Der Bayerische Landesbeauftragte für den Datenschutz informiert die Öffentlichkeit

29. Tätigkeitsbericht

Berichtszeitraum
2019

29. Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz

gemäß Art. 59 Datenschutz-Grundverordnung

Berichtszeitraum: 1. Januar 2019 bis 31. Dezember 2019
Veröffentlichungsdatum: 25. Mai 2020

Inhaltsverzeichnis

Hinweis zu Abkürzungen

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

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

1 Überblick

1.1 Künstliche Intelligenz und Datenschutz

Mit der „Hightech Agenda Bayern“ hat die Bayerische Staatsregierung am 10. Oktober 2019 erhebliche Investitionen in die Entwicklung von Künstlicher Intelligenz (KI) und „SuperTech“ angekündigt. Mit insgesamt rund 2 Milliarden Euro will die Staatsregierung die Beforschung und Entwicklung von Künstlicher Intelligenz und von zukunftsträchtigen Technologien wie Quantentechnologie, Luft- und Raumfahrt sowie Klimabezogene Technologien (CleanTech) fördern.

Die Hightech Agenda Bayern steht inhaltlich in einem engen Zusammenhang mit der Gründung des Bayerischen Instituts für Digitale Transformation durch die Staatsregierung im Juni 2018, das den Auftrag hat, ein fundiertes Verständnis der digitalen Transformation zu erarbeiten, auf dessen Basis bestehende Stärken Bayerns, Deutschlands und Europas in der digitalen Welt ausgebaut und neu entwickelt werden können.

Nach meiner persönlichen Überzeugung wird es keine Frage sein, **ob** unsere Gesellschaft künftig mit KI-Systemen leben wird – das wird sie. Vielmehr lautet die entscheidende Frage, **wie** unsere Gesellschaft mit KI leben soll. Angesprochen sind damit zahlreiche soziale und ethische Gesichtspunkte, die nur im Diskurs zwischen Politik, Gesellschaft und Wissenschaft geklärt werden können.

Als Bayerischer Landesbeauftragter für den Datenschutz würde ich es begrüßen, wenn der Freistaat Bayern mit seiner Initiative einen gewichtigen Beitrag zu einer Entwicklung von Künstlicher Intelligenz leistet, die auf der Grundlage europäischer Werte steht. Angesprochen sind damit vor allem die Freiheitsgewährleistungen, wie sie in der Verfassung des Freistaates Bayern, im Grundgesetz für die Bundesrepublik Deutschland und in der Charta der Grundrechte der Europäischen Union garantiert werden. Letztlich geht es darum, wie auch im Zeitalter der digitalen Transformation die Achtung der Menschenwürde gewährleistet werden kann.

Soweit mit der Anwendung von KI auch eine Verarbeitung personenbezogener Daten erfolgt, hat der Datenschutz die Aufgabe, die neuen Technikentwicklungen im Sinne des Persönlichkeitsrechtsschutzes aktiv zu begleiten. Insoweit sind der Einsatz von KI-Systemen und der Datenschutz keine Gegensätze; vielmehr ist Datenschutz eine zentrale Voraussetzung für eine menschenfreundliche KI. Dabei hat KI den datenschutzrechtlichen Regeln insbesondere der Datenschutz-Grundverordnung zu folgen. Insbesondere bei regelbasierten KI-Systemen, die in sensiblen Lebensbereichen Entscheidungen unterstützen oder selbst treffen sollen, kommt es darauf an, dass sie die Regeln transparent machen, die hauptursächlich für eine konkrete automatisierte Entscheidung oder einen Entscheidungsvorschlag gewesen sind. Insoweit dürften für die Datenschutzaufsicht kurz- und mittelfristig beispielsweise Scoring-Systeme, medizinische Diagnosesysteme und das autonome Fahren relevant werden. Nach meiner Einschätzung sind die beiden bayerischen Datenschutz-Aufsichtsbehörden gegenwärtig noch nicht in der Lage, KI-Anwendungen im Sinne des Grundrechtsschutzes effektiv zu überprüfen. Dazu müssten sie entsprechend ertüchtigt werden.

Die 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) hat eine „Hambacher Erklärung zur Künstlichen Intelligenz“ verabschiedet, die einige datenschutzrechtliche Kernanforderungen an die Entwicklung von KI formuliert. Die 98. Datenschutzkonferenz hat die Hambacher Erklärung am 6. November 2019 durch Empfehlungen für eine datenschutzkonforme Gestaltung von KI-Systemen ergänzt. Die Empfehlungen in Gestalt eines Positionspapiers sind diesem Tätigkeitsbericht als Anlage 1 beigegeben.

Die datenschutzrechtlichen Grundlagen für die Entwicklung von KI werden in Abschnitt 12.1 näher beleuchtet.

1.2 Evaluierung der Datenschutz-Grundverordnung (DSGVO)

Nach Art. 97 Abs. 1 DSGVO hat die Europäische Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung der Datenschutz-Grundverordnung vorzulegen (Evaluierung). Der Europäische Datenschutzausschuss (EDSA) hat dazu am 18. Februar 2020 einen gemeinsamen Antwortbeitrag zur Evaluierung der DSGVO beschlossen. Die Europäische Kommission hatte den EDSA um einen Beitrag zum Evaluierungsverfahren gebeten. Der Ausschuss hat in seiner Antwort die Bedeutung der Datenschutz-Grundverordnung für den Schutz und die Stärkung des Grundrechts auf Datenschutz innerhalb der EU hervorgehoben. In die Stellungnahme eingeflossen war auch die Position der deutschen Aufsichtsbehörden, die im Berichtszeitraum entstanden ist und an der ich mitgewirkt habe (vgl. Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DSGVO vom November 2019, Internet: https://www.datenschutzkonferenz-online.de, Rubrik „Infothek – Beschlüsse“).

1.3 Das neue Polizeiaufgabengesetz

Im Mai 2018 hat der bayerische Gesetzgeber eine umfassende Neuordnung des Polizeiaufgabengesetzes (PAG) verabschiedet. Im Vorfeld des Inkrafttretens hatte ich mich wiederholt sehr kritisch zu einigen im Gesetzentwurf vorgesehenen neuen Befugnissen geäußert, allerdings auch auf einige positive Aspekte des Vorhabens hingewiesen. Nach wie vor halte ich beispielsweise die neuen Regelungen der Art. 37 und 38 PAG zum Einsatz von verdeckten Ermittlern und von Vertrauensleuten jedenfalls im Grundsatz für einen rechtsstaatlichen Gewinn. Meine umfassende Stellungnahme im Rahmen der Verbandsanhörung ist auf meiner Webseite https://www.datenschutz-bayern.de in der Rubrik „Themengebiete – Polizei“ veröffentlicht.

1.3.1 Kommission zur Begleitung des neuen Polizeiaufgabengesetzes

Das Gesetz zur Neuordnung des bayerischen Polizeirechts wurde politisch heftig angegriffen und ist noch Gegenstand verfassungsgerichtlicher Verfahren. Vor dem Hintergrund dieser Kritik beauftragte der Ministerrat mit Beschluss vom 12. Juni 2018 den Bayerischen Staatsminister des Innern und für Integration damit, eine Kommission zur Begleitung des neuen Polizeiaufgabengesetzes (PAG-Begleitkommission) unter Vorsitz des Präsidenten des Bayerischen Verfassungs-

gerichtshofs a. D. Dr. Karl Huber einzurichten. Der Auftrag der Kommission bestand in einer „unabhängigen Begleitung und Prüfung der Anwendung des Polizeiaufgabengesetzes“. Mit anderen Worten sollte die Kommission nicht neu eingefügte Befugnisse verfassungsrechtlich beurteilen, sondern sie sollte überprüfen, wie die Polizei die Vorschriften konkret im Vollzug handhabt.

Auch ich wurde zu einem Mitglied der PAG-Begleitkommission bestellt. Ich habe diese Bestellung als ein Ersuchen der Bayerischen Staatsregierung im Sinne des Art. 15 Abs. 3 BayDSG gewertet, zu den tatsächlichen Vollzugsgegebenheiten Stellung zu nehmen. Gleichwohl hatte ich zunächst Bedenken gegen eine solche Bestellung. Denn zum einen evaluierte die PAG-Begleitkommission nicht nur neue Bestimmungen mit Datenschutzbezügen. Vor allem aber durfte die Tätigkeit in der PAG-Begleitkommission nicht meine unabhängige Amtsführung beeinträchtigen. Deshalb machte ich gegenüber der Staatsregierung ausdrücklich einen Beitritt in dieses Gremium davon abhängig, dass die Mitgliedschaft meine unabhängige Amtsführung im Übrigen unberührt lässt. Dieses Anliegen haben die Staatsregierung und die PAG-Begleitkommission gleichermaßen vollumfänglich respektiert. Dementsprechend sind beispielsweise meine Erkenntnisse aus konkreten Bürgereingaben schon deshalb nicht in die Arbeit der PAG-Begleitkommission eingeflossen, weil ich insoweit einer Schweigepflicht unterliege.

1.3.2 Abschlussbericht der PAG-Begleitkommission

Die PAG-Begleitkommission hat ihren Auftrag mit Abgabe eines Abschlussberichts vom 30. August 2019 erfüllt. Die Empfehlungen der PAG-Begleitkommission zum Gesetzesvollzug und zur Änderung des Gesetzes habe ich sehr weitgehend mittragen können. Allerdings hatte ich bereits im Vorfeld der Kommissionstätigkeit rechtliche Stellungnahmen etwa zur drohenden Gefahr abgegeben. An diesen Stellungnahmen halte ich auch weiterhin fest, wie im Abschlussbericht auch vermerkt ist.

Insgesamt habe ich den Eindruck, dass die Arbeit der Kommission zur Versachlichung der sehr kontrovers geführten Diskussion um die Neuordnung des bayerischen Polizeirechts beitragen konnte. Deshalb würde ich es begrüßen, wenn die Staatsregierung die Empfehlungen der Kommission aufgreifen würde.

Ich mache allerdings auch darauf aufmerksam, dass die Kommission nicht alle datenschutzrechtlich problematischen Regelungen des neuen Polizeirechts evaluieren konnte. Nicht untersucht wurde beispielsweise die Durchsuchung von elektronischen Speichermedien in Art. 22 Abs. 2 PAG, die dringend strenger gefasst und unter grundsätzlichen Richtervorbehalt gestellt werden sollte.

Der Abschlussbericht der PAG-Begleitkommission ist gegenwärtig im Internet unter https://www.polizeiaufgabengesetz.bayern.de abrufbar.

1.4 Gesundheitseinrichtungen: Datensicherheitsvorfälle nehmen zu

Die Zahl der bekannten Pannen bei Datensicherheit und Datenschutz in Kliniken hat im Jahr 2019 deutlich zugenommen. Das zeigt: Viele Krankenhäuser setzen wichtige datenschutzrechtliche und sicherheitstechnische Vorgaben nicht ausreichend um.

Nach der Datenschutz-Grundverordnung dürfen personenbezogen Daten nur verarbeitet werden, wenn es dafür eine Rechtsgrundlage gibt. Und schon die Möglichkeit des Zugriffs ist als Bereitstellung personenbezogener Daten eine solche Verarbeitung. Bei Gesundheitsdaten ist zudem Art. 9 DSGVO zu beachten, der ein grundsätzliches Verarbeitungsverbot vorsieht. Solche Daten unterliegen zudem nach straf- und berufsrechtlichen Regelungen einem besonderen Vertraulichkeitsschutz.

Zur Absicherung einer rechtskonformen Verarbeitung von Gesundheitsdaten verlangt das Datenschutzrecht gemäß Art. 24, 25 und 32 DSGVO spezifische technisch-organisatorische Schutzmaßnahmen auf mehreren Ebenen: Dies betrifft zum einen die Basis-IT-Sicherheit der eingesetzten Netzwerke, Komponenten und Software, zum anderen die speziellen Anforderungen an ein datenschutzgerechtes Klinikinformationssystem. Hierzu gehört auch die beim Klinikpersonal unbeliebte Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle. Sie lässt sich vereinfacht durch das Need-to-Know-Prinzip ausdrücken: Personal, das keinen Zugang zu den Daten haben muss – weil es etwa nicht an der Behandlung von Patieninnen und Patienten beteiligt ist – darf insoweit auch keinen Zugang zu den Patientendaten erhalten. Die Klinikverantwortlichen haben diese Beschränkung auf erforderliche Zugriffe im Rahmen von Berechtigungskonzepten sicherzustellen. Sie sind ein elementarer Baustein des technisch-organisatorischen Datenschutzes und eine zentrale Voraussetzung für den Schutz der Integrität und Vertraulichkeit von Patientendaten. Der Schutz vor unbefugter Verarbeitung stellt einen zentralen Datenschutzgrundsatz dar, für dessen Beachtung der Krankenhausbetreiber verantwortlich ist.

Im Ergebnis geht es dabei nicht darum, dem Klinikpersonal Datenzugriffe zu verweigern, die es für eine effektive Behandlung benötigt. Vielmehr sollen unbefugte Zugriffe im Rahmen des technisch Möglichen erschwert werden.

Um es ausdrücklich klarzustellen: Natürlich soll Klinikpersonal gerade in Notfallsituationen möglichst schnell und vollständig auf Patientendaten im Klinikinformationssystem zugreifen können. Allerdings darf im digitalen Zeitalter dieser legitime Bedarf nicht dazu führen, dass Kliniken mehr oder weniger aus Bequemlichkeitsgründen grundlegende Datenschutz- und Datensicherheitsvorgaben gänzlich außer Acht lassen. Die eingangs genannten Beispiele verdeutlichen, dass die zentralen datenschutzrechtlichen Prinzipien „Brandschutzmauern“ darstellen, die heutzutage für eine stabile klinische Gesundheitsversorgung unabdingbar sind.

Angesichts zahlreicher schwerwiegender Sicherheitsvorfälle wirkt es auf mich skurril, wenn immer noch ein angeblich zu strenges Datenschutzreglement beklagt und behauptet wird, dieses würde effektive Heilbehandlungen verhindern. Das Gegenteil ist der Fall: Letztlich trägt die Einhaltung der zentralen datenschutzrechtlichen Prinzipien dazu bei, dass auch im Zeitalter der Datenvernetzung, App-Nutzung, elektronischer Patientenakten und Künstlicher Intelligenz eine flächendeckende stabile Gesundheitsversorgung durch sichere und datenschutzgerechte IT-Systeme möglich bleibt.

Allerdings wäre es wünschenswert, wenn Krankenhäuser mit ihrer datenschutzrechtlichen Verantwortlichkeit nicht allein gelassen werden. Kliniken fehlt es oft weniger am guten Willen, sondern vielmehr an der hinreichenden finanziellen Ausstattung. Das gilt namentlich für kleinere Häuser, die nicht auf wichtige Fördermittel für IT-Sicherheit zugreifen können. Vor diesem Hintergrund habe ich im Berichtszeitraum ungeachtet erheblicher Datenschutzverstöße darauf verzichtet,

Bußgelder gegen Kliniken zu verhängen, um nicht die Gelder abzuziehen, welche die betroffenen Häuser zur Ertüchtigung ihrer IT-Sicherheit dringend benötigen. Ich weise allerdings in aller Deutlichkeit darauf hin, dass diese „Schonfrist“ abläuft. Knappe Ressourcen entbinden nicht von der Pflicht, das gesetzlich gebotene Mindestmaß an Datenschutz und Datensicherheit zu gewährleisten.

1.5 Schlussbemerkung

Die nachfolgenden Kapitel geben unter anderem einen Überblick über meine Beteiligung an Gesetzgebungsvorhaben und die Wahrnehmung der Datenschutzaufsicht bei den bayerischen öffentlichen Stellen im Jahr 2019.

2 Allgemeines Datenschutzrecht

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

Verstöße gegen datenschutzrechtliche Vorgaben wie auch Verfehlungen technisch-organisatorischer Standards können Verantwortliche oftmals vermeiden, wenn sie sich mit diesen Vorgaben und Standards sowie mit Instrumenten des Datenschutzes vertraut machen. Ein solcher **präventiver Datenschutz** ist zwar nicht ohne einen gewissen Aufwand an personellen und sachlichen Ressourcen zu haben; langfristig zahlt es sich aber aus, wenn ein Verantwortlicher nicht „alles dem Zufall überlässt“.

Vor diesem Hintergrund habe ich schon vor dem Geltungsbeginn der Datenschutz-Grundverordnung damit begonnen, ein **Informationsangebot** für bayerische öffentliche – insbesondere staatliche und kommunale – Stellen als gemäß Art. 3 Abs. 2 BayDSG datenschutzrechtlich Verantwortliche aufzubauen (siehe bereits meinen 28. Tätigkeitsbericht 2018 unter Nr. 2.1). Im Berichtszeitraum habe ich wiederum zahlreiche neue Orientierungshilfen, Arbeitspapiere und Aktuelle Kurz-Informationen veröffentlicht. Alle diese Materialien stehen auf meiner Internetpräsenz https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018“ zum kostenfreien Abruf bereit.

Meine **Orientierungshilfen** behandeln größere Themenkreise, wobei sie Elemente eines Kommentars mit praktischen Hinweisen verbinden. Bayerische öffentliche Stellen erhalten so das datenschutzfachliche „Rüstzeug“ für eine sichere Rechtsanwendung.

- Im Juni 2019 erschien die Orientierungshilfe **„Meldepflicht und Benachrichtigungspflicht des Verantwortlichen“**. Auf der Grundlage der bisher gewonnenen Erfahrungen greift die Orientierungshilfe zahlreiche Zweifelsfragen auf und erläutert für die bayerische Verwaltungspraxis umfassend die insoweit einschlägigen Vorschriften der Datenschutz-Grundverordnung sowie des bayerischen Landesrechts. Dabei macht die Orientierungshilfe deutlich, dass nicht jeder Verstoß gegen datenschutzrechtliche Vorschriften, sondern nur eine Verletzung der Sicherheit personenbezogener Daten die Melde- und gegebenenfalls auch die Benachrichtigungspflicht auslöst. Sie gibt Rat suchenden öffentlichen Stellen weiterhin Empfehlungen für eine vereinfachte Risikoanalyse sowie für die Nutzung meines mit Geltungsbeginn der Datenschutz-Grundverordnung eingeführten Online-Meldeformulars.

- Im Dezember 2019 habe ich zudem eine Orientierungshilfe **„Das Recht auf Auskunft nach der Datenschutz-Grundverordnung“** bereitgestellt. Das Recht auf Auskunft nach Art. 15 DSGVO nimmt unter den Betroffenenrechten eine Schlüsselfunktion ein. Erst mit einer Auskunft lässt sich die Rechtmäßigkeit einer Verarbeitung der eigenen personenbezogenen Daten realistisch einschätzen. Die Auskunft schafft zudem eine Voraussetzung für den Gebrauch weiterer Betroffenenrechte, insbesondere auf Berichti-

gung und auf Löschung. Seit Geltungsbeginn der Datenschutz-Grundverordnung habe ich zu Art. 15 DSGVO viele Anfragen von Bürgerinnen und Bürgern, aber auch von Behörden beantwortet. In der Orientierungshilfe ist die so gewonnene Beratungspraxis zusammengefasst; die Erläuterungen beziehen überdies zu zahlreichen in Rechtsprechung und Literatur erörterten Fragen Stellung.

— Ausgebaut habe ich mein Informationsangebot zum Themenkreis **„Datenschutz-Folgenabschätzung (DSFA)“**. Die Datenschutz-Folgenabschätzung gab es vor der Datenschutzreform noch nicht. Hat eine Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, muss der für sie Verantwortliche nach dem neuen Recht nun eine Datenschutz-Folgenabschätzung durchführen. Dabei erarbeitet er strukturiert eine Beschreibung der Risiken und setzt ihnen geeignete technische und organisatorische Maßnahmen entgegen. Bayerische Behörden sind für zahllose Datenverarbeitungen verantwortlich. Darunter können sich auch solche Verarbeitungen befinden, die einer Datenschutz-Folgenabschätzung bedürfen.

  Um die Identifizierung von „Hochrisiko-Verarbeitungen“ zu erleichtern, habe ich die **„Bayerische Blacklist“** veröffentlicht, welche die wichtigsten Fälle aufzählt. Dazu bin ich nach der Datenschutz-Grundverordnung im Übrigen verpflichtet (siehe Art. 35 Abs. 4 DSGVO).

  Zur Unterstützung der bayerischen Behörden habe ich außerdem meine bereits Mitte Mai 2018 veröffentlichte **Orientierungshilfe** „Datenschutz-Folgenabschätzung“ überarbeitet und um ein neues, ausführliches **Arbeitspapier zur Methodik** ergänzt. Eine **Fallstudie** zeigt hier beispielhaft, wie eine Datenschutz-Folgenabschätzung IT-gestützt effektiv und effizient erarbeitet werden kann. Sie illustriert zugleich den Nutzen, den dieses Instrument im Rahmen eines geordneten Risikomanagements hat.

  Zur Verfügung gestellt habe ich den bayerischen öffentlichen Stellen zudem eine Software, welche die Durchführung von Datenschutz-Folgenabschätzungen unterstützen soll. Das von der französischen Datenschutz-Aufsichtsbehörde entwickelte **PIA-Tool** liegt nun in deutscher Übersetzung vor. Ergänzend erscheinen sukzessive einige **Werkzeuge**, welche verschiedene Arbeitsschritte der Datenschutz-Folgenabschätzung erleichtern sollen. Alle diese Angebote sind auf meiner Homepage in der Rubrik „DSFA“ näher erläutert (siehe vertiefend auch den Beitrag Nr. 12.2).

— Eine Überarbeitung erfuhr schließlich die Orientierungshilfe **„Auftragsverarbeitung“**, die von Verantwortlichen besonders häufig nachgefragt wird.

Mit den **Arbeitspapieren** habe ich ein neues Format etabliert, das „kleineren“ Themen gewidmet ist.

— Im Berichtszeitraum erschien zunächst das Arbeitspapier **„Verarbeitung von Sozialdaten durch Beistand, Amtspfleger und Amtsvormund“** (Februar 2019), das einen Themenkreis insbesondere aus dem Bereich der Ämter für Kinder, Jugend und Familie aufgreift (siehe näher den Beitrag Nr. 8.1).

- Das Arbeitspapier **„Die förmliche Verpflichtung als Instrument des Datenschutzes“** (September 2019) beantwortet Fragen rund um die Verpflichtung nach dem Verpflichtungsgesetz. Mit diesem Instrument können Personen, die für öffentliche Stellen tätig werden, dem für Beamtinnen und Beamte geltenden strafrechtlichen Vertraulichkeitsschutz unterworfen werden.

- In dem Arbeitspapier **„Offenkundig unbegründete und exzessive Anträge“** (September 2019) geht es dagegen um das Verständnis von Art. 12 Abs. 5 DSGVO, einer Vorschrift, die von Verantwortlichen öfter als rechtsmissbräuchlich eingeschätzten Auskunftsersuchen entgegengehalten wird. Das Arbeitspapier macht deutlich, dass bei der Anwendung dieser Vorschrift Zurückhaltung angezeigt ist.

Meine **Aktuellen Kurz-Informationen** greifen häufige Gegenstände aus der Beratungspraxis auf; vereinzelt ordnen sie auch neue Rechtsprechung ein. Im Berichtszeitraum sind mit den Aktuellen Kurz-Informationen 17 bis 26 insgesamt zehn dieser Beiträge erschienen. Die Reihe wird auch im folgenden Berichtszeitraum fortgesetzt.

Von dem in erster Linie für die Bürgerinnen und Bürger im Freistaat gedachten Buch **„Meine Daten, die Verwaltung und ich“** habe ich zunächst im Juli 2019 eine erste Auflage elektronisch zur Verfügung gestellt. Die durchgesehene zweite Auflage kann seit Dezember 2019 auch in gedruckter Fassung kostenfrei bezogen werden. Dieses Buch soll den bayerischen Bürgerinnen und Bürgern das notwendige Know-How vermitteln, um in einer zunehmend digitalisierten Welt den eigenen Freiheitsraum sichern zu können. Nach einer Darstellung der wichtigsten Grundstrukturen und Begriffe des Datenschutzrechts befasst sich das Buch zentral mit den Betroffenenrechten der Datenschutz-Grundverordnung, etwa den Rechten auf Auskunft, auf Berichtigung und auf Löschung. Hieran schließen sich Erläuterungen zur Datenschutzaufsicht und zum Beschwerderecht an. Bürgerinnen und Bürgern soll somit aufgezeigt werden, wie sie ihre Datenschutzrechte effektiv wahrnehmen und verteidigen können.

In den Berichtszeitraum fiel zudem eine Neugestaltung der Rubrik **„Recht & Normen“** auf meiner Homepage. Bürgerinnen und Bürger finden hier – thematisch sortiert und aus unterschiedlichen Quellen zusammengeführt – zahlreiche Vorschriftentexte, die datenschutzrechtliche Regelungen enthalten und daher für meine Beratungspraxis von Bedeutung sind.

2.2 Identifizierung bei der Geltendmachung von Betroffenenrechten

Jede betroffene Person kann von einer öffentlichen Stelle Auskunft unter anderem darüber verlangen, welche personenbezogenen Daten über sie gespeichert sind, zu welchen Zwecken diese Daten verarbeitet und wem gegenüber sie offen gelegt werden. Dieses Auskunftsrecht sowie weitere Betroffenenrechte sind in Kapitel III (Art. 12 bis 23) DSGVO geregelt. Sie stehen (nur) der betroffenen Person selbst zu. Wird ein Auskunftsantrag gestellt, so kann es nun in der Praxis zweifelhaft sein, ob es sich bei der Antragstellerin oder dem Antragsteller um diejenige Person handelt, deren Betroffenenrechte geltend gemacht werden. Das gilt insbesondere bei einer telefonischen Kontaktaufnahme.

Die öffentliche Stelle muss eine betroffene Person bei der Antragstellung unterstützen (vgl. Art. 12 Abs. 2 Satz 1 DSGVO) und einem Antrag möglichst rasch und bürgerfreundlich entsprechen. Zugleich muss sie aber sicherstellen, dass sie personenbezogene Daten nicht an Unbefugte übermittelt. Zweifel an der Identität einer Antragstellerin oder eines Antragstellers darf die öffentliche Stelle daher weder vorschnell annehmen noch leichtfertig unterdrücken.

Vor diesem Hintergrund bestimmt Art. 12 Abs. 6 DSGVO:

„Hat der Verantwortliche begründete Zweifel an der Identität der natürlichen Person, die den Antrag gemäß den Artikeln 15 bis 21 stellt, so kann er unbeschadet des Artikels 11 zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind."

Der vorliegende Beitrag beantwortet einige in der Verwaltungspraxis immer wieder auftretende Fragen, die sich bei der Anwendung dieser Vorschriften stellen. Im Vordergrund steht dabei das Recht auf Auskunft nach Art. 15 Abs. 1 DSGVO.

2.2.1 Wann bestehen „Zweifel an der Identität" eines Antragstellers oder einer Antragstellerin?

Bei Beantwortung der Frage, ob Zweifel an der Identität des Antragstellers oder der Antragstellerin bestehen (vgl. Art. 12 Abs. 6 DSGVO), sollte zunächst einmal danach unterschieden werden, ob die betreffende Person bekannt ist oder nicht.

— **Regelmäßig** bestehen **keine Zweifel**, wenn der Antragsteller oder die Antragstellerin dem Verantwortlichen **persönlich bekannt** ist, etwa weil der zuständige Sachbearbeiter oder die zuständige Sachbearbeiterin den Antragsteller oder die Antragstellerin samt der Kontaktdaten (E-Mail-Adresse, Postanschrift) aus einem Verwaltungsvorgang kennt. Gleichwohl ist auch hier Aufmerksamkeit geboten:

  Ist die betroffene Person dem Verantwortlichen zwar grundsätzlich bekannt, können **Zweifel** an der Identität des Antragstellers oder der Antragstellerin insbesondere bei der **Verwendung unbekannter Kontaktdaten** (bislang unbekannte E-Mail-Adresse, Fax-Nummer oder Postanschrift) aufkommen.

  Zweifel können auch entstehen, wenn ein **Antrag** als **ungewöhnlich** erscheint, weil er in seiner äußeren Form oder seiner sprachlichen Gestaltung von der bisherigen Korrespondenz abweicht. Zu beachten ist dabei, dass im Internet gerade für Auskunftsanträge Formulare mit vorgefertigten Standardtexten angeboten werden.

— Die bloße Tatsache, dass ein Antragsteller oder eine Antragstellerin der öffentlichen Stelle – etwa aufgrund bereits vorhandener Kontaktdaten – **nicht persönlich bekannt** ist, führt **nicht automatisch zu Zweifeln** an seiner oder ihrer Identität. Art. 12 Abs. 6 DSGVO zielt nicht darauf, dass Verantwortliche für jeden Fall der Geltendmachung von Betroffenenrechten routinemäßige Identitätsprüfungen einrichten.

Dennoch werden unbekannte Personen durch Umstände ihres Auftretens häufiger Identitätszweifel wecken als bekannte. Dabei kann auch die Bedeutung des Antrags für die betroffene Person eine Rolle spielen. Der Antrag, eine allgemeine Auskunft über den Zweck einer Datenverarbeitung zu erhalten (vgl. Art. 15 Abs. 1 Satz 1 Halbsatz 2 Buchst. a DSGVO), ist weniger gewichtig als ein Antrag, der sich auf einen Aufenthalt in einer psychiatrischen Klinik eines Bezirks bezieht und auch medizinische Befunde erfasst. In diesem Fall drohen erhebliche Nachteile für die Rechte und Freiheiten der betroffenen Person, wenn die Informationen auf Grund einer Identitätstäuschung an einen Dritten herausgegeben werden. Mit steigender Bedeutung des Antrags für die Rechte und Freiheiten betroffener Personen tritt die Funktion des Art. 12 Abs. 6 DSGVO in den Vordergrund, einer Beeinträchtigung der Datenvertraulichkeit präventiv entgegenzuwirken. Wird Auskunft über besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO begehrt, ist es regelmäßig angezeigt, dass sich der Verantwortliche in geeigneter Form über die Identität der antragstellenden Person vergewissert und/oder Maßnahmen trifft, dass die Informationen nur die betroffene Person erreichen können.

2.2.2 Wann sind die Zweifel an der Identität eines Antragstellers oder einer Antragstellerin „begründet“?

Die öffentliche Stelle darf gemäß Art. 12 Abs. 6 DSGVO Nachweise für die Identität eines Antragstellers oder einer Antragstellerin fordern, wenn ihre Zweifel an der Identität des Antragstellers oder der Antragstellerin „begründet“ sind. Aus der Gesetzesformulierung ergibt sich, dass die pauschale Behauptung von Zweifeln nicht genügt, um einen Antrag nach den Art. 15 bis 21 DSGVO abzulehnen. Der Verantwortliche muss insofern auch seiner Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) nachkommen, sodass eine Dokumentation der begründeten Zweifel angebracht ist. Die **Zweifel** an der Identität des Antragstellers oder der Antragstellerin sind **einzelfallbezogen plausibel darzulegen**.

2.2.3 Welche Maßnahmen kann oder muss der Verantwortliche selbst treffen, um eine antragstellende Person zu identifizieren?

Nach Erwägungsgrund 64 Satz 1 DSGVO hat die öffentliche Stelle alle vertretbaren Mittel zur Identifikation einer Auskunft suchenden Person zu nutzen. Daraus ergibt sich eine Pflicht, Identitätszweifel mithilfe vorhandener Informationen möglichst selbst zu beseitigen.

— Ein einfaches – allerdings nicht in jedem Fall praktikables – Mittel ist der **Abgleich mit vorhandenen Kontaktinformationen**. Anschließend kann der Verantwortliche personenbezogene Daten über den **„verifizierten“ Rückkanal** versenden, indem er etwa ein entsprechendes Dokument der betroffenen Person unter ihrer bekannten Adresse per Briefpost zuleitet. Die erforderlichen Adressdaten der betroffenen Person werden den maßgeblichen Verwaltungsvorgängen oder – etwa bei wirtschaftlicher Betätigung von Kommunen – einer Kundendatei entnommen.

— Zum **Abgleich** der vom Antragsteller oder der Antragstellerin angegebenen Daten können auch **Meldedaten** genutzt werden:

Nach § 37 Abs. 1 in Verbindung mit § 34 Abs. 1 Bundesmeldegesetz (BMG) dürfen innerhalb der Verwaltungseinheit, der die Meldebehörde angehört, bestimmte Meldedaten weitergegeben werden, wenn dies zur Erfüllung der in ihrer Zuständigkeit liegenden öffentlichen Aufgaben erforderlich ist. Zu diesen Aufgaben zählt es auch, datenschutzrechtlichen Ansprüchen nachzukommen.

Hat die öffentliche Stelle keinen eigenen Zugriff auf die Meldedaten, kann sie diese bei der Meldebehörde anfordern. Zwar sind personenbezogene Daten gemäß Art. 4 Abs. 2 Satz 1 BayDSG vorrangig bei der betroffenen Person zu erheben. Sie können aber gemäß Art. 4 Abs. 2 Satz 2 Nr. 4 BayDSG bei einer anderen öffentlichen Stelle erhoben werden, wenn die Daten von der anderen Stelle an die erhebende Stelle übermittelt werden dürfen. Diese Voraussetzungen sind grundsätzlich erfüllt. Die Meldebehörden dürfen gemäß § 34 Abs. 1 BMG die dort genannten Daten (zum Beispiel Name, Anschrift, Geburtsort) öffentlichen Stellen der Länder im Sinne von § 2 Abs. 2 Bundesdatenschutzgesetz übermitteln, wenn dies zur Erfüllung einer öffentlichen Aufgabe des Empfängers erforderlich ist.

Meldedaten können häufig im Rahmen des auf der Grundlage der Verordnung zur Übermittlung von Meldedaten (MeldDV) eingerichteten Bayerischen Behördeninformationssystems (BayBIS) abgerufen werden (zum BayBIS erläuternd meine Ausführungen im 28. Tätigkeitsbericht 2018 unter Nr. 7.1).

Erwägungsgrund 64 Satz 1 DSGVO beschränkt die Pflicht der öffentlichen Stelle zur Beseitigung von Zweifeln an der Identität der Person des Antragstellers oder der Antragstellerin auf **„vertretbare" Maßnahmen**. Die öffentliche Stelle muss daher nicht „um jeden Preis" die Identität des Antragstellers oder der Antragstellerin zu ermitteln suchen. Hat sie keinen eigenen Zugang zu den Meldedaten, wird es regelmäßig auch nicht zu bemängeln sein, wenn sie von einer Anfrage bei der Meldebehörde absieht.

2.2.4 Welche Identitätsnachweise können bei begründeten Zweifeln von einer antragstellenden Person gefordert werden?

Können im Einzelfall bestehende Zweifel an der Identität des Antragstellers oder der Antragstellerin durch die öffentliche Stelle nicht vertretbar mithilfe verfügbarer Informationen überwunden werden, wird die öffentliche Stelle **von dem Antragsteller oder der Antragstellerin einen Identitätsnachweis verlangen**. Im Interesse der **Datenminimierung** (Art. 5 Abs. 1 Buchst. c DSGVO) sollen dabei nur Daten gefordert werden, die zur Identifizierung zwingend erforderlich sind.

