren im Oktober 2021 durchgeführte Datenlöschungen im Ermittlungs- und Analyseunterstützendes System (EASy). EASy steht landesweit allen Ermittlungsdienststellen der Bayerischen Polizei als Fallbearbeitungssystem zur Verfügung. Mit Hilfe von EASy lassen sich ermittlungsrelevante Daten und Sachverhalte, die bereits in unterschiedlichen polizeilichen Quellen (wie beispielsweise als Zeugenaussagen in Vernehmungsprotokollen) vorhanden sind, in eine einheitlich festgelegte Struktur übertragen und insbesondere grafisch darstellen.

Über die Datenlöschungen in EASy hatte mich das Bayerische Landeskriminalamt (BLKA) im Zuge einer Meldung von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DSGVO in Verbindung mit Art. 2 Satz 1, Art. 28 Abs. 1, Abs. 2 Satz 2, Art. 33 BayDSG am 28. Juni 2022 informiert. Das BLKA nahm eine Datenpanne an, da die gelöschten Daten von einem vom damaligen Bayerischen Staatsministerium des Innern, für Bau und Verkehr am 23. November 2015 (Az. IC5-1334.1-438) anlässlich des 3. Parlamentarischen Untersuchungsausschusses des 18. Deutschen Bundestages zur Thematik „NSU" angeordneten sowie im Wesentlichen immer noch geltenden Löschmoratorium umfasst und daher nicht zur Aussonderung bestimmt waren. Das BLKA meldete vor diesem Hintergrund eine Verletzung der Integrität und der Verfügbarkeit der betroffenen Daten.

Da den Mitteilungen des BLKA in diesem Zusammenhang zu entnehmen war, dass an einer Wiederherstellung der gelöschten Daten gearbeitet werde, sah ich mich veranlasst, eine datenschutzrechtliche Prüfung bezüglich der Löschroutinen im Fallbearbeitungssystem EASy der Bayerischen Polizei einzuleiten. Bei dieser Prüfung ging es vor allem um die Frage, ob es sich in datenschutzrechtlicher Hinsicht überhaupt um Löschungen handelt, wenn Daten nach einer fristgerechten Aussonderung aus EASy-Dateien beispielsweise aus Protokolldaten rekonstruiert

78 Internet: https://www.datenschutz-bayern.de/0/bericht-qtkue.pdf.

79 Einsetzungsbeschluss: Landtags-Drucksache 18/22844.

werden können. Meine Prüfung zielte darauf ab, zu klären, ob im Falle umfassender Rekonstruktionsmöglichkeiten die Datenschutzrechte von betroffenen Bürgerinnen und Bürgern grundsätzlich gewahrt werden.

Die bereits laufende Prüfung zu alltäglichen Löschroutinen wies einige Überschneidungen mit den an mich gerichteten Fragestellungen des UA „NSU II“ auf, insbesondere im Hinblick auf das technische Grundverständnis der Anwendung EASy. Daher konnte ich hierzu in großen Teilen Stellung beziehen und dem UA „NSU II“ in meinem Bericht im Frühjahr 2023 letztendlich eine intensive datenschutztechnische Plausibilitätsprüfung der Angaben des BLKA zum fraglichen Löschvorgang präsentieren. Ebenso konnte ich die Fragestellungen meines ursprünglichen Prüfungsanlasses umfassend aufklären. Dabei habe ich unter anderem die Oberfläche des Systems EASy, Auszüge aus den Protokolldaten sowie Auszüge des fehlerhaften Skripts überprüft, das wohl zur unbeabsichtigten vorzeitigen Löschung von Daten beigetragen hat. Gegenstand meiner Prüfung waren des Weiteren das Betriebskonzept sowie das Nutzungs- und Berechtigungskonzept. Diese und weitere für die Prüfung notwendige Informationen wurden im Zuge zweier Vor-Ort-Termine im BLKA und mehrerer begleitender schriftlicher Anfragen eingeholt.

Da die Ergebnisse meiner Prüfung als „Verschlusssache – Nur für den Dienstgebrauch“ eingestuft sind, kann ich zum genauen Inhalt meiner Stellungnahme gegenüber dem UA „NSU II“ keine tiefergehenden Informationen veröffentlichen. Allgemein kann ich aber festhalten, dass die alltäglichen Löschroutinen in EASy die Datenschutzrechte von Bürgerinnen und Bürgern grundsätzlich wahren und es für mich nachvollziehbar wurde, dass die personenbezogenen Daten in EASy technisch gesetzeskonform gelöscht werden.

Wichtig ist mir an dieser Stelle noch zu erwähnen, dass ich im Rahmen meiner Stellungnahme erneut auf meine generell kritische Haltung hinsichtlich der zunehmenden Anzahl an Löschmoratorien, die mit Parlamentarischen Untersuchungsausschüssen einhergehen, hingewiesen habe (siehe auch in meinem 27. Tätigkeitsbericht 2015/2016 unter Nr. 4.3 sowie in meinem 32. Tätigkeitsbericht 2022 unter Nr. 3.5).

3.2 Konzept zur Bearbeitung von Auskunfts- und Löschersuchen durch die Bayerische Polizei

Eine Vielzahl von Anfragen und Beschwerden, die mich rund um die Speicherung von personenbezogenen Daten durch die Bayerische Polizei erreicht haben, betraf wieder das Thema „Auskunft und Löschung aus polizeilichen Dateien“. Die dafür maßgeblichen Bestimmungen finden sich vor allem im Polizeiaufgabengesetz (PAG):

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

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

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

Art. 62 PAG
Berichtigung, Löschung und Verarbeitungseinschränkung von Daten
[…]
(2) [1]In Dateien gespeicherte personenbezogene Daten sind unverzüglich zu löschen und die zu dem Betroffenen geführten Akten zu vernichten, wenn
1. ihre Erhebung oder weitere Verarbeitung unzulässig war,
2. sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen oder
3. bei der zu bestimmten Fristen oder Terminen vorzunehmenden Überprüfung oder aus Anlaß einer Einzelfallbearbeitung festgestellt wird, daß ihre Kenntnis für die speichernde Stelle zur Erfüllung der ihr obliegenden Aufgaben nicht mehr erforderlich ist. Art. 54 Abs. 2 Satz 3 bis 5 gilt entsprechend.

[2]Wurden die Daten übermittelt, ist dem Empfänger die Löschung unverzüglich mitzuteilen.
[…]

In den letzten Jahren konnte ich oftmals keine einheitliche Vorgehensweise feststellen, was den praktischen Umgang der verschiedenen Präsidien der Bayerischen Polizei mit Bürgeranträgen auf Auskunft gemäß Art. 65 PAG und/oder Löschung gemäß Art. 62 PAG aus den komplexen polizeilichen Dateisystemen anging. Daher war die Absicht des Bayerischen Staatsministeriums des Innern, für Sport und Integration zu begrüßen, mit einem zentralen Konzept eine hohe Qualität sowie eine einheitliche Form bei der Bearbeitung von Auskunfts- und Löschersuchen durch die Bayerische Polizei zu gewährleisten. Daneben soll durch die Harmonisierung von Abläufen eine Effizienzsteigerung der Arbeitsprozesse bei der Polizei erzielt werden, was vor dem Hintergrund stetig steigender Zahlen von Auskunfts- und Löschersuchen geboten erscheint. Aus meiner Sicht könnte sich dies insgesamt positiv auf die Bearbeitungsdauer entsprechender Anträge auswirken, was ich ausdrücklich gutheiße, sofern es dadurch keine Einbußen bei der Qualität in der Bearbeitung solcher Bürgerersuchen gibt (zur Bearbeitungsdauer von Auskunftsersuchen bei der Polizei siehe auch meinen 32. Tätigkeitsbericht 2022 unter Nr. 3.2).

Nachdem mir das Innenministerium den Entwurf für ein derartiges Konzept zugesandt hatte, konnte ich dazu umfassend Stellung nehmen. Dabei habe ich unter anderem auf Aspekte hingewiesen, die nach meiner Erfahrung immer wieder zu Beschwerden über die Polizei und zu Anfragen bei mir geführt hatten. Dies betraf beispielsweise die Frage, ob die Polizei auch Kurztexte in der sog. Vorgangsverwaltung (Integrationsverfahren Polizei – IGVP) beauskunften muss, oder wie konkret die Polizei im Rahmen der Auskunftserteilung Empfänger von Datenübermittlungen benennen muss.

Ende 2022 hat mich das Innenministerium schließlich darüber in Kenntnis gesetzt, dass das entstandene „Konzept zur Bearbeitung von Auskunfts- und Löschersuchen nach Art. 65, 62 PAG durch die Bayerische Polizei" in Kraft getreten und von den Polizeipräsidien ab sofort umzusetzen sei.

Wie ich erfreut feststellen konnte, wurden einige meiner Hinweise wie etwa bei der Auskunft zur Festlegung des maßgeblichen Zeitpunkts (Eingang des Antrags) oder bei der Prüfung von Löschungsanträgen zur besonderen Gewichtung der datenschutzrechtlichen Erforderlichkeit im Zusammenhang mit sog. Mitziehfällen (vgl. hierzu in meinem 30. Tätigkeitsbericht 2020 unter Nr. 5.5) berücksichtigt und in das Konzept aufgenommen.

Weitere positive Aspekte sind die nun einheitlich vorgesehene Beauskunftung von IGVP-Kurztexten (beschränkt auf die Daten der antragstellenden Person; siehe hierzu meinen 28. Tätigkeitsbericht 2017/2018 unter Nr. 4.6), die möglichst konkrete Darlegung der Empfänger von Datenübermittlungen anstatt der früheren oftmals nur allgemeinen Aussagen sowie die Offenlegung etwaiger Datenabfragen (zumindest, wenn der Auskunftsantrag eine konkrete Anfrage dazu enthält).

Auch wenn das Konzept gewiss in die richtige Richtung weist, habe ich dem Innenministerium im Februar 2023 den aus meiner Sicht bestehenden Optimierungsbedarf erläutert, insbesondere was die Vorgehensweise bei der Beauskunftung aus Fachdateien betrifft, die nur einzelnen Fachdienststellen zugänglich sind.

Wie das Konzept in der Praxis umgesetzt wird, und ob sich daraus die erhofften Vorteile sowohl für die Bürgerinnen und Bürger als auch für die Polizei ergeben, wird sich im weiteren Verlauf zeigen. Erfahrungsgemäß bedarf es einer gewissen Übergangszeit, bis sich neue Richtlinien bei allen relevanten Stellen etabliert haben.

Die besten Anlässe und Beispiele, um ein gutes Konzept noch besser zu machen, liefert regelmäßig die Praxis. Aus diesem Grund werde ich dem Innenministerium auch weiterhin Hinweise geben, wie das Konzept innerhalb der gesetzlichen Rahmenbedingungen datenschutzfreundlich fortentwickelt werden kann.

3.3 Antrag auf Löschung führt zu weiteren Speicherungen im Vorgangsbearbeitungssystem IGVP

Speicherungen im polizeilichen Vorgangsbearbeitungssystem IGVP werden von mir regelmäßig – aufgrund von Eingaben wie auch von Amts wegen – geprüft (siehe aus den letzten zehn Jahre die Beiträge in meinem 31. Tätigkeitsbericht 2021 unter Nr. 3.5, in meinem 30. Tätigkeitsbericht 2020 unter Nr. 5.4, in meinem 29. Tätigkeitsbericht 2019 unter Nr. 3.2, in meinem 28. Tätigkeitsbericht 2017/

2018 unter Nr. 4.4.1, in meinem 27. Tätigkeitsbericht 2015/2016 unter Nr. 3.6.4 und in meinem 26. Tätigkeitsbericht 2013/2014 unter Nr. 3.5.1).

Einen Fall, bei dem ich aufgrund einer Eingabe tätig wurde, möchte ich beispielshaft schildern:

Eine Anwältin wandte sich im Auftrag ihres Mandanten an mich, der ihn betreffende Speicherungen der Bayerischen Polizei überprüft haben wollte. Zuvor hatte die Anwältin bereits ein Auskunftsersuchen gestellt, das vom zuständigen Polizeipräsidium ordnungsgemäß beantwortet worden war. In dem Schreiben der Polizei wurden eine Speicherung nach Art. 54 Abs. 2 Satz 1 Polizeiaufgabengesetz (PAG) im Kriminalaktennachweis (KAN) und mehrere nach Art. 54 Abs. 1 PAG im IGVP genannt.

Art. 54 PAG
Speicherung, Veränderung und Nutzung von Daten
(1) Die Polizei kann personenbezogene Daten in Akten oder Dateien speichern und anderweitig verarbeiten, soweit dies zur Erfüllung ihrer Aufgaben, zu einer zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung erforderlich ist.
(2) [1]Die Polizei kann insbesondere personenbezogene Daten, die sie im Rahmen strafrechtlicher Ermittlungsverfahren oder von Personen gewonnen hat, die verdächtig sind, eine Straftat begangen zu haben, speichern und anderweitig verarbeiten, soweit dies zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. […]

Im Nachgang wandte sich die Kanzlei erneut an die Polizei, begründete, dass eine Fortsetzung der Speicherungen zur Erfüllung polizeilicher Aufgaben nicht mehr erforderlich sei und beantragte die Löschung der Einträge. Daraufhin löschte die Polizei die Speicherung im KAN. Die Speicherung im IGVP hierzu erhielt sie zu Dokumentationszwecken (Art. 54 Abs. 1 PAG) aufrecht, schrieb allerdings die Personenart von „Beschuldigter“ auf „Auskunftsperson“ sowie die Vorgangsart von „Anzeige“ auf „Meldung“ um. Dieses Vorgehen ist, sofern eine Speicherung etwa zur Dokumentation des polizeilichen Handelns erforderlich ist, aus datenschutzrechtlicher Sicht grundsätzlich vertretbar, da durch die Änderung die bisherige, nunmehr aber weggefallene Beschuldigteneigenschaft nicht mehr genannt wird.

Anlässlich der Beschwerde habe ich die Speicherungen des Petenten im IGVP geprüft. Im Rahmen meiner Prüfung musste ich feststellen, dass das zuständige Polizeipräsidium in IGVP Folgendes gespeichert hatte: „Aufgrund Antrag Löschung personenbezogener Daten aus dem KAN […] wurden […] die KAN-Einträge gelöscht“. Außerdem wurde die oben beschriebene Änderung der Personen- sowie Vorgangsart erwähnt. Es liegt auf der Hand, dass eine solche Vorgehensweise den Sinn und Zweck einer Löschung aus dem KAN sowie der Umbenennung der Personen- und Vorgangsart konterkariert. Nach Darlegung meiner datenschutzrechtlichen Bewertung konnte ich die Löschung des Zusatzes erreichen.

3.4 Privatzonenausblendungen bei Videoüberwachungsmaßnahmen der Polizei

Als ein wesentliches Instrument der Gefahrenabwehr nimmt die polizeiliche Videoüberwachung von öffentlichen Straßen und Plätzen seit Jahren einen immer

größeren Stellenwert in der Polizeiarbeit ein. Daher muss ich mich mit datenschutzrechtlichen Fragen solcher Maßnahmen regelmäßig kritisch beschäftigen (siehe meinen 30. Tätigkeitsbericht 2020 unter Nr. 5.2, meinen 29. Tätigkeitsbericht 2019 unter Nr. 3.5, meinen 28. Tätigkeitsbericht 2017/2018 unter Nr. 4.3, meinen 27. Tätigkeitsbericht 2015/2016 unter Nr. 3.5 sowie meinen 26. Tätigkeitsbericht 2013/2014 unter Nr. 3.4).

Dass die polizeiliche Videoüberwachung von öffentlichen Straßen und Plätzen einen wichtigen Beitrag zur Prävention und zur Aufklärung von Straftaten leisten kann, steht außer Frage. Gleichwohl muss das rechte Verhältnis von Überwachungszweck und Grundrechtsschutz zu jeder Zeit gewahrt werden. Eine offene polizeiliche Videoüberwachung ist unter anderem an gefährlichen Orten unter den Voraussetzungen von Art. 33 Abs. 2 Nr. 2 und Nr. 3 Polizeiaufgabengesetz (PAG) möglich. Grundlage für die Auswahl der zu überwachenden Örtlichkeiten sind dabei konkrete polizeiliche Lageerkenntnisse.

Bei der Erfüllung des polizeilichen Präventionsziels darf der Schutz der Privatsphäre allerdings nicht vernachlässigt werden. Bei einer grundsätzlich rechtmäßigen polizeilichen Datenerhebung mittels Videokamera kann es aufgrund der geografischen Gegebenheiten an öffentlichen Straßen und Plätzen leicht zu einer ungewollten Aufnahme angrenzender Wohn- und Geschäftsbereiche kommen. Soweit Kameras den Innenbereich von Wohnungen erfassen, ist das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 Grundgesetz) beeinträchtigt. Überdies können besondere Kategorien personenbezogener Daten verarbeitet werden, etwa wenn durch die Videoüberwachung der Publikumsverkehr einer Arztpraxis aufgezeichnet wird.

Diesem Problem kann inzwischen durch technische Mittel unkompliziert begegnet werden. Die entsprechenden Erfassungsbereiche werden irreversibel verpixelt beziehungsweise schwarz dargestellt, so dass selbst bei einer schwenkbaren Kamera keine Möglichkeit besteht, den besagten Bereich einzusehen und personenbezogene Daten zu verarbeiten (sogenannte Privatzonenausblendung). So kann einer datenschutzrechtlichen Vorgabe in der Regel ohne Probleme entsprochen werden.

Im Rahmen von Prüfungen stellte ich fest, dass die dauerhaft installierten polizeilichen Videoanlagen am Plärrer und am Königstor in Nürnberg in diesem Punkt anfänglich Schwierigkeiten bereiteten: Zwar war bei beiden Anlagen die Technik der Privatzonenausblendung implementiert. Allerdings konnte die Privatzonenausblendung zunächst anlassbezogen für einen gewissen Zeitraum ausgeschaltet werden. Diese Vorgehensweise habe ich kritisch gewürdigt. Ich konnte schließlich erreichen, dass diese Deaktivierungsoption technisch blockiert wurde und eine Einsichtnahme in Privatzonen somit auch für einzelne Situationen nicht mehr möglich ist.

3.5 Datenschutzrechtliche Prüfung des Abrufs von Daten aus dem Ausländerzentralregister (AZR) im automatisierten Verfahren durch die Bayerische Polizei

Das Ausländerzentralregister (AZR) wird vom Bundesverwaltungsamt betrieben und vom Bundesamt für Migration und Flüchtlinge geführt. Mit seinen rund 26 Millionen personenbezogenen Datensätzen ist das AZR eines der umfangreichsten automatisierten Register der öffentlichen Verwaltung in Deutschland. Es besteht

aus einem allgemeinen Datenbestand und einer Visadatei. Im allgemeinen Datenbestand werden unter anderem Daten von Ausländerinnen und Ausländern gespeichert, die sich längerfristig, also mindestens drei Monate, in Deutschland aufhalten, die einen Asylantrag gestellt haben oder gegen deren Einreise Bedenken bestehen. Die Visadatei enthält die Daten von Visumantragstellerinnen und Visumantragstellern, die im Regelfall nur kurz in Deutschland bleiben.

Gemäß § 22 Abs. 1 Nr. 4 AZR-Gesetz (im Folgenden: AZRG) sowie § 32 Abs. 1 Nr. 4 und 5 AZRG in Verbindung mit § 33 AZRG ist die Bayerische Polizei berechtigt, im automatisierten Verfahren Daten aus dem AZR abzurufen.

Um zu prüfen, ob hierbei die rechtlichen Voraussetzungen des AZR-Gesetzes eingehalten werden, habe ich ein Polizeipräsidium insofern einer anlasslosen datenschutzrechtlichen Kontrolle unterzogen. Zugleich kam ich hiermit meiner gesetzlichen Verpflichtung aus § 34a AZRG nach, hinsichtlich des AZR „regelmäßig die Durchführung des Datenschutzes zu kontrollieren".

Schon zu Beginn meiner Prüfung musste ich feststellen, dass es für die gesamte Bayerische Polizei kein spezielles Berechtigungskonzept für das AZR gab, obwohl § 22 Abs. 3 Satz 3 AZRG ein solches ausdrücklich verlangt. Um eine wirksame Zugangskontrolle zu etablieren und den rechtmäßigen Abruf grundrechtssensibler Daten zu gewährleisten, habe ich daher das Bayerische Staatsministerium des Innern, für Sport und Integration darauf hingewiesen, dass ein entsprechendes Berechtigungskonzept gesetzlich vorzusehen ist. Hierauf teilte mir das Innenministerium mit, das Bayerische Landeskriminalamt (BLKA) über meine ausführlichen Anmerkungen zum Thema „Berechtigungskonzept der Bayerischen Polizei zum Abruf von AZR-Daten im automatisierten Verfahren" unterrichtet zu haben. Zeitgleich sei das BLKA beauftragt worden, ein Berechtigungskonzept für die Bayerische Polizei zeitnah zu erarbeiten.

Auch die Prüfung von AZR-Abrufen gab Anlass zu Kritik. So war eine nicht korrekte Angabe des Abfrageanlasses festzustellen: Bei allen Stichproben war – offensichtlich standardisiert und/oder gewohnheitsmäßig – als Abfrageanlass „asylrechtliche Aufgaben" angegeben. Diese Eingabe führte zur weitestreichenden Einsichtnahme in die gespeicherten Datensätze. Denn der gewählte Abfrageanlass bestimmt den Umfang der Auskunft und dokumentiert gleichzeitig die rechtliche Grundlage. So stehen etwa die Abfrageanlässe „ausländer- oder asylrechtliche Aufgaben" und „Strafverfolgung gegen Betroffenen" oder „Gefahrenabwehr" zur Verfügung. Beim Abfrageanlass „Strafverfolgung" oder „Gefahrenabwehr" werden die angezeigten Datensätze um mögliche Treffer zu freizügigkeitsberechtigten Unionsbürgern bereinigt. Beim Abfrageanlass „asylrechtliche Aufgaben" ist dies jedoch nicht der Fall, so dass hier ein umfangreicherer Datenbestand abgerufen werden kann, der auch alle Speicherungen zu freizügigkeitsberechtigten Unionsbürger umfasst. Zumindest in einem Fall war dies rechtlich nicht zulässig (siehe § 10 Abs. 1a AZRG). Daher habe ich auch diese Vorgehensweise bemängelt und angeraten, Weiterbildungs- und Sensibilisierungsmaßnahmen zu diesem Thema durchzuführen. Gerade bei automatisierten Verfahren ist es erforderlich, sowohl die Einhaltung der rechtlichen Zugangsvoraussetzungen als auch die praktische Handhabung stets im Blick zu behalten. Vor diesem Hintergrund werde ich künftig die polizeilichen Datenabrufe aus dem AZR im Rahmen meiner Möglichkeiten verstärkt kontrollieren.

3.6 Postsicherstellung nach Art. 35 Polizeiaufgabengesetz –turnusmäßige Prüfung

Mit dem PAG-Neuordnungsgesetz wurde das Polizeiaufgabengesetz 2018 um zahlreiche Befugnisse erweitert. So nahm der Gesetzgeber unter anderem die präventivpolizeiliche Postsicherstellung in Art. 35 Polizeiaufgabengesetz (PAG) neu auf.

Art. 35 PAG
Postsicherstellung
(1) [1]Die Polizei kann auf Anordnung durch den Richter ohne Wissen des Betroffenen Postsendungen sicherstellen, wenn sich diese im Gewahrsam von Personen oder Unternehmen befinden, die geschäftsmäßig Post- oder Telekommunikationsdienste erbringen oder daran mitwirken (Postdienstleister), und von einer Person versandt wurden oder an eine Person gerichtet sind,

1. *die für eine Gefahr oder eine drohende Gefahr für ein in Art. 11a Abs. 2 Nr. 1, 2 oder Nr. 4 genanntes bedeutendes Rechtsgut verantwortlich ist, oder*
2. *bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie für eine Person nach Nr. 1 bestimmte oder von dieser herrührende Postsendungen entgegennimmt oder weitergibt und sie daher in Zusammenhang mit der Gefahrenlage steht, ohne diesbezüglich das Recht zur Verweigerung des Zeugnisses nach den §§ 53, 53a StPO zu haben,*

sofern die Abwehr der Gefahr auf andere Weise aussichtslos oder wesentlich erschwert wäre. [2]Postdienstleister haben die Sicherstellung zu ermöglichen und unter den Voraussetzungen des Satzes 1 der Polizei auf Verlangen Auskünfte über derzeit oder ehemals in ihrem Gewahrsam befindliche oder angekündigte Postsendungen zu erteilen.
[…]

In Anbetracht meiner nach Art. 51 Abs. 2 Satz 1 PAG bestehenden Prüfungsverpflichtung hatte ich für den Berichtszeitraum die Prüfung der Befugnis zur Postsicherstellung nach Art. 35 PAG vorgesehen. 2021 war überhaupt keine Postsicherstellung nach dieser Vorschrift angeordnet worden; 2022 kam es zu einer einzigen Anordnung. So wurde lediglich in einem Fall die Sicherstellung von Postsendungen in Form eines Auskunftsersuchens zu Absender- und Empfängerdaten angeordnet. Grundlage hierfür war ein amtsgerichtlicher Beschluss nach Art. 35 Abs. 1 Satz 1 Nr. 1 in Verbindung mit Satz 2 PAG wegen einer konkreten Gefahr für die Gesundheit und das Leben der Kundinnen und Kunden eines Webshops für neue psychoaktive Stoffe.

Zwar untersagt Art. 34 Abs. 2 Satz 2 BayDSG eine datenschutzrechtliche Überprüfung einer Datenverarbeitung, die gerichtlich überprüft wurde. Unabhängig davon lagen die gesetzlichen Voraussetzungen nach Art. 35 Abs. 1 Satz 1 Nr. 1, Satz 2 PAG unzweifelhaft vor. Letztendlich kam es zu keiner weiteren Nutzung der übersandten Daten, da der betreffende Webshop seine Tätigkeit einstellte. Die Maßnahme war zutreffend nach Art. 35 Abs. 2 Satz 2 PAG auf drei Monate befristet. Auch die Zentrale Datenprüfstelle wurde im Vorfeld der Maßnahme eingebunden (siehe Art. 35 Abs. 3 Satz 3, Art. 41 Abs. 5 Satz 1 PAG, Art. 13 und 14 Polizeiorganisationsgesetz). Des Weiteren waren weder der Kernbereich privater Lebensgestaltung noch ein Berufsgeheimnisträger betroffen.

Die Prüfung konnte ich daher ohne Feststellung eines datenschutzrechtlichen Mangels abschließen.

3.7 Zuverlässigkeitsüberprüfungen beim G7-Gipfel 2022

Zuverlässigkeitsüberprüfungen sind in Akkreditierungsverfahren bei Großereignissen seit Jahren ein fester Bestandteil der polizeilichen Praxis. Sie haben mich in der Vergangenheit häufig beschäftigt (siehe etwa in meinem 31. Tätigkeitsbericht 2021 unter Nr. 3.2 sowie in meinem 27. Tätigkeitsbericht 2015/2016 unter Nr. 3.2). Zuverlässigkeitsüberprüfungen führen insbesondere bei Großveranstaltungen aufgrund ihrer Bedeutung und ihres Umfangs zu erheblichen Eingriffen in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz) einer Vielzahl betroffener Personen. Von besonderer Bedeutung ist dabei, dass die Polizei auch solche Daten speichert, die etwa in das Bundeszentralregister gar nicht eingetragen werden, dort bereits getilgt sind oder aus diesem Register – sofern es um ein Führungszeugnis und nicht um eine unbeschränkte Auskunft geht – nicht übermittelt werden dürfen.

Seit 2021 sind Zuverlässigkeitsüberprüfungen in Art. 60a Bayerisches Polizeiaufgabengesetz (PAG) geregelt (zur Entstehungsgeschichte dieser Vorschrift siehe bereits in meinem 31. Tätigkeitsbericht 2021 unter Nr. 3.2).

Eine der bislang wichtigsten polizeilichen Zuverlässigkeitsüberprüfungen fand im Rahmen des Akkreditierungsverfahrens für den G7-Gipfel 2022 vom 26. bis 28. Juni 2022 auf Schloss Elmau (G7-Gipfel) statt. Das ursprüngliche Konzept sah unter anderem auch eine Überprüfung von Anwohnerinnen und Anwohnern und anderen Personen ohne Tätigkeitsbezug zur Veranstaltung (beispielsweise Forstwirtinnen und Forstwirte, Postzustellerinnen und Postzusteller), durch die Bayerische Polizei vor.

Nach Art. 60a Abs. 1 Satz 1 PAG kann eine Zuverlässigkeitsüberprüfung bei Personen stattfinden, „soweit dies im Hinblick auf den Anlass **und die Tätigkeit der betroffenen Person** erforderlich und angemessen ist." Aus dieser gesetzlichen Formulierung folgt, dass **eine sicherheitsrechtliche Überprüfung von Personen, die keine berufliche Verbindung zu der Veranstaltung haben, auf Grundlage von Art. 60a PAG nicht möglich ist.** Eine Überprüfung stünde nicht nur im Widerspruch zum klaren Wortlaut der gesetzlichen Regelung, sondern auch zu ihrer Entstehungsgeschichte sowie der mittlerweile ergangenen Rechtsprechung des Bayerischen Verfassungsgerichtshofes. Dieser hatte in seiner Entscheidung vom 17. Mai 2022 hervorgehoben, Art. 60a Abs. 1 Satz 1 PAG stelle durch den geforderten tätigkeitsbezogenen Konnex hinreichend sicher, dass regelmäßig nur solche Personen überprüft würden, deren **spezifische „Tätigkeit" im Rahmen des mit einem erheblichen Sicherheitsrisiko verbundenen Anlasses** Grund für die Überprüfung biete.[80] Mit anderen Worten: Art. 60a PAG kann nicht die Grundlage für Sicherheitsüberprüfungen von Anwohnerinnen und Anwohnern oder sonstigen Personen sein, die keinen tätigkeitsbasierten Bezug zur Veranstaltung haben.

Da demgemäß schon die Tatbestandsvoraussetzungen von Art. 60a Abs. 1 Satz 1 PAG nicht gewahrt waren, spielte auch die in dem polizeilichen Konzept geplante abgestufte Überprüfungsintensität, die für Anwohnerinnen und Anwohner vorgesehen war, von vornherein keine Rolle.

[80] Bayerischer Verfassungsgerichtshof, Entscheidung vom 17. Mai 2022, Vf. 47-VII-21, Rn. 93, juris.

Auf meinen Hinweis hin wurde die Überprüfung von Anwohnerinnen und Anwohnern sowie weiteren Personen, die keine in unmittelbaren Zusammenhang mit der Veranstaltung stehende Tätigkeit ausüben, ersatzlos gestrichen.

3.8 Verfolgung von Verkehrsordnungswidrigkeiten – überschießende Datenübermittlungen bei Lichtbildanforderungen

Im Zuge einer Prüfung fielen mir einige Anfragen nach Lichtbildern aus dem Personalausweisregister und entsprechende Übermittlungen durch die zuständigen Verwaltungsgemeinschaften und Gemeinden auf. Den um Übermittlung (nur) eines Lichtbildes nachsuchenden Zweckverbänden waren weitere – nicht angeforderte Daten – aus dem Personalausweisregister übermittelt worden. Die gesetzlichen Rahmenbedingungen bei Lichtbildanforderungen im Rahmen von Verkehrsordnungswidrigkeiten habe ich zuletzt in meinem 31. Tätigkeitsbericht 2021 unter Nr. 4.5 dargestellt.

Das geschilderte Vorgehen der Verwaltungsgemeinschaften und Gemeinden war von den Übermittlungsbefugnissen in § 24 Abs. 2 Satz 1 Nr. 2 Personalausweisgesetz (PAuswG) sowie entsprechend in § 22 Abs. 2 Nr. 2 Paßgesetz nicht gedeckt. Danach hätten nur solche Daten an die Zweckverbände übermittelt werden dürfen, die für deren Aufgabenerfüllung erforderlich waren; das waren im Hinblick auf die Übermittlungsersuchen nur die Lichtbilder.

§ 24 PAuswG
Verwendung im Personalausweisregister gespeicherter Daten
(2) Die Personalausweisbehörden dürfen anderen Behörden auf deren Ersuchen Daten aus dem Personalausweisregister übermitteln, wenn
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 ersuchende Behörde die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erheben kann oder wenn nach der Art der Aufgabe, zu deren Erfüllung die Daten erforderlich sind, von einer solchen Datenerhebung abgesehen werden muss.*

[…]

Ich habe die betroffenen Verwaltungsgemeinschaften und Gemeinden darauf hingewiesen, dass im Zusammenhang mit Lichtbildanfragen auf den Umfang des zu übermittelnden Datensatzes zu achten ist und nicht relevante Daten wie beispielsweise der Körpergröße oder Augenfarbe von einer Übermittlung auszunehmen sind. Des Weiteren habe ich die jeweiligen Stellen zur Vermeidung künftiger überschießender Datenübermittlungen gebeten, die Mitarbeiterinnen und Mitarbeiter entsprechend zu sensibilisieren.

3.9 Abfragen aus dem Fahreignungsregister

Die datenschutzrechtliche Zulässigkeit von Maßnahmen im Rahmen der Verfolgung und Ahndung von Ordnungswidrigkeiten im Straßenverkehr ist ein wiederkehrendes Thema in meiner Prüfungs- und Beratungspraxis. Dies zeigen meine Tätigkeitsberichte; Ausführungen zu diesem Thema bieten der Schwerpunktbei-

trag in meinem 30. Tätigkeitsbericht 2020 unter Nr. 2, ferner der 29. Tätigkeitsbericht 2019 unter Nr. 4.5, der 27. Tätigkeitsbericht 2015/2016 unter Nr. 5.6 und der 26. Tätigkeitsbericht 2013/2014 unter Nr. 5.5.

Im Berichtszeitraum habe ich drei kommunale Zweckverbände um Darlegung gebeten, wie bei Abfragen aus dem Fahreignungsregister (FAER) verfahren wird. Dieses Register wird vom Kraftfahrt-Bundesamt nach §§ 28 ff. Straßenverkehrsgesetz (StVG) und §§ 59 ff. Fahrerlaubnis-Verordnung geführt. Es dient unter anderem der Ahndung von Verkehrsordnungswidrigkeiten, da verwertbare Voreintragungen im FAER gemäß § 3 Abs. 1 Bußgeldkatalog-Verordnung (BKatV) zur Erhöhung der verhängten Bußgelder führen können: § 3 Abs. 1 BKatV stellt klar, dass Voreintragungen im Fahreignungsregister bei der Festlegung des Regelsatzes grundsätzlich unberücksichtigt geblieben sind, soweit im Bußgeldkatalog (bezüglich der Nr. 152.1, 241.1, 241.2, 242.1 und 242.2) nichts anderes bestimmt ist. Daraus folgt, dass entsprechende Voreintragungen besondere Umstände darstellen, die gegen das Vorliegen eines Regelfalles sprechen, so dass die Geldbuße erhöht werden kann.[81]

§ 3 BKatV
Bußgeldregelsätze
(1) Etwaige Eintragungen des Betroffenen im Fahreignungsregister sind im Bußgeldkatalog nicht berücksichtigt, soweit nicht in den Nummern 152.1, 241.1, 241.2, 242.1 und 242.2 des Bußgeldkatalogs etwas anderes bestimmt ist.
[…]

Die Rechtsgrundlage für die Führung und den Inhalt des FAER ist in § 28 StVG normiert.

§ 28 StVG
Führung und Inhalt des Fahreignungsregisters
(1) Das Kraftfahrt-Bundesamt führt das Fahreignungsregister nach den Vorschriften dieses Abschnitts.
(2) Das Fahreignungsregister wird geführt zur Speicherung von Daten, die erforderlich sind
1. für die Beurteilung der Eignung und der Befähigung von Personen zum Führen von Kraftfahrzeugen oder zum Begleiten eines Kraftfahrzeugführers entsprechend einer nach § 6e Abs. 1 erlassenen Rechtsverordnung,
2. für die Prüfung der Berechtigung zum Führen von Fahrzeugen,
3. für die Ahndung der Verstöße von Personen, die wiederholt Straftaten oder Ordnungswidrigkeiten, die im Zusammenhang mit dem Straßenverkehr stehen, begehen oder
4. für die Beurteilung von Personen im Hinblick auf ihre Zuverlässigkeit bei der Wahrnehmung der ihnen durch Gesetz, Satzung oder Vertrag übertragenen Verantwortung für die Einhaltung der zur Sicherheit im Straßenverkehr bestehenden Vorschriften.
(3) Im Fahreignungsregister werden Daten gespeichert über
1. rechtskräftige Entscheidungen der Strafgerichte wegen einer Straftat, die in der Rechtsverordnung nach § 6 Absatz 1 Satz 1 Nummer 4 bezeichnet ist, soweit sie auf Strafe, Verwarnung mit Strafvorbehalt erkennen oder einen Schuldspruch enthalten,
2. rechtskräftige Entscheidungen der Strafgerichte, die die Entziehung der Fahrerlaubnis, eine isolierte Sperre oder ein Fahrverbot anordnen, sofern

[81] Euler, in: Graf, Beck'scher Online-Kommentar OWiG, Stand 1/2023, § 3 BKatV Rn. 2.

sie nicht von Nummer 1 erfasst sind, sowie Entscheidungen der Strafgerichte, die die vorläufige Entziehung der Fahrerlaubnis anordnen,

3. rechtskräftige Entscheidungen wegen einer Ordnungswidrigkeit
   a) nach den § 24 Absatz 1, § 24a oder § 24c, soweit sie in der Rechtsverordnung nach § 6 Absatz 1 Satz 1 Nummer 4 bezeichnet ist und gegen die betroffene Person
      aa) ein Fahrverbot nach § 25 angeordnet worden ist oder
      bb) eine Geldbuße von mindestens sechzig Euro festgesetzt worden ist und § 28a nichts anderes bestimmt,
   b) nach den § 24 Absatz 1, § 24a oder § 24c, soweit kein Fall des Buchstaben a vorliegt und ein Fahrverbot angeordnet worden ist,
   c) nach § 10 des Gefahrgutbeförderungsgesetzes, soweit sie in der Rechtsverordnung nach § 6 Absatz 1 Satz 1 Nummer 4 bezeichnet ist,

4. unanfechtbare oder sofort vollziehbare Verbote oder Beschränkungen, ein fahrerlaubnisfreies Fahrzeug zu führen,

5. unanfechtbare Versagungen einer Fahrerlaubnis,

6. unanfechtbare oder sofort vollziehbare
   a) Entziehungen, Widerrufe oder Rücknahmen einer Fahrerlaubnis,
   b) Feststellungen über die fehlende Berechtigung, von einer ausländischen Fahrerlaubnis im Inland Gebrauch zu machen,

7. Verzichte auf die Fahrerlaubnis,

8. unanfechtbare Ablehnungen eines Antrags auf Verlängerung der Geltungsdauer einer Fahrerlaubnis,

9. die Beschlagnahme, Sicherstellung oder Verwahrung von Führerscheinen nach § 94 der Strafprozessordnung,

10. (weggefallen)

11. Maßnahmen der Fahrerlaubnisbehörde nach § 2a Abs. 2 Satz 1 Nr. 1 und 2 und § 4 Absatz 5 Satz 1 Nr. 1 und 2,

12. die Teilnahme an einem Aufbauseminar, an einem besonderen Aufbauseminar und an einer verkehrspsychologischen Beratung, soweit dies für die Anwendung der Regelungen der Fahrerlaubnis auf Probe (§ 2a) erforderlich ist,

13. die Teilnahme an einem Fahreignungsseminar, soweit dies für die Anwendung der Regelungen des Fahreignungs-Bewertungssystems (§ 4) erforderlich ist,

14. Entscheidungen oder Änderungen, die sich auf eine der in den Nummern 1 bis 13 genannten Eintragungen beziehen.

[…]

Um die Rechtsfolge im Bußgeldbescheid – insbesondere das Bußgeld – zutreffend bemessen zu können, sind daher Abfragen der Ordnungswidrigkeitenbehörden im FAER unerlässlich. Bereits in meinem 30. Tätigkeitsbericht 2020 unter Nr. 2.4 habe ich mich umfassend zur Fahrerermittlung geäußert. Zur Feststellung der Fahreridentität werden in der Regel zunächst Anhörungsbögen oder Zeugenfragebögen an die jeweiligen Halter oder Halterinnen versandt.

Bei zwei Zweckverbänden musste ich im Rahmen meiner Prüfung feststellen, dass die Abfragen im FAER bereits zeitlich mit der Versendung der ersten Anhör- oder Zeugenfragebögen zusammenfielen. In diesem Zeitpunkt besteht aber noch kein gesicherter Tatnachweis gegen eine konkrete Betroffene oder einen konkreten Betroffenen. Die Daten aus dem FAER wurden in diesen Fällen daher gewissermaßen „ins Blaue“ abgerufen.

Dieses Vorgehen verstößt gegen § 30 Abs. 1 Nr. 2 in Verbindung mit § 28 Abs. 2 Nr. 3 StVG, da nach diesen Vorschriften eine Datenübermittlung aus dem FAER an die für die Verfolgung von Ordnungswidrigkeiten zuständige Stelle nur gestattet ist, wenn dies zur Erfüllung der dieser Stelle obliegenden Aufgabe erforderlich ist. Wird ein Auszug aus dem FAER bereits zu einem Zeitpunkt eingeholt, in welchem noch nicht geklärt ist, ob gegen die jeweilige Person überhaupt ein gesicherter Tatnachweis im Ordnungswidrigkeitenverfahren besteht, verstößt die betreffende Behörde gegen den oben genannten Grundsatz der Erforderlichkeit.

Die beiden Zweckverbände wurden von mir auf diese Zusammenhänge aufmerksam gemacht und haben in der Folge mit Änderungen in den entsprechenden Softwareeinstellungen) geeignete Maßnahmen ergriffen, um eine datenschutzkonforme Vorgehensweise zu erreichen. So konnte ich erreichen, dass die datenschutzrechtlich fehlerhafte Verwaltungspraxis revidiert wurde.

3.10 Datenschutz bei der Staatsanwaltschaft: Nennung personenbezogener Daten in einer Einstellungsverfügung

Weiterhin erhalte ich Eingaben, mit denen betroffene Personen die Nennung personenbezogener Daten im Rahmen von Anklageschriften oder Einstellungsverfügungen der Staatsanwaltschaften rügen (siehe zuletzt den 32. Tätigkeitsbericht 2022 unter Nr. 4.4).

Auch im Berichtszeitraum wandte sich eine durch eine Straftat geschädigte Person an mich, weil ihre personenbezogenen Daten durch eine Einstellungsverfügung allen weiteren Geschädigten zur Kenntnis gelangt waren.

Das betreffende Ermittlungsverfahren hatte vier Betrugsvorwürfe umfasst, die zu einem gemeinsamen Verfahren gegen einen Beschuldigten verbunden worden waren. Zwar war dessen Vorgehensweise in allen vier Fällen ähnlich, es waren jedoch unterschiedliche Geschädigte betroffen. Mangels Tatnachweises stellte die Staatsanwaltschaft schließlich das Verfahren nach § 170 Abs. 2 Strafprozessordnung (StPO) ein. Dabei wurde versehentlich eine gemeinsame Einstellungsverfügung mit einer gemeinsamen Begründung für alle vier Taten verfasst, in der neben dem jeweils vergleichbar gelagerten Tathergang auch der Vor- und Nachnamen aller vier Geschädigten aufgeführt wurden. Mit der Mitteilung der Einstellung an die Geschädigten wurde auch die gemeinsame Einstellungsbegründung mit der Nennung aller vier Geschädigten an die jeweiligen Geschädigten übermittelt.

Diese nicht erforderliche Offenlegung personenbezogener Daten läuft dem in § 47 Nr. 3 BDSG verankerten Grundsatz der Datenminimierung entgegen. Sie war daher nach Art. 1 Abs. 5 BayDSG, § 500 Abs. 1 StPO, § 47 Nr. 3 Var. 2 BDSG datenschutzrechtlich unzulässig.

Die betreffende Staatsanwaltschaft räumte den Verstoß ein, bedauerte ihn und ergriff weitergehende Maßnahmen zur Sensibilisierung ihrer Bediensteten, um zukünftige Verstöße möglichst auszuschließen.

3.11 Prüfung eines abgelehnten Löschungsantrags beim Bayerischen Landesamt für Verfassungsschutz

Das Bayerische Landesamt für Verfassungsschutz hat den gesetzlichen Auftrag, Informationen unter anderem über Bestrebungen, die gegen die freiheitliche demokratische Grundordnung gerichtet sind, zu sammeln und auszuwerten. Im Rahmen dieser Aufgabe wird zwangsläufig eine Vielzahl an personenbezogenen Daten verarbeitet.

Auch im Bereich nachrichtendienstlicher Arbeit muss für Bürgerinnen und Bürger ein ausreichendes Maß an Transparenz sichergestellt sein. Zu diesem Zweck sieht Art. 23 Abs. 1 Bayerisches Verfassungsschutzgesetz (BayVSG) ein Recht auf Auskunft vor (siehe bereits meine Ausführungen im 28. Tätigkeitsbericht 2017/2018 unter Nr. 5.4 und 5.5 sowie im 29. Tätigkeitsbericht 2019 unter Nr. 3.6).

Teilweise wenden sich die von Speicherungen betroffenen Personen nach einer erteilten Auskunft mit einem Löschungsantrag an das Landesamt als speichernde Behörde. Die Voraussetzungen für eine Löschung legt Art. 21 Abs. 1 Satz 1 BayVSG fest:

„Personenbezogene Daten sind zu löschen, wenn
1. ihre Speicherung unzulässig ist,
2. ihre Kenntnis zur Erfüllung der Aufgaben nicht mehr erforderlich ist oder
3. seit der letzten gespeicherten relevanten Information 15 Jahre vergangen sind, es sei denn, die zuständige Abteilungsleitung oder deren Vertretung trifft im Einzelfall ausnahmsweise eine andere Entscheidung.“

Vor dem Hintergrund meiner Verpflichtung aus Art. 32 Abs. 2 BayVSG, mindestens alle zwei Jahre die Einhaltung der Vorschriften über den Datenschutz zu kontrollieren, lasse ich mich durch das Landesamt regelmäßig über abgelehnte Löschungsanträge informieren. So kann ich die Entscheidung der Behörde über die Ablehnung einer Datenlöschung auch ohne Beschwerde der betroffenen Person nachprüfen.

Im Berichtszeitraum habe ich bei einem Vor-Ort-Termin den betreffenden Aktenrückhalt zu den Erkenntnissen eingesehen, die maßgeblich für die Ablehnung des Löschungsantrags und für die Aufrechterhaltung der Speicherungen waren. Hierbei konnte ich in dem gesichteten Material keine Mängel feststellen. Gleichwohl werde ich auch zukünftig an dieser Praxis festhalten, weil sie ein wirksames Mittel ist, die Zulässigkeit nachrichtendienstlicher Speicherungen zu überprüfen.

3.12 Prüfung Antiterrordatei (ATD) und Rechtsextremismus-Datei (RED)

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

Auch in diesem Berichtszeitraum habe ich daher eine entsprechende Vor-Ort-Prüfung beim Bayerischen Landesamt für Verfassungsschutz durchgeführt. Dabei habe ich stichprobenartig die Speicherungen durch das Landesamt überprüft.

Meine Prüfung gab keinen Anlass zu Beanstandungen. In allen überprüften Fällen wurden die gesetzlichen Speicherungsvoraussetzungen des Antiterrordateigesetz eingehalten. Aus datenschutzrechtlicher Sicht erfreulich ist im Übrigen, dass sich die Einträge in der ATD seit der letzten Prüfung nahezu halbiert haben.

Weiterhin werden seit 2012 Daten zur Bekämpfung des gewaltbezogenen Rechtsextremismus in der Rechtsextremismus-Datei (RED) gespeichert. Gesetzliche Grundlage hierfür ist das Rechtsextremismus-Datei-Gesetz (RED-G), das hinsichtlich der Rahmenbedingungen mit dem Antiterrordateigesetz vergleichbar ist und ebenfalls mindestens alle zwei Jahre datenschutzrechtliche Pflichtprüfungen vorsieht.

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

Im Rahmen dieser Prüfung ließen sich bei einer Person, deren Speicherung sich auf § 2 Satz 1 Nr. 1 Buchst. b RED-G stützte, weder die der betroffenen Person konkret vorgeworfenen Tathandlungen noch eine strafrechtliche Verfolgung aus dem Aktenrückhalt entnehmen. Auf meinen Hinweis prüfte das Landesamt nochmals die Speicherungsvoraussetzung und löschte die betreffende Speicherung schließlich.

Zudem fiel mir bei Prüfung eine Speicherung auf, die nach Auskunft des Landesamtes eigentlich bereits aus der RED gelöscht worden sein sollte, aber wegen des im Rahmen von NSU-Untersuchungsausschüssen verhängten Löschmoratoriums für Akten und Daten des Landesamtes (siehe hierzu meinen 32. Tätigkeitsbericht 2022 unter Nr. 3.5) nach wie vor dort sichtbar war. Eine Sperrung der betreffenden Person in der RED – wie bei Löschmoratorien aufgrund von Art. 21 Abs. 2 Nr. 2 Bayerisches Verfassungsschutzgesetz vorgesehen– war nicht vorgenommen worden, weil dies als technisch unmöglich angesehen wurde. Ich äußerte hier rechtliche Bedenken und konnte schließlich erreichen, dass die betreffende technische Gestaltung datenschutzgerecht überarbeitet wurde.

4 Allgemeine Innere Verwaltung

4.1 Datenschutzbeauftragte bei Kommunen: geschäftsleitende Beamte scheiden regelmäßig aus

In meiner Aktuellen Kurz-Information 7 „Datenschutzbeauftragte kreisangehöriger Gemeinden in Bayern: Inkompatibilitäten, Qualifikation, Zeitbudget“[82] habe ich bereits eingehend erläutert, warum die gerade bei kleineren Gemeinden bis etwa 10.000 Einwohnern regelmäßig anzutreffenden geschäftsleitenden Beamten, welche im Alltagsgeschäft die Abläufe in der Gemeindeverwaltung koordinieren sowie die Sitzungen des Gemeinderats vorbereiten und begleiten, nicht als behördliche Datenschutzbeauftragte benannt werden dürfen. Daran habe ich im Berichtszeitraum – trotz einzelner anfänglicher Widerstände vor Ort – festgehalten. Im Hinblick auf die teilweise vorgebrachten juristischen Einwände habe ich ergänzend auf Folgendes hingewiesen:

4.1.1 Vermeidung von „Inkompatibilitäten“ unionsrechtlich geboten

Die von den Gemeinden zu benennenden Datenschutzbeauftragten können nach Art. 38 Abs. 6 Satz 1 DSGVO neben den Aufgaben des Datenschutzbeauftragten grundsätzlich weitere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche muss nach Art. 38 Abs. 6 Satz 2 DSGVO aber sicherstellen, dass derartige Aufgaben und Pflichten nicht zu einem Interessenskonflikt führen. Die Vermeidung solcher Inkompatibilitäten war übrigens auch schon vor in Kraft treten der Datenschutz-Grundverordnung geboten (siehe die Ausführungen in meinem 26. Tätigkeitsbericht 2013/2014 unter Nr. 2.3.11).

Ein potentieller Interessenskonflikt liegt vor, wenn die jeweilige Person neben den Aufgaben und Pflichten der oder des Datenschutzbeauftragten auch mit der Erfüllung von Aufgaben betraut wird, welche die Datenschutz-Grundverordnung dem Verantwortlichen zuordnet. Darunter fällt die Aufgabe, für rechtmäßige Verarbeitungen zu sorgen, ebenso aber etwa die Erfüllung der Betroffenenrechte nach Art. 15 ff. DSGVO oder die Umsetzung technischer und organisatorischer Schutzmaßnahmen nach Art. 24 Abs. 1 DSGVO sicherzustellen. Dies ist bei geschäftsleitenden Beamten sowie vergleichbaren Angestellten regelmäßig der Fall, welche meist durch ein formelles Weisungsrecht oder auf andere Art Einfluss auf die Arbeit der gesamten Gemeindeverwaltung und damit auch auf die in den einzelnen Funktionseinheiten durchzuführenden Datenverarbeitungen nehmen können; in der Datenschutz-Dienstanweisung wird ihr oder ihm daher häufig die Rolle einer oder eines „Organisationsverantwortlichen“ zugewiesen.

[82] Bayerischer Landesbeauftragter für den Datenschutz, Datenschutzbeauftragte kreisangehöriger Gemeinden in Bayern: Inkompatibilitäten, Qualifikation, Zeitbudget, Aktuelle Kurz-Information 7, Stand 10/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018“.

4.1.2 Zulässige Einschränkung der kommunalen Selbstverwaltungsgarantie

Die Garantie der kommunalen Selbstverwaltung (Art. 28 Abs. 2 Grundgesetz) umfasst auch die Organisationshoheit, also das Recht, im Rahmen der Gesetze über den Aufbau der Gemeindeverwaltung und die Verteilung der Geschäfte unter die einzelnen Funktionseinheiten eigenverantwortlich zu entscheiden.[83] Die Garantie der kommunalen Selbstverwaltung steht also unter Gesetzesvorbehalt. Gemeinden können daher zwar grundsätzlich frei bestimmen, welche Beschäftigten sie mit der Erfüllung welcher Aufgaben betrauen. Art. 38 Abs. 6 Satz 2 DSGVO als Teil des innerstaatlich anwendbaren Rechts schränkt die Organisationsfreiheit jedoch zulässigerweise im Rahmen des insoweit bestehenden Gesetzesvorbehalts ein: Die Gemeinde kann zwar festlegen, wer Aufgaben des Verantwortlichen und wer die Aufgaben der oder des Datenschutzbeauftragten wahrnehmen soll, diese Aufgaben dürfen aber nicht in ein und derselben Person zusammenfallen.

4.1.3 Beamtenrechtliche Regelungen entheben nicht von der Notwendigkeit, Interessenskonflikte zu vermeiden

Beamtinnen und Beamte müssen nach § 36 Abs. 1 Beamtenstatusgesetz (BeamtStG) die volle persönliche Verantwortung für die Rechtmäßigkeit ihrer dienstlichen Handlungen tragen; eine schuldhafte Verletzung ihrer Pflichten stellt nach § 47 Abs. 1 Satz 1 BeamtStG ein Dienstvergehen dar. Einzelne Kommunen haben unter Berufung hierauf mir gegenüber vorgebracht, dieser Personenkreis könne schon deshalb keinem Interessenskonflikt unterliegen, weil kraft Beamtenrecht jederzeit ein vertretbarer, das heißt rechtmäßiger Interessenausgleich hergestellt werden müsse. Auch geschäftsleitende Beamte könnten deswegen durchaus als Datenschutzbeauftragte bestellt werden.

Ich habe insoweit darauf hingewiesen, dass dieser Rückschluss schon mit den Vorschriften zur Befangenheit oder zur Besorgnis der Befangenheit[84] im nationalen Verwaltungsverfahrensrecht unvereinbar ist. Diese Vorschriften bringen den allgemeinen Grundsatz zum Ausdruck, dass in einem konkreten Verwaltungsverfahren nur solche Personen für eine Behörde tätig werden dürfen, bei denen keine Umstände vorliegen, die objektiv geeignet sind, Misstrauen gegen ein neutrales, unparteiisches Verhalten zu rechtfertigen.[85] Bürgerinnen und Bürger sollen die Gewähr haben, dass Einzelfallentscheidungen allein nach Recht und Gesetz ergehen und an deren inhaltlicher Vorbereitung keine Personen teilnehmen, deren Unbefangenheit gegenüber der zu treffenden Entscheidung wegen mangelnder Distanz zum Gegenstand des Verfahrens gefährdet sein könnte.[86] Insoweit geht bereits der nationale Gesetzgeber davon aus, dass die statusrechtliche Pflicht des Beamten zu rechtmäßigem Handeln auch einer verwaltungsverfahrensrechtlichen Absicherung bedarf.[87]

Die im nationalen Recht für das konkrete Verwaltungsverfahren vorgesehene verfahrensmäßige Absicherung der abstrakten beamtenrechtlichen Pflichten verfolgt letztlich einen ähnlichen Ansatz wie Art. 38 Abs. 6 Satz 2 DSGVO. Datenschutzbeauftragte haben nach Art. 38 Abs. 4 DSGVO gerade auch die Funktion, konkrete

83 Mehde, in: Dürig/Herzog/Scholz, Grundgesetz, Stand 9/2022, Art. 28 Rn. 65.
84 Siehe hierzu im bayerischen Recht Art. 20, 21 Bayerisches Verwaltungsverfahrensgesetz.
85 Schmitz, in: Stelkens/Bonk/Sachs, Verwaltungsverfahrensgesetz, 10. Aufl. 2023, § 20 Rn. 1.
86 Schmitz, in: Stelkens/Bonk/Sachs, Verwaltungsverfahrensgesetz, 10. Aufl. 2023, § 20 Rn. 1.
87 Schmitz, in: Stelkens/Bonk/Sachs, Verwaltungsverfahrensgesetz, 10. Aufl. 2023, § 20 Rn. 2.

betroffene Personen bei der Wahrnehmung ihrer Datenschutzrechte gegenüber der verantwortlichen Stelle zu beraten. Das Vertrauen betroffener Personen in die Unabhängigkeit der Datenschutzbeauftragten wäre jedoch von vornherein stark beschädigt, wenn dies zulässigerweise dieselbe Person sein könnte, die die in Frage stehende Datenverarbeitung der Gemeinde (potentiell) maßgeblich beeinflussen kann.

4.2 Keine Einbindung der Datenschutz-Aufsichtsbehörde in Zuwendungsverfahren per Bescheid

Nicht zuletzt die COVID-19-Pandemie hat dazu beigetragen, dass Innenstädte verwaist sind und in der Folge aufgrund veränderten Einkaufs- und Ausgehgewohnheiten viele Geschäfte oder Restaurants von ihren Inhabern aus wirtschaftlichen Gründen geschlossen wurden. Kommunen stehen hier vor dem Problem, die Innenstädte wieder attraktiver zu machen. In diesem Zusammenhang wurde ich im Berichtszeitraum von einer Kommune um datenschutzrechtliche Prüfung einer Lokalisierungs- und Ortungstechnologie für Innen- und Außenräume gebeten. Die Technologie sollte mithelfen, die Attraktivität der Innenstadt durch die Analyse von Bewegungsströmen und Verhaltensmustern von Passantinnen und Passanten zu verbessern.

Ursächlich für die Beratungsanfrage war eine entsprechende, im Zuwendungsbescheid des über die Bewilligung einer Förderung entscheidenden Staatsministeriums enthaltene Nebenbestimmung. Danach erging die Bewilligung der Zuwendung für den Einsatz der Technologie unter dem Vorbehalt, dass eine Vorlage des Projektes bei mir zu keinen Beanstandungen führt. Auch wenn ich es natürlich begrüßt habe, dass nur datenschutzkonforme Leistungen gefördert werden sollen, habe ich dem Anliegen der Kommune nicht entsprochen. Der vom Staatsministerium gewählte Weg meiner Einbindung stand mit weder mit meiner Unabhängigkeit noch mit der gesetzlichen Zuständigkeitsordnung in Einklang.

4.2.1 Prüfung der Datenschutzkonformität einer geförderten Leistung hat vor Erlass des Zuwendungsbescheides zu erfolgen

Zuwendungen dürfen nach Art. 44 Abs. 1 Satz 1 Bayerische Haushaltsordnung (BayHO) nur unter den Voraussetzungen des Art. 23 BayHO gewährt werden. Nach Art. 23 BayHO dürfen Ausgaben und Verpflichtungsermächtigungen für Leistungen an Stellen außerhalb der Staatsverwaltung zur Erfüllung bestimmter Zwecke (Zuwendungen) nur veranschlagt werden, wenn der Staat an der Erfüllung durch solche Stellen ein erhebliches Interesse hat, das ohne die Zuwendungen nicht oder nicht im notwendigen Umfang befriedigt werden kann. Der jeweilige Zuwendungsgeber muss ein solches Interesse überhaupt entwickeln dürfen.[88] Das ist nicht der Fall, wenn die konkrete Umsetzung des zu fördernden Vorhabens mit gesetzlichen Regelungen nicht vereinbar ist. So ist in den zuwendungsrechtlichen Bewilligungsverfahren regelmäßig die Vereinbarkeit der Zuwendung mit dem EU-Beihilferecht zu prüfen.[89] Hinsichtlich des (EU-) Datenschutzrechts kann hier nichts anderes gelten. Die Vereinbarkeit des zu fördernden

[88] Müller/Richter/Ziekow, Handbuch Zuwendungsrecht, 2017, Kap. A Rn. 222.
[89] Müller/Richter/Ziekow, Handbuch Zuwendungsrecht, 2017, Kap. B Rn. 71.

Vorhabens mit dem Datenschutzrecht ist deshalb grundsätzlich vor Erlass des Zuwendungsbescheides zu würdigen. Dafür bieten sich zwei Alternativen an:

Die Bewilligungsbehörde kann entweder dem potentiellen Zuwendungsempfänger aufgeben, mit den Antragsunterlagen eine Stellungnahme zur Vereinbarkeit des Vorhabens mit dem Datenschutzrecht vorzulegen. Wenn eine Kommune eine bestimmte Technologie einsetzen will und dabei die Verarbeitung personenbezogener Daten im Raum steht, ist sie dafür verantwortlich, dass der Einsatz datenschutzkonform erfolgt. Die Kommune muss dann ohnehin ihre Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO erfüllen, also dokumentieren, dass und aus welchen Gründen den datenschutzrechtlichen Anforderungen genügt ist. Die datenschutzrechtliche Beratung der Kommune als Verantwortlicher ist in erster Linie eine eigenständige Aufgabe der vor Ort zu benennenden behördlichen Datenschutzbeauftragten (vgl. Art. 39 Abs. 1 Buchst. a DSGVO). Die behördlichen Datenschutzbeauftragten können sich zwar im Rahmen der Zusammenarbeit mit der Datenschutz-Aufsichtsbehörde unter vertiefter Darlegung ihrer eigenen rechtlichen Erwägungen in einem Zweifelsfall auch an den Landesbeauftragten wenden. Das im konkreten Fall beabsichtigte pauschale „Outsourcing" der datenschutzrechtlichen Prüfung des Vorhabens an mich ist so allerdings nicht zu erreichen.

Soweit den geförderten Kommunen eine komplexe datenschutzrechtliche Prüfung nicht zugemutet werden soll, kann – und muss – die Bewilligungsbehörde eben selbst eine solche Prüfung vornehmen.

4.2.2 Unabhängigkeit des Landesbeauftragten für den Datenschutz

Der Landesbeauftragte für den Datenschutz ist gemäß Art. 52 Abs. 1 DSGVO und Art. 33a Abs. 3 Satz 1 Verfassung des Freistaates Bayern eine völlig unabhängige Aufsichtsbehörde. Er ist weisungsfrei. Daher können ihm grundsätzlich keine Prüfaufträge erteilt werden. Nach Art. 15 Abs. 3 BayDSG können nur der Landtag oder die Staatsregierung den Landesbeauftragten unbeschadet seiner Unabhängigkeit ersuchen, zu bestimmten Vorgängen aus seinem Aufgabenbereich Stellung zu nehmen. Der Landesbeauftragte entscheidet aber auch in diesem Fall selbst, ob und in welchem Umfang er auf das Ersuchen eingeht. In der aufsichtsbehördlichen Praxis gibt der Landesbeauftragte auf entsprechende Ersuchen regelmäßig gern ausführliche Hinweise.

Durch die Nebenbestimmung im Zuwendungsbescheid hat die Bewilligungsbehörde unzulässigerweise versucht, außerhalb von Art. 15 Abs. 3 BayDSG einen Prüfauftrag zu erteilen. Der Landesbeauftragte war zwar nicht förmlicher Adressat der fraglichen Nebenbestimmung. Gegenüber der Zuwendungsempfängerin wurde aber der Eindruck erweckt, er sei zu einer datenschutzrechtlichen Prüfung des zuwendungsgegenständlichen Vorhabens verpflichtet. Die Zuwendungsempfängerin musste danach annehmen, die Realisierung „hänge nur noch vom Landesbeauftragten ab". Aus dieser Perspektive folgerichtig hat die Zuwendungsempfängerin mit dem Landesbeauftragten in der offenkundigen Erwartung Kontakt aufgenommen, zeitnah die gleichsam behördlich angeordnete „Unbedenklichkeitsbescheinigung" zu erhalten.

4.2.3 Feststellung der Datenschutzkonformität einer geförderten Leistung ist nicht Aufgabe des Landesbeauftragten

Der geförderten Kommune erwuchs aus der im Zuwendungsbescheid enthaltenen Nebenbestimmung kein Anspruch auf eine Prüfung ihres Vorhabens durch den Landesbeauftragten. Dessen Aufgaben sind maßgeblich in Art. 57 Abs. 1 DSGVO festgelegt. Die Tatbestände dieser Norm waren jedoch nicht einschlägig. Insbesondere Art. 57 Abs. 1 Buchst. v DSGVO war in Anbetracht der Unabhängigkeit der Datenschutz-Aufsichtsbehörde nicht dahin zu verstehen, dass beliebige Aufgaben von dritter Seite zugewiesen werden können. Die vorherige Konsultation einer Datenschutz-Aufsichtsbehörde mit Blick auf geplante Verarbeitungen ist unter der Datenschutz-Grundverordnung ein seltener Ausnahmefall; sie kann insbesondere nach einer „ungünstigen" Datenschutz-Folgenabschätzung in Betracht kommen (siehe Art. 36 DSGVO).

4.2.4 Ergebnis

Vor diesem Hintergrund habe ich die Bewilligungsbehörde gebeten sicherzustellen, dass in Zuwendungsbescheiden zukünftig auf Nebenbestimmungen der erwähnten Art verzichtet wird. Dies wurde mir vom betroffenen Staatsministerium zugesichert. Zudem habe ich mich für die Zukunft gern dazu bereit erklärt, die Bewilligungsbehörde bei der Entwicklung einer Best Practice für die datenschutzgerechte Steuerung von Bewilligungsverfahren zu unterstützen.

4.3 Datenschutzgerechte Behandlung eines Antrags auf Änderung des Gemeindewappens in öffentlicher Gemeinderatssitzung

Bayerische Gemeinden haben nach Art. 4 Gemeindeordnung (GO) das Recht zur Führung ihrer geschichtlichen Wappen. Auch wenn Herkunft und Bedeutung der teils jahrhundertealten Gemeindewappen nicht immer vollständig bekannt sein mögen, spielen diese für das Selbstbild der örtlichen Gemeinschaft doch auch heute noch durchaus eine Rolle.

Im Berichtszeitraum stellte eine Bürgerin bei der Gemeindeverwaltung einen Antrag auf Änderung des Gemeindewappens. Nach ihrer Auffassung enthielt das Wappen ein diskriminierendes Bildelement. Der Antrag wurde in öffentlicher Sitzung des Gemeinderats behandelt. Zu diesem Zweck wurde der vollständige Wortlaut des Antrags einschließlich des Namens der Antragstellerin verlesen. In der Folge erschien in der örtlichen Presse ein Bericht, in welchem ebenfalls der Name der Antragstellerin genannt wurde. Gegen das Handeln der Gemeinde hat sich die Bürgerin zu Recht bei mir beschwert. Ich habe gegenüber der Gemeinde einen Verstoß gegen datenschutzrechtliche Vorschriften festgestellt.

Die Gemeinde hat durch die Namensnennung personenbezogene Daten der Antragstellerin offengelegt. Dafür war eine Rechtsgrundlage erforderlich (Art. 6 Abs. 1 UAbs. 1 DSGVO). Da eine Einwilligung nicht erteilt war, kam dafür allenfalls die allgemeine Übermittlungsbefugnis aus Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG in Betracht. Danach ist eine Übermittlung personenbezogener Daten durch eine öffentliche Stelle nur zulässig, wenn sie zur Erfüllung einer der übermittelnden oder der empfangenden öffentlichen Stelle obliegenden Aufgabe erforderlich ist. Diese Voraussetzungen waren jedoch nicht erfüllt.

Zwar wollte die Gemeinde mit der Behandlung des Antrags dem Petitionsrecht nach Art. 56 Abs. 3 GO entsprechen. Dort heißt es:

„Jeder Gemeindeeinwohner kann sich mit Eingaben und Beschwerden an den Gemeinderat wenden."

Um diese Aufgabe zu erfüllen, war es für die Gemeinde jedoch nicht erforderlich, den Antrag unter Namensnennung zu verlesen. Der Begriff der Erforderlichkeit ist als Bestandteil von Verarbeitungsbefugnissen, die auf Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO gestützt sind, unionsrechtlich zu verstehen. Er ist im Lichte des unionalen Verhältnismäßigkeitsprinzips zu interpretieren. Geboten ist danach eine Abwägung zwischen den Grundrechten der betroffenen Person einerseits und dem gegenläufigen öffentlichen Interesse andererseits.[90] Eine Verarbeitung personenbezogener Daten ist daher nicht schon deshalb zulässig, weil sie für die Aufgabenerfüllung einer öffentlichen Stelle förderlich ist.[91] Zwar mag ein öffentliches Interesse bestehen, dass der zur Entscheidung über den Antrag berufene Gemeinderat bei einer Petition die Identität des Antragstellers erfährt, zumal das Petitionsrecht nicht jedermann, sondern nur Gemeindeeinwohnern zukommt. Dies gilt aber nicht entsprechend für die Allgemeinheit. Insoweit überwiegt jedenfalls das im Recht auf informationelle Selbstbestimmung fundierte Vertraulichkeitsinteresse von Antragstellern. Die Eingabe nach Art. 56 Abs. 3 GO ist kein auf die Öffentlichkeit angelegtes Instrument der demokratischen Mitwirkung wie etwa ein Bürgerbegehren oder ein Bürgerantrag; sie bleibt im bilateralen Verhältnis von Gemeinde und Eingabeführerin oder Eingabeführer. Auf ein Risiko von Anfeindungen gegenüber Antragstellern kommt es vor diesem Hintergrund nicht an.

Selbst wenn man vor diesem rechtlichen Hintergrund im konkreten Fall annähme, dass für eine abschließende Willensbildung des Gemeinderats über die Petition zwingend die Kenntnis der Identität der Antragstellerin erforderlich wäre – etwa um die Ernsthaftigkeit des Anliegens einschätzen zu können –, rechtfertigt dies nicht die Nennung des Namens in öffentlicher Sitzung. Der Name hätte vielmehr im Rahmen der internen und vertraulichen Sitzungsvorlagen für die Gemeinderatsmitglieder genannt werden können. Der Gemeinderat ist dann über den Antrag im Detail und die Identität der Eingabeführerin informiert, während in der öffentlichen Sitzung über den Antrag seinem wesentlichen Inhalt nach und ohne Namensnennung diskutiert werden kann.

Die von der Gemeinde gewählte Sachbehandlung konnte im Übrigen auch schon deswegen nicht auf Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG gestützt werden, weil diese Vorschrift keine initiativen Datenübermittlungen legitimiert.

4.4 Gesetz zur Änderung des Gemeinde- und Landkreiswahlgesetzes und weiterer Rechtsvorschriften

Im Jahr 2023 hat der bayerische Gesetzgeber das Kommunalrecht umfassend novelliert; die Änderungen sind gestaffelt bis zum 1. Januar 2024 in Kraft getreten. Nicht wenige der Neuerungen waren auch datenschutzrechtlich relevant. Insoweit zutreffend hat mich das Bayerische Staatsministerium des Innern, für Sport und

[90] Vgl. Bayerisches Oberstes Landesgericht, Beschluss vom 6. August 2020 , 1 VA 33/20, BeckRS 2020, 18859, Rn. 59.

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

Integration daher im Gesetzgebungsverfahren beteiligt. Leider geschah dies aber erst im Zuge der Verbandsanhörung und nicht bereits bei der Erarbeitung des Referentenentwurfs – also nicht „frühzeitig", wie § 7 Abs. 4 Satz 1 Geschäftsordnung der Bayerischen Staatsregierung dies an sich fordert. Obwohl mir daher wenig Zeit zur Verfügung stand, habe ich eine umfangreiche Stellungnahme abgegeben.

Im Mittelpunkt meiner Stellungnahme standen dabei zunächst die Neuregelungen zur Live-Übertragung von Bürgerversammlungen sowie von Gremiensitzungen ins Internet, ferner die Speicherung von Sitzungsaufzeichnungen in einer Mediathek. Mit diesen Themen habe ich mich in der Vergangenheit in meinen Tätigkeitsberichten bereits mehrfach befasst (siehe 21. Tätigkeitsbericht 2003/2004 unter Nr. 11.2 und 29. Tätigkeitsbericht 2019 unter Nr. 5.2). Dabei habe ich für Live-Übertragungen und Mediatheken das Erfordernis einer gesetzlichen Rechtsgrundlage betont, weil insbesondere die weltweite, im Fall der Mediathek zudem längerfristige Verbreitung von Redebeiträgen in Bild und Ton erhebliche Grundrechtseingriffe für die Teilnehmerinnen und Teilnehmer von Bürgerversammlungen oder Gremiensitzungen mit sich bringt. Soweit unter Geltung des bisherigen Rechts diskutiert wurde, die erforderliche Rechtsgrundlage jeweils im Einzelfall durch Einholung einer Einwilligung zu schaffen, habe ich auf die geringe Praktikabilität einer solchen Lösung aufmerksam gemacht (siehe insbesondere mein 27. Tätigkeitsbericht 2015/2016 unter Nr. 6.10.1). Vor diesem Hintergrund hat es mich gefreut, dass der Gesetzgeber meine Position nun aufgegriffen hat. Auch zu dem im Gesetzentwurf vorgesehenen Recht auf Kopie von Niederschriften kommunaler Gremiensitzungen habe ich Hinweise gegeben. Eine klar ablehnende Haltung habe ich demgegenüber zu dem Vorhaben eingenommen, die erst 2018 unter meiner Beteiligung eingeführten datenschutzfreundlichen Regelungen zum Einbau und Betrieb elektronischer Wasserzähler mit Funkmodul wieder aufzuheben.

4.4.1 Bürgerversammlung: Live-Übertragung ins Internet

Der Gesetzesentwurf sah ursprünglich vor, dass die Bürgermeisterin oder der Bürgermeister allein über die Live-Übertragung einer Bürgerversammlung in Ton und Bild in das Internet entscheidet; die Einholung von Einwilligungen, Vorgaben zur Ausrichtung der Kameras, oder die Aufklärung darüber, dass eine Internetübertragung erfolgt, waren nicht vorgesehen. In meiner Stellungnahme habe ich insoweit die Bedeutung des **Grundrechts auf informationelle Selbstbestimmung** (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz – GG), insbesondere unter dem Aspekt der Verhältnismäßigkeit von Eingriffen in dieses Recht betont. Konkret habe ich empfohlen, über die Echtzeitübertragung den Gemeinderat einen Beschluss fassen zu lassen, Redebeiträge teilnehmender Personen nur bei Vorliegen wirksamer **Einwilligungen** (Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO) zu übertragen, und dafür Sorge zu tragen, dass Kameras nur die Versammlungsleitung sowie das Rednerpult erfassen und ansonsten nur Übersichtsaufnahmen gefertigt werden dürfen, die keine Identifizierung erlauben. Zudem sollten offene Abstimmungen nicht übertragen oder aufgezeichnet werden dürfen und die Gemeinde bei der Einladung zur Bürgerversammlung sowie vor deren Beginn über eine Echtzeitübertragung informieren. Meine Empfehlungen wurden zu einem großen Teil übernommen. Art.18 Abs. 4 Gemeindeordnung (GO) lautet in der ab 1. Januar 2024 geltenden Fassung nun wie folgt:

„[1]Die Bürgerversammlung findet in einem der Allgemeinheit zugänglichen Raum statt. [2]Ergänzend kann die Gemeinde durch Satzung oder durch Beschluss des

Gemeinderats eine Echtzeitübertragung der Bürgerversammlung in Ton und Bild über das Internet zulassen. [3]Ein Redebeitrag einer teilnehmenden Person darf nur übertragen werden, wenn sie dafür eine Einwilligung erteilt hat. [4]Kameras sind so einzurichten, dass nur die Versammlungsleitung sowie die redenden Personen erfasst werden. [5]Die Gemeinde informiert bei der Einladung zur Bürgerversammlung sowie vor Beginn über eine Echtzeitübertragung nach Satz 2. [6]Die Gemeinden können durch Satzung zulassen, dass Personen nicht persönlich anwesend sein müssen, um sich nach Abs. 3 zu beteiligen, sondern sich dazu auch über das Internet zuschalten können. [7]In der Satzung ist das Nähere zu den Voraussetzungen und zur Ausübung des Äußerungs- und Stimmrechts durch die zugeschalteten Personen zu regeln."

4.4.2 Gemeinderats-, Kreistags- und Bezirkstagssitzungen: Live-Übertragung ins Internet und Speicherung in einer Mediathek

Bei der Normierung einer Live-Übertragung von Gemeinderats-, Kreistags- und Bezirkstagssitzungen in das Internet und deren Speicherung in einer Mediathek, wurde dem Grundrecht auf informationelle Selbstbestimmung im Gesetzesentwurf bereits grundsätzlich Beachtung geschenkt. Lediglich die geplante Speicherdauer in der Mediathek von drei Monaten sowie die Verwendung teils nicht hinreichend bestimmter Begriffe im Gesetzesentwurf waren aus datenschutzrechtlicher Sicht zu kritisieren. Insoweit habe ich unter Verweis auf die Grundsätze der Datenminimierung und der Speicherbegrenzung (vgl. Art. 5 Abs. 1 Nr. c und e DSGVO) eine **kürzere Speicherdauer** und die Verwendung einheitlicher und klarer Begrifflichkeiten angemahnt. Im Ergebnis wurde die reguläre Speicherdauer auf sechs Wochen verkürzt. Die Neuregelungen finden sich in Art. 52 Abs. 4 Sätze 2 bis 7 GO, Art. 46 Abs. 4 Landkreisordnung (LKrO), Art. 43 Abs. 4 Bezirksordnung (BezO). Beispielsweise in Art. 52 Abs. 4 Sätze 2 bis 7 GO heißt es ab dem 1. Januar 2024 nun wie folgt:

„[2]Ergänzend kann die Gemeinde eine Echtzeitübertragung der öffentlichen Sitzungen des Gemeinderats in Ton und Bild über das Internet zulassen und die Aufzeichnungen in einer Sammlung audiovisueller Medien für die Dauer von sechs Wochen zum Abruf für jedermann bereitstellen. [3]Findet die nächste Sitzung nicht innerhalb von sechs Wochen statt, können die Aufzeichnungen bis zum Ende der nächsten Sitzung zum Abruf für jedermann bereitgestellt werden. [4]Danach sind die Aufzeichnungen jeweils zu löschen. [5]Die Beschlüsse nach Satz 2 bedürfen jeweils einer Zweidrittelmehrheit der abstimmenden Mitglieder des Gemeinderats. [6]Mit Ausnahme der oder des Vorsitzenden dürfen Ton und Bild von an der Sitzung teilnehmenden Personen nur mit deren Einwilligung übertragen, aufgezeichnet und gespeichert werden. [7]Eine Übertragung, Aufzeichnung und Speicherung des Bildes einer unbeteiligten Person ist nur im Rahmen von Übersichts- oder Hintergrundaufnahmen zulässig und dies auch nur, falls die räumlichen Verhältnisse Aufnahmen ohne unbeteiligte Personen nicht zulassen."

4.4.3 Kopien von Niederschriften kommunaler Gremiensitzungen

Das in Art. 54 Abs. 3 GO, Art. 48 Abs. 3 LKrO und Art. 45 Abs. 3 BezO neu vorgesehene Recht auf Kopien von Niederschriften öffentlicher Sitzungen kommunaler Gremien macht es aus meiner Sicht besonders dringlich, dass die gesetzlichen Anforderungen an den Inhalt derartiger Sitzungsniederschriften beachtet werden. Gesetzlich vorgesehen ist in Art. 54 Abs. 1 Satz 2 GO, Art. 48 Abs. 1 Satz 2 LKrO

und Art. 45 Abs. 1 Satz 2 BezO, dass eine Niederschrift den Tag und Ort der Sitzung, die anwesenden Gremiumsmitglieder, die behandelten Gegenstände, die Beschlüsse und das Abstimmungsergebnis enthält. Zudem kann ein Gremiumsmitglied verlangen, dass das eigene Abstimmungsergebnis in die Niederschrift aufgenommen wird. Gegenüber dem Innenministerium habe ich insoweit angemahnt, dass die **Niederschriften** von Sitzungen kommunaler Gremien nun noch strikter als bisher schon vorgesehen, auf die **gesetzlich vorgeschriebenen Mindestinhalte beschränkt bleiben müssen** und auf — die in der Praxis nach meinem Eindruck verbreiteten — überschießenden Inhalte verzichtet wird. Insbesondere dürfen derartige Niederschriften **nur im gesetzlich vorgesehenen Umfang personenbezogene Daten** enthalten. Beispielsweise Art. 54 Abs. 3 GO lautet in der ab 1. Januar 2024 geltenden Fassung nun wie folgt:

„[1]Die Gemeinderatsmitglieder können jederzeit die Niederschriften der öffentlichen sowie der nichtöffentlichen Sitzungen des Gemeinderats einsehen und sich unentgeltlich Kopien der Niederschriften der öffentlichen Sitzungen erteilen lassen. [2]Die Gemeindebürgerinnen und Gemeindebürger können Einsicht in die Niederschriften der öffentlichen Sitzungen des Gemeinderats nehmen und sich Kopien erteilen lassen. [3]Für die Fertigung der Kopien nach Satz 2 können die Gemeinden Kosten nach Maßgabe des Kostengesetzes erheben. [4]Die Sätze 2 und 3 gelten für auswärts wohnende Personen hinsichtlich ihres Grundbesitzes oder ihrer gewerblichen Niederlassungen im Gemeindegebiet entsprechend.“

4.4.4 Einbau und Betrieb elektronischer Wasserzähler mit Funkmodul

Der Gesetzentwurf sah des Weiteren vor, dass zukünftig die bisherigen datenschutzfreundlichen Regelungen zum Einbau und Betrieb elektronischer Wasserzähler mit Funkmodul entfallen. Diese bürgerfreundlichen Regelungen hatte das Innenministerium in enger Abstimmung mit mir entwickelt; sie waren fast sechs Jahre lang geltendes Recht, in der Rechtsprechung akzeptiert und in der kommunalen Praxis meinen Eindrücken aus Prüfung und Beratung zufolge auch „angekommen“ (vgl. näher meine Ausführungen im 27. Tätigkeitsbericht 2015/2016 unter Nr. 6.3, im 28. Tätigkeitsbericht 2017/2018 unter Nr. 7.3 sowie im 30. Tätigkeitsbericht 2020 unter Nr. 6.2). Art. 24 Abs. 4 GO sah in der bis zum 31. Dezember 2023 geltenden Fassung das Recht für die Gemeinden vor, nach Erlass entsprechender Satzungen für Einrichtungen der Wasserversorgung auch elektronische Wasserzähler mit oder ohne Funkmodul einzusetzen und zu betreiben. Betroffenen Personen wurde ein fristgebundenes, ansonsten voraussetzungsloses Widerspruchsrecht gegen den Einsatz des Funkmoduls gewährt. Insgesamt war mit dieser Regelung ein **ausgewogener Kompromiss** gefunden worden.

Vor diesem Hintergrund war ich negativ überrascht, dass der Gesetzesentwurf nun vorsah, diese **datenschutzfreundlichen Regelungen ersatzlos zu streichen.** Ich habe mich mit Nachdruck hierzu kritisch geäußert, weil mit dieser Streichung ein „Rückbau“ des Grundrechtsschutzes nicht nur beim Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG), sondern auch beim Recht auf Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG) verbunden ist. Das Innenministerium begründete die Änderung mit einem (angeblichen) Vorrang bereits bestehender bundesrechtlicher Bestimmungen, konkret von § 18 Abs. 2 Verordnung über Allgemeine Bedingungen für die Versorgung mit Wasser (AVBWasserV). Diese Regelung bietet aus datenschutzrechtlicher Sicht allerdings **keine tragfähige Rechtsgrundlage** für die Verarbeitung personenbezogener Verbrauchsdaten aus elektronischen Funkwasserzählern. Meiner Einschätzung

steht auch die vom Innenministerium insoweit angeführte Entscheidung des Bayerischen Verfassungsgerichtshofs vom 26. April 2022[92] nicht entgegen. Der Verfassungsgerichtshof bestätigt in dieser Entscheidung vielmehr gerade die **Verfassungskonformität der bestehenden Regelung**.

Hinzu kommt, dass mit den Streichungen zugleich die bislang in Art. 24 Abs. 4 Satz 3 Nr. 2 GO getroffene Regelung, wonach eine anlassbezogene Datenverarbeitung **im Einzelfall** zur Abwehr von Gefahren für den ordnungsgemäßen Betrieb der Wasserversorgungseinrichtung und zur Aufklärung von Störungen im Wasserversorgungsnetz zulässig ist, ausgeweitet werden sollte. Künftig sollten elektronische Funkwasserzähler schon „soweit dies zur Abwehr von Gefahren für den ordnungsgemäßen Betrieb der Wasserversorgungseinrichtung und zur Aufklärung von Störungen im Wasserversorgungsnetz erforderlich ist“ und damit nicht mehr nur „im Einzelfall“ ausgelesen werden können. Dadurch wird ein von mir stets als datenschutzrechtlich problematisch erachtetes, periodisch und autonom erfolgendes Funken von Zählernummer und Zählerständen über das Jahr hinweg ohne konkreten Anlass begünstigt.

Meine Bedenken hinsichtlich dieser Änderungen habe ich dem Innenministerium mehrmals umfassend erläutert und eindringlich gefordert, den alten Rechtszustand beizubehalten. Leider fanden meine Bedenken keine Berücksichtigung. Entgegen meiner expliziten datenschutzrechtlichen Forderung sind **Satzungsermächtigung, voraussetzungsloses Widerspruchsrecht sowie die sonstigen datenschutzfreundlichen Beschränkungen aus Art. 24 Abs. 4 GO in der bis zum 31. Dezember 2023 geltenden Fassung mit dem Jahresbeginn 2024 entfallen. Daher stellt sich die Situation der Bürgerinnen und Bürger, was den Einbau und Betrieb elektronischer Wasserzähler mit Funkmodul betrifft, wieder vergleichbar ebenso schutzlos dar wie schon vor der Datenschutzreform 2018. Das bedaure ich sehr.**

4.5 Landtags- und Bezirkswahl: Verbesserung bei der Bekanntmachung der Wahlkreisvorschläge

Im Zusammenhang mit der Landtags- und Bezirkswahl am 8. Oktober 2023 wandten sich mehrere Kandidatinnen und Kandidaten mit Beschwerden an mich. Sie rügten übereinstimmend die Bekanntmachung ihrer privaten Anschriften im Bayerischen Staatsanzeiger, der als ePaper auch im Internet zugänglich ist. Die Beschwerdeführerinnen und Beschwerdeführer seien in der Vergangenheit bereits Bedrohungen durch politisch Andersdenkende ausgesetzt gewesen und verstünden nicht, weshalb die Bekanntmachung ihrer privaten Adressen für eine wirksame Kandidatur notwendig sei. Insoweit habe ich den Beschwerdeführerinnen und Beschwerdeführern zunächst die Rechtslage bei der Bekanntmachung der Wahlkreisvorschläge erläutert.

Die Veröffentlichung der Anschriften von Wahlkreisbewerberinnen und Wahlkreisbewerbern im Bayerischen Staatsanzeiger stellt eine Verarbeitung personenbezogener Daten dar, für die öffentliche Stellen eine Rechtsgrundlage benötigen. § 35 Abs. 1 Satz 1 Nr. 2 Landeswahlordnung (LWO)[93] bestimmt, welche personenbezogenen Daten die Bekanntmachung der Wahlkreisvorschläge enthält.

[92] Vf. 5-VII-19, BeckRS 2022, 9317.

[93] Die Landeswahlordnung ist gemäß Art. 6 Bezirkswahlgesetz unter den dort genannten Maßgaben auf die Bezirkswahl anwendbar.

Dazu zählen grundsätzlich Familienname, Vorname, Beruf oder Stand, Geburtsjahr und **Anschrift der sich bewerbenden Personen**. Gemäß § 88 Abs. 1 Nr. 1 LWO erfolgt die Bekanntmachung der Wahlkreisvorschläge im Staatsanzeiger. Dieser erscheint seit jeher als Druckwerk, inzwischen zusätzlich aber auch als ePaper im Internet. Die von den Beschwerdeführern gerügte Bekanntmachung der privaten Anschriften lässt sich also grundsätzlich auf eine Rechtsgrundlage stützen. Dieser Grundsatz erfährt jedoch zwei Einschränkungen.

Erstens: Weist eine sich bewerbende Person bis zum Ablauf der Einreichungsfrist nach Art. 26 Landeswahlgesetz gegenüber dem Wahlkreisleiter nach, dass für sie im Melderegister eine **Auskunftssperre** nach § 51 Bundesmeldegesetz eingetragen ist, ist an Stelle der (Wohn-)Anschrift eine **Erreichbarkeitsanschrift** zu verwenden.

Zweitens: Kommt es neben der oben erläuterten Bekanntmachung der Wahlkreisvorschläge im Staatsanzeiger zusätzlich zu einer sogenannten **„Sekundärveröffentlichung"** im **Internet** nach § 88 Abs. 2 Satz 1 LWO, ist nach Satz 3 der Vorschrift hierbei dann **statt** einer **Anschrift** nur der **Wohnort** anzugeben.

§ 35 LWO
Bekanntmachung der Wahlkreisvorschläge
(1) [1]Die Bekanntmachung nach Art. 35 LWG enthält für jeden Wahlkreisvorschlag
1. […]
2. Familienname, Vorname, Beruf oder Stand, Geburtsjahr und Anschrift der sich bewerbenden Personen. Weist eine sich bewerbende Person bis zum Ablauf der Einreichungsfrist nach Art. 26 LWG gegenüber dem Wahlkreisleiter nach, dass für sie im Melderegister eine Auskunftssperre nach dem Bundesmeldegesetz eingetragen ist, ist an Stelle ihrer Anschrift eine Erreichbarkeitsanschrift zu verwenden; die Angabe eines Postfachs genügt nicht; der Wahlkreisleiter unterrichtet unverzüglich den Landeswahlleiter über die Erreichbarkeitsanschrift.

§ 88 LWO
Bekanntmachungen
(1) Soweit im Landeswahlgesetz und in dieser Verordnung nichts anderes bestimmt ist, erfolgen die dort vorgesehenen Bekanntmachungen
1. der Staatsregierung, des Staatsministeriums des Innern, für Sport und Integration, des Landeswahlleiters und der Wahlkreisleiter im Staatsanzeiger,
2. der Gemeinden durch öffentlichen Anschlag oder Aushang an möglichst mehreren Stellen der Gemeinde oder entsprechend den Vorschriften, die für die Bekanntmachung von Satzungen der Gemeinde gelten.
(2) [1]Der Inhalt der nach dem Landeswahlgesetz und dieser Verordnung vorgeschriebenen öffentlichen Bekanntmachungen kann zusätzlich im Internet veröffentlicht werden. [2]Dabei sind die Unversehrtheit, Vollständigkeit und Ursprungszuordnung der Veröffentlichung nach aktuellem Stand der Technik zu gewährleisten. [3]Statt einer Anschrift ist nur der Wohnort anzugeben. [4]Personenbezogene Daten in Internetveröffentlichungen von öffentlichen Bekanntmachungen nach § 35 sind spätestens sechs Monate nach Bekanntgabe des endgültigen Wahlergebnisses, von öffentlichen Bekanntmachungen nach § 70 Abs. 4 spätestens sechs Monate nach dem Ende der Wahlperiode zu löschen.

Um das aus datenschutzrechtlicher Sicht berechtigte Anliegen der Beschwerdeführerinnen und Beschwerdeführer zu unterstützen, habe ich mich an das für das Wahlrecht fachlich zuständige Bayerische Staatsministerium des Innern, für Sport

und Integration gewandt. Hinsichtlich des ePapers[94] des Staatsanzeigers vertrat das Innenministerium auch nach mehrfachem Schriftwechsel weiterhin den Standpunkt, dass dessen Erscheinen im Internet keine Sekundärveröffentlichung nach § 88 Abs. 2 Satz 1 LWO darstelle und somit auch keine Anpassung des Inhalts — Wohnort statt Anschrift — angezeigt sei. Insoweit konnte ich mit meinem Anliegen, § 88 Abs. 2 Satz 3 LWO auf das ePaper jedenfalls entsprechend anzuwenden und den bekanntgemachten Datenumfang so einzuschränken, zunächst leider nicht durchdringen.

Erfreulicherweise wird dies für zukünftige Wahlen jedoch voraussichtlich keine Rolle mehr spielen. In meinem Schreiben an das Innenministerium hatte ich nämlich auch angeregt, die in § 35 Abs. 1 Satz 1 Nr. 2 LWO aufgeführten Datenkategorien im Hinblick auf den Grundsatz der Datensparsamkeit (Art. 5 Abs. 1 Buchst. c DSGVO) ganz generell daraufhin zu **überprüfen**, ob es wirklich (weiterhin) **erforderlich** ist, die **Anschriften** der Wahlkreisvorschläge im Staatsanzeiger bekanntzumachen, oder ob es nicht vielmehr **ausreicht, nur den Wohnort anzugeben**. Das Innenministerium hat diese Anregung in ein fachlich zuständiges Bund-Länder-Gremium eingebracht. Die Beratungen ergaben erfreulicherweise, dass meiner datenschutzrechtlichen Anregung deutschlandweit Rechnung getragen werden soll. Angestrebt sind nun Änderungen der einschlägigen Wahlordnungen dahin, dass statt der vollen Anschrift nur der Wohnort (Ort der Hauptwohnung) anzugeben ist. Eine vergleichbare Vorgabe enthält bereits § 37 Abs. 1 Satz 2 und 3 Europawahlordnung:

„[2]Die Bekanntmachung enthält für jeden Wahlvorschlag die in § 32 Abs. 1 Satz 2 bezeichneten Angaben, wobei statt des Geburtsdatums nur das Geburtsjahr und statt der Anschrift nur der Wohnort (Ort der Hauptwohnung) der Bewerber und Ersatzbewerber anzugeben ist, sowie den Hinweis, für welches Land der Wahlvorschlag oder ob er als gemeinsame Liste für alle Länder aufgestellt ist. [3]Weist ein Bewerber bis zum Ablauf der Einreichungsfrist gegenüber dem Bundeswahlleiter nach, dass für ihn im Melderegister ein Sperrvermerk gemäß § 51 Absatz 1 des Bundesmeldegesetzes eingetragen ist, ist an Stelle seines Wohnortes der Ort seiner Erreichbarkeitsanschrift zu verwenden; die Angabe eines Postfachs genügt nicht.“

Aus datenschutzrechtlicher Sicht ist mit einer entsprechenden Normänderung generell eine deutliche Erhöhung des Schutzniveaus für Wahlbewerberinnen und Wahlbewerber verbunden. Dies geht weit über die bisher bloß vorgesehene Möglichkeit, die eigene Anschrift bei einer bereits eingetragenen Auskunftssperre nicht veröffentlichen lassen zu müssen, hinaus.

4.6 Anforderungen an die Videoüberwachung durch Kommunen: Bestätigung meiner Prüfpraxis durch den Bayerischen Verwaltungsgerichtshof

Auch oder gerade weil das Vorhandensein von Videoüberwachung im Alltag mittlerweile ein großes Ausmaß angenommen hat, ist der Datenschutz besonders gefordert, denn mit der personenscharfen Videoüberwachung sind stets Risiken für das Grundrecht auf informationelle Selbstbestimmung verbunden. Kommunale

[94] Das ePaper des Staatsanzeigers kann ausschließlich von Abonnenten auf der Internetseite der Bayerischen Staatszeitung abgerufen werden. Ein Auffinden des Dokuments über Google oder andere Suchmaschinen ist nicht möglich.

Videoüberwachungsmaßnahmen und die hiermit verbundenen Grundrechtseingriffe unterliegen daher insbesondere den in Art. 24 BayDSG geregelten Voraussetzungen, die ich in einer Orientierungshilfe detailliert erläutert habe.[95] In einer aktuellen Entscheidung hat sich der Bayerische Verwaltungsgerichtshof[96] mit der Auslegung des Art. 24 BayDSG befasst und hierbei Maßstäbe angelegt, die meine **Prüfpraxis bestätigen**. Anlass der Entscheidung war eine Videoüberwachungsanlage in einer zentralen Parkanlage einer bayerischen Stadt, gegen die ein Bürger Unterlassungsklage erhoben hatte. Das in erster Instanz zuständige Verwaltungsgericht hatte diese Klage noch abgewiesen. Der Bayerische Verwaltungsgerichtshof teilte diese Einschätzung in zweiter Instanz jedoch nicht, sondern gab dem Kläger Recht: Die Kommune hatte ihre Befugnisse mit der Videoüberwachung überschritten, die **Videoüberwachung** des Klägers in der zentralen Parkanlage **ist zu unterlassen**.

Die Befugnis in Art. 24 Abs. 1 BayDSG erfordert insbesondere das Bestehen einer **Gefahrenlage**, die durch die Videoüberwachungsanlage abgewehrt werden soll (vgl. den Wortlaut des Art. 24 Abs. 1 BayDSG: „zu schützen"). Zutreffend definiert der Bayerische Verwaltungsgerichtshof den Gefahrentatbestand in seinem Urteil als „Gefahrensituation", „Gefährdungs-" oder „Gefahrenlage" (Rn. 48 f., 58).[97] Zu deren Annahme bedarf es grundsätzlich **konkreter, ortsbezogener Tatsachen,** die eine entsprechende Gefahrbeurteilung tragen. In der Regel bedeutet dies, dass es bereits in der Vergangenheit einschlägige **Vorfälle am Ort der geplanten Videoüberwachung** gegeben haben muss. Nicht ausreichend ist dagegen ein allgemeines **Gefahrenpotential**. Die erforderliche Gefahr muss vielmehr unter Berücksichtigung von Standort und Einfallswinkel **individuell** begründet werden, da kommunale Videoüberwachungen durch eine kleinräumige Überwachung eines Gefahrenbereichs gekennzeichnet sind. Dies macht grundsätzlich eine kameraspezifische Vorfallsdokumentation notwendig. Gerade auch die Notwendigkeit einer solchen detaillierten Vorfallsdokumentation hat der Bayerische Verwaltungsgerichtshof nun bestätigt und ausdrücklich klargestellt, dass ein theoretisches oder nur subjektiv empfundenes, allgemeinen Unsicherheitsgefühl keine Videoüberwachung rechtfertigt.

Zur Einschätzung der Gefahrensituation bedarf es zunächst einmal einer Prognose, die auf einer **Tatsachenbasis** beruhen muss. Hierzu muss die verantwortliche Stelle eine ausführliche Vorfallsdokumentation führen, in der die relevanten Vorfälle genau protokolliert werden. Bloße Schätzungen auf der Basis von Erinnerungswissen reichen insoweit nicht aus.