Nach Möglichkeit sollten dem Antragsteller oder der Antragstellerin **verschiedene Optionen** zur Identifikation angeboten werden. Art. 12 Abs. 1 Satz 3 und Abs. 3 Satz 4 DSGVO weisen darauf hin, dass grundsätzlich die betroffene Person die freie Wahl der Kommunikationsmittel hat. Die folgenden Beispiele beschreiben Möglichkeiten, die dem Antragsteller oder der Antragstellerin angeboten werden können.

– Haben die betroffene Person und die öffentliche Stelle **bisher elektronisch** unter Verwendung sicherer Authentifizierungsmittel **kommuniziert**,

kann die öffentliche Stelle anregen, dass der Antragsteller oder die Antragstellerin seinen oder ihren Antrag auf dem bislang üblichen Weg stellt. Ist die betroffene Person etwa mit einem „Bürgerkonto“ bei einer Gemeinde registriert und dient dieses allgemein zur digitalen Abwicklung von Verwaltungsvorgängen, kann die Gemeinde dem Antragsteller oder der Antragstellerin die Nutzung dieses Zugangs empfehlen.

— Bei Verwendung einer bisher unbekannten E-Mail-Adresse kann auch vorgeschlagen werden, den **Antrag über eine schon bekannte Adresse** kurz zu **bestätigen**. Das gilt jedenfalls dann, wenn Anhaltspunkte dafür fehlen, dass die Kennung oder sonstige Zugangsberechtigung unbefugt benutzt wird. Die öffentliche Stelle kann aber nicht verlangen, dass der Antragsteller oder die Antragstellerin zur Identifizierung Nutzer oder Nutzerin des Online-Dienstes wird.

— In Betracht kommt auch die Abfrage von Informationen, die zum Zweck der Kommunikation zwischen der betroffenen Person und dem Verantwortlichen vereinbart wurden (zum Beispiel **Kennwort, Kundennummer, Transaktionsnummer**). So könnte ein kommunaler Wasserversorger die Angabe spezifizierender Kundendaten verlangen, von denen nur die betroffene Person weiß, wenn ihm ein Antragsteller oder eine Antragstellerin auf eine nach dem bisherigen Kontakt ungewöhnliche Weise entgegentritt.

— Je nach Bedeutung des Antrags kommt zudem eine **persönliche Vorsprache** und/oder die Identifizierung durch ein **amtliches Ausweisdokument** in Betracht.

Die Anforderung einer **Ausweiskopie**[1] ist aus datenschutzrechtlicher Sicht regelmäßig nicht erforderlich. Anderes kann etwa gelten, wenn eine Auskunft besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) betrifft. Die Anforderung unterliegt jedenfalls den in § 20 Abs. 2 Personalausweisgesetz und § 18 Abs. 3 Paßgesetz genannten Grenzen. Danach muss insbesondere sichergestellt sein, dass eine Kopie dauerhaft als solche erkennbar ist. Grundsätzlich wird es allerdings genügen, sich den Ausweis vorlegen zu lassen und darüber eine Aktennotiz zu fertigen. Es ist ausreichend, dabei Name, Vorname, Geburtsdatum und Seriennummer des Ausweisdokuments festzuhalten (beim Personalausweis und auf der Datenseite des Reisepasses jeweils in der rechten oberen Ecke). Wird im Ausnahmefall zulässigerweise eine Ausweiskopie gefordert, ist die betroffene Person auf die Möglichkeit einer Schwärzung der nicht benötigten Daten hinzuweisen.

2.2.5 Was geschieht, wenn der Identitätsnachweis scheitert?

Hat die öffentliche Stelle alle vertretbaren Mittel zur Identifikation erfolglos eingesetzt und auch der Antragsteller oder die Antragstellerin nicht an der Beseitigung der bestehenden Zweifel mitgewirkt, wird sie dem Antrag nicht entsprechen.

Dieses Ergebnis steht mit der Pflicht der öffentlichen Stelle zu einem angemessenen Schutz der verarbeiteten Daten (Art. 5 Abs. 1 Buchst. f DSGVO) in Einklang

[1] Zur Anforderung von Ausweiskopien siehe mein 26. Tätigkeitsbericht 2014 unter Nr. 2.1.5 und Nr. 3.7. Diese Ausführungen gelten sinngemäß auch unter der Datenschutz-Grundverordnung und dem neuen Polizeiaufgabengesetz.

und spiegelt sich auch in Art. 12 Abs. 2 Satz 2 und Art. 11 Abs. 2 DSGVO wider. Danach kann der Verantwortliche sich weigern, einem Antrag nach Art. 15 ff. DSGVO zu entsprechen, wenn er glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu identifizieren. Diese Pflicht zur Glaubhaftmachung konkretisiert die Rechenschaftspflicht in Art. 5 Abs. 2 DSGVO. Die öffentliche Stelle ist verpflichtet, ihre begründeten Zweifel an der Identität des Antragstellers oder der Antragstellerin und seine oder ihre unzureichende Mitwirkung an der Identifizierung zu dokumentieren und erforderlichenfalls gegenüber der Datenschutz-Aufsichtsbehörde nachzuweisen.

Ist der Antragsteller oder die Antragstellerin der Auffassung, die Weigerung sei nicht rechtmäßig, kann er oder sie sich an die Datenschutz-Aufsichtsbehörde wenden (vgl. Art. 77 Abs. 1 DSGVO). Hierauf ist er oder sie hinzuweisen (vgl. Art. 12 Abs. 4 DSGVO).

2.2.6 Dürfen erhobene Identitätsnachweise gespeichert werden?

Art. 12 Abs. 6 DSGVO gestattet der öffentlichen Stelle, die zur Identifizierung erforderlichen Daten zu erheben und für diesen Zweck zu verarbeiten. Die dauerhafte Speicherung der Identifizierungsdaten für künftige Identitätsprüfungen sieht Art. 12 Abs. 6 DSGVO nicht vor (vgl. Erwägungsgrund 64 Satz 2 DSGVO). Sofern nicht eine bereichsspezifische Rechtsgrundlage die Speicherung der Identifizierungsdaten zulässt, sind diese nach Zweckerreichung zu löschen. Das entspricht dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO).

2.2.7 Welche vorbeugenden Maßnahmen können öffentliche Stellen treffen?

Öffentliche Stellen sollten prüfen, ob sie durch vorbeugende Maßnahmen späteren Schwierigkeiten bei der Identifizierung von Antragstellern oder Antragstellerinnen entgegenwirken können.

Beim Recht auf Auskunft (Art. 15 DSGVO) steht dabei die Gewährleistung eines sicheren Rückkanals im Vordergrund. Je nach dem Grad der Schutzwürdigkeit zu übermittelnder personenbezogener Daten kann dabei die Dokumentation einer Telefonnummer für einen „Kontrollanruf“ oder die Vereinbarung eines Kennworts in Betracht kommen. Sicherheit und Komfort lassen sich auch in Auskunftsportalen verbinden (vgl. Erwägungsgrund 63 Satz 4 DSGVO). Dort können betroffene Personen, die nach Verifizierung der angegebenen Identität ein (Einmal-)Passwort erhalten haben, die beantragten Informationen gesichert herunterladen.

So entspricht die öffentliche Stelle der Verpflichtung, die Ausübung der Betroffenenrechte zu erleichtern; zugleich gestaltet sie ihre Verwaltungsarbeit effizient, insbesondere wenn sie ihre Dienstleistungen ohnehin bereits elektronisch anbietet.

3 Polizei und Verfassungsschutz

3.1 Erkennungsdienstliche Behandlung und beabsichtigte DNA-Speicherung bei einem 78-jährigen Rentner

Es begann harmlos mit den Tücken der modernen Technik und endete für einen 78-jährigen Rentner mit einer erkennungsdienstlichen Behandlung, einer Speichelabgabe für eine DNA-Analyse und der polizeilich gespeicherten Einschätzung, er könne sexuelle Interessen gegenüber Kindern haben. Doch der Reihe nach:

Als der Betroffene mit seinem Fahrrad an einem belebten Spielplatz vorbeifuhr, wollte er die dortige Hüpfburg fotografieren, um das Bild später seinem Enkel zu zeigen. Dabei erregte er offenbar Aufsehen und verstrickte sich anschließend – so zumindest die Auffassung empörter Eltern – in Widersprüche, was seine Motivlage anging.

Eine von den Eltern verständigte Streifenbesatzung stellte die Identität des Rentners fest, befragte ihn, stellte das besagte Mobiltelefon sicher und behandelte ihn im Anschluss daran zur „Abwehr einer konkreten Gefahr“ erkennungsdienstlich. Zudem wurde ein Mundhöhlenabstrich zur Feststellung eines DNA-Identifizierungsmusters durchgeführt. Die dabei dem Betroffenen ausgehändigte Rechtsbelehrung verwies auf eine nicht zutreffende Rechtsgrundlage nach der Strafprozessordnung.

Zwar verfügt die Polizei gemäß Art. 14 Abs. 1, 2 Polizeiaufgabengesetz (PAG) über die Befugnis, im Rahmen einer sogenannten „Erkennungsdienstlichen Behandlung“ insbesondere Finger- und Handflächenabdrucke eines Betroffenen abzunehmen sowie Lichtbilder, Messungen und eine Personenbeschreibung der Person anzufertigen. Dafür müssen jedoch die jeweiligen Voraussetzungen der Befugnisnorm erfüllt sein. Dies sind die Aufklärung einer unbekannten oder zweifelhaften Identität einer Person, die Abwehr einer Gefahr oder einer drohenden Gefahr für ein bedeutendes Rechtsgut oder die Erforderlichkeit zur vorbeugenden Bekämpfung von Straftaten, sofern vom Verdächtigen eine Wiederholungsgefahr ausgeht.

Nur zwei Monate vor diesem Zusammentreffen erhielt die Bayerische Polizei zudem die Befugnis, einer betroffenen Person gemäß Art. 14 Abs. 3 PAG Körperzellen zu entnehmen und diese zur Feststellung des DNA-Identifizierungsmusters molekulargenetisch untersuchen zu lassen, wenn dies zur Abwehr einer Gefahr für ein bedeutendes Rechtsgut erforderlich ist und andere erkennungsdienstliche Maßnahmen nicht hinreichend sind.

Doch all diese Voraussetzungen trafen auf den hier kontrollierten Rentner nicht zu, insbesondere ging von ihm keine „konkrete Gefahr“ aus. Ein strafrechtlicher Tatvorwurf wurde zu keinem Zeitpunkt erhoben, auch lagen keinerlei belastende Vorerkenntnisse über den Betroffenen vor. Erst mehrere Stunden nach dem eigentlichen Geschehen konnte der 78-Jährige schließlich nach einer „eindringlichen Ansprache“ die Polizeidienststelle wieder verlassen.

Die über den Rentner gewonnenen Informationen wurden an ein für Sexualdelikte zuständiges Kommissariat übersandt. Obwohl man dort zu dem Schluss kam, dass keine Hinweise auf eine sexuelle Motivation des Rentners vorlagen, zog der Vorfall auf Landes- und sogar Bundesebene zahlreiche Speicherungen zur „polizeilichen Gefahrenabwehr" nach sich.

Das sichergestellte Smartphone erhielt der Betroffene circa einen Monat später wieder zurück. Mit seinem Einverständnis wurde eine Videosequenz von dem Telefon gelöscht, obwohl weder rechtlich problematische Daten noch Aufnahmen der besagten Kinder von der Hüpfburg darauf erkennbar waren.

Der Rentner glaubte nun, das Schlimmste überstanden zu haben und wandte sich, da ihm im Nachgang das Verhalten der Polizei seltsam erschien, mit einem Auskunfts-und Löschungsantrag an das Bayerische Landeskriminalamt. Doch dort wurde eine Datenlöschung unter anderem mit der Begründung abgelehnt, es bestehe die konkrete Gefahr, dass er weitere Hemmschwellen abbauen und aus einer sexuellen Motivation heraus Kinder fotografieren werde. Ihm wurde mitgeteilt, dass seine von der Polizei erhobenen Daten geeignet wären, ihn im Rahmen möglicher zukünftiger Verfahren in den Kreis von Beteiligten oder auch Verdächtigen einzuordnen oder auch auszuschließen. Aus Sicht des Landeskriminalamts sei die Speicherung der Daten aus der erkennungsdienstlichen Behandlung angemessen und verhältnismäßig.

Dieser Einschätzung der Polizei musste ich entschieden widersprechen, als mich der Betroffene aufsuchte und um Hilfe bat. Gegenüber der Polizei stellte ich klar, dass eine erste Abklärung des Sachverhalts geboten war, um die Rechte der Kinder auf dem Spielplatz zu wahren. Als sich dann jedoch frühzeitig herausstellte, dass der Betroffene keine gezielten Aufnahmen von Kindern gefertigt hatte und auch sonst nichts auf eine sexuelle Motivation des Rentners hindeutete, hätte die Polizei die Situation allerdings sofort neu bewerten müssen. Obwohl ab diesem Zeitpunkt keine „Gefahr" im polizeirechtlichen Sinne begründbar war, wich die Polizei nicht mehr von ihrem eingeschlagenen Weg ab. Stattdessen unterstellte sie dem Betroffenen selbst nach dessen Löschungsantrag und offenkundig im Widerspruch zur Aktenlage weiterhin ein sexuelles Interesse an Kindern.

Meiner Aufforderung, die gespeicherten personenbezogenen Daten unverzüglich zu löschen und die zu dem Betroffenen geführten Akten zu vernichten, wurde schließlich im vollen Umfang Folge geleistet. Nur der zuletzt konsequente Kurswechsel der Polizei ließ mich in diesem Fall von einer Beanstandung absehen.

3.2 Kein Löschungsantrag notwendig, wenn eine polizeiliche Speicherung nicht mehr erforderlich ist

Die Prüfung der Zulässigkeit polizeilicher Datenspeicherungen gehört zu meinen Kernaufgaben und ist dementsprechend fester Bestandteil meiner Tätigkeitsberichte, siehe unter anderem meine Ausführungen im 28. Tätigkeitsbericht 2018 unter Nr. 4.4.

Polizeiliche Speicherungen können weitreichende Folgen für die betroffene Person haben, da sie sich beispielsweise bei sogenannten Zuverlässigkeitsüberprüfungen (etwa nach dem Luftsicherheitsgesetz) unter Umständen negativ auf beantragte Zugangsberechtigungen auswirken. Daher nahm ich eine solche Zuver-

lässigkeitsüberprüfung zum Anlass, die vorhandenen Speicherungen einer datenschutzrechtlichen Überprüfung zu unterziehen. Art. 54 Abs. 1 und 2 Polizeiaufgabengesetz (PAG) ist zu entnehmen, dass die Polizei personenbezogene Daten nur speichern darf, wenn dies für die polizeiliche Arbeit erforderlich ist. Dort heißt es:

„(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. [2]Entfällt der der Speicherung zugrunde liegende Verdacht, sind die Daten unverzüglich zu löschen. [3]Die nach Art. 53 Abs. 5 festzulegenden Prüfungstermine oder Aufbewahrungsfristen betragen in der Regel bei Erwachsenen zehn Jahre, bei Jugendlichen fünf Jahre und bei Kindern zwei Jahre. [4]In Fällen von geringerer Bedeutung sind kürzere Fristen festzusetzen. [5]Die Frist beginnt regelmäßig mit dem Ende des Jahres, in dem das letzte Ereignis erfaßt worden ist, das zur Speicherung der Daten geführt hat, jedoch nicht vor Entlassung des Betroffenen aus einer Justizvollzugsanstalt oder der Beendigung einer mit Freiheitsentziehung verbundenen Maßregel der Besserung und Sicherung. [6]Werden innerhalb der Frist der Sätze 3 bis 5 weitere personenbezogene Daten über dieselbe Person gespeichert, so gilt für alle Speicherungen gemeinsam der Prüfungstermin, der als letzter eintritt, oder die Aufbewahrungsfrist, die als letzte endet."

Gerade bei älteren Speicherungen ist es oftmals so, dass zum Zeitpunkt der Entstehung der Speicherung diese rechtliche Voraussetzung zwar gegeben war, aus aktueller Sicht die weitere Erforderlichkeit der Speicherung aber nicht mehr vorliegt.

Im Rahmen der erwähnten Prüfung wurde ich bezüglich einer Speicherung von einem Polizeipräsidium mit der überraschenden Aussage konfrontiert, dass man „sofern" die betroffene Person „zum heutigen Zeitpunkt eine Löschung beantragen sollte" den Sachverhalt neu bewerten könne, da die Speicherung aus polizeilicher Sicht nicht mehr notwendig sei. Ich habe das Polizeipräsidium sodann darauf aufmerksam gemacht, dass, sobald die Erforderlichkeit einer Speicherung nicht mehr gegeben ist, eine Löschung von Amts wegen geboten ist (siehe Art. 54 Abs. 1, 2 PAG). Die Polizei darf in solchen Fällen die datenschutzrechtliche Verantwortung für die Fortführung solcher Speicherungen nicht auf betroffene Personen abwälzen. Vor dem Hintergrund, dass vielen gar nicht bekannt ist, dass bei der Polizei Datensätze über sie vorhanden sind, wäre die zusätzliche Stellung eines Löschungsantrags im Übrigen auch nicht praxistauglich.

Das Polizeipräsidium hat daraufhin auch ohne einen Löschungsantrag des Betroffenen die Speicherung gelöscht.

3.3 Reduzierte Dauer bei der Speicherung von Erstkonsumenten „weicher" Drogen

In meinem 27. Tätigkeitsbericht 2016 unter Nr. 3.6.6 habe ich darüber berichtet, dass ein Polizeipräsidium meine Anregung aufgenommen hat, die Regelspeicherfrist im Kriminalaktennachweis auf zwei Jahre zu reduzieren, wenn Jugendliche

oder Heranwachsende erstmals wegen strafbaren Erwerbs oder Besitzes von geringen Mengen Cannabis in Erscheinung treten. Im meinem letzten Tätigkeitsbericht (28. Tätigkeitsbericht 2018 unter Nr. 4.1.3) konnte ich erfreulicherweise mitteilen, dass sich das Bayerische Staatsministerium des Innern, für Sport und Integration dieser Verfahrensweise im Grundsatz angeschlossen und durch eine Regelung in den entsprechenden Verwaltungsvorschriften veranlasst hat, dass alle Polizeiverbände in solchen Fällen verkürzte Speicherfristen festzulegen haben.

Die Umsetzung dieser Verfahrensweise habe ich stichprobenhaft bei einem Polizeipräsidium überprüft. Hierbei musste ich feststellen, dass in beinahe allen Fällen entweder aus mangelnder Kenntnis der neuen Verwaltungsvorschrift oder aus Versehen keine verkürzte Speicherfrist geprüft worden war.

Das betroffene Polizeipräsidium berichtigte die entsprechenden Speicherungsfristen umgehend und teilte mir mit, dass alle Dienststellen angehalten wurden, die neue Verwaltungsvorschrift zu beachten.

Diese Prüfung hat gezeigt, wie wichtig es ist, nach datenschutzrechtlichen Verbesserungen stets auch ein Augenmerk darauf zu haben, ob diese „in der Praxis" auch ankommen.

3.4 „Cloud-Durchsuchung" zur Gefahrenabwehr

Im Mai 2019 prüfte ich den Einsatz der ein Jahr zuvor neu eingeführten präventivpolizeilichen Befugnis zur Durchsuchung eines von einem elektronischen Speichermedium räumlich getrennten weiteren Speichermediums. Im Gesetzgebungsverfahren hatte ich diese Regelung grundsätzlich kritisiert. Sie gestattet es, sogenannte „Clouds" zu durchsuchen. Eine solche Durchsuchung eines Speichermediums hat in der Regel eine deutlich weitreichendere Eingriffstiefe als die Durchsuchung einer herkömmlichen Sache, zum Beispiel einer Tasche. Diese erhöhte Eingriffsintensität wird in der Norm nicht hinreichend berücksichtigt.

Art. 22 Abs. 2 Polizeiaufgabengesetz (PAG) lautet:

„(2) [1]Betrifft die Durchsuchung ein elektronisches Speichermedium, können auch vom Durchsuchungsobjekt räumlich getrennte Speichermedien durchsucht werden, soweit von diesem aus auf sie zugegriffen werden kann. [2]Personenbezogene Daten dürfen darüber hinaus nur dann weiterverarbeitet werden, wenn dies gesetzlich zugelassen ist."

Meine Prüfung führte zu dem Ergebnis, dass diese neue polizeiliche Befugnis seit ihrer Einführung lediglich in einem Fall zur Anwendung kam. Bei der Durchsuchung konnten keine weiteren Erkenntnisse gewonnen werden, sodass keine personenbezogenen Daten verwertet wurden.

Ich werde weiterhin beobachten, wie sich diese Thematik entwickelt. Unabhängig davon habe ich das Bayerische Staatsministerium des Innern, für Sport und Integration darum gebeten, mich einzubeziehen, sollte es aufgrund einer Zunahme des Einsatzes der Befugnis aus Art. 22 Abs. 2 PAG eine bayernweite Handlungsanweisung erstellen.

3.5 Gesonderte Hinweispflicht bei einer polizeilichen Videoüberwachung mittels einer Drohne

Unter der etwas sperrigen Bezeichnung „Einsatz von unbemannten Luftfahrtsystemen“ regelt Art. 47 Polizeiaufgabengesetz (PAG) die Voraussetzungen für Datenerhebungen mittels sogenannter „Drohnen“. Diese Vorschrift wurde im Zuge der Polizeirechtsreform im Mai 2018 eingeführt und bietet der Polizei unter anderem die Möglichkeit, bei Großveranstaltungen die Einsatzsteuerung zu vereinfachen. So kann die Polizei mit einer an der Drohne fest installierten Kamera im Livebild erkennen, wohin sich Menschenmassen bewegen und ob sich beispielsweise an Engstellen Gefahren durch eine Überfüllung ergeben.

Dabei muss der Betrieb dieser Polizei-Drohnen für die betroffenen Besucher einer Großveranstaltung allerdings erkennbar sein. So dürfen unbemannte Luftfahrtsysteme bei einem solchen Anlass nur eingesetzt werden, wenn die Offenheit der Maßnahme gewahrt bleibt. Neben den üblichen Hinweisschildern auf eine polizeiliche Videoüberwachung sieht das Polizeiaufgabengesetz daher vor, dass ein gesonderter Hinweis auf den Einsatz dieser „unbemannten Luftfahrtsysteme“ erfolgt.

Art. 47 PAG
Einsatz von unbemannten Luftfahrtsystemen
(1) Bei den nachfolgenden Maßnahmen dürfen Daten unter den dort genannten Voraussetzungen auch durch den Einsatz unbemannter Luftfahrtsysteme erhoben werden:
1. offene Bild- und Tonaufnahmen oder -aufzeichnungen nach Art. 33 Abs. 1 bis 3,
[…]
(2) [1]In den Fällen des Abs. 1 Nr. 1 dürfen unbemannte Luftfahrtsysteme nur dann eingesetzt werden, wenn die Offenheit der Maßnahme gewahrt bleibt. [2]In diesen Fällen soll auf die Verwendung unbemannter Luftfahrtsysteme durch die Polizei gesondert hingewiesen werden.

Als im Rahmen des Pilotprojekts „Multicoptersysteme“ mehrere Polizeipräsidien bei sportlichen Großveranstaltungen auf Drohnen zurückgriffen, stand dieses Transparenzgebot nicht immer im Fokus der Einsatzplanerinnen und Einsatzplaner. In einem Fall konnte ich erst aus dem angeforderten Erfahrungsbericht entnehmen, dass neben der „klassischen“ Videokameras auch eine Drohne zum Einsatz kam. Auf meine Nachfrage hin musste das betreffende Polizeipräsidium einräumen, dass die gesonderte Hinweispflicht unbeachtet blieb. Man sicherte mir jedoch zu, dass man dieser Verpflichtung durch die Verwendung geeigneter Piktogramme zukünftig nachkommen werde.

Werde ich von Polizeipräsidien über bevorstehende Videoüberwachungen bei Großveranstaltungen informiert, weise ich vor diesem Hintergrund regelmäßig darauf hin, dass ein etwaiger Drohnen-Einsatz frühzeitig in die Planungen der Polizei einfließen müsse und immer nur als offene Maßnahme erfolgen dürfe.

3.6 Prüfung der Vollständigkeit und Richtigkeit von Auskünften

Das Bayerische Landesamt für Verfassungsschutz hat den gesetzlichen Auftrag, Informationen unter anderem über Bestrebungen, die gegen die freiheitliche de-

mokratische Grundordnung gerichtet sind, zu sammeln und auszuwerten. Um dieser wichtigen Aufgabe gerecht zu werden, muss dort zwangsläufig eine Vielzahl an Daten verarbeitet werden.

Auch die nachrichtendienstliche Arbeit muss für Bürgerinnen und Bürger ein ausreichendes Maß von Transparenz sicherstellen. Zu diesem Zweck sieht Art. 23 Abs. 1 Bayerisches Verfassungsschutzgesetz (BayVSG) ein Recht auf Selbstauskunft vor (siehe bereits meine Ausführungen im 28. Tätigkeitsbericht unter Nr. 5.4 und Nr. 5.5). Die Ablehnung von Auskünften durch das Bayerische Landesamt für Verfassungsschutz ist zwar im Einzelfall möglich, unterliegt jedoch gemäß Art. 23 Abs. 2 BayVSG engen gesetzlichen Voraussetzungen.

Art. 23 BayVSG
Auskunft
(1) [1]Das Landesamt erteilt dem Betroffenen auf Antrag, in dem ein besonderes Interesse an einer Auskunft dargelegt ist, kostenfrei Auskunft über die zu seiner Person gespeicherten Daten. [2]Legt der Betroffene nach Aufforderung ein besonderes Interesse nicht dar, entscheidet das Landesamt über den Antrag nach pflichtgemäßem Ermessen. [3]Die Auskunft erstreckt sich nicht auf

1. *die Herkunft der Daten und die Empfänger von Übermittlungen,*
2. *Daten, die nicht strukturiert in automatisierten Dateien gespeichert sind, es sei denn, der Betroffene macht Angaben, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand steht nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse und*
3. *Daten, die zur Erfüllung der Aufgaben nicht mehr erforderlich sind und die ausschließlich für eine zukünftige Übergabe an das Hauptstaatsarchiv gespeichert sind.*

[4]Das Landesamt bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.
(2) Die Auskunftserteilung unterbleibt, soweit durch sie

1. *eine Gefährdung der Erfüllung der Aufgaben zu besorgen ist,*
2. *Nachrichtenzugänge gefährdet sein können oder die Ausforschung des Erkenntnisstandes oder der Arbeitsweise des Landesamts zu befürchten ist,*
3. *die öffentliche Sicherheit gefährdet oder sonst dem Wohl des Bundes oder eines Landes ein Nachteil bereitet würde oder*
4. *Daten oder die Tatsache ihrer Speicherung preisgegeben werden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.*

(3) [1]Die Ablehnung der Auskunftserteilung bedarf keiner Begründung. [2]Sie enthält einen Hinweis auf die Rechtsgrundlage für das Fehlen der Begründung und darauf, dass sich der Betroffene an den Landesbeauftragten für den Datenschutz wenden kann. [3]Mitteilungen des Landesbeauftragten an den Betroffenen dürfen ohne Zustimmung des Landesamts keine Rückschlüsse auf den Kenntnisstand des Landesamts zulassen.

Aufgrund der datenschutzrechtlichen Bedeutung dieses Selbstauskunftsrechts prüfe ich regelmäßig, ob im Falle einer Auskunftsverweigerung die rechtlichen Vorgaben eingehalten werden. Zusätzlich erstrecken sich meine datenschutzrechtlichen Prüfungen auch darauf, ob zugesagte Datenlöschungen durch das Bayerische Landesamt für Verfassungsschutz auch tatsächlich vollzogen werden. Im Berichtszeitraum konnte ich diesbezüglich keine grundsätzlichen Mängel feststellen.

4 Justiz

4.1 Einsicht in notarielle Urkunden zu Forschungszwecken

Bereits im Jahr 2016 hat mir das Bayerische Staatsministerium der Justiz Gelegenheit gegeben, zur Schaffung einer neuen Akteneinsichtsregelung im Notarrecht Stellung zu nehmen. Anlass hierfür war eine Anfrage des Bundesministeriums der Justiz und für Verbraucherschutz zur Einsichtnahme in notarielle Urkunden aus der Zeit des Nationalsozialismus zu wissenschaftlichen Zwecken.

Nach derzeitiger Rechtslage ist die Einsichtnahme in notarielle Urkunden zu Forschungszwecken nicht eindeutig geregelt. Es findet sich keine explizite Rechtsgrundlage in der Bundesnotarordnung (BNotO) oder im Beurkundungsgesetz (BeurkG). Die Regelung des § 18 BNotO zur Verschwiegenheitspflicht des Notars und die Regelung des § 51 BeurkG zum Einsichtsrecht in Urkunden könnten einer Einsichtnahme entgegenstehen.

In meiner Stellungnahme zu der geplanten Regelung schlug ich vor, die notariellen Urkunden mit eine Schutzfrist von 70 Jahren zu belegen, um eine uferlose Ausweitung der Einsichtnahme zu vermeiden und den Interessen der Beteiligten sowie ihrer Angehörigen am Schutz des Urkundeninhalts ausreichend Rechnung zu tragen.

Des Weiteren empfahl ich, sich für die nähere Ausgestaltung der neuen Rechtsgrundlage an den Vorgaben von § 476 Strafprozessordnung (StPO) zu orientieren. Diese Regelung zur Datenübermittlung für wissenschaftliche Zwecke in Strafverfahren bringt das Grundrecht auf informationelle Selbstbestimmung der Beteiligten und die Wissenschaftsfreiheit der Forscher in einen angemessenen Ausgleich. Die Voraussetzungen des § 476 StPO können auf eine Vorschrift betreffend die Einsichtsgewährung in notarielle Urkunden übertragen werden. Denn sowohl im Strafverfolgungsbereich als auch im Bereich der Rechtsvorsorge sind sensible Daten betroffen.

§ 476 Abs. 1 StPO setzt für eine Datenübermittlung an Forschungseinrichtungen voraus, dass die Daten für die Durchführung der wissenschaftlichen Forschungsarbeit erforderlich sind (Erforderlichkeitsklausel), eine Nutzung anonymisierter Daten zu diesem Zweck nicht möglich oder die Anonymisierung mit einem unverhältnismäßigen Aufwand verbunden ist (Subsidiaritätsklausel) und das öffentliche Interesse an der Forschungsarbeit das schutzwürdige Interesse des Betroffenen am Ausschluss der Übermittlung erheblich überwiegt (Interessenabwägung). Diese drei Voraussetzungen sollten in jedem Fall Gegenstand einer Regelung zur Einsichtsgewährung in notarielle Urkunden sein.

Weiterhin sollte ein Vorrang der Auskunftserteilung vor der Einsichtsgewährung geregelt und der Empfängerkreis eng begrenzt werden. Ferner sollten Schutzvorkehrungen zur Verhinderung unbefugter Kenntnisnahme der im Rahmen der Einsicht erlangten Informationen getroffen werden.

Mittlerweile hat das Bundesjustizministerium einen Regelungsentwurf ausgearbeitet, der in der Bundesnotarordnung die Einfügung entsprechender Vorschriften (§§ 18a bis 18d BNotO-Entwurf) zur Einsichtsgewährung in notarielle Urkunden und Verzeichnisse zu Forschungszwecken vorsieht. Besonders erfreulich ist hierbei, dass alle meine Anregungen und Forderungen aufgegriffen und im Regelungsentwurf umgesetzt wurden. Ich würde es daher sehr begrüßen, wenn der sich zum Zeitpunkt des Redaktionsschlusses noch im Entwurfsstadium befindende Regelungsvorschlag zeitnah in den Bundestag eingebracht und verabschiedet würde.

4.2 Videoüberwachung eines Fachgerichts

Auch in diesem Berichtszeitraum habe ich Videoüberwachungsanlagen verschiedener Justizeinrichtungen geprüft. Bei einem Fachgericht stellte ich fest, dass sämtliche Sitzungssäle mit Videokameras ausgestattet waren. Diese zeichneten permanent das Geschehen im Sitzungssaal für mindestens 15 Minuten auf. Mit Betätigen einer am Richtertisch angebrachten Notfalltaste wären die Aufzeichnungen der vergangenen 15 sowie der darauffolgenden 30 Minuten dauerhaft auf einem Server gespeichert sowie zugleich eine Videobeobachtung auf einem Monitor in der Pforte des Gerichts gestartet worden. Während ich gegen Letzteres keine Bedenken hatte, hielt ich aber die permanente und vor allem anlasslose fünfzehnminütige Aufzeichnung für sehr problematisch.

Zwar erlaubt Art. 24 Abs. 1 BayDSG eine Videoüberwachung in Ausübung des Hausrechts zum Schutz von Leben und Gesundheit von Personen im Bereich öffentlicher Einrichtungen oder zum Schutz der öffentlichen Einrichtungen selbst. Eine permanente anlasslose Videoaufzeichnung in den Sitzungssälen ist zur Abwendung der in Art. 24 Abs. 1 BayDSG genannten Gefahren jedoch weder geeignet noch erforderlich.

Durch die Speicherung der übertragenen Bilder kann eine Gefahr im Sinne des Art. 24 Abs. 1 BayDSG nicht abgewehrt werden. Lediglich die Live-Beobachtung im Alarmierungsfall ermöglicht oder erleichtert schnelles Reagieren. Der „auf Vorrat“ erfolgenden Aufzeichnung der Situation kommt hingegen keinerlei gefahrenabwehrende Wirkung zu.

Zudem besteht durch die dauerhafte Videoaufzeichnung der Sitzungssäle die Möglichkeit einer Verhaltens- und Leistungskontrolle der Richterinnen und Richter, was mit deren verfassungsrechtlich garantierter Unabhängigkeit gemäß Art. 97 Abs. 1 Grundgesetz kaum in Einklang zu bringen ist. Des Weiteren sind Konflikte mit der einschlägigen Prozessordnung und dem Gerichtsverfassungsgesetz nicht auszuschließen.

Das Gericht hat meinen Bedenken Rechnung getragen und die bisher anlasslose Daueraufzeichnung aufgegeben. Stattdessen werden die Videokameras in den Sitzungssälen nur noch im Alarmierungsfall aktiviert, wenn also der an der Richterbank angebrachte Alarmknopf gedrückt wird. Diese Beschränkung auf konkrete, anlassbezogene Fälle begrüße ich ausdrücklich. Damit werden die schutzwürdigen Interessen der Richterschaft wie auch die schutzwürdigen Interessen der betroffenen Parteien und des Publikums einem angemessenen Ausgleich zugeführt.