Außerdem ist nicht jeder Vorfall, der sich im zu überwachenden Bereich ereignet hat, auch relevant für eine Videoüberwachung und darf in die Vorfallsdokumentation aufgenommen werden. Dies hat der Bayerische Verwaltungsgerichtshof deutlich gemacht und alle protokollierten Fälle als unerheblich angesehen, die keine Aussagekraft für eine Gefährdungslage vor Ort hatten. Hiervon betroffen waren in dem der Entscheidung zugrundeliegenden Sachverhalt etwa „Fund/Verlust"-Fälle sowie verbale Beleidigungen, die „von der Videoüberwachung ohnehin nicht eingedämmt werden". Außerdem seien „aus der Emotion heraus – spontan

[95] Bayerischer Landesbeauftragter für den Datenschutz, Videoüberwachung durch bayerische öffentliche Stellen, Stand 2/2020, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018".

[96] Bayerischer Verwaltungsgerichtshof, Urteil vom 30. Mai 2023, 5 BV 20.2104, BeckRS 2023, 12517.

[97] Vgl. Rn. 45, 48 f., 50, 55, 58 und 65.

und affektiv – begangene Körperverletzungen“ für die Videoüberwachung ebenfalls nicht relevant.[98]

Zusammengefasst sind damit hohe Anforderungen an die Vorfallsdokumentation, welche eine eindeutige Einordung der Schadensfälle und eine Einstufung der Örtlichkeit als „gefährlich“ ermöglichen muss, zu stellen. Insbesondere Bagatellrisiken, die eine Vorfallsdokumentation „aufblähen“, reichen gerade bei Vollüberwachung einer zentralen Kommunikationsfläche nicht aus, um eine Videoüberwachung zu rechtfertigen.

4.7 Datenschutzrechtliche Vorgaben für eine automatisierte Kennzeichenerfassung beim Kameraparken

Das Passieren einer durch Schranke verschlossenen Parkplatzeinfahrt nach dem Ziehen eines Parktickets und die sich nach dem Ende des Parkvorgangs anschließende Entwertung dieses Tickets mittels (Bar-)Zahlung am Automaten vor der ebenfalls beschrankten Ausfahrt: alltägliche und über lange Zeit unveränderte, weitgehend anonyme Vorgänge. Mittlerweile gehen jedoch auch öffentliche Stellen dazu über, beim sogenannten Kameraparken von ihnen betriebene Parkhäuser, Tiefgaragen oder Parkplätze mittels automatisierter Kennzeichenerfassung zu digitalisieren. Hierbei wird auf das Passieren von Schranken und das Ziehen von Parktickets bei der Einfahrt sowie eine Entwertung vor der Ausfahrt verzichtet. Vielmehr werden bei allen einfahrenden Kraftfahrzeugen die Kennzeichen mittels Kamera als (Einzel-)Bilder erfasst und jeweils zusammen mit der Uhrzeit gespeichert. Bei der Ausfahrt werden die Kennzeichen nochmals als (Einzel-)Bilder erfasst; dabei wird überprüft, ob das nach der jeweiligen Parkdauer geschuldete Entgelt am Kassenautomaten – regelhaft ist hierfür die Eingabe des Kennzeichens erforderlich – entrichtet wurde. Maßgeblich für diese Digitalisierung scheinen zwei Gründe zu sein: Zunächst einmal sehen die Betreiber darin eine betriebswirtschaftlich vorteilhafte Möglichkeit, auf die störanfällige und damit personalintensive technische Infrastruktur in Gestalt von Schranken und Ticketautomaten verzichten zu können. Zum anderen kann die uhrzeitgenaue Kennzeichenerfassung die derzeit beim Verlust des Parktickets entstehenden Nachweisprobleme der Kundinnen und Kunden hinsichtlich der Parkdauer lösen beziehungsweise Betrugsversuche erschweren.

Die digitalisierte Abrechnung des Parkvorgangs – anders als früher an die Verarbeitung personenbezogener Daten in Gestalt des Kfz-Kennzeichens gekoppelt – wird datenschutzrechtlich relevant. Insoweit habe ich einer privatrechtlich organisierten — und damit in Bezug auf den Parkvorgang auf Ebene der Gleichordnung zum Bürger agierenden — öffentlichen Stelle, auf deren entsprechende Planungen ich durch eine Bürgereingabe aufmerksam wurde, die datenschutzrechtlichen Vorgaben für eine automatisierte Kennzeichenerfassung beim Kameraparken zu Abrechnungszwecken erläutert.

4.7.1 Erfordernis einer Rechtsgrundlage für die Datenverarbeitung

Die Kennzeichen von Kraftfahrzeugen, deren Halterinnen oder Halter natürliche Personen sind, stellen regelmäßig personenbezogene Daten gemäß Art. 4 Nr. 1 DSGVO dar. Daher sind die mit dem Kameraparken verbundenen Vorgänge wie

[98] Vgl. Rn. 50 ff.

Kennzeichenerfassung, Speicherung und Abgleich mit Uhrzeit und Zahlvorgang Verarbeitungen nach Art. 4 Nr. 2 DSGVO, die einer Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO bedürfen.

4.7.2 Keine Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO

Eine spezialgesetzliche Rechtsgrundlage für die Verarbeitung personenbezogener Daten beim Kameraparken ist nicht ersichtlich, insbesondere ist aufgrund der bloßen Erstellung von (Einzel-)Bildaufnahmen Art. 24 BayDSG als spezielle Befugnis für eine Videoüberwachung durch öffentliche Stellen nicht einschlägig. Zwar ist mit diesem Befund ein Rückgriff auf die allgemeine Datenverarbeitungsbefugnis des Art. 4 Abs. 1 BayDSG nicht von vornherein ausgeschlossen, jedoch hatte ich erhebliche Bedenken hinsichtlich der Erforderlichkeit einer auf Art. 4 Abs. 1 BayDSG gestützten Datenverarbeitung, da die Abwicklung der Parkvorgänge unzweifelhaft auch analog möglich war und ist.

4.7.3 Keine Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 Buchst. b und f DSGVO

Soweit von der öffentlichen Stelle Art. 6 Abs. 1 UAbs. 1 Buchst. b und f DSGVO als mögliche Rechtsgrundlagen für die Datenverarbeitung ins Spiel gebracht wurden, habe ich zum einen darauf hingewiesen, dass für die Erforderlichkeit einer Datenverarbeitung zur Vertragserfüllung gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO nicht der bloße Bezug des Verarbeitungsvorgangs zu einem Vertragsverhältnis (hier wohl Miete nach § 535 Bürgerliches Gesetzbuch) genügt. Vielmehr muss ein **unmittelbarer Zusammenhang** zwischen der Verarbeitung und dem konkreten Zweck des Vertragsverhältnisses bestehen,[99] beziehungsweise die Datenverarbeitung muss **objektiv unerlässlich** sein, um den Hauptgegenstand des Vertrags zu erfüllen,[100] was ich jedoch beim unschwer analog abwickelbaren Parkverhältnis **nicht** erkennen konnte. Im Hinblick auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO habe ich darauf hingewiesen, dass einseitige, also nicht beiderseitig konsentierte Datenverarbeitungen im hier vorliegenden Kontext rechtsgeschäftlicher Beziehungen auf Ebene der Gleichordnung einen Fremdkörper darstellen und daher eine auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO gestützte Erforderlichkeit der Datenverarbeitung insoweit nur angenommen werden kann, wenn insbesondere die **Einholung von Einwilligungen** nach Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO **unzumutbar** ist.[101] Diese Unzumutbarkeit konnte ich jedoch **nicht** erkennen, da die Einholung von Einwilligungen – unter den sogleich näher dargelegten Voraussetzungen – möglich ist.

4.7.4 Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO

Nicht von vornherein ausgeschlossen schien es mir dagegen, die uhrzeitgenaue (Einzel-)Bilderfassung der Kfz-Kennzeichen und die anderen bereits erläuterten

[99] Vgl. auch Albers/Veit, in: Wolff/Brink/v. Ungern-Sternberg, Beck'scher Online-Kommentar Datenschutzrecht, Stand 5/2023, Art. 6 DSGVO Rn. 44.

[100] Vgl. Europäischer Gerichtshof, Urteil vom 4. Juli 2023, C-252/21, Rn. 97 ff.

[101] Vgl. auch Albers/Veit, in: Wolff/Brink/v. Ungern-Sternberg, Beck'scher Online-Kommentar Datenschutzrecht, Stand 5/2023, Art. 6 DSGVO Rn. 69.

Datenverarbeitungen beim Kameraparken auf **wirksame Einwilligungen** der Parkierenden nach Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO zu stützen.

Angesichts der Tatsache, dass öffentliche Stellen primär aufgrund von gesetzlichen Befugnissen handeln sollen und diese nicht beliebig durch die Einholung von Einwilligungen ausweiten können (siehe meine Ausführungen im 29. Tätigkeitsbericht 2019 unter Nr. 5.6.2), ist es jedoch, um hiervon Gebrauch machen zu können, erforderlich, zunächst einmal gemäß Art. 5 Abs. 2 DSGVO den Nachweis zu erbringen, dass es eine **signifikante Zahl von Betrugsversuchen oder kundenverursachten (vorsätzlichen) Störfällen gibt, die eine Kennzeichenerfassung rechtfertigen** (Grundsatz der Datenminimierung, Art. 5 Abs. 1 Buchst. c DSGVO). Bloße technikbedingte Störanfälligkeiten bei der Verarbeitung von Papiertickets können insoweit nicht berücksichtigt werden, da dieses Risiko vom Betreiber zu tragen ist.

Die Wirksamkeit der Einwilligung als solcher ist des Weiteren nur gegeben, wenn Betroffene eine „echte", freie Wahl haben und **über die Datenverarbeitung bereits vor der Erfassung durch die Kennzeichenkameras** adäquat **informiert sind**.[102] Bereits im Zufahrtsbereich vor dem Passieren der Schranke und damit vor erstmaliger Aufzeichnung durch die Kennzeichenkamera sollte potentiellen Benutzern daher die Möglichkeit eröffnet werden, zu wenden und sich damit gegen eine Aufzeichnung zu entscheiden. Hierzu bedarf es entsprechender Hinweistafeln an den Einfahrten. Außerdem sollte an etwaigen Fußgängerausgängen, am Einfahrtsterminal und auf der Website des Betreibers auf die Datenverarbeitung hingewiesen werden. Gerade letzteres ermöglicht es Betroffenen, sich vorab über Alternativen zu informieren.

Schließlich muss gewährleistet sein, dass Betroffene zumindest während einer gewissen „Karenzzeit" wieder aus der Parkanlage ausfahren können, ohne dass ihre Kennzeichendaten (weiter) gespeichert werden. Den Betroffenen soll so ermöglicht werden, auf andere Anlagen ohne Kennzeichenerfassung ausweichen zu können.

Gemäß dem Zweckbindungsgrundsatz nach Art. 5 Abs. 1 Buchst. b DSGVO dürfen die im Rahmen der Kennzeichenerfassung erhobenen Daten **ausschließlich zur Abwicklung des Bezahlvorgangs und etwaiger weiterer notwendiger Maßnahmen**, nicht jedoch für weitere Analysen oder zur Reichweitenmessung oder gar zur Erstellung von Bewegungsprofilen verwendet werden.

[102] Vgl. Bayerischer Landesbeauftragter für den Datenschutz, Die Einwilligung nach der Datenschutz-Grundverordnung, Orientierungshilfe, Stand 9/2021, dort insbesondere Rn. 65 ff., Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018".

5 E-Government und öffentliche Register

5.1 Unzulässige Melderegisterauskunft für Kinderfest einer politischen Partei

Ein wiederkehrendes Thema in meiner Prüfungs- und Beratungspraxis sind Gruppenauskünfte aus dem Melderegister zum Zweck der Wahlwerbung. Auch vor den Wahlen zum 19. Bayerischen Landtag sowie den 17. Bezirkswahlen erreichten mich zahlreiche Anfragen, die ich oftmals bereits durch Hinweis auf meine bereits seit längerem auf meiner Website bereitgehaltene Handreichung[103] beantworten kann. Von dieser Publikation können auch Kommunen profitieren, wie sich im Berichtszeitraum wieder einmal zeigte:

Die Meldebehörde einer kreisangehörigen Gemeinde hatte auf Anweisung des Bürgermeisters die **Adressdaten von Schulkindern** unter zwölf Jahren abgerufen. Diese Daten hat der erste Bürgermeister dann verwendet, um die Betreffenden zu einer Veranstaltung „seiner" Partei, nämlich einem **Kinderfest**, mittels persönlich an sie adressierter Schreiben **einladen** zu lassen. Diesen Verstoß gegen datenschutzrechtliche Vorgaben des Melderechts habe ich förmlich beanstandet.

Die **Verarbeitung** von **Meldedaten** bedarf stets einer **Rechtsgrundlage**. Dabei handelt es sich übrigens nicht um Neuerung im Zuge der Datenschutzreform 2018. Die Verarbeitung von Meldedaten ist schon seit langer Zeit in detaillierten Befugnissen geregelt, die festlegen, was die Meldebehörden dürfen, und was eben nicht. Am „Dürfen" hat es im konkreten Fall offensichtlich gefehlt. Dies habe ich der Gemeinde im Wesentlichen wie folgt erläutert:

Zwar dürfen gemäß § 37 Abs. 1 in Verbindung mit § 34 Abs. 1 Bundesmeldegesetz (BMG) bestimmte Meldedaten innerhalb der Gemeindeverwaltung weitergegeben werden, soweit dies zur Erfüllung einer öffentlichen Aufgabe der Gemeinde erforderlich ist. Im vorliegenden Fall wurden die Meldedaten aber **nicht** im Rahmen der **Aufgabenerfüllung der Gemeinde** verwendet, sondern zu **parteipolitischen Zwecken**. Der Bürgermeister hat insoweit nicht als Gemeindeorgan, sondern als Mitglied seiner Partei gehandelt. Die Befugnisnorm war damit nicht einschlägig.

§ 37 BMG
Datenweitergabe
(1) Innerhalb der Verwaltungseinheit, der die Meldebehörde angehört, dürfen unter den in § 34 Absatz 1 genannten Voraussetzungen sämtliche der in § 3 Absatz 1 aufgeführten Daten und Hinweise weitergegeben werden. Für die Einsichtnahme und Weitergabe von Daten und Hinweisen nach § 3 Absatz 2 gilt § 34 Absatz 3 entsprechend.
[…]

[103] Bayerischer Landesbeauftragter für den Datenschutz, Auskunft aus dem Melderegister an politische Parteien vor Wahlen, Aktuelle Kurz-Information 28, Stand 2/2020, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018"

Auch der die Übermittlung von Meldedaten zu Wahlwerbezwecken an Parteien regelnde und von mir in meiner erwähnten Handreichung im Einzelnen erläuterte § 50 Abs. 1 BMG war nicht einschlägig. Nach dieser Vorschrift darf die Meldebehörde Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen in den sechs der Wahl oder Abstimmung vorangehenden Monaten Auskunft über zu bestimmten Altersgruppen gehörende Personen aus dem Melderegister (regelmäßig deren Familienname, Vornamen und Anschrift) erteilen. Diese Norm beschränkt sich jedoch auf die Meldedaten von **Wahlberechtigten**, zu denen die im konkreten Fall betroffenen **Kinder unter zwölf Jahren** offensichtlich **nicht** zählten. Die Übermittlung der Adressdaten konnte damit nicht auf § 50 Abs. 1 BMG gestützt werden.

Auch eine Gruppenauskunft im „öffentlichen Interesse" gemäß § 46 BMG schied aus. Eine solche hätte das Vorliegen eines öffentlichen Interesses vorausgesetzt. Unter einem öffentlichen Interesse ist das **Interesse der Allgemeinheit** zu verstehen, welches von dem Interesse einzelner Personen oder Gruppen zu unterscheiden ist. **Interessen von politischen Parteien** stellen grundsätzlich **kein öffentliches Interesse** dar.[104]

Der Datenschutzverstoß hat ein erhebliches Gewicht. Die Gemeinde hat nicht nur die Zweckbindungen der Meldedaten auf eine besonders augenfällige Weise missachtet, sie hat auch leichtfertig in großem Umfang personenbezogene Daten von Kindern offengelegt, die nicht nur aus Sicht des Datenschutzrechts besonders schutzbedürftig sind. Ein solcher Missbrauch des Melderegisters ist ein in meiner Prüfungspraxis zum Glück seltener Einzelfall. Gleichwohl möchte ich den Vorfall zum Anlass nehmen, eindringlich daran zu erinnern, dass Meldedaten innerhalb der Gemeinde nicht „einfach so" ohne Rücksicht auf rechtliche Vorgaben abgerufen werden dürfen.

5.2 Örtliche Fahrzeugregister: keine Nutzung für personalisierte Informationsschreiben über Dieselfahrverbote

Eine öffentliche Stelle plante im Berichtszeitraum, bereits bestehende Dieselfahrverbote in ihrer innerstädtischen Umweltzone erneut zu verschärfen. Anders als in der Vergangenheit ging die Information der hiervon betroffenen Halterinnen und Halter von Kraftfahrzeugen über die Verschärfung diesmal aber mit einer Verarbeitung deren personenbezogener Daten einher: Um die betroffenen Fahrzeughalterinnen und Fahrzeughalter mittels personalisierter Anschreiben zu informieren, ermittelte zunächst die KfZ-Zulassungsbehörde Namen und Adressen aus dem örtlichen Fahrzeugregister. Diese Daten stellte sie dann dem IT-Referat zur Verfügung, welches schließlich personalisierte Informationsschreiben für das Klima- und Umweltschutzreferat versandte. Empfängerinnen und Empfänger derartiger Schreiben haben sich bei mir über die Datenverarbeitungen beschwert, was ich zum Anlass einer eingehenden Überprüfung genommen habe. Insoweit kam ich trotz der mit der Information verfolgten erkennbar grundsätzlich guten Absicht der öffentlichen Stelle nicht umhin, einen **Datenschutzverstoß** festzustellen, da es an der von Art. 6 Abs. 1 UAbs. 1 DSGVO geforderten Rechtsgrundlage für die Datenverarbeitungen fehlte.

[104] Schwabenbauer, in: Engelbrecht/Schwabenbauer, BMG, § 46 Rn. 18.

5.2.1 Keine Befugnis für Datenauslesung aus dem örtlichen Fahrzeugregister

Umweltzonen oder sog. Niedrig-Emissions-Gebiete gibt es in deutschen Kommunen seit 2008. Diese haben ihren Niederschlag auch im Straßenverkehrsrecht, etwa in der Straßenverkehrs-Ordnung (StVO) in Gestalt der Kenntlichmachung mittels der Vorschriftszeichen Nr. 270.1 und 2 gemäß § 45 Abs. 1 Buchst. f StVO gefunden. Somit kann davon ausgegangen werden, dass deren Existenz dem Gesetzgeber 2021 sehr wohl bewusst war, als er die Möglichkeit von speziell auch dem Umweltschutz dienenden Halterinformationen durch eine Ergänzung des Straßenverkehrsgesetzes (StVG) um die § 32 Abs. 3 und § 63 d geregelt hat. Die Nutzung der örtlichen Fahrzeugregister durch die Kommunen für die Information betroffener Halter über örtliche Fahrverbote hat der Gesetzgeber hierbei aber gerade nicht geregelt. Vielmehr ist nur eine Rechtsgrundlage für die Information über fahrzeugbezogene Maßnahmen durch das Kraftfahrbundesamt anhand des zentralen Fahrzeugregisters geschaffen worden. Die betroffene öffentliche Stelle habe ich daher auf Folgendes hingewiesen:

Fachgesetzliche Befugnisnormen für die Datenauslesung waren **nicht** ersichtlich. Insbesondere schied § 63d StVG offensichtlich schon deswegen aus, weil diese Norm gerade nicht die örtliche Zulassungsbehörde, sondern nur das Kraftfahrt-Bundesamt zur Verwendung der Daten zwecks Halterinformation – über dem Umweltschutz dienende fahrzeugbezogene Maßnahmen – ermächtigt.

§ 63d StVG
Informationen an die Halter
Das Kraftfahrt-Bundesamt darf die nach § 33 Absatz 1 gespeicherten Fahrzeugdaten und Halterdaten im Einvernehmen mit dem Bundesministerium für Verkehr und digitale Infrastruktur zu den in § 32 Absatz 3 genannten Zwecken verwenden und im Einzelfall schriftliche Informationen an die Fahrzeughalter übermitteln, um sie über Maßnahmen im Sinne des § 32 Absatz 3 zu informieren. Das Bundesministerium für Verkehr und digitale Infrastruktur erteilt sein Einvernehmen nach Satz 1, wenn es die jeweilige Maßnahme für geeignet hält, die in § 32 Absatz 3 Nummer 2 genannten Zwecke unter Berücksichtigung der Umstände des Einzelfalls und unter Abwägung dieser Zwecke mit den Interessen der betroffenen Fahrzeughalter angemessen zu fördern. Die Eignung der angemessenen Zweckförderung wird bei staatlich geförderten Maßnahmen vermutet, so dass das Einvernehmen ohne nähere Prüfung erteilt werden darf.

Die Datenauslesung konnte – unabhängig von der hier mangels Relevanz offen gelassenen Frage, ob dies für eine derart weitreichende, weil massenhafte Verarbeitung überhaupt möglich gewesen wäre – auch **nicht** auf die allgemeine Befugnisnorm des **Art. 4 Abs. 1 BayDSG** gestützt werden. Zum einen war die Datenverarbeitung nicht zur Erfüllung einer öffentlichen Aufgabe der Zulassungsbehörde erforderlich. Die Aufgaben einer öffentlichen Stelle ergeben sich primär aus den entsprechenden gesetzlichen Aufgabenzuweisungen im nationalen oder europäischen Recht.[105] Angesichts der in § 63d StVG getroffenen klaren Entscheidung des Gesetzgebers für eine umweltschutzrechtlich motivierte Halterinformation durch das Kraftfahrt-Bundesamt erschien eine darauf gerichtete Auslesung des örtlichen Fahrzeugregisters durch die öffentliche Stelle schon nicht für deren Aufgabenerfüllung erforderlich. Zum anderen unterliegen personenbezogene Daten einer **Zweckbindung** (vgl. Art. 5 Abs. 1 Buchst. b DSGVO), wobei der

[105] Vgl. Stief, in: Schröder, Bayerisches Datenschutzgesetz, 2021, Art. 4 BayDSG Rn. 38.

Zweckbindungsgrundsatz in § 32 StVG für Fahrzeugregister **spezialgesetzlich** ausgeformt ist.

§ 32 StVG
Zweckbestimmung der Fahrzeugregister
(1) Die Fahrzeugregister werden geführt zur Speicherung von Daten
1. für die Zulassung und Überwachung von Fahrzeugen nach diesem Gesetz oder den darauf beruhenden Rechtsvorschriften,
2. für Maßnahmen zur Gewährleistung des Versicherungsschutzes im Rahmen der Kraftfahrzeughaftpflichtversicherung,
3. für Maßnahmen zur Durchführung des Kraftfahrzeugsteuerrechts,
4. für Maßnahmen nach dem Bundesleistungsgesetz, dem Verkehrssicherstellungsgesetz, dem Verkehrsleistungsgesetz oder den darauf beruhenden Rechtsvorschriften,
5. für Maßnahmen des Katastrophenschutzes nach den hierzu erlassenen Gesetzen der Länder oder den darauf beruhenden Rechtsvorschriften,
6. für Maßnahmen zur Durchführung des Altfahrzeugrechts,
7. für Maßnahmen zur Durchführung des Infrastrukturabgabenrechts,
8. für Maßnahmen zur Durchführung der Datenverarbeitung bei Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion nach diesem Gesetz oder nach den auf diesem Gesetz beruhenden Rechtsvorschriften und
9. für Maßnahmen nach oder zur Umsetzung von unionsrechtlichen Vorschriften, soweit diese die Verwendung von in den Fahrzeugregistern gespeicherten Daten erfordern.
(2) Die Fahrzeugregister werden außerdem geführt zur Speicherung von Daten für die Erteilung von Auskünften, um
1. Personen in ihrer Eigenschaft als Halter von Fahrzeugen,
2. Fahrzeuge eines Halters oder
3. Fahrzeugdaten
festzustellen oder zu bestimmen.
(3) Das Zentrale Fahrzeugregister wird außerdem geführt zur Verwendung und Übermittlung der nach § 33 Absatz 1 gespeicherten Daten, um im Einzelfall Halter von Fahrzeugen zu informieren über fahrzeugbezogene Maßnahmen,
1. die für ihre Fahrzeuge in Betracht kommen und
2. die dem Schutz der Verkehrssicherheit, der Gesundheit von Personen oder der Umwelt dienen.
Fahrzeugbezogene Maßnahmen können insbesondere auf die Verbesserung von Fahrzeugeigenschaften, insbesondere auf die Verbesserung des Abgasverhaltens, des Geräuschverhaltens, des Kraftstoffverbrauchs oder des Fahrverhaltens abzielen.

Umweltschutzbezogene Halterinformationen gehören in dem in **§ 32 Abs. 3 StVG** geregelten Umfang zu den zulässigen Zwecken. Darauf konnte sich die öffentliche Stelle aber nicht berufen, denn die Norm betrifft ausweislich ihres klaren Wortlauts nur das **zentrale Fahrzeugregister**. Eine von der öffentlichen Stelle ins Spiel gebrachte analoge Anwendung auf das örtliche Fahrzeugregister schied schon mangels Regelungslücke aus. Daneben war im Hinblick auf die für eine Analogie erforderliche Vergleichbarkeit aber gerade auch fraglich, ob es sich bei einem Dieselfahrverbot überhaupt um eine der Umwelt dienende fahrzeugbezogene Maßnahme in diesem Sinne handelt. Die in Satz 2 der Norm genannten Hauptfälle zielen nämlich auf eine Verbesserung von Fahrzeugeigenschaften, insbesondere auf die Verbesserung des Abgasverhaltens, des Geräuschverhaltens, des Kraftstoffverbrauchs oder des Fahrverhaltens ab. Somit hatte der Gesetzge-

ber primär technisch – deutschlandweit – mögliche Verbesserungen **am Fahrzeug selbst** im Blick. Die Umweltzone veranlasst hingegen nicht Änderungen am Fahrzeug selbst, sondern **– primär örtlich vorgegebene – Veränderungen am Fahrverhalten** (Einfahrverbot).

Denkbar wäre es vor diesem rechtlichen Hintergrund daher allein gewesen, die speziell umweltschutzrechtlich motivierten und fahrzeugbezogenen §§ 32 Abs. 3, § 63 d StVG gleichsam beiseite zu schieben und die Nutzung des örtlichen Fahrzeugregisters auf die allgemeinen Vorschriften der §§ 35 Abs. 1 Nr. 1, 32 Abs. 1 Nr. 9 StVG zu stützen. Dies musste aber letztlich auch ausscheiden, da der ebenfalls im Jahr 2021 neu – und damit im Bewusstsein der Existenz unionsrechtlicher Vorgaben über die Luftqualität [106] – eingeführte Registerzweck des § 32 Abs. 1 Nr. 9 StVG ausweislich der Begründung des Gesetzentwurfs [107] diesen Zweck weder nennt noch ersichtlich ist, dass die Verschärfung lokaler Umweltzonen die Verarbeitung von örtlichen Fahrzeugregisterdaten erfordert. Dies kann schon deswegen nicht der Fall sein, da von derartigen Maßnahmen auch in erheblichem Umfang der überörtliche Durchgangsverkehr betroffen ist und sich zu diesen Fahrzeugen gar keine Daten im örtlichen Fahrzeugregister finden.

5.2.2 Keine Befugnis für Versand individualisierter Informationsschreiben

Auch insoweit war wiederum **keine fachgesetzliche Befugnisnorm** ersichtlich. Wie bereits erläutert, weisen §§ 63d, 32 Abs. 3 StVG die Befugnis zur Halterinformation bewusst dem **Kraftfahrt-Bundesamt** zu, und zwar mittels der Daten aus dem **zentralen Fahrzeugregister**.

Der Versand der individualisierten Schreiben konnte auch **nicht** etwa auf die allgemeine Befugnisnorm des **Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG** gestützt werden. Selbst wenn man nicht so weit geht, insoweit einen Rückgriff auf die Norm bereits durch §§ 63d, 32 Abs. 3 StVG gemäß Art. 1 Abs. 5 BayDSG von vornherein als gesperrt anzusehen, weil Fragen der Übermittlung in diesen Normen direkt adressiert sind, **fehlte** es doch jedenfalls an einer **öffentlichen Aufgabe** bei der öffentlichen Stelle. Eine individualisierte Information betroffener Halter über die Verschärfung von Dieselfahrverboten war nämlich materiell-rechtlich im anzuwendenden Umweltrecht nicht vorgesehen und die Regelungen des Straßenverkehrsgesetzes (§§ 63d, 32 Abs. 3 StVG) weisen die Halterinformation ausschließlich dem **Kraftfahrt-Bundesamt** zu. Im Übrigen waren weder bei der Einführung noch bei den bisherigen Verschärfungen der Umweltzone entsprechende Informationsschreiben versandt worden. Dagegen konnte auch nicht mit Erfolg vorgebracht werden, dass es sich um eine deutschlandweit einmalige Konstellation handele, die der Gesetzgeber in seine Überlegungen noch nicht habe einstellen können und zudem die Rechtslage mittlerweile komplizierter geworden sei. Selbst wenn nun ein derart gestiegener Informationsbedarf bestünde, wäre es Aufgabe des Gesetzgebers gewesen, diese Aufgabe (entweder im Umweltrecht oder im StVG) zu normieren und Rahmenbedingungen für die Information der Betroffenen zu schaffen. Daneben bestanden aber auch insoweit **Zweifel an der Erfor-**

[106] Richtlinie 2008/50/EG des Europäischen Parlaments und des Rates vom 21. Mai 2008 über Luftqualität und saubere Luft für Europa (ABl. L 152 vom 11. Juni 2008, S. 1, berichtigt ABl. L 336 vom 8. Dezember 2012, S. 101), zuletzt geändert durch Richtlinie (EU) 2015/1480 der Kommission vom 28. August 2015 (ABl. L 226 vom 29. August 2015, S. 4).

[107] Vgl. Bundestags-Drucksache 19/28684, S. 53.

derlichkeit einer auf Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG gestützten individualisierten Halterinformation, weil Alternativen vorhanden waren, die keinen Rückgriff auf personenbezogene Daten erforderten. Insbesondere kam das **Aufstellen entsprechender Schilder** mit zeitlichem Vorlauf in Betracht, was bei vergleichbaren Situationen, wie etwa der Einrichtung von Parkverbotszonen, durch das Aufstellen mobiler Halteverbotsschilder praktiziert wird.[108] Wer am Verkehr teilnimmt, hat die angeordneten Gebote und Verbote zu befolgen (§ 41 Abs. 1 StVO) und sich zuvor über die Verkehrsschilder und ihre Bedeutung zu informieren. Die Rechtsordnung gewährt grundsätzlich keinen Schutz der allgemeinen Erwartung, die geltende Rechtslage werde zukünftig unverändert **fortbestehen**. Zudem wurde die Rechtslage auf der Webseite der öffentlichen Stelle sowie in der Presse ausreichend thematisiert.

Insoweit war es auch unerheblich, dass das Umweltreferat selbst die Daten gar nicht erlangt hat, da diese von der Zulassungsbehörde an das IT-Referat übermittelt wurden, welches den Versand der Schreiben für das Referat für Klima- und Umweltschutz übernahm. Diese Vorgehensweise ähnelt zwar dem sog. Adressmittlungsverfahren.[109] Wie ich aber bereits in meinem 29. Tätigkeitsbericht 2019 unter Nr. 6.1.2.5 ausgeführt habe, gelten auch insoweit die Erfordernisse des Vorliegens entsprechender Rechtsgrundlagen für die erfolgten Datenverarbeitungen. Daran fehlte es aber wie erläutert bei der öffentlichen Stelle.

[108] Vgl. Bundesverwaltungsgericht, Urteil vom 24. Mai 2018, 3 C 25.16.

[109] Bei dem sog. Adressmittlungsverfahren übergeben die eine Befragung durchführenden Stellen oder Personen nicht adressierte Briefumschläge mit dem zu versendenden Material an diejenigen Stellen, welche die Adressen der Befragungsempfänger kennen und die Briefe dann versenden.

6 Soziales und Gesundheit

6.1 Uneingeschränktes Widerspruchsrecht im Bayerischen Krebsregister

Patientinnen und Patienten, die einen Widerspruch gegen ihre Registrierung im Bayerischen Krebsregister eingelegt haben, konnten lange Zeit nur eine Löschung ihrer Identitätsdaten erreichen. Die Daten zur Krankheitsgeschichte blieben im Krebsregister gespeichert. Die einschlägigen Regelungen habe ich stets als unzureichend kritisiert (vgl. etwa meinen 32. Tätigkeitsbericht 2022 unter Nr. 7.3).

Der Gesetzgeber hat meine Kritik nun aufgegriffen und zum 1. August 2023 für das Bayerische Krebsregister ein **uneingeschränktes Widerspruchsrecht** eingeführt. Art. 5 Abs. 1 Bayerisches Krebsregistergesetz (BayKRegG) lautet nun wie folgt:

„[1]Jeder kann der dauerhaften Speicherung der Identitätsdaten sowie der nach Art. 4 meldepflichtigen Daten im Bayerischen Krebsregister widersprechen, soweit sie ihn selbst oder eine seiner Personensorge oder Betreuung unterstehende Person betreffen. [2]Diese Daten sind unverzüglich aus dem Bayerischen Krebsregister zu löschen, sobald ihre Kenntnis nicht mehr für gesetzliche Abrechnungszwecke erforderlich ist. [3]Der Widerspruch ist schriftlich bei der Vertrauensstelle einzulegen. [4]Er kann auch über Personen, die gemäß Art. 4 Abs. 2 Satz 3 über das Widerspruchsrecht belehrt haben, bei der Vertrauensstelle eingelegt werden. [5]Der Widerspruch betrifft bereits erfasste Daten nach Satz 1 sowie künftig eingehende Meldungen. [6]Unbeschadet der Löschung gemäß Satz 2 ist die Vertrauensstelle im Falle eines Widerspruchs befugt, die jeweiligen Identitätsdaten in einer gesondert zu führenden, vertraulichen Liste zu speichern und ausschließlich zu Zwecken eines Datenabgleichs mit zukünftigen Meldungen zu verwenden. [7]Wurden Daten zu dieser Person von oder an ein anderes Landeskrebsregister gemeldet, ist dieses Landeskrebsregister über die Erhebung des Widerspruchs zu informieren.“

Art. 5 Abs. 1 Satz 1 BayKRegG stellt ausdrücklich klar, dass vom Widerspruchsrecht neben den Identitätsdaten auch sämtliche nach Art. 4 BayKRegG meldepflichtigen Daten umfasst sind, also die erstmalige gesicherte Diagnose einer Krebserkrankung, der zu einer Krebserkrankung vorliegende histologische, labortechnische oder zytologische Befund, die Art sowie die Zeitpunkte des Beginns und des Abschlusses einer therapeutischen Maßnahme, die Diagnose von Rezidiven, Metastasen, Zweittumoren und anderen Änderungen im Krankheitsverlauf sowie der Tod einer Person, die eine Krebserkrankung hatte. Nähere Informationen zu den Voraussetzungen zur Einlegung und zu den Folgen eines Widerspruchs habe ich im Rahmen einer Aktuellen Kurz-Information im August 2023 bereitgestellt.[110]

Dass der Gesetzgeber nun eine grundrechtlich ausgewogene Regelung gefunden hat, hat mich sehr gefreut. So steht der Patientenwille endlich im Mittelpunkt. Das

[110] Bayerischer Landesbeauftragter für den Datenschutz, Bayerisches Krebsregistergesetz jetzt mit uneingeschränktem Widerspruchsrecht, Aktuelle Kurz-Information 52, Stand 8/2023, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018“.

stärkt nicht nur das Vertrauen in das Krebsregister, sondern auch in die mit seinen Daten arbeitende Forschung. Es ist zu hoffen, dass das Krebsregister zukünftig beides bietet: eine hochwertige Datenqualität für die medizinische Krebsforschung und zugleich einen hochwertigen Datenschutz für die betroffenen Patientinnen und Patienten.

6.2 Vorangekreuzte Datenschutzformulare in einem Krankenhaus

Eine Beschwerde betraf den Einsatz **vorangekreuzter datenschutzrechtlicher Einwilligungsformulare** durch ein bayerisches Universitätsklinikum. Der Beschwerdeführer hatte frühmorgens das Universitätsklinikum aufgesucht. In der Patientenaufnahme fügte die diensthabende Pflegekraft dem Behandlungsvertrag ein ausgedrucktes Datenschutzformular bei, in dem zu allen aufgeführten Fragen das jeweilige Antwortfeld mit „Ja“ **vorbelegt** war. Auf Nachfrage erklärte sie dem Patienten, das System ermögliche nur einen Ausdruck mit „Ja“. Er könne entsprechende Antworten manuell streichen.

In der Folge wandte sich der Beschwerdeführer an mich. Ich ersuchte das Klinikum um Stellungnahme; dabei wollte ich insbesondere in Erfahrung bringen, ob das eingesetzte IT-System nur dann einen Ausdruck des Formulars ermöglichte, wenn bei allen datenschutzrechtlich relevanten Einwilligungsfeldern die voreingestellte Antwort „Ja“ lautete.

Das Klinikum führte aus, es treffe zwar zu, dass die Auswahlfelder systemseitig mit „Ja“ vorbelegt gewesen seien, da dies den „in der überwiegenden Zahl der Rückmeldungen erwarteten Antworten“ entsprochen habe. Allerdings sei das Personal gehalten, diese Vorbelegung der Auswahlfelder auf Wunsch der betroffenen Person komplett zu entfernen. Dass ein Ausdruck des Formulars nur bei Vorbelegung aller Felder mit „Ja“ möglich gewesen wäre, bestätigte das Klinikum jedoch nicht. Im Fall des Beschwerdeführers sei es trotz entsprechender Schulungen zu einem Fehler gekommen. Ursächlich sei möglicherweise, dass die Pflegekräfte in der Nacht neben den pflegerischen Tätigkeiten auch die administrative Aufnahme der Patienten abwickeln müssten.

Das Verwenden vorangekreuzter Einwilligungsformulare im Rahmen der Patientenaufnahme im Krankenhaus verstößt gegen den **Grundsatz der Verarbeitung auf rechtmäßige Weise und nach Treu und Glauben** gemäß Art. 5 Abs. 1 Buchst. a DSGVO.

In der Vorbelegung mit „Ja“ kommt die Erwartung zum Ausdruck, dass die betroffene Person der Verarbeitung zu verschiedenen, im Formular beschriebenen Zwecken zustimmt; sie wirkt somit suggestiv und hemmt letztlich die freie Willensausübung der betroffenen Person. In Anbetracht des Kräfteungleichgewichts zwischen einem Klinikum einerseits und den auf Hilfe angewiesenen Patientinnen und Patienten andererseits ist ein solches Prozedere im Ergebnis als unfair und treuwidrig zu bewerten. Zudem erscheint die Freiwilligkeit einer unter solchen Umständen erteilten Einwilligung als sehr zweifelhaft.

Offenbar war auch dem Normgeber das Problem der vorbelegten Auswahlfelder in Einwilligungsformularen bereits bekannt, wie **EG 32 Satz 3 DSGVO** zeigt:

„Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen.“

Das Klinikum korrigierte aus Anlass der Beschwerde seine datenschutzwidrige Praxis und versicherte mir, in seinem Verantwortungsbereich systemseitig keine Einwilligungsmuster mit vorbelegten Feldern mehr zuzulassen.

Auch unter Berücksichtigung der weiteren Einlassungen des Universitätsklinikums war aus meiner Sicht nicht mit weiteren Vorfällen dieser Art zu rechnen. Wenngleich ich daher von einer förmlichen Beanstandung absah, war der festgestellte Verstoß doch als gravierend zu bewerten. Aus diesem Grund setzte ich das Bayerische Staatsministerium für Wissenschaft und Kunst als zuständige Rechtsaufsichtsbehörde über die datenschutzrechtliche Problematik in Kenntnis. Ich bat darum, auch den anderen bayerischen Universitätskliniken gegenüber auf die Vermeidung vergleichbarer Defizite hinzuwirken.

Das Wissenschaftsministerium hat daraufhin zeitnah alle bayerischen Universitätskliniken mit ministeriellem Schreiben über die Problematik informiert, auf Maßnahmen im Falle weiterer Verstöße hingewiesen und so einen wesentlichen Beitrag zur Sensibilisierung der Universitätskliniken geleistet.

6.3 Anforderung von Wundverlaufsprotokollen durch Krankenkassen

Die Frage, inwieweit Krankenkassen Gesundheitsdaten verarbeiten dürfen, ist ein wiederkehrendes Prüfungs- und Beratungsthema (siehe etwa im 26. Tätigkeitsbericht 2013/2014 unter Nr. 8.1.2 bis 8.1.6, im 27. Tätigkeitsbericht 2015/2016 unter Nr. 8.1.1 bis 8.1.3 sowie im 28. Tätigkeitsbericht 2017/2018 unter Nr. 9.2.2). Eine mehrfach an mich herangetragene Fragestellung war nun die Anforderung sog. Wundverlaufsprotokolle durch eine bayerische Krankenkasse.

Den krankenversicherungsrechtlichen Hintergrund bildet § 37 Fünftes Buch Sozialgesetzbuch (SGB V). Die Vorschrift regelt den Anspruch der gesetzlich Versicherten auf häusliche Krankenpflege. Zu den Leistungen der häuslichen Krankenpflege gehört unter anderem auch die Versorgung von chronischen und schwer heilenden Wunden, die – aufgrund ärztlicher Verordnung und nach Genehmigung durch die Krankenkasse – von Pflegedienstleistern erbracht und gegenüber der Krankenkasse abgerechnet wird. Die Wundversorgung wird von den Pflegefachkräften durch Wundverlaufsprotokolle dokumentiert, die auch Gesundheitsdaten der Versicherten enthalten.

Die betroffene Krankenkasse hatte bei Pflegediensten die Vorlage von Wundverlaufsprotokollen angefordert, um damit ihre Leistungspflicht für die abgerechneten Pflegeleistungen zu prüfen. Hiergegen erhoben Pflegedienste und Pflegeverbände datenschutzrechtliche Bedenken. Sie waren der Auffassung, die Krankenkasse dürfe die Wundverlaufsprotokolle nichts selbst einsehen, sondern könne aufgrund der Regelung des § 276 Abs. 2 Satz 2 SGB V nur eine unmittelbare Übermittlung an den Medizinischen Dienst zur Einholung einer gutachterlichen Stellungnahme verlangen.

Im Ausgangspunkt konnte ich diese Bedenken nachvollziehen. Innerhalb des Anwendungsbereichs von § 276 Abs. 2 Satz 2 SGB V sind die Leistungserbringer verpflichtet, die für eine Begutachtung erforderlichen Daten unmittelbar an den Medizinischen Dienst, und nicht etwa an die Krankenkasse, zu übermitteln.

Allerdings setzt die Vorschrift tatbestandlich einen Sachverhalt voraus, der die Krankenkasse bei der Erbringung von Leistungen verpflichtet (oder berechtigt),

eine gutachtliche Stellungnahme des Medizinischen Dienstes einzuholen. Wann ein solcher Sachverhalt vorliegt, lässt sich § 276 Abs. 2 Satz 2 SGB V nicht entnehmen. Dies ist vielmehr nach § 275 SGB V zu bestimmen. Im Übrigen gilt der Grundsatz, wonach Krankenkassen Sozialdaten für Zwecke der Krankenversicherung erheben und speichern dürfen, soweit diese zur Prüfung der Leistungspflicht und der Erbringung von Leistungen an Versicherte – hier häusliche Krankenpflege – erforderlich sind (§ 284 Abs. 1 Satz 1 Nr. 4 SGB V).

Eine ausdrückliche Pflicht zur Beauftragung des Medizinischen Dienstes besteht bei häuslicher Krankenpflege nur für die Frage, ob und für welchen Zeitraum diese länger als vier Wochen erforderlich ist (vgl. § 275 Abs. 2 Satz 1 Nr. 3 SGB V). Für die Erbringung sonstiger Leistungen der häuslichen Krankenpflege – wie der Wundversorgung – kommt es darauf an, ob es nach Art, Schwere, Dauer oder Häufigkeit der Erkrankung oder nach dem Krankheitsverlauf erforderlich ist, eine gutachtliche Stellungnahme des Medizinischen Dienstes einzuholen (§ 275 Abs. 1 Satz 1 Nr. 1 SGB V). Ob die Beauftragung des Medizinischen Dienstes erforderlich ist, hat die Krankenkasse jeweils anhand der Umstände des Einzelfalles zu beurteilen. An der Erforderlichkeit einer gutachtlichen Stellungnahme durch den Medizinischen Dienst kann es insbesondere dann fehlen, wenn die Krankenkasse selbst über zur Prüfung der abgerechneten Leistungen medizinisch qualifiziertes Personal verfügt.

So lag der Fall bei der betroffenen Krankenkasse. Aufgrund einer ähnlich gelagerten Kontrollanregung befand ich mich bereits in der Vergangenheit mit dieser Krankenkasse in Bezug auf die Verarbeitung von Wundprotokollen im Austausch. Seinerzeit hatte die Krankenkasse mitgeteilt, sie verfüge über ein besonders qualifiziertes Team an examinierten Pflegefachkräften. Diese Beschäftigten besäßen – wohl im Gegensatz zu anderen Krankenkassen – eine medizinisch-pflegerische Qualifikation, die auch die Ausbildung zur Wundmanagerin oder zum Wundmanager beziehungsweise als Wundtherapeutin oder als Wundtherapeut umfasse.

Vor diesem besonderen Hintergrund konnte ich anhand der mir geschilderten Sachverhalte keinen datenschutzrechtlichen Verstoß der betroffenen Krankenkasse feststellen.

6.4 Datenübermittlung des Jugendamtes im Rahmen der Mitwirkung im Verfahren vor dem Familiengericht

Zu den gesetzlichen Aufgaben der Jugendämter zählt die Mitwirkung in Verfahren vor den Familiengerichten. Insbesondere unterstützt das Jugendamt das Familiengericht bei allen Maßnahmen, welche die Sorge für die Person von Kindern und Jugendlichen betreffen (§ 50 Abs. 1 Satz 1 Achtes Buch Sozialgesetzbuch – SGB VIII). Regelmäßig wirkt das Jugendamt im Wege von schriftlichen Stellungnahmen an das Gericht mit. Eine im Berichtszeitraum eingegangene Beschwerde verdeutlicht exemplarisch, wie leicht mangelnde Sorgfalt bei der Verarbeitung sensibler Sozialdaten auch in vermeintlich unkritischen Verarbeitungskonstellationen erhebliche Risiken für betroffene Personen bewirken kann.

Die Beschwerdeführer, ein Ehepaar, hatten auf Vermittlung des Jugendamtes ein Pflegekind aufgenommen. Mit dem Jugendamt bestand die Absprache, dass die persönliche Wohnanschrift der Pflegeltern den leiblichen Eltern des Kindes, welche sich zur gleichen Zeit in einem laufenden Familiengerichtsverfahren um das

Sorgerecht bemühten, nicht mitgeteilt wird. Umso erstaunter waren die Eingabeführer, als ihnen die leiblichen Eltern anlässlich eines Umgangstermins eröffneten, ihre Wohnanschrift aus einem Schreiben des Jugendamtes erfahren zu haben.

Im Zuge des daraufhin eingeleiteten Beschwerdeverfahrens teilte mir das Jugendamt mit, dass es gemäß § 50 SGB VIII an dem familiengerichtlichen Verfahren über die elterliche Sorge mitwirke. Eine in diesem Zusammenhang an das Familiengericht übermittelte Stellungnahme des Jugendamtes habe auch die Adressdaten der Pflegeltern enthalten. Auf die Vertraulichkeit dieser Daten sei das Gericht nicht hingewiesen worden. Durch das Familiengericht sei die Stellungnahme des Jugendamtes dann ungeschwärzt den leiblichen Eltern zugeleitet worden.

Datenschutzrechtlich war die Übermittlung der Adressdaten durch das Jugendamt an das Familiengericht als Verletzung des Sozialgeheimnisses nach § 35 Abs. 1 Satz 1 Erstes Buch Sozialgesetzbuch (SGB I) zu bewerten. Nach der Vorschrift hat jeder Anspruch darauf, dass die ihn betreffenden Sozialdaten von den Leistungsträgern nicht unbefugt verarbeitet werden. Die Übermittlung der Adressdaten an das Familiengericht war unbefugt, weil sie nicht auf eine Rechtsgrundlage gestützt werden konnte.

Zwar kommt im Rahmen der Mitwirkung in Verfahren vor den Familiengerichten zur Rechtfertigung der Übermittlung von Adressdaten einer Pflegefamilie grundsätzlich § 69 Abs. 1 Nr. 1 Var. 2 Zehntes Buch Sozialgesetzbuch (SGB X) in Betracht. Hiernach ist die Übermittlung von Sozialdaten erlaubt, sofern sie für die Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle erforderlich ist. Sie kann erforderlich sein, wenn zu erwarten ist, dass das Familiengericht – welches den Sachverhalt regelmäßig von Amts wegen zu ermitteln hat (vgl. § 26 FamFG) – für seine Entscheidung eine Stellungnahme der Pflegeltern benötigen oder die Pflegekinder selbst anhören wird. Hierzu benötigt das Familiengericht Kenntnis der Adressdaten, welche es nur vom Jugendamt erhalten kann.

Aufgrund der Sachverhaltsschilderung konnte ich aber nicht feststellen, dass das Familiengericht im Beschwerdefall zu diesen Zwecken der Adressdaten der Eingabeführer bedurft hätte. Vielmehr hat das Jugendamt selbst eingeräumt, dass die Übermittlung der Adressdaten der Eingabeführer an das Familiengericht für das betreffende Verfahren, welches die Erziehungsfähigkeit der leiblichen Eltern zum Gegenstand hatte, nicht zwingend erforderlich war.

Zwar hat das Jugendamt durch die Übermittlung der Adressdaten die Ursache für die spätere Weitergabe der Daten an die leiblichen Eltern gesetzt. Die eigentlich kritische Weitergabe der Adressdaten erfolgte aber erst durch das Familiengericht.

Zudem hat sich das Jugendamt im Nachgang zu dem Vorfall um Aufklärung bemüht und – insbesondere durch Ansprache der leiblichen Eltern – Maßnahmen ergriffen, um das Gefährdungsrisiko einzuschätzen und möglichst zu minimieren. Demnach waren wohl bislang auch keine konkreten Anhaltspunkte dafür ersichtlich, dass von den leiblichen Eltern eine Gefährdung ausgehen könnte.

Das Jugendamt hat die Datenschutzverletzung zudem unmittelbar eingeräumt und angekündigt, künftig sorgsamer zu prüfen, dass nur zwingend notwendige personenbezogene Angaben Dritter in Stellungnahmen an das Familiengericht genannt werden. Vor diesem Hintergrund war anzunehmen, dass vergleichbare

Datenschutzverstöße künftig nicht mehr zu erwarten sind. Von einer förmlichen Beanstandung habe ich daher abgesehen.

6.5 Weitere Entwicklungen zum Masernschutzgesetz

Das zum 1. März 2020 in Kraft getretene **Masernschutzgesetz** beschäftigte nicht nur die Bürgerinnen und Bürger, sondern auch mich als Datenschutz-Aufsichtsbehörde weiterhin (vgl. bereits den 30. Tätigkeitsbericht 2020 unter Nr. 10.2.1 und den 31. Tätigkeitsbericht 2021 unter Nr. 7.1).

6.5.1 Inhalt eines Kontraindikationsattests

Besonders umstritten war insbesondere die Frage, welche Angaben ein **sog. Kontraindikationsattest** beinhalten muss (§ 20 Abs. 9 Satz 1 Nr. 2 Halbsatz 2 Infektionsschutzgesetz – IfSG). Ein Kontraindikationsattest ist ein ärztliches Zeugnis darüber, dass eine Person aufgrund einer dauerhaften medizinischen Kontraindikation/Gegenanzeige nicht gegen Masern geimpft werden kann oder sollte.

Welche medizinischen Angaben bei einem solchen ärztlichen Attest über die Impfunfähigkeit gegenüber dem Gesundheitsamt erforderlich sind, ist zunächst eine fachliche Frage, die aus (amts-) ärztlicher Sicht zu beantworten ist.

Aus diesem Grund hatte ich im 31. Tätigkeitsbericht 2021 unter Nr. 7.1.1 darauf Bezug genommen, wie sich das Bayerische Staatsministerium für Gesundheit und Pflege mir gegenüber positioniert hatte. Zum damaligen Zeitpunkt war das **Gesundheitsministerium** zu dem Schluss gekommen, dass im Kontraindikationsattest keine Angaben zum medizinischen Grund der Kontraindikation gemacht werden müssten. Mittlerweile liegt zu dieser Frage auch obergerichtliche Rechtsprechung vor. Der Bayerische Verwaltungsgerichtshof hat in diesem Zusammenhang ausgeführt:[111]

„Das ärztliche Zeugnis im Sinne von § 20 Abs. 9 Satz 1 Nr. 2 Alt. 2 IfSG darf sich nicht damit begnügen, den Gesetzeswortlaut zum Bestehen einer medizinischen Kontraindikation zu wiederholen. Es muss vielmehr wenigstens solche Angaben zur Art der medizinischen Kontraindikation enthalten, die das Gesundheitsamt in die Lage versetzen, das ärztliche Zeugnis auf Plausibilität hin zu überprüfen […]. Hierfür sprechen neben dem Zweck der Regelung, eine ausreichend hohe Impfquote zu erreichen und hierfür u.a. dem Gesundheitsamt eine Grundlage für das weitere Vorgehen (z. B. in einem Beratungsgespräch nach § 20 Abs. 12 Satz 2 IfSG) zu geben, auch systematische Erwägungen, denn das IfSG unterscheidet auch an anderer Stelle die schlichte Bescheinigung vom Nachweis durch ein ärztliches Zeugnis (vgl. etwa § 43 Abs. 1 Satz 2 IfSG). Die Entstehungsgeschichte der Norm bestätigt diese Annahme.“

Bei der Beurteilung des Vorgehens von Gesundheitsämtern, die Nachfragen zum Kontraindikationsattest bei betroffenen Personen stellen und weitere Nachweise verlangen, ist diese Rechtsprechung zu berücksichtigen. Daher habe ich das Vor-

[111] Bayerischer Verwaltungsgerichtshof, Beschluss vom 7. Juli 2021, 25 CS 21.1651, BeckRS 2021, 18528, Rn. 14.

gehen von Gesundheitsämtern, sich Angaben zur Art der medizinischen Kontraindikation vorlegen zu lassen, in den mir vorgetragenen Einzelfällen nicht als Datenschutzverstoß bewertet.

6.5.2 Zweifel des Gesundheitsamtes im Zusammenhang mit dem Kontraindikationsattest

Beschäftigt habe ich mich zudem mit dem Sachverhalt, dass das Gesundheitsamt Kontraindikationsatteste auch mit Angaben zur Art der medizinischen Kontraindikation nicht akzeptiert und **weitere Nachweise** anfordert.

Aufgabe des Gesundheitsamtes ist nach § 20 Abs. 12 IfSG die Prüfung des Nachweises gemäß Masernschutzgesetz. Dies umfasst nach § 20 Abs. 9 Satz 1 Nr. 2 IfSG auch die Prüfung des ärztlichen Zeugnisses darüber, dass die zum Nachweis verpflichteten Personen aufgrund einer medizinischen Kontraindikation nicht geimpft werden können.

Im Rahmen dieser Regelung wurde dem Gesundheitsamt in **§ 20 Abs. 12 Satz 2 IfSG** (zuletzt geändert mit Wirkung zum 17. September 2022) folgende Befugnis übertragen:

„Bestehen Zweifel an der Echtheit oder inhaltlichen Richtigkeit des vorgelegten Nachweises, so kann das Gesundheitsamt eine ärztliche Untersuchung dazu anordnen, ob die betroffene Person auf Grund einer medizinischen Kontraindikation nicht gegen Masern geimpft werden kann; Personen, die über die Echtheit oder inhaltliche Richtigkeit des vorgelegten Nachweises Auskunft geben können, sind verpflichtet, auf Verlangen des Gesundheitsamtes die erforderlichen Auskünfte insbesondere über die dem Nachweis zugrundeliegenden Tatsachen zu erteilen, Unterlagen vorzulegen und Einsicht zu gewähren; § 15a Absatz 2 Satz 2 gilt entsprechend.“

Soweit das Gesundheitsamt plausibel darlegt, dass Zweifel an der inhaltlichen Richtigkeit der vorgelegten Nachweise für eine medizinische Kontraindikation einer Masernimpfung bestehen, darf es daher insbesondere weitere aus Sicht des Gesundheitsamtes erforderliche Auskünfte über die dem Nachweis zugrundeliegenden Tatsachen **verlangen**.

7 Personalverwaltung

7.1 Bayerisches Personalaktenrecht und unionales Datenschutzrecht

Im März 2023 hat der Europäische Gerichtshof eine vielbeachtete[112] Entscheidung zum Beschäftigtendatenschutz getroffen.[113] Gegenstand des Verfahrens waren Vorschriften des hessischen Landesrechts zur Verarbeitung von Beschäftigtendaten. Im Kern ging es dabei zunächst um die Frage, welche Anforderungen nationale Rechtsvorschriften erfüllen müssen, die auf Grundlage von Art. 88 DSGVO erlassen worden sind. Ferner hat der Gerichtshof dazu Stellung genommen, ob mitgliedstaatliche Regelungen, die hinter den Anforderungen dieser Vorschrift zurückbleiben, weiter angewendet werden können.

Der vorliegende Beitrag stellt zunächst Hintergrund und wesentliche Aussagen des Urteils dar. Anschließend widmet er sich der Frage, ob die Entscheidung des Europäischen Gerichtshofs auch Auswirkungen für das bayerische Personalaktenrecht hat.

7.1.1 Zum Hintergrund

Die Datenschutz-Grundverordnung gilt grundsätzlich unmittelbar in jedem Mitgliedstaat – und zwar auch im Bereich des Beschäftigtendatenschutzes. Allerdings räumt sie den nationalen Gesetzgebern verschiedene Regelungs- und Gestaltungsspielräume ein. Solche bestehen etwa bei der Verarbeitung personenbezogener Daten zur Wahrnehmung von Aufgaben, die im öffentlichen Interesse liegen (vgl. Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2 und 3 DSGVO), aber auch, wenn es um die Verarbeitung von Beschäftigtendaten geht (Art. 88 DSGVO). Da der europäische Gesetzgeber mit der Datenschutz-Grundverordnung eigentlich eine Vollharmonisierung des Datenschutzrechts in Europa erreichen wollte, bestehen solche nationalen Gestaltungsspielräume nicht voraussetzungslos: Die in der Datenschutz-Grundverordnung enthaltenen „Öffnungsklauseln" formulieren vielmehr unterschiedliche Anforderungen an das auf ihrer Grundlage erlassene nationale Recht. So erlaubt Art. 88 Abs. 1 DSGVO als mitgliedstaatliches Recht (lediglich) „spezifischere Vorschriften", die den Schutz der Rechte und Freiheiten betroffener Personen bei der Verarbeitung von Beschäftigtendaten gewährleisten sollen. Art. 88 Abs. 2 DSGVO fordert in diesem Zusammenhang, dass solche Vorschriften „geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person" umfassen.

Im Bundesrecht ist § 26 Bundesdatenschutzgesetz (BDSG) die zentrale Norm für die Verarbeitung personenbezogener Daten im Beschäftigungskontext. Diese

[112] Vgl. insbesondere die Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 11. Mai 2023 „Notwendigkeit spezifischer Regelungen zum Beschäftigtendatenschutz! – Rechtsprechung des Europäischen Gerichtshofs hat Auswirkungen auf zahlreiche deutsche Vorschriften im Beschäftigungskontext", abrufbar unter https://datenschutzkonferenz-online.de/entschliessungen.html.

[113] Europäischer Gerichtshof, Urteil vom 30. März 2023, C-34/21, BeckRS 2023, 5635.

vom Bundesgesetzgeber auf Art. 88 DSGVO gestützte[114] Vorschrift ist vor allem für Arbeitgeber und Beschäftigte in der Privatwirtschaft von Bedeutung. Für bayerische Dienstherren und öffentliche Arbeitgeber bestimmt sich die Zulässigkeit von Datenverarbeitungen im Beschäftigungskontext hingegen insbesondere nach Art. 103 ff. Bayerisches Beamtengesetz (BayBG) und § 50 Beamtenstatusgesetz. Für vertraglich im bayerischen öffentlichen Dienst Beschäftigte gelten diese Vorschriften grundsätzlich entsprechend (Art. 145 Abs. 2 BayBG).

7.1.2 Worum ging es in dem Verfahren?

Die Corona-Pandemie hat – wie viele öffentliche Stellen – auch die Schulen vor besondere Herausforderungen gestellt. Insbesondere war Präsenzunterricht nicht oder nur eingeschränkt möglich. Als Alternative wurde daher vielfach auf Distanzunterricht per Videokonferenz zurückgegriffen. Die damit zusammenhängende Verarbeitung personenbezogener Daten sowohl von Schülerinnen und Schülern als auch von Lehrkräften bedurfte freilich einer hinreichenden Rechtsgrundlage.

Mit zwei Erlassen im Jahr 2020 legte das Hessische Kultusministerium Rahmenbedingungen zum Schulunterricht während der Corona-Pandemie fest. Vorgesehen war dabei insbesondere, dass eine Zuschaltung von Schülerinnen und Schülern zum Unterricht per Videokonferenzdienst deren vorherige Einwilligung oder – bei Minderjährigen – die Einwilligung der Eltern voraussetzte. Für die Teilnahme der Lehrkräfte war ein solches Verfahren hingegen nicht vorgesehen; hier sollte nach Auffassung des Hessischen Kultusministeriums bereits § 23 Abs. 1 Satz 1 Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG) eine hinreichende Verarbeitungsbefugnis liefern. Nach dieser Vorschrift – die insoweit im Wesentlichen § 26 Abs. 1 Satz 1 BDSG entspricht – dürfen personenbezogene Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses unter anderem dann verarbeitet werden, wenn dies für die Durchführung des Beschäftigungsverhältnisses sowie zur Durchführung innerdienstlicher planerischer, organisatorischer, sozialer und personeller Maßnahmen erforderlich ist.

Der Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium erhob hiergegen Klage beim Verwaltungsgericht Wiesbaden. Dem Gericht kamen dabei Zweifel, ob § 23 Abs. 1 Satz 1 HDSIG sowie der alternativ als Rechtsgrundlage in Betracht gezogene – und in Teilen Art. 103 Abs. 1 Satz 1 Nr. 1 BayBG entsprechende – § 86 Abs. 4 Hessisches Beamtengesetz (HBG) mit den Anforderungen von Art. 88 Abs. 2 DSGVO vereinbar seien. Nach § 86 Abs. 4 Satz 1 HBG darf der Dienstherr unter anderem personenbezogene Daten über Beamtinnen und Beamte nur erheben, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift oder eine Dienstvereinbarung dies erlaubt.

Das Gericht beschloss daher, das Verfahren auszusetzen und dem Europäischen Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

— Ist Art. 88 Abs. 1 DSGVO dahin auszulegen, dass eine Rechtsvorschrift, um eine spezifischere Vorschrift zur Gewährleistung des Schutzes der Rechte

[114] Vgl. Bundestags-Drucksache 18/11325, S. 96.

und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext im Sinne des Art. 88 Abs. 1 DSGVO zu sein, die an solche Vorschriften nach Art. 88 Abs. 2 DSGVO gestellten Anforderungen erfüllen muss?

— Kann eine nationale Norm, wenn diese die Anforderungen nach Art. 88 Abs. 2 DSGVO offensichtlich nicht erfüllt, trotzdem noch anwendbar bleiben?[115]

7.1.3 Was hat der Europäische Gerichtshof konkret entschieden?

Als „Vorfragen" prüft der Europäische Gerichtshof zunächst, ob die betreffenden Verarbeitungen personenbezogener Daten der Lehrkräfte überhaupt in den Anwendungsbereich der Datenschutz-Grundverordnung im Allgemeinen und des Art. 88 DSGVO im Speziellen fallen. Bei der letztgenannten Frage spielt insbesondere eine Rolle, ob die betroffenen Lehrkräfte als Angestellte oder Beamtinnen und Beamte im öffentlichen Dienst des Landes Hessen vom Beschäftigtenbegriff und dem Begriff des Beschäftigtenkontexts im Sinne von Art. 88 DSGVO erfasst sind. Diese „Vorfragen" bejaht der Gerichtshof jeweils.[116]

Hinsichtlich der **ersten Vorlagefrage** kommt der Europäische Gerichtshof zu dem Ergebnis, dass „spezifischere Vorschriften" im Sinne von Art. 88 Abs. 1 DSGVO die Vorgaben von Art. 88 Abs. 2 DSGVO erfüllen müssen.[117] Art. 88 DSGVO verlangt nach Auffassung des Gerichts demnach zweierlei:

— Zum einen müssen „spezifischere Vorschriften" im Sinne von Art. 88 Abs. 1 DSGVO einen Regelungsgehalt aufweisen, der sich von den allgemeinen Vorgaben der Datenschutz-Grundverordnung unterscheidet. Nicht ausreichend ist es demnach insbesondere, wenn nationale Vorschriften, die auf Grundlage von Art. 88 DSGVO erlassen werden, lediglich die Rechtmäßigkeitsbedingungen nach Art. 6 DSGVO oder die Datenschutz-Grundsätze nach Art. 5 DSGVO wiederholen oder auf diese verweisen.[118]

— „Spezifischere Vorschriften" im Sinne von Art. 88 Abs. 1 DSGVO müssen ferner nach Art. 88 Abs. 2 DSGVO „auf den Schutz der Rechte und Freiheiten der Beschäftigten hinsichtlich der Verarbeitung ihrer personenbezogenen Daten im Beschäftigungskontext abzielen und geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person umfassen."[119]

Vereinfacht ausgedrückt könnte man sagen: Nationale Regelungen zum Beschäftigtendatenschutz sind nur dann „spezifischere Vorschriften" im Sinne von Art. 88

[115] Ausführlich zu Sachverhalt und Vorlagefragen Europäischer Gerichtshof, Urteil vom 30. März 2023, C-34/21, BeckRS 2023, 5635, Rn. 14 ff.

[116] Europäischer Gerichtshof, Urteil vom 30. März 2023, C-34/21, BeckRS 2023, 5635, Rn. 31 ff., 37 sowie Rn. 38 ff., 56.

[117] Europäischer Gerichtshof, Urteil vom 30. März 2023, C-34/21, BeckRS 2023, 5635, Rn. 75.

[118] Europäischer Gerichtshof, Urteil vom 30. März 2023, C-34/21, BeckRS 2023, 5635, Rn. 61 und 71.

[119] Europäischer Gerichtshof, Urteil vom 30. März 2023, C-34/21, BeckRS 2023, 5635, Rn. 74.

Abs. 1 DSGVO, wenn sie sowohl hinsichtlich ihres Regelungsgehalts als auch hinsichtlich des Schutzes der (Grund-)Rechte und Freiheiten der betroffenen Beschäftigten einen „echten Mehrwert“ mit sich bringen.

Was die **zweite Vorlagefrage** – und damit die Anwendbarkeit von nationalen Normen, welche die Anforderungen nach Art. 88 Abs. 2 DSGVO nicht erfüllen – betrifft, stellt der Gerichtshof im Ausgangspunkt zunächst fest, dass auf Grundlage von Öffnungsklauseln erlassene mitgliedstaatliche Rechtsvorschriften „nicht gegen den Inhalt und die Ziele der DSGVO verstoßen“ dürfen.[120] Ob § 23 Abs. 1 Satz 1 HDSIG und § 86 Abs. 4 HBG die Voraussetzungen und Grenzen des Art. 88 DSGVO tatsächlich beachten, entscheidet der Europäische Gerichtshof selbst jedoch nicht – dies sei, wie er betont, „Sache des für die Auslegung des nationalen Rechts allein zuständigen vorlegenden Gerichts“.[121] Gleichwohl bezweifelt der Gerichtshof im Folgenden recht deutlich, dass die genannten Vorschriften des hessischen Landesrechts zum Beschäftigtendatenschutz gegenüber den allgemeinen Regeln der Datenschutz-Grundverordnung den zuvor geforderten inhaltlichen Mehrwert aufweisen.[122]

Aufgrund des Anwendungsvorrangs der Datenschutz-Grundverordnung müsste das vorlegende Gericht nationale Bestimmungen, welche seiner Ansicht nach gegen Voraussetzungen und Grenzen des Art. 88 DSGVO verstoßen, eigentlich unangewendet lassen.[123] Da die gegenständliche Datenverarbeitung im Rahmen des öffentlichen Schulunterrichts und damit zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erfolgt, bringt der Europäische Gerichtshof an dieser Stelle jedoch Art. 6 Abs. 1 UAbs. 1 Buchst. c und e, Abs. 3 DSGVO ins Spiel: Das vorlegende Gericht muss demnach gegebenenfalls auch prüfen, ob Vorschriften, welche die Anforderungen von Art. 88 DSGVO nicht erfüllen, als „Rechtsgrundlagen“ im Sinne von Art. 6 Abs. 3 DSGVO gleichwohl weiter angewandt werden müssen.[124] Dies kommt vorliegend insbesondere aus dem Grunde in Betracht, dass Art. 6 Abs. 3 Satz 3 DSGVO als „Kann“-Vorschrift formuliert ist. Im Unterschied zu Art. 88 Abs. 2 DSGVO führt die Norm keine obligatorischen, sondern fakultative Regelungsinhalte auf.[125]

7.1.4 Welche Folgen ergeben sich aus dieser Entscheidung für das bayerische Personalaktenrecht?

Für das bayerische Personalaktenrecht ergeben sich aus dem Urteil zunächst einmal keine unmittelbaren Folgen: Eine dem § 23 Abs. 1 Satz 1 HDSIG vergleichbare Regelung enthält das bayerische Landesrecht – anders als das Bundesrecht mit § 26 BDSG –[126] nicht. Art. 103 Abs. 1 Satz 1 Nr. 1 BayBG ähnelt zwar § 86 Abs. 4 Satz 1 HBG (zu dessen Regelungsinhalt vgl. bereits Nr. 7.1.2), sodass für

120 Europäischer Gerichtshof, Urteil vom 30. März 2023, C-34/21, BeckRS 2023, 5635, Rn. 79.
121 Europäischer Gerichtshof, Urteil vom 30. März 2023, C-34/21, BeckRS 2023, 5635, Rn. 80.
122 Europäischer Gerichtshof, Urteil vom 30. März 2023, C-34/21, BeckRS 2023, 5635, Rn. 81.
123 Europäischer Gerichtshof, Urteil vom 30. März 2023, C-34/21, BeckRS 2023, 5635, Rn. 82 f.
124 Europäischer Gerichtshof, Urteil vom 30. März 2023, C-34/21, BeckRS 2023, 5635, Rn. 85 ff.
125 Hinsichtlich der Verarbeitung von Beschäftigtendaten im öffentlichen Bereich in diese Richtung auch Hessischer Beauftragter für Datenschutz und Informationsfreiheit, Handreichung zur Verarbeitung personenbezogener Daten von Beschäftigten im Lichte des EuGH-Urteils vom 30. März 2023 Rs. C-34/21, S. 5 f., abrufbar unter https://datenschutz.hessen.de/datenschutz/arbeitgeber-und-beschaeftigte/handreichung-zur-verarbeitung-personenbezogener-daten-von-beschaeftigten.
126 Vgl. hierzu die Entschließung der DSK vom 11. Mai 2023 (Fn. 112).

jene Vorschrift grundsätzlich zu prüfen wäre, ob sie eine spezifischere Vorschrift im Sinne von Art. 88 DSGVO darstellt. Zu beachten ist aber zum einen, dass sich das Urteil des Europäischen Gerichtshofs nur auf die hessische Rechtslage bezieht und zudem zur (Nicht-)Vereinbarkeit von § 86 Abs. 4 Satz 1 HBG mit den Anforderungen des Art. 88 DSGVO keine endgültige Aussage trifft. Das bayerische Personalaktenrecht befand sich hier schon gar nicht „auf dem Prüfstand". Zum anderen ist Art. 103 Satz 1 Nr. 1 BayBG Teil eines regulatorischen Gesamtsystems und steht insbesondere mit der personellen Verarbeitungsbeschränkung nach Art. 103 Satz 2 BayBG in einem engen Zusammenhang. Die weiteren Vorschriften des bayerischen Personalaktenrechts enthalten überwiegend ohnehin teils sehr spezifische Vorgaben zum Schutz betroffener Beschäftigter. Die „Kritik" des Europäischen Gerichtshof an § 86 Abs. 4 Satz 1 HBG kann damit jedenfalls nicht unbesehen auf Art. 103 Satz 1 Nr. 1 BayBG übertragen werden. Unabhängig hiervon kommt freilich in Betracht, Art. 103 Satz 1 Nr. 1 BayBG als Rechtsgrundlage im Sinne von Art. 6 Abs. 3 in Verbindung mit Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO aufzufassen. Zu der dargestellten Prüfung ist zunächst der bayerische Gesetzgeber aufgerufen, im Streitfall gegebenenfalls auch die Gerichte.

Das Urteil des Europäischen Gerichtshofs kann jedoch über die Grenzen des Beschäftigtendatenschutzes hinaus als „Weckruf" verstanden werden: Denn auch andere Öffnungsklauseln enthalten – vielfach zwingende – Vorgaben, in deren Grenzen sich mitgliedstaatliches Recht bewegen muss. Der Gesetzgeber sollte damit die Ausführungen des Europäischen Gerichtshofs in dem hier vorgestellten Urteil im Blick behalten, wenn er künftig von den Öffnungsklauseln der Datenschutz-Grundverordnung Gebrauch machen möchte. Die Entscheidung kann für den Gesetzgeber ferner Anlass sein, den bestehenden datenschutzrechtlichen Normenbestand auf etwaigen „Nachbesserungsbedarf" hin zu überprüfen. In diesem Zusammenhang ist im Blick zu behalten, dass der Europäische Gerichtshof jedenfalls bei der Verarbeitung von Beschäftigtendaten im öffentlichen Dienst einen „Austausch von Öffnungsklauseln" für möglich hält: Auch wenn eine ursprünglich auf Art. 88 DSGVO gestützte nationale Rechtsvorschrift die Anforderungen dieser Öffnungsklausel im Lichte der Rechtsprechung des Europäischen Gerichtshofs womöglich nicht erfüllt, kann sie gegebenenfalls auf Art. 6 Abs. 1 UAbs. 1 Buchst. c und e, Abs. 3 DSGVO gestützt werden.

7.1.5 Fazit

Die Entscheidung des Europäischen Gerichtshofs macht deutlich, dass mitgliedstaatliches „Durchführungsrecht", welches auf Grundlage von Öffnungsklauseln der Datenschutz-Grundverordnung erlassen wird, die Anforderungen und Grenzen der jeweiligen Öffnungsklausel beachten muss. Zugleich legt sie nahe, dass nationale Regelungen gegebenenfalls auch auf unterschiedliche Öffnungsklauseln gestützt werden können. Unmittelbare Auswirkungen auf das bayerische Personalaktenrecht hat das Urteil zunächst jedoch nicht.

7.2 Neuerungen im bayerischen Dienstrecht

Zum Ende der vergangenen Legislaturperiode hat das bayerische Dienstrecht Änderungen erfahren. Soweit diese datenschutzrechtlich von Bedeutung waren, war ich in die „einschlägigen" Rechtsetzungsverfahren eingebunden. Ausgewählte Rechtsänderungen mit Datenschutzbezug möchte ich im Folgenden vorstellen.

7.2.1 Unfallfürsorge: Übermittlung von Untersuchungs- oder Beobachtungsbefunden

Das Gesetz zur Änderung dienstrechtlicher Vorschriften[127] hat unter anderem einen Regelungsbedarf im Bereich der Unfallfürsorge adressiert, auf den ich schon vor Jahren hingewiesen hatte (vgl. meinen 24. Tätigkeitsbericht 2009/2010 unter Nr. 11.1.2):

Wird ein Beamter oder eine Beamtin durch einen Dienstunfall verletzt, wird Unfallfürsorge gewährt (Art. 45 Abs. 1 Satz 1 Bayerisches Beamtenversorgungsgesetz – BayBeamtVG). Soweit dies zur Entscheidung über die Gewährung von Unfallfürsorge erforderlich ist, sind Beamte und Beamtinnen gemäß Art. 45 Abs. 3 Satz 1 BayBeamtVG verpflichtet, sich auf Verlangen der Pensionsbehörde ärztlich oder psychologisch untersuchen oder beobachten zu lassen und die erforderlichen Auskünfte zu erteilen. Zu diesem Zweck darf die Pensionsbehörde Erkenntnisse und Beweismittel an die begutachtende Stelle, etwa an ein Gesundheitsamt, weitergeben (Art. 45 Abs. 3 Satz 2 BayBeamtVG).

Bislang enthielt Art. 45 Abs. 3 BayBeamtVG allerdings keine datenschutzrechtliche Rechtsgrundlage für den „Rückkanal", also für die Übermittlung von Untersuchungs- oder Beobachtungsbefunden von den begutachtenden Stellen an die Pensionsbehörde, obgleich ich schon frühzeitig vorgeschlagen hatte, insoweit Art. 67 Bayerisches Beamtengesetz (BayBG) für entsprechend anwendbar zu erklären (siehe meinen 24. Tätigkeitsbericht 2009/2010 unter Nr. 11.1.2). Diese Vorschrift betrifft die Mitteilung aus amtsärztlichen Untersuchungsbefunden bei Begutachtungen zur Dienstfähigkeit. Sie schafft mit materiellen und Verfahrensvorgaben einen Ausgleich zwischen den berechtigten Informationsinteressen der personalverwaltenden Stelle und den Persönlichkeitsrechten der begutachteten Personen: Während Art. 67 Abs. 1 BayBG den zulässigen Mitteilungsumfang normiert, enthalten Art. 67 Abs. 2 und 3 BayBG Vorgaben zur Übermittlung, Aufbewahrung und zweckgebundenen Verwendung der amtsärztlichen Mitteilung sowie zur Verfahrenstransparenz.

Entgegen dieser Empfehlung musste sich die Praxis damit behelfen, die Übermittlung von Untersuchungs- oder Beobachtungsbefunden an die Pensionsbehörde auf ausdrückliche Einwilligungen der begutachteten Personen zu stützen. Diese „Einwilligungslösung" bringt in Unfallfürsorgeangelegenheiten jedoch schon aufgrund der zwischenzeitlich mit Einführung der Datenschutz-Grundverordnung europarechtlich zwingend vorgegebenen freien Widerruflichkeit einer Einwilligung (vgl. Art. 7 Abs. 3 Satz 1 DSGVO) sowohl für die betroffenen Personen als Beteiligte als auch für die begutachtenden Stellen, insbesondere die Gesundheitsämter, eine erhebliche Rechtsunsicherheit mit sich.

Endlich, muss man sagen, hat sich der Gesetzgeber dieses im Grunde einfach zu behebenden Defizits angenommen: Für die Übermittlung von Untersuchungs- oder Beobachtungsbefunden gilt Art. 67 BayBG nach dem neuen Art. 45 Abs. 3 Satz 3 BayBeamtVG nun entsprechend.

[127] Vom 7. Juli 2023 (GVBl. S. 313).

7.2.2 Elektronische Fernprüfungen

Die mit der COVID-19-Pandemie verbundenen Einschränkungen hatten auch auf das Prüfungswesen erheblichen Einfluss. Sie brachten es insbesondere mit sich, dass Prüfungen gegebenenfalls nicht mehr in Präsenz, sondern als digitale Fernprüfungen durchgeführt werden mussten. Für den Hochschulbereich wurden einschlägige Vorgaben in der Bayerischen Fernprüfungserprobungsverordnung geregelt (siehe hierzu ausführlich meinen 30. Tätigkeitsbericht 2020 unter Nr. 10.1.4). Prüfungen nach dem bayerischen Leistungslaufbahnrecht wurden zu Pandemiezeiten in erforderlichem Umfang auf Basis von Art. 70a Leistungslaufbahngesetz (LlbG) als elektronische Fernprüfungen durchgeführt. Die dabei gewonnenen Erfahrungen haben den Gesetzgeber dazu bewogen, die Möglichkeit elektronischer Fernprüfungen auch im Prüfungsrecht des bayerischen öffentlichen Dienstes dauerhaft zu eröffnen.[128]

Grundlegende Vorgaben zu beamtenrechtlichen Prüfungen enthält das Leistungslaufbahngesetz (LlbG). Der durch das Gesetz zur Änderung dienstrechtlicher Vorschriften[129] neugefasste Art. 22 Abs. 2 Satz 2 LlbG sieht vor, Prüfungen bei Regelbewerberinnen und Regelbewerbern als elektronische Fernprüfungen durchzuführen. Diese Option wurde auch in anderen beamtenrechtlichen Prüfungsbereichen verankert.[130] Näheres zu elektronischen Fernprüfungen ist durch Rechtsverordnung festzulegen (vgl. insbesondere Art. 22 Abs. 2 Satz 2 LlbG). Für Prüfungen bei Regelbewerberinnen und Regelbewerbern geschieht dies in der Allgemeinen Prüfungsordnung (APO), die zugleich als „Rahmenordnung" für etwaige spezifischere Prüfungsordnungen (vgl. etwa Art. 37 Abs. 3 Satz 4 und 5 in Verbindung mit Art. 67 LlbG) angesehen werden kann. Art. 22 Abs. 7 LlbG gibt den Mindestinhalt dieser Rechtsverordnung vor, wozu auch Bestimmungen „zur Sicherung des Datenschutzes" zählen (Art. 22 Abs. 7 Satz 3 Nr. 1 LlbG).

Bei meiner Beteiligung im Gesetzgebungsverfahren habe ich empfohlen, sich bei den hiernach in datenschutzrechtlicher Hinsicht notwendigen Anpassungen der Allgemeinen Prüfungsordnung an den einschlägigen Vorschriften der Bayerischen Fernprüfungserprobungsverordnung zu orientieren. Diese Empfehlung hat der Verordnungsgeber in der Verordnung zur Änderung der Allgemeinen Prüfungsordnung[131] weitgehend aufgegriffen: Der Regelungsinhalt der §§ 3 bis 7 sowie § 9 BayFEV findet sich im Wesentlichen in Art. 15 Abs. 4 sowie in §§ 56 bis 60 APO wieder – die Allgemeine Prüfungsordnung trifft damit insbesondere Vorgaben zur Datenverarbeitung (§ 57 APO) sowie zur Aufsicht bei Fernklausuren (§ 58 APO).

7.2.3 Art. 103a BayBG: Datenverarbeitung bei Aufgabenübertragung

Der neue Art. 103a Satz 1 BayBG enthält eine Verarbeitungsbefugnis für Fälle, in denen ein Dienstherr oder Arbeitgeber (vgl. Art. 145 Abs. 2 BayBG) außerhalb des staatlichen Bereichs die Abrechnung von Bezügen oder weiteren (Neben-) Leistungen auf das Landesamt für Finanzen übertragen hat (vgl. hierzu insbesondere Art. 101 Abs. 2 Bayerisches Besoldungsgesetz – BayBesG – in Verbindung

[128] Vgl. zum Ganzen Landtags-Drucksache 18/28504, S. 2.
[129] Siehe Fn. 127.
[130] Vgl. etwa Art. 37 Abs. 3 Satz 4 LlbG oder Art. 48 Abs. 5 Satz 2 LlbG.
[131] Vom 19. September 2023 (GVBl. S. 570).

mit Art. 14 Satz 3 BayBesG). In diesem Rahmen darf das Landesamt auch besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO verarbeiten, soweit dies zur Erfüllung der ihm übertragenen Aufgaben erforderlich ist. Bei diesen Verarbeitungen ist das Landesamt Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO (Art. 103a Satz 3 BayBG).

7.2.4 Fazit

Die dargestellten Rechtsänderungen zeigen einmal mehr die hohe Bedeutung des Datenschutzes im öffentlichen Dienstrecht. „Einschlägige" Gesetzgebungsverfahren werde ich weiterhin eng begleiten. Dabei ist es mein Ziel, den Datenschutzrechten der im bayerischen öffentlichen Dienst Beschäftigten bestmöglich zur Geltung zu verhelfen. Auch wenn, wie im geschilderten Fall der Unfallfürsorge, mitunter ein gewisses Maß an Ausdauer und Beharrlichkeit geboten ist: Ich bin weiter zuversichtlich, dass meine datenschutzrechtlichen Empfehlungen beim Gesetzgeber auch in Zukunft Gehör finden. Schließlich ist ein gut aufgestellter Beschäftigtendatenschutz auch ein Zeichen der Fairness und Berechenbarkeit bayerischer Dienstherren und öffentlicher Arbeitgeber.

7.3 Vorstellungsgespräche in Gruppen

Personalgewinnung ist auch für bayerische – insbesondere, aber nicht nur staatliche und kommunale – Dienstherren und öffentliche Arbeitgeber ein Dauerthema. Um in Stellenbesetzungsverfahren fundierte Auswahlentscheidungen treffen zu können, müssen sie sich im Vorfeld ein aussagekräftiges „Bild" von den Bewerberinnen und Bewerbern machen. Als Grundlage hierfür dienen neben schriftlichen Bewerbungsunterlagen insbesondere Vorstellungsgespräche. Bei der Gestaltung dieser Gespräche sind allerdings die Datenschutzrechte der betroffenen Bewerberinnen und Bewerber im Blick zu behalten.

Eine bayerische öffentliche Stelle hatte auf ihrer Internetseite Bewerberinnen und Bewerber über den Ablauf des Auswahlverfahrens für neu oder nachzubesetzende Stellen informiert. Dabei wurde unter anderem darauf hingewiesen, dass ein „Erstgespräch" eventuell auch als „Gruppengespräch mit drei bis vier Mitbewerberinnen und Mitbewerbern" durchgeführt werden könne. Mit einer auf den ersten Blick ähnlichen Konstellation, nämlich einem besonderen Auswahlverfahren im Rahmen der Berufung in das Beamtenverhältnis, hatte ich mich bereits in meinem 26. Tätigkeitsberichts 2013/2014 unter Nr. 11.5 befasst.

Aus datenschutzrechtlicher Sicht sind solche Gruppengespräche bedenklich, weil hier nicht nur der potentielle Beschäftigungsgeber, sondern gegebenenfalls auch andere Bewerberinnen und Bewerber Einzelheiten zu persönlichen und beruflichen Verhältnissen ihrer Mitbewerbenden erfahren können. Schon die Tatsache, dass sich eine Person auf eine bestimmte Stelle beworben hat, geht Dritte eigentlich „nichts an".

Ich habe mich deshalb an die betreffende öffentliche Stelle gewandt und auf Folgendes hingewiesen:

Angesichts des verfassungsrechtlich gewährleisteten Grundsatzes der Bestenauslese (Art. 33 Abs. 2 Grundgesetz – GG, Art. 94 Abs. 2 Satz 1 Verfassung des Freistaates Bayern) haben bayerische Dienstherren und öffentliche Arbeitgeber

zwar einen gewissen Spielraum bei der Ausgestaltung von Auswahlverfahren für Stellennach- und -neubesetzungen. Dies entbindet sie freilich nicht von bestehenden rechtlichen Vorgaben – einschließlich des Datenschutzrechts. Im Hinblick auf die Grundrechte jeder Bewerberin und jedes Bewerbers auf Datenschutz (Art. 8 Charta der Grundrechte der Europäischen Union) sowie auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) ist ein Vorstellungsgespräch so zu gestalten, dass die Bewerberinnen und Bewerber möglichst wenige Daten ihrer Mitbewerbenden erfahren.

Für bayerische Dienstherren und öffentliche Arbeitgeber ergibt sich dies einfachgesetzlich aus Art. 103 Satz 1 Nr. 1 Bayerisches Beamtengesetz (BayBG), der gemäß Art. 145 Abs. 2 BayBG auch auf vertraglich Beschäftigte im bayerischen öffentlichen Dienst grundsätzlich entsprechend anwendbar ist: Hiernach ist eine Verarbeitung – einschließlich der Offenlegung – personenbezogener Bewerbungsdaten durch bayerische Dienstherren und öffentliche Arbeitgeber nur zulässig, soweit dies insbesondere für Zwecke der Personalverwaltung und Personalwirtschaft erforderlich ist.

Aus datenschutzrechtlicher Sicht sind in Auswahlverfahren daher grundsätzlich Einzelgespräche vorzugswürdig; jedenfalls sind aber alle sensiblen und persönlichen Daten der Mitbewerbenden in einem Einzelgespräch zu klären, wie beispielsweise die Vorstellung der einzelnen Bewerberinnen und Bewerber oder die Erörterung ihrer lebenslaufbezogenen Daten. Sollten jedoch Teile des Vorstellungsgesprächs aus fachlichen Gründen zwingend in Gruppen durchzuführen sein, so dürfen die Bewerberinnen und Bewerber nur die für die fachliche Auswahl unbedingt erforderlichen personenbezogenen Daten ihrer Mitbewerbenden erfahren. Ich habe die öffentliche Stelle aufgefordert, die bestehende Praxis anhand dieser Maßstäbe kritisch zu überprüfen.

In ihrer Stellungnahme hat die öffentliche Stelle mir sowohl die Grundsätze ihres Auswahlverfahrens als auch hiervon mögliche Ausnahmen dargelegt. Danach würden die aus datenschutzrechtlicher Sicht bedenklichen Gruppengespräche nur in wenigen Fällen und nur dann stattfinden, wenn fachliche Gründe dies geböten. Dies sei insbesondere bei schriftlichen Einstellungstests, die zeitgleich mit mehreren Bewerbern durchgeführt werden, sowie beim Testen von Softskills wie Kommunikations- und Informationsverhalten und dem Interagieren in einer Gruppe der Fall. Alle sensiblen und persönlichen Daten der Mitbewerbenden würden in Einzelgesprächen geklärt. Vorsorglich sei das Personalreferat um Kontrolle und gegebenenfalls Nachbesserung der bisherigen Abläufe gebeten worden.

Die insoweit missverständlichen Ausführungen auf ihrer Internetseite hat die öffentliche Stelle zwischenzeitlich entfernt. Vor diesem Hintergrund habe ich von weiteren Maßnahmen abgesehen.

7.4 Fehlerhafte Zugriffsrechte auf Personalaktendaten

Die Verarbeitung von Personalaktendaten ist grundsätzlich den personalverwaltenden Stellen vorbehalten. Diese „personelle Verarbeitungsbeschränkung“ ist durch technische und organisatorische Maßnahmen hinreichend abzusichern – gleich, ob Personalaktendaten in Papierform oder digital verarbeitet werden. Dass gerade bei der elektronischen Aufbewahrung solcher Daten etwas schiefgehen kann, zeigen zwei Meldungen von Datenschutzverletzungen (vgl. Art. 33 DSGVO), denen ähnliche „Pannen“ bei der Rechteverwaltung zugrunde lagen. Bei meiner

Überprüfung dieser Meldungen musste ich auch leider feststellen, dass fehlerhafte Zugriffsrechte nicht das einzige Datenschutzproblem waren.

7.4.1 Sachverhalt

Im **ersten Fall** hatte eine oberste Landesbehörde über ein Jahrzehnt hinweg quartalsmäßige Excel-Exporte aus dem Personal- und Stellenmanagementsystem VIVA[132] (im Folgenden: VIVA-Exporte) in einem speziellen, eigentlich der Personalstelle vorbehaltenen Ordner digital abgelegt und aufbewahrt. Die VIVA-Exporte enthielten eine Vielzahl an Personaldaten, neben Namen und Geburtsdaten Beschäftigter etwa Angaben zu Qualifikation, tarif- oder besoldungsrechtlichen Zuordnungen sowie zu Art und Umfang der Beschäftigung. Vereinzelt waren mit dem Grad der Behinderung auch Gesundheitsdaten umfasst. Der Unterordner mit den VIVA-Exporten befand sich allerdings in einem allgemein zugänglichen Ordner auf einem IT-System der obersten Landesbehörde. Diese nahm unzutreffend an, dass nur Beschäftigte ihrer Personalstelle auf den Ordner mit den VIVA-Exporten zugreifen konnten. Sie musste dann jedoch feststellen, dass jedenfalls zeitweise alle Beschäftigten der obersten Landesbehörde zugriffsberechtigt gewesen waren. Wie es zu einer ungeplanten Ausweitung von Zugriffsbefugnissen kommen konnte, ließ sich im Nachhinein nicht mehr nachvollziehen.

Im **zweiten Fall** hielt das Schulverwaltungsamt einer großen kreisfreien Stadt vertrauliche Dokumente der Amtsleitung in einem Ordner digital auf dem Amtslaufwerk vor. Die gespeicherten Dokumente umfassten unter anderem eine Datei mit Bewerbungsunterlagen für ein Stellenbesetzungsverfahren aus dem Jahr 2017, Beschäftigtendaten im Zusammenhang mit der COVID-19-Pandemie sowie Beurteilungen und Zeugnisse Beschäftigter, die teilweise bis in das Jahr 2005 zurückreichten. Der Zugriff auf diesen Ordner sowie auf die in ihm enthaltenen Dokumente war planmäßig der Amtsleitung vorbehalten. Aufgrund versehentlich fehlerhaft gesetzter Zugriffsrechte konnten allerdings alle Beschäftigten des Amtes über einen Zeitraum von etwa zwei Jahren auf den Ordner zugreifen.

Ob „außerhalb“ der vorgesehenen Zugriffsberechtigungen tatsächlich auf den betreffenden Ordner zugegriffen wurde, konnte mir die oberste Landesbehörde im ersten Fall nicht sicher beantworten. Im zweiten Fall waren der betreffenden Stadt zumindest Zugriffe durch zwei ihrer Beschäftigten bekannt; weitere Zugriffe konnten mangels Protokollierung nicht nachgewiesen werden.

7.4.2 Rechtliche Würdigung

7.4.2.1 Fehlerhafte Zugriffsrechte

Verantwortliche müssen bei „ihren“ Verarbeitungen in technischer und organisatorischer Hinsicht verschiedene Vorgaben des Datenschutzrechts beachten. So haben sie insbesondere durch geeignete technische und organisatorische Maßnahmen nachweisbar sicherzustellen, dass ihre Verarbeitungen im Einklang mit der Datenschutz-Grundverordnung stehen (Art. 24 Abs. 1 Satz 1 DSGVO). Art. 32 Abs. 1 DSGVO verpflichtet Verantwortliche, geeignete technische und organisatorische Maßnahmen zu ergreifen, „um ein dem Risiko der Verarbeitung angemes-

[132] Vgl. zu diesem System meinen 24. Tätigkeitsbericht 2009/2010 unter Nr. 11.2.1.

senes Schutzniveau zu gewährleisten“. In Umsetzung des Grundsatzes der „Vertraulichkeit“ einer Verarbeitung (Art. 5 Abs. 1 Buchst. f DSGVO) umfassen solche Maßnahmen auch die Fähigkeit, die Vertraulichkeit der im Rahmen der Verarbeitung verwendeten Systeme und Dienste auf Dauer sicherzustellen (Art. 32 Abs. 1 Buchst. b DSGVO). Bei der Verarbeitung von besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO (etwa Gesundheitsdaten) haben bayerische öffentliche Stellen nach Art. 8 Abs. 2 Satz 1 BayDSG zudem angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Solche Maßnahmen können unter anderem darin bestehen, den Zugang zu diesen sensiblen Daten innerhalb des Verantwortlichen zu beschränken.[133]

Die Excel-Exporte aus dem Personal- und Stellenmanagementsystem VIVA enthielten zumindest überwiegend Personalaktendaten im Sinne von Art. 103 ff. Bayerisches Beamtengesetz (BayBG), § 50 Satz 2 Beamtenstatusgesetz; diese Vorschriften finden auf vertraglich im bayerischen öffentlichen Dienst Beschäftigte grundsätzlich entsprechende Anwendung (Art. 145 Abs. 2 BayBG). Im zweiten Fall wurden neben Personalaktendaten (Beschäftigtendaten im Zusammenhang mit der COVID-19-Pandemie sowie Beurteilungen und Zeugnisse Beschäftigter) auch Bewerbungsdaten verarbeitet. Für die Verarbeitung von Bewerbungs- und Personalaktendaten enthält die personelle Verarbeitungsbeschränkung nach Art. 103 Satz 2 BayBG ein spezifisches Vertraulichkeitserfordernis: Nur Beschäftigte, die vom Dienstherrn mit der Bearbeitung von Personalangelegenheiten betraut worden sind, dürfen diese Daten verarbeiten.

Angesichts dieser Vorgaben hätten die digital aufbewahrten Bewerbungs- und Personalaktendaten in den gemeldeten Sachverhalten somit gegen unbefugte Zugriffe hinreichend gesichert werden müssen. Dem sind die Verantwortlichen in beiden Fällen nicht nachgekommen: Zwar haben sie im Ausgangspunkt entsprechende Zugriffsbeschränkungen vorgesehen und damit im Grundsatz Problembewusstsein gezeigt. Sie haben es aber versäumt, das fortdauernde Bestehen sowie die Wirksamkeit dieser Beschränkungen im Weiteren hinreichend zu überprüfen (vgl. auch Art. 24 Abs. 1 Satz 2 sowie Art. 32 Abs. 1 Buchst. d DSGVO). In der Folge stand die „digitale Tür“ zu diesen Daten für einen erheblichen Zeitraum auch Beschäftigten offen, die nicht mit Personalangelegenheiten betraut waren.

7.4.2.2 Erforderlichkeit der Verarbeitung

Das geschilderte Zurückbleiben hinter technischen und organisatorischen Vorgaben war schon misslich genug. In beiden Fällen kam aber noch hinzu, dass die jeweiligen Dateiordner personenbezogene Daten enthielten, die entweder überhaupt nicht (erster Fall) oder nicht mehr (zweiter Fall) hätten aufbewahrt werden dürfen. Die fehlerhaft gesetzten Zugriffsrechte ermöglichten damit – jedenfalls theoretisch – einen unbefugten Zugang zu unrechtmäßig gespeicherten Daten.

Ausgangspunkt meiner Prüfung waren insoweit die Datenschutz-Grundsätze in Art. 5 Abs. 1 DSGVO, die Verantwortliche bei jeder Verarbeitung personenbezogener Daten zu beachten haben. Personenbezogene Daten müssen danach insbesondere auf rechtmäßige und in einer auf das zur Zweckerreichung notwendige Maß beschränkten Weise verarbeitet werden (Grundsätze der „Rechtmäßigkeit“ und der „Datenminimierung“, Art. 5 Abs. 1 Buchst. a und c DSGVO). Eine Speiche-

[133] Vgl. Landtags-Drucksache 17/19628, S. 35 f.

rung personenbezogener Daten ist dabei nur solange zulässig, wie dies zur Erreichung der Verarbeitungszwecke erforderlich ist (Grundsatz der „Speicherbegrenzung“, Art. 5 Abs. 1 Buchst. e DSGVO). Rechtmäßig im Sinne von Art. 5 Abs. 1 Buchst. a DSGVO ist eine Verarbeitung, wenn sie auf eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO, gegebenenfalls in Verbindung mit nationalem Durchführungsrecht, gestützt werden kann. Bei der Verarbeitung von besonderen Kategorien personenbezogener Daten (etwa von Gesundheitsdaten) muss ferner ein Zulässigkeitstatbestand nach Art. 9 Abs. 2 DSGVO erfüllt sein.