4.3 Grundbuch: Protokollierungspflicht bei mündlicher Bestätigungsauskunft

Anlässlich eines Familienstreits hatte sich eine an einem Grundstück dinglich berechtigte Petentin mit dem Verdacht an mich gewandt, dass jemand aus ihrem familiären Umfeld unberechtigterweise Informationen aus dem Grundbuch erhalten haben könnte.

Auf meine diesbezügliche Anfrage beim zuständigen Grundbuchamt wurde mir mitgeteilt, dass eine mündliche Auskunftserteilung stattgefunden habe. Derartige mündliche Auskünfte würden nach Prüfung der Auskunftsberechtigung nur in Form von Bestätigungsauskünften erteilt, das heißt, es würden lediglich einer einsichtsersuchenden Person bekannte und von ihr vorgetragene Tatsachen bestätigt. Da mangels einer entsprechenden Pflicht derartige mündliche Auskünfte nicht protokolliert würden, sei es nicht möglich, nachzuvollziehen, wer eine solche erhalten habe.

Der Petentin konnte ich folglich bei der Aufklärung des von ihr geschilderten Sachverhaltes nicht weiterhelfen. Allerdings habe ich den Fall zum Anlass genommen, sowohl das betreffende Grundbuchamt als auch das Bayerische Staatsministerium der Justiz darauf aufmerksam zu machen, dass auch für mündliche Bestätigungsauskünfte eine Protokollierungspflicht besteht:

Eine mündliche Auskunft aus dem Grundbuch ist ein „Weniger" als eine Einsicht in das Grundbuch. § 12 Abs. 1 Satz 1 Grundbuchordnung (GBO) umfasst daher auch die Befugnis zur Erteilung mündlicher Auskünfte aus dem Grundbuch. In der Folge bedeutet dies, dass die in § 12 Abs. 4 GBO in Verbindung mit § 46a Grundbuchverfügung (GBV) geregelte Protokollierungspflicht auch bei mündlichen Bestätigungsauskünften zu beachten ist.

§ 12 GBO
(1) Die Einsicht des Grundbuchs ist jedem gestattet, der ein berechtigtes Interesse darlegt. Das gleiche gilt von Urkunden, auf die im Grundbuch zur Ergänzung einer Eintragung Bezug genommen ist, sowie von den noch nicht erledigten Eintragungsanträgen.
[…]
(4) Über Einsichten in Grundbücher und Grundakten sowie über die Erteilung von Abschriften aus Grundbüchern und Grundakten ist ein Protokoll zu führen. Dem Eigentümer des betroffenen Grundstücks oder dem Inhaber eines grundstücksgleichen Rechts ist auf Verlangen Auskunft aus diesem Protokoll zu geben, es sei denn, die Bekanntgabe würde den Erfolg strafrechtlicher Ermittlungen oder die Aufgabenwahrnehmung einer Verfassungsschutzbehörde, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes gefährden. Das Protokoll kann nach Ablauf von zwei Jahren vernichtet werden. Einer Protokollierung bedarf es nicht, wenn die Einsicht oder Abschrift dem Auskunftsberechtigten nach Satz 2 gewährt wird.

§ 46a GBV
(1) Das Protokoll, das nach § 12 Absatz 4 der Grundbuchordnung über Einsichten in das Grundbuch zu führen ist, muss enthalten:
1. das Datum der Einsicht,
2. die Bezeichnung des Grundbuchblatts,
3. die Bezeichnung der Einsicht nehmenden Person und gegebenenfalls die Bezeichnung der von dieser vertretenen Person oder Stelle,
4. Angaben über den Umfang der Einsichtsgewährung sowie

5. eine Beschreibung des der Einsicht zugrunde liegenden berechtigten Interesses; dies gilt nicht in den Fällen des § 43.

Erfolgt die Einsicht durch einen Bevollmächtigten des Eigentümers oder des Inhabers eines grundstücksgleichen Rechts, sind nur die Angaben nach Satz 1 Nummer 1 bis 3 in das Protokoll aufzunehmen.

(2) Dem Eigentümer des jeweils betroffenen Grundstücks oder dem Inhaber des grundstücksgleichen Rechts wird die Auskunft darüber, wer Einsicht in das Grundbuch genommen hat, auf der Grundlage der Protokolldaten nach Absatz 1 erteilt.

(3) […]

(4) Nach Ablauf des zweiten auf die Erstellung der Protokolle folgenden Kalenderjahres werden die nach Absatz 1 gefertigten Protokolle gelöscht. Die Protokolldaten zu Grundbucheinsichten nach Absatz 3 Satz 1 und Absatz 3a Satz 1 werden für die Dauer von zwei Jahren nach Ablauf der Frist, in der eine Bekanntgabe nicht erfolgen darf, für Auskünfte an den Grundstückseigentümer oder den Inhaber eines grundstücksgleichen Rechts aufbewahrt; danach werden sie gelöscht.

(5) Zuständig für die Führung des Protokolls nach Absatz 1 und die Erteilung von Auskünften nach Absatz 2 ist der Urkundsbeamte der Geschäftsstelle des Grundbuchamts, das das betroffene Grundbuchblatt führt.

(6) Für die Erteilung von Grundbuchabschriften, die Einsicht in die Grundakte sowie die Erteilung von Abschriften aus der Grundakte gelten die Absätze 1 bis 5 entsprechend. Das Gleiche gilt für die Einsicht in ein Verzeichnis nach § 12a Absatz 1 der Grundbuchordnung und die Erteilung von Auskünften aus einem solchen Verzeichnis, wenn hierdurch personenbezogene Daten bekanntgegeben werden.

Das betroffene Grundbuchamt hat mir versichert, dass es seine diesbezügliche Praxis geändert habe. Als besonders erfreulich möchte ich in diesem Zusammenhang hervorheben, dass auch das Justizministerium unverzüglich auf meinen Hinweis reagiert und „die grundbuchamtliche Praxis“ über den Umfang der Protokollierungspflicht nach § 12 Abs. 4 GBO in Verbindung mit § 46a GBV informiert hat.

4.4 Beanstandung einer Maßregelvollzugseinrichtung

Im Berichtszeitraum erfuhr ich von folgendem Sachverhalt:

Eine Maßregelvollzugseinrichtung ließ durch ein externes Beratungsunternehmen eine Organisationsuntersuchung sowie eine Mitarbeiterbefragung zur Organisationsentwicklung und Personalbemessung der Maßregelvollzugseinrichtung durchführen. Im Rahmen dieser Untersuchung wurde durch das Beratungsunternehmen Einsicht in die Pflegedokumentation und in die Therapiepläne der Patientinnen und Patienten genommen. Zudem wurden Ausdrucke der Pflegedokumentation sowie der Therapiepläne an das externe Beratungsunternehmen ausgehändigt.

Nach Angabe der Maßregelvollzugseinrichtung waren in den übermittelten Therapieplänen die Patientennamen und die Aktenzeichen geschwärzt. Im Übrigen wurden die Therapiepläne ungeschwärzt übergeben und enthielten beispielsweise die Namen von Angehörigen. Die Pflegedokumentation wurde ungeschwärzt an das externe Beratungsunternehmen herausgegeben. Dabei wurde allerdings das Stammblatt der Pflegedokumentation mit personenbezogenen Daten der Angehörigen, des gesetzlichen Betreuers und der einweisenden oder vorbehandelnden Klinik nicht an das Beratungsunternehmen übermittelt. Die übrigen in der Pflegedokumentation erfassten personenbezogenen Daten – wie Namen

und Geburtsdaten der Patientinnen und Patienten – wurden jedoch nicht geschwärzt.

Für eine solche Datenübermittlung durch die Maßregelvollzugseinrichtung an das externe Beratungsunternehmen bestand keine gesetzliche Befugnis. Die Maßregelvollzugseinrichtung beging deshalb durch die Datenübermittlung einen Datenschutzverstoß.

Den Verstoß gegen datenschutzrechtliche Vorschriften habe ich förmlich beanstandet (Art. 28 Abs. 2 Satz 2, Abs. 3, Art. 34 Abs. 1, Art. 16 Abs. 4 BayDSG).

Die Einrichtung stellte mir gegenüber in Aussicht, Maßnahmen zu ergreifen, um eine Wiederholung auszuschließen. Unabhängig davon ließ ich mich darüber informieren, dass die Unterlagen nach Durchsicht und Auswertung seitens des externen Beratungsunternehmens vernichtet wurden. Außerdem wurde mir versichert, dass eine Weitergabe oder gar Speicherung der übermittelten personenbezogenen Daten nicht erfolgt sei.

4.5 Abruf von Kraftfahrzeughalterdaten bei Verwarnungen im ruhenden Verkehr

In Bayern sind neben der Landespolizei auch die Gemeinden für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 24 Straßenverkehrsgesetz (StVG) zuständig (§ 88 Abs. 3 Verordnung über Zuständigkeiten im Ordnungswidrigkeitenrecht). Darunter fallen insbesondere bestimmte Geschwindigkeits- oder Parkverstöße. Die Aufgabe der Verkehrsüberwachung kann auch von Zweckverbänden wahrgenommen werden. In Bayern bestehen mehrere kommunale Zusammenschlüsse dieser Art, die entsprechende Leistungen anbieten.

Eine von mir durchgeführte datenschutzrechtliche Prüfung bei verschiedenen Gemeinden und Zweckverbänden betreffend die Ahndung von Parkverstößen kam zu dem Ergebnis, dass von dort beim Kraftfahrtbundesamt personenbezogene Daten von Kraftfahrzeughaltern in nicht erforderlicher Weise abgerufen wurden. So erfolgte im Anschluss an das Anbringen eines „Strafzettels“ an die Windschutzscheibe des betroffenen Fahrzeugs stets ein automatisierter Abruf der Halterdaten beim Kraftfahrtbundesamt. Aus datenschutzrechtlicher Sicht ist eine solche Datenerhebung noch vor Ablauf der eingeräumten einwöchigen Zahlungsfrist des § 56 Abs. 2 Ordnungswidrigkeitengesetz (OWiG) nicht erforderlich nach § 35 Abs. 1 StVG. Wird das Verwarnungsgeld fristgerecht bezahlt, ist eine Erhebung der Halterdaten des falschparkenden Kraftfahrzeugs entbehrlich. Erst nach erfolgslosem Ablauf der Zahlungsfrist oder für den Fall, dass aus technischen Gründen kein Strafzettel angebracht oder ausgestellt werden kann, ist ein Abruf der Halterdaten beim Kraftfahrtbundesamt erforderlich, um den Halter ermitteln und anschreiben zu können.

Ich konnte erreichen, dass die verwendeten Fachanwendungen so umprogrammiert wurden, dass nunmehr erst nach erfolglosem Ablauf der Zahlungsfrist eine automatisierte Abfrage der Halterdaten beim Kraftfahrtbundesamt erfolgt.

5 Allgemeine Innere Verwaltung

5.1 Behandlung von Bausachen im Gemeinderat

Im Berichtszeitraum war ich mehrfach mit datenschutzrechtlichen Problemen bei der Behandlung von Bausachen im Gemeinderat befasst. Die zentralen Fragestellungen waren hierbei der Umgang mit Bauanträgen sowie der Umgang mit Einwendungen im Rahmen der kommunalen Bauleitplanung. Im Einzelnen ist zu bemerken:

5.1.1 Umgang mit Bauanträgen

Bauanträge sind häufig in den gemeindlichen Gremien zu behandeln, insbesondere im Gemeinderat oder einem – vorberatenden oder beschließenden – Ausschuss des Gemeinderats.

5.1.1.1 Bekanntgabe personenbezogener Daten in der Tagesordnung

Wie bereits in meinem Beitrag „Bekanntgabe von Bauherrendaten in öffentlicher Gemeinderatssitzung und der Tagesordnung“[2] erläutert, sind Bauanträge grundsätzlich in öffentlicher Gemeinderatssitzung zu behandeln (vgl. Art. 52 Abs. 2 Satz 1 Gemeindeordnung – GO). Zeitpunkt und Ort der öffentlichen Sitzungen des Gemeinderats sind gemäß Art. 52 Abs. 1 Satz 1 GO unter Angabe der Tagesordnung ortsüblich bekannt zu machen. Ziel dieser Bekanntmachung ist unter anderem, das gemeindliche Handeln für die Bürger transparent zu machen.

Dabei enthält die Tagesordnung üblicherweise Bauherreninformationen, insbesondere Name und Adresse der Antragstellerin oder des Antragstellers sowie die Adresse des Baugrundstücks. Diese Angaben stellen – soweit natürliche Personen betroffen sind – personenbezogene Daten dar (vgl. Art. 4 Nr. 1 DSGVO). Eine Verarbeitung dieser personenbezogenen Daten – hier die Offenlegung gegenüber der Allgemeinheit – erfordert eine Rechtsgrundlage (Art. 6 Abs. 1 DSGVO). Bayerische öffentliche Stellen stützen sich insoweit regelmäßig auf gesetzliche Verarbeitungsbefugnisse des nationalen Rechts (vgl. Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 UAbs. 1 Buchst. b DSGVO).

Art. 52 Abs. 1 Satz 1 GO stellt nach meiner derzeitigen rechtlichen Einschätzung keine Rechtsgrundlage gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 UAbs. 1 Buchst. b DSGVO dar, weil der Vorschrift der erforderliche datenschutzbezogene Regelungsgehalt fehlt, sie insbesondere weder Übermittlungsvoraussetzungen hinreichend konkret regelt noch eine Übermittlung als Rechtsfolge anordnet, sondern letztlich nur eine Aufgabenzuweisung enthält, die datenschutzrechtlich einer Einbettung bedarf, dieser aber auch zugänglich ist. Art. 52 Abs. 1 Satz 1 GO lautet:

[2] Bayerischer Landesbeauftragter für den Datenschutz, Bekanntgabe von Bauherrendaten in öffentlicher Gemeinderatssitzung und der Tagesordnung, Internet: https://www.datenschutz-bayern.de, Rubrik „Themengebiete – Kommunales – Themen“.

„Zeitpunkt und Ort der öffentlichen Sitzungen des Gemeinderats sind unter Angabe der Tagesordnung, spätestens am dritten Tag vor der Sitzung, ortsüblich bekanntzumachen."

Sofern spezialgesetzliche Vorschriften für eine Übermittlung personenbezogener Daten fehlen, besteht für bayerische öffentliche Stellen grundsätzlich die Möglichkeit, auf Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG als allgemeine Rechtsgrundlage zurückzugreifen. Danach ist eine Übermittlung personenbezogener Daten insbesondere dann zulässig, wenn sie zur Erfüllung der Aufgaben der übermittelnden öffentlichen Stelle **erforderlich** ist. Zu den Aufgaben des ersten Bürgermeisters einer Gemeinde gehört es auch, für eine (unter anderem) den Vorgaben in Art. 52 Abs. 1 Satz 1 GO entsprechende Tagesordnung zu sorgen. Die Tagesordnung muss die in der Sitzung zu behandelnden Gegenstände so konkret benennen, dass den Gemeinderatsmitgliedern eine Vorbereitung möglich ist. In diesem Zusammenhang ist allerdings auch der Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) zu berücksichtigen.

In der Tagesordnung sind vor diesem Hintergrund die zur Bezeichnung des Bauvorhabens erforderlichen Informationen bekanntzugeben. Insoweit ist es aber regelmäßig ausreichend, den **Bauort** (Straße und Hausnummer oder Flurstücksnummer) und die **Art des Bauvorhabens** zu nennen. Darüber hinaus kann regelmäßig auch der **Name** der Bauherrin beziehungsweise des Bauherrn genannt werden, da die mit der Veröffentlichung der Tagesordnung und der Behandlung in öffentlicher Sitzung verbundene **Kontrollfunktion** – beispielsweise im Hinblick auf eine mögliche Ungleichbehandlung – **ansonsten nicht ausgeübt werden** kann. **Nicht** erforderlich ist jedoch die Bekanntgabe eines vom Bauort abweichenden **Wohnortes** der Bauherrin oder des Bauherrn. Bei Identität von Bau- und Wohnort bleibt die Veröffentlichung des Bauorts zulässig.

Soll die Tagesordnung zusätzlich zur ortsüblichen Bekanntmachung auch im **Internet**, etwa auf der Homepage der Gemeinde, veröffentlicht werden, ist auch ein für die Ausübung der Kontrollfunktion im obigen Sinne erforderlicher **Name wegzulassen beziehungsweise zu anonymisieren**, soweit dies für die Information der Öffentlichkeit nicht ausnahmsweise zwingend erforderlich ist. Diese Einschränkung beruht darauf, dass das Kommunalrecht lediglich eine ortübliche Bekanntmachung fordert und der Wirkungskreis der Gemeinde örtlich begrenzt ist.

5.1.1.2 Information der Presse durch Übermittlung von Sitzungsvorlagen

Soll die Presse bereits vor der Sitzung durch Übermittlung von Sitzungsvorlagen über die geplanten Tagesordnungspunkte näher unterrichtet werden, müssen diese durch Kürzen, Schwärzen oder vergleichbare Maßnahmen dergestalt **anonymisiert** sein, dass nur noch Informationen enthalten sind, die ohne Bedenken der Öffentlichkeit zugänglich gemacht werden dürfen.

5.1.1.3 Behandlung von Nachbareinwendungen in öffentlicher Sitzung

Auch in der öffentlichen Sitzung selbst dürfen nur diejenigen personenbezogenen Informationen bekannt gemacht werden, die für die Behandlung des Tagesordnungspunktes **erforderlich** sind. Nachbareinwendungen gegen Bauvorhaben sind zwar grundsätzlich in öffentlicher Gemeinderatssitzung zu behandeln, da insoweit kein generelles schutzwürdiges Geheimhaltungsinteresse besteht. Soweit zur sachgerechten Behandlung erforderlich – sind überhaupt nachbarliche Be-

lange berührt? – darf auch die **Adresse** der Einwenderin oder des Einwenders genannt werden. Die Bekanntgabe des **Namens** wird dagegen **regelmäßig nicht erforderlich** sein und kann nur ausnahmsweise erfolgen, wenn im Einzelfall ein besonderes sachliches Interesse besteht.

Auch bezüglich der Form der Behandlung in der Sitzung muss die Kommune den Datenschutz berücksichtigen. Insbesondere ist es **nicht erforderlich**, Einwendungsschreiben im **Original per Beamer an die Wand zu projizieren**. Dies gilt selbst dann, wenn im Einzelfall die Nennung des Namens der Einwenderin oder des Einwenders für die sachgerechte Behandlung des Sachverhalts erforderlich ist. Auch dann reicht es regelmäßig aus, die betreffenden Einwendungen inhaltlich wiederzugeben.

5.1.1.4 Veröffentlichung der Sitzungsniederschrift

Häufig werden mittlerweile Niederschriften öffentlicher Gemeinderatssitzungen veröffentlicht. Nach Abs. 54 Abs. 1 und Abs. 2 GO gefertigte Niederschriften sind jedoch offizielle Dokumente der Gemeinde mit dem Charakter öffentlicher Urkunden. Deren Veröffentlichung sieht die Gemeindeordnung nicht vor. Geregelt ist lediglich ein Einsichtsrecht für Gemeinderatsmitglieder und für die Gemeindebürgerinnen und Gemeindebürger (vgl. Art. 54 Abs. 3 GO). In meinem Beitrag „Veröffentlichung von Niederschriften über öffentliche Sitzungen des Gemeinderats im Internet“[3] habe ich die Problematik näher beleuchtet.

Zusammengefasst halte ich die Veröffentlichung von Niederschriften, welche nur den **Mindestinhalt des Art. 54 Abs. 1 GO** enthalten, im **gemeindlichen Mitteilungsblatt** und die Weitergabe derartiger Niederschriften an die **örtliche Presse** für zulässig. Soll die Veröffentlichung darüber hinaus im **Internet** erfolgen, so muss die Gemeinde das **Risiko berücksichtigen**, dass die Informationen dann regelmäßig weltweit abgerufen und ausgewertet werden können.

5.1.2 Umgang mit Einwendungen im Rahmen der kommunalen Bauleitplanung

Mehrfach wurde ich mit der Behandlung von Bürgereinwendungen im Rahmen der kommunalen Bauleitplanung befasst. Insoweit habe ich folgende Hinweise gegeben:

5.1.2.1 Bekanntgabe personenbezogener Daten bei der Öffentlichkeitsbeteiligung

Im Rahmen der Bauleitplanung können Bürgerinnen und Bürger Stellungnahmen zum Planungsvorhaben abgeben, dies sowohl bei der frühzeitigen Beteiligung der Öffentlichkeit gemäß § 3 Abs. 1 Baugesetzbuch (BauGB) als auch bei der förmlichen Öffentlichkeitsbeteiligung nach § 3 Abs. 2 BauGB. Teil der förmlichen Öffentlichkeitsbeteiligung ist auch eine Information über die Ergebnisse der frühzeitigen Öffentlichkeitsbeteiligung. Insoweit sind die Entwürfe der Bauleitpläne mit deren Begründung und den nach Einschätzung der Gemeinde wesentlichen, bereits vorliegenden umweltbezogenen Stellungnahmen öffentlich auszulegen. Der Inhalt der ortsüblichen Bekanntmachung und die auszulegenden Unterlagen sind nach

[3] Bayerischer Landesbeauftragter für den Datenschutz, Veröffentlichung von Niederschriften über öffentliche Sitzungen des Gemeinderats im Internet, Internet: https://www.datenschutz-bayern.de, Rubrik „Themengebiete – Kommunales – Themen“.

§ 4a Abs. 4 Satz 1 BauGB zusätzlich in das Internet einzustellen und über ein zentrales Internetportal zugänglich zu machen. Derartige Stellungnahmen sind aber personenbezogene Daten, soweit sie mit Informationen zu natürlichen Personen verknüpft sind. Die Verarbeitung bedarf daher einer Rechtsgrundlage.

Zwar lässt sich zunächst einmal schon bezweifeln, ob jede private Bürgereinwendung tatsächlich eine wesentliche umweltbezogene Stellungnahme im oben erläuterten Sinn ist. Jedenfalls aber sind datenschutzrechtliche Vorgaben zu beachten, wenn private Einwendungen öffentlich ausgelegt und in das Internet eingestellt werden sollen. Aus datenschutzrechtlicher Sicht hat die Gemeinde zwar die ihr durch § 3 Abs. 2 Satz 1 und § 4a Abs. 4 Satz 1 BauGB auferlegten Pflichten zu erfüllen. Diese Vorschriften sehen allerdings nicht vor, dass auch personenbezogene Daten zu übermitteln sind. Deren Übermittlung ist daher regelmäßig **nicht erforderlich** und nach Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG nicht zulässig. Sollen private Einwendungen öffentlich ausgelegt und in das Internet eingestellt werden, sind daher **personenbezogene Daten zu anonymisieren**. Dies betrifft insbesondere **Name** und **Anschrift**, aber auch **Sachangaben**, aus denen **Rückschlüsse auf die Identität** der Bürgerinnen und Bürger möglich sind.

5.1.2.2 Auftragsverarbeitung bei Einschaltung eines Planungsbüros

Die Einschaltung eines Planungsbüros und insoweit gegebenenfalls auch die Übermittlung personenbezogener Einwendungen an dieses begegnet aus datenschutzrechtlicher Sicht keinen grundsätzlichen Bedenken, solange die Gemeinde weiterhin über Mittel und Zwecke der hiermit verbundenen Datenverarbeitung entscheidet, also Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO bleibt. In § 4b BauGB hat der Gesetzgeber die Möglichkeit der Übertragung einzelner Verfahrensschritte auf private Dritte sogar explizit vorgesehen. Erforderlich ist jedoch beim Umgang des Planungsbüros mit personenbezogenen Daten der Abschluss eines Auftragsverarbeitungsvertrages gemäß Art. 28 Abs. 3 DSGVO. Zu den Einzelheiten verweise ich auf meine Orientierungshilfe Auftragsverarbeitung.[4]

5.1.2.3 Behandlung von Einwendungen in öffentlicher Sitzung

Entscheidungen in Bauleitplanverfahren werden grundsätzlich in öffentlicher Sitzung getroffen. Dies gilt auch für die planerische Abwägung. In diesem Rahmen werden auch die erhobenen Einwendungen behandelt. Die Öffentlichkeitsbeteiligung gemäß § 3 BauGB ist darauf gerichtet, die von der Planung berührten Belange umfassend ermitteln und bewerten zu können. Sie hat den Zweck, notwendiges Abwägungsmaterial zu beschaffen beziehungsweise zu vervollständigen. Die vorgebrachten Anregungen sind daraufhin zu überprüfen, ob und gegebenenfalls in welcher Weise sie berücksichtigt werden können und sollen. Die Möglichkeit der Bürgerinnen und Bürger im Rahmen der Öffentlichkeitsbeteiligung Einwendungen und Stellungnahmen abzugeben, soll das von der Kommune zusammenzustellende Abwägungsmaterial vervollständigen und so die materielle Rechtmäßigkeit von Bauleitplänen gewährleisten.

Daher ist es **regelmäßig nicht erforderlich, Bürgereinwendungen in ihrem gesamten Inhalt** bis hin zum letzten Komma **zu analysieren**. Vielmehr **genügt** es in der Regel, wenn die **anonymisierten Einwendungen** in **ihren Kernaussagen**

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

aufgelistet und jeweils den Ausführungen der Verwaltung gegenüber gestellt werden. Es geht dabei nicht um den Wortlaut der Stellungnahme, sondern um deren Inhalt. Eine öffentliche Beratung von Stellungnahmen in personenbezogener Form ist insoweit grundsätzlich nicht erforderlich. Betroffene Personen müssen zur Gewährleistung der Transparenz der gemeindlichen Verwaltungstätigkeit damit zwar hinnehmen, dass ihre Einwendungen in öffentlicher Gemeinderatssitzung behandelt werden. Dabei kann im Einzelfall die Angabe der **Adresse** (oder noch seltener des Namens) erforderlich sein, um die **Betroffenheit vom Planungsvorhaben** festzustellen. Regelmäßig wird es für die öffentliche Erörterung jedoch ausreichen, Einwendungen eine für die Öffentlichkeit anonyme Nummer zuzuweisen und unter dieser das Anliegen in öffentlicher Sitzung zu behandeln.

Selbst bei einer im Einzelfall bestehenden Erforderlichkeit der Bekanntgabe personenbezogener Daten, ist aber wiederum **kein Bedürfnis erkennbar, Originaleinwendungen** welche mittels Name, Adresse oder weiteren Informationen bestimmten Personen zugeordnet werden können, **mittels Beamer an die Wand zu projizieren**.

5.1.2.4 Veröffentlichung der Sitzungsniederschrift

Was die Veröffentlichung der Sitzungsniederschrift betrifft, gelten meine Ausführungen unter Nr. 5.1.1.4 entsprechend.

5.2 Live-Übertragung einer Bürgerversammlung ins Internet

Die fortschreitende Digitalisierung eröffnet immer neue Möglichkeiten für Information und Partizipation. Auch viele bayerische Kommunen möchten neue Formate für sich nutzen. Allerdings dürfen bei allem Verständnis für die Chancen der Digitalisierung die hiermit verbundenen datenschutzrechtlichen Risiken nicht ausgeblendet werden. Aus gutem Grund ist nicht alles, was technisch möglich ist auch (datenschutz-)rechtlich erlaubt. Dies gilt auch für den im Berichtszeitraum an mich herangetragenen Wunsch, Bürgerversammlungen live ins Internet zu übertragen, damit interessierte Bürgerinnen und Bürger diese ortsungebunden verfolgen können.

5.2.1 Live-Übertragungen öffentlicher Gemeinderatssitzungen

In meinem 21. Tätigkeitsbericht 2004 unter Nr. 11.2 habe ich mich zu der ähnlich gelagerten Frage geäußert, ob und unter welchen Umständen öffentliche Gemeinderatssitzungen live ins Internet übertragen werden können. Auch unter Geltung der Datenschutz-Grundverordnung halte ich an den im Beitrag getroffenen Aussagen inhaltlich fest. Da eine gesetzliche Rechtsgrundlage weiterhin fehlt, kommt in Bezug auf Sitzungs- und Redebeiträge von Gemeinderatsmitgliedern oder Gemeindebediensteten allenfalls eine Datenverarbeitung aufgrund wirksamer Einwilligung in Betracht (vgl. Art. 4 Nr. 11, Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 7 DSGVO). Die Einwilligung zur Übertragung ins Internet muss sich dabei sowohl auf Bild- als auch Tondaten der betroffenen Personen beziehen. Die Entscheidung über die Zustimmung muss ohne psychischen Druck auf der Grundlage ausreichender Informationen über die besonderen Modalitäten einer Interneteinstellung und mit ausreichender Überlegungsfrist erfolgen können. Die Verweigerung der Zustimmung darf nicht in diskriminierender Weise zur Kenntnis gebracht werden. Der Zuschauerraum darf nicht so in die Übertragung einbezogen werden,

dass einzelne Zuschauer erkannt werden können. Gegebenenfalls ist statt einer Liveübertragung eine Aufzeichnung ins Internet einzustellen.

5.2.2 Live-Übertragung von Bürgerversammlungen ins Internet

Die eben erläuterten Grundsätze gelten auch für die Live-Übertragung von Bürgerversammlungen ins Internet. Im Ergebnis dürfte diese allerdings **kaum einmal datenschutzrechtlich zulässig sein**. Im Einzelnen:

5.2.2.1 Bürgerversammlung als Ausdruck einer bürgernahen Selbstverwaltung

Die Bürgerversammlung nach Art. 18 Gemeindeordnung (GO) ist ein „Gremium der kommunalen Selbstverwaltung".[5] Sie dient der Sicherstellung der bürgerschaftlichen Teilhabe an und der Einbeziehung in die gemeindliche Willensbildung und damit einer bürgernahen Selbstverwaltung.[6] In der Bürgerversammlung können Gemeindeangehörige das Wort erhalten (Art. 18 Abs. 3 Satz 1 GO). Der Vorsitzende soll einem Vertreter der Aufsichtsbehörde auf Verlangen das Wort erteilen (Art. 18 Abs. 3 Satz 2 GO).

Art. 18 GO
Mitberatungsrecht (Bürgerversammlung)
(1) [1]In jeder Gemeinde hat der erste Bürgermeister mindestens einmal jährlich, auf Verlangen des Gemeinderats auch öfter, eine Bürgerversammlung zur Erörterung gemeindlicher Angelegenheiten einzuberufen. [2]In größeren Gemeinden sollen Bürgerversammlungen auf Teile des Gemeindegebiets beschränkt werden.
(2) […]
(3) [1]Das Wort können grundsätzlich nur Gemeindeangehörige erhalten. [2]Ausnahmen kann die Bürgerversammlung beschließen; der Vorsitzende soll einem Vertreter der Aufsichtsbehörde auf Verlangen das Wort erteilen. [3]Den Vorsitz in der Versammlung führt der erste Bürgermeister oder ein von ihm bestellter Vertreter. [4]Stimmberechtigt sind ausschließlich Gemeindebürger.

(4) […]

Werden durch die Gemeinde Ton- und Filmaufnahmen von Gemeindeangehörigen, Vertreterinnen und Vertretern von Aufsichtsbehörden oder anderen Personen, die auf der Bürgerversammlung das Wort erhalten oder dieser als Zuschauerinnen oder Zuschauer beiwohnen, angefertigt und live ins Internet übertragen, so liegt eine **Verarbeitung personenbezogener Daten durch die Gemeinde** vor, für die (jeweils) eine **Rechtsgrundlage benötigt wird** (vgl. Art. 6 Abs. 1 DSGVO). Dies gilt auch in Bezug auf die Daten von Bürgerinnen und Bürgern, deren Angelegenheiten auf der Bürgerversammlung personenbezogen oder personenbeziehbar behandelt werden, wenn eine Übertragung ins Internet beabsichtigt ist.

5.2.2.2 Fehlen einer gesetzlichen Befugnis für die Datenverarbeitung

Öffentliche Stellen sollen sich bei der Erfüllung ihrer öffentlichen Aufgaben vorrangig auf die speziellen **fachgesetzlichen Rechtsgrundlagen** zur Verarbeitung personenbezogener Daten nachrangig auf die allgemeine Befugnisnorm des

5 Vgl. Landtags-Drucksache 17/14651, S. 16.
6 Suerbaum/Retzmann, in: Dietlein/Suerbaum, BeckOK Kommunalrecht Bayern, 3. Edition 8/2019, Art. 18 Rn. 4 m. w. N.

Art. 4 Abs. 1 BayDSG, respektive für die Übermittlung von personenbezogenen Daten auf **Art. 5 Abs. 1 BayDSG** stützen. Eine fachgesetzliche Vorschrift zur Übermittlung von Bild- und Tonaufnahmen bei Bürgerversammlungen ins Internet ist indes nicht ersichtlich. Insbesondere enthält Art. 18 GO keine derartige Regelung.

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

Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG scheidet als Rechtsgrundlage aber **aus**, da die Übermittlung von Bild- und Tonaufnahmen bei Bürgerversammlungen gerade nicht zu den gesetzlichen Aufgaben der Gemeinde gehört. Insbesondere kann eine solche Aufgabe nicht Art. 18 GO entnommen werden.

Auch kann ich nicht erkennen, dass die Voraussetzungen des **Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG** erfüllbar wären. Die Norm setzt nämlich in Bezug auf die jede fragliche Datenverarbeitung eine konkrete Interessenabwägung und Prüfung der Berechtigung des Interesses der oder des Auskunftsersuchenden durch den Verantwortlichen (also die Gemeinde) voraus. Auf eine pauschale Übermittlung von personenbezogenen Daten an eine nicht näher bekannte oder gar unbegrenzte Anzahl von Empfängern, wie es bei einer Live-Übertragung ins Internet der Fall wäre, ist Art. 5 Abs. 1 Satz 1 Nr. 2 BayDSG ebenso wenig zugeschnitten wie auf eine initiative Übermittlung (siehe Beitrag Nr. 5.3). In diesem Zusammenhang ist bei einer Übertragung im Internet auch zu berücksichtigen, dass damit eine völlig **neue Qualität der Veröffentlichung** erreicht wird. Die Veröffentlichung im Internet wird weltweit einen ungleich größeren Personenkreis zugänglich als jede auflagenbegrenzte schriftliche Presseveröffentlichung oder die Berichterstattung in einem lokalen Rundfunksender. Bild und Ton können von jedermann abgerufen, aufgezeichnet und ausgewertet werden, und die weitere Verwendung dieser Aufnahme ist nicht abzusehen. Bei der Direktübertragung einer Bürgerversammlung im Internet werden Teilnehmerinnen und Teilnehmer mit ihrer Mimik und Gestik sowie ihren Redebeiträge im Wortlaut weltweit abrufbar. Dies kann dazu führen, dass sich Gemeindeangehörige nicht mehr unbefangen und spontan äußern. Damit besteht durchaus die Gefahr, dass **Funktion und Idee der Bürgerversammlung beeinträchtigt werden** und damit der Demokratie insgesamt Schaden zugefügt wird.