Im **ersten Fall** war die Speicherung der Excel-Exporte aus dem Personal- und Stellenmanagementsystem VIVA an Art. 103 Satz 1 BayBG zu messen:

„[1]Der Dienstherr darf personenbezogene Daten über Bewerber und Bewerberinnen sowie aktive und ehemalige Beamte und Beamtinnen verarbeiten, soweit dies
1. zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere zu Zwecken der Personalverwaltung oder Personalwirtschaft erforderlich ist,
2. zusätzlich bei der Verarbeitung besonderer Kategorien personenbezogener Daten Art. 8 Abs. 1 Nr. 2, 3 und 5 sowie Abs. 2 des Bayerischen Datenschutzgesetzes (BayDSG) erlaubt
und nachfolgend nichts anderes bestimmt ist.“

Die Vorschrift kommt auch zur Anwendung, wenn Personalakten in automatisierten Verfahren (zum Beispiel in VIVA) verarbeitet werden (Art. 111 Satz 2 BayBG). Sie lässt die Verarbeitung solcher Daten durch personalverwaltende Stellen damit insbesondere für Zwecke der Personalverwaltung und Personalwirtschaft zu – allerdings nur, soweit die Verarbeitung zur Erreichung dieser Zwecke auch erforderlich ist. Erforderlich ist eine Verarbeitung dabei nicht schon dann, wenn sie für die verfolgten Verarbeitungszwecke lediglich „‚förderlich‘ oder ‚nützlich‘, also in irgendeiner Weise hilfreich“ ist.[134]

Vor diesem Hintergrund hat sich mir schon nicht erschlossen, weshalb die – sowohl in zeitlicher als auch in inhaltlicher Hinsicht – umfangreiche Speicherung von VIVA-Exporten in einem Dateiordner der personalverwaltenden Stelle für die vorgenannten Zwecke erforderlich sein sollte. Schließlich kann die oberste Landesbehörde die Daten ihrer Beschäftigten unmittelbar in VIVA einsehen und abrufen. Die insoweit praktizierte „doppelte Datenhaltung“ habe ich gerade angesichts des Grundsatzes der Datenminimierung kritisch gesehen. Die oberste Landesbehörde hat die Speicherung der VIVA-Exporte damit begründet, verschiedene personalwirtschaftliche Auswertungen (etwa zur Personalentwicklung oder zur Personalbemessung) zu ermöglichen. In VIVA selbst seien diese Auswertungen nicht oder nur mit erheblichem Aufwand durchführbar.

Zwar nennt Art. 103 Satz 1 BayBG die Personalwirtschaft ausdrücklich als legitimen Zweck zur Verarbeitung von Personalaktendaten. Damit konnte die insoweit rechenschaftspflichtige (vgl. Art. 5 Abs. 2 DSGVO) oberste Landesbehörde aber noch nicht begründen, weshalb die umfangreiche Speicherung von VIVA-Exporten für diesen Zweck erforderlich gewesen war: Zunächst hätte die Behörde nämlich prüfen müssen, ob die genannten Auswertungszwecke eine Speicherung der VIVA-Exporte mit den „Klardaten“ der Beschäftigten überhaupt notwendig machten oder – was aus meiner Sicht nahe lag – ob es nicht ausgereicht hätte, insoweit

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

mit anonymisierten oder zumindest pseudonymisierten Datensätzen zu arbeiten. Ferner wäre zu prüfen gewesen, ob eine Speicherung der VIVA-Exporte in größerem zeitlichem Abstand (etwa jährlich statt quartalsweise) genügt hätte. Diese Prüfungen hatte die öffentliche Stelle nicht vorgenommen.

Im **zweiten Fall** konnte mir die insoweit rechenschaftspflichtige (vgl. Art. 5 Abs. 2 DSGVO) Stadt zwar erläutern, weshalb die Speicherung von Bewerbungs- und Personalaktendaten anfangs erforderlich gewesen war. Wie die Stadt selbst eingeräumt hat, hätte ihr Schulverwaltungsamt die betreffenden Daten allerdings schon längst wieder löschen müssen:

Bewerbungsunterlagen dürfen nach Art. 103 Satz 1 BayBG verarbeitet werden, soweit dies für die dort genannten Zwecke erforderlich ist. Daten unterlegener Bewerberinnen und Bewerber dürfen ohne deren Einwilligung dabei regelmäßig allenfalls sechs Monate nach Abschluss des Bewerbungsverfahrens aufbewahrt werden.[135] Die von der Amtsleitung aufbewahrten Bewerbungsdaten betrafen ein Stellenbesetzungsverfahren aus dem Jahr 2017; der sechsmonatige Aufbewahrungszeitraum war damit weit überschritten. Die Daten erfolgreicher Bewerberinnen und Bewerber werden Teil des jeweiligen Personalakts, der von der personalverwaltenden Stelle bei der Stadt geführt wird. Nach Abschluss des Bewerbungsverfahrens haben diese Daten bei der Leitung des Schulverwaltungsamts nichts mehr zu suchen.

Die eingangs genannten Personalaktendaten (Beschäftigtendaten im Zusammenhang mit der COVID-19-Pandemie sowie Beurteilungen und Zeugnisse Beschäftigter) hat die Amtsleitung nach Darstellung der Stadt als unselbstständigen Personalnebenakt im Sinn des Art. 104 Abs. 1 Satz 3 BayBG vorgehalten.

Das Führen einer Personalnebenakte bedingt eine gesetzlich vorgesehene „doppelte Datenhaltung". Deren Erforderlichkeit ist angesichts des Grundsatzes der Datenminimierung stets kritisch zu prüfen:

Im Rahmen der „3G-Zutrittsregel" am Arbeitsplatz waren zwar auch bayerische Dienstherren und öffentliche Arbeitgeber zunächst befugt, Angaben zum Impf- oder Genesungsstatus Beschäftigter in gewissem Umfang zu verarbeiten, vgl. insbesondere § 28b Abs. 3 Satz 3 Infektionsschutzgesetz (IfSG) a. F. Wie die 3G-Zutrittsregelung nach § 28b Abs. 1 bis 3 IfSG a. F. insgesamt ist auch diese Verarbeitungsbefugnis allerdings zum 19. März 2022 aufgehoben worden.[136] Die auf Grundlage von § 28b Abs. 3 Satz 3 IfSG a. F. (rechtmäßig) erhobenen Daten waren spätestens am Ende des sechsten Monats nach ihrer Erhebung zu löschen, § 28 Abs. 3 Satz 10 Halbsatz 1 IfSG a. F. Schon dem Wortlaut nach handelte es sich hierbei um eine Höchstfrist, deren Einhaltung Verantwortliche durch geeignete Löschroutinen sicherzustellen hatten.[137] Zum Zeitpunkt des Bekanntwerdens des Vorfalls bei der Stadt war diese Höchstfrist bereits überschritten.

Soweit dienstliche Beurteilungen sowie Zeugnisentwürfe Beschäftigte des Schulverwaltungsamts betrafen, sah die Stadt eine Aufbewahrung dieser Dokumente

[135] Siehe hierzu meinen 25. Tätigkeitsbericht 2011/2012 unter Nr. 11.8.2.

[136] Art. 1 Nr. 6 Buchst. a Gesetz zur Änderung des Infektionsschutzgesetzes und anderer Vorschriften vom 18. März 2022 (BGBl. I S. 466).

[137] Vgl. ausführlich zum Ganzen Bayerischer Landesbeauftragter für den Datenschutz, 3G-Zutrittsregel im bayerischen öffentlichen Dienst, Aktuelle Kurz-Information 38, Stand 12/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018".

bei der Amtsleitung zwar in gewissem Umfang als erforderlich im Sinne von Art. 103 Satz 1, Art. 104 Abs. 1 Satz 3 BayBG an. Die vorgebrachten zeitlichen Erforderlichkeitsgrenzen[138] waren im vorliegenden Fall jedoch deutlich verletzt worden, da die bei der Amtsleitung gespeicherten Beurteilungen und Zeugnisse teilweise bis in das Jahr 2005 zurückreichten.

In beiden Fällen ist die Speicherung von Beschäftigtendaten folglich unrechtmäßig erfolgt. Die öffentlichen Stellen haben damit nicht nur gegen technische und organisatorische Vorgaben, sondern auch gegen die Grundsätze der Rechtmäßigkeit der Verarbeitung (Art. 5 Abs. 1 Buchst. a, Art. 6 Abs. 1 DSGVO) sowie der Speicherbegrenzung (Art. 5 Abs. 1 Buchst. e DSGVO) verstoßen.

7.4.3 Ergriffene Maßnahmen

Angesichts des Gewichts der Datenschutzverstöße habe ich in beiden Fällen eine förmliche datenschutzrechtliche Beanstandung ausgesprochen. Zugleich habe ich beiden Verantwortlichen Hinweise zur datenschutzkonformen Ausgestaltung ihrer Verarbeitungsvorgänge erteilt.

Im **ersten Fall** hat die oberste Landesbehörde ihr Vorgehen zur Erstellung von Auswertungen überarbeitet und im Zuge dessen den Umfang der vorgehaltenen Datensätze erheblich reduziert. Durch diese Maßnahmen sei ein Personenbezug bei den vorgehaltenen und künftigen Datensätzen weitgehend entfallen. Die dergestalt verschlankten Datensätze seien zudem in ein neu erstelltes „Personallaufwerk“ überführt worden, auf welches grundsätzlich nur die Personalverwaltung sowie die IT-Administration Zugriff hätten.

Der gemeldeten Datenschutzverletzung im **zweiten Fall** lag aus Sicht der Stadt ein individuelles Fehlverhalten zugrunde. Zur Vorhaltung von Personalunterlagen habe es bereits im Vorfeld spezifische Regeln gegeben; im Nachgang zur geschilderten Datenschutzverletzung seien die Dienststellenleitungen nun noch einmal grundsätzlich zu dieser Thematik informiert worden. In technischer und organisatorischer Hinsicht hat die Stadt ebenfalls Maßnahmen ergriffen, um vergleichbare Vorfälle künftig zu verhindern. Diesbezüglich befinde ich mich mit der Stadt noch im Austausch.

7.4.4 Fazit

Über die konkreten Vorkommnisse hinaus haben die beiden gemeldeten Datenpannen Dreierlei aufgezeigt:

— Erstens sind notwendige technische und organisatorische Maßnahmen – vorliegend in Form von Zugriffsbeschränkungen – hinreichend effektiv auszugestalten. Dazu gehört es auch, die Wirksamkeit dieser Maßnahmen im erforderlichen Umfang fortlaufend zu überprüfen.

— Zweitens haben Verantwortliche die Erforderlichkeit der von ihnen durchgeführten Verarbeitungen kritisch in den Blick zu nehmen – nicht nur, aber gerade dann, wenn sensible Personalaktendaten verarbeitet werden. Die

[138] Siehe zur Aufbewahrung von Beurteilungsunterlagen auch meinen 31. Tätigkeitsbericht 2021 unter Nr. 8.2.

Erforderlichkeit hat dabei auch eine zeitliche Komponente; vorbehaltlich gesetzlicher Aufbewahrungspflichten wird sie nach Erreichen des Verarbeitungszwecks regelmäßig entfallen. Die Einhaltung des Datenschutzrechts ist für Verantwortliche eine Daueraufgabe.

— So bedauerlich die gemeldeten Vorfälle für sich genommen sind, belegen sie schließlich drittens, dass die in Art. 33 DSGVO vorgesehene Meldepflicht bei Datensicherheitsverletzungen zu einer nachhaltigen Verbesserung des Datenschutzniveaus bei Verantwortlichen beitragen kann.

7.5 Kontaktdaten kommunaler Beschäftigter auf der Plattform BayernPortal

Durch eine Beratungsanfrage zur Plattform BayernPortal wurde ich darauf aufmerksam, dass bayerische Kommunen, insbesondere Gemeinden und Landkreise, zur Bereitstellung von Kontaktdaten ihrer Beschäftigten durchaus unterschiedliche Ansätze entwickelt haben. Viele öffentliche Stellen geben im BayernPortal nur Namen und Kontaktdaten der Behördenleitung und der oder des behördlichen Datenschutzbeauftragten an. Andere erwähnen auch Beschäftigte mit leitender Funktion, während einige Gemeinden und Landratsämter die Kontaktdaten aller potentiellen Ansprechpartnerinnen und Ansprechpartner preisgeben. Dabei werden regelmäßig (zumindest) die vollständigen Namen und die dienstlichen Kontaktdaten (Telefonnummer, E-Mail-Adresse) sowie vielfach auch Angaben zu Dienstgebäude und Zimmernummer vorgehalten.

7.5.1 Beschäftigtendaten im Publikumsverkehr

Die Veröffentlichung von Beschäftigtendaten zum Zwecke einer unkomplizierten Kontaktaufnahme mit bayerischen öffentlichen Stellen ist ein regelmäßiges Beratungsthema, das bereits mehrfach Gegenstand meiner Veröffentlichungen war. Zur Frage der Verarbeitung von Beschäftigtendaten im Publikumsverkehr habe ich mich etwa in meinem 25. Tätigkeitsbericht 2011/2012 unter Nr. 11.8.7 und in meinem 22. Tätigkeitsbericht 2005/2006 unter Nr. 19.1 geäußert.

Aus datenschutzrechtlicher Sicht ist die Veröffentlichung von Beschäftigtendaten im Internet grundsätzlich als eine Verarbeitung personenbezogener Sachaktendaten zu organisatorischen Zwecken anzusehen. Sie kann auf Art. 4 Abs. 1 BayDSG oder Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG gestützt werden, wenn sie zur Erfüllung einer der öffentlichen Stelle obliegenden Aufgabe erforderlich ist. Zu den Aufgaben einer bayerischen öffentlichen Stelle gehört es auch, Bürgerinnen und Bürger darüber zu informieren, welche Beschäftigten die richtigen Ansprechpartnerinnen und Ansprechpartner für ihre Anliegen sind.

7.5.2 Verarbeitungszweck

Die Erforderlichkeit einer Verarbeitung personenbezogener Daten ist am Verarbeitungszweck auszurichten. Datenverarbeitungen, die nichts mit dem Verarbeitungszweck zu tun haben, können auch nicht zur Aufgabenerfüllung der öffentlichen Stelle erforderlich sein. Zur Verfolgung des Zwecks, Bürgerinnen und Bürger über behördliche Ansprechpartnerinnen und Ansprechpartner zu informieren, ist die Bereitstellung von dienstlichen Kontaktdaten ausreichend und allein zielführend. Datenverarbeitungen, die das Ziel der Kontaktaufnahme nicht erleichtern,

sind auch zur Aufgabenerfüllung der öffentlichen Stelle nicht erforderlich. Die Veröffentlichung von Lichtbildern oder Lebensläufen etwa kann die öffentliche Stelle daher von vornherein nicht auf die gesetzliche Verarbeitungsbefugnis zum Zwecke ihrer Aufgabenerfüllung stützen. Die Kenntnis dieser Informationen ist für die Kontaktherstellung grundsätzlich nicht relevant. Lichtbilder dürfen allenfalls auf der Grundlage einer – datenschutzkonformen – Einwilligung (vgl. Art. 4 Nr. 11, Art. 7 DSGVO) veröffentlicht werden. Von der Einholung von Einwilligungen rate ich aber ab. In einem Beschäftigungsverhältnis wird sich die betroffene Person bei der Einwilligung in eine ihr nicht vorteilhafte Verarbeitung häufig einem Druck ausgesetzt sehen, der die Freiwilligkeit ausschließt. Die Einwilligung ist in diesem Fall rechtlich nicht wirksam.

7.5.3 Erforderlichkeit zur Aufgabenerfüllung

Eine Verarbeitung personenbezogener Daten ist erforderlich, wenn die öffentliche Stelle ihre Aufgabe ohne die Verarbeitung nicht, nicht vollständig oder nicht in rechtmäßiger oder zumutbarer Weise erfüllen kann.[139] Der bei der Anwendung des Erforderlichkeitskriteriums zu beachtende Grundsatz der Verhältnismäßigkeit[140] zielt auf eine Güterabwägung, wobei die jeweiligen Gesamtumstände einzubeziehen sind. Das Interesse der öffentlichen Stelle, bürgerfreundlich aufzutreten und eine Kontaktaufnahme mit Beschäftigten möglichst einfach zu gestalten, ist mit den Datenschutzinteressen des oder der jeweils betroffenen Beschäftigten in Einklang zu bringen.

Der Erforderlichkeitsgrundsatz setzt in Bezug auf die Verarbeitung bestimmter Kontaktdaten Grenzen – auch unabhängig von der individuellen Situation der betroffenen Person. So könnte die Veröffentlichung privater Adressdaten von Beschäftigten zwar den Zweck der Kontaktvermittlung verfolgen; die Verarbeitung wäre aber nicht zur Aufgabenerfüllung der öffentlichen Stelle erforderlich.

Private Adressdaten von Beschäftigten sind im Übrigen Personalaktendaten und dürfen nur unter Einhaltung der Voraussetzungen der Art. 103 ff. Bayerisches Beamtengesetz (BayBG) und § 50 Beamtenstatusgesetz (BeamtStG) verarbeitet werden. Diese Vorschriften gelten für vertraglich Beschäftigte im bayerischen öffentlichen Dienst gemäß Art. 145 Abs. 2 BayBG entsprechend. Eine Veröffentlichung von Personalaktendaten im Internet ist nicht mit dem Vertraulichkeitsgebot gemäß § 50 Satz 3 BeamtStG vereinbar und kann nicht auf eine Verarbeitungsbefugnis gemäß Art. 103 ff. BayBG gestützt werden. Die Veröffentlichung privater Adressdaten von Beschäftigten bayerischer öffentlicher Stellen würde somit gegen den Grundsatz der Rechtmäßigkeit gemäß Art. 5 Abs. 1 Buchst. a DSGVO verstoßen.

7.5.4 Beschäftigte mit „Außenwirkung“

Welche Beschäftigten die Veröffentlichung dienstlicher Kontaktdaten dulden müssen, hängt maßgeblich von deren individueller Situation ab. Die Kontaktdaten von Beschäftigten, die nur wenig Bürgerkontakt haben, dürfen nicht veröffentlicht werden. Das Interesse an Vertraulichkeit überwiegt bei diesem Personenkreis das

[139] Vgl. Stief, in Schröder, Bayerisches Datenschutzgesetz, 2021, Art. 4 BayDSG Rn. 43.

[140] Vgl. Bayerisches Oberstes Landesgericht, Beschluss vom 6. August 2020, 1 VA 33/20, BeckRS 2020, 18859, Rn. 59.

Interesse der öffentlichen Stelle, die Daten preiszugeben. Bei Beschäftigten ohne jeglichen Bürgerkontakt besteht bereits keine Veranlassung zur Veröffentlichung von Kontaktdaten, weil die öffentliche Stelle insofern den Verarbeitungszweck (Transparenz durch Benennen von Ansprechpersonen) nicht verfolgen kann.

Dagegen müssen Beschäftigte, die eine Funktion mit „Außenwirkung" wahrnehmen, die Veröffentlichung ihres Namens (grundsätzlich nur des Nachnamens), ihrer dienstlichen Kontaktdaten (Telefonnummer und E-Mail-Adresse) und ihrer Zuständigkeiten hinnehmen. Wann genau eine solche Außenwirkung vorliegt, lässt sich im Einzelfall oft nicht trennscharf bestimmen. Unter „Personen mit Außenwirkung" sind nicht bereits alle zu verstehen, die irgendwie in Bürgerkontakt geraten könnten. Maßgeblich ist, ob ihnen eine auf die Öffentlichkeit bezogene, in einem gewissen Sinn „repräsentative" Aufgabe zukommt. Dies ist insbesondere bei Personen anzunehmen, die eine herausgehobene Funktion innerhalb der öffentlichen Stelle wahrnehmen, die sie zur direkten Ansprechpartnerin oder zum direkten Ansprechpartner macht.

Je nach Aufbau und Größe der öffentlichen Stelle können Positionen „mit Außenwirkung" unterschiedlich eingeordnet sein. Im Zweifelsfall ist die konkrete Funktion der betroffenen Person innerhalb der öffentlichen Stelle zu beurteilen. Dabei kann insbesondere eine Rolle spielen, ob die betroffene Person aufgrund ihrer Aufgaben einen Bezug zur Presseberichterstattung hat. Der Größe einer Kommune kann allenfalls eine Indizwirkung zukommen. Zwar mag in kleineren Kommunen auch aufgrund flacher Hierarchiestrukturen und Aufgabenkonzentrationen auf wenige Personen eine relativ große Anzahl Beschäftigter eine Funktion „mit Außenwirkung" wahrnehmen. Allein die Einwohnerzahl oder die Anzahl der Beschäftigten ist für sich genommen aber kein geeignetes Differenzierungskriterium.

Gegen die bei den bayerischen Landratsämtern gängige namentliche Bezeichnung der Abteilungs-/Geschäftsbereichs- sowie Sachgebiets-/Fachbereichsleitungen mit den üblichen Kontaktdaten erhebe ich grundsätzlich keine Einwände. Dies gilt entsprechend für Gemeinden mit vergleichbarer Organisationsstruktur.

Soweit Beschäftigte die notwendige Funktion „mit Außenwirkung" wahrnehmen, haben bayerische öffentliche Stellen bei der Veröffentlichung von Kontaktdaten einen gewissen Gestaltungsspielraum. Sie können insbesondere entscheiden, ob alle zulässigen Angaben oder einzelne offengelegt werden, ob nur Kontaktdaten von Beschäftigten bestimmter Hierarchieebenen oder von allen Beschäftigten „mit Außenwirkung" veröffentlicht werden.

7.5.5 Ausnahmen aufgrund individueller Situation

Hat eine Position „Außenwirkung", so bedeutet das allerdings nicht, dass in jedem Fall dienstliche Kontaktdaten veröffentlicht werden dürfen. Die bei der Prüfung der Erforderlichkeit anzustellende Güterabwägung kann in einer konkreten Situation auch einmal dazu führen, dass das „Pendel in Richtung der Datenschutzinteressen der betroffenen Person ausschlägt". So kann etwa in realen Bedrohungsszenarien das Vertraulichkeitsinteresse der betroffenen Person das Verarbeitungsinteresse der öffentlichen Stelle überwiegen. Eine Veröffentlichung von Kontaktdaten hat dann zu unterbleiben.

7.5.6 Rechenschaftspflicht

Datenschutzrechtlich Verantwortliche sind nicht nur verpflichtet, personenbezogene Daten rechtmäßig zu verarbeiten. Sie müssen dies im Rahmen ihrer Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) auch nachweisen können. Der Veröffentlichung von Kontaktdaten hat daher immer eine Rechtmäßigkeitsprüfung vorauszugehen, deren Ergebnis zu dokumentieren ist.

7.5.7 Fazit

Dienstliche Kontaktdaten von Beschäftigten bayerischer öffentlicher Stellen sind personenbezogene Daten. Bei der Veröffentlichung gerade auch im Internet ist dafür Sorge zu tragen, dass nur die für die Kontaktaufnahme erforderlichen Daten offengelegt werden. Die sehr unterschiedliche Handhabung durch bayerische Kommunen hat Unsicherheiten und Beratungsbedarf erkennen lassen. Ich habe dies zum Anlass genommen, gemeinsam mit dem Bayerischen Staatsministerium des Innern, für Sport und Integration alle bayerischen Kommunen, vor allem Gemeinden und Landkreise, über die Rechtslage zu informieren und zu einer datenschutzgerechten Veröffentlichungstätigkeit insbesondere auf der Plattform BayernPortal anzuhalten.

7.6 Personalaktendaten in der Zeitung

Personalaktendaten sind ihrer Natur nach sensibel. Dies gilt umso mehr, wenn Gesundheitsdaten Beschäftigter betroffen sind. Aus gutem Grund werden diese Daten sowohl durch das Datenschutzrecht als auch durch das Personalaktenrecht besonders geschützt.

Eine im bayerischen öffentlichen Dienst Beschäftigte erkrankte und kündigte in der Folgezeit. Kurz vor Beendigung des Arbeitsverhältnisses fand sie in der heimischen Presse Äußerungen ihres Vorgesetzten zu ihrer mehrmonatigen Krankschreibung sowie dazu, dass sie aufgrund gesundheitlicher Probleme nicht auf ihre Stelle zurückkehren werde. Daraufhin wandte sie sich mit einer datenschutzrechtlichen Beschwerde an mich.

Mit den beschriebenen Äußerungen des Vorgesetzten der Beschwerdeführerin hat die öffentliche Stelle personenbezogene Daten der Beschwerdeführerin gegenüber der Presse offengelegt. Als Verarbeitung im Sinne von Art. 4 Nr. 2 DSGVO bedarf diese Offenlegung einer Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 DSGVO. Da sich die Äußerung auch auf den Gesundheitszustand der Beschwerdeführerin bezog und damit besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO umfasste, war zusätzlich ein Zulässigkeitstatbestand nach Art. 9 Abs. 2 DSGVO erforderlich.

Informationen des Arbeitgebers über etwaige Erkrankungen oder Kündigungsgründe von Beschäftigten stehen in einem unmittelbaren inneren Zusammenhang mit dem jeweiligen Dienst- oder Arbeitsverhältnis. Es handelt sich bei diesen Informationen demnach um Personalaktendaten im Sinne von § 50 Satz 2 Beamtenstatusgesetz, Art. 103 ff. Bayerisches Beamtengesetz (BayBG). Die Zulässigkeit von Auskünften aus der Personalakte an Dritte – wie hier an die lokale Zei-

tung – richtete sich vorliegend nach Art. 108 Abs. 4 BayBG. Die genannten Vorschriften gelten auch für vertraglich Beschäftigte im bayerischen öffentlichen Dienst grundsätzlich entsprechend (Art. 145 Abs. 2 BayBG).

Art. 108 BayBG
Übermittlung von Personalakten und Auskunft an nicht betroffene Personen
[…]
(4) [1]Auskünfte an Dritte dürfen nur mit Einwilligung des Beamten oder der Beamtin erteilt werden, es sei denn, dass die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz berechtigter, höherrangiger Interessen des Dritten die Auskunftserteilung zwingend erfordert. [2]Inhalt und Empfänger der Auskunft sind dem Beamten oder der Beamtin schriftlich mitzuteilen.
[…]

Auskünfte aus der Personalakte sind hiernach grundsätzlich nur mit Einwilligung der betroffenen Person zulässig (Art. 108 Abs. 4 Satz 1 Halbsatz 1 BayBG). Von diesem Grundsatz sieht Art. 108 Abs. 4 Satz 1 Halbsatz 2 BayBG Ausnahmen vor: Wenn und soweit die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz berechtigter, höherrangiger Interessen des Dritten die Auskunftserteilung zwingend erfordert, können Auskünfte aus der Personalakte auch ohne Einwilligung erteilt werden.

Die öffentliche Stelle hat in ihrer Stellungnahme mir gegenüber umgehend einen Datenschutzverstoß eingeräumt. Es fehlte an einer – im Beschäftigungsverhältnis ohnehin nur selten freiwillig und damit wirksam (vgl. Art. 4 Nr. 11 DSGVO) erteilten – Einwilligung der Beschwerdeführerin; zudem war für das Vorliegen des Ausnahmetatbestands gemäß Art. 108 Abs. 4 Satz 1 Halbsatz 2 BayBG nichts ersichtlich. Die Äußerungen gegenüber der lokalen Presse waren damit auch nach Auffassung der insoweit rechenschaftspflichtigen (vgl. Art. 5 Abs. 2 DSGVO) öffentlichen Stelle unrechtmäßig erfolgt.

Im Ergebnis hat die öffentliche Stelle personenbezogenen Daten – einschließlich Gesundheitsdaten – der Beschwerdeführerin ohne Rechtsgrundlage der lokalen Zeitung offengelegt und damit gegen den Grundsatz der Rechtmäßigkeit einer Verarbeitung nach Art. 5 Abs. 1 Buchst. a DSGVO, Art. 6 Abs. 1 UAbs. 1, Art. 9 Abs. 1 DSGVO verstoßen.

Aufgrund des Gewichts dieses Verstoßes und der nachteiligen Folgen für die Beschwerdeführerin habe ich das geschilderte Vorgehen der öffentlichen Stelle gemäß Art. 16 Abs. 4 Satz 1 BayDSG förmlich datenschutzrechtlich beanstandet.

7.7 Stufenvorweggewährung nur gegen „Schein-Bewerbung“?

An der Bindung qualifizierter Fachkräfte haben auch bayerische Behörden ein großes Interesse. So nimmt Wunder, dass eine bayerische öffentliche Stelle das dazu dienende Instrument der „Stufenvorweggewährung“ an die Vorlage von Arbeitsverträgen oder Arbeitsangeboten anderer Arbeitgeber knüpfen wollte. Eine solche Verwaltungspraxis kann sich nicht nur leicht als personalwirtschaftlich kontraproduktiv erweisen; sie steht auch mit den datenschutzrechtlichen Vorgaben nicht in Einklang.

7.7.1 Tarifvertragsrechtlicher Hintergrund

Tarifbeschäftigte des Freistaates Bayern erhalten ein Entgelt, dessen Höhe zunächst von der Entgeltgruppe abhängt, in welche sie eingruppiert sind (vgl. § 12 Abs. 1 Satz 2 Tarifvertrag für den öffentlichen Dienst der Länder – TV-L). Jede Entgeltgruppe umfasst in der Regel sechs Stufen mit steigender Entgelthöhe (§ 16 Abs. 1 Satz 1 TV-L). Für das Erreichen der jeweils nächsthöheren Stufe sieht § 16 Abs. 3 Satz 1 TV-L bestimmte Stufenlaufzeiten vor. Abweichend hiervon ermöglicht es § 16 Abs. 5 Satz 1 TV-L unter bestimmten Voraussetzungen, Tarifbeschäftigten ein bis zu zwei Stufen höheres Entgelt vorzeitig zu gewähren. Diese „Stufenvorweggewährung" soll unter anderem dazu dienen, qualifizierte Fachkräfte an den Arbeitgeber zu binden. In § 16 Abs. 5 Satz 1 TV-L heißt es:

„Zur regionalen Differenzierung, zur Deckung des Personalbedarfs, zur Bindung von qualifizierten Fachkräften oder zum Ausgleich höherer Lebenshaltungskosten kann Beschäftigten abweichend von der tarifvertraglichen Einstufung ein bis zu zwei Stufen höheres Entgelt ganz oder teilweise vorweg gewährt werden."

7.7.2 Sachverhalt

Eine bayerische staatliche Behörde hatte eine Stufenvorweggewährung bei einer Beschäftigten (der späteren Beschwerdeführerin) zu prüfen. Die Behörde machte der Beschwerdeführerin gegenüber wiederholt deutlich, von dieser Option nur im Falle einer „konkreten Abwanderungsgefahr" Gebrauch machen zu können. Zuvor hatte die Beschwerdeführerin Unterlagen in Form einer Dokumentation ihrer Leistungen und eines Antrags ihrer Vorgesetzten auf eine höhere Einstufung vorgelegt. Die Beschäftigungsbehörde hatte diese Unterlagen allerdings nicht als ausreichende Belege für eine konkrete Abwanderungsgefahr angesehen. Vielmehr sei eine solche mit Arbeitsangeboten anderer Arbeitgeber nachzuweisen. Zur Begründung für diese Verwaltungspraxis berief sich die Behörde auch auf Vorgaben des Bayerischen Staatsministerium der Finanzen und für Heimat.

In ihrer Stellungnahme teilte mir die Behörde mit, dass laut einem Schreiben des Finanzministeriums nur sehr restriktiv von einer Stufenvorweggewährung Gebrauch gemacht werden solle. Die Beschäftigungsbehörde zog daraus den Schluss, die Stufenvorweggewährung von einer konkreten Gefahr der Abwanderung der oder des Beschäftigten abhängig machen zu müssen. Diese Gefahr sei hinreichend zu belegen. Dabei genüge es nicht, wenn die Fachkraft Abwanderungsabsichten lediglich mündlich zum Ausdruck bringe. Die Vorlage eines konkreten Arbeitsangebots eines anderen Arbeitgebers sei jedoch auch keine zwingende Voraussetzung für eine Stufenvorweggewährung; man habe diesen Nachweis der Beschwerdeführerin gegenüber lediglich als Beispiel aufgeführt, wie eine konkrete Abwanderungsgefahr belegt werden könne. Welche alternativen Nachweismöglichkeiten sie akzeptieren würde, führte die Behörde allerdings nicht näher aus.

7.7.3 Rechtliche Würdigung

Zunächst habe ich die Beschwerdeführerin wie auch die Behörde darauf aufmerksam gemacht, dass meine Aufsichtszuständigkeit auf die Einhaltung datenschutzrechtlicher Vorschriften durch bayerische öffentliche Stellen beschränkt ist. Der personalrechtlichen Entscheidung der Behörde, ob sie von der vorgezogenen

Stufengewährung nach § 16 Abs. 5 Satz 1 TV-L im vorliegenden Fall Gebrauch macht, konnte ich nicht vorgreifen. Klar war aber auch: Datenverarbeitungen, welche die Beschäftigungsbehörde in ihrem Entscheidungsprozess durchführt, unterliegen durchaus meiner Aufsichtszuständigkeit. Aus dieser Perspektive habe ich die beschriebene Verwaltungspraxis kritisch beurteilt:

Wenn die Behörde das konkrete Arbeitsangebot eines anderen Arbeitgebers verlangt und dann Einsicht nimmt, erhebt sie personenbezogene Daten. Dafür benötigt sie eine Rechtsgrundlage. Nach Art. 103 Satz 1 Nr. 1 Bayerisches Beamtengesetz (BayBG) darf der Dienstherr personenbezogene Daten von Beschäftigten grundsätzlich nur zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere für Zwecke der Personalverwaltung oder -wirtschaft und nur im Rahmen des Erforderlichen verarbeiten. Diese Vorschrift gilt gemäß Art. 145 Abs. 2 BayBG für die bei bayerischen öffentlichen Stellen vertraglich Beschäftigten grundsätzlich entsprechend. Bei der Verarbeitung muss auch der Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) beachtet werden.

Das Verfahren zur Stufenvorweggewährung nach § 16 Abs. 5 TV-L ist ein Instrument der Personalverwaltung; eine damit zusammenhängende Verarbeitung personenbezogener Daten der Beschwerdeführerin dient daher einem in Art. 103 Satz 1 BayBG genannten Zweck. Entscheidend war die Erforderlichkeit der konkreten Verarbeitung: Insofern kam es auf die Voraussetzungen von § 16 Abs. 5 TV-L an: Erforderlich sind nur die Informationen, welche die Behörde benötigt, um die Stufenvorweggewährung verantwortlich entscheiden zu können. Die Vorschrift bietet nach meiner Auffassung keine genügenden Anhaltspunkte, dass die in ihr geregelten Vorteile von einer „konkreten Abwanderungsgefahr“ abhängig sein sollen.

Zum einen dürfte im Falle der Vorlage eines konkreten Angebots eines anderen Arbeitgebers oder gar eines unterschriftsreifen Arbeitsvertrags die berufliche Neuorientierung der jeweiligen Beschäftigten regelmäßig bereits so weit gediehen sein, dass ein Verbleib auch mithilfe einer Zulage aller Voraussicht nach nicht mehr erreicht werden kann.[141] Angesichts dessen war bereits zu bezweifeln, ob das Vorgehen der Beschäftigungsbehörde überhaupt geeignet war, Fachkräfte zu binden. Zum anderen spielen bei der Prüfung der Erforderlichkeit auch Verhältnismäßigkeitserwägungen eine Rolle.[142] In diesem Zusammenhang erschien es mir kaum vermittelbar, wenn die Beschäftigten gezwungen würden, sich „zum Schein“ bei einem anderen Arbeitgeber zu bewerben, um das Nachweisverlangen der Beschäftigungsbehörde erfüllen zu können. Auch aus diesem Grund konnte ich nicht erkennen, weshalb die mit der Anforderung entsprechender Nachweise oder Belege (insbesondere in Form von konkreten Angeboten anderer Arbeitgeber) zusammenhängende Erhebung personenbezogener Daten bei den Beschäftigten im Sinne von Art. 103 Satz 1 BayBG erforderlich sein sollte.

Zur weiteren Klärung der Rechtslage habe ich mich unmittelbar an das Finanzministerium gewandt, welches meine Rechtsauffassung bestätigte. Zwar sei in dem von der Beschäftigungsbehörde genannten Schreiben eine restriktive Handha-

[141] So auch Breier/Dassau/Kiefer/Thivessen, TV-L, Kommentar, Stand 4/2022, § 16 TV-L Erl. 95.20.

[142] Vgl. etwa Bayerisches Oberstes Landesgericht, Beschluss vom 6. August 2020. 1 VA 33/20, BeckRS 2020, 18859, Rn. 59.

bung der Stufenvorweggewährung nach § 16 Abs. 5 TV-L gefordert worden; einen zwingenden Nachweis einer konkreten Abwanderungsgefahr der oder des Beschäftigten habe man in diesem Rahmen aber zu keiner Zeit vorausgesetzt.

Die Behörde konnte mir also nicht darlegen, weshalb die im Rahmen der Stufenvorweggewährung nach § 16 Abs. 5 TV-L geforderten Nachweise fachrechtlich zwingend und die damit zusammenhängende Erhebung personenbezogener Daten im Sinne von Art. 103 Satz 1 BayBG erforderlich waren. Dies galt insbesondere auch für die an die Beschwerdeführerin gerichtete Aufforderung, eine konkrete Abwanderungsgefahr durch die Vorlage eines konkreten Arbeitsangebots eines anderen Arbeitgebers nachzuweisen. Die Behörde hatte für die Datenerhebung mithin keine Rechtsgrundlage.

Ich habe die Behörde daher aufgefordert, die bestehende, rechtswidrige Verwaltungspraxis unverzüglich zu beenden. Die Behörde hat mir zwischenzeitlich bestätigt, zukünftig bei der Anwendung von § 16 Abs. 5 TV-L auf den Nachweis einer konkreten Abwanderungsgefahr zu verzichten, soweit mit dieser Nachweisführung – was in aller Regel der Fall sein wird – eine Erhebung personenbezogener Daten einhergeht.

7.8 „Störfälle“ beim JobBike Bayern

Im Gegensatz zu vernetzten Autos, die nicht immer völlig transparent personenbezogene Daten verarbeiten, ist das klassische Fahrrad aus Datenschutzsicht zunächst „unverdächtig“. Möchte ein Dienstherr oder öffentlicher Arbeitgeber seinen Beschäftigten allerdings ein Dienstfahrrad- oder JobBike-Leasing anbieten, sind bei dessen Ausgestaltung auch datenschutzrechtliche Aspekte zu beachten: Schließlich müssen zur Durchführung eines solchen Angebots Beschäftigtendaten verarbeitet werden – je nach Ausgestaltung unter Beteiligung mehrerer – öffentlicher wie auch nicht öffentlicher – Stellen. Das „JobBike Bayern“ zeigt, dass sich dabei genaues Hinsehen lohnt: Manches Mal versteckt sich das potentielle Datenschutzproblem nämlich im Detail.

7.8.1 „JobBike Bayern“

Über „JobBike Bayern“ können insbesondere Beschäftigte des Freistaates Bayern Fahrräder beziehen. Das Angebot ist für die Beschäftigten freiwillig; als Vorteile werden vor allem eine Ratenzahlung durch „Entgeltumwandlung“ sowie diverse Zusatzleistungen („Rundum-Sorglos-Paket“) beworben.[143] Zur Umsetzung von „JobBike Bayern“ wurde eine Rahmenvereinbarung mit einem Dienstleister und einem Leasinggeber geschlossen.

Im Wesentlichen läuft ein Fahrradbezug über „JobBike Bayern“ wie folgt ab: Beschäftigte erhalten über das Online-Portal „Mitarbeiterservice Bayern“ Zugang zu „JobBike Bayern“. Unter Einbindung der Onlineplattform des Dienstleisters suchen sie sich ein passendes Fahrrad online oder beim örtlichen Händler aus. Der Dienstherr oder Arbeitgeber schließt daraufhin Einzelleasingverträge mit einem Leasinggeber über die ausgewählten Fahrräder ab und entrichtet die vorgesehenen Leasingraten an diesen. Die Fahrräder werden den Beschäftigten durch Kooperationspartner des Dienstleisters bereitgestellt. Grundlage hierfür ist ein

[143] Vgl. zu Einzelheiten die „FAQ“ auf der Website https://jobbike-bayern.deutsche-dienstrad.de/.

„Überlassungs- und Entgeltumwandlungsvertrag“ zwischen den Beschäftigten und ihren Dienstherren oder Arbeitgebern.[144] Dieser sieht vor, dass die Leasingraten für ein JobBike im Wege einer sogenannten „Entgeltumwandlung“ finanziert werden: Das monatliche Gehalt der Beschäftigten wird um die Leasingrate für das gewählte Fahrrad verringert und in einen Anspruch auf Nutzung des JobBikes umgewandelt (für Beamtinnen und Beamten ist diese Möglichkeit in Art. 3 Abs. 3 Satz 1 Bayerisches Besoldungsgesetz vorgesehen).[145]

Auch wenn Beschäftigte, die ein Fahrrad über „JobBike Bayern“ beziehen, hiervon im Regelfall nichts mitbekommen werden, zeigt diese Darstellung bereits: Das vertragsrechtliche Fundament von „JobBike Bayern“ ist komplex und ohne die Verarbeitung von Beschäftigtendaten nicht umsetzbar. In datenschutzrechtlicher Hinsicht sind an dem Verfahren mehrere öffentliche sowie nicht öffentliche Stellen beteiligt: Das Bayerische Staatsministerium für Wohnen, Bau und Verkehr, welches die Beschäftigungsgeber vertritt, das Landesamt für Finanzen als staatliche Bezügestelle sowie als nicht öffentliche Stellen Dienstleister und Leasinggeber. Die beteiligten Stellen nahmen dabei nachvollziehbar an, Beschäftigtendaten im Rahmen von „JobBike Bayern“ als gemeinsam Verantwortliche im Sinne von Art. 26 DSGVO zu verarbeiten.[146]

7.8.2 Der „Störfall“ als Datenschutzproblem?

Vor Einführung von „JobBike Bayern“ wurde der Landesbeauftragte – wie in § 7 Abs. 4 Satz 1 Geschäftsordnung der Bayerischen Staatsregierung vorgesehen – beteiligt; leider geschah dies sehr kurzfristig. Gleichwohl ließen die vorgelegten, recht umfangreichen Unterlagen aber erkennen, dass der Datenschutz bei der Ausgestaltung von „JobBike Bayern“ grundsätzlich mitbedacht worden ist. Soweit es die auf bayerische öffentliche Stellen beschränkte Aufsichtszuständigkeit betrifft, stellte sich allerdings das vorgesehene „Störfallmanagement“ als problematisch dar.

„Störfälle“ bezeichnen in diesem Zusammenhang Konstellationen, in denen nach Abschluss eines Überlassungs- und Entgeltumwandlungsvertrags umwandlungsfähige Bezüge fortfallen und der vorgesehenen ratenweisen Zahlung des „JobBikes“ in der Folge die Grundlage entzogen wird. Die Gründe für solche Störfälle sind vielfältig; erfasst sind beispielhaft Elternzeiten und Beurlaubungen ohne Bezüge, eine dauerhaft Dienst-, Erwerbs- oder Arbeitsunfähigkeit oder eine außerplanmäßige Beendigung des Beschäftigungsverhältnisses.[147] Die beteiligten Stellen haben für diese Fälle vereinbart, den Dienstherrn und Arbeitgeber als Leasingnehmer von wirtschaftlichen Nachteilen freizustellen. Hierfür hat der Leasinggeber ein „Störfallmanagement“ vorzuhalten, in dessen Rahmen er zusammen mit dem Dienstleister gegebenenfalls auch die weitere Abwicklung des Störfalles (Beendigung des Fahrradleasings oder anderweitige Finanzierung) mit den betroffenen Beschäftigten klärt. Für bestimmte vorübergehende Störfälle besteht dabei ein Versicherungsschutz zugunsten der Beschäftigten.

144 Dieser ist der BayJobBikeBekanntmachung (BayJBBek) vom 26. Januar 2024 (BayMBl Nr. 103) als Anlage beigefügt.

145 Vgl. zu Einzelheiten auch Nr. 6 und Nr. 72 der BayJobBikeBekanntmachung (Fn. 144).

146 Vgl. hierzu Nr. 17.1 des Überlassungs- und Entgeltumwandlungsvertrags (Fn. 144).

147 Siehe zu Einzelheiten auch Nr. 10 der BayJobBikeBekanntmachung (Fn. 144).

Zur Durchführung des Störfallmanagements hatten die Beteiligten zunächst vorgesehen, dass der Dienstherr oder Arbeitgeber eingetretene Störfälle personenbezogen unter Angabe des Störfallgrundes an den Dienstleister meldet. Eine solche Datenweitergabe bedarf auch dann einer hinreichenden Rechtsgrundlage, wenn sie zwischen gemeinsam Verantwortlichen stattfindet.[148] Nachdem die betroffenen Beschäftigten selbst Vertragspartei der jeweiligen Überlassungs- und Entgeltumwandlungsverträge sind, kann ihr Dienstherr oder Arbeitgeber die zur Vertragsdurchführung erforderliche Verarbeitung von Beschäftigtendaten grundsätzlich auf Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO stützen. Diese Vorschrift erlaubt dem Verantwortlichen die Verarbeitung personenbezogener Daten, soweit dies zur Erfüllung eines Vertrags mit der betroffenen Person erforderlich ist.

Bei der vorgesehenen Angabe des spezifischen Störfallgrundes ergaben sich jedoch Probleme: Zunächst wird dabei nämlich die rechtliche Fundierung für einen zeitweisen oder dauerhaften Bezügefortfall offenbar. Regelmäßig geht es um Informationen, die in einem unmittelbaren inneren Zusammenhang mit dem Dienstverhältnis stehen, und damit um Personalaktendaten im Sinne von § 50 Satz 2 Beamtenstatusgesetz, Art. 103 ff. Bayerisches Beamtengesetz (BayBG); diese Vorschriften finden nach Art. 145 Abs. 2 BayBG auch auf vertraglich im bayerischen öffentlichen Dienst Beschäftigte grundsätzlich Anwendung. Ohne die Einwilligung der betroffenen Beschäftigten sind Auskünfte über Personalaktendaten jedoch nur in eng begrenzten Fällen (vgl. etwa Art. 108 Abs. 5 Satz 1 Nr. 1 in Verbindung mit Abs. 2 BayBG) zulässig.

Hinzu kommt, dass der Dienstherr oder Arbeitgeber zumindest in Einzelfällen (insbesondere bei einer Arbeits- oder Erwerbsunfähigkeit Beschäftigter) Gesundheitsdaten und damit besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO an den Dienstleister übermittelt. Hierfür bedarf es neben einer Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO zusätzlich eines Zulässigkeitstatbestands nach Art. 9 Abs. 2 DSGVO. Im Unterschied zu Art. 6 Abs. 1 DSGVO sind Datenverarbeitungen zur Vertragserfüllung in Art. 9 Abs. 2 DSGVO nicht als allgemeiner Tatbestand erfasst.

Da die mir vorliegenden Unterlagen zunächst keine Ausführungen zu den Rechtsgrundlagen für die geschilderte Datenweitergabe enthielten, habe ich das Bauministerium insoweit um zusätzliche Ausführungen gebeten. Zugleich habe ich um kritische Prüfung ersucht, ob das Störfallmanagement nicht auch anders und angesichts des Grundsatzes der Datenminimierung nach Art. 5 Abs. 1 Buchst. c DSGVO insbesondere datensparsamer abgewickelt werden könnte.

Das Bauministerium hat mir im Folgenden ausführlich dargelegt, weshalb es einer Meldung von „Störfällen“ an den Dienstleister bedarf; anders sei die hiermit bezweckte finanzielle Schadloshaltung des Dienstherrn und Arbeitgebers sowie die Haushaltsneutralität von „JobBike Bayern“ nicht umsetzbar.

Als Rechtsgrundlage für die vorgesehenen Datenübermittlungen hat es zunächst Einwilligungen der Beschäftigten nach Art. 6 Abs. 1 UAbs. 1 Buchst. a und Art. 9 Abs. 2 Buchst. a DSGVO in Betracht gezogen. Im Beschäftigungsverhältnis ist die Einwilligung als Rechtsgrundlage für Datenverarbeitungen zwar grundsätzlich problematisch; aufgrund des strukturellen Machtungleichgewichts zwischen dem Dienstherrn oder Arbeitgeber sowie den Beschäftigten fehlt es solchen Erklärun-

[148] Vgl. ausführlich hierzu Lang, in: Taeger/Gabel, 4. Aufl. 2022, Art. 26 DSGVO Rn. 112 f.

gen nämlich regelmäßig an der nach Art. 4 Nr. 11 DSGVO erforderlichen Freiwilligkeit. Da es sich bei „JobBike Bayern“ allerdings um ein Zusatzangebot handelt, auf welches die Beschäftigten ohne weitere Nachteile verzichten können, erschienen wirksame Einwilligungen möglich. Es stellte sich allerdings schnell heraus, dass die Einwilligung aufgrund ihrer freien Widerruflichkeit (vgl. Art. 7 Abs. 3 Satz 1 DSGVO) gegebenenfalls Folgeprobleme für die vertragliche Abwicklung nach Eintritt des Störfalls mit sich gebracht hätte.

Meiner Empfehlung entsprechend hat das Bauministerium daraufhin die vorgesehene Abwicklung des Störfallmanagements noch einmal kritisch überdacht. Ausgangspunkt war dabei die Erwägung, dass die Störfälle verschiedenen Kategorien zugeordnet werden können, die vertraglich jeweils unterschiedlich behandelt werden. In der Folge haben sich die Beteiligten darauf verständigt, dem Dienstleister lediglich das Vorliegen und die Dauer eines Störfalls sowie dessen vertragliche Auswirkungen mitzuteilen, ohne dabei den Grund des Störfalls offenzulegen. Die Mitteilung enthält damit regelmäßig weder Personalaktendaten noch besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO. Im Ergebnis ist das Störfallmanagement nunmehr deutlich datensparsamer ausgestaltet worden; im Wesentlichen lässt es sich auf Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO als Rechtsgrundlage stützen.

In Einzelfällen kann eine solche Meldung den jeweiligen Störfallgrund gleichwohl mittelbar offenlegen, etwa dann, wenn eine Störfallkategorie so eng gefasst ist, dass bei Kenntnis der einschlägigen vertraglichen Regelungen der vorliegende Störfallgrund zweifelsfrei zuordenbar ist. Das Bauministerium und das Landesamt für Finanzen haben mir ausführlich dargelegt, weshalb in diesen Fällen Art. 108 Abs. 5 Satz 1 Nr. 1 in Verbindung mit Abs. 2 Nr. 2 BayBG als Rechtsgrundlage für eine mittelbare Offenlegung von Personalaktendaten herangezogen werden kann. Diese Vorschriften erlauben Auskünfte über Personalaktendaten, soweit dies zur Festsetzung, Berechnung und Rückforderung der Bezüge erforderlich ist.

Die diesbezügliche Argumentation lässt sich wie folgt zusammenfassen: Da Störfälle der Entgeltumwandlung die Grundlage entziehen, haben sie Auswirkungen auf die Bezügeberechnung und -festsetzung. Sie müssen daher, auch im Hinblick auf einen etwaigen Versicherungsschutz, ordnungsgemäß mit dem Dienstleister abgewickelt werden, was die vorherige Information über den Störfall, dessen Dauer und vertragliche Auswirkungen notwendig macht. Wenn und soweit eine solche, inhaltlich bereits reduzierte Mitteilung in Einzelfällen den Störfallgrund mittelbar erkennen lässt, wäre dies als erforderlich im Sinne von Art. 108 Abs. 5 Satz 1 Nr. 1 in Verbindung mit Abs. 2 Nr. 2 BayBG anzusehen. In diesem Rahmen sei auch eine Offenlegung von Gesundheitsdaten im Einzelfall zulässig, Art. 108 Abs. 5 Satz 1 Nr. 1, Abs. 2 Nr. 2 BayBG in Verbindung mit Art. 8 Abs. 1 Satz 1 Nr. 2 DSGVO. Diese Begründung konnte ich im Ergebnis nachvollziehen.

Vor Abschluss von Überlassungs- und Entgeltumwandlungsverträgen werden die Beschäftigten über die mögliche Verarbeitung ihrer personenbezogenen Daten ausführlich informiert.[149]

[149] Siehe hierzu auch Nr. 17.4 des Überlassungs- und Entgeltumwandlungsvertrags (Fn. 144).

7.8.3 Fazit

„JobBike Bayern“ ist ein Zusatzangebot für Beschäftigte des Freistaates Bayern. Im Rahmen dieses Angebots muss der Dienstherr oder Arbeitgeber gleichwohl personenbezogene Daten seiner Beschäftigten verarbeiten. Wie in anderen Fällen auch, ist dabei insbesondere zu prüfen, inwieweit die Verarbeitung personenbezogener Daten zur Erreichung eines festgelegten Zwecks auch tatsächlich erforderlich ist. Soweit vorhanden, sind datensparsamere Alternativen auf ihre Umsetzbarkeit hin zu untersuchen. Es freut mich, dass meine Beratung zu einer datensparsameren Ausgestaltung des Störfallmanagements bei „JobBike Bayern“ geführt hat. Allen Beschäftigten, die sich für den Bezug eines JobBikes entscheiden, wünsche ich eine allzeit gute und – nicht nur aus Datenschutzsicht – störfallfreie Fahrt.

7.9 Änderungen im bayerischen Personalvertretungsrecht

Neben dem bayerischen Dienstrecht (vgl. hierzu den Beitrag Nr. 7.2) ist im Berichtszeitraum auch das bayerische Personalvertretungsrecht geändert worden. Aus datenschutzrechtlicher Sicht war dabei insbesondere Folgendes von Bedeutung:

7.9.1 Mitbestimmungsrecht bei der Benennung und Abberufung von behördlichen Datenschutzbeauftragten

Der Personalrat einer bayerischen öffentlichen Stelle ist meiner Auffassung nach nicht als eigenständiger Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO anzusehen. Vielmehr bleibt die jeweilige bayerische öffentliche Stelle auch für die Verarbeitung personenbezogener Daten „ihres“ Personalrats datenschutzrechtlich verantwortlich. Die Beratungs- und Überwachungsaufgaben von behördlichen Datenschutzbeauftragten (vgl. insbesondere Art. 39 Abs. 1 Buchst. a und b DSGVO) bestehen damit auch gegenüber dem Personalrat als Teil des Verantwortlichen. Bei der Erfüllung seiner Aufgaben hat der behördliche Datenschutzbeauftragte der besonderen Stellung des Personalrats jedoch weitestmöglich Rechnung zu tragen.[150] Im Beschäftigungskontext bestehen datenschutzrechtliche Vorgaben zudem grundsätzlich zugunsten der Beschäftigten. Der Personalrat hat daher unter anderem dafür zu sorgen, dass diese Vorgaben umgesetzt werden (vgl. Art. 69 Abs. 1 Buchst. b Bayerisches Personalvertretungsgesetz – BayPVG).

Die Arbeit von Personalräten und behördlichen Datenschutzbeauftragten hat somit einige Berührungspunkte. Zugleich ist ein gewisses „Reibungspotential“ nicht zu verkennen: Schließlich ist es grundsätzlich Sache des Verantwortlichen und damit der Dienststellenleitungen, die behördlichen Datenschutzbeauftragten zu benennen.[151] Zwar sieht die Datenschutz-Grundverordnung ausdrücklich vor, dass Datenschutzbeauftragte weisungsfrei tätig und auch gegenüber dem Verantwortlichen zur Verschwiegenheit verpflichtet sind (Art. 38 Abs. 3 Satz 1, Abs. 5

[150] Vgl. ausführlich zum Ganzen Bayerischer Landesbeauftragter für den Datenschutz, Der Personalrat – Verantwortlicher im Sinne des Datenschutzrechts?, Aktuelle Kurz-Information 23, Stand 7/2019, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018“.

[151] Im staatlichen Bereich können behördliche Datenschutzbeauftragte gegebenenfalls durch eine höhere Behörde benannt werden, Art. 12 Abs. 3 BayDSG.

DSGVO). Gleichwohl ist nicht auszuschließen, dass die Wahrnehmung der Überwachungsaufgaben von behördlichen Datenschutzbeauftragten aus Sicht von Personalräten im Einzelfall einmal als „übergriffig“ aufgefasst wird.

Nicht zuletzt vor diesem Hintergrund habe ich anlässlich meiner Beteiligung in zurückliegenden Gesetzgebungsverfahren mehrfach angeregt, ein umfassendes Mitbestimmungsrecht für Personalräte bei der Benennung und Abberufung von behördlichen Datenschutzbeauftragten gesetzlich vorzusehen. Ein solches Mitbestimmungsrecht würde zudem die gesetzlich vorgeschriebene Weisungsfreiheit von Datenschutzbeauftragten untermauern. Insbesondere würde es dem Eindruck entgegenwirken, die im Gegensatz zum Personalrat nicht von den Beschäftigten gewählten, sondern allein von den Dienststellenleitungen benannten behördlichen Datenschutzbeauftragten stünden – trotz Verschwiegenheitspflicht und Weisungsfreiheit – „im Lager“ der Dienststellenleitungen. Schließlich dürfte ein solches Mitbestimmungsrecht auch bei den Personalräten die Akzeptanz gegenüber Maßnahmen fördern, die behördliche Datenschutzbeauftragte in Ausübung ihrer Überwachungsaufgaben (vgl. Art. 39 Abs. 1 Buchst. b DSGVO) treffen.

Erfreulicherweise hat der bayerische Gesetzgeber diese Anregung nun aufgegriffen und mit dem Gesetz zur Änderung des Bayerischen Personalvertretungsgesetzes und weiterer Rechtsvorschriften[152] in Art. 75 Abs. 4 Satz 1 Nr. 7 BayPVG ein solches Mitbestimmungsrecht verankert.

7.9.2 Digitalisierung der Arbeit von Personalvertretungen und Wahlvorständen

In Anbetracht von Erfahrungen aus der COVID19-Pandemie war es ein erklärtes Ziel des bayerischen Gesetzgebers, den Personalvertretungen die Nutzung von Video- und Telefonkonferenzen dauerhaft rechtssicher zu ermöglichen.[153] Mit dem Gesetz zur Änderung des Bayerischen Personalvertretungsgesetzes und weiterer Rechtsvorschriften[154] ist dieses Vorhaben nunmehr umgesetzt worden: Insbesondere können nun Sitzungen und Sprechstunden des Personalrats (vgl. Art. 35 Abs. 2 Satz 2, Art. 43 Abs. 1 Sätze 3 und 4 BayPVG) sowie Verhandlungen und Beschlussfassungen der Einigungsstelle (Art. 71 Abs. 2 Sätze 4 bis 6 BayPVG) vollständig oder teilweise (unter Zuschaltung einzelner Beteiligter) mittels Video- oder Telefonkonferenz durchgeführt werden. Ferner können Personalversammlungen im Einvernehmen mit der Dienststellenleitung ganz oder teilweise mittels Videokonferenz abgehalten werden (Art. 48 Abs. 3 BayPVG).

Dabei sind natürlich auch datenschutzrechtliche Vorgaben zu beachten. Das Bayerische Personalvertretungsgesetz sieht insoweit vor, dass

— vorhandene Einrichtungen genutzt werden, die von der Dienststelle zur dienstlichen Nutzung vorgesehen sind,

— geeignete organisatorische Maßnahmen getroffen werden, um sicherzustellen, dass Dritte vom Inhalt der jeweiligen Veranstaltung keine Kenntnis nehmen können sowie

[152] Vom 7. Juli 2023 (GVBl S. 318).
[153] Vgl. Landtags-Drucksache 18/28503, S. 12.
[154] Siehe Fn. 152.

— eine Aufzeichnung der jeweiligen Veranstaltung unzulässig ist.

Für Personalratssitzungen ergeben sich diese Anforderungen unmittelbar aus Art. 35 Abs. 2 Satz 2 Nr. 1 und 3, Satz 3 BayPVG; in den anderen genannten Bereichen gelten sie entsprechend (Art. 43 Abs. 1 Satz 4, Art. 48 Abs. 3 Satz 2, Art. 71 Abs. 2 Satz 4 BayPVG). Im Hinblick auf Sitzungen des Personalrats und der Einigungsstelle bestehen gegen eine Durchführung mittels Telefon- und Videokonferenzen (teils qualifizierte) Widerspruchsmöglichkeiten (Art. 35 Abs. 2 Satz 2 Nr. 2, Art. 71 Abs. 2 Satz 5 BayPVG).

Bei Wahlen nach dem Bayerischen Personalvertretungsgesetz besteht nun ebenfalls dauerhaft die Möglichkeit, nichtöffentliche Sitzungen des Wahlvorstands per Videokonferenz abzuhalten. Eine entsprechende Änderung der Wahlordnung zum Bayerischen Personalvertretungsgesetz (WO-BayPVG), insbesondere von § 1 Abs. 2 WO-BayPVG ist mit der Verordnung zur Änderung der Wahlordnung zum Bayerischen Personalvertretungsgesetz[155] erfolgt. Die dabei zu beachtenden datenschutzrechtlichen Vorgaben wurden denjenigen in Art. 35 Abs. 2 BayPVG nachgebildet.

7.9.3 Fazit

Bayerische Personalräte können nun bei der Benennung und Abberufung von behördlichen Datenschutzbeauftragten mitbestimmen. Es freut mich sehr, dass der bayerische Gesetzgeber meine diesbezügliche Anregung aufgegriffen hat. Gerade angesichts der europarechtlich vorgegebenen umfassenden Beratungs- und Überwachungsaufgaben von Datenschutzbeauftragten einerseits und der personalvertretungsrechtlich vorgesehenen „eigenständigen" Stellung von Personalräten andererseits dürfte diese Neuregelung zu einer erheblich gesteigerten innerbehördlichen „Akzeptanz" benannter Datenschutzbeauftragter und damit zu einer datenschutzrechtlichen Verbesserung bei bayerischen öffentlichen Stellen beitragen.

Die gesetzlichen Vorgaben zur Durchführung von Video- und Telefonkonferenzen bei Personalvertretungen und Wahlvorständen sind aus Gründen der Rechtssicherheit und Rechtsklarheit zu begrüßen. Die allgemeinen technischen und organisatorischen Vorgaben der Datenschutz-Grundverordnung (etwa nach Art. 24 und 32 DSGVO) bleiben hiervon unberührt. In der Praxis wird insbesondere darauf zu achten sein, dass Personalvertretungen und Wahlvorstände im Rahmen der eröffneten Gestaltungsspielräume ausschließlich datenschutzkonforme Verfahren und Systeme einsetzen.

7.10 Datenschutzrechtliche Aufsichtszuständigkeit für Richterräte

In bayerischen öffentlichen Stellen sind grundsätzlich Personalvertretungen – insbesondere Personalräte – zu bilden (Art. 1 Bayerisches Personalvertretungsgesetz – BayPVG). Richterinnen und Richter zählen gemäß Art. 4 Abs. 1 Satz 2 BayPVG nicht zu den Beschäftigten im Sinne des Bayerischen Personalvertretungsrechts. Für diese Berufsgruppe sieht das Bayerische Richter- und Staatsanwaltsgesetz (BayRiStAG) die Errichtung sogenannter Richterräte vor (Art. 17

[155] Vom 18. Juli 2023 (GVBl. S. 470).

Abs. 1 Nr. 1 BayRiStAG). Für diese gelten die Vorschriften des Bayerischen Personalvertretungsrechts grundsätzlich entsprechend, soweit sich aus dem Bayerischen Richter- und Staatsanwaltsgesetz nichts Abweichendes ergibt (Art. 17 Abs. 4 Satz 1 BayRiStAG). Abweichungen bestehen etwa im Hinblick auf die Mitbestimmungs- und Mitwirkungsrechte von Richterräten (vgl. Art. 28 f. BayRiStAG).

Auch Richterräte verarbeiten in Erfüllung ihrer Aufgaben personenbezogene Daten. In diesem Zusammenhang bin ich gefragt worden, ob sich meine Aufsichtszuständigkeit auf Richterräte erstreckt. Diese Anfrage hatte den folgenden rechtlichen Hintergrund:

Die Datenschutz-Grundverordnung verpflichtet Mitgliedstaaten dazu, unabhängige Aufsichtsbehörden einzurichten (Art. 51 ff. DSGVO). Deren Aufgabe ist es insbesondere, die Einhaltung des Datenschutzrechts in ihrem jeweiligen Zuständigkeitsbereich zu überwachen (Art. 51 Abs. 1, Art. 57 Abs. 1 Buchst. a DSGVO). Hierfür verfügen die Aufsichtsbehörden über verschiedene Untersuchungs- und Abhilfebefugnisse; letztere umfassen auch Anweisungsmöglichkeiten (vgl. Art. 58 Abs. 2 Buchst. c bis e DSGVO).

Unabhängig sind jedoch nicht nur die Aufsichtsbehörden, sondern auch die Gerichte (vgl. Art. 47 Abs. 2 Satz 1 Charta der Grundrechte der Europäischen Union) sowie die Richterinnen und Richter (Art. 97 Grundgesetz – GG), die im Rahmen ihrer rechtsprechenden Tätigkeit eine Vielzahl personenbezogener Daten verarbeiten. Auch für diese Verarbeitungen gilt – mit Ausnahme der „Strafjustiz“ (vgl. Art. 2 Abs. 2 Buchst. d DSGVO) – die Datenschutz-Grundverordnung.[156] Eine Datenschutzaufsicht „von außen“ auch im justiziellen Bereich könnte allerdings die grundgesetzlich garantierte richterliche Unabhängigkeit gefährden; schließlich müssten sich Richterinnen und Richter dann gegebenenfalls mit aufsichtlichen Abhilfebefugnissen und insbesondere Anweisungen auseinandersetzen, die ihre Entscheidungsfindung beeinflussen könnten. Dieses Konfliktpotential hat der Verordnungsgeber erkannt und die Zuständigkeit der Aufsichtsbehörden insoweit durch Art. 55 Abs. 3 DSGVO begrenzt:[157]

„Die Aufsichtsbehörden sind nicht zuständig für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen.“

Für bayerische öffentliche Stellen bin grundsätzlich ich die zuständige Aufsichtsbehörde (Art. 15 Abs. 1 Satz 1 BayDSG). Im Hinblick auf Gerichte gilt dies gemäß Art. 1 Abs. 1 Satz 3 BayDSG jedoch nur, soweit diese in Verwaltungsangelegenheiten tätig werden. Diese Vorschrift bestand bereits vor Inkrafttreten der Datenschutz-Grundverordnung (vgl. Art. 2 Abs. 5 BayDSG a. F.); sie ist gerade auch in Ansehung von Art. 55 Abs. 3 DSGVO beibehalten worden.[158] „Verwaltungsangelegenheiten“ im Sinne von Art. 1 Abs. 1 Satz 3 BayDSG erfassen vor diesem Hintergrund gerichtliche Datenverarbeitungen nur, aber immerhin, soweit sie außerhalb der justiziellen, also rechtsprechenden Tätigkeit der Gerichte erfolgen.

Damit stellt sich die Frage, ob Verarbeitungen personenbezogener Daten durch Richterräte den Verwaltungsangelegenheiten, also dem nicht-justiziellen Bereich

[156] Vgl. nur EG 20 Satz 1 DSGVO sowie Europäischer Gerichtshof, Urteil vom 2. März 2023, C-268/21, Rn. 26.

[157] Vgl. hierzu auch Europäischer Gerichtshof, Urteil vom 24. März 2022, C-245/20, Rn. 29 ff.

[158] Landtags-Drucksache 17/19628, S. 31.

zuzuordnen sind. Bezweifeln ließe sich dies angesichts der Rechtsprechung des Europäischen Gerichtshofes, der die „justizielle Tätigkeit“ im Sinne des Art. 55 Abs. 3 DSGVO grundsätzlich weit auslegt: Im Ergebnis sieht der Gerichtshof alle Verarbeitungen von der Ausnahmevorschrift des Art. 55 Abs. 3 DSGVO erfasst, deren Kontrolle durch eine Aufsichtsbehörde nach Art. 51 DSGVO „mittelbar oder unmittelbar die Unabhängigkeit der Mitglieder oder der Entscheidungen der Gerichte beeinflussen könnte.“ [159] Zur Tätigkeit von Personalvertretungen bei Gerichten oder zur gerichtlichen Personalverwaltung insgesamt hat sich der Gerichtshof allerdings nicht geäußert.

Vor diesem Hintergrund bin ich unverändert und übereinstimmend mit der Kommentarliteratur der Auffassung, dass die Tätigkeit eines Gerichts als personalverwaltende Stelle grundsätzlich den Verwaltungsangelegenheiten im Sinne von Art. 1 Abs. 1 Satz 3 BayDSG zuzuordnen ist.[160] Auch damit zusammenhängende Datenverarbeitungen durch Richterräte sehe ich demnach von den Verwaltungsangelegenheiten nach Art. 1 Abs. 1 Satz 3 BayDSG als erfasst an. Dabei gehe ich davon aus, dass die Besonderheiten, die sich aufgrund der richterlichen Unabhängigkeit für die Tätigkeit der Richterräte im Vergleich etwa zu Personalräten ergeben, bereits in Art. 17 ff. BayRiStAG hinreichend berücksichtigt worden sind.

Im Ergebnis bin ich damit grundsätzlich auch für die datenschutzrechtliche Aufsicht über Richterräte zuständig.

[159] Europäischer Gerichtshof, Urteil vom 24. März 2022, C-245/20 Rn. 34.

[160] Vgl. Engelbrecht, in: Schröder, Bayerisches Datenschutzgesetz, Art. 1 Rn. 85; Niese, in: Wilde/Ehmann/Niese/Knoblauch, Datenschutz in Bayern, Stand 4/2023, Art. 1 BayDSG Rn. 34 f.

8 Schulen, Hochschulen, Kultur

8.1 Beratung bei der Änderung schulrechtlicher Vorschriften

Das Bayerische Gesetz über das Erziehungs- und Unterrichtswesen, das Bayerische Schulfinanzierungsgesetz sowie die Bayerische Schulordnung wurden im Jahr 2023 teils mehrfach geändert; betroffen waren auch datenschutzrelevante Vorschriften. Hierzu habe ich das Bayerische Staatsministerium für Unterricht und Kultus jeweils eingehend beraten.

8.1.1 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen

Gemäß § 31a Drittes Buch Sozialgesetzbuch – Arbeitsförderung – (SGB III) **hat die Agentur für Arbeit junge Menschen**, die nach ihrer Kenntnis bei Beendigung der Schule oder einer vergleichbaren Ersatzmaßnahme keine konkrete berufliche Anschlussperspektive haben, zu kontaktieren und **über Angebote der Berufsberatung und Berufsorientierung zu informieren**, soweit diese noch nicht genutzt werden. Zu diesem Zweck erhebt die Agentur für Arbeit bestimmte Daten wie Name, Wohnanschrift und erreichter Abschluss, soweit sie ihr von den Ländern übermittelt werden. § 31a SGB III trat zum 1. Juli 2020 in Kraft. Für die Übermittlung dieser Daten durch die Schulen bedurfte es ergänzend landesrechtlicher Regelungen. Diese wurden mit Wirkung zum 1. August 2023 erlassen.[161]

Das Kultusministerium hatte mich frühzeitig um Beratung zu den in Aussicht genommenen Regelungen gebeten. So konnte ich erhebliche datenschutzrechtliche Verbesserungen erreichen, die im ursprünglichen Regelungsentwurf nicht vorgesehen waren:

— Art. 85 Abs. 2 Satz 5 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG) enthält nun ein **voraussetzungsloses Widerspruchsrecht** der oder des Betroffenen bereits im Hinblick auf eine Datenübermittlung der Schule an die Agentur für Arbeit. Ursprünglich war nur ein Hinweis auf das Widerspruchsrecht nach Art. 21 DSGVO vorgesehen. Dieses Widerspruchsrecht gilt zum einen ohnehin, zum anderen räumt es nicht die in § 31a Abs. 2 Satz 4 SGB III geregelte voraussetzungslose Widerspruchsmöglichkeit an der „Datenquelle“ ein. Der Eingriff in das informationelle Selbstbestimmungsrecht von Schülerinnen und Schülern wäre nicht so umfassend abgefedert, wenn Daten erst an die Agentur für Arbeit übermittelt würden und ein voraussetzungsloses Widerspruchsrecht erst dort zugebilligt würde.

— Die Betroffenen müssen zudem gemäß Art. 85 Abs. 2 Satz 6 BayEUG auf ihr Widerspruchsrecht nach Art. 85 Abs. 2 Satz 5 BayEUG **hingewiesen werden.** Ein Widerspruchsrecht kann nämlich nur ausgeübt werden, wenn die berechtigten Personen davon auch Kenntnis haben.

[161] Gesetz zur Änderung des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen und des Gesetzes zur Ausführung der Sozialgesetze vom 24. Juli 2023 (GVBl. S. 443).

8.1.2 Bayerisches Schulfinanzierungsgesetz

Auf meine Initiative hin hat der Gesetzgeber Lücken beim Datenschutz durch Änderungen im Bayerischen Schulfinanzierungsgesetz geschlossen.

Schon vor dem Berichtszeitraum hatte ich auf einen Impuls aus der Schulpraxis hin das Kultusministerium auf erforderliche Änderungen betreffend die Schnittstelle des Datenaustauschs von Schulen, kommunalen Aufwandsträgern und Ausländerbehörden im Zusammenhang mit dem Kostenersatz für Gastschüler hingewiesen sowie auf Abhilfe gedrängt.

Kommunale Aufwandsträger erhalten vom Freistaat Bayern für die Beschulung von Gastschülerinnen und Gastschülern einen Gastschulbeitrag beziehungsweise Kostenersatz, bei den meisten Schularten in Form von Pauschalen. Als Gastschülerinnen und Gastschüler gelten unter anderem auch Schülerinnen und Schüler, die eine Aufenthaltsgestattung nach dem Asylgesetz besitzen, soweit sie nicht in einem Berufsausbildungsverhältnis oder einem Beschäftigungsverhältnis stehen. Der Gastschulbeitrag beziehungsweise der Kostenersatz weist nicht nur je nach Schulart eine unterschiedliche Höhe auf, sondern ist in der hier relevanten Fallgruppe an einen bestimmten ausländerrechtlichen Aufenthaltsstatus der einzelnen Schülerin oder des einzelnen Schülers gebunden. Für die kommunalen Aufwandsträger stehen dabei teilweise erhebliche Summen im Raum.

Die insofern relevanten Datenumgänge stellten sich folgendermaßen dar: Um die Gastschulbeiträge zu erhalten, mussten die Aufwandsträger nach Schulart getrennt die fraglichen Personen mit **Angabe des jeweiligen ausländerrechtlichen Status per Formblatt melden**. Auf diesem Formblatt mussten die Ausländerbehörden den jeweiligen ausländerrechtlichen Status bestätigen.

Um die in Betracht kommenden Personen zu ermitteln, bat der Aufwandsträger die Schulen, eine **Liste** der Schülerinnen und Schüler **ohne EU-Staatsangehörigkeit** zu übersenden. Diese Liste reichte der Aufwandsträger dann an die zuständige Ausländerbehörde weiter, damit dort der entsprechende ausländerrechtliche Status festgestellt werden konnte. Die Ausländerbehörde übermittelte die Liste dann wieder an den Aufwandsträger, der nach Auswertung bei der zuständigen Regierung oder dem Bayerischen Landesamt für Schule die gewünschten Finanzierungshilfen beantragte.

Befugnisse für die dargestellten Datenübermittlungen der Schule konnten weder die von mir angeschriebene Schule noch das Kultusministerium überzeugend darlegen:

— Eine Norm, die insoweit der Schule eine gesetzliche Aufgabe im Sinne von Art. 85 Abs. 1 BayEUG zuwies, war nicht erkennbar. Dies galt auch in Bezug auf die von der Schule herangezogenen Art. 10 Abs. 1 Satz 3 in Verbindung mit Art. 10 Abs. 5 Satz 1 Nr. 6 Bayerisches Schulfinanzierungsgesetz (BaySchFG). Denn Art. 10 Abs. 1 Satz 3 BaySchFG definiert lediglich, wer auch als Gastschüler gilt. Art. 10 Abs. 5 Satz 1 Nr. 6 BaySchFG legt fest, wer Beitrags- oder Kostenschuldner ist.

— § 87 Abs. 1 Aufenthaltsgesetz schied als Rechtgrundlage für Datenübermittlungen durch Schulen schon deshalb aus, weil Schulen in der Vorschrift ausdrücklich ausgenommen sind.

— Auch die Voraussetzungen von Art. 85 Abs. 2 BayEUG lagen nicht vor. Zudem hätte die Schule gemäß Art. 5 Abs. 2 DSGVO die Pflicht getroffen, einen entsprechenden Nachweis zu führen, was ihr nicht gelang.

— Auch Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO konnte keine Rechtsgrundlage vermitteln. Art. 6 Abs. 3 DSGVO verlangt auch mit Blick auf Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO eine Regelung durch Unionsrecht oder durch das Recht der Mitgliedstaaten. Um den Tatbestand des Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO vom Tatbestand des Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO abzugrenzen, muss die unionsrechtliche oder mitgliedstaatliche Norm nach Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO konkret eine rechtliche Pflicht in Bezug auf die Datenverarbeitung vorsehen. Mit anderen Worten: Erforderlich ist, dass sich die in einer Vorschrift normierte Verpflichtung unmittelbar auf eine Datenverarbeitung bezieht. Allein der Umstand, dass ein Verantwortlicher, um irgendeine rechtliche Verpflichtung erfüllen zu können, auch personenbezogene Daten verarbeiten muss, reicht demgegenüber nicht aus. Aus den von der Schule angeführten Regelungen des Bayerischen Schulfinanzierungsgesetzes konnte eine Verpflichtung der Schulen zu personenbezogenen Datenerhebungen oder Datenübermittlungen im Sinne von Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO nicht gewonnen werden.

— Soweit die Schule als Rechtsgrundlage für die Datenübermittlung auf Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG abstellte, übersah sie, dass diese allgemeine datenschutzrechtliche Vorschrift durch die spezialgesetzlichen Regelungen in Art. 85 Abs. 1 und Abs. 2 BayEUG verdrängt wird.

— Schließlich fehlte einer einschlägigen Bekanntmachung des Kultusministeriums[162] der Charakter einer außenwirkenden Norm. So konnte die Vorgabe in Nr. 2.2 dieser Bekanntmachung, wonach die Schulleiter verpflichtet seien, die Aufwandsträger zu unterstützen, weder eine Pflicht im Sinne von Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO noch eine Aufgabenzuweisung im Sinne von Art. 85 Abs. 1 Satz 1 BayEUG begründen. Im Übrigen trifft die Bekanntmachung in Bezug auf den Datenschutz auch keine Aussagen.

Im weiteren Schriftverkehr mit dem Kultusministerium zeigte ich den datenschutzfreundlichen Lösungsansatz auf, wie der bisherige Informationsfluss zwischen Schule, Aufwandsträger und Ausländerbehörde organisatorisch umgestaltet werden könnte. Idealerweise sollten keine personenbezogenen Daten übermittelt werden, sondern **pauschalierte Finanzzuweisungen** erfolgen, gegebenenfalls auf Basis bisheriger Erfahrungswerte. Sollte dies nicht möglich sein, müssten jedenfalls klare gesetzliche Grundlagen geschaffen werden; dabei müsste vor allem ausdrücklich geregelt werden, dass es der Ausländerbehörde untersagt ist, die Daten für andere Zwecke, insbesondere aufenthaltsrechtliche Maßnahmen zu verwenden.

Das Kultusministerium hatte mir dazu mitgeteilt, es habe die von mir skizzierte Möglichkeit einer Pauschalierung intensiv geprüft. Es habe sich jedoch gezeigt, dass die durchschnittlichen Kosten je Kommune stark divergieren. Eine entweder

[162] Bekanntmachung des Bayerischen Staatsministeriums für Unterricht und Kultus über Erstattungen an Gemeinden und Gemeindeverbände für die Beschulung von Asylbewerberkindern (Art. 10 Abs. 5 Satz 1 Nr. 6 BaySchFG) vom 27. Juni 2003 (KWMBl. I S. 261), zuletzt geändert durch Bekanntmachung vom 16. März 2018 (KWMBl. S. 146).

zu Akzeptanzzwecken auf die höher belasteten Kommunen oder zu Wirtschaftlichkeitszwecken auf den Landesdurchschnitt angepasste Pauschale weiche zu weit von den tatsächlichen Gegebenheiten ab und erscheine daher nicht umsetzbar. Des Weiteren fehle es an geeigneten Parametern wie den Schülerzahlen bei den interkommunalen Gastschülern, um eine Pauschale bei Bedarf anzupassen. Daher würde geprüft, in welcher Form Rechtsgrundlagen geschaffen werden könnten. Hierzu habe ich das Kultusministerium in der Folge beraten.

Im Ergebnis wurde Art. 10 BaySchFG durch das Gesetz zur Änderung des Bayerischen Schulfinanzierungsgesetzes[163] mit Wirkung vom 1. August 2023 ein Absatz 10 angefügt. Erfreulicherweise wurden die von mir eingeforderten gesetzlichen Änderungen umgesetzt. So ist nun im Gesetz eine **zweckgebundene Übermittlungsbefugnis** der Schule an den Aufwandsträger geregelt. Vor allem aber ist nun ausdrücklich gesetzlich festgelegt, dass die Ausländerbehörden die vom Aufwandsträger übermittelten personenbezogenen Daten nicht für andere Zwecke verarbeiten dürfen, insbesondere nicht zum Zweck aufenthaltsrechtlicher Maßnahmen. Zudem sind die Ausländerbehörden verpflichtet, alle personenbezogenen Daten nach Übermittlung an den Aufwandsträger unverzüglich zu löschen (vgl. Art. 10 Abs. 10 Satz 4 und 5 BaySchFG).

8.1.3 Bayerische Schulordnung

Auch bei Änderungen der Bayerischen Schulordnung konnte ich durch meine Beratung wesentliche datenschutzrechtliche Verbesserungen erreichen:

— Abschnitt 7 von Anlage 2 der Bayerischen Schulordnung regelt Datenverarbeitungen der Schulen mittels **digitalen Kommunikations- und Kollaborationswerkzeugen**. Danach waren entsprechende Datenverarbeitungen in bestimmten Fallgruppen (wie Unterstützung der Schulentwicklung, Ergänzung der pädagogischen Arbeit durch virtuelle Klassenräume, ortsunabhängiges Arbeiten mit digitalen Unterrichtswerkzeugen, Innen- und Außenkommunikation der Schule) nur zulässig, wenn eine wirksame Einwilligung der Erziehungsberechtigten beziehungsweise der Schülerinnen und Schüler vorlag. Das Kultusministerium wollte diesen **Einwilligungsvorbehalt** zunächst gänzlich abschaffen. Meine Kritik an diesem Vorhaben hatte zur Folge, dass der Einwilligungsvorbehalt in den genannten Fallgruppen nicht vollständig aufgegeben wird, sondern nur insofern, als das digitale Kommunikations- und Kollaborationswerkzeug zentral vom Freistaat Bayern über das Kultusministerium bereitgestellt wird.

  Diese Lösung ist sowohl datenschutzfreundlich als auch praxisorientiert. Zwar entfällt in den genannten Fallgruppen der Einwilligungsvorbehalt beim Einsatz von **Werkzeugen der BayernCloud Schule**. Da Vorprüfungen durch das Kultusministerium – sowie die begleitende Beratung durch mich – auf eine datenschutzfreundliche Gestaltung dieser Werkzeuge hinwirken, ist damit aber kein Nachteil verbunden. Bei Änderungsbedarf kann zudem zentral reagiert werden. Da insofern das aufwändige und ergebnisoffene Einholen von Einwilligungserklärungen bei den Schülerinnen und Schülern sowie den Erziehungsberechtigten durch die Schulen entfällt, werden die Schulen zusätzlich motiviert, diese Werkzeuge einzusetzen.

[163] Vom 24. Juli 2023 (GVBl. S. 445).

Dies hat erhebliche Vorteile gegenüber einem „Wildwuchs“ von Anwendungen in den Schulen, zumal diese von einer umfassenden eigenen Prüfung der Datenschutzkonformität oftmals überfordert sind. Zugleich bleibt der Einsatz anderer Werkzeuge im Einzelfall aber möglich. Auf Basis der sich aus der Praxis ergebenden Erfahrungen können Regelungsstruktur und Anwendungen bei Bedarf weiterentwickelt werden.

— In Abschnitt 8 von Anlage 2 der Bayerischen Schulordnung („Zentrale vom Freistaat Bayern über das Staatsministerium bereitgestellte **Nutzerverwaltung und Anmeldeinfrastruktur**“) wollte das Kultusministerium in Nr. 3.1.2 folgende Datenverarbeitungen einfügen:

  - Zertifikats- und Schlüsseldaten,
  - Zeitpunkt der Zuweisung der Zertifikats- und Schlüsseldaten,
  - Zeitpunkt der Sperrung der Zertifikats- und Schlüsseldaten,
  - Persönliche Identifikationsnummer zur Entsperrung der Zertifikats- und Schlüsseldaten und
  - **Biometrische Daten** (etwa Fingerabdruck oder Gesichtserkennung) **für die Entsperrung der Zertifikats- und Schlüsseldaten** (nur freiwillig).

Diese Ergänzungen sollten laut Kultusministerium eine Zwei-Faktor-Authentifizierung in Bezug auf den gemeinsamen Anmeldeserver für die Anwendungen des Programms BayernCloud Schule ermöglichen. Dadurch sollte eine **erhöhte Sicherheitsstufe bei der Authentifizierung** geschaffen werden, die hinsichtlich spezieller Anwendungen der BayernCloud Schule erforderlich sei. So würden gleichzeitig besonders schützenswerte Daten im Verwaltungsbereich der BayernCloud Schule verschlüsselt werden können. Es werde ausdrücklich sichergestellt, dass dabei die optionale Verarbeitung biometrischer Daten nur freiwillig erfolgen dürfe, mithin stets einer Einwilligung bedürfe.

Die Schaffung einer erhöhten Sicherheitsstufe im Hinblick auf sensible Daten und die Verschlüsselung derselben begrüße ich im Grundsatz ausdrücklich. Zu beachten bleibt aber, dass biometrische Daten nach Art. 9 DSGVO einem besonderen Schutz unterliegen. Vorliegend soll die Verarbeitung biometrischer Daten nur auf Grundlage einer Einwilligung nach Art. 9 Abs. 2 Buchst. a DSGVO zulässig sein. Doch auch dann müssen die allgemeinen Voraussetzungen für eine rechtmäßige Verarbeitung erfüllt sein. Nach Art. 5 Abs. 1 Buchst. c DSGVO müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“). Zweck der Zwei-Faktor-Authentifizierung beziehungsweise der Verschlüsselung ist der Schutz sensibler Daten. Insoweit kann die Verwendung biometrischer Daten zur Authentifizierung und Verschlüsselung – eine wirksame Einwilligung der betroffenen Personen vorausgesetzt – durchaus angemessen sein. Zur Absicherung nicht sensibler Daten ist die Verarbeitung biometrischer Daten jedoch nicht angemessen, weil insoweit kein erhöhter Schutzbedarf gegeben ist. In diesem Fall stünde die Verarbeitung biometrischer Daten trotz wirksamer Einwilligung im Widerspruch zum allgemeinen Grundsatz der Datenminimierung aus Art. 5 Abs. 1 Buchst. c DSGVO.

Erfreulicherweise hat das Kultusministerium meiner Argumentation Rechnung getragen und die Zulässigkeit der Verarbeitung biometrischer Daten durch die aufgenommene Formulierung „bei Anwendungen mit erhöhtem Schutzbedarf“ entsprechend eingeschränkt.

8.2 Masernschutz – Atteste über Kontraindikationen

Im Berichtszeitraum haben mich mehrere Beschwerden erreicht, die sich gegen die **Weitergabe ärztlicher Atteste von Schulen an Gesundheitsämter** im Zusammenhang mit Masernschutzimpfungen wendeten.

In einem Fall hatten Eltern vorgetragen, sie hätten für ihren Sohn bei dessen Realschule eine **„ärztliche Impfunfähigkeitsbescheinigung“** vorgelegt. Die Realschule habe das ärztliche Attest aus ihrer Sicht unzulässig an das Gesundheitsamt weitergegeben.

Im Zuge meiner Erkundigungen bei der Realschule und beim Gesundheitsamt hatte sich dann herausgestellt, dass die Realschule zwar das Gesundheitsamt darüber benachrichtigt hatte, dass Zweifel an der Echtheit oder inhaltlichen Richtigkeit des vorgelegten Nachweises bestünden. Das ärztliche Attest hatte dem Gesundheitsamt jedoch nicht die Realschule übermittelt, sondern ein Gymnasium, an das der Schüler zwischenzeitlich gewechselt war.

Ferner war festzustellen, dass das Gesundheitsamt zuvor alle Schulen in seinem Zuständigkeitsbereich mit einem Schreiben „ermutigt“ hatte, ihnen vorgelegte Atteste über Kontraindikationen gegen die Masernimpfung an das Gesundheitsamt weiterzuleiten. Andernfalls – so das Gesundheitsamt – übernähmen die Schulen die Verantwortung für die Korrektheit der Atteste. Laut Gesetzgeber läge es im Ermessen der Schule, solche Atteste selbst zu prüfen und zu akzeptieren. Dadurch hafteten die Leitungen der Schule dann aber persönlich für deren Richtigkeit. Um den Schulen diesen Arbeitsaufwand und die Verantwortung abzunehmen, biete das Gesundheitsamt an, dass die Schulen die vorgelegten Atteste an das Gesundheitsamt weiterleiten.

Gemäß § 20 Abs. 9 Satz 1 Infektionsschutzgesetz (IfSG) haben Schülerinnen und Schüler ihrer Schule vor Beginn ihrer dortigen Betreuung einen Nachweis bezüglich einer Impfung gegen Masern vorzulegen. Dies kann insbesondere ein Nachweis über eine erfolgte Impfung oder ein ärztliches Attest darüber sein, dass sie aufgrund einer medizinischen Kontraindikation nicht geimpft werden können.

Wenn der nach § 20 Abs. 9 Satz 1 IfSG erforderliche Nachweis nicht vorgelegt wird oder wenn Zweifel an der Echtheit oder inhaltlichen Richtigkeit des vorgelegten Nachweises bestehen, hat die Leitung der Schule gemäß § 20 Abs. 9 Satz 2 IfSG unverzüglich das Gesundheitsamt, in dessen Bezirk sich die Einrichtung befindet, darüber zu benachrichtigen.

Dies bedeutet konkret:

– Der Gesetzgeber setzt für die Übermittlungsbefugnis keine umfassende medizinisch-inhaltliche Überprüfung des vorgelegten Nachweises durch die Schule voraus. Dies kann eine Schule auch nicht leisten. Allerdings knüpft der Gesetzgeber die Befugnis zu einer Datenübermittlung daran, dass **Zweifel an der inhaltlichen Richtigkeit oder Echtheit** bestehen.

Ohne derartige Zweifel ist eine Schule nach dem Willen des Gesetzgebers nicht berechtigt, auf Basis von § 20 Abs. 9 Satz 2 Var. 2 und 3 IfSG personenbezogene Daten an das Gesundheitsamt zu übermitteln. Die Zweifel der Schule müssen auf konkreten Gründen beruhen. Solche Zweifel könnten sich unter Würdigung der Gesamtumstände beispielsweise daraus ergeben, dass der den Nachweis ausstellende Arzt nur in einer weit entfernten Stadt praktiziert. Allein eine unsubstantiierte Aussage „ich habe Zweifel" kann nicht genügen, denn ansonsten liefe die gesetzliche Regelung ins Leere.

— Nach der gesetzgeberischen Entscheidung ist es jedoch grundsätzlich nicht zulässig, das Attest an das Gesundheitsamt zu übermitteln. Denn die Schule darf nur „darüber" benachrichtigen, also über das Bestehen der Zweifel. Wenn ein Gesundheitsamt von einer Schule gemäß Art. 20 Abs. 9 Satz 2 IfSG über bestehende Zweifel benachrichtigt wird, kann es eigenständig die ihm vom Gesetzgeber in § 20 Abs. 12 IfSG eingeräumten Ermittlungsmöglichkeiten nutzen.

— Verantwortlicher für die Datenübermittlung ist die Schule. Diese hat zu prüfen, ob nach den für sie geltenden Vorschriften eine Übermittlung personenbezogener Daten zulässig ist. Hieran ändert sich grundsätzlich auch nichts, wenn eine andere Behörde – mit unrichtigen Rechtsausführungen – zu einer Datenübermittlung „ermutigt". Dies gilt umso mehr, als das Kultusministerium einige Monate zuvor die Schulen zutreffend auf die bestehende und einzuhaltende Rechtslage in einem Rundschreiben hingewiesen hatte.

  Das Schreiben des Gesundheitsamtes an die Schulen gab den rechtlichen Rahmen unzutreffend wieder:

  Bereits die Aussagen zur persönlichen Verantwortung der Schulleitungen für die Richtigkeit von Attesten waren datenschutzrechtlich mehr als zweifelhaft. Wer keine – begründeten – Zweifel hat, darf nach den datenschutzrechtlichen Vorschriften nicht benachrichtigen. Wer hingegen – begründete – Zweifel hat, darf nach den datenschutzrechtlichen Vorschriften benachrichtigen beziehungsweise muss dies sogar tun. Ein darüberhinausgehendes Einstehen oder eine Haftung für die Richtigkeit eines Attestes ist aus den datenschutzrechtlichen Vorschriften nicht ersichtlich. Auch nach allgemeinem Sprachverständnis steht eine Schulleitung nicht automatisch für die (inhaltliche) Richtigkeit eines ärztlichen Attestes ein oder „haftet" gar persönlich für die Richtigkeit, wenn sie keine begründeten Zweifel hat. Jedenfalls aber unterstellten die Formulierungen des Gesundheitsamtes datenschutzrechtliche Befugnisse der Schulen, die tatsächlich nicht bestehen (siehe soeben oben). Denn die Weitergabe eines vorgelegten ärztlichen Attestes ist nicht zulässig – unabhängig vom Vorliegen begründeter Zweifel als Voraussetzung für eine Benachrichtigung.

Daher waren folgende Maßnahmen veranlasst:

— Die Realschule hatte mir auf meine ausführlichen Hinweise zur Rechtslage und Aufforderung zur Stellungnahme keinerlei Zweifel an der inhaltlichen Richtigkeit oder Echtheit des vorgelegten Attestes dargelegt. Die Voraussetzungen für eine personenbezogene Benachrichtigung des Gesundheitsamtes lagen daher offenbar nicht vor. Ich stellte daher einen Verstoß

gegen datenschutzrechtliche Bestimmungen (Art. 6 Abs. 1 UAbs. 1, Abs. 2 und 3 DSGVO) fest. Zudem forderte ich die Realschule auf, die datenschutzrechtlichen Vorschriften künftig strikt zu beachten.

– Auch das Gymnasium hatte auf meine ausdrückliche Frage nach den dort im Zeitpunkt der Datenübermittlung bestehenden Zweifeln solche nicht dargelegt. Die Voraussetzungen des § 20 Abs. 9 Satz 2 IfSG konnte ich daher nicht als erfüllt ansehen. Allein die abstrakte Mitteilung, dass das Attest erhebliche Zweifel habe aufkommen lassen, ohne den Bezugspunkt und die konkreten Anhaltspunkte für die Zweifel zu erläutern, war nicht ausreichend. Unabhängig davon hätte selbst bei entsprechend begründeten Zweifeln keine Befugnis des Gymnasiums bestanden, dem Gesundheitsamt das ärztliche Attest zu übermitteln. Ich stellte daher ebenfalls einen Verstoß gegen Art. 6 Abs. 1 UAbs. 1, Abs. 2 und 3 DSGVO fest. Zudem forderte ich das Gymnasium auf, die datenschutzrechtlichen Vorschriften künftig strikt zu beachten.

– Das Gesundheitsamt hatte ich über die Rechtslage aufgeklärt und zur Richtigstellung gegenüber den Schulen aufgefordert. Daraufhin korrigierte es seine Aussagen gegenüber den Schulen in einem gesonderten Schreiben und stellte die Rechtslage auf Basis meiner Hinweise dar.

8.3 Einsichtnahme durch Lehrkräfte in private Tablets

Wohl aufgrund des stetig zunehmenden Einsatzes von Tablets im Schulunterricht haben mich zuletzt vermehrt Anfragen und Beschwerden erreicht, die sich auf die Reichweite der Zugriffsrechte von Lehrkräften auf diese Geräte bezogen.

Bei einer Schule beanstandete ich sogar einen Datenschutzverstoß. Die Lehrkraft einer sogenannten „Tablet-Klasse“ hatte zur Prüfung der Lernunterlagen/mobilen Hefte die privaten Geräte eingesammelt und ohne Ankündigung oder Wissen der Schülerinnen und Schüler auch **private Fotos gesichtet**. Dies fiel letztlich nur deshalb auf, weil die Lehrkraft damit im Zusammenhang stehend Verweise erteilt hatte.

Auf die zentrale Befugnisnorm des Art. 85 Abs. 1 Satz 1 BayEUG konnte die Schule die Durchsicht der privaten Fotos mangels einer gesetzlich zugewiesenen Aufgabe nicht stützen. Wirksame Einwilligungen nach Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 7 DSGVO hatte die Schule ebenfalls nicht nachweisen können. Damit lag ein Datenschutzverstoß vor: Die Schule hatte durch die Einsicht nehmende Lehrkraft personenbezogene Daten von Schülerinnen und Schülern ohne Rechtsgrundlage verarbeitet.

Die Durchsicht privater Fotos stellt – gerade in der heutigen Zeit – einen ganz erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Außerdem hatte das Kultusministerium erst wenige Monate zuvor alle bayerischen Schulen in einem Schreiben auf die Unzulässigkeit eines solchen Vorgehens hingewiesen.

8.4 Auskunft über Prüfungsarbeiten an Hochschulen

Im Berichtszeitraum beschwerte sich ein Student bei mir, weil eine Hochschule seinen **Antrag auf eine Kopie (vgl. Art. 15 Abs. 3 DSGVO)** seiner – im Rahmen einer Prüfungsleistung von der Hochschule verarbeiteten – personenbezogenen Daten abgelehnt hatte. Sie hätte dies damit begründet, dass eine Kopie einer Prüfungsleistung gemäß der Allgemeinen Prüfungsordnung der Hochschule (im Folgenden: Prüfungsordnung) ausschließlich im Rahmen einer persönlichen Teilnahme an einem Einsichtnahmetermin erfolgen könnte. Die **Prüfungsordnung** wäre als prüfungsrechtliche Spezialregelung anzusehen, die den Auskunftsanspruch nach Art. 15 Abs. 3 DSGVO näher konkretisiere.