5.2.2.3 Einwilligung wird regelmäßig an mangelnder Freiwilligkeit scheitern

Damit bleibt nur noch die – allerdings eher theoretische – Möglichkeit, die Verarbeitung auf Einwilligungen im Sinne von Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO zu stützen. Allerdings müssten für die Wirksamkeit die gesetzlichen Anforderungen erfüllt sein. Die Einwilligung muss danach insbesondere **freiwillig** (Art. 4 Nr. 11, Art. 7 Abs. 3 Satz 3 DSGVO), informiert (Art. 4 Nr. 11 DSGVO), auf einen bestimmten Zweck (Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO) und auf eine bestimmte Verarbeitung bezogen (Art. 4 Nr. 11 DSGVO) sowie unmissverständlich (Art. 4 Nr. 11 DSGVO) sein. Sie wirkt grundsätzlich bis zu ihrem Widerruf (Art. 7 Abs. 3 Sätze 1

und 2 DSGVO). Indes habe ich erhebliche **Zweifel, ob** die Gemeinde die erforderliche **Freiwilligkeit** garantieren kann (zur Nachweispflicht der Gemeinde vgl. Art. 5 Abs. 2, Art. 7 Abs. 1 DSGVO).

Freiwilligkeit setzt voraus, dass der Einwilligende eine echte und freie Wahl hat und in der Lage sein muss, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden (Erwägungsgrund 42 DSGVO). Um sicherzustellen, dass die Einwilligung freiwillig erfolgt ist, sollte diese in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern (Erwägungsgrund 43 DSGVO). Auch wenn die Einholung von Einwilligungen durch Behörden damit nicht völlig ausgeschlossen ist, müssen diese doch speziell bei der geplanten Live-Übertragung vor Bürgerversammlungen ins Internet Folgendes berücksichtigen:

Zunächst müsste die Gemeinde darauf hinweisen, dass bei einer Internet-Übertragung Bild und Ton weltweit von einem unbegrenzten Kreis von Personen abgerufen, aufgezeichnet, unter Umständen verändert und ausgewertet werden können und die weitere Verwendung dieser Aufnahmen nicht abzusehen ist. Vor allem aber dürfen Teilnehmerinnen und Teilnehmer der Bürgerversammlung **nicht unter Entscheidungsdruck gesetzt** werden. Das wäre etwa der Fall, wenn sie erst während der Veranstaltung, also im Beisein von Anderen und gegebenenfalls der Presse mit dem Wunsch nach einer Übertragung der Bürgerversammlung ins Internet konfrontiert würden. Eine freiwillige Einwilligung könnte in einem solchen Fall nicht angenommen werden. Teilnehmenden muss vielmehr eine **angemessene Überlegungsfrist** für ihre Entscheidung eingeräumt werden. Da bei Bürgerversammlungen jedoch – anders als etwa bei Gemeinderatssitzungen, bei welchen im Voraus grundsätzlich feststeht, welche Gemeinderatsmitglieder zugegen sind – im Vorfeld nicht absehbar ist, wer anwesend sein und das Wort ergreifen wird, dürfte es kaum möglich sein, die Freiwilligkeit von Einwilligungen zu gewährleisten. Auch auf dieser Rechtsgrundlage wird daher regelmäßig keine Live-Übertragung von Bürgerversammlungen ins Internet möglich sein. Hinzu kommt, dass auch diejenigen Bürgerinnen und Bürger, die die Einwilligung verweigern, nicht vom Besuch der Bürgerversammlung ausgeschlossen werden dürfen. Für diese wäre dann zusätzlich ein erfassungsfreier Bereich vorzusehen und es wäre zusätzlich sicherzustellen, dass deren eventuelle Wortbeiträge nicht in einer Art und Weise erfasst werden, dass diese konkreten Personen zuordenbar sind.

5.3 Informantenschutz bei Datenübermittlungen unter Geltung der Datenschutz-Grundverordnung

Zu der Frage, wie öffentliche Stellen datenschutzkonform mit Hinweisen von Bürgerinnen und Bürger auf (vermeintlich) rechtswidrige Handlungen Dritter umgehen sollen, habe ich mich bereits in meinem 24. Tätigkeitsbericht 2010 unter Nr. 6.10 geäußert. Die Vielzahl von Eingaben, die mich hierzu seit Geltungsbeginn der Datenschutz-Grundverordnung erreicht haben, veranlasst mich jedoch, meine damaligen Ausführungen zu aktualisieren und in einen größeren Zusammenhang einzubetten.

Gleichsam vor die Klammer gezogen möchte ich jedoch schon an dieser Stelle betonen, dass sich die dem Informantenschutz zugrundeliegenden Wertungen mit

Geltungsbeginn der Datenschutz-Grundverordnung nicht wesentlich geändert haben und insbesondere ein reflexhaftes In-Kenntnis-Setzen der „Gegenpartei" von erhobenen Vorwürfen weiterhin datenschutzrechtlich unzulässig ist.

Nur hinweisen möchte ich an dieser Stelle auf das verwandte Thema „Informantenschutz bei Auskunftsanträgen". Nach Art. 15 Abs. 1 Halbsatz 2 Buchst. g DSGVO kann eine betroffene Person Informationen über die Herkunft von personenbezogenen Daten verlangen, die der Verantwortliche nicht bei ihr erhoben hat. Dazu können auch „Beschuldigungen" von dritter Seite zählen. Auch insoweit kommt ein Informantenschutz in Betracht. Insofern möchte ich auf meine Orientierungshilfe zu Art. 15 DSGVO[7] sowie auf den Beitrag Nr. 8.2 in diesem Tätigkeitsbericht verweisen.

5.3.1 Datenschutzrechtliche Bewertung anhand Art. 5 Abs. 1 BayDSG

Leitet eine öffentliche Stelle Bürgereingaben wie etwa Beschwerden oder sonstige Hinweise auf (vermeintlich) rechtswidrige Handlungen Dritter an andere öffentliche oder nicht öffentliche Stellen weiter, insbesondere an denjenigen, der Anlass der Beschwerde war, und ist hierbei – etwa über den Namen oder die E-Mail Adresse – ein Rückschluss auf die Person der oder des Eingebenden möglich, liegt eine Verarbeitung personenbezogener Daten vor. Diese Verarbeitung bedarf nach Art. 6 Abs. 1 DSGVO einer Rechtsgrundlage. Soweit – wie regelmäßig der Fall –, weder eine Einwilligung (vgl. Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO) noch eine (mitgliedsstaatliche) spezialgesetzliche Befugnisnorm (vgl. Art. 6 Abs. 1 UAbs. 1 Buchst. e in Verbindung mit Abs. 3 UAbs. 1 Buchst. b DSGVO) vorliegt, kann eine personenbezogene Weiterleitung von Bürgereingaben allenfalls auf Art. 5 Abs. 1 BayDSG gestützt werden. Diese Vorschrift lautet:

„[1]Eine Übermittlung personenbezogener Daten ist zulässig, wenn
1. sie zur Erfüllung einer der übermittelnden oder der empfangenden öffentlichen Stelle obliegenden Aufgabe erforderlich ist oder
2. der Empfänger eine nicht öffentliche Stelle ist, diese Stelle ein berechtigtes Interesse an ihrer Kenntnis glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat; dies gilt auch, soweit die Daten zu anderen Zwecken als denjenigen, zu denen sie erhoben wurden, übermittelt werden.
[2]Bei einer Übermittlung nach Satz 1 Nr. 2 darf der Empfänger die übermittelten Daten nur für den Zweck verarbeiten, zu dem sie ihm übermittelt wurden."

Nach Art. 5 Abs. 1 Satz 1 **Nr. 1** BayDSG ist die Übermittlung personenbezogener Daten zulässig, wenn sie zur Erfüllung einer der übermittelnden oder der empfangenden öffentlichen Stelle obliegenden Aufgabe **erforderlich** ist.

An der Erforderlichkeit fehlt es insbesondere dann, wenn der geschilderte Sachverhalt auch ohne Offenlegung der Identität der oder des Eingebenden bewertbar ist und – gegebenenfalls nach weiteren behördlichen Ermittlungen – etwaigen Verwaltungshandlungen zu Grunde gelegt werden kann.

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

Verdeutlichen möchte ich dies an folgendem **Beispielsfall aus dem Berichtszeitraum**: Eine öffentliche Stelle wurde von privater Seite über Sicherheitsbedenken hinsichtlich einer geplanten Veranstaltung in einer Einrichtung für Schutzsuchende informiert und hat diese Information personenbezogen an den Veranstalter weitergeleitet. Zur Begründung hierfür wurde angeführt, dass ein sachlicher Hinweis auf die geäußerten Bedenken ohne Übermittlung des vollständigen Schriftverkehrs samt personenbezogener Daten zur Risikoabschätzung des Veranstalters und damit mittelbar auch zur Erfüllung der öffentlichen Aufgabe des Schutzes von Leib und Leben der Bevölkerung, nicht ausgereicht hätte. Dem Sachverhalt ließen sich aber keine Hinweise darauf entnehmen, dass der Veranstalter zu einer anderen Bewertung des Warnhinweises gekommen wäre, hätte er den Namen der eingebenden Person nicht gekannt. Die dargelegten Gründe für die Bedenken ließen vielmehr eine Einschätzung auch ohne weitere personenbezogene Informationen zu. Insbesondere war gerade **keine Bedrohungslage durch die eingebende Person selbst** erkennbar, welche deren Identifizierung seitens des Veranstalters erfordert hätte. Die **Übermittlung des Schriftverkehrs samt Namen der eingebenden Person** war damit zur Erfüllung von Aufgaben der öffentlichen Stelle **nicht erforderlich**. Die bloße Sachinformation oder gegebenenfalls die Übermittlung einer hinsichtlich der personenbezogenen Daten geschwärzten E-Mail hätte vollkommen ausgereicht.

Auch Art. 5 Abs. 1 **Nr. 2** BayDSG wird regelmäßig kein anderes Ergebnis rechtfertigen. Nach dieser Norm ist die Übermittlung personenbezogener Daten zulässig, wenn der Empfänger eine **nicht öffentliche Stelle** ist, diese Stelle ein **berechtigtes Interesse an ihrer Kenntnis glaubhaft darlegt** und die betroffene Person **kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung** hat.

Insoweit ist vorneweg klarzustellen, dass Art. 5 Abs. 1 Nr. 2 BayDSG Datenübermittlungen an andere öffentliche Stellen schon vom klaren Wortlaut her nicht umfasst. Gleiches gilt aber grundsätzlich auch für eigeninitiativ erfolgte Datenübermittlungen an nicht öffentliche Stellen, da es dann regelmäßig an der vorherigen glaubhaften Darlegung eines berechtigten Interesses an der Kenntnis fehlen wird. Ein berechtigtes Interesse ist jedes nach vernünftigen Erwägungen unter Berücksichtigung der Besonderheiten des Falles anzuerkennendes, der Rechtsordnung nicht widersprechendes Interesse. Umfasst sind damit nicht nur die im Zusammenhang mit der Verfolgung von Rechten stehenden rechtlichen Interessen, sondern auch ideelle und wirtschaftliche Interessen. Ein berechtigtes Interesse an der Datenkenntnis setzt aber immer voraus, dass die Empfängerin oder der Empfänger die Daten in irgendeiner Form **benötigt**, wofür schon das Interesse an der Schaffung eines vernünftigerweise zuzubilligenden Informationsstandes an sich ausreichen kann. Unterhaltungsbedürfnis, Neugier und Sensationslust allein bedingen demgegenüber kein berechtigtes Interesse.[8]

Das schutzwürdige Interesse der von einer Datenübermittlung betroffenen Person ist bei der Entscheidung, ob diese zulässig ist, gegenüber dem berechtigten Interesse der Empfängerin oder des Empfängers der Daten abzuwägen, wobei an dieser Stelle **das schutzwürdige Interesse der eingebenden Person regelmäßig überwiegt**. Insbesondere ist zu berücksichtigen, dass einer Bürgerin oder einem Bürger, **die oder der eine Behörde auf tatsächliche oder vermeintliche Gefahren hinweist, dadurch keine Nachteile entstehen sollen.** Dies ist letztlich

[8] Vgl. Niese, in: Wilde/Ehmann/Niese/Knoblauch, Datenschutz in Bayern, Stand 6/2019, Art. 5 BayDSG Rn. 18.

auch im Interesse von Behörden, die zur ordnungsgemäßen Erfüllung ihrer Aufgaben auf derartige Informationen angewiesen sind. Die Bürgerinnen und Bürger vertrauen darauf, dass ihre Hinweise im Bereich der Verwaltung verbleiben. **Dies gilt unabhängig davon, ob um vertrauliche Behandlung gebeten wurde.** Dem Interesse des potentiellen Informationsempfängers steht das Interesse der eingebenden Person nur dann nicht entgegen, wenn es sich um haltlose, grob unwahre oder gar verleumderische Angaben handelt, gegen die sich eine die Anzeige betreffende Person zur Wehr setzen will.[9]

5.3.2 Parallele Maßstäbe bei (verwaltungsverfahrensrechtlicher) Akteneinsicht

Ein Verwaltungsverfahren ist gemäß Art. 9 Bayerisches Verwaltungsverfahrensgesetz (BayVwVfG) die nach außen wirkende Tätigkeit der Behörden, die auf die Prüfung der Voraussetzungen, die Vorbereitung und den Erlass eines **Verwaltungsakts** oder auf den Abschluss eines **öffentlich-rechtlichen Vertrags** gerichtet ist. Nach Art. 29 Abs. 1 BayVwVfG hat die Behörde den Beteiligten Einsicht in die einzelnen Teile der das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Die Norm kann wohl als Ausdruck eines allgemeinen Rechtsgedankens entsprechend für sonstige behördliche Auskünfte herangezogen werden.[10] So kommt wohl neben Zugangsansprüchen nach Art. 39 BayDSG und § 9 Allgemeine Geschäftsordnung für die Behörden des Freistaates Bayern und den insoweit geregelten Anforderungen auch ein Akteneinsichtsrecht im Rahmen einer Ermessensentscheidung in Betracht, wenn die Antragstellerin oder der Antragsteller ein berechtigtes Interesse hieran geltend macht. Zur Gewährung von Akteneinsicht hat eine Behörde ihre Ermessensentscheidung so zu treffen, dass unter Berücksichtigung des Grundprinzips des rechtsstaatlichen und fairen Verfahrens eine beiderseits sachgerechte Interessenwahrung möglich ist. Außerdem muss die Kenntnis des Akteninhalts Voraussetzung für eine wirksame Rechtsverfolgung sein.[11]

Umfasst eine begehrte Akteneinsicht Erkenntnisse mit Personenbezug zu einer Hinweisgeberin oder einem Hinweisgeber, so muss das Zugangsinteresse der die Akteneinsicht begehrenden Person gegen das Vertraulichkeitsinteresse der Hinweisgeberin oder des Hinweisgebers abgewogen werden. Diesen steht auch **bei einer Akteneinsicht regelmäßig ein schutzwürdiges Interesse an der Geheimhaltung ihrer Identität** zu. Auch insoweit muss berücksichtigt werden, dass Bürgerinnen und Bürger, die eine Behörde auf tatsächliche oder vermeintliche Missstände und Verstöße gegen Rechtsvorschriften aufmerksam machen, dadurch keine Nachteile entstehen sollen. Ich verweise hierzu auf meine Ausführungen unter Nr. 5.3.1. Liegt ein solches schutzwürdiges Interesse vor, so ist darauf zu achten, dass bei der Akteneinsicht die personenbezogenen Daten der eingebenden Person in der Akte **nicht** enthalten sind. Regelmäßig dürfte insoweit die Schwärzung der entsprechenden Passagen erforderlich sein.

9 Vgl. hierzu die weiterhin heranziehbare Kommentierung von Ehmann, in: Wilde/Ehmann/Niese/Knoblauch, Datenschutz in Bayern, Stand 3/2016, Art. 10 BayDSG-alt Rn. 49a–k.

10 Kritisch aber Herrmann, in: Bader/Ronellenfitsch, BeckOK VwVfG, 45. Edition 10/2019, § 29 VwVfG Rn. 7 f.

11 Bayerischer Verwaltungsgerichtshof, Urteil vom 17. Februar 1998, 23 B 95.1954, BeckRS 1998, 100012, Rn. 30 ff.

5.3.3 Besonderheiten im Ordnungswidrigkeitenverfahren

Gibt die Eingabe jedoch Anlass zur Einleitung eines Ordnungswidrigkeitenverfahrens, bemisst sich der Informantenschutz nicht an den Vorgaben der Datenschutz-Grundverordnung. Vielmehr fällt die Datenverarbeitung in einem Ordnungswidrigkeitenverfahren in den Anwendungsbereich der Datenschutzrichtlinie für Polizei und Strafjustiz, so dass sich die datenschutzrechtlichen Vorgaben aus dem Gesetz über Ordnungswidrigkeiten (OWiG), der Strafprozessordnung und Art. 28 ff. BayDSG ergeben. Das Recht auf Akteneinsicht bei der Verwaltungsbehörde besteht insoweit nach Maßgabe des § 49 Abs. 1 OWiG. Dort heißt es:

„Die Verwaltungsbehörde gewährt dem Betroffenen auf Antrag Einsicht in die Akten, soweit der Untersuchungszweck, auch in einem anderen Straf- oder Bußgeldverfahren, nicht gefährdet werden kann und nicht überwiegende schutzwürdige Interessen Dritter entgegenstehen. Werden die Akten nicht elektronisch geführt, können an Stelle der Einsichtnahme in die Akten Kopien aus den Akten übermittelt werden."

Gemäß § 49 Abs. 1 Satz 1 OWiG gewährt die Verwaltungsbehörde der Betroffenen oder dem Betroffenen auf Antrag Einsicht in die Akten, soweit der Untersuchungszweck, auch in einem anderen Straf- oder Bußgeldverfahren, nicht gefährdet werden kann und nicht überwiegende schutzwürdige Interessen Dritter **entgegenstehen**.

Der Informantenschutz wiegt hier allerdings weniger stark als im Verwaltungsverfahren; er muss im Ordnungswidrigkeitenverfahren regelmäßig zurücktreten. Nimmt die anzeigende Person den Status einer Zeugin oder eines Zeugen ein, so ist nur unter sehr engen Voraussetzungen ein Informantenschutz möglich. Hintergrund für die Änderung des Bewertungsmaßstabs ist die Maxime, dass die betroffene Person, gegen die ein Bußgeld erlassen wird, eine angemessene Möglichkeit zur Verteidigung erhalten soll, zu der auch die Kenntnis der Beweismittel gehört.

5.4 Datenschutzkonformität von (staatlichen) Förderungen

Im Berichtszeitraum war ich auch mit der Datenschutzkonformität von (staatlichen) Förderungen befasst. Exemplarisch greife ich die Beantragung von Aufwandsentschädigungen im Rahmen der Tierseuchenprävention heraus. Ein Antragsteller hatte sich an mich gewandt und das Förderverfahren hinterfragt. Meine datenschutzrechtliche Überprüfung ergab insoweit eine Reihe von Mängeln, die nach intensiven Diskussionen mit dem fachlich zuständigen Staatsministerium im Wesentlichen behoben werden konnten. Auf folgende Punkte, welche von generellem Interesse sind, möchte ich hinweisen:

5.4.1 Einwilligung regelmäßig keine Rechtsgrundlage

Gerade bei der staatlichen Leistungsgewährung im Rahmen von Förderverfahren wird von den Verantwortlichen als Rechtsgrundlage für eine Verarbeitung personenbezogener Daten gerne die Einwilligung (vgl. Art. 6 Abs. 1 Uabs. 1 Buchst. a DSGVO) herangezogen. Beispielsweise findet sich in den verwendeten Antragsformularen etwa folgende Formulierung:

„Mit der Verarbeitung meiner mit diesem Antrag erhobenen Daten zur Auszahlung der Aufwandsentschädigung im Zusammenhang mit vorbeugenden Präventionsmaßnahmen gegen […] besteht Einverständnis."

Hierzu ist aus datenschutzrechtlicher Sicht (siehe näher Beitrag Nr. 5.2.2.3) darauf hinzuweisen, dass öffentliche Stellen Verarbeitungen personenbezogener Daten regelmäßig auf eine gesetzliche Befugnis gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 UAbs. 1 Buchst. b DSGVO stützen sollen. Sie dürfen personenbezogene Daten auf der Grundlage von **Einwilligungen nur in Ausnahmefällen** verarbeiten.

Daran ändert es auch nichts, dass im Bereich der Leistungsverwaltung in Gestalt von Förderverfahren regelmäßig keine Verpflichtung zur (vollständigen) Antragstellung besteht, die Antragsteller also eigenverantwortlich entscheiden, ob sie eine Leistung in Anspruch nehmen möchten. Wenn sie dies tun, müssen sie nach Maßgabe des Fachrechts vollständige und zutreffende Angaben machen, um die Leistung zu bekommen. Dies ist jedoch nicht originär eine Frage der Rechtsgrundlage für die Datenverarbeitung als solche, sondern vielmehr Gegenstand der Hinweispflicht nach Art. 13 Abs. 2 Buchst. e DSGVO bei der Datenerhebung (dazu näher allgemein sogleich unter Nr. 5.4.4) auf die möglichen Folgen einer Nichtbereitstellung personenbezogener Daten. Auch die Verarbeitung personenbezogener Daten in einem Förderverfahren bedarf gleichwohl regelmäßig einer (parlaments-)gesetzlichen Befugnis und kann nicht auf eine Einwilligung gestützt werden. Sollte es an einer speziellen fachrechtlichen Regelung fehlen, steht bayerischen öffentlichen Stellen regelmäßig die allgemeine Verarbeitungsbefugnis aus Art. 4 Abs. 1 BayDSG zur Verfügung. Entscheidend ist danach, ob und inwieweit die konkrete Datenverarbeitung zur Aufgabenerfüllung erforderlich ist.

5.4.2 Umfang der zulässigen Aufgabenerfüllung ergibt sich aus der jeweiligen Aufgabenzuweisungsnorm

Ob und in welchem Umfang eine Verarbeitung personenbezogener Daten zur Aufgabenerfüllung tatsächlich erforderlich ist, muss anhand der konkreten Aufgabenzuweisung an die das Förderverfahren durchführende Stelle beurteilt werden. Der bloße pauschale **Verweis auf eine erfolgte Zuweisung von Haushaltsmitteln** durch übergeordnete Stellen **genügt insoweit gerade nicht** (vgl. Art. 77 Abs. 1 Verfassung des Freistaates Bayern). Sollen im Rahmen des Antragsverfahrens Unterlagen beigefügt werden, welche auch Angaben enthalten können, die für die Zwecke des Förderverfahrens nicht erforderlich sind, ist unmissverständlich darauf hinzuweisen, dass diese **überschießenden Angaben unkenntlich gemacht werden dürfen**.

5.4.3 Anforderungen bei einer Einbindung von Dritten in das Förderverfahren

Sollen Dritte, insbesondere nicht-öffentliche Stellen wie etwa im jeweiligen Sachbereich tätige private Verbände, in die technisch-organisatorische Abwicklung des Förderverfahrens unter Oberhoheit einer öffentliche Stelle eingebunden werden und kommt es in diesem Rahmen zur Verarbeitung personenbezogener Daten von Antragstellerinnen und Antragstellern, sollte geprüft werden, ob der Abschluss einer Auftragsverarbeitungsvereinbarung nach Art. 28 DSGVO angezeigt ist. Zum

erforderlichen Inhalt solcher Auftragsverarbeitungsvereinbarungen verweise ich allgemein auf meine Orientierungshilfe Auftragsvereinbarung.[12]

Insoweit wird es mit der die Auftragsverarbeitung prägenden Rollenverteilung zwischen der das Förderverfahren durchführenden öffentlichen Stelle als Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO und dem zur Abwicklung eingebundenen Dritten als Auftragsverarbeiter gemäß Art. 4 Nr. 8 DSGVO regelmäßig nicht vereinbar sein, wenn das an prominenter Stelle das Logo beziehungsweise Wappen des Dritten zeigende Antragsformular nur bei diesem bezogen werden kann und gleichzeitig im Förderverfahren in keiner Weise auf die eigentliche Verfahrensherrschaft der öffentlichen Stelle hingewiesen wird. Die im Rahmen der Hinweispflicht nach Art. 13 Abs. 1 Buchst. a DSGVO bei der der Datenerhebung (dazu Näher allgemein sogleich unter Nr. 5.4.4) gemachten Angaben zum Verantwortlichen müssen mit dem realen Ablauf des Förderverfahrens übereinstimmen.

5.4.4 Umsetzung der Informationspflichten nach Art. 13 DSGVO

Als Ausfluss der soeben erläuterten Kritikpunkte hat auch die datenschutzkonforme Umsetzung der Informationspflichten nach Art. 13 DSGVO nicht unerhebliche Schwierigkeiten bereitet. Art. 13 DSGVO fordert, dass betroffenen Personen zum Zeitpunkt der Erhebung ihrer personenbezogenen Daten eine Vielzahl von Informationen zur Verfügung gestellt werden.

Art. 13 DSGVO
Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person
(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere

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

Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

b) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und

f) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

[...]

Wie ich in meiner Orientierungshilfe „Informationspflichten des Verantwortlichen“[13] ausgeführt habe, hat die in Art. 13 DSGVO festgelegte Verpflichtung den Zweck, betroffenen Personen die Möglichkeit zu eröffnen, sich einen Überblick insbesondere über Zweck und Umfang der Verarbeitung ihrer personenbezogenen Daten zu verschaffen. Sie sollen damit auch in die Lage versetzt werden, die Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen einschätzen zu können. Zugleich sollen die betroffenen Person erfahren, welche Rechte ihnen in diesem Zusammenhang zustehen (beispielsweise das Recht auf Auskunft nach Art. 15 DSGVO oder das Recht auf Berichtigung nach Art. 16 DSGVO).

Gerade bei (staatlichen) Förderungen unter technisch-organisatorischer Einbindung von privaten Verbänden in die Durchführung des Verfahrens ist besonderes Augenmerk darauf zu richten, dass Name und Kontaktdaten des (tatsächlich) Verantwortlichen (vgl. Art. 13 Abs. 1 Buchst. a DSGVO), Zwecke und Rechtsgrundlage (regelmäßig nicht Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO) für die Verarbeitung (vgl. Art. 13 Abs. 1 Buchst. c DSGVO) sowie die Folgen einer Nichtbereitstellung personenbezogener Daten (vgl. Art. 13 Abs. 2 Buchst. e DSGVO) zutreffend erläutert werden. Daneben sind natürlich wie stets alle sonstigen Anforderungen des Art. 13 Abs. 1 und 2 DSGVO zu erfüllen.

5.5 Datenschutz bei Mobilitätsuntersuchungen auf Landkreisebene

Sowohl der Bau von Kreisstraßen (vgl. Art. 51 Abs. 2 in Verbindung mit Abs. 1 Landkreisordnung – LKrO) als auch Planung, Organisation und Sicherstellung des

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

allgemeinen öffentlichen Personennahverkehrs (vgl. Art. 8 Abs. 1 Gesetz über den öffentlichen Personennahverkehr in Bayern – BayÖPNVG) gehören grundsätzlich zu den Aufgaben der Landkreise.

Wenn etwa Landkreise Konzepte für zukünftige Infrastrukturprojekte entwickeln, kann es sinnvoll sein, vorab sogenannte Mobilitätsuntersuchungen durchzuführen. Diese sehen unter anderem Befragungen vor, anhand welcher der künftige Bedarf an Straßen, Fahrradwegen und öffentlichen Nahverkehrsverbindungen ermittelt werden soll. Ausdrücklich gesetzlich in Art. 13 BayÖPNVG geregelt ist der Nahverkehrsplan, bei dem das künftig zu erwartende Verkehrsaufkommen im motorisierten Individualverkehr und im öffentlichen Personennahverkehr auf Schiene und Straße zu prognostizieren ist (vgl. Art. 13 Abs. 1 Satz 3 Nr. 2 BayÖPNVG). Mobilitätsuntersuchungen auf Landkreisebene sind daher grundsätzlich von der Aufgabenzuweisung an die Landkreise umfasst.

Art. 51 LKrO
Aufgaben des eigenen Wirkungskreises
(1) Im eigenen Wirkungskreis sollen die Landkreise in den Grenzen ihrer Leistungsfähigkeit die öffentlichen Einrichtungen schaffen, die für das wirtschaftliche, soziale und kulturelle Wohl ihrer Einwohner nach den Verhältnissen des Kreisgebiets erforderlich sind; hierbei sind die Belange des Natur- und Umweltschutzes zu berücksichtigen.
(2) Im Rahmen des Absatzes 1 sind die Landkreise, unbeschadet bestehender Verbindlichkeiten Dritter, verpflichtet, nach Maßgabe der gesetzlichen Vorschriften die erforderlichen Maßnahmen auf den Gebieten der Straßenverwaltung, der Feuersicherheit, des Gesundheitswesens sowie der öffentlichen Fürsorge und Wohlfahrtspflege zu treffen oder die nötigen Leistungen für solche Maßnahmen aufzuwenden.
[…]

Art. 8 BayÖPNVG
Aufgabenträger
(1) [1]Die Planung, Organisation und Sicherstellung des allgemeinen öffentlichen Personennahverkehrs ist eine freiwillige Aufgabe der Landkreise und kreisfreien Gemeinden im eigenen Wirkungskreis. [2]Sie führen diese Aufgaben in den Grenzen ihrer Leistungsfähigkeit durch. [3]Sie sollen sich für diese Aufgaben Dritter, insbesondere der privaten Planungsbüros und der privaten Verkehrsunternehmen, bedienen.
[…]

Art. 13 BayÖPNVG
Nahverkehrsplan
(1) [1]Die Aufgabenträger des allgemeinen öffentlichen Personennahverkehrs können auf ihrem Gebiet und, sofern nach Art. 6 Abs. 1 Satz 1 ein regionaler Nahverkehrsraum abgegrenzt worden ist, für diesen Nahverkehrsraum Planungen zur Sicherung und zur Verbesserung des öffentlichen Personennahverkehrs gemäß den Anforderungen dieses Gesetzes durchführen. [2]Für die vorhandenen Verkehrsunternehmen ist dabei eine angemessene Mitwirkung sicherzustellen. [3]Dabei sind insbesondere
1. die im Nahverkehrsraum vorhandenen Verkehrseinrichtungen zu erfassen,
2. das künftig zu erwartende Verkehrsaufkommen im motorisierten Individualverkehr und im öffentlichen Personennahverkehr auf Schiene und Straße zu prognostizieren,

3. Zielvorstellungen über das künftig anzustrebende Verkehrsaufkommen im öffentlichen Personennahverkehr auf Schiene und Straße zu entwickeln und

4. planerische Maßnahmen vorzusehen, die eine bestmögliche Gestaltung des öffentlichen Personennahverkehrs unter Berücksichtigung der Belange des Gesamtverkehrs zulassen.

(2) [1]Der Nahverkehrsplan enthält Ziele und Konzeption des allgemeinen öffentlichen Personennahverkehrs und muß mit den anerkannten Grundsätzen der Nahverkehrsplanung, den Erfordernissen der Raumordnung und Landesplanung, der Städtebauplanung, den Belangen des Umweltschutzes sowie mit den Grundsätzen der Wirtschaftlichkeit und Sparsamkeit übereinstimmen. [2]Soweit erforderlich ist die Planung mit anderen Planungsträgern sowie anderen Aufgabenträgern des ÖPNV abzustimmen. [3]Der Nahverkehrsplan ist in regelmäßigen Zeitabständen zu überprüfen und bei Bedarf fortzuschreiben.

Im Rahmen meiner Beratungstätigkeit war ich mit folgendem Sachverhalt befasst: Für eine Mobilitätsuntersuchung sollte ein vom Landkreis beauftragtes Unternehmen Bürgerinnen und Bürger des Landkreises zu ihrem Mobilitätsverhalten befragen. Zu diesem Zweck sollten die Gemeinden des Landkreises aus den Meldedaten nach einem vorgegebenen Muster Adressdaten ermitteln und diese an das beauftragte Unternehmen übermitteln. Das Unternehmen sollte dann an die Bürgerinnen und Bürger zur freiwilligen Beantwortung einen anonymen Fragenbogen verschicken. Alternativ konnten die Fragen auch in einem Online-Portal beantwortet werden. Insoweit habe ich die nachfolgenden Hinweise gegeben.

Grundsätzlich kann ein für die Verarbeitung personenbezogener Daten Verantwortlicher unter Beachtung der Anforderungen des Art. 28 DSGVO (vgl. ausführlich hierzu meine Orientierungshilfe Auftragsverarbeitung[14]) externe Dienstleister als Auftragsverarbeiter einbinden. Die Einbeziehung privater Planungsbüros in die Planung, Organisation und Sicherstellung des allgemeinen öffentlichen Personennahverkehrs ist im Übrigen in Art. 8 Abs. 1 Satz 3 BayÖPNVG sogar ausdrücklich vorgesehen.

Da der Landkreis die Adressdaten zur Erfüllung seiner oben erläuterten Aufgaben benötigt, dürfen die Gemeinden als Meldebehörden die in § 34 Abs. 1 Bundesmeldegesetz genannten Daten übermitteln. Diese Befugnis erfasst zwar grundsätzlich nur die Übermittlung an eine andere öffentliche Stelle wie hier den Landkreis. Soweit jedoch eine direkte Übermittlung der Daten durch die Meldebehörde an den externen Dienstleister erfolgt, liegt letztlich nur eine unwesentliche Umsetzungsmodalität vor. Bei Vorliegen eines dem Art. 28 DSGVO genügenden Auftragsverarbeitungsverhältnisses zwischen Landkreis und externem Dienstleister ist eine direkte Datenübermittlung an diesen gleichsam als „verlängerten Arm" des Verantwortlichen zulässig.

Sollten die Gemeinden an der Mobilitätsuntersuchung darüber hinaus dergestalt beteiligt sein, dass sie hierbei eigene Interessen bezüglich des örtlichen Verkehrs verfolgen, mithin auch selbst über den Zweck der Verarbeitung bestimmen, würden diese wohl selbst zu Verantwortlichen für die Datenverarbeitung werden. Sie müssten in diesem Fall mit dem Landkreis eine Vereinbarung nach Art. 26 DSGVO

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

als gemeinsam für die Verarbeitung Verantwortliche abschließen. In dieser Vereinbarung könnte dann unter anderem festgelegt werden, dass mit dem externen Dritten nur ein gemeinsamer Auftragsverarbeitungsvertrag begründet wird (vorzugsweise durch den Landkreis im eigenen Namen und zugleich als Vertreter der übrigen gemeinsam Verantwortlichen).

Ergänzend habe ich in diesem Zusammenhang auch auf die Informationspflichten nach Art. 13 DSGVO hingewiesen. Da keine gesetzliche Pflicht besteht, über das Mobilitätsverhalten Auskunft zu geben, sind die angeschriebenen Personen insbesondere darüber zu informieren, zu welchem Zweck die Daten erhoben und wie diese behandelt werden, sowie dass ihre Mitteilung **freiwillig** erfolgt. Insbesondere ist in den Hinweisen darauf einzugehen, wie bei der Online-Umfrage die Anonymisierung sichergestellt wird, und dass auch die Angabe weiterer Daten, wie etwa einer Telefonnummer für Rückrufe, freiwillig ist.

Da die Rückantwort in der Regel anonym erfolgen soll, ist der Fragebogen so auszugestalten, dass keine Rückschlüsse auf die betreffende Person möglich sind. Es dürfen daher keine Angaben gefordert werden, welche (auch in Kombination oder unter Zuhilfenahme anderer verfügbarer Datenbestände) eine Identifizierbarkeit ermöglichen. Zur Absicherung, dass die Fragebögen tatsächlich in der Regel anonym zurückgesandt werden, empfiehlt sich der ausdrückliche Hinweis auf dem Rückantwortkuvert, dass Name und Anschrift nicht anzugeben sind.

5.6 Unzulässigkeit einer flächendeckenden Speicherung von Kopien amtlicher Ausweisdokumente durch Kfz-Zulassungsbehörden bei Erteilung von Ausfuhr- und Kurzzeitkennzeichen

Im Berichtszeitraum wurde ich von einer Zulassungsbehörde mit der Frage befasst, ob es datenschutzrechtlich zulässig ist, auf Bitten der Polizei und mit Einwilligung der Antragstellerinnen und Antragsteller bei der Erteilung von Ausfuhr- und Kurzzeitkennzeichen generell Kopien amtlicher Ausweisdokumente anzufertigen und zu den Zulassungsakten zu nehmen. Die Frage war vor folgendem Hintergrund zu sehen:

Das **Ausfuhrkennzeichen** ist ein amtliches Kraftfahrzeug-Kennzeichen für Kraftfahrzeuge, welche aus Deutschland ausgeführt werden sollen. Näheres dazu regelt § 19 Fahrzeug-Zulassungsverordnung (FZV). Mit dem **Kurzzeitkennzeichen** – umgangssprachlich auch „Überführungskennzeichen" genannt – darf man Fahrzeuge innerhalb Deutschlands bewegen. Es wird nur für fünf Tage von der Zulassungsstelle ausgestellt. Näheres dazu regelt § 16a FZV.

Seitens der Polizei wird derzeit ein Anstieg von Urkundenfälschungen bei der Zuteilung von derartigen Kennzeichen beobachtet. Die Fälschungen betreffen dabei neben Versicherungsnachweisen gerade auch amtliche Ausweisdokumente. Für polizeiliche Ermittlungen wäre es daher wohl eine Erleichterung, wenn die Zulassungsbehörden bei der Ausstellung von Ausfuhr- und Kurzzeitkennzeichen generell Ausweiskopien der Antragstellerinnen und Antragsteller anfertigen und zu den Zulassungsakten nehmen würden. Rechtswidrigen Zulassungen könnte auf diese Weise unter Umständen besser als bisher Einhalt geboten werden.

Aus datenschutzrechtlicher Sicht habe ich dies wie folgt bewertet:

5.6.1 Fehlen einer gesetzlichen Befugnis für die Datenverarbeitung

Die Anfertigung von Kopien amtlicher Ausweise ist eine Verarbeitung personenbezogener Daten, für deren Rechtmäßigkeit eine Rechtsgrundlage notwendig ist (Art. 6 Abs. 1 DSGVO). Öffentliche Stellen stützen sich bei Datenverarbeitungen regelmäßig auf eine gesetzliche Befugnis. Nach Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 UAbs. 1 Buchst. b DSGVO haben die Mitgliedstaaten die Möglichkeit, nationale Rechtsgrundlagen für die Verarbeitung personenbezogener Daten zu schaffen. Da für die erwogene Datenverarbeitung keine (vorrangige) bereichsspezifische Rechtsgrundlage vorhanden ist, kam als Verarbeitungsbefugnis allein Art. 4 Abs. 1 BayDSG in Betracht. Maßgeblich war insbesondere die Frage nach der Erforderlichkeit zur Aufgabenerfüllung.

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

Die für die Aufgabe der Zuteilung von **Ausfuhrkennzeichen** erforderlichen personenbezogenen Daten von Antragstellerinnen und Antragsstellern richten sich nach § 19 Abs. 2 FZV in Verbindung mit § 6 Abs. 1 Satz 2 Nr. 1 und Abs. 4 Nr. 3 FZV.

§ 19 FZV
Fahrten zur dauerhaften Verbringung eines Fahrzeugs in das Ausland
[…]
(2) Bei der Zuteilung eines Ausfuhrkennzeichens sind der Zulassungsbehörde zur Speicherung in den Fahrzeugregistern neben den in § 6 Absatz 1 Satz 2 bezeichneten Halterdaten die in § 6 Absatz 4 Nummer 3 bezeichneten Daten zur Kraftfahrzeug-Haftpflichtversicherung und das Ende des Versicherungsverhältnisses sowie die zur Ausstellung der Zulassungsbescheinigung erforderlichen Fahrzeugdaten und bei Personenkraftwagen die vom Hersteller aufgebrachte Farbe des Fahrzeugs mitzuteilen und auf Verlangen nachzuweisen.
[…]

§ 6 FZV
Antrag auf Zulassung
(1) Die Zulassung eines Fahrzeugs ist bei der nach § 46 örtlich zuständigen Zulassungsbehörde zu beantragen. Im Antrag sind zur Speicherung in den Fahrzeugregistern folgende Halterdaten nach § 33 Absatz 1 Satz 1 Nummer 2 des Straßenverkehrsgesetzes anzugeben und auf Verlangen nachzuweisen:
1. bei natürlichen Personen:
Familienname, Geburtsname, Vornamen, vom Halter für die Zuteilung oder die Ausgabe des Kennzeichens angegebener Ordens- oder Künstlername, Datum und Ort der Geburt, Geschlecht und Anschrift des Halters;
[…]
(4) Im Antrag sind zur Speicherung in den Fahrzeugregistern folgende Fahrzeugdaten anzugeben und auf Verlangen nachzuweisen:
[…]
3. folgende Daten zur Kraftfahrzeug-Haftpflichtversicherung:
a) Name und Anschrift oder Schlüsselnummer des Versicherers,

b) Nummer des Versicherungsscheins oder der Versicherungsbestätigung und
c) Beginn des Versicherungsschutzes oder
d) die Angabe, dass der Halter von der gesetzlichen Versicherungspflicht befreit ist;
[…]

Die für die Zuteilung von **Kurzzeitkennzeichen** erforderlichen personenbezogenen Daten von Antragstellerinnen und Antragstellern richten sich nach § 16a Abs. 2 Satz 2 Nr. 1 bis 3 FZV in Verbindung mit § 6 Abs. 1 Satz 2 Nr. 1 FZV.

§ 16a FZV
Probefahrten und Überführungsfahrten mit Kurzzeitkennzeichen
[…]
(2) Auf Antrag hat die örtlich zuständige Zulassungsbehörde oder die für den Standort des Fahrzeugs zuständige Zulassungsbehörde ein Kurzzeitkennzeichen nach den Absätzen 3 und 4 zuzuteilen und einen auf den Antragsteller ausgestellten Fahrzeugschein für Fahrzeuge mit Kurzzeitkennzeichen nach Absatz 5 auszufertigen. Mit dem Antrag auf Zuteilung eines Kurzzeitkennzeichens hat der Antragsteller
1. die Angaben über den Fahrzeughalter nach § 6 Absatz 1 Satz 2,
2. die Daten zur Kraftfahrzeug-Haftpflichtversicherung nach § 6 Absatz 4 Nummer 3 sowie das Ende des Versicherungsschutzes,
3. die Angaben über einen Empfangsbevollmächtigten nach § 6 Absatz 4 Nummer 3,
[…]
zur Speicherung in den Fahrzeugregistern mitzuteilen und auf Verlangen nachzuweisen.
[…]

Zur Erfüllung der danach bestehenden **Nachweispflicht** hinsichtlich der Identifizierung der Antragstellerinnen und Antragsteller war ein Vermerk – etwa dergestalt: „Personalausweis/Reisepass hat vorgelegen" – völlig ausreichend. Dies fordert bereits der Grundsatz der Datenminimierung (vgl. Art. 5 Abs. 1 Satz 1 Buchst. c DSGVO). Die Anfertigung von Ausweiskopien durch die Zulassungsbehörde war für die Zuteilung von Ausfuhr- und Kurzzeitkennzeichen auch nach dem Vortrag der bei mir anfragenden Zulassungsbehörde gerade **nicht erforderlich**.

Daran ändert es auch nichts, dass die Beamtinnen und Beamten des Polizeidienstes gemäß § 163 Abs. 1 Strafprozessordnung befugt sind, alle Behörden um Auskunft zu ersuchen. Die Vorschrift bezieht sich nur auf Sachverhalte, bei denen im Ermittlungsverfahren auf bei anderen Stellen bereits vorliegende Informationen und Unterlagen zugegriffen werden kann. Hier sollen diese dagegen erst für eventuelle zukünftige Zugriffe quasi auf Verdacht erhoben werden. Daher greift auch Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO nicht und begründet keine Verarbeitungsbefugnis für die Zulassungsbehörde. Daten dürfen nicht auf Vorrat für den Fall erhoben werden, dass sie später einmal (möglicherweise) für die Polizei nützlich sein könnten. Vielmehr ist die Datenerhebung auf konkrete und aktuell zur Bewältigung anstehende eigene Aufgaben zu beschränken.

5.6.2 Einwilligung kein Mittel zur beliebigen Erweiterung des Aufgabenkreises

Soweit der mit einer Datenverarbeitung verbundene Eingriff nicht von gesetzlich festgelegten Befugnissen der Zulassungsbehörde abgedeckt ist, scheidet auch eine „Überbrückung" dieser Limitierung mittels flächendeckend eingeholter Einwilligungen der Antragstellerinnen und Antragsteller (vgl. Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO) aus. Der verfassungsrechtliche Gesetzesvorbehalt verlangt, dass Eingriffe in die Grundrechte der Bürgerinnen und Bürger vom (Parlaments-) Gesetzgeber durch hinreichend bestimmte Vorgaben geregelt werden. Lassen diese Vorgaben den „gewünschten" Eingriff nicht zu, dürfen bayerische öffentliche Stellen nicht flächendeckend versuchen, Einwilligungen zu erlangen, um so „doch noch" eine Rechtsgrundlage für die als zweckmäßig erachtete Verarbeitung zu gewinnen.

An diesem Ergebnis ändert auch die generelle Möglichkeit der Anfertigung von Kopien amtlicher Ausweisdokumente mit Zustimmung der Inhaberin oder des Inhabers gemäß § 20 Abs. 2 Personalausweisgesetz (PAuswG, vergleichbar § 18 Abs. 3 Paßgesetz) nichts.

§ 20 PAuswG
Verwendung durch öffentliche und nichtöffentliche Stellen
[. . .]
(2) Der Ausweis darf nur vom Ausweisinhaber oder von anderen Personen mit Zustimmung des Ausweisinhabers in der Weise abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist. Andere Personen als der Ausweisinhaber dürfen die Kopie nicht an Dritte weitergeben. Werden durch Ablichtung personenbezogene Daten aus dem Personalausweis erhoben oder verarbeitet, so darf die datenerhebende oder -verarbeitende Stelle dies nur mit Einwilligung des Ausweisinhabers tun. Die Vorschriften des allgemeinen Datenschutzrechts über die Erhebung und Verwendung personenbezogener Daten bleiben unberührt.
[. . .]

Dies folgt schon jeweils aus **§ 20 Abs. 2 Satz 4 PAuswG**, wonach die Vorschriften des allgemeinen Datenschutzrechts über die Erhebung und Verwendung personenbezogener Daten unberührt bleiben. Das damit gerade auch von öffentlichen Stelle zu befolgende Gebot der Datenminimierung nach Art. 5 Abs. 1 Satz 1 Buchst. c DSGVO gilt unverändert, selbst wenn die betroffene Person mit der Kopie einverstanden ist. Mit einer Kopie würden außerdem über die zur Identifizierung einer Ausweisinhaberin oder eines Ausweisinhabers hinausgehende und somit nicht erforderliche Daten erhoben (zum Beispiel die Ausweisnummer oder die sog. Zugangsnummer), was dem Grundsatz der Datenminimierung widerspricht und daher unzulässig ist.

5.6.3 Ergebnis

Die **flächendeckende Anfertigung von Kopien amtlicher Ausweisdokumente** bei der Zuteilung von Ausfuhr- und Kurzzeitkennzeichen durch die Zulassungsbehörde auf Bitten der Polizei ist auch bei Vorliegen entsprechender Einwilligungen der betroffenen Personen datenschutzrechtlich **nicht zulässig**. Insbesondere dürfen Antragstellerinnen und Antragsteller nicht unter den abstrakten Generalverdacht einer möglicherweise bevorstehenden Begehung von Straftaten gestellt werden.

6 E-Government und öffentliche Register

6.1 Melderegisterauskünfte für (wissenschaftliche) Studien; insbesondere Adressmittlungsverfahren

6.1.1 Sachverhalt

Im Rahmen meiner Prüftätigkeit habe ich erfahren, dass ein Schaustellerverband durch eine Universität eine Studie zur Attraktivität des in einer Stadt regelmäßig stattfindenden Volksfests durchführen hat lassen. Durch die Online-Studie wollte der Verband ermitteln lassen, welche Bevölkerungsgruppen besonderes Interesse an dem Volksfest haben, welche Teile des Festes besonders geschätzt werden und welche Wünsche für die Zukunft bestehen. Hierzu forderte der Verband von der Stadt eine Gruppenauskunft aus dem Melderegister an. Um die Teilnahmebereitschaft zu fördern, veranstaltete der Verband zudem unter den Studienteilnehmern eine Lotterie.

Vom Einwohnermeldeamt der Stadt wurden aufgrund der Anforderung des Verbands zwei Dateien angefertigt: erstens eine personenbezogene Adressdatei, die die Adressen samt einer zufällig generierten Losnummer (diese war zugleich der [Online-]Zugangscode für die Umfrageteilnehmer) enthielt; zweitens eine anonymisierte Analysedatei, die neben der Losnummer/Zugangscode nur das Geschlecht sowie die Staatsangehörigkeit enthielt. Die Adressdatei wurde dann aber **nicht** dem Verband übermittelt. Auch der Universität wurden **keine** personenbezogenen Adressdaten übermittelt, sondern nur die anonymisierte Analysedatei mit 6.000 Datensätzen. **Stattdessen hat die Stadt**, welche die Studie auch finanziell gefördert hat, aufgrund einer mündlichen Absprache mit dem Verband **als dessen Dienstleister den Postversand übernommen**. Dies umfasste zunächst die Versendung von Anschreiben des Verbands an die von der Gruppenauskunft betroffenen Personen. Ein schriftlicher Vertrag zur Verarbeitung im Auftrag oder ein sonstiger detaillierter Vertrag hinsichtlich der Hintergründe und Abläufe des Vorgehens wurde zwischen dem Verband und der Stadt insoweit jedoch nicht geschlossen.

Nach Durchführung der Studie unter den teilnehmenden Losnummern durch die Universität wurden die Gewinnlosnummern von der Universität der Stadt mitgeteilt. Diese verknüpfte sodann anhand der Zugangscodes die Gewinnlosnummern mit den Namen und Adressen anhand der Adressdatei und teilte diese Daten schließlich dem Verband zur Aushändigung der Gewinne mit. Abgesehen davon erhielt auch der Schaustellerverband keine personenbezogenen Daten. Nach Abschluss der Studie und Lotterie wurden die von der Gruppenauskunft betroffenen Daten von der Stadt gelöscht und die entsprechenden Speichermedien vernichtet.

6.1.2 Datenschutzrechtliche Bewertung

Diesen Vorgang habe ich datenschutzrechtlich wie folgt bewertet:

6.1.2.1 Verarbeitung von Meldedaten

Meldedaten stellen personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO dar. Das Übermitteln von Meldedaten oder die Auskunftserteilung über Meldedaten stellt eine Verarbeitung personenbezogener Daten dar, für deren Rechtmäßigkeit eine Befugnis benötigt wird (Art. 6 Abs. 1 DSGVO). Das Bundesmeldegesetz (BMG) enthält speziell zur Melderegisterauskunft in den §§ 44 ff. BMG entsprechende Befugnisse.

6.1.2.2 Zulässigkeit einer hypothetischen Gruppenauskunft

Die Ziehung von Personenstichproben aus Einwohnermelderegistern stellt rechtlich eine **Gruppenauskunft** dar. Diese ist in § 46 BMG geregelt, der wie folgt lautet:

„(1) Eine Melderegisterauskunft über eine Vielzahl nicht namentlich bezeichneter Personen (Gruppenauskunft) darf nur erteilt werden, wenn sie im öffentlichen Interesse liegt. Für die Zusammensetzung der Personengruppe dürfen die folgenden Daten herangezogen werden:

1. *Geburtsdatum,*
2. *Geschlecht,*
3. *derzeitige Staatsangehörigkeit,*
4. *derzeitige Anschriften,*
5. *Einzugsdatum und Auszugsdatum,*
6. *Familienstand mit der Angabe, ob ledig, verheiratet, geschieden, verwitwet, eine Lebenspartnerschaft führend, Lebenspartnerschaft aufgehoben oder Lebenspartner verstorben.*

(2) Außer der Tatsache der Zugehörigkeit zu der Gruppe dürfen folgende Daten mitgeteilt werden:

1. *Familienname,*
2. *Vornamen,*
3. *Doktorgrad,*
4. *Alter,*
5. *Geschlecht,*
6. *Staatsangehörigkeiten,*
7. *derzeitige Anschriften und*
8. *gesetzliche Vertreter mit Familienname und Vornamen sowie Anschrift.“*

Voraussetzung für die Gruppenauskunft ist danach vor allem, dass ein **öffentliches Interesse** für die Gruppenauskunft vorliegt. Unter öffentlichem Interesse ist das Interesse der Allgemeinheit zu verstehen, das von dem Interesse einzelner Personen oder Gruppen zu unterscheiden ist (Nr. 46 Allgemeine Verwaltungsvorschrift zur Durchführung des Bundesmeldegesetzes – BMGVwV). Rein kommerzielle Interessen stellen kein öffentliches Interesse dar. Dagegen lässt sich wohl ein Forschungsinteresse als öffentliches Interesse ansehen.

Vorliegend wäre es vor diesem rechtlichen Hintergrund wohl gerade noch vertretbar gewesen, ein öffentliches Interesse für die Gruppenauskunft an den Schaustellerverband anzunehmen. Die Gruppenauskunft diente der Durchführung einer Studie zur Ermittlung des Interesses der lokalen Bevölkerung an dem öffentlichen Volksfest in der Stadt. Der dahinterstehende Zweck war die Steigerung der Attraktivität des Volksfests und damit eines Kulturguts. Indem der Verband durch die Ergebnisse der Studie die Attraktivität des Volksfests möglicherweise verbessern kann, profitiert mittelbar auch die Öffentlichkeit und die Stadt. Somit muss nicht

davon ausgegangen werden, dass die Gruppenauskunft allein einem reinen kommerziellen Interesse des Schaustellerverbands als Veranstalter des Festes oder seiner Verbandsmitglieder diente. Noch deutlicher würde dies allerdings zu Tage treten, wenn die Stadt die Ergebnisse der Studie erfährt oder – vorzugswürdiger – diese selbst in Auftrag gegeben hätte. Dies habe ich bei zukünftigen vergleichbaren Fällen zu berücksichtigen gebeten.

Allerdings wurde hier entgegen der ursprünglichen Intention des Verbands und des vom Gesetzgeber vorgesehenen Weges keine Gruppenauskunft von der Meldebehörde der Stadt an den Schaustellerverband erteilt. Vielmehr hat das Einwohneramt der Stadt die von der Gruppenauskunft betroffenen Meldedaten einer anderen Stelle der Stadt zur dortigen weiteren Verarbeitung weitergegeben. Die Stadt hat somit faktisch über die Mittel und Zwecke der weiteren Verarbeitung dieser personenbezogenen Meldedaten entschieden und war somit weiterhin und auch insoweit Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO.

6.1.2.3 Keine Verarbeitung im Auftrag

Theoretisch wäre es zwar auch denkbar, den hier in Rede stehenden Vorgang zwischen der Stadt und dem Schaustellerverband als eine Art Auftragsverarbeitung im Sinne von Art. 4 Nr. 8, Art. 28 DSGVO anzusehen. Unabhängig davon, ob dieses Begeben einer öffentlichen Stelle in die Rolle eines Dienstleisters für einen privaten Verband mit den öffentlichen Aufgaben einer Kommune in Einklang steht – dies stellt keine Frage des Datenschutzes dar –, hätte dann aber auch ein Vertrag zur Auftragsverarbeitung mit dem Inhalt des Art. 28 Abs. 3 DSGVO geschlossen werden müssen, was hier nicht erfolgt war. Im Übrigen bestehen aber auch tiefgreifende Bedenken gegen eine solche Auftragsverhältniskonstruktion, da sie die datenschutzrechtlichen Verantwortlichkeiten zwischen einer öffentlichen Stelle als „Herrin" über die Daten, die sich auf ihre öffentlich-rechtlichen Befugnisse zur Datenverarbeitung stützen kann (Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2, Abs. 3 DSGVO) und nichtöffentlichen Stellen, mit den für diese in Betracht kommenden eigenen Datenverarbeitungsbefugnissen (vgl. Art. 6 Abs. 1 UAbs. 1 Buchst. f, UAbs. 2 DSGVO) verwischt oder gleichsam umkehrt.

6.1.2.4 Erfordernis einer eigenen Rechtsgrundlage für die Stadt

Somit war die Stadt hier als Verantwortliche für die folgende Datenverarbeitungsvorgänge anzusehen: Weiterleitung der Meldedaten vom Meldeamt an die andere Stelle der Stadt, Verarbeitung der Meldedaten zu zwei Dateien (Versanddatei, Analysedatei), Verwendung der Adressdaten zur Versendung der Anschreiben des Schaustellerverbands, Zusammenfügung der von der Universität an die Stadt übermittelten Gewinnlosnummern mit den entsprechenden Meldedaten und Übermittlung der Gewinnerdaten an den Schaustellerverband.

Für diese Datenverarbeitungsvorgänge benötigte die Stadt jeweils eine eigene Befugnis (Art. 6 Abs. 1 DSGVO). Eine solche Befugnis war hier im Wesentlichen – allenfalls die Übermittlung der Gewinnerdaten an den Schaustellerverband kann auf Art. 5 Abs. 1 Nr. 2 BayDSG gestützt werden – **nicht** erkennbar.

Insbesondere schien mir Art. 4 Abs. 1 BayDSG **nicht** vorzuliegen. Danach ist die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle unbeschadet sonstiger Bestimmungen zulässig, wenn sie zur **Erfüllung einer ihr obliegenden Aufgabe erforderlich** ist. Da die Stadt selbst nicht Veranstalter des in Rede stehenden Volksfests war, nicht die Studie veranlasst hat und wohl auch nicht die

Studienergebnisse erhalten hat, sondern vielmehr nur der Schaustellerverband, diente die Datenverarbeitung nicht der Erfüllung einer eigenen öffentlichen Aufgabe der Stadt. In der Sache wurde damit **nur die Erfüllung der Studie des Schaustellerverbands ermöglicht**. Die **mittelbaren Vorteile für die Stadt,** wenn der Schaustellerverband durch die Ergebnisse der Studie gegebenenfalls die Attraktivität des Volksfests in der Stadt steigern kann, mögen im Rahmen des § 46 BMG für ein öffentliches Interesse gerade noch **genügen, nicht jedoch für die Bejahung einer eigenen Aufgabe der Stadt**.

Auch eine Verarbeitung zur Wahrung berechtigter Interessen eines Dritten (hier des Schaustellerverbands) nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO kam nicht in Betracht, da diese Befugnis nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommenen Verarbeitungen gilt (Art. 6 Abs. 1 UAbs. 2 DSGVO).

6.1.2.5 Adressmittlungsverfahren rechtfertigte keine andere Bewertung

Anderes ergibt sich auch nicht unter dem Aspekt des sog. **Adressmittlungsverfahrens**. Bei einem 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. Dieses Adressmittlungsverfahren wurde in der Vergangenheit von den Aufsichtsbehörden als datenschutzfreundliches Verfahren angesehen, mit dem insbesondere Forschungsvorhaben ermöglicht werden sollten (vgl. hierzu mein 23. Tätigkeitsbericht 2008 unter Nr. 17.1.1. und Nr. 14.3.). Allerdings stellt auch die Verarbeitung von Adressen (insbesondere Versendung von [Teilnahmeeinladungs-]Briefen) durch die versendende öffentliche Stelle (konkret: die Meldebehörde oder eine andere städtische Stelle) eine Datenverarbeitung dar, für die diese eine Befugnis benötigt (vgl. Art. 6 Abs. 1 DSGVO). Dies gilt gerade im Bereich des Melderechts, welches eine Art „Zwangsregister" darstellt. Die letztlich ordnungsrechtlichen Maßgaben des Gesetzgebers zum Umgang mit diesem Datenbestand sind hier besonders strikt einzuhalten. Eine eigene Befugnis für die Stadt ist hier jedoch für die in Rede stehenden Verarbeitungsvorgänge, wie eben erwähnt, nicht erkennbar.

Denkbar wäre nach meiner derzeitigen Einschätzung daher allenfalls, das Adressmittlungsverfahren im Bereich von Meldedaten auf Basis eines detaillierten, die Hintergründe und Abläufe regelnden (Dienstleistungs-)Vertrags – gegebenenfalls im Rahmen einer Wirtschaftsförderung – zwischen der die Befragung durchführenden Stelle oder Person und derjenigen öffentlichen Stelle, die die Adressen der Befragungsempfängerinnen und Befragungsempfänger kennt und die Briefe dann versenden soll, abzuwickeln – freilich vorausgesetzt, dass dies nach den maßgeblichen öffentlich-rechtlichen Vorschriften, insbesondere den kommunalrechtlichen Vorgaben, zulässig sein sollte. Rechtsgrundlage für die im Rahmen des Adressmittlungsverfahrens anfallenden Datenverarbeitungen wäre dann wohl Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO.

Aber auch in diesem Fall ist zusätzlich zu fordern, dass eine (fiktive) Datenübermittlung der Meldedaten an den die Befragung Durchführenden rechtmäßig wäre, da öffentliche Stellen nicht durch den Abschluss von Verträgen beliebig ihre Befugnisse erweitern können, sondern sich grundsätzlich in dem Rahmen bewegen müssen, den ihnen der Gesetzgeber zuweist.

Hier schied diese Möglichkeit schon deswegen aus, da kein Dienstleistungsvertrag geschlossen war.

6.1.2.6 Fazit

Ich habe daher gegenüber der Stadt einen Datenschutzverstoß festgestellt. Von einer förmlichen Beanstandung habe ich vor allem auch deshalb abgesehen, da die Stadt den hier gewählten und kritisierten Weg wohl in guter datenschutzrechtlicher Absicht, nämlich im Sinne der Datensparsamkeit und um zu vermeiden, dass der Schaustellerverband die Melderegisterdaten erhält, gegangen ist.

Die generelle Eignung einer Fortführung des Adressmittlungsverfahrens unter Geltung der Datenschutz-Grundverordnung werde ich auch in Zukunft weiterhin aufmerksam beobachten.

6.2 Geplante Änderung des Rundfunkbeitragsstaatsvertrages; Einführung eines regelmäßigen Meldedatenabgleichs

Regelmäßig beschäftige ich mich mit Anfragen von Bürgerinnen und Bürgern, die sich gegen eine Übermittlung von Meldedaten an die öffentlich-rechtlichen Rundfunkanstalten und die dann dort vorgenommenen Datenverarbeitungen wenden. Anlass dafür war bisher häufig der im Jahr 2018 durchgeführte „einmalige" Meldedatenabgleich. Hierzu habe ich mich bereits in meinem 28. Tätigkeitsbericht 2018 unter Nr. 14.3 geäußert.

Im Berichtszeitraum hat sich die Situation dahin entwickelt, dass gemäß einem Entwurf eines 23. Rundfunkänderungsstaatsvertrages die Vorschriften des Rundfunkbeitragsstaatsvertrages geändert werden sollen. Die bisher als „einmaliger" Abgleich vorgesehene Datenübertragung soll danach zukünftig regelmäßig in einem Abgleichrhythmus von vier Jahren etabliert werden. Der Entwurf sieht vor, dass nun alle vier Jahre stichtagsgenau folgende Daten aller volljährigen Personen von der Meldebehörde an die jeweils zuständige Landesrundfunkanstalt übermittelt werden: der Familienname, Vornamen, frühere Namen, Doktorgrad, Familienstand, Geburtsdatum, gegenwärtige und letzte Anschrift von Haupt- und Nebenwohnungen einschließlich aller vorhandenen Angaben zur Lage der Wohnung und der Tag des Einzugs in die Wohnung.

Die beabsichtigte Neuregelung hat Bürgerinnen und Bürger veranlasst, sich mit Datenschutzbedenken an mich zu wenden.

Bereits im Frühstadium der geplanten Änderung habe ich in Übereinstimmung mit den unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder auf die datenschutzrechtlichen Bedenken im Zusammenhang mit der Einführung eines regelmäßigen Datenabgleichs hingewiesen, zumal ich bereits die Einführung eines „einmaligen" Datenabgleichs kritisch gesehen hatte. Auf der Grundlage des zu diesem Zeitpunkt zur Verfügung stehenden Referentenentwurfs fasste die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) unter meiner Beteiligung bereits im April 2019 folgenden Beschluss:

Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 26. April 2019

Geplante Einführung eines regelmäßigen vollständigen Meldedatenabgleichs zum Zweck des Einzugs des Rundfunkbeitrags stoppen

Zukünftig sollen nach einem Referentenentwurf zur Änderung des Rundfunkbeitragsstaatsvertrags (RBStV) regelmäßig alle vier Jahre Meldedaten sämtlicher volljähriger Personen an die jeweils zuständige Landesrundfunkanstalt zur Sicherstellung der Aktualität des dortigen Datenbestandes übermittelt werden. Gemäß Art. 1 Ziffer 7 dieses Entwurfs des 23. Rundfunkänderungsstaatsvertrages vom 5. Februar 2019 zählen zu den Meldedaten neben Namen und gegenwärtiger und letzter Anschrift insbesondere auch Geburtstag, Titel, Familienstand sowie die genaue Lage der Wohnung.

Bereits der im Jahr 2013 durchgeführte vollständige Meldedatenabgleich war seinerzeit auf erhebliche datenschutzrechtliche Bedenken gestoßen (vgl. Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 11. Oktober 2010). Die DSK stellte ihre Bedenken nur deshalb teilweise zurück, weil lediglich ein einmaliger Meldedatenabgleich vorgenommen werden sollte, um den Start in das neue Beitragsmodell zu erleichtern. Mit der nun vorgesehenen Regelung wären die - bereits damals zweifelhaften - Zusicherungen des Gesetzgebers, dass es sich bei den anlasslosen vollständigen Meldedatenabgleichen aus den Jahren 2013 und 2018 um einmalige Vorgänge handeln würde, endgültig hinfällig.

Gegen die geplante Einführung eines regelmäßigen vollständigen Meldedatenabgleichs bestehen weiterhin grundlegende verfassungsrechtliche und datenschutzrechtliche Bedenken.

Ein solcher Abgleich stellt einen unverhältnismäßigen Eingriff in die informationelle Selbstbestimmung dar und gerät in Konflikt mit den Grundsätzen der Datenminimierung und der Erforderlichkeit gemäß Art. 5 Abs. 1 lit. a und c, Art. 6 Abs. 1 der Datenschutz-Grundverordnung (DSGVO).

Bei einem vollständigen Meldedatenabgleich werden in großem Umfang personenbezogene Daten von Betroffenen, die überhaupt nicht beitragspflichtig sind, weil sie entweder in einer Wohnung leben, für die bereits durch andere Personen Beiträge gezahlt werden oder weil sie von der Beitragspflicht befreit sind, an die Rundfunkanstalten übermittelt und von diesen verarbeitet. Zudem werden auch Daten von all denjenigen Einwohnerinnen und Einwohnern erhoben und verarbeitet, die sich bereits bei der Landesrundfunkanstalt angemeldet haben und regelmäßig ihre Beiträge zahlen. Dabei betrifft der geplante Meldedatenabgleich mehr personenbezogene Daten, als die Beitragszahlerinnen und -zahler bei der Anmeldung mitteilen müssen, z. B. Doktorgrad und Familienstand (vgl. § 8 Abs. 4 RBStV). Es sollen also personenbezogene Daten an die Rundfunkanstalten übermittelt werden, die nicht zur Beitragserhebung notwendig sind.

Die Meldedaten-Übermittlungsverordnungen der Länder bieten mit der anlassbezogenen Meldedatenübermittlung an die Rundfunkanstalten bereits eine angemessene und ausreichende Möglichkeit, die Aktualität des Datenbestandes des Beitragsservices auch bei Veränderungen der Meldesituation der Beitragsschuldnerinnen und Beitragsschuldner zu gewährleisten. Auch wenn die Meldebehörden in Einzelfällen eine Änderungsmitteilung unterlassen sollten, würde ein erneuter vollständiger Meldedatenabgleich in unverhältnismäßiger Weise in das Recht auf informationelle Selbstbestimmung der Beitragsschuldner eingreifen, ohne dass

dies durch andere Gesichtspunkte, etwa das Ziel der Gebührengerechtigkeit, gerechtfertigt wäre.

Die Landesrundfunkanstalten gehen selbst davon aus, dass ein vollständiger Meldedatenabgleich letztlich in weniger als einem Prozent der Fälle zu einer zusätzlichen, dauerhaften Anmeldung von Beitragspflichtigen führt (vgl. Evaluierungsbericht der Länder gem. § 14 Abs. 9a RBStV vom 20. März 2019).

Die geplanten Regelungen berücksichtigen zudem die Maßstäbe der DS-GVO nicht ausreichend. Nationale Datenschutzvorschriften müssen aufgrund des Anwendungsvorrangs europäischer Verordnungen auf eine Öffnungsklausel der DS-GVO gestützt werden können. Art. 85 Abs. 2 DS-GVO ist nicht einschlägig, da die Datenverarbeitung zum Zweck des Einzugs des Rundfunkbeitrags nicht in dem Anwendungsbereich dieser Norm liegt. Bei Regelungen, die auf die Öffnungsklausel nach Art. 6 Abs. 2 und Abs. 3 i. V. m. Art. 6 Abs. 1 lit. e) DS-GVO gestützt werden, sind die Grundsätze der Datenminimierung und Erforderlichkeit zu beachten. Mitgliedstaatliche Regelungen für die Erfüllung von Aufgaben, die im öffentlichen Interesse liegen, dürfen danach eingeführt werden, wenn diese die DS-GVO zwar präzisieren, nicht aber deren Grenzen überschreiten. Regelungen, die sich auf diese Öffnungsklausel beziehen, müssen sich folglich in dem Rahmen halten, den die DS-GVO vorgibt. Hier bestehen erhebliche Bedenken im Hinblick auf die Grundsätze der Datenminimierung und der Erforderlichkeit.