Die Regelungen der Prüfungsordnung lauteten unter anderem wie folgt:

- Studierende können nach Feststellung des Prüfungsergebnisses Einsicht in ihre bewerteten schriftlichen Prüfungsarbeiten nehmen.

- Die/der Studierende kann nur persönlich im Einsichtnahmetermin gegenüber dem Prüfer oder der Prüferin die Erstellung einer Kopie seiner/ihrer Prüfungsarbeit durch das jeweilige Fakultätssekretariat anfordern.

- Nach Anfertigung der Kopie teilt das jeweilige Fakultätssekretariat der/dem Studierenden Ort und Termin der Abholung der Kopien mit.

Bereits in meiner Bitte um Stellungnahme gab ich der Hochschule unter anderem folgende Hinweise:

- Art. 15 Abs. 1 DSGVO vermittelt den Betroffenen einen Auskunftsanspruch im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten. Art. 15 Abs. 3 Satz 1 DSGVO ergänzt diesen Anspruch. Danach stellt der Verantwortliche eine Kopie der personenbezogenen Daten zur Verfügung, die Gegenstand der Verarbeitung sind.

- **Die in einer Prüfungsleistung eines Studierenden enthaltenen Ausführungen** sowie die diesbezüglichen Anmerkungen des Prüfers oder der Prüferin **sind personenbezogene Daten** im Sinne von Art. 4 Nr. 1 DSGVO.[164] Diese personenbezogenen Daten werden von der Hochschule grundsätzlich auch im Sinne des Art. 4 Nr. 2 DSGVO verarbeitet, solange die jeweiligen Prüfungsleistungen von Studierenden aufbewahrt werden.

- Wenn eine betroffene Person eine Kopie ihrer personenbezogenen Daten unter ausdrücklicher Berufung auf Art. 15 Abs. 3 DSGVO beantragt, handelt es sich nicht um ein allgemeines Einsichtsbegehren in Prüfungsunterlagen gestützt auf ein Recht auf Akteneinsicht (nach Art. 29 Bayerisches Verwaltungsverfahrensgesetz oder der Prüfungsordnung). Das Auskunftsrecht nach Art. 15 Abs. 3 DSGVO ist davon rechtlich zu trennen.

- Soweit die Hochschule offenbar die Regelungen der Prüfungsordnung auf Auskunftsverlangen nach Art. 15 Abs. 3 DSGVO anwenden will, ist zunächst festzustellen, dass der Anspruch aus Art. 15 Abs. 3 DSGVO dadurch eingeschränkt würde, beispielsweise weil danach die Erstellung einer Kopie

[164] Näher Europäischer Gerichtshof, Urteil vom 20. Dezember 2017, C-434/16, Rn. 40, 42, 44, 46, 62.

grundsätzlich nur in einem persönlichen Einsichtnahmetermin beantragt werden könnte.

— Ich kann allerdings schon nicht erkennen, inwieweit die Prüfungsordnung überhaupt einen einschränkenden Regelungscharakter zu Art. 15 DSGVO haben soll. Denn sie lässt weder im Wortlaut noch in sonstiger Weise einen Regelungsbezug zu einem Auskunftsrecht erkennen, insbesondere nicht zum Auskunftsanspruch nach Art. 15 DSGVO.

Daraufhin teilte mir die Hochschule mit, sie würde dem Studenten nunmehr doch eine Kopie nach Maßgabe von Art. 15 Abs. 3 DSGVO zur Verfügung stellen. Zugleich ließ mich die Hochschule wissen, sie sehe eine einschränkende Regelung des Auskunftsrechts nach Art. 15 DSGVO auf Satzungsebene als zwingend erforderlich an. Die Prüfungsordnung werde daher in diesem Sinne mit ausdrücklichem und einschränkendem Bezug zu Art. 15 DSGVO überarbeitet.

Dies veranlasste mich, der Hochschule Folgendes mitzuteilen:

Die von der Hochschule angedachte Einschränkung des Art. 15 (Abs. 3) DSGVO durch eine Regelung in der Prüfungsordnung ist derzeit rechtlich schon dem Grunde nach nicht gangbar.

Zwar lässt Art. 23 DSGVO unter den dort genannten Voraussetzungen Beschränkungen des Auskunftsrechts aus Art. 15 DSGVO durch Rechtsvorschriften der Mitgliedstaaten zu. **Einschränkende Rechtsvorschriften** der Mitgliedstaaten können grundsätzlich auch in untergesetzlichen Normen bestehen. Jedoch können Einschränkungen in untergesetzlichen Normen nur in dem Rahmen erfolgen, den das mitgliedstaatliche Recht vorgibt. Hochschulrechtliches Satzungsrecht muss sich **im Rahmen der landesgesetzlichen (Ermächtigungs-) Normen** halten.

Die Ermächtigung zum Erlass von Prüfungsordnungen durch die Hochschulen findet sich in Art. 84 Abs. 2 und Abs. 3 Bayerisches Hochschulinnovationsgesetz (BayHIG). Nach Art. 84 Abs. 3 Satz 1 Nr. 7 BayHIG regelt die Prüfungsordnung die wesentlichen Fragen im Hinblick auf Prüfungsanforderungen und Prüfungsverfahren, insbesondere die Bekanntmachung der Prüfung und die Benachrichtigung der Prüfungsteilnehmerinnen und Prüfungsteilnehmer. Die Ermächtigung zum Erlass von Prüfungsordnungen hat keinerlei Regelungsbezug zum Auskunftsrecht nach Art. 15 DSGVO.

Vielmehr hat der bayerische Gesetzgeber bereits in Art. 10 Abs. 2 BayDSG ausdrücklich Beschränkungen des Auskunftsrechts aus Art. 15 DSGVO geregelt. Auch dies legt nahe, dass der Gesetzgeber im Bayerisches Hochschulinnovationsgesetz nicht zu einer Beschränkung von Art. 15 DSGVO ermächtigen wollte. Art. 84 BayHIG lässt eine solche Beschränkung also nicht zu.

Die Hochschule verzichtete in der Folge auf eine Art. 15 Abs. 3 DSGVO einschränkende Regelung in der Prüfungsordnung.

In meinem Schreiben hatte ich die Hochschule zudem darauf hingewiesen, dass inzwischen auch die Entscheidungsgründe des **Urteils des Bundesverwaltungsgerichts** vom 30. November 2022 (6 C 10.21) zu Auskunftsansprüchen nach Art. 15 DSGVO veröffentlicht worden sind: Danach stellen die in einer berufsbezo-

genen Prüfung unter einer Kennziffer angefertigten schriftlichen Prüfungsleistungen und die zugehörigen Prüfergutachten jeweils ihrem gesamten Inhalt nach personenbezogene Daten des Prüflings dar. Der Prüfling kann nach Art. 15 DSGVO die Überlassung einer unentgeltlichen Kopie dieser Unterlagen verlangen.

Die Entscheidung entspricht meiner bereits zuvor vertretenen Auffassung.

8.5 Datenschutzverstoß im Datenschutzkurs

Natürlich begrüße ich es, wenn Hochschulen Kurse zur Aus- und Fortbildung im Bereich des Datenschutzes anbieten. Ein wenig peinlich wirkt es allerdings, wenn es gerade bei der Durchführung eines solchen Kurses zu einem Verstoß gegen datenschutzrechtliche Vorschriften kommt. Ein solcher Vorfall wurde mir durch eine Meldung der Hochschule selbst sowie eine Eingabe der betroffenen Person bekannt.

Bei der Anmeldung zum Datenschutzkurs hatte die teilnehmende Person persönliche Angaben gemacht. Sie hatte auch ein (Einwilligungs-)**Formular zur Datenverarbeitung** erhalten, verbunden mit der Frage, ob sie ihre Daten auch anderen Teilnehmern zur Verfügung stellen wolle. Im Formular hatte sie bewusst keine **Angaben zu ihrem aktuellen Arbeitgeber** eingetragen, sondern diesen Bereich händisch durchgestrichen. Zudem hatte sie in einer begleitenden E-Mail zusätzlich und ausdrücklich darauf hingewiesen, dass sie als Privatperson teilnehme und keine Information zu ihrem Arbeitgeber bekannt geben wolle.

Im Rahmen des Kurses hat ein Dozent gleichwohl vor allen Teilnehmenden den Arbeitgeber der betroffenen Person erwähnt. Die Information stammte aus einer Liste, die der Dozent vorab zu allen Teilnehmenden erstellt hatte. Dafür hatte er die Lebensläufe ausgewertet, welche die Kursteilnehmer zur Prüfung der Zulassungsvoraussetzungen eingereicht hatten. Eine Rechtsgrundlage insbesondere für die Weitergabe der Informationen an die anderen Teilnehmenden bestand nicht.

In der Korrespondenz mit mir machte die Hochschule schließlich geltend, dass es sich bei dem Verstoß um einen Einzelfehler gehandelt habe. Bereits in den Dozentenverträgen seien entsprechende Datenschutzbelehrungen enthalten gewesen. Nunmehr werde die Hochschule zusätzlich vor jedem Kursdurchlauf alle Lehrkräfte ausdrücklich schriftlich darauf hinweisen, dass eine Teilnehmerliste nicht im Kurs verlesen werden dürfe. Außerdem würden nun vor jedem Kursdurchlauf die Teilnehmenden ausdrücklich schriftlich um Rückmeldung (Einwilligung) gebeten, ob und welche personenbezogenen Daten der Teilnehmenden an die Dozierenden zum Zweck der Lehrvorbereitung (konkretes Eingehen etwa auf Unternehmensbereich, Position) weitergegeben werden dürfen.

Auf diese Weise dürfte sichergestellt sein, dass auch der Datenschutzkurs zukünftig datenschutzkonform durchgeführt wird.

9 Zensus

Die Phase der Datenerhebungen für den Zensus 2022 endete bereits im Herbst 2022. Gleichwohl beschäftigten mich damit im Zusammenhang stehende Themen auch noch im aktuellen Berichtszeitraum.

Die aufgetretenen Fragen

— inwiefern eine öffentliche Stelle amtlich bestätigte Identitätsnachweise verlangen (siehe sogleich Nr. 9.1) oder

— private E-Mail-Adressen nutzen kann (siehe sogleich Nr. 9.2), und

— ob das Kontaktieren des Arbeitgebers zulässig ist (siehe sogleich Nr. 9.3),

können sich im Übrigen auch in anderen Bereichen stellen.

9.1 Vorlage von amtlich bestätigten Identitätsnachweisen zur Geltendmachung von Auskunftsansprüchen

In Bezug auf den Zensus 2022 hatten einige Bürgerinnen und Bürger bei einer zuständigen Behörde Auskunft nach Art. 15 DSGVO beantragt. Die Behörde hat die Erteilung der Auskunft jedoch vielfach von der Vorlage eines amtlich bestätigten Identitätsnachweises abhängig gemacht, etwa in Form einer beglaubigten Kopie des Personalausweises, Reisepasses oder einer Meldebescheinigung. Daraufhin sind mehrere Beschwerden bei mir eingegangen, die sich gegen diese zusätzliche Anforderung sowie gegen die damit verbundenen Kosten richteten.

Art. 12 Abs. 6 DSGVO bestimmt, dass der Verantwortliche zusätzliche Informationen, die zur Bestätigung der Identität der betroffenen Person erforderlich sind, anfordern kann, wenn er begründete Zweifel an der Identität hat. Derartige Zweifel waren im konkreten Fall insbesondere jedoch deshalb fernliegend, weil die Antragsteller teilweise bereits mit dem Auskunftsantrag die Zensusfragebogennummer und das behördliche Aktenzeichen mitgeteilt hatten. Warum trotzdem Zweifel an der Identität bestehen sollten, konnte mir die Behörde nicht plausibel, vor allem nicht einzelfallbezogen darlegen. Vielmehr schien diese – aufgrund des aus ihrer Sicht hohen Schutzbedarfs der gespeicherten Zensusdaten – pauschal Zweifel an der Identität aller Antragsteller anzunehmen.

Ein Abweichen von Art. 12 Abs. 6 DSGVO allein aufgrund eines besonderen Schutzbedarfes der Daten ist vom europäischen Gesetzgeber jedoch nicht vorgesehen.

Ich habe die Behörde deshalb aufgefordert, die betreffenden Auskünfte nach Art. 15 DSGVO zu erteilen, ohne dass die Antragsteller zusätzlich einen amtlich bestätigten Identitätsnachweis erbringen müssen. Die Behörde ist dem nachgekommen.

9.2 Nutzung privater E-Mail-Adressen durch Erhebungsbeauftragte

Zu Recht waren einige Bürgerinnen und Bürger verunsichert, die im Rahmen des Zensus 2022 oder des Mikrozensus 2023 von der zuständigen Behörde angeschrieben worden waren und für Terminabsprachen anstelle amtlicher Kontaktdaten die private E-Mail-Adresse der oder des Erhebungsbeauftragten (vgl. mein 32. Tätigkeitsbericht 2022 unter Nr. 11.1.2) vorgefunden hatten. Diese private E-Mail-Adresse hatte bei den Auskunftspflichtigen vielfach sowohl Zweifel an der Legitimation der Erhebungsbeauftragten hervorgerufen als auch Fragen zur Sicherheit der Daten im Zusammenhang mit einer Verarbeitung durch einen privaten E-Mail-Provider aufkommen lassen. Einige von Ihnen wandten sich deshalb auch an mich.

Bei Erhebungsbeauftragten handelt es sich in der Regel um **amtlich betraute Privatpersonen** (vgl. § 14 Bundesstatistikgesetz, § 12 Mikrozensusgesetz), die nur temporär zur Unterstützung der Befragung eingesetzt werden.

Wie mir die zuständige Behörde auf Nachfrage erläuterte, würden sich bei der Verwendung einer amtlichen E-Mail-Adresse Schwierigkeiten, insbesondere im Hinblick auf den sozialrechtlichen Status der Erhebungsbeauftragten ergeben. Die Suche nach einer echten Alternative zur Verwendung einer privaten E-Mail-Adresse sei deshalb bisher – auch im Austausch mit anderen Bundeländern – leider erfolglos geblieben.

Aus Datenschutzsicht ist die Nutzung eines privatwirtschaftlichen Unternehmens als E-Mail-Provider **nicht grundsätzlich unzulässig**, zumindest solange die eigentliche Abfrage der Zensus- oder Mikrozensusdaten nicht per E-Mail stattfindet. Bei den mir zur Prüfung vorgelegenen Fällen konnte ich eine solche Abfrage nicht feststellen, vielmehr fanden über die E-Mail-Adresse lediglich Terminabsprachen statt. Damit wurden nur in geringem Umfang personenbezogene Daten verarbeitet. Die Nutzung der E-Mail-Adresse war außerdem freiwillig, da in allen Fällen auch eine Telefonnummer zur Verfügung gestanden hätte.

Gleichwohl habe ich die zuständige Behörde aufgefordert, für die Zukunft eine andere, datenschutzfreundlichere Verfahrensweise zu etablieren. Die Behörde hat mich hieraufhin informiert, dass man meinen Vorschlag prüfe, ob mittelfristig ein Online-System zur Terminvereinbarung genutzt werde könne.

Ich konnte außerdem erreichen, dass für die Übergangszeit das Anschreiben und der ergänzende Informationsflyer von der zuständigen Behörde überarbeitet wurden, um den Auskunftspflichtigen zumindest die besondere Rolle der ehrenamtlichen Erhebungsbeauftragten und den Hintergrund der Angabe der privaten E-Mail-Adresse genauer zu erläutern.

9.3 Unzulässige Information des Arbeitgebers eines Erhebungsbeauftragten

Ein ehemaliger Erhebungsbeauftragter des Zensus 2022 beschwerte sich bei mir über den Umgang der Erhebungsstelle mit seinen eigenen personenbezogenen Daten. Hintergrund war die noch ausstehende Rückgabe eines Tablets, welches ihm zum Zwecke der Zensuserhebungen zur Verfügung gestellt worden war. Nach Abschluss der Erhebungen forderte die Behörde ab Ende Oktober 2022 die Tablets von allen Erhebungsbeauftragten zurück, indem sie darum bat, einen Rückgabetermin zu vereinbaren. Der Beschwerdeführer kam dem zunächst nicht nach,

sondern wartete vorerst auf die Abrechnung der Aufwandsentschädigung. Telefonisch war der Beschwerdeführer zu den Geschäftszeiten nicht zu erreichen. Ob ein postalisches Aufforderungsschreiben zugegangen war, konnte ich nicht zweifelsfrei feststellen. Anfang 2023 kontaktierte die Erhebungsstelle sodann den Arbeitgeber des Beschwerdeführers telefonisch und teilte ihm mit, der Beschwerdeführer sei als Erhebungsbeauftragter tätig gewesen und müsse noch Unterlagen zurückgeben. Eine Einwilligung in diese Kontaktaufnahme lag nicht vor.

Ich habe gegenüber der Erhebungsstelle einen Datenschutzverstoß festgestellt: Für die Kontaktaufnahme mit dem Arbeitgeber hatte die Behörde keine Rechtsgrundlage. Die vorgenommenen Datenverarbeitungen (zweckändernde Nutzung und Übermittlung) waren für die Aufgabenerfüllung nicht erforderlich.

Eine Verarbeitung personenbezogener Daten ist nur dann erforderlich im Sinne des Art. 4 Abs. 1 oder Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG, wenn die öffentliche Stelle ihre jeweilige Aufgabe ohne die Verarbeitung nicht, nicht vollständig oder nicht in rechtmäßiger oder zumutbarer Weise erfüllen kann. Dabei ist auch stets der Grundsatz der Verhältnismäßigkeit zu beachten.

Nach Einholung mehrerer Stellungnahmen bin ich zu dem Ergebnis gekommen, dass die Erhebungsstelle die direkten Kontaktmöglichkeiten zum Beschwerdeführer nicht vollständig ausgeschöpft hatte und ihr somit mildere Mittel zur Aufgabenerfüllung zur Verfügung gestanden hätten. Die Behörde hat den Fehler eingeräumt und sich für die Kontaktierung des Arbeitgebers entschuldigt.

10 Informationsfreiheit

Nachfolgend berichte ich über meine Prüfungs- und Beratungspraxis zum Vollzug des allgemeinen Auskunftsrechts nach Art. 39 BayDSG durch bayerische öffentliche Stellen. Aus einer Vielzahl von Vorgängen greife ich dabei einen Fall heraus, bei dem ich meine Position zur **Auskunftspflicht von Kommunen bei Grundstücksgeschäften** fortentwickeln konnte (Nr. 10.1). Ein anderer Vorgang hat einen Platz in diesem Bericht dadurch verdient, dass eine erhebliche Anzahl von Kommunen über viele Monate nicht auf einen gestellten Antrag geantwortet hat: Ein Verein hatte vorgetragen, er habe bei 174 Kommunen inhaltsgleiche Anträge auf Auskunft nach Art. 39 BayDSG gestellt. Trotz Erinnerungen des Vereins reagierten offenbar über 60 dieser Kommunen weiterhin nicht. Auch nach meiner Aufforderung an die Kommunen, den Antrag zu beantworten, erhielt der Verein nach seiner Aussage von 19 Kommunen weiterhin keine Antwort (Nr. 10.2). Im abschließenden Beitrag habe ich einige kleine Fälle zusammengestellt, in denen sich Optimierungsbedarfe gezeigt haben (Nr. 10.3).

10.1 Grundstücksankauf durch eine Kommune

Eine Gemeindebürgerin beantragte im Berichtszeitraum bei ihrer Gemeinde im Zusammenhang mit einem Ankauf eines Grundstücks durch die Gemeinde Auskunft über den Kaufpreis des Grundstücks, den Zeitpunkt des Kaufvertragsschlusses sowie mögliche Nebenabsprachen mit dem Verkäufer.

Sie begründete ihren Antrag insbesondere damit, dass sie sich als kommunalpolitisch interessierte Bürgerin eine Meinung über den Grundstückskauf bilden und die Arbeit des Gemeinderats überprüfen wolle. Sie berief sich dabei ausdrücklich auf Art. 39 BayDSG und wies auf meine Veröffentlichung zur **Transparenz bei Grundstücksverkäufen bayerischer Gemeinden** hin, in der ich auch Hinweise zum Vollzug des Art. 39 BayDSG gegeben hatte (enthalten unter anderem in meinem 30. Tätigkeitsbericht 2020 unter Nr. 13.1).

Da die Gemeinde die Auskunft nicht erteilt und sich die Antragstellerin bei mir darüber beschwert hatte, forderte ich bei der Gemeinde eine Stellungnahme an. Ich machte dabei deutlich, dass die Empfehlungen aus der angesprochenen Veröffentlichung grundsätzlich auch auf Auskunftsansprüche bei Grundstückskäufen anzuwenden sind. Dies gilt umso mehr als – wie sich herausstellte – das Grundstücksgeschäft teilweise als Tauschgeschäft ausgestaltet war, also die Veräußerung eines gemeindlichen Grundstücks einschloss. Zudem gab ich der Gemeinde für ihre nochmalige Prüfung des Antrags verschiedene rechtliche Hinweise.

Die Gemeinde legte mir nachvollziehbar dar, dass der Vertragspartner in der Gemeinde identifizierbar wäre, auch wenn man seinen Namen nicht nennen und in den Unterlagen schwärzen würde. Die Gemeinde musste daher auch die Zulässigkeit der im Raum stehenden Übermittlung personenbezogener Daten des Vertragspartners datenschutzrechtlich prüfen. Denn ein Anspruch auf Auskunft besteht nur soweit, als eine solche Übermittlung an nicht öffentliche Stellen zulässig ist (vgl. Art. 39 Abs. 1 Satz 1 Nr. 1, Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG). Mit Blick auf die im Rahmen des Art. 5 BayDSG anzustellende Abwägung sollte die Gemeinde

den Vertragspartner anhören. Im Übrigen wies ich erneut auf meine Veröffentlichung und die dort aufgeführten Kriterien hin.

Nach einiger Zeit teilte mir die Gemeinde mit, dass sie den Vertragspartner angehört habe und dieser nicht mit einer Einsicht Dritter in den Kaufvertrag einverstanden sei. Er habe jedoch keine triftige Begründung der Verweigerung geben können. Im Ergebnis versicherte mir die Gemeinde, sie werde die entsprechenden Passagen des Kaufvertrags kopieren und der Antragstellerin zur Verfügung stellen. Es freut mich, dass ich der Antragstellerin bei der Durchsetzung ihres Anliegens helfen konnte.

10.2 Ignorieren von Auskunftsanträgen – keine gute Option

Im Berichtszeitraum hatte ein eingetragener Verein vorgetragen, er habe an **174 bayerische Kommunen gleichlautende Auskunftsbegehren** per E-Mail gesendet.

Die Satzung des Vereins regelt die Zwecke und Ziele des Vereins. Sie stehen in einem unmittelbaren Zusammenhang mit den gestellten Fragen.

Da der Verein von zahlreichen Kommunen keine Auskunft erhalten hatte, wandte er sich im weiteren Verlauf auch mehrmals an mich. Der Verein wollte sich zunächst ausdrücklich nicht über einzelne Kommunen beschweren, bat mich jedoch um Beratung zu verschiedenen Fragen, die bei ihm zum Auskunftsrecht entstanden seien. Meine Antworten übersandte der Verein auch an viele Kommunen. Zudem berief sich der Verein gegenüber den Kommunen inzwischen auch ausdrücklich auf Art. 39 BayDSG.

Die Reaktionen der Kommunen auf den gestellten Antrag waren sehr unterschiedlich:

- Manche Kommunen erteilten unmittelbar die erbetene Auskunft.
- Andere Kommunen erteilten nach Erinnerungen des Vereins die Auskunft – teilweise auch erst nach Bezugnahme des Vereins auf die Beratung durch mich.
- Einige Kommunen teilten dem Verein mit, die Auskunftserteilung werde von einer Kostenerstattung gemäß den kostenrechtlichen Vorschriften abhängig gemacht (vgl. Art. 39 Abs. 5 BayDSG).
- Eine gewisse Zahl von Kommunen lehnte die Auskunft (ganz oder teilweise) mit unterschiedlichen Begründungen ab.

Am Schluss verblieben nach Darstellung des Vereins **68 Kommunen, die** ihm **nach** mehreren Schreiben über einen Zeitraum von insgesamt **mehr als fünf Monaten überhaupt nicht geantwortet** hatten. Der Verein übersandte mir in der Folge eine Liste mit den 68 Kommunen und bat mich, diese zur Beantwortung seines Antrags zu bewegen.

Daraufhin forderte ich die 68 Kommunen unter Hinweis auf die Sachdarstellung des Vereins zur Beantwortung des Auskunftsantrags auf und setzte hierfür eine Frist. Dabei teilte ich ihnen unter anderem Folgendes mit:

Behörden sind dazu gehalten, grundsätzlich innerhalb eines angemessenen Zeitraums Entscheidungen zu treffen und das Verwaltungsverfahren zügig durchzuführen (vgl. Art. 10 Satz 2 und Art. 25 Abs. 2 BayVwVfG). Dies gilt auch im Hinblick auf Anträge nach Art. 39 BayDSG. § 75 Satz 2 Verwaltungsgerichtsordnung geht im Regelfall von einer Drei-Monats-Frist als Voraussetzung für eine Untätigkeitsklage aus. Diese Frist kann als Anhaltspunkt gesehen werden, dass spätestens dann kein angemessener Zeitraum mehr vorliegt. Dies bedeutet jedoch nicht, dass dieser Zeitraum ohne konkrete Notwendigkeit ausgeschöpft werden dürfte.

Sollte die jeweilige Kommune den Antrag nach Art. 39 BayDSG bis zu dem gesetzten Termin nicht beantwortet haben, stellte ich bereits mit meinem Aufforderungsschreiben eine Beanstandung nach Art. 16 Abs. 4 BayDSG in Aussicht. Denn unabhängig vom Inhalt einer Entscheidung über den Antrag ist dieser jedenfalls zu beantworten.

Des Weiteren gab ich diesen Kommunen unter anderem folgende Hinweise zur inhaltlichen Prüfung des Antrags:

— Auf meiner Internetpräsenz https://www.datenschutz-bayern.de habe ich in der Rubrik „Auskunftsanspruch“ verschiedene Materialien bereitgestellt, welche die ordnungsgemäße Anwendung von Art. 39 BayDSG erleichtern sollen.

— Antragsteller und Anspruchsberechtigter nach Art. 39 Abs. 1 Satz 1 BayDSG kann auch eine juristische Person sein, insbesondere also auch ein eingetragener Verein.

— Ein berechtigtes Interesse im Sinne von Art. 39 Abs. 1 Satz 1 BayDSG kann grundsätzlich jedes rechtliche, wirtschaftliche oder ideelle Interesse sein. Ein Verein kann als berechtigtes Interesse auch ein für seine Mitglieder gruppennützliches Interesse darlegen.[165]

— Am Vorliegen eines berechtigten Interesses bestehen im konkreten Fall keine ernsthaften Zweifel.

— Da der Antrag von einzelnen anderen Kommunen zunächst unter Hinweis auf einen unverhältnismäßigen Aufwand (Art. 39 Abs. 1 Satz 2 Nr. 3 BayDSG) abgelehnt wurde, weise ich unter Bezugnahme auf die von mir veröffentlichten Informationsmaterialien darauf hin, dass die Anforderungen für die Bejahung eines unverhältnismäßigen Aufwands sehr hoch sind.

— Sollte eine Kommune zum Ergebnis kommen, dass keine Auskunft erteilt werden kann, sollte sie die Ablehnung am Maßstab des Art. 39 BayDSG unter genauer Zitierung der zugrundeliegenden Vorschrift gegenüber dem Verein konkret begründen. Dies gilt gesondert für jedes einzelne im Antrag dargelegte Auskunftsverlangen. Vor einer vollständigen Ablehnung sollte immer die Möglichkeit einer Teilauskunft geprüft werden.

— Im Rahmen meiner Zuständigkeit als Datenschutz-Aufsichtsbehörde obliegt mir gemäß Art. 15 Abs. 1 Satz 1 BayDSG die Prüfung der Einhaltung des Bayerischen Datenschutzgesetzes bei den Kommunen. Da Art. 39

[165] Vgl. Bayerischer Verwaltungsgerichtshof, Urteil vom 13. Mai 2019, 4 B 18.1515, BeckRS 2019, 17760, Rn. 29.

BayDSG formell in das Bayerische Datenschutzgesetz integriert ist, bezieht sich meine Zuständigkeit auch auf diese Vorschrift.

Zudem teilte ich den Kommunen mit, dass ich im Falle von geltend gemachten Ablehnungsgründen und einer Überprüfung durch mich – etwa angesichts einer späteren Beschwerde des Vereins hierzu – berücksichtigen würde, dass ich mit meinem Schreiben bereits Hinweise zur inhaltlichen Prüfung erteilt und der jeweiligen Kommune auch eine Beratung angeboten habe.

Nach Klärung von Fragen zum bisher erfolgten Schriftverkehr verblieben auf dieser Grundlage letztlich über 60 Kommunen, die bis zum Zeitpunkt meines Aufforderungsschreibens offenbar nicht auf den Antrag reagiert hatten.

Nach Angaben des Vereins hatten auch kurz nach Ablauf der von mir gesetzten Frist 19 Kommunen weiterhin nicht auf den Auskunftsantrag des Vereins reagiert. Daraufhin sendete ich diesen Kommunen ein Anhörungsschreiben zu einer Beanstandung. Die Anhörungsverfahren waren zum Redaktionsschluss dieses Berichts noch nicht beendet.

10.3 Unerfreuliches und Erfreuliches – ein Überblick

Naturgemäß erhalte ich – aufgrund von Beschwerden – überwiegend Kenntnis von Sachverhalten, in denen es möglicherweise zu einem Verstoß gegen Art. 39 BayDSG gekommen ist. Gleichwohl stellt sich in manchem Beschwerdefall heraus, dass die jeweilige Behörde bei ihrer (Teil-)Ablehnung eines Auskunftsersuchens Art. 39 BayDSG zutreffend angewandt hatte. Auch verwiesen zahlreiche Beratungsanfragen von Behörden auf das Anliegen, die gesetzlichen Vorgaben einzuhalten.

Soweit Behörden Art. 39 BayDSG nicht ordnungsgemäß angewandt hatten, waren sie manchmal „nur“ rechtlichen Fehleinschätzungen erlegen. Allerdings drängte sich in einzelnen Fällen der Eindruck auf, dass die (nicht) handelnde Behörde nur begrenzt eine gründliche und umfassende Prüfung des gestellten Antrags durchgeführt oder gar vermeintliche Gründe gesucht hatte, um möglichst keine Auskunft erteilen zu müssen. Dies führte dazu, dass ich mehrere Beanstandungen ausgesprochen habe.

Nachfolgend stelle ich **ausgewählte Fallgestaltungen** aus dem Berichtszeitraum dar. Auf die Sachverhalte und zugrundeliegenden Auskunftsanträge gehe ich dabei nicht näher ein. Alle folgenden Punkte hätten die jeweiligen Behörden übrigens bereits anhand des Gesetzestextes oder jedenfalls mit Hilfe der Informationsmaterialien auf meiner Internetpräsenz eigenständig klären können.

— Viele Behörden beantworteten Anträge zunächst gar nicht (siehe insbesondere soeben Nr. 10.2).

— Zwei Behörden lehnten Anträge mit der Begründung ab, das Auskunftsverlangen beziehe sich nicht auf personenbezogene Daten und daher sei Art. 39 BayDSG gar nicht anwendbar. Richtig ist hingegen, dass Gegenstand eines möglichen Anspruchs auf Auskunft nach Art. 39 BayDSG ganz allgemein der Inhalt von Dateien und Akten der Behörde ist, also **gerade (auch) Dateien und Akten, die keine personenbezogenen Daten enthalten.** Dies ergibt sich eindeutig aus dem Wortlaut und der Systematik des

Gesetzes. Dass das Bayerische Datenschutzgesetz ansonsten im Wesentlichen die Verarbeitung personenbezogener Daten regelt, ändert daran nichts. Dies ist auch in der Rechtsprechung anerkannt.[166]

— Einzelne Behörden lehnten Anträge mit der Begründung ab, die Antragstellenden hätten kein berechtigtes Interesse glaubhaft dargelegt. Tatsächlich genügt allein die Aussage „Bitte senden Sie mir das Dokument XY zu" nach der gesetzlichen Regelung nicht, wenn das berechtigte Interesse im Antrag auch sonst nicht ausreichend zum Ausdruck kommt. Doch scheint noch immer nicht allen Behörden klar zu sein, dass ein berechtigtes Interesse im Sinne von Art. 39 Abs. 1 Satz 1 BayDSG grundsätzlich jedes rechtliche, wirtschaftliche oder ideelle Interesse sein kann.[167] So hat eine Gemeinde vehement vorgetragen, das vom Antragsteller bekundete kommunalpolitische Interesse sei nur vorgeschoben, in Wirklichkeit gehe es dem Antragsteller darum, Informationen zu erlangen, um das geplante Vorgehen der Gemeinde aus Gründen eigener Betroffenheit möglichst zu verhindern. Gerade diese Einschätzung der Gemeinde zugrunde gelegt, bestand aber ein berechtigtes Interesse des Antragstellers. Die Gemeinde muss dieses Interesse ja inhaltlich nicht teilen, es darf ihrem Interesse sogar konträr sein.

— Einzelne Behörden verweigerten eine Auskunft pauschal unter Berufung auf einen Ablehnungsgrund, obwohl der Auskunftsantrag mehrere Auskunftsbegehren enthielt und eine differenzierte Auseinandersetzung am Maßstab des Art. 39 BayDSG erforderlich gewesen wäre. Einzelne Punkte wären zu beauskunften gewesen, der Ablehnungsgrund traf nicht auf alle einzelnen Auskunftsbegehren zu.

— Mehrere Behörden lehnten Anträge ab, da für die Auskunft ein unverhältnismäßiger Aufwand entstehen würde (vgl. Art. 39 Abs. 1 Satz 2 Nr. 3 BayDSG). Dabei wurde regelmäßig übersehen, dass eine Versagung des Auskunftsanspruchs aus diesem Grund nur in Ausnahmefällen in Betracht kommt. Die Gewährung des Informationszugangs gehört zu den Verwaltungsaufgaben auskunftspflichtiger Stellen. Für die Bejahung eines unverhältnismäßigen Aufwandes im Sinne des Art. 39 Abs. 1 Satz 2 Nr. 3 BayDSG müssen zum einen sehr hohe Anforderungen erfüllt sein, zum anderen bedingt dies eine genauere Prüfung des zu erwartenden Aufwandes auch unter Berücksichtigung von Kosten, die bei der antragstellenden Person vereinnahmt werden können.[168]

— Eine Behörde lehnte einen Antrag unter **bloßer (Teil-)Zitierung des Gesetzestextes des Art. 39 BayDSG ab,** ohne dass für die antragstellende Person oder für mich nachvollziehbar war, ob die Norm im vorliegenden Fall eine Ablehnung trägt. Denn der in Bezug genommene Ablehnungstatbestand wurde nicht erläutert oder begründet.

— Eine andere Behörde teilte mir unter anderem mit, vor einer möglichen Auskunft solle zunächst ich prüfen und ihr dann mitteilen, ob die **Daten der Behörde bei der Antragstellerin „sicher"** seien. Dieser Behörde habe ich

166 Bayerischer Verwaltungsgerichtshof, Urteil vom 13. Mai 2019, 4 B 18.1515, BeckRS 2019, 17760, Rn. 28.

167 Vgl. die Begründung des Gesetzentwurfs, Landtags-Drucksache 17/7537, S. 49.

168 Zu Einzelheiten vgl. näher Hessischer Verwaltungsgerichtshof, Beschluss vom 2. Februar 2010, 6 A 1684/08, BeckRS 2010, 46976.

deutlich gemacht, dass sie zum einen mir keine Prüfaufträge zu erteilen hat, zum anderen ein Antrag nach Art. 39 BayDSG ausschließlich am gesetzlichen Maßstab zu prüfen ist.

— Eine Behörde hatte erst nach einem längeren Schriftwechsel mit mir sowie der Androhung einer Beanstandung die beantragte Auskunft erteilt. Im Vorfeld der Beschwerde der Antragstellerin an mich hatte die Behörde ihr außerdem – unzutreffend – mitgeteilt, das Ablehnungsschreiben sei nicht als Verwaltungsakt einzuordnen, da „dieses Schreiben mangels gewisser Bestandteile nicht als Bescheid einzuordnen" wäre. Eine Rechtsbehelfsbelehrung fügte die Behörde ihrem Ablehnungsschreiben nicht bei. Hier konnte man jedenfalls insgesamt den Eindruck gewinnen, die Behörde wollte die Antragstellerin ins Leere laufen lassen: Einerseits den Antrag ablehnen, andererseits mögliche Rechtsmittel gegen diese Entscheidung aber nicht offenlegen.

— Gegenüber zwei Gemeinden musste ich Beanstandungen nach Art. 16 Abs. 4 BayDSG aussprechen, da sie ihrer Unterstützungspflicht mir gegenüber nicht nachgekommen sind.

  Eine Gemeinde lehnte einen Auskunftsantrag ab. Daraufhin legte der Antragsteller Beschwerde bei mir ein. Ich forderte die Gemeinde daher auf, den Antrag unter Beachtung meiner Hinweise erneut zu prüfen. Die Gemeinde lehnte den Antrag daraufhin nochmals ab. Da die Ablehnungsbegründung der Gemeinde nicht alle entscheidungsrelevanten Punkte abgedeckt hatte, forderte ich die Gemeinde zur ergänzenden Stellungnahme auf. Die Antwort der Gemeinde ging auf die von mir konkret gestellten Fragen nahezu nicht ein. Da die Gemeinde auch meine letzte Fristsetzung zur Beantwortung meiner Fragen verstreichen ließ, ohne Hinderungsgründe mitzuteilen, sprach ich gegenüber der Gemeinde wegen des Verstoßes gegen ihre Unterstützungspflicht (Art. 16 Abs. 1 BayDSG) eine Beanstandung aus und informierte die zuständige Rechtsaufsichtsbehörde hierüber. Im anschließenden Kontakt mit der Gemeinde zeigte sie sich zugänglicher und erteilte letztlich die beantragte Auskunft.

  Eine weitere Gemeinde hatte ebenfalls auf meine Schreiben nicht ausreichend reagiert, so dass ich auch hier eine Beanstandung ausgesprochen habe. Daraufhin antwortete mir die Gemeinde dann doch. Aus der Antwort wurde deutlich, dass es sich bei den begehrten Auskünften um Umweltinformationen handelte. Für diese Informationen gibt es einen spezialgesetzlich geregelten Auskunftsanspruch nach Art. 3 und 4 Bayerisches Umweltinformationsgesetz (BayUIG). Der allgemeine Auskunftsanspruch nach Art. 39 BayDSG war somit gar nicht anwendbar (vgl. Art. 39 Abs. 2 BayDSG). Dem Antragsteller konnte ich daher bei diesem Vorgang nicht weiter behilflich sein. Denn meine Aufsichtszuständigkeit bezieht sich allein auf datenschutzrechtliche Vorschriften einschließlich des Art. 39 BayDSG, nicht hingegen auf den Informationszugang nach Art. 3 und 4 BayUIG als solchen.

Soweit mein aufsichtsrechtliches Tätigwerden erforderlich wurde, kann ich allerdings – wiederum erfreulich – feststellen, dass die jeweiligen Behörden letztlich regelmäßig Einsicht gezeigt haben. In schriftlichen und persönlichen Kontakten vermittelte ich dabei insbesondere, dass **Art. 39 BayDSG kein „Recht zweiter Klasse"** gegenüber einem oft so empfundenen und abgegrenzten „Kerngeschäft"

der jeweiligen Behörde ist. Dies möchte ich auch an dieser Stelle nochmals betonen. Art. 39 BayDSG ist von den Behörden **mit derselben Sorgfalt zu vollziehen wie auch alle anderen gesetzlichen Regelungen.** Dies gilt auch dann, wenn einzelne Antragstellende vermeintlich überproportional wissbegierig sind. Auch ein unfreundlicher Tonfall oder unsachliche Ergänzungen im Schriftwechsel sind keine Ablehnungsgründe im Sinne des Art. 39 BayDSG. Im Ergebnis konnte ich bei hierzu eingegangenen Beschwerden die nach Art. 39 BayDSG bestehenden Auskunftsansprüche durchsetzen. Ich gehe davon aus, dass ich auch in den unter Nr. 10.2 dargestellten, noch offenen Fällen die Kommunen dazu bewegen werde, auf den Auskunftsantrag zu antworten.

Allerdings wäre der Aufwand bei den Antragstellenden, bei mir und auch bei den Behörden selbst weitaus geringer gewesen, wenn sie sogleich die Auskunft erteilt oder den Antrag beantwortet hätten. Zudem ist es nicht fernliegend, dass bei Antragstellenden durch die Verhaltensweise einer Behörde im Einzelfall der Eindruck entstanden ist, die Behörde habe etwas zu verbergen oder sperre sich grundsätzlich.

Insgesamt bin ich weiterhin optimistisch, dass Art. 39 BayDSG in der bayerischen Verwaltungspraxis „ankommt" und Defizite beim Vollzug – auch auf Grund meiner Bemühungen – immer weniger vorkommen.

11 Technik und Organisation

11.1 Nutzung von nicht dienstlichen E-Mail-Adressen

Die Nutzung dienstlicher E-Mail-Adressen ist für öffentlicher Stellen grundsätzlich unverzichtbar, weil durch Verwendung von internen E-Mail-Servern ein geschützterer Austausch von Informationen innerhalb der Organisation sichergestellt wird. Ein solches System erleichtert die Implementierung von Verschlüsselungstechnologien, um die Integrität übermittelter Daten auch an externe Empfänger sicherzustellen. Im Gegenzug können externe Empfänger Behördenkontakte leichter verifizieren. Das reduziert die Gefahr von Phishing-Angriffen und anderen betrügerischen Aktivitäten.

Dienstliche E-Mail-Adressen sind damit eine nahezu notwendige Voraussetzung für die Sicherung sensibler Daten bei der Übertragung per E-Mail und der Gewährleistung einer zuverlässigen behördlichen Kommunikation.

Leider erreichten mich auch in diesem Jahr wieder Beschwerden gegen bayerische öffentliche Stellen, bei denen private E-Mail-Accounts außerhalb der behördlichen Infrastruktur zur Kommunikation dienstlicher Inhalte genutzt wurden. Einzelne Fälle betrafen etwa Lehrkräfte öffentlicher Schulen, sowie Gerichtsvollzieherinnen und Gerichtsvollzieher.

Bei frei verfügbaren, kostenlos angebotenen E-Mail-Accounts („Freemail-Diensten“) sind die Allgemeinen Geschäftsbedingungen (AGB) oft nicht mit dienstlichen Belangen vereinbar. Solche AGB gewähren den Providern zum Teil weitreichende Einsichtsrechte in die E-Mail-Inhalte ihrer Nutzerinnen und Nutzer, um beispielsweise personalisierte Werbung ausbringen zu können. Für eine Verarbeitung der in den E-Mails enthaltenen personenbezogenen Daten zu diesem Zweck fehlt es typischerweise an einer Rechtsgrundlage.

Die Einräumung solcher Einsichtsrechte durch die AGB von Freemail-Diensten birgt erhebliche Risiken für die Vertraulichkeit von behördlichen Informationen; sie kann auch zu einem ernsthaften Sicherheitsrisiko für die behördliche Kommunikation werden.

Darüber hinaus untergräbt die Nutzung privater E-Mail-Dienste die Möglichkeit einer sicheren Kommunikation innerhalb öffentlicher Stellen. Freemail-Anbieter sind oft nicht auf die spezifischen Sicherheitsanforderungen von Behörden ausgerichtet, was die Gefahr von Datenlecks und unautorisiertem Zugriff erhöht.

Unabhängig von solchen Risiken werden private-E-Mail-Accounts häufig auch in einem weniger abgesicherten Umfeld genutzt als dienstliche E-Mail-Accounts, etwa auf privaten Endgeräten wie Laptops oder Smartphones. Diese Geräte sind tendenziell schlechter gesichert als dienstliche und damit insbesondere einem höheren Risiko für Diebstahl oder Kompromittierung ausgesetzt. Zudem werden private E-Mail-Adressen naturgemäß eben auch für die private Kommunikation – etwa mit Shopping- und Social-Media-Plattformen – genutzt. Dadurch sind sie einem erhöhten Risiko für Phishing- und Malware-Angriffen ausgesetzt.

Ich empfehle nachdrücklich allen Bediensteten bayerischer öffentlicher Stellen die Nutzung ihrer in aller Regel standardmäßig bereitgestellten, zumindest auf Wunsch verfügbaren, dienstlichen E-Mail-Adressen für die Kommunikation in der Rolle von Beschäftigten. Selbst wenn im Einzelfall Dienstvereinbarungen oder vergleichbare Regelungen eine freie Wahl des Kommunikationsmittels erlauben, ist die Nutzung privater Accounts – insbesondere von Freemail-Anbietern – mit erheblichen Risiken verbunden. Selbst wenn die „Flucht ins Private" in bestimmten Situationen eine bequeme Lösung sein mag: Wer die IT-Sicherheit und den Datenschutz ernst nimmt, ist mit der behördlichen Kommunikationsinfrastruktur im Zweifelsfall besser bedient.

11.2 E-Mail und Copy & Paste

Dass beim Kopieren und Einfügen von Texten besondere Sorgfalt erforderlich ist, zeigt ein ungewöhnlicher Vorfall aus einer bayerischen Justizvollzugsanstalt: Dort hatte eine Mitarbeiterin vor Urlaubsantritt eine automatische Abwesenheitsbenachrichtigung für ihren dienstlichen E-Mail-Account eingerichtet. Dabei hatte sie jedoch nach dem eigentlich gewollten Benachrichtigungstext versehentlich personenbezogene Daten eines Gefangenen aus einem zuvor bearbeiteten Vorgang miteingefügt („Copy & Paste").

In der Folge erhielten die Kommunikationspartner durch die Abwesenheitsnotiz aufschlussreiche Angaben zu sozialen Bindungen, Delikten sowie schulischer und beruflicher Laufbahn eines bestimmten Gefangenen. Wenigstens war dieser nur mit seinem im deutschsprachigen Raum verbreiteten Nachnamen bezeichnet.

Nach dem Bekanntwerden des Vorfalls wurde der automatisierte Abwesenheitsassistent unverzüglich deaktiviert, der Vorfall mit der Bediensteten besprochen und auch die übrige Belegschaft sensibilisiert.

Die Verletzung des Schutzes personenbezogener Daten hatte voraussichtlich kein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Person zur Folge, weil eine konkrete Zuordnung anhand der versehentlich preisgegebenen Daten nahezu ausgeschlossen werden konnte. Gleichwohl verweist der Fall auf eine wichtige und gern vergessene „Windows-Routine": Beim Einfügen von kopierten Inhalten muss immer geprüft werden, ob nicht unbeabsichtigt zu viele Daten weitergegeben werden.

11.3 Jugend pentestet

11.3.1 Schulische Netzwerke

An staatlichen Schulen in Bayern werden in der Regel zwei getrennte Netzwerke genutzt, die unterschiedlichen Verarbeitungszwecken dienen. Einerseits soll den Bildungseinrichtungen der Einsatz vielfältiger pädagogischer Methoden für den Unterricht ermöglicht werden – etwa um Inhalte zu teilen, Informationen aus dem Internet abzurufen oder auf interaktiven Tafeln im Klassenzimmer anzuzeigen. Dazu dient das **pädagogische Netz**. Bei diesem stehen insbesondere die Verfügbarkeit und der leichte Zugang im Vordergrund. Eine Verarbeitung personenbezogener Daten ist dort grundsätzlich nicht vorgesehen. Aus Gründen der Autori-

sierung beziehungsweise Authentisierung lässt sich jedoch nicht gänzlich vermeiden, dass etwa Benutzernamen oder Geräteadressen geprüft werden, um zu gewährleisten, dass nur befugte Nutzerinnen und Nutzer Zugriff auf das Netzwerk und die darin zu pädagogischen Zwecken vorhandenen Geräte haben. Das Gegenstück dazu bildet das **Verwaltungsnetz**. Dabei handelt es sich um ein separates und stärker geschütztes Netzwerk. Dieses Netz dient zur Verarbeitung von Personal- und Schülerdaten, hier können also gezielt personenbezogene und teils auch sensible Daten verarbeitet werden. Daher gelten in diesem Bereich auch strikte Sicherheitsrichtlinien.

11.3.2 Ein Schüler als Pentester

Ein Schüler hatte im Rahmen eines Forschungsprojekts unter Aufsicht einer Lehrkraft einen **Penetrationstest** (kurz: Pentest) im pädagogischen Netzwerk seiner Schule durchgeführt. Solche Tests dienen üblicherweise dem Zweck, einzelne Systeme oder ganze Netzwerke auf Schwachstellen zu prüfen und diese zu dokumentieren, um sie dann – mit dem Ziel einer Behebung – dem Betreiber mitzuteilen. In der Regel werden solche Tests durch spezialisierte IT-Sicherheits-Dienstleister in Absprache mit dem Verantwortlichen durchgeführt.

Dem Schüler, dessen Lehrer zugleich die Rolle des Datenschutzbeauftragten der Schule bekleidete, gelang bei seinem Pentest ein erfolgreicher Angriff: Durch einen nicht ausreichend sicher konfigurierten LDAP-Dienst konnte er Zugriff auf das „historisch gewachsene“ pädagogische Netzwerk erhalten. Unsichere Praktiken der Systemadministration (etwa in Scriptdateien im Klartext gespeicherte Zugangsdaten oder einfach zu erratende Passwörter für privilegierte Accounts) waren „Altlasten“, die wohl wiederholt übersehen worden waren. Der Schüler konnte seine Systemrechte schrittweise bis hin zum Domänen-Administrator ausbauen (sog. **Privilege Escalation**) und in der Folge einen Vollzugriff auf die Systeme und Dateien innerhalb der Domäne des pädagogischen Netzes erlangen. Er fand heraus, dass sich dieses Netz nicht nur auf seine Schule beschränkte, sodass der Schüler schließlich auch auf Daten weiterer Schulen zugreifen konnte.