Positiv hervorzuheben ist zwar, dass die bisherige Vermieterauskunft im Hinblick auf Mietwohnungen aus § 9 Abs. 1 Satz 2 und 3 RBStV gestrichen werden soll. Ebenso soll der Ankauf von Adressdaten von Privatpersonen ausdrücklich ausgeschlossen werden. Beide Datenverarbeitungen sind aus Sicht des Datenschutzes kritisch zu sehen und ihre Streichung ist zu begrüßen. Dabei darf jedoch nicht übersehen werden, dass mit dem geplanten regelmäßigen vollständigen Meldedatenabgleich eine weitaus umfassendere, datenschutzrechtlich ebenfalls sehr

bedenkliche Möglichkeit der Datenerhebung geschaffen werden soll, die das praktische Bedürfnis der Vermieterauskunft und des Ankaufs privater Adressen ohnehin entfallen lässt.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder fordert, den geplanten regelmäßigen vollständigen Meldedatenabgleich nicht einzuführen, da gegen die vorgesehenen Regelungen grundlegende verfassungsrechtliche Bedenken bestehen und diese die Maßstäbe der DS-GVO nicht ausreichend berücksichtigen.

Diesen Beschluss habe ich zum Anlass genommen, sowohl die Bayerische Staatskanzlei als auch das Bayerische Staatsministerium des Innern, für Sport und Integration auf die Auffassung der Datenschutzkonferenz hinzuweisen.

Zwar sieht ein später im Ministerrat behandelter, ergänzter Entwurf nunmehr vor, dass „zur Wahrung der Verhältnismäßigkeit zwischen Beitragsgerechtigkeit und dem Schutz persönlicher Daten […] der Meldedatenabgleich nach Satz 1 nicht [erfolgt], wenn die Kommission zur Ermittlung des Finanzbedarfs der Rundfunkanstalten (KEF) in ihrem Bericht nach § 3 Abs. 8 des Rundfunkfinanzierungsstaatsvertrages feststellt, dass der Datenbestand hinreichend aktuell ist." Dies kann jedoch die datenschutzrechtlichen Bedenken bezüglich der Einführung eines regelmäßigen Meldedatenabgleichs nicht entkräften. Das habe ich auch anlässlich der Ressortanhörung klargestellt.

Ich bin daher weiterhin der Auffassung, dass die geplante Änderung des Rundfunkbeitragsstaatsvertrages im Hinblick auf die Einführung eines regelmäßigen Meldedatenabgleichs aus datenschutzrechtlichen Gründen unterbleiben sollte.

Die Bayerische Staatsregierung hat am 11. November 2019 um Zustimmung des Bayerischen Landtags zum 23. Rundfunkänderungsstaatsvertrag gebeten. Die dortige Behandlung bleibt abzuwarten.

6.3 IT-Outsourcing durch Kommunen: Anforderungskatalog

IT-Outsourcing meint eine **Auslagerung von Aufgaben und Verantwortung** aus der eigenen IT-Abteilung an einen externen Dienstleister gegen Entgelt. Die Gründe hierfür sind vielfältig: Neben einem Mangel an qualifizierten Fachkräften bei gleichzeitig steigender Komplexität der IT-Verfahren spielen auch wirtschaftliche Erwägungen eine Rolle, so etwa eine bessere Planbarkeit der Kosten des externen Dienstleisters, die Verringerung von Wartungs- und Unterhaltskosten und nicht zuletzt die Vermeidung eigener Investitionen. Vielfach wird auch erhofft, ein spezialisierter externer Dienstleister könne flexibler auf veränderte Anforderungen reagieren, wodurch es der auslagernden Stelle möglich sei, sich mehr auf ihre Kernkompetenzen zu konzentrieren.

Diese oder ähnliche Überlegungen stellen offenbar auch immer mehr Kommunen an, so dass ich von verschiedener Seite mit der Thematik konfrontiert wurde. Die **Spannbreite** des IT-Outsourcings im kommunalen Bereich **variiert dabei erheblich**. Neben vergleichsweise unproblematischen Anfragen zu Erstellung und Betrieb von kommunalen Homepages durch externe Anbieter sowie der Videoüberwachung kommunaler Einrichtungen durch Externe habe ich auch von Fällen einer vollständigen Auslagerung der kommunalen Informationstechnologie erfahren.

Die **Entwicklung** in Richtung einer immer umfassenderen Auslagerung ist **in datenschutzrechtlicher Hinsicht bedenklich**. Darauf weist exemplarisch ein pressewirksamer Fall hin, in welchem von einem Landratsamt geleaste Festplatten nach Rückgabe an den Leasinggeber dort unter Missachtung technischer Standards entsorgt und dabei personenbezogene Daten von Bürgerinnen und Bürgern offenbart wurden. Um der eigenen Verantwortung gerecht zu werden, muss eine Kommune nicht nur Dienstleister sorgfältig und streng auswählen, vielmehr muss sie auch im Fall einer Auslagerung Fachwissen vorhalten und bereit sein, sich mit IT-Vorgängen auseinanderzusetzen.

Auch wenn ich aus datenschutzrechtlicher Sicht den **Zusammenschluss mehrerer Kommunen zum Zweck des gemeinsamen Betriebs der Informationstechnologie gegenüber einem IT-Outsourcing für vorzugswürdig** halte, erkenne ich doch, dass sich viele Kommunen aufgrund der voranschreitenden Digitalisierung mit dem Thema beschäftigen. Daher habe ich einen **Abstimmungsprozess** zu Grenzen und Voraussetzungen des IT-Outsourcings im kommunalen Bereich **angestoßen**. Hieran nehmen im Rahmen einer Arbeitsgruppe neben mir auch das Bayerische Staatsministerium des Innern, für Sport und Integration, der Bayerische Kommunale Prüfungsverband, das Bayerische Landesamt für Sicherheit in der Informationstechnik, der Bayerische Städtetag und der Bayerische Gemeindetag teil. Ziel ist es, einen **abgestimmten Anforderungskatalog** zu erarbeiten, der den Kommunen bei der Entscheidung hilft, ob und inwieweit ein IT-

Outsourcing im Einzelfall zulässig ist. Dieser Anforderungskatalog, welcher fachgesetzliche, datenschutz- und haushaltsrechtliche sowie technisch-organisatorische Kriterien enthalten soll, wird derzeit von der Arbeitsgruppe abgestimmt. Aus Datenschutzsicht haben die folgenden Kriterien besondere Bedeutung:

— sorgfältige Auswahl des Auftragsverarbeiters,
— Wahrung des Datengeheimnisses,
— Sicherstellung des Zugriffs auf die Daten,
— tatsächliche Überprüfungen,
— Erteilung fachkundiger Weisungen,
— Sicherstellung von Prüfungsrechten,
— Regelung einer Rückgabe der Daten.

Aus diesem Grund wird der aktuell in Abstimmung befindliche Katalog im Bereich der technisch-organisatorischen Kriterien sowohl strenge, von externen Dienstleistern einzuhaltende Anforderungen zu den IT-Sicherheitszielen Vertraulichkeit, Verfügbarkeit und Integrität enthalten als auch Kriterien für die Einhaltung der Rechenschaftspflichten nach Art. 5 Abs. 2 DSGVO definieren und IT-Kompetenzen festlegen, die zwingend in der Kommune verbleiben müssen. Denn auch wenn sich eine Kommune dazu entscheidet, Teile ihrer IT auszulagern, muss sie dennoch dafür sorgen, dass sie die Kontrolle über die Tätigkeit des Externen nicht verliert. Die Kommune bleibt für die Verarbeitung der Daten Verantwortlicher im datenschutzrechtlichen Sinne. Sie muss in der Lage sein, Weisungen zu erteilen und aus Überprüfungen die richtigen Schlüsse zu ziehen. Folgende besonders wichtige Themenbereiche zur Erfüllung der Anforderungen bezüglich Vertraulichkeit, Verfügbarkeit, Integrität und Rechenschaftspflichten möchte ich im Anforderungskatalog mindestens konkretisieren:

— notwendiger physischer Schutz,
— Wiederherstellbarkeit und Ausfallsicherheit,
— Trennung von Dienstleistungen für öffentliche und nicht-öffentliche Kunden sowie strikte Mandantentrennung innerhalb der öffentlichen Kunden,
— Verschlüsselung der Kommunikation mit sowie der Daten beim Dienstleister,
— Vertraulichkeit bei Backup und Archivierung,
— Berechtigungskonzept und Protokollierung,
— Fremd- und Fernwartung,
— Positivliste Zertifizierungen,
— Umgang mit IT-Sicherheitsvorfällen,
— Kontrollen/Audits durch die Kommune,
— Nachweis des Dienstleisters zur Einhaltung der IT-Sicherheit.

Speziell in datenschutzrechtlicher Hinsicht weise ich darauf hin, dass ein IT-Outsourcing regelmäßig nur dann zulässig sein wird, wenn es sich als Auftragsverarbeitung nach Art. 28 DSGVO[15] darstellt. Grund hierfür ist folgende rechtliche Privilegierung: Liegt eine rechtmäßige Auftragsverarbeitung vor, ist für die Weitergabe personenbezogener Daten an den Auftraggeber und die Verarbeitung durch diesen regelmäßig keine eigene Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO notwendig, da der Auftragsverarbeiter als „verlängerter Arm“ des Verantwortlichen

[15] Siehe allgemein zur Auftragsverarbeitung Bayerischer Landesbeauftragter für den Datenschutz, Auftragsverarbeitung, Stand 4/2019, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Auftragsverarbeitung“.

handelt. Die von der Datenschutz-Grundverordnung bereitgestellte Auftragsverarbeitung ist jedoch nur ein Modell. Auf die Frage, ob von diesem Modell auch tatsächlich im kommunalen Bereich vollumfänglich Gebrauch gemacht werden darf, gibt die Datenschutz-Grundverordnung jedoch in Art. 28 DSGVO keine Antwort. Diese ist in der DSGVO an anderer Stelle, so wie im nationalen Recht zu suchen (dazu näher sogleich).

Die Kommunen verarbeiten aufgrund ihrer breit gefächerten Zuständigkeiten Daten aus den verschiedensten fachlichen Bereichen– teilweise besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO oder Daten, die speziellen fachgesetzlichen Regelungen unterliegen, wie beispielsweise solche aus den Bereichen Meldewesen, Steuern, Personal, Gesundheits- oder Sozialwesen. Sofern daher bereichsspezifische Anforderungen bestehen, müssen diese auch im Rahmen der Auftragsverarbeitung beachtet werden. Zur Beurteilung, ob und inwieweit ein IT-Outsourcing in datenschutzrechtlicher Hinsicht zulässig ist, sind daher zum einen die Wertungen des nationalen Fachrechts heranzuziehen. Daneben sind die in Art. 24, 25 und 32 DSGVO enthaltenen Pflichten des Verantwortlichen, geeignete technisch-organisatorische Maßnahmen umzusetzen, zu beachten, um eine datenschutzkonforme Verarbeitung zu gewährleisten. Vor allem ist aber auch die Wertung des Art. 33 Abs. 4 Grundgesetz gebührend zu berücksichtigen, wonach die Ausübung hoheitsrechtlicher Befugnisse als ständige Aufgabe in der Regel Angehörigen des öffentlichen Dienstes zu übertragen ist, die in einem öffentlich-rechtlichen Dienst- und Treueverhältnis stehen. Vor diesem rechtlichen Hintergrund stehe ich daher derzeit einer **vollständigen Auslagerung der kommunalen Informationstechnologie an externe Dienstleister generell kritisch** gegenüber.

7 Gesundheitsverwaltung und Krankenhäuser

7.1 Verarbeitung von Mitteilungen der Polizei durch das Gesundheitsamt

Wiederholt haben mich Mitteilungen von Gesundheitsämtern erreicht, wonach sie von Polizeibehörden Ereignismeldungen über Verhaltensauffälligkeiten, Verdachte auf psychische Erkrankungen, Suchtverhalten oder Ähnliches erhalten würden. Die Gesundheitsämter halten diese Praxis zu Recht für nicht mit dem Datenschutzrecht vereinbar.

Entsprechende Datenübermittlungen an die jeweils zuständigen Kreisverwaltungsbehörden sind gemäß Art. 56 Abs. 1 Nr. 2 Polizeiaufgabengesetz (PAG) in Verbindung mit Art. 11 Bayerisches Psychisch-Kranken-Hilfe-Gesetz (BayPsychKHG) für Zwecke der sofortigen vorläufigen Unterbringung zulässig:

Art. 11 BayPsychKHG
Sofortige vorläufige Unterbringung durch die Kreisverwaltungsbehörde
[1]Sind dringende Gründe für die Annahme vorhanden, dass die Voraussetzungen für eine Unterbringung nach Art. 5 vorliegen, und kann eine gerichtliche Entscheidung nicht rechtzeitig ergehen, kann die Kreisverwaltungsbehörde die sofortige vorläufige Unterbringung anordnen und vollziehen.[2][…]

Allerdings ergibt sich aus dem Umstand, dass das Gesundheitsamt Teil des Landratsamts als Kreisverwaltungsbehörde ist, nicht automatisch, dass diese Daten auch an das Gesundheitsamt übermittelt werden dürfen, obwohl dieses die Daten für eigene Aufgaben zunächst nicht benötigt. Das Gesundheitsamt erhält regelmäßig erst vor einer vorläufigen gerichtlichen Unterbringung Gelegenheit zur Äußerung und benötigt auch nur dann, wenn es dazu kommt, personenbezogene Daten:

Art. 16 BayPsychKHG
Vorläufige gerichtliche Unterbringung
(1) [1]Die vorläufige gerichtliche Unterbringung wird auf Antrag der Kreisverwaltungsbehörde angeordnet.[2]Vor einer vorläufigen gerichtlichen Unterbringung gibt das Gericht dem Gesundheitsamt, in dessen Bezirk die betroffene Person ihren gewöhnlichen Aufenthalt hat, Gelegenheit zur Äußerung.[3][…]

Diese Rechtslage rechtfertigt es aber nicht, bereits zuvor das Gesundheitsamt durch die Polizeibehörden miteinzubeziehen. Der Zugang zu personenbezogenen Daten muss vielmehr auf diejenigen Stellen begrenzt werden, welche sie für die konkreten Zwecke im Einzelfall auch tatsächlich benötigen:

Art. 5 DSGVO
Grundsätze für die Verarbeitung personenbezogener Daten
(1) Personenbezogene Daten müssen
[…]
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung");

[…]

In diesem Zusammenhang haben die Gesundheitsämter auch die Frage aufgeworfen, wie sie mit derartigen unzulässigen Meldungen der Polizeibehörden umgehen sollen, das heißt, ob sie diese insbesondere in dringenden Fällen an die zuständigen Stellen im Landratsamt weiterleiten dürfen oder die Datenübermittlung an die zuständige Stelle auf dem „Umweg" über die Polizeibehörden erfolgen müsse.

Ich habe den Gesundheitsämtern den Ratschlag gegeben, die beim Gesundheitsamt unzuständigerweise eingegangenen Meldungen an die zuständige Abteilung der Kreisverwaltungsbehörde weiterzuleiten. Das Gesundheitsamt sollte die zuständige Polizeibehörde auf den Fehler sowie auf die Weiterleitung der übermittelten Daten hinweisen.

Darüber hinaus hat ein Gesundheitsamt die Frage aufgeworfen, ob es auf Grundlage der fälschlich an das Gesundheitsamt übermittelten Daten eine betroffene Person fragen dürfe, ob sie eine in die Verantwortung des Gesundheitsamtes fallende Beratung möchte. Dazu wäre es erforderlich, die Daten auch übergangsweise beim Gesundheitsamt zu speichern.

Wann eine Verarbeitung im Sinne der Datenschutz-Grundverordnung vorliegt, welche stets einer Rechtsgrundlage bedarf, ist in Art. 4 Nr. 2 DSGVO geregelt:

Art. 4 DSGVO
Begriffsbestimmungen
Im Sinne dieser Verordnung bezeichnet der Ausdruck:
[…]
2. „Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;
[…]

Wann eine Verarbeitung personenbezogener Daten zulässig ist, ist in Art. 6 DSGVO geregelt, wobei Art. 9 DSGVO für besondere Kategorien personenbezogener Daten zusätzliche Anforderungen enthält. Da gerade keine gesetzliche Grundlage für die vom Gesundheitsamt gewünschte Datenverarbeitung existiert, kommt nur eine Datenverarbeitung gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 9 Abs. 2 Buchst. a DSGVO auf Grundlage einer Einwilligung in Betracht.

Ob eine Einwilligung auch, wie vom Gesundheitsamt erfragt, nachträglich eingeholt werden kann, lässt sich aus den Regelungen in der Datenschutz-Grundverordnung (insbesondere Art. 4 Nr. 11, Art. 7 DSGVO sowie Erwägungsgründen 32, 33, 42 und 43 DSGVO) nicht unmittelbar entnehmen. Allerdings stellt beispielsweise Erwägungsgrund 33 Satz 1 DSGVO (ausdrücklich nur für den Bereich der wissenschaftlichen Forschung) auf den „Zeitpunkt der Erhebung der personenbezogenen Daten" ab. Dieser Zeitpunkt muss für sonstige Verarbeitungen gleichermaßen gelten. Es ist demnach nicht zulässig, Daten mit dem Vorsatz, nachträglich eine Einwilligung in die Verarbeitung personenbezogener Daten einzuholen, zu

verarbeiten. Dies ist schon deshalb nicht möglich, weil dabei bewusst in Kauf genommen werden müsste, dass zumindest ein gewisser Anteil an Verarbeitungen rechtswidrig erfolgen würde, weil sich der Betroffene (nachträglich) gegen eine Einwilligung entscheidet.

Eine rechtsgrundlose Verarbeitung personenbezogener Daten für Zwecke des Gesundheitsamtes ist zwar noch nicht anzunehmen, wenn Daten von Polizeibehörden (unzulässigerweise, aber dafür trägt das Gesundheitsamt nicht die Verantwortung) an das Gesundheitsamt übermittelt werden. Auch die Weiterleitung dieser Daten an den eigentlichen Adressaten der Datenübermittlung stellt mangels eigener Entscheidung des Gesundheitsamtes über Mittel und Zwecke der Datenverarbeitung keinen rechtfertigungsbedürftigen Vorgang dar. Sobald diese Daten aber durch das Gesundheitsamt gespeichert oder dazu verwendet werden, um die betroffene Person zu kontaktieren, liegt eine Verarbeitung unter eigener Verantwortung vor, welche nur unter den Bedingungen der Art. 6, 9 DSGVO zulässig wäre.

7.2 Krankenhausseelsorge

Viele Krankenhäuser sind verunsichert, wie sie mit Daten von Patientinnen und Patienten umgehen sollen, wenn diese Daten für die Behandlung nicht erforderlich sind, sie aber erhoben werden müssen, um den Zugang von Seelsorgerinnen und Seelsorgern zu den Patientinnen und Patienten zu ermöglichen.

Eine Verarbeitung der besonders sensiblen Daten zu religiösen oder weltanschaulichen Überzeugungen einschließlich der Datenübermittlung durch das Krankenhaus ist nur nach Maßgabe von Art. 9 DSGVO und damit regelmäßig ausschließlich auf ausdrücklichen Wunsch der Patientin oder des Patienten hin zulässig. Art. 9 DSGVO lautet auszugsweise:

Art. 9 DSGVO
Verarbeitung besonderer Kategorien personenbezogener Daten
(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.
(2) Absatz 1 gilt nicht in folgenden Fällen:
a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,
[…]

Seit Geltungsbeginn der Datenschutz-Grundverordnung genügt dabei eine schlüssige oder auch nur mutmaßliche Einwilligung oder die Belehrung über ein Widerspruchsrecht („opt-out“) nicht mehr den Anforderungen an eine wirksame Einwilligung. Es muss vielmehr eine ausdrückliche Einwilligung („opt-in“) in die Verarbeitung speziell dieser besonders sensiblen personenbezogenen Daten eingeholt werden. Art. 4 Nr. 11 DSGVO schreibt dazu konkret vor:

Art. 4 DSGVO
Begriffsbestimmungen
Im Sinne dieser Verordnung bezeichnet der Ausdruck:
[…]
11. „Einwilligung" der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;
[…]

Ich habe deshalb im Beurteilungszeitraum einige Kliniken bei der Erarbeitung datenschutzkonformer Unterlagen zur Einholung dieser nun erforderlichen Einwilligungen begleitet. Dabei habe ich insbesondere auch darauf geachtet, dass sich die Datenerhebung am Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 Buchst. c DSGVO orientiert. Krankenhäuser dürfen danach Daten nur insoweit verarbeiten, als dies für den jeweiligen Zweck erforderlich ist. Art. 5 Abs. 1 Buchst. c DSGVO lautet:

Art. 5 DSGVO
Grundsätze für die Verarbeitung personenbezogener Daten
(1) Personenbezogene Daten müssen
[…]
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung");
[…]

Die Kliniken haben mir dabei wiederholt von Praxisproblemen bei der Umsetzung der neuen datenschutzrechtlichen Notwendigkeiten berichtet. So sei es schwierig, Daten zur Religionszugehörigkeit zu löschen, wenn eine Patientin oder ein Patient zunächst seine Einwilligung erteilt, diese aber anschließend widerrufen hat. Diese Möglichkeit sieht die Datenschutz-Grundverordnung ausdrücklich vor, es muss sogar über das Widerrufsrecht bei Einholung einer Einwilligung informiert werden. Art. 7 Abs. 3 DSGVO regelt dazu:

Art. 7 DSGVO
Bedingungen für die Einwilligung
[…]
(3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.
[…]

Aufgrund der geschilderten Praxisprobleme und auch wegen des Grundsatzes der Datenminimierung habe ich in einigen Krankenhäusern angeregt, das Gespräch mit den betroffenen Kirchen zu suchen. Möglicherweise könnte der Informationsfluss von den Patientinnen und Patienten zu den Krankenhausseelsorgerinnen und Krankenhausseelsorgern und umgekehrt so gestaltet werden, dass die wertvolle Arbeit der Krankenhausseelsorge gewährleistet bleibt, ohne dass die Krankenhäuser selbst Daten verarbeiten müssten. Diese könnten weiterhin die Informationsweitergabe an die kirchlichen Seelsorgeeinrichtungen gewährleisten,

ohne dass sie selbst als datenschutzrechtlich Verantwortliche angesehen werden müssten, weil sie selbst nicht über Mittel und Zwecke der Datenverarbeitung mitbestimmen. Möglicherweise könnte sogar eine Rechtsstellung als Auftragsverarbeiter, welche ebenfalls mit zusätzlichen datenschutzrechtlichen Pflichten verbunden wäre, vermieden werden, indem die Kliniken Daten ausschließlich als eine Art Bote zwischen den Patientinnen und Patienten sowie den Krankenhausseelsorgerinnen und Krankenhausseelsorgern vermitteln. Insbesondere kommt in Betracht, dass die Kirchen eigenverantwortlich Unterlagen erstellen, die sie durch die Krankenhäuser an Patientinnen oder Patienten weitergeben. Ob die sonstigen Prozesse im Klinikalltag, insbesondere bei der Aufnahme einer Patientin oder eines Patienten, derartige Regelungen organisatorisch zulassen und ob auch die kirchlichen Interessen dabei umfassend berücksichtigt werden können, kann ich als staatliche Datenschutz-Aufsichtsbehörde nicht abschließend beurteilen.

7.3 Datenschutzgerechte Gestaltung von Einladungen zum Mammographie-Screening

Das Thema Mammographie-Screening beschäftigt mich seit vielen Jahren. Die grundlegenden Abläufe zum Mammographie-Screening und zum Einladungswesen der Zentralen Stelle Mammographie-Screening Bayern wurden bereits in den Tätigkeitsberichten vergangener Jahre dargestellt (siehe meine Ausführungen im 24. Tätigkeitsbericht 2010 unter Nr. 2.2.7 sowie im 23. Tätigkeitsbericht 2008 unter Nr. 15.2).

Im Berichtszeitraum haben mich erneut viele Anfragen von Bürgerinnen zur Gestaltung der Briefumschläge erreicht, mit denen das Einladungsschreiben der Zentralen Stelle Mammographie-Screening Bayern versandt worden ist. Die Briefumschläge waren mit einem auffälligen Logo und Absenderaufdruck versehen. Die Empfängerinnen störte dabei insbesondere, dass für alle Personen, denen die Sendung in die Hand gelangen kann (beispielsweise Postbeschäftigte) und denen außerdem die Hintergründe des Mammographie-Screenings bekannt sind, ein Rückschluss auf das Alter der Frauen (über 50 Jahre) möglich war.

Art. 31a Satz 1 Gesundheitsdienst- und Verbraucherschutzgesetz (GDVG) bestimmt, dass „Zentrale Stellen“, die befugt sind, Maßnahmen zur Früherkennung von Erkrankungen der Bevölkerung zu koordinieren, von den Meldebehörden Daten aus dem Melderegister verarbeiten können, soweit es zur Erfüllung ihrer Aufgaben erforderlich ist.

Die Zentrale Stelle Mammographie-Screening Bayern bezweckte mit der auffälligen Optik der Umschläge, den Aufmerksamkeitswert zu erhöhen. Damit sollte vermieden werden, dass die zur Portooptimierung per Dialogpost versandten Einladungsschreiben versehentlich mit Werbesendungen verwechselt und ungesehen vernichtet würden.

Die in Art. 31a Satz 1 GDVG enthaltene Einschränkung, dass Daten nur insoweit verarbeitet werden dürfen, als es zur Aufgabenerfüllung erforderlich ist, ist Ausdruck des in Art. 5 Abs. 1 Buchst. c DSGVO verankerten Grundsatzes der Datenminimierung. Ob die markante Gestaltung der Briefumschläge als Mittel zur Erreichung des Zwecks der Datenverarbeitung erforderlich ist, erschien mir hier fraglich.

Auf meine Bitte hin, die für die Versendung der Einladungsschreiben verwendeten Briefumschläge datenschutzfreundlicher zu gestalten, sagte die Zentrale Stelle Mammographie-Screening Bayern daher zu, wieder auf neutrale Kuverts für die Einladung zum Mammographie Screening umzustellen, sobald – aus Gründen der Wirtschaftlichkeit – die bereits vorhandenen Briefumschläge aufgebraucht seien. Die neutralen Kuverts würden dann für mindestens ein Jahr verwendet, um zu eruieren, ob die Fallzahlen bei der Inanspruchnahme der Früherkennungsuntersuchung durch diese Umstellung signifikant zurückgingen. Sollte ein solcher Effekt ausbleiben, werde die Zentrale Stelle Mammographie-Screening Bayern die neutralen Briefumschläge beibehalten. Eine unauffällige Angabe des Absenders auf dem Kuvert ist nach meinem Dafürhalten dabei auch weiterhin aus datenschutzrechtlicher Sicht nicht zu beanstanden, da diese für die Rücksendung von falsch adressierten Briefen notwendig ist.

Ich begrüße, dass durch die Änderung der Kuverts dem Anliegen vieler Bürgerinnen entsprochen wird, zum Mammographie-Screening eingeladen zu werden, ohne dabei Aufsehen bei Dritten zu erregen.

7.4 Veröffentlichung von Jubiläumsdaten

Eine betroffene Person beschwerte sich bei mir darüber, dass ein **Zahnärztlicher Bezirksverband** Jubiläumsdaten seiner Mitglieder veröffentlicht habe, obwohl sie dafür keine Einwilligung gemäß der Datenschutz-Grundverordnung erteilt habe.

Weiterhin hatte eine bayerische **Kammer eines freien Berufs** Jubiläumsdaten ihrer Mitglieder in einer von einer dritten Stelle herausgegebenen Zeitschrift veröffentlichen lassen, welcher sie personenbezogene Daten ihrer Mitglieder zuvor übermittelt hatte.

In meiner Prüfungspraxis musste ich wiederholt feststellen, dass Verantwortliche die Anforderungen des neuen Datenschutzrechts an Einwilligungen nicht ausreichend berücksichtigen.

Im Fall des **Zahnärztlichen Bezirksverbands** war zunächst zu bedenken, dass Behörden gemäß Art. 6 Abs. 1 UAbs. 2 DSGVO – anders als private Stellen – regelmäßig nicht nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO Daten unmittelbar auf Grundlage einer Interessenabwägung verarbeiten dürfen.

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

Außerdem ergibt sich insbesondere aus Art. 6 Abs. 3 UAbs. 1 DSGVO, dass auch die Datenverarbeitung im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt auf Grundlage von Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO nur zulässig ist, wenn dies in einem (nationalen) Gesetz ausdrücklich erlaubt wird:

Art. 6 DSGVO
Rechtmäßigkeit der Verarbeitung
[…]
(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch
a) Unionsrecht oder
b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.
[…]

Allerdings dürfen Behörden bei Wahrnehmung ihrer Aufgaben dann, wenn es dafür keine gesetzliche Regelung gibt, allenfalls ausnahmsweise Daten auf Grundlage einer Einwilligung verarbeiten. Da es nicht zu den eigentlichen Aufgaben eines Berufsverbandes oder einer Kammer gehört, über Jubiläumsdaten ihrer Mitglieder zu informieren, schied insbesondere eine Rechtfertigung der Veröffentlichung von Jubiläumsdaten auf Grundlage von Art. 4 Abs. 1 BayDSG aus.

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

Hier lag bereits der Fehler beim Zahnärztlichen Bezirksverband, welcher offenbar davon ausging, dass die Einholung einer Einwilligung überhaupt nicht erforderlich sei.

Im Fall der **Kammer eines freien Berufs** war von Bedeutung, dass sich die formellen Anforderungen an eine wirksame Einwilligung mit Geltungsbeginn der Datenschutz-Grundverordnung verschärft haben. Insbesondere kann es nach Art. 4 Nr. 11 DSGVO nicht mehr genügen, wenn die von einer Datenverarbeitung betroffene Person auf ein Widerspruchsrecht hingewiesen wird (sog. „opt-out"), sie muss vielmehr eine ausdrückliche, das heißt eine mit einer bestätigenden Handlung der betroffenen Person verbundene und informierte Einwilligung für den Einzelfall abgeben (sog. „opt-in"):

Art. 4 DSGVO
Begriffsbestimmungen
Im Sinne dieser Verordnung bezeichnet der Ausdruck:
[…]
11. „Einwilligung" der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;
[…]

Die von der Berufskammer initiierte Veröffentlichungsrubrik in der von einer dritten Stelle herausgegebenen Zeitschrift war lediglich mit folgendem wiederkehrenden Hinweis versehen worden: „Mitteilungen für diese Rubrik werden gerne entgegengenommen und kostenlos veröffentlicht. Bitte teilen Sie uns rechtzeitig mit, falls Sie keine Veröffentlichung wünschen." Nach geltender Rechtslage kann dieser allgemeine Hinweis, der möglicherweise nicht von jeder von der Datenverarbeitung betroffenen Person wahrgenommen wird, eine Einwilligung nicht ersetzen.

Eine Geldbuße nach Art. 83 DSGVO konnte ich in beiden Fällen nicht verhängen. Nach Art. 22 BayDSG dürfen gegen öffentliche Stellen Geldbußen nur verhängt werden, soweit diese als Unternehmen am Wettbewerb teilnehmen. Das ist bei dem Zahnärztlichen Bezirksverband sowie der Berufskammer nicht der Fall.

8 Sozialverwaltung

8.1 Arbeitspapier zur Verarbeitung von Sozialdaten im Bereich der Beistandschaft, Amtspflegschaft und der Amtsvormundschaft

Beistandschaft, Amtspflegschaft und Amtsvormundschaft stellen spezielle Formen der gesetzlichen Vertretung eines Kindes dar. Übernommen wird diese Vertretung grundsätzlich von Bediensteten des Jugendamtes. Bei Ausübung dieser Tätigkeiten nehmen die Beschäftigten eine Art „Sonderrolle" innerhalb des Jugendamtes ein. Dies zeigt sich unter anderem daran, dass das Achte Buch Sozialgesetzbuch – Kinder und Jugendhilfe – (SGB VIII) für die im Zusammenhang mit diesen Tätigkeiten vorzunehmenden Datenverarbeitungen mit § 68 Abs. 1 SGB VIII eine besondere Vorschrift enthält:

„Der Beamte oder Angestellte, dem die Ausübung der Beistandschaft, Amtspflegschaft oder Amtsvormundschaft übertragen ist, darf Sozialdaten nur verarbeiten, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist. Die Nutzung dieser Sozialdaten zum Zwecke der Aufsicht, Kontrolle oder Rechnungsprüfung durch die dafür zuständigen Stellen sowie die Übermittlung an diese ist im Hinblick auf den Einzelfall zulässig."

Hinsichtlich des Vollzugs dieser Vorschrift durch die bayerischen Jugendämter habe ich eine datenschutzrechtliche Querschnittsprüfung durchgeführt. Dabei ging es schwerpunktmäßig um die Organisationsstruktur der Jugendämter in Bayern sowie um den Austausch der Beistände, Amtspfleger und Amtsvormünder mit anderen Bereichen des Jugendamtes.

Als ein zentraler Aspekt lässt sich insbesondere festhalten, dass die Bereiche der Beistandschaft, Amtspflegschaft und Amtsvormundschaft datenschutzrechtlich **privilegiert** sind, indem die Regelungen des Sozialdatenschutzes nur eingeschränkt Anwendung finden (Umkehrschluss aus § 61 Abs. 2 SGB VIII). Dieses Privileg hat allerdings zur Folge, dass die **Abschottung** gegenüber anderen Teilen der Kommune oder des Landratsamtes, auch und gerade innerhalb des Jugendamtes, gewährleistet sein muss.

Des Weiteren stellt eine Datenweitergabe zwischen zwei Sachgebieten eines Jugendamtes eine **Datenübermittlung** dar, da im Jugendamt jede Organisationseinheit, die eine Aufgabe nach einem der Besonderen Teile des Sozialgesetzbuchs (Zweites bis Zwölftes Buch Sozialgesetzbuch sowie Gesetze im Sinne von § 68 Erstes Buch Sozialgesetzbuch – Allgemeiner Teil –) wahrnimmt, jeweils als Verantwortlicher gilt (siehe § 67 Abs. 4 Satz 2 SGB X, sog. funktionaler Stellenbegriff). Das bedeutet, dass es für die Zulässigkeit eines Austausches personenbezogener Daten (= Datenübermittlung) einer **Rechtsgrundlage** bedarf. Eine solche kann sich insbesondere aus einer gesetzlichen Verarbeitungsbefugnis oder ausnahmsweise aus einer Einwilligung ergeben.

Die in den Bereichen Beistandschaft, Amtspflegschaft und Amtsvormundschaft zu beachtenden datenschutzrechtlichen Anforderungen habe ich in einem Arbeitspapier[16] zusammengefasst.

8.2 Schutz von Informantinnen und Informanten bei Meldung einer Kindeswohlgefährdung

Im Berichtszeitraum habe ich mich – wie bereits in der Vergangenheit (siehe meinen 23. Tätigkeitsbericht 2008 unter Nr. 17.8) – mehrfach mit der Frage beschäftigt, ob die personenbezogenen Daten einer Informantin oder eines Informanten im Zusammenhang mit der Meldung einer Kindeswohlgefährdung den betroffenen Eltern oder dem betroffenen Elternteil gegenüber genannt werden dürfen.

Wenn Eltern oder ein Elternteil in Erfahrung bringen möchte(n), wer dem Jugendamt Informationen über sie oder ihn mitgeteilt hat, können sie oder kann er zunächst grundsätzlich das Recht auf Auskunft gemäß Art. 15 Abs. 1 DSGVO geltend machen. Nach dieser Vorschrift hat eine betroffene Person einen Anspruch darauf, zu erfahren, ob personenbezogene Daten über die eigene Person verarbeitet werden. Wenn dies bei einer öffentlichen Stelle, hier beim Jugendamt, der Fall sein sollte, hat die jeweilige Person insbesondere das Recht auf Auskunft, um welche Daten es sich dabei konkret handelt. Soweit Daten nicht bei der betroffenen Person selbst erhoben, sondern beispielsweise von Dritten dem Jugendamt gegenüber mitgeteilt worden sind, muss das Jugendamt gemäß Art. 15 Abs. 1 Buchst. g DSGVO grundsätzlich über die Herkunft dieser Daten, also auch über die Identität von Informanten, Auskunft geben.[17]

Es gibt jedoch Ausnahmen zum Auskunftsrecht, in denen eine Auskunft teilweise oder sogar ganz verweigert werden darf. Dieser Umstand ist auf Art. 23 DSGVO zurückzuführen, der den Mitgliedstaaten unter anderem erlaubt, das Recht auf Auskunft einzuschränken. Hierfür bedarf es einer gesetzlichen Regelung. Eine solche findet sich zum Beispiel im Zehnten Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X). Demnach besteht das Recht auf Auskunft dann nicht, soweit die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten geheim gehalten werden müssen und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss (§ 83 Abs. 1 Nr. 1 und § 82a Abs. 1 Nr. 2 SGB X).

Eine solche Rechtsvorschrift stellt § 65 Achtes Buch Sozialgesetzbuch – Kinder und Jugendhilfe – (SGB VIII) dar. Danach kommt dem Jugendamt anvertrauten Daten ein besonderer Vertrauensschutz zu. Solche Daten liegen vor, wenn die Informationen dem Jugendamt zum Zweck persönlicher und erzieherischer Hilfe anvertraut worden sind. Anvertraut sind die Informationen nicht nur, wenn die Mitteilung „unter dem Siegel der Verschwiegenheit“ erfolgt, sondern immer dann, wenn derjenige, der die Information der Mitarbeiterin oder dem Mitarbeiter des Ju-

16 Bayerischer Landesbeauftragter für den Datenschutz, Verarbeitung von Sozialdaten durch Beistand, Amtspfleger und Amtsvormund, Stand 2/2019, Internet: https://www.datenschutz-bayern.de, Rubrik „Veröffentlichungen – Informationsreihe – Einzelthemen“.

17 Dix, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 15 DSGVO Rn. 24.

gendamtes preisgibt, im Sinne einer subjektiven Zweckbindung von dessen Verschwiegenheit ausgeht und dies ausdrücklich signalisiert wird oder aus dem Zusammenhang erkennbar ist.[18] Unter diesen Voraussetzungen besteht grundsätzlich ein Weitergabeverbot; nur in den gemäß § 65 Abs. 1 Satz 1 Nr. 1 bis 5 SGB VIII genannten Fällen dürfen anvertraute Sozialdaten weitergegeben werden, das heißt insbesondere, wenn beispielsweise eine Informantin oder ein Informant in die Weitergabe einwilligt.

Der Name einer Informantin oder eines Informanten sowie deren oder dessen Angaben zur Sache werden meines Erachtens von § 65 SGB VIII geschützt und sind daher grundsätzlich geheim zu halten.[19] Diese Daten sind nach der Rechtsprechung des Bayerischen Verwaltungsgerichtshofs sogar dann geheim zu halten, wenn die (anvertrauten) Informationen möglicherweise wider besseres Wissen und in Schädigungsabsicht mitgeteilt worden sind.[20] Begründet wird dies damit, dass der Gesetzgeber unter anderem mit § 65 SGB VIII den Datenschutz im Jugendhilferecht höher gewichtet hat als das nachvollziehbare Interesse von betroffenen Personen, sich über die Herkunft von personenbezogenen Daten zu informieren, um sich gegebenenfalls gegen haltlose Anschuldigungen wehren zu können.

Die Jugendämter sind auf die Anzeige von Verdachtsfällen durch Personen, die sich um das Wohlergehen von Kindern und Jugendlichen sorgen, angewiesen, um zum Schutz der jungen Menschen eingreifen zu können. Die Tatsache, dass gerade nahestehende Personen, wie Verwandte, Nachbarinnen und Nachbarn oder auch Familienangehörige über den dafür notwendigen Einblick in familieninterne Konfliktlagen verfügen, macht es nachvollziehbar, dass eine solche Anzeige entweder gänzlich anonym oder aber unter Angabe von Personendaten unter der Zusicherung erfolgt, dass diese vom Jugendamt nicht weitergegeben werden. Könnten die Jugendämter diese Vertraulichkeit nicht garantieren, wären sie eines wichtigen Mittels beraubt, um eventuelle familiäre Probleme rechtzeitig zu entdecken und zu lösen.[21]

§ 65 SGB VIII ist im Übrigen auch bei einem Antrag auf Akteneinsicht zu berücksichtigen (siehe § 25 Abs. 3 SGB X).

8.3 Datenübermittlung an die Staatsanwaltschaft in strafrechtlichen Ermittlungsverfahren

Einige Sozialbehörden haben sich an mich gewandt und um datenschutzrechtliche Beratung im Hinblick auf die Anwendung der **Übermittlungsbefugnis** des § 69 Abs. 1 **Nr. 2** Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X) im Zusammenhang mit **strafrechtlichen Ermittlungsverfahren** gebeten.

18 Mörsberger, in: Wiesner, SGB VIII, Kinder- und Jugendhilfe, 5. Aufl. 2015, § 65 Rn. 12.

19 So auch Verwaltungsgericht Augsburg, Urteil vom 27. September 2011, 3 K 09.1571, BeckRS 2012, 46919, Rn. 21; Verwaltungsgericht Karlsruhe, Beschluss vom 16. Oktober 2012, 4 K 2344/12, BeckRS 2012, 58469.

20 Bayerischer Verwaltungsgerichtshof, Beschluss vom 1. Juni 2011, 12 C 10.1510, BeckRS 2011, 30537, Rn. 6, und Beschluss vom 23. Dezember 2011, 12 ZB 10.482, BeckRS 2012, 52367, Rn. 10.

21 So auch Verwaltungsgericht Regensburg, Urteil vom 27. Mai 2014, RO 4 K 14.423, BeckRS 2014, 59641.

§ 69 Abs. 1 **Nr. 2** SGB X regelt eine Befugnis zur Übermittlung von Sozialdaten für die Durchführung eines Gerichtsverfahrens einschließlich eines Strafverfahrens:

„Eine Übermittlung von Sozialdaten ist zulässig, soweit sie erforderlich ist
[…]
2. für die Durchführung eines mit der Erfüllung einer Aufgabe nach Nummer 1 zusammenhängenden gerichtlichen Verfahrens einschließlich eines Strafverfahrens […]".

§ 69 Abs. 1 **Nr. 2** SGB X ist vom Wortlaut her eng mit § 69 Abs. 1 **Nr. 1** SGB X verknüpft. Diese Vorschrift lautet:

„Eine Übermittlung von Sozialdaten ist zulässig, soweit sie erforderlich ist
1. für die Erfüllung der Zwecke, für die sie erhoben worden sind, oder für die Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle nach diesem Gesetzbuch oder einer solchen Aufgabe des Dritten, an den die Daten übermittelt werden, wenn er eine in § 35 des Ersten Buches genannte Stelle ist".

Im Rahmen der Beratung ging es zum einen um die Frage, ob § 69 Abs. 1 Nr. 2 SGB X auch das strafrechtliche Ermittlungsverfahren umfasst.

Zum anderen stellte sich die Frage, ob eine Sozialbehörde aufgrund dieser Vorschrift auch Sozialdaten übermitteln darf, wenn sich eine Ermittlungsbehörde (allein) aufgrund eines Strafverfolgungsinteresses an diese Sozialbehörde wendet.

Beide Fragestellungen sind – soweit ersichtlich – durch höchstrichterliche Rechtsprechung bislang nicht abschließend geklärt.

Im Rahmen der Beurteilung dieser Fragestellungen war auch eine Abgrenzung zu einer anderen Vorschrift – nämlich § 73 SGB X – notwendig. Dessen Absatz 1 lautet wie folgt:

„Eine Übermittlung von Sozialdaten ist zulässig, soweit sie zur Durchführung eines Strafverfahrens wegen eines Verbrechens oder wegen einer sonstigen Straftat von erheblicher Bedeutung erforderlich ist."

8.3.1 Strafrechtliches Ermittlungsverfahren

Bezüglich der ersten Frage habe ich gegenüber der Sozialbehörde die Auffassung vertreten, dass ich das strafrechtliche Ermittlungsverfahren als vom Anwendungsbereich des § 69 Abs. 1 Nr. 2 SGB X mitumfasst erachte.[22]

Hierfür spricht bereits der Wortlaut dieser Vorschrift. Das straf**gerichtliche** Verfahren wäre bereits von der ersten Textpassage („eines damit zusammenhängenden gerichtlichen Verfahrens") erfasst. Die ausdrückliche Nennung des „Strafver-

[22] So auch Landgericht Stuttgart, Beschluss vom 11. Mai 1993, 14 Qs 23/93, BeckRS 9998, 34887; Amtsgericht Kiel, Beschluss vom 5. Mai 2011, 43 Gs 612/11, BeckRS 9998, 32958.

fahrens“ neben dem gerichtlichen Verfahren macht nur dann Sinn, wenn der Gesetzgeber auch das Verfahren außerhalb des gerichtlichen Strafverfahrens erfassen wollte.

Des Weiteren stützt meine Auffassung auch die amtliche Gesetzesbegründung[23] zu einer anderen gesetzlichen Regelung, nämlich des § 73 SGB X-alt. Die damalige Überschrift zu dieser Vorschrift lautete „Offenbarung für die Durchführung eines Strafverfahrens“ (seit 1. Juli 1994: „Übermittlung für die Durchführung eines Strafverfahrens“). Der Gesetzesbegründung ist ausdrücklich zu entnehmen, dass diese Vorschrift auch für das Ermittlungsverfahren gelten soll. Aufgrund der Verwendung der gleichen Formulierung in § 69 Abs. 1 Nr. 2 SGB X gehe ich davon aus, dass auch das Verständnis des Gesetzgebers für das Wort „Strafverfahren“ in § 69 Abs. 1 Nr. 2 SGB X mit demjenigen in § 73 SGB X-alt übereinstimmt.

8.3.2 Strafverfolgungsinteresse der Ermittlungsbehörden

Meiner Ansicht nach ist der Anwendungsbereich von § 69 Abs. 1 Nr. 2 SGB X allerdings grundsätzlich nur dann eröffnet, wenn eine Sozialbehörde von sich aus die Ermittlungsbehörden einschaltet und nicht, wenn sich eine Ermittlungsbehörde aus eigenem Strafverfolgungsinteresse an eine Sozialbehörde wendet.

Die Sozialbehörde hat im Rahmen von § 69 Abs. 1 Nr. 2 SGB X selbst zu entscheiden, ob sie Sozialdaten übermitteln möchte und darf. Sie muss also prüfen, ob die Übermittlung zur Erfüllung einer **eigenen gesetzlichen Aufgabe** erforderlich ist. Meines Erachtens ist eine Übermittlung von Sozialdaten an Ermittlungsbehörden jedoch nur dann **erforderlich**, wenn die Sozialbehörde **ein eigenes Interesse an einer Strafverfolgung** hat. Zudem muss das jeweilige Verfahren mit der Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch zusammenhängen. Ob dieser Zusammenhang besteht, muss auch seitens der Sozialbehörde beurteilt werden, da sie für die Aufgabenerfüllung zuständig ist.

Wenn sich eine Ermittlungsbehörde aus eigenem Strafverfolgungsinteresse an eine Sozialbehörde wendet, wäre die Zulässigkeit einer Datenübermittlung vielmehr anhand der Voraussetzungen von § 73 SGB X zu prüfen.

8.4 Unterschrift unter Datenschutzhinweise

Im Berichtszeitraum erreichten mich wiederholt Anfragen von Bürgerinnen und Bürgern, die von einer öffentlichen Stelle dazu aufgefordert wurden, den Erhalt und die Kenntnisnahme von Merkblättern mit Datenschutzhinweisen durch Unterschrift zu bestätigen.

Dabei gingen die Behörden teilweise sehr beharrlich vor. So forderte ein Amt für Kinder, Jugendliche und Familien einen Bürger sogar dreimal mit Erinnerungsschreiben auf, ein Hinweisblatt zum Datenschutz für den Bereich der Beistandschaft unterschrieben zurückzusenden.

Die Datenschutz-Grundverordnung regelt in Art. 13 und 14 DSGVO, welche hier nach § 35 Abs. 2 Satz 1 Erstes Buch Sozialgesetzbuch – Allgemeiner Teil – (SGB I) unmittelbar neben den Regelungen zum Sozialdatenschutz anzuwenden

[23] Bundestags-Drucksache 8/4022, S. 86.

sind, dass die für eine Datenverarbeitung verantwortliche Stelle verpflichtet ist, die von einer Datenverarbeitung betroffenen Personen in gewisser Art und Weise zu informieren. Das Gesetz sieht jedoch weder keine Pflicht zur Kenntnisnahme von Informationen nach Art. 13 und 14 DSGVO vor – und erste recht keine Pflicht, die Kenntnisnahme durch Unterschrift zu bestätigen.

Ich habe in solchen Fällen die Behörden darauf hingewiesen, dass die Unterschrift einer betroffenen Person zur Bestätigung des Erhalts der Datenschutzhinweise nicht verpflichtend gefordert werden kann – auch nicht mit der Begründung, die Behörde wolle mit ihrem Vorgehen einen Nachweis über die Erfüllung der ihr obliegenden Informationspflicht schaffen (Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO).

Die öffentlichen Stellen haben daraufhin ihre Verfahrensweise dahingehend umgestellt, dass künftig auf eine Empfangsbestätigung durch Unterschrift verzichtet wird, und haben eine andere Form der Nachweisführung gewählt. So hat beispielsweise die eingangs erwähnte Behörde veranlasst, dass anstelle eines Zugangsnachweises durch Unterschrift die Ausgabe der Datenschutzhinweise durch die Sachbearbeiterin oder den Sachbearbeiter in der Akte der betroffenen Person vermerkt wird.

9 Personalverwaltung

9.1 Informationspflicht des Verantwortlichen bei Stellenbesetzungsverfahren in der bayerischen öffentlichen Verwaltung

Im Zusammenhang mit der Besetzung von Dienstposten und Arbeitsplätzen gehen bei den bayerischen öffentlichen Stellen Jahr für Jahr zahllose Bewerbungen ein. Diese Bewerbungen enthalten oftmals sehr detaillierte, in jedem Fall aber aussagekräftige personenbezogene Daten. Dass hier auch datenschutzrechtliche Informationspflichten zu erfüllen sind, liegt auf der Hand. Mich hat bereits eine Vielzahl von Anfragen bayerischer öffentlicher Stellen erreicht, welche Maßgaben insofern zu beachten sind. Für die Beantwortung dieser Frage sind im Wesentlichen zwei Konstellationen zu unterscheiden: die Bewerbung auf eine Stellenausschreibung und die Initiativbewerbung.

Die **Stellenausschreibung** (nachfolgend Nr. 9.1.1) kann einen konkreten (Beamten-)Dienstposten oder (Tarifbeschäftigten-)Arbeitsplatz betreffen – das ist die Regel –, sie kann aber auch unabhängig davon zur Abgabe von Bewerbungen auffordern. Das ist insbesondere dann der Fall, wenn die öffentliche Stelle einen „Bewerberpool" für die Besetzung zukünftig neu zu schaffender oder frei werdender Stellen bilden möchte. Diese Vorgehensweise ist etwa bei der Nachwuchsgewinnung für den Direkteinstieg in der vierten Qualifikationsebene (ehemals: beim Zugang zum Eingangsamt des höheren Dienstes) anzutreffen.

Bei einer **Initiativbewerbung** (nachfolgend Nr. 9.1.2) verhält sich die öffentliche Stelle zunächst passiv; sie hat keine Stellenausschreibung veröffentlicht. Eine interessierte Bewerberin oder ein interessierter Bewerber reicht von sich aus eine Bewerbung ein, weil sie oder er bei zukünftigen Stellenbesetzungen berücksichtigt werden möchte.

9.1.1 Informationspflicht bei Bewerbungen auf eine Stellenausschreibung

9.1.1.1 Ausgangslage

Erhalten bayerische öffentliche Stellen Bewerbungen auf eine Ausschreibung hin, so erheben sie personenbezogene Daten bei den Bewerberinnen und Bewerbern. Datenerhebungen dieser Art lösen die Informationspflicht nach Art. 13 DSGVO aus.[24]

Daher bemisst sich der Umfang an Informationen, die den Bewerberinnen und Bewerbern zur Verfügung zu stellen sind, nach Art. 13 Abs. 1 und 2 DSGVO. Eine Information kann (nur) dann unterbleiben, wenn und soweit eine Bewerberin oder ein Bewerber bereits über die jeweilige Information verfügt (Art. 13 Abs. 4 DSGVO). Zwar dürften die Bewerberinnen und Bewerber wissen, wer für die Verarbeitung personenbezogener Daten im Rahmen des Bewerbungsverfahrens

[24] Zu Informationspflichten allgemein siehe Bayerischer Landesbeauftragter für den Datenschutz, Informationspflichten des Verantwortlichen, Stand 11/2018, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Informationspflichten".

verantwortlich ist (die ausschreibende Stelle) und zu welchen Zwecken die Daten erhoben werden (Durchführung des Stellenbesetzungsverfahrens). Die übrigen in Art. 13 Abs. 1 und 2 DSGVO aufgeführten Angaben werden ihnen jedoch regelmäßig nicht umfassend bekannt sein.

Die ausschreibende öffentliche Stelle muss deshalb für die Bewerberinnen und Bewerber stets eine unter dem Gesichtspunkt von Art. 13 Abs. 1 und 2 DSGVO vollständige Information vorhalten.

9.1.1.2 Form der Information

Im Rahmen eines Bewerbungsverfahrens kann eine öffentliche Stelle ihrer Informationspflicht in unterschiedlicher Weise nachkommen. Sie kann grundsätzlich

— die Informationen nach Art. 13 DSGVO einer Bewerberin oder einem Bewerber direkt übermitteln (etwa in Gestalt eines Ausdrucks oder eines PDF-Dokuments) oder

— die Informationen auf ihrer jeweiligen Internetpräsenz zum Abruf bereithalten.

Hält die öffentliche Stelle die Informationen nach Art. 13 DSGVO zum Abruf bereit, kann sie auf eine direkte Übermittlung an Bewerberinnen und Bewerber (nur) unter den folgenden Voraussetzungen verzichten:

— Die öffentliche Stelle muss Bewerberinnen und Bewerber ausdrücklich darauf hinweisen, dass die Informationen nach Art. 13 DSGVO im Internet abgerufen werden können, und

— die Informationen nach Art. 13 DSGVO sind den Bewerberinnen und Bewerbern unter anderem in „leicht zugänglicher Form" zur Verfügung zu stellen (Art. 12 Abs. 1 Satz 1 DSGVO). Hieraus folgt zweierlei:

  Die bereitgestellten Informationen sind den Bewerberinnen und Bewerbern entweder mittels eines Direktlinks oder durch einfach zu befolgende Navigationshinweise zugänglich zu machen, sodass sich die betroffenen Personen nicht erst umständlich zu diesen Informationen „durchklicken" müssen.

  Da bei schriftlichen Bewerbungsverfahren nicht anzunehmen ist, dass alle Bewerberinnen und Bewerber über einen Internetzugang verfügen, ist im Regelfall eine Alternative anzugeben, mittels derer die Informationen zur Verfügung gestellt werden. Hier bietet sich etwa ein Bezug über den behördlichen Datenschutzbeauftragten, über die Personalabteilung der öffentlichen Stelle oder über die in der Stellenausschreibung für Rückfragen angegebene Kontaktperson an.

Demgemäß lässt sich ein Hinweis auf im Internet zum Abruf vorgehaltene Informationen nach Art. 13 DSGVO beispielhaft wie folgt formulieren:

„Informationen zur Verarbeitung Ihrer Bewerbungsdaten durch [Bezeichnung der öffentlichen Stelle] finden Sie unter [Angabe eines Direktlinks]. Alternativ können Sie sich auch an [Kontaktdaten eines Ansprechpartners] wenden."

9.1.1.3 Zeitpunkt der Information

Informationen nach Art. 13 DSGVO sind „zum Zeitpunkt der Erhebung“ mitzuteilen oder zur Verfügung zu stellen. Hier bieten sich verschiedene Möglichkeiten:

— Die öffentliche Stelle kann ihrer Informationspflicht bereits in der Ausschreibung nachkommen. Da eine unmittelbare Aufnahme der vollständigen Informationen wenig praktikabel ist, sollten die Informationen nach Art. 13 DSGVO in diesem Fall im Internet zum Abruf bereitgehalten werden. In die Ausschreibung wird dann ein entsprechender Hinweis aufgenommen. Die diesbezüglichen Anforderungen sind unter Nr. 9.1.1.2 dargestellt.

  Diese Vorgehensweise ist sowohl möglich, wenn die Stellenausschreibung ausschließlich in einem Printmedium veröffentlicht wird, als auch, wenn in einem Printmedium lediglich ein Hinweis auf die zu besetzende Stelle abgedruckt wird und im Weiteren auf die diesbezügliche vollständige Ausschreibung (etwa) auf der Homepage der öffentlichen Stelle verwiesen wird. Aus datenschutzrechtlicher Sicht ist sie im Grundsatz vorzugswürdig, weil die betroffenen Bewerberinnen und Bewerber sich rechtzeitig auf die konkrete Datenverwendung einstellen können.

— Kommt eine öffentliche Stelle ihrer Informationspflicht nicht bereits im Rahmen der Stellenausschreibung nach, hat sie einer Bewerberin oder einem Bewerber die Informationen nach Art. 13 DSGVO bei Eingang der Bewerbung zur Verfügung zu stellen.

  Dies erfordert eine Kontaktaufnahme (die etwa auch im Rahmen einer Eingangsbestätigung erfolgen kann) mit der jeweiligen Bewerberin oder dem jeweiligen Bewerber. Im Rahmen dieser Kontaktaufnahme sind die Informationen nach Art. 13 DSGVO entweder unmittelbar beizufügen (etwa als Merkblatt bei analoger oder als PDF-Datei bei elektronischer Kommunikation); alternativ kann unter Angabe eines Links darauf hingewiesen werden, dass die Informationen nach Art. 13 DSGVO für Bewerberinnen und Bewerber im Internet zum Abruf bereit stehen (vgl. bereits oben Nr. 9.1.1.2).

9.1.2 Informationspflicht bei Initiativbewerbungen

Bei einer Initiativbewerbung fehlt der Bezug auf eine Ausschreibung, und die öffentliche Stelle hat auch nicht auf andere Weise zur Einreichung von Bewerbungsdaten aufgefordert. Somit liegt bei Eingang der Initiativbewerbung zunächst keine „Erhebung“ im Sinne von Art. 13 DSGVO durch die jeweilige öffentliche Stelle vor.

Die öffentliche Stelle erhebt personenbezogene Daten allerdings dann, wenn sie anlässlich der Initiativbewerbung weitere personenbezogene Daten von der Bewerberin oder dem Bewerber erfragt. Das ist regelmäßig beim Einsatz eines Bewerberfragebogens, im Rahmen eines Assessment-Centers oder im Verlauf eines Vorstellungsgesprächs der Fall.

Spätestens zu diesen Anlässen sind die betreffenden Bewerberinnen und Bewerber gemäß Art. 13 DSGVO zu informieren. Allerdings bleibt es der öffentlichen Stelle unbenommen – und ist es aus Datenschutzsicht zu begrüßen –, wenn die öffentliche Stelle bereits bei Eingang einer Initiativbewerbung (etwa im Rahmen einer Eingangsbestätigung) eine betroffene Person im Umfang des Art. 13

DSGVO unterrichtet, und zwar unabhängig davon, ob es im Weiteren zu einer auf den Gewinn ergänzender Informationen gerichteten Datenerhebung durch die öffentliche Stelle kommt oder nicht.

9.1.3 Fazit

Grundsätzlich entsteht mit jeder Erhebung personenbezogener Daten eine Informationspflicht des Verantwortlichen gegenüber der betroffenen Person. Eine Datenerhebung im Rahmen eines Stellenbesetzungsverfahrens bildet hiervon keine Ausnahme. Einer bayerischen öffentlichen Stelle bieten sich dabei verschiedene Möglichkeiten, ihrer diesbezüglichen Informationspflicht ordnungsgemäß und mit vertretbarem Aufwand nachzukommen. Insbesondere bei Stellenausschreibungen können die entsprechenden Informationen für Bewerberinnen und Bewerber auf der Internetseite der jeweiligen öffentlichen Stelle zum Abruf bereitgehalten werden. In einer Stellenausschreibung kann hierauf mittels Verlinkung verwiesen werden. Im Regelfall ist zusätzlich noch ein alternativer Bezugsweg anzugeben, etwa über den behördlichen Datenschutzbeauftragten oder die in der Stellenausschreibung für Rückfragen genannte Kontaktperson.

9.2 Bekanntgabe von Personalentscheidungen gemeindlicher Gremien

Gemeindliche Gremien – der Gemeinderat und seine beschließenden Ausschüsse – sind für eine Vielzahl von **Personalentscheidungen** zuständig, die in einer Gemeinde zu treffen sind. Art. 43 Abs. 1 Satz 1 Gemeindeordnung (GO) bestimmt insofern:

„(1) [1]Der Gemeinderat ist zuständig,
1. die Beamten der Gemeinde ab Besoldungsgruppe A 9 zu ernennen, zu befördern, abzuordnen oder zu versetzen, an eine Einrichtung zuzuweisen, in den Ruhestand zu versetzen und zu entlassen,
2. die Arbeitnehmer der Gemeinde ab Entgeltgruppe 9 des Tarifvertrags für den öffentlichen Dienst oder ab einem entsprechenden Entgelt einzustellen, höherzugruppieren, abzuordnen oder zu versetzen, einem Dritten zuzuweisen, mittels Personalgestellung zu beschäftigen und zu entlassen.“

Diese Befugnisse können auf einen beschließenden Ausschuss übertragen werden (Art. 43 Abs. 1 Satz 2 GO). (Nur) in kreisfreien Gemeinden ist auch eine Übertragung auf den Oberbürgermeister möglich, soweit es um Beamte bis zur Besoldungsgruppe A 14 oder Beschäftigte bis zur Entgeltgruppe 14 des Tarifvertrags für den öffentlichen Dienst oder mit einem entsprechenden Entgelt geht (Art. 43 Abs. 1 Satz 3 GO).

Die in die Zuständigkeit des Gemeinderats oder seiner beschließenden Ausschüsse fallenden Personalentscheidungen werden grundsätzlich **in nichtöffentlicher Sitzung** getroffen, weil einer öffentlichen Behandlung regelmäßig „berechtigte Ansprüche einzelner entgegenstehen“ (Art. 52 Abs. 2 Satz 1 GO). Dementsprechend sehen auch die vom Bayerischen Gemeindetag bereitgestellten Muster für Geschäftsordnungen des Gemeinderats eine nichtöffentliche Behandlung

der „Personalangelegenheiten in Einzelfällen“ vor.[25] Allerdings bestimmt Art. 52 Abs. 3 GO:

„Die in nichtöffentlicher Sitzung gefaßten Beschlüsse sind der Öffentlichkeit bekanntzugeben, sobald die Gründe für die Geheimhaltung weggefallen sind.“

Die Bedeutung dieser Vorschrift im Zusammenhang mit Personalentscheidungen war bereits mehrfach Gegenstand an mich gerichteter Anfragen. Ich gebe aus datenschutzrechtlicher Sicht die folgenden Hinweise:

9.2.1 Bekanntgabe nur der Beschlüsse

Gegenstand der **Bekanntgabe** sind „[d]ie in nichtöffentlicher Sitzung gefaßten Beschlüsse“. Die Gemeinde genügt dem Bekanntgabeerfordernis, wenn sie den **Beschlusstenor** mitteilt. Die gesetzliche Vorgabe steht vor dem Hintergrund einer Verwaltungspraxis, die den Beschlusstenor nicht mit Begründungselementen vermischt. Das ist insbesondere (auch) bei Beschlussvorschlägen zu beachten, die im Rahmen der Beratung inhaltlich modifiziert werden oder aus der Mitte des Gemeinderats stammen.

Nicht öffentlich zu machen sind insbesondere etwa für die Gemeinderatsmitglieder bereitgestellte **Sitzungsunterlagen** sowie der **Hergang der Beratung**, wie er in der Niederschrift festgehalten ist. Daher sieht Art. 54 Abs. 3 GO insofern auch kein Zugangsrecht der Gemeindebürger vor.

9.2.2 Personenbezogene Daten im Beschlusstenor

Geht es um die Bekanntgabe einer Personalentscheidung in einem Einzelfall, wird der Beschlusstenor typischerweise personenbezogene Daten enthalten, wie folgende Praxisbeispiele zeigen:

Beispiel 1 (Einstellung einer Stadtjuristin): „Frau Josefa Huber wird zum 1. Juni 2019 unter Berufung in das Beamtenverhältnis auf Probe zur Rechtsrätin ernannt.“

Beispiel 2 (Höhergruppierung eines Tarifbeschäftigten): „Herr Josef Huber wird mit Wirkung zum 1. Juni 2019 in die Entgeltgruppe 10 Tarifvertrag für den öffentlichen Dienst höhergruppiert.“

Eine Bekanntgabe würde der Öffentlichkeit an personenbezogenen Daten in Beispiel 1 die Informationen über Josefa Huber vermitteln, dass diese (1) zu der betreffenden Gemeinde (2) ab dem 1. Juni 2019 (3) in einem Beamtenverhältnis (4) auf Probe steht, und zwar (5) im statusrechtlichen Amt einer Rechtsrätin, in Beispiel 2 die Informationen über Josef Huber, dass dieser (1) bei der betreffenden Gemeinde (2) tariflich beschäftigt ist und (3) ab dem 1. Juni 2019 der Entgeltgruppe 10 Tarifvertrag für den öffentlichen Dienst angehört. In beiden Fällen ist

[25] Siehe § 17 Abs. 1 Satz 1 Nr. 1 des Musters für kleinere und § 22 Abs. 1 Satz 1 Nr. 1 des Musters für größere Gemeinden, abgedruckt in der Verbandszeitschrift Bayerischer Gemeindetag 2014, S. 105 ff. und S. 116 ff.

zudem anhand der veröffentlichten Besoldungs- oder Entgelttabellen jedenfalls eine ungefähre Einschätzung des Berufseinkommens möglich.

9.2.3 Grundsätzlich keine Bekanntgabe von Personalaktendaten

Gremienbeschlüsse wie in den Beispielen 1 und 2 enthalten bereits im Tenor jeweils (ein Gefüge von) Informationen, die für sich genommen, jedoch auch im Verbund als **Personalaktendaten** anzusehen sind. Insofern ist **bereichsspezifisches Datenschutzrecht** zu beachten (§ 50 Beamtenstatusgesetz, Art. 103 ff. Bayerisches Beamtengesetz – BayBG), das für Beamtinnen und Beamte sowie – nach Art. 145 Abs. 2 BayBG im Grundsatz entsprechend – auch für Tarifbeschäftigte gilt.

Eine Bekanntgabe nach Art. 52 Abs. 3 GO ist datenschutzrechtlich als Initiativübermittlung an eine unbestimmte Vielzahl (nicht)öffentlicher Stellen zu werten. Dafür ist nach Art. 6 Abs. 1 DSGVO eine **Rechtsgrundlage** erforderlich, wobei zunächst nach einer Rechtsgrundlage in der Form einer **Verarbeitungsbefugnis** (Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 3 UAbs. 1 Buchst. b DSGVO) zu suchen ist.

— Aus den Übermittlungsbefugnissen in **Art. 108 Abs. 1 und 2 BayBG** kommt ersichtlich keine als Rechtsgrundlage für eine solche Bekanntgabe in Betracht.

— Unabhängig vom Vorliegen der Tatbestandsvoraussetzungen ist eine Heranziehung von **Art. 108 Abs. 4 BayBG** schon deshalb nicht angezeigt, weil die Erteilung einer Auskunft eine „Abfragesituation" voraussetzt, die bei einer Initiativübermittlung nicht vorliegt.

Ein „Ausweichen" auf die allgemeine Übermittlungsbefugnis in **Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG** ist ebenfalls nicht möglich, weil die Personalaktendaten betreffende (Gesamt-)Regelung im Bayerischen Beamtengesetz grundsätzlich abschließend ist.

Die Rechtsgrundlage für eine Bekanntmachung könnte daher grundsätzlich nur durch eine **Einwilligung** der oder des betroffenen Bediensteten vermittelt sein (vgl. Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 4 Nr. 11, Art. 7 DSGVO).

Dabei ist allerdings zu beachten, dass die Einwilligung nur wirksam ist, wenn sie **freiwillig** erteilt wurde (Art. 4 Nr. 11 DSGVO). Das Vorliegen dieses Merkmals ist bei der Einwilligung in die Bekanntgabe einer – oftmals günstigen – Personalentscheidung regelmäßig fraglich; eine beschäftigte Person könnte sich nämlich gedrängt sehen, gegenüber ihrem Dienstherrn oder Arbeitgeber „Wohlverhalten" zu zeigen. Eine Gemeinde ist unter keinem Gesichtspunkt verpflichtet, nur zum Zweck einer Bekanntgabe nach Art. 52 Abs. 3 GO um eine Einwilligung nachzusuchen. Selbstverständlich besteht auch für die Beschäftigten keine „Pflicht zur Einwilligung".