11.3.3 Responsible Disclosure unerwünscht

Der Pentest fand zwar unter Aufsicht einer Lehrkraft statt, allerdings ohne vorherige Rücksprache mit dem technischen Betreiber des pädagogischen Schulnetzes. Immerhin wurden die Ergebnisse dem Dienstleister im Rahmen einer Präsentation vorgestellt. Dieses Vorgehen wird **Responsible Disclosure** genannt. Dabei soll die Offenlegung einer gefundenen Sicherheitslücke mit dem Hersteller abgestimmt und die breite Öffentlichkeit erst informiert werden, sobald die Sicherheitslücke behoben wurde. **Full Disclosure** bezeichnet im Gegensatz dazu die Praxis, Informationen über die Sicherheitslücke ohne vorherige Absprache mit den verantwortlichen Stellen zu veröffentlichen. Ziel dieses Vorgehens kann es etwa sein, hohen Druck auf einen Hersteller oder Betreiber auszuüben, die Sicherheitslücke schnellstmöglich zu schließen. Benutzerinnen und Benutzer werden dann zwar gewarnt; Hacker könnten die Schwachstelle allerdings ausnutzen, bevor der Betreiber sie schließen kann.

Die Reaktion des Betreibers auf diese Responsible Disclosure fiel aus Sicht des Schülers und des Lehrers ernüchternd aus: Der offenkundig nicht IT-inkompetente Schülers erhielt weder Anerkennung noch wurde er in einen gemeinsamen

Lösungsfindungsprozess eingebunden; der Betreiber wies stattdessen darauf hin, dass ein solches Vorgehen – insbesondere ohne Absprache – zukünftig zu unterlassen sei und Schüler wie Lehrkraft Passwörter absolut vertraulich zu behandeln hätten. Auch mit konkreten Maßnahmen zur Stärkung der Sicherheit seines IT-Systems zögerte der Betreiber zunächst, obwohl die Lücke eklatant erschien – immerhin hatte ein Schüler Adminrechte für die gesamte Domäne erlangt.

11.3.4 Frust und Neugier

Die Reaktion des Betreibers forderte den Schüler nun heraus: Einige Zeit nach der Präsentation verschaffte er sich ohne Absprache mit dem Betreiber oder seiner Lehrkraft nochmals Zugang zum pädagogischen Netz. Dies geschah über seinen eigenen Computer im privaten Umfeld außerhalb der Unterrichtszeit. Der Schüler nutzte einen SSH-Tunnel zu einem derjenigen Server, auf den er zuvor Zugriff erlangt hatte und auf dem er sich offenbar eine Hintertür eingerichtet hatte. So konnte er mehrere weitere Server kompromittieren, Dienste verändern und Pakete nachinstallieren. Darüber hinaus gelang ihm, Daten des LDAP-Verzeichnisses einer anderen Schule sowie von der Softwarepaketierung und Softwarebereitstellung abzuziehen.

11.3.5 Aufarbeitung und Lessons Learned

Ich habe mich im Rahmen der Aufarbeitung des Falls sowohl mit dem Lehrer als auch mit den Betreibern des pädagogischen wie auch des Verwaltungsnetzes der Schule auseinandergesetzt. Entstandene Schäden wurden behoben und Sicherheitslücken geschlossen. Auch Sensibilisierungsmaßnahmen – etwa mit der Schulleitung – wurden ergriffen. Nach meiner derzeitigen Kenntnis fand kein Zugriff auf das Verwaltungsnetz statt. Die Risiken durch die Möglichkeit des Zugriffs auf personenbezogene Daten in den LDAP-Verzeichnissen blieben in Anbetracht der Datenkategorien und der Motivation des Schülers überschaubar.

Aus dem Vorfall lassen sich mehrere Lehren und Empfehlungen für bayerische öffentliche Stellen – insbesondere für öffentliche Schulen – gewinnen:

— Zugangsdaten dürfen nicht im Klartext in Scriptdateien gespeichert werden. Historisch gewachsene Systeme und Netzwerke sollten systematisch einer Prüfung unterzogen werden. Dies gilt insbesondere bei einem Betreiberwechsel, bei dem die vorhandene IT-Infrastruktur beibehalten wird.

— Privilegierte Benutzeraccounts (wie Domänen-Administrationskonten) sollten nicht einfach zu erratende oder in Wörterbüchern gelistete Passwörter verwenden. Gerade im Falle weiterreichender Zugriffsrechte ist die Nutzung einer Zwei-Faktor-Authentifizierung zu prüfen.

— LDAP-Verzeichnisse sollten auf ihre Sicherheit geprüft werden; dies gilt insbesondere für die Lese- und Schreibberechtigungen. Die darin gespeicherten Informationen sollten auf das notwendige Maß beschränkt sein (Grundsätze der Datenminimierung und der Datensparsamkeit).

— Responsible Disclosure ist aus Sicht einer bayerischen Behörde eine als positiv zu beurteilende Vorgehensweise von Dritten, die Sicherheitslücken gefunden haben: Gewiss ist es für Behördenleitungen und IT-Sicherheits-

Verantwortliche im ersten Moment unerfreulich, von Lücken im eigenen System zu erfahren. Dennoch ist Responsible Disclosure einem erfolgreichen Cyberangriff vorzuziehen, bei der die Lücke schadhaft ausgenutzt wurde und ihr Bestehen sich erst im Nachhinein bei einer forensischen Untersuchung herausstellt.

— Penetrationstests sind ein wichtiges Mittel zur Absicherung: Betreiber sollten im besten Fall regelmäßig oder auch nach größeren Umstellungen der Infrastruktur oder bei Betreiberwechseln die Systeme und Netze prüfen oder prüfen lassen, insbesondere dann, wenn es sich um komplexe und historisch gewachsene Umgebungen handelt.

— Allerdings möchte ich auch **von Laien-Pentests in einer Produktivumgebung abraten**. Auch wenn es verlockend sein mag, im Rahmen schulischen oder akademischen Unterrichts kostengünstig Pentests durchführen zu lassen, sind damit Risiken verbunden. Auf Betreiberseite kann die Verfügbarkeit von Diensten gefährdet sein, wenn diese im Zuge eines Angriffsversuchs abstürzen oder überlastet werden. Auch können Daten verloren gehen oder verfälscht werden (etwa bei einer SQL-Injection). Nicht zuletzt besteht ein Risiko für nicht abgesprochene „Einzelgängeraktionen" wie im hier beschriebenen Fall. Auch „gut gemeinte" Angriffe können für Hobbyhackerinnen und Hobbyhacker schwerwiegende Konsequenzen haben: Schon das Vorbereiten des Ausspähens und Abfangens von Daten ist zudem ein Straftatbestand, der nach § 202c Abs. 1 Nr. 1 Strafgesetzbuch mit einer Freiheitsstrafe bis zu zwei Jahren geahndet werden kann.

11.4 Beratungstätigkeit für Datenschutz-Folgenabschätzung (DSFA) und Risikoanalyse

In meinem Beratungsalltag stelle ich fest, dass sich die Datenschutz-Folgenabschätzung (DSFA) sowie die allgemeine datenschutzrechtliche Risikoanalyse von einem einstmals neuen, noch unbekannten Instrument zu gut eingeübten Routinen entwickeln. Diese Entwicklung ist sehr zu begrüßen. Neben Gerichtsentscheidungen, die in bestimmten Konstellationen eine DSFA ausdrücklich fordern, ohne dabei auf die DSFA-Methode näher einzugehen, zeichnen sich mittlerweile wichtige Anwendungsfelder ab. Insbesondere dort, wo innovative technische Betriebsmittel oder die deutliche Ausweitung bestehender Datennutzungsansätze im Raum stehen, ist oft der Ruf nach einer DSFA zu vernehmen, die eine rechtskonforme Verarbeitung nachweisen soll.

Da mein umfangreiches Informationspaket[169] zu DSFA und allgemeiner Risikoanalyse bereits in ganz unterschiedlichen fachlichen Kontexten (zum Beispiel Gesundheitswesen, Personalwirtschaft, Kommunen, Justiz) zur Anwendung gekommen ist, konnten sich sowohl die zugrundeliegende systematisch hergeleitete Methodik als auch die Good-Practice-Empfehlungen in der Praxis bewähren. Dieser gesetzte Rahmen erlaubt den bayerischen öffentlichen Stellen eine Fokussierung auf die eigentlichen Inhalte der einzelnen DSFA oder allgemeinen Risikoanalyse, nachdem der zeitliche Beginn für die jeweilige Durchführung festgelegt wurde.

Der Verantwortliche muss geeignete technische und organisatorische Maßnahmen bereits planen und veranlassen, wenn er die Mittel der Verarbeitung festlegt;

[169] Siehe die Ausführungen in meinem 32. Tätigkeitsbericht 2022 unter Nr. 12.2.

wird diese produktiv, müssen die Maßnahmen implementiert, überwacht und erforderlichenfalls ergänzt werden. Bei einer Hochrisikoverarbeitung muss die dann erforderliche DSFA, die auch die zur Bewältigung der Risiken geplanten technischen und organisatorischen Maßnahmen mit umfasst, vorab durchgeführt und nachgewiesen werden (Art. 35 Abs. 1 DSGVO).

Immer wieder wird mir die Frage gestellt, wann eine DSFA oder allgemeine Risikoanalyse begonnen werden muss. Bei der Beschaffung von datenschutzrelevanten Leistungen im Wege der **Auftragsvergabe**[170] muss regelmäßig bereits als Grundlage für die Bestimmung des Beschaffungsbedarfs geprüft werden, welche Risiken für die Rechte und Freiheiten von betroffenen Personen aus der leistungsgegenständlichen Verarbeitung und gegebenenfalls dem Transfer von personenbezogenen Daten resultieren. Je nach der zu bewertenden Verarbeitung kann eine allgemeine Risikoanalyse ausreichen oder bei einer Hochrisikoverarbeitung eine DSFA erforderlich sein. Beide Instrumente liefern – auch im Hinblick auf die oftmals nur eingeschränkte Möglichkeit der Konkretisierung einer Verarbeitung vor der Beschaffung – wichtige Aspekte, die als funktionale oder nicht-funktionale Anforderungen an den Leistungsgegenstand zu berücksichtigen sind (zum Beispiel Anforderung an die Gestaltung von Zugriffsberechtigung und an die Löschfunktion). Daher ist eine risikobasierte datenschutzrechtliche Betrachtung grundsätzlich bereits vor solchen Beschaffungen durchzuführen, und die relevanten Ergebnisse der Risikoanalyse sind in den Beschaffungsunterlagen zu berücksichtigen. Nach der Beschaffung geht die schrittweise Konfiguration der Betriebsmittel während der Implementierung und der Einführung mit der Konkretisierung der DSFA beziehungsweise der Risikoanalyse einher.

11.5 Umgang mit dem PIA-Tool der CNIL

Digitalisierung erleichtert auch die Erledigung von Datenschutzaufgaben. Die Suche nach einer IT-Anwendung, die bei der Erstellung und der Verwaltung einer Datenschutz-Folgenabschätzung (DSFA) hilft, führt meist rasch zum „PIA-Tool“.[171] Die von der französischen Datenschutz-Aufsichtsbehörde – der Commission Nationale de l' Informatique et des Libertés (CNIL) – Software-Unterstützung beruht auf der dortigen DSFA-Methodik, dem „Privacy Impact Assessment“ (PIA). Mit dem PIA-Tool kann ein DSFA-Bericht im Bereich der Sicherheit der Verarbeitung erstellt und ausgegeben werden.

Die CNIL stellt unterschiedliche Varianten des PIA-Tools als Open-Source-Software zur Verfügung.[172] Weitere Versionen des PIA-Tools sind in unterschiedlichen Bereichen des Onlinedienstes GitHub verfügbar, auf dem die Entwicklungsprojekte für das PIA-Tool bereitstellt werden.[173] Über diese GitHub-Projekte kann mit den Entwicklern des PIA-Tools kommuniziert und weitergehende Information insbesondere zu den einzelnen Software- und Sprachversionen bezogen werden.

[170] Weitere Details: Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz als Kriterium im Vergabeverfahren, Stand 2/2024, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018“.

[171] Internet: https://www.cnil.fr/en/privacy-impact-assessment-pia.

[172] Internet: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment.

[173] Internet: https://github.com/LINCnil/pia und https://github.com/kosmas58/pia-app/releases.

Da bayerische öffentliche Stellen das PIA-Tool zumindest nach meiner Wahrnehmung aus unterschiedlichen Gründen kaum nutzen, sondern meine in der Praxis schon bewährten Arbeitshilfen zu DSFA und allgemeiner datenschutzrechtlicher Risikoanalyse mit „Werkzeugkasten" einsetzen, biete ich das PIA-Tool auf meiner Website nicht mehr an.[174] In meiner Orientierungshilfe „Risikoanalyse und Datenschutz-Folgenabschätzung – Systematik, Anforderungen, Beispiele" ist das Instrument gleichwohl berücksichtigt.

Vor der Beschaffung und dem Einsatz einer IT-Anwendung müssen grundsätzlich im Rahmen des Anforderungsmanagements die fachlichen und technischen Anforderungen an diese IT-Anwendung erhoben, analysiert und bewertet werden. Dieses allgemein angeratene Vorgehen sollte auch vor der Nutzung des PIA-Tools beachtet werden. Dabei zeigt sich unter anderem, dass im PIA-Tool nur die drei Risikobereiche „Unrechtmäßiger Zugriff auf Daten", „unerwünschte Änderung von Daten" und „Datenverlust" behandelt werden. Werden diese drei Bereiche für Verarbeitungsrisiken mit den DSGVO-Anforderungen verglichen, so stellt sich die Frage, ob für eine vollständige DSFA nicht auch weitere Risikobereiche, wie beispielsweise die Bereiche „Datenminimierung", „Transparenz", „Intervenierbarkeit", „Nichtverkettung" und „Richtigkeit", zu betrachten sind.

In meiner Orientierungshilfe „Risikoanalyse und Datenschutz-Folgenabschätzung – Systematik, Anforderungen, Beispiele" wird die Antwort auf diese Frage systematisch auf Basis der Datenschutz-Grundverordnung hergeleitet und die wichtige Frage nach der Vollständigkeit bejaht. Diese Orientierungshilfe erfüllt die Mindestanforderungen an eine rechtskonforme DSFA. Daher sind diese Anforderungen bei jeder IT-Unterstützung für die Erstellung und die Verwaltung einer DSFA von bayerischen öffentlichen Stellen zu beachten.

Feedback bayerischer öffentlicher Stellen zum PIA-Tool lässt zudem erkennen, dass insbesondere auch eine fehlende Benutzerverwaltung, fehlende Unterstützung bei Softwarefehlern sowie eine fehlende Umsetzung von wichtigen Good-Practice-Ansätzen (zum Beispiel eine zweigeteilte DSFA) Schwierigkeiten bei der Verwendung des PIA-Tools bereiten können.

Im Rahmen meiner Beratung zur DSFA konnte ich zudem beobachten, dass bei der erstmaligen Durchführung einer DSFA praxisgerechte Arbeitshilfen mit anschaulichen Beispielen gut geeignet sind, um das Verständnis für das Instrument „DSFA" zu schärfen, die damit verbundene Methodik besser zu verstehen und den Umgang mit der DSFA einzuüben. Regelmäßig erst danach wird für die jeweilige Stelle deutlich, ob und, wenn ja, welche künftige IT-Unterstützung für die DSFA-Erstellung und die DSFA-Verwaltung sinnvoll erscheint.

11.6 Zustellung durch die Post mit Zustellungsurkunde

Die förmliche Zustellung eines Schreibens durch ein Landratsamt veranlasste einen Bürger, sich mit einer Beschwerde an mich zu wenden: **Auf dem Briefumschlag** seien **gut sichtbar** Angaben verzeichnet gewesen, die Rückschlüsse auf den Inhalt des Schreibens zuließen und dort aus Datenschutzgründen nicht hätten vermerkt werden dürfen.

[174] Aktuelles Informationsangebot im Internet: https://www.datenschutz-bayern.de, Rubrik DSFA.

Konkret handelte es sich um die Angabe eines Kfz-Kennzeichens des Beschwerdeführers, das ein personenbezogenes Datum darstellt. Auf dem Briefumschlag konnten zudem, die Felder „Versicherungsschutz“, „Steuer“, „Meldepflicht“, „TÜV“, „AU“ und „SP“ angekreuzt werden, was auf Versäumnisse des Briefadressaten in diesen Kontexten hinweisen könnte.

Wird die Zustellung – wie im Beschwerdefall – mit Postzustellungsurkunde bewirkt, sind Art. 3 Verwaltungszustellungs- und Vollstreckungsgesetz in Verbindung mit §§ 177 bis 182 Zivilprozessordnung zu beachten. Auf dem Umschlag, in dem den das zuzustellende Schriftstück eingelegt ist, sowie auf der Zustellungsurkunde dürfen nur die personenbezogenen Angaben angebracht werden, welche die mit der Zustellungsvordruckverordnung eingeführten Muster vorsehen (zu Einzelheiten vgl. meinen 30. Tätigkeitsbericht 2020 unter Nr. 2.5). Die gesetzliche Formulargestaltung stellt in diesem Fall auch sicher, dass die Beschäftigten mit der Zustellung beauftragter Postdienstleistungsunternehmen oder andere Personen, welche die Sendung zu Gesicht bekommen, möglichst wenig über den Inhalt erfahren.

Alle zusätzlichen Angaben auf dem Umschlag, die öffentliche Stellen eigenmächtig hinzufügen, sind im Zweifelsfall ohne Rechtsgrundlage offengelegt: Für die Zustellung dürfen nämlich nur diejenigen Daten verarbeitet werden, die das Zustellungsrecht als erforderlich ansieht.

Im Zusammenhang mit der oben genannten Beschwerde habe ich das betroffene Landratsamt ersucht, zukünftig auf „überschießende“ Angaben auf dem Briefumschlag zu verzichten und für Zustellungen nur vorschriftsgemäße Vordrucke zu nutzen.

Ich weise darauf hin, dass die Rechtslage im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz hiervon abweichen kann.

11.7 Mehrere Beschwerden zur räumlichen Gestaltung von Bürgerbüro und Zulassungsstelle, technisch-organisatorische Prüfung bei einer Kommune

Aufgrund von Beschwerden wurde ich auf die räumliche Gestaltung des Bürgerbüros sowie der Zulassungsstelle einer größeren bayerischen Stadt aufmerksam.

Hier hatte der Stadtrat trotz entsprechender Bedenken des behördlichen Datenschutzbeauftragten beschlossen, im Rahmen eines modernen und vermeintlich bürgerfreundlichen Konzepts das Bürgerbüro im Erdgeschoß des Atriums eines großen mehrstöckigen Bürogebäudes anzusiedeln, so dass es möglich war, die Mitarbeitenden des Bürgerbüros sowie die Bürgerinnen und Bürger rundum aus allen darüberliegenden Stockwerken zu beobachten. Auch bezüglich der Zulassungsstelle musste ich feststellen, dass wegen der engen Platzverhältnisse in den für die Zulassungsvorgänge verwendeten (eigentlich ungeeigneten) Räumlichkeiten sowie wegen der nicht zuletzt dadurch bedingten Personenströme im „Rücken“ der dort sitzenden Personen eine datenschutzkonforme Abwicklung der Zulassungsvorgänge in vielen Fällen nicht möglich war.

Speziell kam es im Rahmen eines Zulassungsprozesses und einer damit verbundenen routinemäßigen Überprüfung, ob es sich bei dem Bürger um eine steuerpflichtige Person mit (angeblichen) Zahlungsrückständen handelt, zu einer für die betroffene Person sehr unangenehmen Personenverwechslung. Das Gespräch

zu den (angeblichen) Zahlungsrückstände zwischen Bürger und Mitarbeiter war für mehrere weitere Besucher der Zulassungsstelle ohne Weiteres mithörbar.

Leider zeigte sich die Kommune erst nach einer technisch-organisatorischen Vor-Ort-Prüfung einsichtig und sagte zu, die räumliche Ausgestaltung durch Umzüge der entsprechenden Stellen zu ändern. Um bis zur Verlagerung des Bürgerbüros ein Mindestmaß an Vertraulichkeit zu gewährleisten, wurden organisatorische Maßnahmen (unter anderem Aufstockung Sicherheitsdienst, proaktiver Datenschutz durch die Sachbearbeitung) und die Schaffung eines zusätzlichen Ausweichbüros umgesetzt. Auch in der Zulassungsstelle wurden Maßnahmen zum Sicht- und Hörschutz ergriffen.

Wie dieser Fall zeigt, sehen durchaus viele Bürgerinnen und Bürger auch den Datenschutz als ein wichtiges Kriterium hinsichtlich des Aspekts Bürgerfreundlichkeit an. Ich möchte daher noch einmal auf meinen 25. Tätigkeitsbericht 2011/2012 unter Nr. 25.6.2 verweisen; dort sind Details zur datenschutzgerechten Gestaltung von Bürgerbüros aufgelistet.

11.8 Beschwerden zum Verlust einer Patientenakte

Auch im Berichtsjahr erreichten mich wieder zahlreiche Beschwerden zur Verarbeitung von personenbezogenen Daten durch bayerische öffentliche Gesundheitseinrichtungen.

So teilte mir ein Beschwerdeführer mit, dass seine analog geführte Patientenakte in einem Krankenhaus nicht mehr auffindbar, in elektronischer Form dagegen nur teilweise vorhanden sei. Diese Information habe der Beschwerdeführer telefonisch von der Klinik erhalten. Auf meine Nachfrage bei dem Krankenhaus erhielt ich die Auskunft, dass die Akte vorhanden sei.

Auch wenn die Patientenunterlagen offenbar zwischenzeitlich wieder „aufgetaucht“ waren, zeigt die Beschwerde exemplarisch einige **Probleme der hybriden Aktenführung** auf. Werden Akten sowohl analog als auch elektronisch geführt, besteht häufig Unklarheit, welche Akte „führend“ ist, vollständig und im Bedarfsfall zugreifbar sein muss. In solchen Fällen muss insbesondere vorher allgemein festgelegt sein, ob beide Akten den gleichen Inhalt haben sollen und entsprechend gepflegt werden müssen, oder ob nur beide Akten zusammen das „Gesamtbild“ insbesondere über Gesundheitszustand und Behandlung der betroffenen Person bieten sollen. Fehlt eine solche Festlegung, kann dies zum einen die (Weiter-)Behandlung der Patientin oder des Patienten gefährden. Zum anderen können auch Schwierigkeiten bei der Erfüllung von Betroffenenrechten, insbesondere von Auskunftsansprüchen entstehen

Der Umgang mit „gedoppelten“ Patientenakten bedarf einer guten organisatorischen Vorbereitung. Die einschlägigen Vorgaben müssen von vornherein feststehen, klar formuliert sein und handlungsleitend implementiert werden. Sie müssen so „robust“ gestaltet sein, dass sie auch im stressigen und auf andere Aspekte als „Rechtsarbeit“ fokussierten Klinikalltag zuverlässig funktionieren und das medizinische Personal nicht mehr als nötig von seiner Hauptaufgabe – der Patientenversorgung – abhalten. Die Bewährung entsprechender Vorgaben zur Aktenführung muss effektiv überwacht werden. Diese Empfehlungen gelten auch für das Aufnahme- und Entlassmanagement.

Im Übrigen muss darauf geachtet werden, dass auch bei einer (temporären) Nichtauffindbarkeit einer Papierakte eine Datensicherheitsverletzung vorliegen kann, welche die Meldepflicht nach Art. 33 DSGVO auslöst.

Eine datenschutzgerechte Steuerung des Umgangs mit Patientenakten ist eine wesentliche Aufgabe des Krankenhausmanagements, die zielführend nur gemeinsam mit dem medizinischen Personal bewältigt werden kann. Hier kommt regelmäßigen Schulungen eine wesentliche Bedeutung zu.

11.9 Meldungen von Verletzungen des Schutzes von personenbezogenen Daten

Weiterhin hoch ist die Zahl der Meldungen von Datensicherheitsverletzungen (Art. 33 DSGVO); sie lag 2023 im mittleren vierstelligen Bereich.

– Noch immer ist nicht bei allen bayerischen öffentlichen Stellen bekannt, dass die Meldepflicht gegenüber der Datenschutz-Aufsichtsbehörde bei einem **Auftragsverarbeitungsverhältnis den Auftraggeber trifft**, während die Meldepflicht des Auftragnehmers grundsätzlich gegenüber dem Auftraggeber zu erfüllen ist.[175] Diese Konstellation hat in letzter Zeit an Bedeutung gewonnen: Cyberangriffe richteten sich zunehmend gegen Rechenzentrendienstleister, in denen auch bayerische öffentliche Stellen ihre Datenbestände hosten. Das Hosting ist typischerweise als Auftragsverarbeitung ausgestaltet – mit der Folge, dass die Rechenzentren ihren Kunden Datensicherheitsverletzungen melden müssen. Leider musste ich immer wieder feststellen, dass betroffene Stellen zwar in den Medien genannt wurden, mir gegenüber jedoch inaktiv blieben. Mitunter wurde auch die Meldung des Auftragsverarbeiters „durchgereicht", wobei eine eigene Risikobewertung in Bezug auf die konkret betroffenen Datensätze unterblieb, die der Auftragsverarbeiter oftmals nicht leisten kann.

  Wenngleich **Hackerangriffe** mittlerweile der zweithäufigste Gegenstand von Meldungen nach Art. 33 DSGVO sind, hielten sich auf dem „Spitzenplatz" weiterhin Datensicherheitsverletzungen durch **unbeabsichtigten Fehlversand** von personenbezogenen Daten. So gingen im Gesundheitsbereich beispielsweise Abrechnungen oder Arztbriefe unberechtigten Empfängerinnen oder Empfängern zu. Solange Empfängerin oder Empfänger die „falsche" Ärztin oder der „falsche" Arzt, ein Krankenversicherungsträger, eine Reha-Einrichtung oder eine ähnliche Stelle ist, sind diese Unterlagen zwar in der Regel durch dort zu beachtende Verschwiegenheitspflichten geschützt. Das Risiko für betroffene Personen ist dann oft als eher gering zu werten – dennoch kann es auch hier zu einer gravierenden Panne kommen, wenn etwa ein Patient explizit nicht will, dass ein bestimmter Arzt den Arztbrief erhält. Ähnlich verhält es sich beim Fehlversand an Familienangehörige. Auch in scheinbaren „Routinefällen" ist also eine einzelfallspezifische Risikobewertung angezeigt. Auf dieser Grundlage kann der Verantwortliche dann auch entscheiden, ob zusätzlich zur Meldung an die

[175] Näher Bayerischer Landesbeauftragter für den Datenschutz, Meldepflicht und Benachrichtigungspflicht des Verantwortlichen, Orientierungshilfe, Stand 6/2019, Rn. 88 ff., Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018".

Datenschutz-Aufsichtsbehörde betroffene Personen zu benachrichtigen sind (vgl. Art. 34 DSGVO).

– Probleme bereitet immer wieder die **automatisierte Erstellung von Serienbriefen**. Hier kommt es – wie die bei mir eingehenden Meldungen von Datenpannen zeigen – recht häufig zu fehlerhaften Adresszuordnungen. Serienbrieffunktionen sollten trotz der auf den ersten Blick eindrucksvollen Arbeitserleichterung nur (strikt) kontrolliert zum Einsatz kommen. Stets geboten ist eine Plausibilitätskontrolle vor dem Versand anhand einer geeignet großen Stichprobe. Der Umfang hängt von der Länge der Adressliste ab – in der Praxis erwies sich eine Stichprobe von 25 Adressierungen bei (nur) rund 150 Empfängern als deutlich zu klein.

– Verletzungspotenzial birgt ferner die **Kommunikation per E-Mail**, die nach wie vor oftmals unverschlüsselt stattfand. Ich möchte daher noch einmal auf den Beitrag zu diesem Thema in meinem 26. Tätigkeitsbericht 2013/2014 unter Nr. 3.6.6 hinweisen.

  Zudem wurden mir weiterhin Fälle bekannt, in denen Verteilerlisten an mehrere Empfängerinnen und Empfänger ohne **Blind-Carbon-Copy** (BCC) als Adressoption versendet worden sind, wodurch alle Adressatinnen und Adressaten von den Adressen der jeweils anderen Kenntnis nehmen konnten. Mit diesem Thema habe ich mich bereits in meinem 27. Tätigkeitsbericht 2015/2016 unter Nr. 2.1.3 befasst. Verantwortliche sollten stets überlegen, mit welchen Maßnahmen solche Vorfälle vermieden werden können – in Betracht kommt etwa das standardmäßige Einblenden des BCC-Felds im Mail-Client.

– Nicht wenige Datenpannenmeldungen erreichten mich schließlich aus **Kliniken**, wenn Beschäftigte auf Patientendaten außerhalb ihres Behandlungsrahmens zugegriffen haben. Umfassende weiterführende Hinweise zu solchen **Neugierzugriffen**, bei denen Zugriffsrechte missbräuchlich genutzt werden, finden sich in meinem 32. Tätigkeitsbericht 2022 unter Nr. 12.8.

Auch **Witterungseinflüsse** sorgten im Berichtsjahr wieder für eine gemeldete Datenpanne (siehe bereits mein 31. Tätigkeitsbericht 2021 unter Nr. 10.9):

Eine Beschäftigte einer bayerischen öffentlichen Stelle befand sich im Hochsommer auf Dienstfahrt mit einem Kraftwagen. Dabei hatte sie Unterlagen mit personenbezogenen Daten in Form einer losen, mehrseitigen Liste ungesichert auf die Rückbank gelegt. Aufgrund des heißen Wetters fuhr die Beschäftigte mit offenem Fenster. Da sie wegen eines Termins in Eile war, beschleunigte sie so stark, dass durch den entstehenden Luftzug einige Blätter aus der Liste gelöst wurden. Sie konnte zwar beinahe alle Blätter noch auffangen, eines war jedoch bereits durchs Fenster geweht worden und nicht mehr auffindbar.

11.10 Umgang mit Video-/Fotokameras

Sowohl in öffentlichen Krankenhäusern als auch in kommunalen Kindertagesstätteneinrichtungen kommen immer wieder Kameras abhanden, auf denen Video- und Fotoaufnahmen von Patienten oder Kindern gespeichert sind. Gerade in Kindertagesstätten werden häufiger Aufnahmen der Spielsituation zu pädagogischen

Zwecken gemacht. Die Kameras werden leider immer wieder nicht auffindbar verlegt, „im Vorbeigehen“ gestohlen oder sogar im Rahmen von Einbrüchen gewaltsam entwendet. In beiden Fällen handelt es sich um Daten, die einen besonderen Schutzbedarf haben.

Diese Vorfälle machen deutlich, wie wichtig ein sorgfältiger Umgang mit diesen Geräten ist. Die technische Ausrüstung, mit der Fotos oder Videoaufzeichnungen zu dienstlichen Zwecken aufgenommen werden, ist mit der gleichen Sorgfalt aufzubewahren wie Laptops oder Dienst-Smartphones. Sie sollte grundsätzlich in einem verschlossenen Raum oder Schrank aufbewahrt werden. Zutritt und Zugriff zu den technischen Geräten und zu gespeicherten Aufzeichnungen darf nur erhalten, wer dies zur Erfüllung seiner Aufgaben benötigt. Insbesondere sollten sie auch nicht kurzzeitig in Bereichen, zu denen auch Besucherinnen und Besucher, Eltern oder Patientinnen und Patienten Zugang haben, offen liegen gelassen werden.

Da diese Maßnahmen allerdings gegen Einbrüche nur einen beschränkten Schutz bieten, ist insbesondere darauf zu achten, dass die Fotos und Videoaufzeichnungen so bald wie möglich von der Kamera gelöscht werden. Dies entspricht auch den Anforderungen and die Datensparsamkeit. Werden Aufzeichnungen über einen längeren Zeitraum benötigt, so sollten die Daten im Idealfall direkt nach der Aufnahme in ein zentrales IT-System übermittelt werden; im Fall eines Krankenhauses etwa an das Krankenhausinformationssystem (KIS) und im Fall der Kindertagesstätte beispielsweise an einen Server des Trägers in einem geschützten Serverraum.

11.11 Anweisung gemäß Art. 58 Abs. 2 Buchst. d DSGVO wegen Defiziten bei einem Rollen- und Berechtigungskonzept

Krankenhäuser verarbeiten in zunehmendem Umfang Patientendaten in elektronischer Form im Krankenhausinformationssystem (KIS) und daran angegliederten Subsystemen. Bereits im Jahr 2014 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hierzu eine **Orientierungshilfe (OH KIS, 2. Fassung)** verabschiedet, die Anforderungen an eine datenschutzgerechte rechtliche und technisch-organisatorische Ausgestaltung des KIS formuliert (siehe mein 25. Tätigkeitsbericht 2011/2012 unter Nr. 7.2). In der Folgezeit habe ich die Umsetzung dieser Orientierungshilfe in bayerischen öffentlichen Krankenhäusern immer wieder beratend begleitet und geprüft (siehe mein 26. Tätigkeitsbericht 2013/2014 unter Nr. 2.2.3).

Umfangreiche Mängel musste ich in einem bayerischen öffentlichen Klinikum bereits 2019 im Rahmen einer Vor-Ort-Prüfung feststellen. Hier bestand weder ein schriftlich dokumentiertes noch im KIS in ausreichendem Maße implementiertes **Rollen- und Berechtigungskonzept**. Dies führe dazu, dass im Klinikum tätiges medizinisches Personal (sowohl Ärztinnen und Ärzte als auch Pflegekräfte) weit über ihren Zuständigkeits- und Fachbereich hinaus Zugriffsrechte auf sensible Patientendaten hatten. Über die für einen weiten Kreis der Mitarbeiterschaft zugängliche Suchfunktion konnten letztlich Daten zu allen seit Einführung des KIS behandelten Patientinnen und Patienten abgerufen werden.

Ich habe das Klinikum – auch in Anbetracht der COVID-19-Pandemie – über einen längeren Zeitraum bei dem Versuch begleitet, die festgestellten Mängel zu beheben. Dabei kam es immer wieder zu Verzögerungen und Problemen bei der Um-

setzung eines geeigneten Rollen- und Berechtigungskonzepts, so dass im Berichtszeitraum vermehrt Art. 33 DSGVO-Meldungen zu unbefugten Zugriffen durch Beschäftigte bei mir eingingen. Dabei wurden mehrmals Personen im Verwandten- und Bekanntenkreis ohne deren Kenntnis abgefragt und die gewonnenen Informationen zu eigenen Zwecken verwendet. Mir blieb schließlich nur, das Klinikum nach Art. 58 Abs. 2 Buchst. d DSGVO unter Androhung eines Zwangsgelds zur Umsetzung eines adäquaten Rollen- und Berechtigungskonzepts anzuweisen, um eine Behebung der bestehenden Missstände zu erreichen. Da sich das Klinikum im Wettbewerb mit nicht-öffentlichen Krankenhäusern befindet, wäre auch die Verhängung eines Bußgelds nach Art. 83 DSGVO möglich gewesen. Da es jedoch nicht mein primäres Ziel ist, das Klinikum finanziell zu schädigen, sondern einen datenschutzkonformen Zustand herzustellen, habe ich von dieser Möglichkeit einstweilen noch Abstand genommen, behalte mir dies aber für vergleichbare Fälle ausdrücklich vor.

11.12 Forschungsprojekt RACOON, Anonymisierung/Pseudonymisierung und KI in der medizinischen Forschung

Seit April 2022 habe ich mich im Rahmen meiner Beteiligung an der Taskforce Forschungsdaten der DSK ausführlich mit dem Projekt RACOON (Radiological Cooperative Network) befasst, an dem alle deutschen Universitätsklinika beteiligt sind. Im Rahmen dieses Projekts wurde eine bundesweite Netzwerkinfrastruktur zur strukturierten Erfassung, Bereitstellung und Zusammenführung radiologischer Daten von COVID-19-Fällen geschaffen. Neben der eigentlichen Beantwortung von Forschungsfragen, wie dies auch in der Vergangenheit in multizentrischen Projekten üblich war, steht in diesem Projekt speziell das Thema Maschinelles Lernen (ML)/Künstliche Intelligenz (KI) mit im Zentrum. Im Rahmen des Projekts sollen ML-/KI-Verfahren zur Auswertung von Bilddaten entwickelt (die erhobenen radiologischen Daten werden als Trainingsdaten für ML/KI verwendet) als auch Forschungsfragen unter Hinzuziehung von ML/KI beantwortet werden. Das Projekt wirft eine Vielzahl interessanter Fragen aus Sicht des technisch-organisatorischen Datenschutzes auf, deren Beantwortung auch für andere Projekte in diesem Bereich von Bedeutung ist.

Zentral ist die Frage, ob die im Projekt verarbeiteten Daten anonymisiert sind oder ob nur eine Pseudonymisierung möglich ist. Die Datenschutz-Grundverordnung enthält keine Definition der Anonymisierung; das Verständnis ist uneinheitlich.

Der Europäische Datenschutzausschuss überarbeitet derzeit die Leitlinien zur Anonymisierung und Pseudonymisierung, hinsichtlich der Begrifflichkeit und der praktischen Umsetzung und Bewertung von technisch-organisatorischen Maßnahmen mehr Klarheit zu schaffen.

Allgemein ist beim Einsatz von Anonymisierungstechniken zu beachten, dass eine (Re-)Identifizierung nicht nur dann möglich sein kann, wenn Datensätze die identifizierenden Daten eines Patienten (insbesondere den Namen) enthalten, sondern auch, wenn ein Datensatz in verschiedenen Datenbeständen wiedererkannt werden kann und somit eine Profilbildung möglich wäre. Für die Beurteilung der Frage der Anonymisierung im Rahmen von Projekten wie RACOON spielen daher etwa folgende Kriterien eine Rolle:

— **Nutzung großer Datenmengen, Verknüpfung von Datenbeständen:** Je umfassender, strukturierter und feingranularer ein Datenbestand zu einer

Person ist und je mehr Forscherinnen und Forscher diesen Datenbestand über längere Zeiträume nutzen können, umso wahrscheinlicher wird es, dass Daten über einen Abgleich oder eine Verknüpfung mit anderen Datenbeständen sowie Zusatzwissen aus anderen Quellen reidentifiziert werden können.

- **Nutzung von Radiologiedaten:** Bilddaten wurden in der Vergangenheit in vielen Fällen als anonymisiert angesehen, wenn gewisse Bereiche wie etwa der Kopf nicht erfasst waren und die Metadaten entfernt wurden. Durch die Verwendungen von ML/KI-Verfahren, deren besondere Stärke das Finden von Korrelationen in großen Datenbeständen ist, muss diese Einschätzung jedoch kritisch hinterfragt werden, gerade wenn derartige Datenbestände auch anderen Forschergruppen (die wiederum Zugang zu weiteren Datenbeständen haben) zugänglich gemacht werden. Dies machen auch erste Forschungsarbeiten im Bereich der Reidentifizierung von Daten deutlich.[176]

- **Datennutzung zum Training von ML/KI-Verfahren:** ML/KI-Verfahren werden auf Basis von Daten trainiert. Soweit es sich nicht sicher um anonyme oder anonymisierte Daten handelt, besteht ein gewisses Risiko der Extraktion von personenbezogenen Trainingsdaten und somit einer Reidentifizierung, auch wenn die Trainingsdaten eigentlich nicht mit dem ML/KI-Verfahren „mitgeliefert" werden (Schlagwort „memorization").[177] Dies muss gerade bei sensiblen medizinischen Daten sicher verhindert werden.

- **Nutzung von ML/KI-Verfahren im Behandlungszusammenhang zur Beantwortung von Forschungsfragen:** Häufig liefern gängige ML/KI-Verfahren zwar ein Ergebnis, die Nutzerin oder der Nutzer hat jedoch keine Möglichkeit zu überprüfen, aufgrund welcher Informationen und Bewertungen das ML/KI-Verfahren auf dieses Ergebnis gekommen ist. Dies entspricht nicht den in der Datenschutz-Grundverordnung verankerten Transparenzanforderungen, die greifen, sobald eine Verarbeitung von personenbezogenen oder personenbeziehbaren Daten nicht sicher ausgeschlossen werden kann, und kann auch aus Sicht der ärztlichen Haftung zu Schwierigkeiten führen. Werden daher im Rahmen von Forschungsprojekten ML/KI-Verfahren entwickelt, sollten die Aspekte der Transparenz und Nachvollziehbarkeit mitberücksichtigt werden.

- **Berücksichtigung der Verordnung über Künstliche Intelligenz:** Dieser europäische Rechtsakt, der nach dem Berichtszeitraum in Kraft getreten ist, aber noch nicht gilt,[178] sieht Risikoklassen bezüglich ML/KI-Verfahren vor,

[176] Beispielsweise Packhäuser u. a., Deep learning-based patient re-identification is able to exploit the biometric nature of medical chest X-ray data, Sci Rep 12, 14851 (2022), Internet: https://doi.org/10.1038/s41598-022-19045-3.

[177] Siehe etwa Carlini u. a., Extracting Training Data from Large Language Models, Internet: https://www.usenix.org/conference/usenixsecurity21/presentation/carlini-extracting.

[178] Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L 2024/1689 vom 12. Juli 2024).

aus denen sich die erforderlichen Maßnahmen oder auch Nutzungsbeschränkungen ergeben. Auch für Forschungsprojekte im Gesundheitsbereich, die ML/KI-Verfahren nutzen oder entwickeln, sollten daher frühzeitig die Einstufung und ihre Folgen geprüft werden. Dabei ist insbesondere zu beachten, dass auch hier eine Rechtsgrundlage für die Verwendung von personenbezogenen Daten zu Trainingszwecken erforderlich ist: Die Verordnung über Künstliche Intelligenz sieht zukünftig außerdem die Einführung von „KI-Reallaboren" vor, in denen neue Technologien erprobt werden können. Dort sollen auch medizinische Daten verarbeitet werden können, die rechtmäßig erhoben sind.

11.13 Anforderungen an Kontaktinformation zum behördlichen Datenschutzbeauftragten: inkonsistente Information für eine Kontaktaufnahme mit dem Datenschutzbeauftragten

Im Rahmen einer Eingabe habe ich festgestellt, dass eine bayerische Kommune in unterschiedlichen Bereichen ihres Internetauftritts Kontaktdaten für ihren behördlichen Datenschutzbeauftragten auswies. Die Kontaktdaten waren jedoch teilweise veraltet und stimmten nicht überein. Diese inkonsistente Information konnte dazu führen, dass Bürgerinnen und Bürger im Zusammenhang mit datenschutzrechtlichen Fragestellungen zu Personen, die nicht als behördlicher Datenschutzbeauftragter von der Kommune benannt waren, in der Annahme, mit dem Datenschutzbeauftragten zu sprechen, Kontakt aufnahmen. Die oder der aktuelle Datenschutzbeauftragte ist auch nicht immer bei mir gemeldet oder im BayernPortal angegeben. Bayerische öffentliche Stellen sind gemäß Art. 37 Abs. 7 DSGVO verpflichtet, die Kontaktdaten ihrer oder ihres Datenschutzbeauftragten geeignet zu veröffentlichen und an mich zu melden, insbesondere auch im Falle von Änderungen. Genaueres hierzu kann in meiner einschlägigen Orientierungshilfe nachgelesen werden.[179]

[179] Bayerischer Landesbeauftragter für den Datenschutz, Der behördliche Datenschutzbeauftragte, Stand 5/2018, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018".

12 Datenschutzkommission

Der Datenschutzkommission beim Bayerischen Landtag gehörten zu Beginn der 19. Wahlperiode folgende Mitglieder und stellvertretende Mitglieder an:

Aus dem Landtag:

Mitglieder:

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

Stellvertretende Mitglieder:

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

Auf Vorschlag der Staatsregierung:

Mitglied:

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

Stellvertretendes Mitglied:

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

Auf Vorschlag der kommunalen Spitzenverbände in Bayern:

Mitglied:

Rudolf Schleyer, Vorstandsvorsitzender der Anstalt für Kommunale Datenverarbeitung in Bayern

Stellvertretendes Mitglied:

Cynthia Derra, Datenschutzbeauftragte des Bayerischen Landkreistags

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

Mitglied:

Werner Krempl, Erster Direktor und Geschäftsführer der Deutschen Rentenversicherung Nordbayern

Stellvertretendes Mitglied:

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

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

Mitglied:

Dr. Till Schemmann, Notar

Stellvertretendes Mitglied:

Dr. Thomas Kuhn, Rechtsanwalt

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

Die Datenschutzkommission beim Bayerischen Landtag tagte im Berichtszeitraum zwei Mal.

13 Ländervertreter im EDSA

Der Bundesrat hat mich 2021 gemäß § 17 Abs. 1 Satz 2 Bundesdatenschutzgesetz für fünf Jahre zum Ländervertreter im Europäischen Datenschutzausschuss (EDSA) gewählt (allgemein zu diesem Ausschuss und zu meinen Aufgaben als Ländervertreter siehe meinen 31. Tätigkeitsbericht 2021 unter Nr. 12). Der EDSA hat 2023 insgesamt 15-mal getagt. Um die europaweit einheitliche Anwendung des Datenschutzrechts zu gewährleisten, hat der EDSA insbesondere Leitlinien erlassen und Empfehlungen ausgesprochen, Stellungnahmen in Rechtsetzungsverfahren abgegeben sowie Meinungsverschiedenheiten zwischen einzelnen Aufsichtsbehörden entschieden (vgl. Art. 70 Abs. 1 DSGVO). Durch diese Tätigkeiten trägt der EDSA in besonderem Maße zu einer verbesserten Zusammenarbeit der Aufsichtsbehörden in grenzüberschreitenden Sachverhalten bei.

Besonders hervorheben möchte ich folgende Maßnahmen des EDSA im Berichtsjahr:

— die redaktionelle Überarbeitung der Leitlinien 01/2022 zu den Rechten der betroffenen Personen – Recht auf Auskunft;[180]

— die Überarbeitung der Leitlinien 05/2022 für den Einsatz von Gesichtserkennungstechnologie im Bereich der Strafverfolgung hinsichtlich Aspekten der menschlichen Intervention, der Rechenschaftspflicht und Risiken betreffend das Recht auf ein faires Verfahren sowie der Unschuldsvermutung;[181]

— die Verabschiedung der Leitlinien 04/2022 zur Berechnung von Bußgeldern;[182]

— die Leitlinien 01/2023 zu Art. 37 RLDSJ zu „geeigneten Garantien“ bei der Übermittlung von Daten an Drittstaaten und Internationale Organisationen;[183]

— die Gemeinsamen Stellungnahmen des EDSA und des Europäischen Datenschutzbeauftragten zum Vorschlag der Europäischen Kommission für eine Verordnung zur Einführung des digitalen Euro,[184] die insbesondere einen stärkeren Datenschutz durch Technikgestaltung sowie datenschutzfreundliche Voreinstellungen fordert, und zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung zusätzlicher Verfahrensvorschriften für die Durchsetzung der Datenschutz-

[180] Internet: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_en.
[181] Internet: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en
[182] Internet: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_de.
[183] Internet: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2023/guidelines-012023-article-37-law-enforcement_en.
[184] Internet: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-022023-proposal_en.

Grundverordnung,[185] mit der die Zusammenarbeit der Aufsichtsbehörden der EU-Mitgliedstaaten und des EWR verbessert werden soll;

— die Verbindlichen Beschlüsse 1/2023[186] und 2/2023[187] in Streitbeilegungsverfahren betreffend den Datenschutz in sozialen Netzwerken sowie in diesem Zusammenhang die Anweisung einer Datenschutzaufsichtsbehörde, endgültige Maßnahmen zu erlassen.[188]

Die angesprochenen Dokumente sowie umfangreiche weitere den EDSA betreffende Informationen können unter https://edpb.europa.eu/edpb_de abgerufen werden.

[185] Internet: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-012023-proposal_de.

[186] Internet: https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12023-dispute-submitted_de.

[187] Internet: https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22023-dispute-submitted_de.

[188] Internet: https://edpb.europa.eu/our-work-tools/our-documents/urgent-binding-decision-board-art-66/urgent-binding-decision-012023_de.

Abkürzungsverzeichnis

ABl.	Amtsblatt der Europäischen Union
Abs.	Absatz
a. F.	alte Fassung
AfD	Alternative für Deutschland
Art.	Artikel
Aufl.	Auflage
BayDSG	Bayerisches Datenschutzgesetz
BeckRS	Beck-Rechtsprechung (Datenbank)
BDSG	Bundesdatenschutzgesetz
BGBl.	Bundesgesetzblatt
Buchst.	Buchstabe
bzw.	beziehungsweise
CSU	Christlich-Soziale Union in Bayern
DSFA	Datenschutzfolgenabschätzung
DSGVO	Datenschutz-Grundverordnung
EDV	Elektronische Datenverarbeitung
EG	Erwägungsgrund
FDP	Freie Demokratische Partei
ff.	(nach)folgende
GVBl.	Bayerisches Gesetz- und Verordnungsblatt
https	Hyper Text Transfer Protocol Secure
IP	Internet Protocol
IT	Informationstechnik
MdL	Mitglied des Landtages
Nr.	Nummer
PC	Personalcomputer
RLDSJ	Datenschutz-Richtlinie für Polizei und Strafjustiz
Rn.	Randnummer
sog.	sogenannt
SPD	Sozialdemokratische Partei Deutschlands
SSL	Secure Socket Layer
u. a.	unter anderem/und andere
UAbs.	Unterabsatz
vgl.	vergleiche
www	World Wide Web

Stichwortverzeichnis