Die Bekanntgabepflicht aus **Art. 52 Abs. 3 GO** selbst kann die für eine Initiativübermittlung an eine unbestimmte Vielzahl (nicht)öffentlicher Stellen erforderliche Rechtsgrundlage ebenfalls nicht bereitstellen. Da eine Befugnis zu einer entsprechenden Übermittlung von Personalaktendaten fehlt, liegen – vorbehaltlich einer Einwilligung – grundsätzlich dauerhaft „Gründe für die Geheimhaltung" (Art. 52 Abs. 3 GO) vor, die einer Bekanntgabe entgegenstehen.

9.2.4 Möglichkeiten der Information über Personalentscheidungen im Einzelfall

Eine **Information**, die **ohne Personalaktendaten** auskommt, ist gleichwohl auch nach Personalentscheidungen im Einzelfall möglich. Die Gemeinde kann eine anonymisierte Information wählen (Nr. 9.2.4.1); soll die Identität einer bestimmten beschäftigten Person offengelegt werden, kann dies im (eher engen) Rahmen von Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG geschehen oder auf der Grundlage einer Einwilligung (Nr. 9.2.4.2).

9.2.4.1 Anonymisierte Information

Zum einen kann die Gemeinde entsprechende **Beschlüsse** datenschutzgerecht **ohne Nennung von Namen und Statusdetails bekanntgeben** (anonymisierte Bekanntgabe). Diese Vorgehensweise setzt voraus, dass nicht anderweit – beispielsweise aus einem veröffentlichten Organisationsplan – Rückschlüsse auf die Identität einer beschäftigten Person gezogen werden können. Die anonymisierte Bekanntgabe kommt deshalb **insbesondere für größere Städte** in Betracht, die für den Zugang zu ihren Verwaltungsdienstleistungen datenschutzfreundlich Funktions-E-Mail-Adressen und zentrale Rufnummern verwenden. Eine anonymisierte Bekanntgabe könnte in den oben gebildeten Beispielen folgendermaßen formuliert werden:

Beispiel 1 (Einstellung einer Stadtjuristin): „Der Stadtrat hat beschlossen, eine Juristin für das Rechtsamt einzustellen."

Beispiel 2 (Höhergruppierung eines Tarifbeschäftigten): „Der Hauptausschuss hat beschlossen, einen Mitarbeiter im Ordnungsamt höherzugruppieren."

9.2.4.2 Nicht anonymisierte Information

Zum anderen kommt eine **Information über Personalentscheidungen im Rahmen der kommunalen Öffentlichkeitsarbeit** in Betracht. Dabei geht es allerdings nicht darum, eine Bekanntgabe nach Art. 52 Abs. 3 GO zu bewirken. Das Ziel liegt vielmehr darin, die Gemeindeverwaltung **hinsichtlich wichtiger Ansprechpersonen** transparent zu machen.

Zu beachten ist in diesem Zusammenhang, dass die in Art. 39 Abs. 1 Satz 1 BayDSG zugunsten der Bürgerinnen und Bürger und in Art. 4 Abs. 1 Satz 1 Bayerisches Pressegesetz zugunsten der Presse geregelten Informationszugangsrechte der Gemeinde keine Datenübermittlungsbefugnisse für eine Öffentlichkeitsarbeit aus eigener Initiative vermitteln.

— Rechtsgrundlage: Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG

  Rechtsgrundlage für eine Übermittlung personenbezogener Daten kann in diesem Fall aber **Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG** sein. Wegen der abschließenden Regelung der Übermittlung von Personalaktendaten in Art. 108 BayBG kommen dabei nur solche Personalaktendaten in Betracht, die zugleich im Rahmen der Aufbauorganisation genutzte Sachaktendaten sein können (siehe die Ausführungen in meinem 22. Tätigkeitsbericht 2006 unter Nr. 19.1). Dies gilt insbesondere für die dienstliche Funktion (etwa „Leiter Ordnungsamt") sowie – bei Beamtinnen und Beamten – für die Amtsbezeichnung.

Das in Art. 5 Abs. 1 Satz 1 BayDSG zentrale Merkmal der **Erforderlichkeit** ist im Lichte des Interesses zu würdigen, das die Öffentlichkeit an der Kenntnis der Organisation einer Gemeindeverwaltung üblicherweise hat. Nach meiner Auffassung **kann** die Erforderlichkeit insbesondere bei der **Neueinstellung** einer Führungskraft oder einer (sonstigen) beschäftigten Person, die nach außen für die Gemeinde auftritt, bei der **Versetzung** einer Führungskraft **zu einem anderen Dienstherrn** sowie bei der **Versetzung** einer Führungskraft **in den Ruhestand** gegeben sein.

Führungskräfte sind dabei insbesondere (soweit vorhanden) berufsmäßige Gemeinderatsmitglieder und Geschäftsleitungen, ferner die Geschäftsbereichs- und Fachbereichsleitungen (Abteilungsleitungen, Sachgebietsleitungen). Bei den sonstigen **Beschäftigten, die nach außen für die Gemeinde auftreten** (zu dieser Personengruppe siehe bereits die Ausführungen in meinem 24. Tätigkeitsbericht 2010 unter Nr. 6.11), steht die Funktion als Ansprechpartner im Vordergrund der Aufgaben (Beispiele: Pressesprecher, Koordinatorin für den Bereich Ehrenamt/Vereine, Veranstaltungssachbearbeiter in einem Ordnungsamt; Gegenbeispiele: Mitarbeiterinnen in Kindertageseinrichtungen, Beschäftigte in einer Registratur oder im Archiv, Sachbearbeiterinnen im Personalamt).

— Rechtsgrundlage: Einwilligung

Davon abgesehen kann **Rechtsgrundlage** – unter den oben zu 3. dargestellten Maßgaben – auch eine **Einwilligung**[26] sein. Sie ist erforderlich, wenn über Beschäftigte berichtet werden soll, die nicht zu den herausgehobenen Führungskräften gehören, oder wenn hinsichtlich solcher Führungskräfte ein „Mehr" an Informationen geboten werden soll (Beispiele: Notiz im „Gemeindeboten" über den Eintritt eines verdienten Sachbearbeiters in den Ruhestand; Pressemitteilung über die Einstellung einer Stadtbaumeisterin mit Kurzbiografie und Lichtbild).

9.2.5 Fazit

Die Kommunikation gemeindlicher Personalentscheidungen gegenüber der Öffentlichkeit ist eine regelmäßig wiederkehrende Verwaltungsaufgabe. Art. 52 Abs. 3 GO gibt dazu keine Routine vor. Die Gemeinde muss dem Schutz personenbezogener Daten den erforderlichen Stellenwert einräumen. Die Übermittlungsbefugnis aus Art. 5 Abs. 1 Satz 1 Nr. 1 BayDSG lässt in bestimmten Fällen eine Veröffentlichung grundlegender Informationen zu; im Übrigen kann nur eine Einwilligung die nötige Rechtsgrundlage bieten.

9.3 Umgang mit amtsärztlichen Zeugnissen bei der Bayerischen Polizei

Bei dienstlich veranlassten amtsärztlichen Untersuchungen werden **– teils hochsensible – Gesundheitsdaten** von Beschäftigten verarbeitet. Diese Begutachtungen bilden zudem regelmäßig die sachverständige Grundlage für Entscheidungen des Dienstherrn, welche unter Umständen weitreichende Konsequenzen für

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

die betroffenen Beschäftigten haben können – insbesondere, wenn es um Verfahren der vorzeitigen Ruhestandsversetzung wegen Dienstunfähigkeit geht. Es verwundert deshalb nicht, dass dieser Themenkomplex regelmäßig den Gegenstand entsprechender Eingaben und Anfragen darstellt.

Im Berichtszeitraum hat mich hierzu unter anderem eine Eingabe zu **polizeiärztlichen Begutachtungen der Dienst- und Verwendungsfähigkeit** von Beamtinnen und Beamten der Bayerischen Polizei erreicht. Schwerpunkt dieser Eingabe war die Frage, ob und gegebenenfalls in welchem Umfang **Fachvorgesetzten** der betroffenen Beschäftigten **Feststellungen** aus einer solchen Begutachtung **mitgeteilt werden dürfen**.

9.3.1 Sachverhalt

Im Zuständigkeitsbereich eines Polizeipräsidiums wurde bei Begutachtungen der Dienst- und Verwendungsfähigkeit von Beamtinnen und Beamten die folgende Verfahrensweise praktiziert:

Nach Durchführung der Begutachtung übermittelte der Ärztliche Dienst der Bayerischen Polizei (im Folgenden: polizeiärztlicher Dienst) das Gesundheitszeugnis oder einen Abdruck hiervon sowohl an das Polizeipräsidium als auch an die begutachtete Beamtin oder den begutachteten Beamten. Das Polizeipräsidium gab der Beamtin oder dem Beamten darüber hinaus den **nahezu vollständigen Inhalt des Gesundheitszeugnisses** mittels eines **Schreibens** bekannt, welches der Beamtin oder dem Beamten jedoch nicht unmittelbar, sondern **über die Leitung der jeweiligen Polizeiinspektion** übermittelt wurde. Auf diesem Weg erhielt auch der oder die **(Fach-)Vorgesetzte** der Beamtin oder des Beamten eine recht **umfassende Kenntnis** vom Inhalt des Gesundheitszeugnisses.

Das Polizeipräsidium hat diese Verfahrensweise mir gegenüber damit begründet, dass sie zum einen bezwecke, die Adressatin oder den Adressaten über das Ergebnis der polizeiärztlichen Untersuchung zu informieren, zum anderen aber auch, die Dienststellenleitung über die Beurteilung der dienstlichen Verwendungsfähigkeit und etwaiger Verwendungseinschränkungen der betroffenen Person sowie über die notwendigen zukünftigen Maßnahmen zur Wiederherstellung der Dienstfähigkeit in Kenntnis zu setzen.

9.3.2 Rechtliche Würdigung

Auch wenn das Polizeipräsidium im Weiteren ausgeführt hat, dass „ärztliche Diagnosen, medizinische Gutachten oder Ähnliches, die für eine Übermittlung an den Vorgesetzen nicht geeignet wären“, nicht Bestandteil eines solchen Schreibens seien, habe ich die dargestellte Verfahrensweise aus Datenschutzsicht dem Polizeipräsidium gegenüber **kritisiert**.

Im Einzelnen:

— Die Überprüfung der Dienstfähigkeit eines Beamten oder einer Beamtin ist nach den einschlägigen beamtenrechtlichen Vorschriften **Sache des oder der (unmittelbaren) Dienstvorgesetzten** im Sinn des Art. 3 Satz 1 Bayerisches Beamtengesetz (BayBG):

Art. 65 BayBG
Verfahren bei Ruhestandsversetzungen wegen Dienstunfähigkeit
(1) […]
(2) [1]Bestehen Zweifel über die Dienstunfähigkeit, so ist der Beamte oder die Beamtin verpflichtet, sich nach Weisung des oder der Dienstvorgesetzten ärztlich untersuchen und, falls ein Amtsarzt oder eine Amtsärztin dies für erforderlich hält, beobachten zu lassen. […]
(3) [1]Wird in den Fällen des § 26 Abs. 1 BeamtStG ein Antrag auf Versetzung in den Ruhestand gestellt, so wird die Dienstunfähigkeit dadurch festgestellt, dass der unmittelbare Dienstvorgesetzte oder die unmittelbare Dienstvorgesetzte auf Grund eines amtsärztlichen Gutachtens über den Gesundheitszustand erklärt, er oder sie halte den Beamten oder die Beamtin nach pflichtgemäßem Ermessen für dauernd unfähig, die Dienstpflichten zu erfüllen. […]
(4) […]

Art. 66 BayBG
Zwangspensionierungsverfahren
(1) Hält der oder die Dienstvorgesetzte den Beamten oder die Beamtin für dienstunfähig und beantragt dieser oder diese die Versetzung in den Ruhestand nicht, so teilt der oder die Dienstvorgesetzte dem Beamten, der Beamtin, dessen oder deren Vertreter oder Vertreterin schriftlich mit, dass die Versetzung in den Ruhestand beabsichtigt sei; dabei sind die Gründe für die Versetzung in den Ruhestand anzugeben.
(2) […]

Eine **Zuständigkeit der oder des (Fach-)Vorgesetzten** im Sinn des Art. 3 Satz 2 BayBG **besteht insoweit nicht**.

— Die Kenntnisnahme des oder der (Fach-)Vorgesetzten (vorliegend des Leiters der betreffenden Polizeiinspektion) vom Inhalt des Gesundheitszeugnisses einer Beamtin oder eines Beamten ist danach **nicht regelhaft**, sondern **nur in Ausnahmefällen** und nur insoweit **zulässig**, als eine solche Kenntnisnahme **erforderlich** ist. Dies kann in aller Regel **nur dann und nur insoweit** der Fall sein, als sich aus dem Gesundheitszeugnis unmittelbare Folgerungen und Auswirkungen auf den Dienstbetrieb oder auf die Gestaltung des Arbeitsplatzes des Beamten oder der Beamtin ergeben, welche entsprechende Umsetzungs- oder Durchführungsmaßnahmen der Dienststellenleitung erfordern.

— Diese Vorgaben, die nicht zuletzt Ausfluss des datenschutzrechtlichen **Erforderlichkeitsgrundsatzes** sind (vgl. Art. 5 Abs. 1 Buchst. c DSGVO, Art. 103, 108 BayBG), wurden jedenfalls in dem der besagten Eingabe zugrunde liegenden Fall **nicht hinreichend beachtet**:

So enthielt das – auch der Leitung der jeweiligen Polizeiinspektion zur Kenntnis gebrachte – Schreiben des Polizeipräsidiums neben dem Hinweis, dass der betroffene Beamte „weiterhin dienstunfähig erkrankt“ sei, **detaillierte Ausführungen** zu ambulanten und stationären Therapiemaßnahmen, welche zur Wiederherstellung der Dienstfähigkeit aus ärztlicher Sicht empfohlen wurden. Da diese Ausführungen keinen unmittelbaren Bezug zur Arbeitsplatzgestaltung oder zur konkreten Verwendbarkeit des Beamten aufwiesen, war nicht ersichtlich, weshalb eine Kenntnisnahme durch die Dienststellenleitung erforderlich gewesen wäre. Dies gilt umso

mehr, als die Ausführungen im konkreten Fall auch Rückschlüsse auf das zugrunde liegende Krankheitsbild des Beamten zugelassen haben.

Unabhängig hiervon erschien mir zudem die **„doppelte" Übermittlung** des Inhalts eines Gesundheitszeugnisses an den betroffenen Beamten – einmal durch die Übermittlung eines Abdrucks seitens des polizeiärztlichen Dienstes und einmal durch ein Schreiben des Polizeipräsidiums an den Beschäftigten, welches den Inhalt des Gesundheitszeugnisses lediglich wiederholt, – als **nicht erforderlich**. Vielmehr **genügt** es den gesetzlichen Vorgaben, wenn der polizeiärztliche Dienst der betroffenen Beamtin oder dem betroffenen Beamten einen Abdruck des an die Dienstvorgesetzte oder den Dienstvorgesetzten übermittelten Gesundheitszeugnisses zur Verfügung stellt. Art. 67 Abs. 3 Satz 2 BayBG bestimmt dazu:

„Der Arzt oder die Ärztin übermittelt dem Beamten oder der Beamtin oder, soweit dem ärztliche Gründe entgegenstehen, dem Vertreter oder der Vertreterin eine Ablichtung der auf Grund dieser Vorschrift an die Behörde erteilten Auskünfte."

9.3.3 Bayernweite Verfahrensumstellung

Das Polizeipräsidium hat meine Hinweise in dem der Eingabe zugrunde liegenden Fall aufgegriffen. Ich hatte jedoch Grund zu der Annahme, dass die dargestellte, datenschutzrechtlich bedenkliche Verfahrensweise im Zusammenhang mit der Beurteilung der Dienst- und Verwendungsfähigkeit von Beamtinnen und Beamten im Bereich der Personalverwaltung der gesamten Bayerischen Polizei durchaus verbreitet Anwendung findet. Daher habe ich meine diesbezüglichen Bedenken im Nachgang auch dem Bayerischen Staatsministerium des Innern, für Sport und Integration gegenüber geäußert und darum gebeten, bei allen zuständigen Stellen der Bayerischen Polizei auf die strikte Beachtung der engen Vorgaben des Bayerischen Beamtengesetzes hinzuwirken. Erfreulicherweise ist das Innenministerium dieser Bitte auch zeitnah und ohne weitere Diskussionen nachgekommen.

Insgesamt konnte ich somit anlässlich einer entsprechenden Eingabe dazu beitragen, das Bewusstsein der Personalverwaltung der Bayerischen Polizei für datenschutzrechtliche Vorgaben im besonders sensiblen Bereich der dienstlich veranlassten amtsärztlichen Untersuchungen weiter zu schärfen.

9.3.4 Fazit

Die Überprüfung der Dienstfähigkeit von Beamten oder Beamtinnen ist Sache der jeweiligen Dienstvorgesetzten. (Fach-)Vorgesetzte haben diesbezüglich keine Zuständigkeiten – der Inhalt eines Gesundheitszeugnisses geht diese in aller Regel somit auch „nichts an". Nur soweit sich aus dem Gesundheitszeugnis unmittelbare Folgerungen und Auswirkungen auf den Dienstbetrieb oder auf die Gestaltung des Arbeitsplatzes der Beamtin oder des Beamten ergeben, welche entsprechende Umsetzungs- oder Durchführungsmaßnahmen der Dienststellenleitung erfordern, dürfen (Fach-)Vorgesetzte ausnahmsweise vom Inhalt eines Gesundheitszeugnisses auszugsweise Kenntnis nehmen.

9.4 Führerscheinkontrollen für die Nutzung von Dienstkraftfahrzeugen

Bayerische öffentliche Stellen müssen als Halter von Kraftfahrzeugen sicherstellen, dass nur solche Personen dienstliche Fahrzeuge führen, die über die hierfür erforderliche Fahrerlaubnis verfügen. Die Erfüllung dieser – sogar strafbewehrten („Fahrenlassen ohne Fahrerlaubnis", § 21 Abs. 1 Nr. 2 Straßenverkehrsgesetz) – Pflicht erfordert es in der Regel, die Führerscheine derjenigen Beschäftigten zu kontrollieren, die Dienstkraftfahrzeuge nutzen. Vor diesem Hintergrund haben sich bayerische öffentliche Stellen mit der Frage an mich gewandt, wie diese Führerscheinkontrollen datenschutzgerecht auszugestalten sind. Oftmals war im Rahmen solcher Kontrollen beabsichtigt, Fotokopien der Führerscheine von Beschäftigten zu erstellen und zu den Akten zu nehmen. Ich habe zu diesem Fragenkreis die folgenden Hinweise gegeben:

9.4.1 Rechtsgrundlage

Ein Führerschein enthält **personenbezogene Daten** der Inhaberin oder des Inhabers im Sinn von Art. 4 Nr. 1 DSGVO. Bei einer Führerscheinkontrolle werden diese personenbezogenen Daten in Form einer **Erhebung** und **Speicherung** verarbeitet. Die Verarbeitung personenbezogener Daten von Beschäftigten durch den Dienstherrn ist in bereichsspezifischen Vorschriften (§ 50 Beamtenstatusgesetz, Art. 103 ff. Bayerisches Beamtengesetz – BayBG) geregelt. Diese Vorschriften sind grundsätzlich auch auf die nichtbeamteten Beschäftigten des bayerischen öffentlichen Dienstes, insbesondere die Tarifbeschäftigten, entsprechend anzuwenden (vgl. Art. 145 Abs. 2 BayBG).

Im Zusammenhang mit der Nutzung von Dienstkraftfahrzeugen kann der Dienstherr Führerscheinkontrollen bei seinen Beschäftigten datenschutzrechtlich grundsätzlich auf Art. 103 Satz 1 BayBG stützen. Diese Vorschrift erlaubt die Verarbeitung personenbezogener Daten unter anderem, soweit sie zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere zu Zwecken der Personalverwaltung oder Personalwirtschaft erforderlich ist. **Führerscheinkontrollen** durch den Dienstherrn zur Erfüllung seiner Halterpflichten können dabei als **Maßnahmen der Personalwirtschaft** angesehen werden:

Wie eingangs dargestellt, hat der Dienstherr als Halter von Kraftfahrzeugen durch zumutbare Maßnahmen sicherzustellen, dass nur Personen mit der hierfür erforderlichen Fahrerlaubnis dienstliche Fahrzeuge führen. Im Rahmen seiner Personalwirtschaft muss er somit insbesondere seine Personalplanung und den Personaleinsatz so ausgestalten, dass Beschäftigte ohne die erforderliche Fahrerlaubnis nicht für Tätigkeiten eingesetzt werden, welche die Führung eines (dienstlichen) Kraftfahrzeugs zwingend voraussetzen. Dies erfordert es in einem ersten Schritt, sich durch angemessene Führerscheinkontrollen ein Bild davon zu verschaffen, wer über eine erforderliche Fahrerlaubnis verfügt. Das Ergebnis dieser Prüfung ist zu dokumentieren. Ergibt dabei eine Kontrolle etwa, dass eine Beschäftigte oder ein Beschäftigter nicht oder nicht mehr im Besitz der erforderlichen Fahrerlaubnis ist, muss der Dienstherr dem organisatorisch Rechnung tragen (etwa indem er der oder dem Beschäftigten eine andere Tätigkeit überträgt, ihr oder ihm gegebenenfalls die Nutzung des Dienstkraftfahrzeuges untersagt). Je nach Konstellation können auch weitergehende dienst- oder arbeitsrechtliche Konsequenzen in Betracht kommen, etwa dann, wenn sich Beschäftigte der Einsichtnahme des Dienstherrn in ihre Führerscheine verweigern.

Unter Umständen können bestimmte **Schlüsselzahlen** auf dem Führerschein, die einen **Rückschluss auf körperliche Einschränkungen** der Inhaberin oder des Inhabers zulassen (vgl. Anlage 9 zu § 25 Abs. 3 Verordnung über die Zulassung von Personen zum Straßenverkehr), **Gesundheitsdaten** und damit personenbezogene Daten einer besonderen Kategorie im Sinn von Art. 9 Abs. 1 DSGVO darstellen. Deren Verarbeitung ist ebenfalls zulässig, soweit es die **Wahrnehmung der Rechte und Pflichten des Dienstherrn auf dem Gebiet des Dienst- und Arbeitsrechts** erfordert (Art. 103 Satz 1 Nr. 2 BayBG in Verbindung mit Art. 8 Abs. 1 Satz 1 Nr. 2, Abs. 2 BayDSG).

9.4.2 Erforderlichkeit und Grundsatz der Datenminimierung

Der zulässige Umfang der Datenverarbeitung wird allerdings maßgebend durch die **Erforderlichkeit** (vgl. Art. 103 Satz 1 Nr. 1 BayBG) sowie den Grundsatz der **Datenminimierung** (Art. 5 Abs. 1 Buchst. c DSGVO) mitbestimmt: Der Dienstherr darf personenbezogene Daten nur in dem für die Zweckerfüllung gebotenen Umfang verarbeiten. Er darf also nur die Angaben „aus" dem Führerschein erheben und speichern, die er für die Erfüllung seiner Halterpflichten benötigt.

Hiervon ausgehend ist es datenschutzrechtlich **zulässig**, wenn der **Dienstherr** von den betroffenen Beschäftigten (etwa unter Verwendung eines Formblatts) die **benötigten Angaben** zum Führerschein **einholt**, sich im Rahmen einer regelmäßigen Kontrolle den **Führerschein vorzeigen lässt** und dies entsprechend **dokumentiert**. Durch diese Verfahrensweise dürfte die Erfüllung der Halterpflichten des Dienstherrn hinreichend sichergestellt sein.

Eine Anfertigung von Fotokopien der Führerscheine, die mit der Erhebung und Speicherung nicht benötigter Angaben verbunden ist, sehe ich dagegen in aller Regel als nicht erforderlich und damit als datenschutzrechtlich unzulässig an.

9.4.3 Information der betroffenen Beschäftigten

Die betroffenen Beschäftigten sind zum Zeitpunkt der Erhebung ihrer personenbezogenen Daten, also mit Beginn der Führerscheinkontrollen, durch den Dienstherrn im Umfang von **Art. 13 Abs. 1 und 2 DSGVO** zu informieren. Von der Information kann abgesehen werden, soweit betroffene Beschäftigte bereits über diese Informationen verfügen. Das kommt insbesondere in Betracht, wenn Beschäftigte bereits zuvor, etwa im Rahmen ihrer Einstellung, über die Datenerhebung im Zusammenhang mit den späteren Führerscheinkontrollen informiert worden sind und dies auch dokumentiert ist. Auf die Orientierungshilfe „Informationspflichten"[27] weise ich hin.

[27] Bayerischer Landesbeauftragter für den Datenschutz, Informationspflichten des Verantwortlichen, Stand 11/2018, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Informationspflichten".

9.4.4 Zuständigkeit und Speicherdauer

Die Führerscheinkontrollen sollten durch eine zentrale Einheit durchgeführt werden. So wird sichergestellt, dass möglichst wenige Personen Zugriff auf diese personenbezogenen Daten haben. In Betracht kommt neben der **personalverwaltenden Stelle** insbesondere bei einem großen Fuhrpark (etwa eines städtischen Bauhofs oder einer Straßenmeisterei) auch die für dessen Management zuständige Stelle.

Bei der Speicherung der personenbezogenen Daten, die im Rahmen der Kontrollen angefallen sind, ist der Grundsatz der **Speicherbegrenzung** (Art. 5 Abs. 1 Buchst. e DSGVO) zu beachten: Danach dürfen personenbezogene Daten nur solange gespeichert werden, wie es für die Verarbeitungszwecke erforderlich ist; anschließend sind sie zu löschen. Dabei ist freilich zu berücksichtigen, dass der Dienstherr auch für bereits in der Vergangenheit liegende Zeiträume anhand der dokumentierten Kontrollen nachweisen können muss, dass er seinen Halterpflichten nachgekommen ist.

9.4.5 Fazit

Um seinen Pflichten als Kraftfahrzeughalter nachzukommen, darf ein Dienstherr Führerscheinkontrollen bei denjenigen Beschäftigten durchführen, die Dienstkraftfahrzeuge nutzen. Die Anfertigung von Fotokopien der Führerscheine ist dabei jedoch in aller Regel nicht erforderlich und somit datenschutzrechtlich auch nicht zulässig.

9.5 Der Personalrat – Verantwortlicher im Sinne des Datenschutzrechts?

Der nach Art. 12 Abs. 1 Bayerisches Personalvertretungsgesetz (BayPVG) zu bildende Personalrat verarbeitet im Rahmen seiner Aufgabenerfüllung Beschäftigtendaten. Schon unter Geltung des „alten" Datenschutzrechts ist die Frage diskutiert worden, ob hinsichtlich dieser Verarbeitungen der Personalrat selbst oder aber die öffentliche Stelle, bei der er gebildet ist, als verantwortlich im datenschutzrechtlichen Sinne anzusehen ist. Ich habe mich in diesem Zusammenhang für eine einheitliche Verantwortlichkeit der öffentlichen Stelle ausgesprochen, aber darauf hingewiesen, dass der besonderen Stellung des Personalrats Rechnung zu tragen ist (so etwa im Hinblick auf die Kontrollmöglichkeiten des behördlichen Datenschutzbeauftragten). Diese Auffassung stand im Einklang mit der bisherigen Rechtsprechung des Bundesarbeitsgerichts, welches den Betriebsrat auch datenschutzrechtlich als Teil des jeweiligen Unternehmens und somit als Teil dieser „speichernden Stelle" angesehen hatte.[28]

Mit Geltungsbeginn der Datenschutz-Grundverordnung ist die Diskussion um die datenschutzrechtliche Verantwortlichkeit des Personalrats wieder aufgelebt. Meine Position fasse ich nachstehend zusammen.

[28] Vgl. Bundesarbeitsgericht, Beschluss vom 11. November 1997, 1 ABR 21/97.

9.5.1 Die Rolle des „Verantwortlichen“

Die Verpflichtungen nach der Datenschutz-Grundverordnung treffen in erster Linie den Verantwortlichen. Verantwortlicher ist dabei nach Art. 4 Nr. 7 DSGVO grundsätzlich

„die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden“.

Die Datenschutz-Grundverordnung eröffnet dem mitgliedstaatlichen Gesetzgeber an dieser Stelle somit einen gewissen Gestaltungsspielraum: Unter den Voraussetzungen des Art. 4 Nr. 7 Halbsatz 2 DSGVO kann der mitgliedstaatliche Gesetzgeber den Verantwortlichen somit selbst gesetzlich bestimmen. Hierauf wird zurückzukommen sein.

9.5.2 Der Personalrat als „Verantwortlicher“?

Teilweise wird die Auffassung vertreten, dass der Personalrat nun selbst Verantwortlicher im Sinne der Datenschutz-Grundverordnung sei, da er alleine über die Zwecke und die Mittel der von ihm durchgeführten Verarbeitungen personenbezogener Daten entscheide.[29] Diese Auffassung hätte für Personalräte weitreichende datenschutzrechtliche Konsequenzen. So wären sie als Verantwortliche etwa verpflichtet, einen eigenen Datenschutzbeauftragten zu benennen; ihre Mitglieder wären zudem einem nicht unerheblichen Haftungsrisiko ausgesetzt.

Vorzugswürdig erscheint es, den Personalrat – wie bislang – als Teil der jeweiligen öffentlichen Stelle anzusehen. Diese ist somit auch für Datenverarbeitungen des Personalrats Verantwortlicher im Sinn der Datenschutz-Grundverordnung. Im Anwendungsbereich des Bayerischen Datenschutzgesetzes ergibt sich dies insbesondere aus Art. 3 Abs. 2 BayDSG. Mit dieser Regelung hat der bayerische Gesetzgeber von der Ermächtigung des Art. 4 Nr. 7 Halbsatz 2 DSGVO Gebrauch gemacht. Verantwortlicher für die Verarbeitung personenbezogener Daten ist demnach grundsätzlich die für die Verarbeitung zuständige öffentliche Stelle. Der Begriff der „öffentlichen Stelle“ wird insbesondere in Art. 1 Abs. 1, 2 und 4 BayDSG bestimmt – der Personalrat fällt gerade nicht darunter. Es wird somit grundsätzlich die Behörde oder sonstige öffentliche Stelle einheitlich als Verantwortlicher betrachtet, ohne dass eine weitergehende Untergliederung (etwa in einzelne Ämter oder Abteilungen) erfolgt.

Doch auch wenn man allein Art. 4 Nr. 7 Halbsatz 1 DSGVO in den Blick nimmt, ist der Personalrat nicht als Verantwortlicher anzusehen. Zwar ist der Begriff des Verantwortlichen grundsätzlich weit zu verstehen und mit dem Zusatz „oder andere Stelle“ in Art. 4 Nr. 7 Halbsatz 1 DSGVO auch bewusst offen gehalten. Allerdings steht die „andere Stelle“ in einer alternativen Aufzählung unter anderem mit einer

[29] So etwa für die Parallelproblematik bezüglich des Betriebsrats: Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, Tätigkeitsbericht Datenschutz 2018, S. 37 f.

juristischen Person, einer Behörde oder einer Einrichtung. Dies spricht dafür, dass auch der europäische Gesetzgeber die genannten Organisationsformen grundsätzlich einheitlich als Verantwortliche auffasst. Da der Personalrat aber keine eigene, nach außen hin verselbstständigte Stelle ist, sondern unselbstständiger Teil der jeweiligen Behörde oder sonstigen öffentlichen Stelle, ist er – jedenfalls soweit er seine gesetzlichen Aufgaben wahrnimmt – datenschutzrechtlich auch nicht Verantwortlicher nach Art. 4 Nr. 7 DSGVO.

Für diese Auffassung spricht ferner, dass die Datenschutz-Grundverordnung die Begriffe „Behörde" und „öffentliche Stelle" zwar wiederholt gebraucht, aber selbst nicht definiert. Damit erkennt sie die Organisationshoheit des einzelnen Mitgliedstaates hinsichtlich Aufbau und Struktur seiner Verwaltung an. Würde man dies anders sehen, drohte im Ergebnis eine „Zersplitterung" der datenschutzrechtlichen Verantwortlichkeit im Bereich der öffentlichen Verwaltung: Neben dem Personalrat kämen nämlich auch weitere Stellen einer Behörde als eigenständige Verantwortliche in Betracht, sofern diese Stellen besonderen internen Verschwiegenheitspflichten unterliegen und hinsichtlich der Verarbeitung personenbezogener Daten eine gewisse Unabhängigkeit aufweisen. Dies beträfe etwa die Schwerbehindertenvertretung und nicht zuletzt auch den behördlichen Datenschutzbeauftragten selbst, der im Rahmen seiner Tätigkeit ebenfalls weisungsfrei (vgl. Art. 38 Abs. 3 Satz 1 DSGVO) personenbezogene Daten verarbeitet.

Aufgaben, Rechte und Pflichten der Personalräte bayerischer öffentlicher Stellen sind im Bayerischen Personalvertretungsgesetz geregelt. Es wäre dem bayerischen Gesetzgeber unbenommen geblieben, den Personalrat auf Grundlage von Art. 4 Nr. 7 Halbsatz 2 DSGVO in diesem Zusammenhang als datenschutzrechtlich Verantwortlichen zu bestimmen, wie dies andere Landespersonalvertretungsgesetze vereinzelt vorsehen. Eine solche Regelung hat der bayerische Gesetzgeber jedoch nicht getroffen.

Es bleibt daher bei dem Grundsatz, dass eine bayerische Behörde oder sonstige öffentliche Stelle einheitlich als Verantwortlicher anzusehen ist – auch für die Verarbeitungen personenbezogener Daten durch ihren Personalrat.

9.5.3 Datenschutz innerhalb des Personalrats

Die jeweilige öffentliche Stelle muss als Verantwortlicher somit grundsätzlich sicherstellen, dass auch ihr Personalrat die einschlägigen datenschutzrechtlichen Vorgaben einhält. Hierbei ist allerdings der besonderen Stellung des Personalrats Rechnung zu tragen, insbesondere im Hinblick auf die Schweigepflicht seiner Mitglieder nach Art. 10 BayPVG. Insoweit hat die Dienststellenleitung gegenüber dem Personalrat nur begrenzte Einflussmöglichkeiten.

In der praktischen Umsetzung folgt für bayerische öffentliche Stellen hieraus insbesondere:

9.5.3.1 Der Personalrat und der behördliche Datenschutzbeauftragte

Dem behördlichen Datenschutzbeauftragten obliegen unter anderem Beratungs- und Überwachungsaufgaben gegenüber dem Verantwortlichen sowie dessen Beschäftigten, die Datenverarbeitungen durchführen (vgl. Art. 39 Abs. 1 Buchst. a und b DSGVO). Diese Aufgaben bestehen somit auch gegenüber dem Personal-

rat als Teil des Verantwortlichen. Die noch zur alten Rechtslage ergangene Rechtsprechung des Bundesarbeitsgerichts, wonach im Bereich des Betriebsverfassungsgesetzes ein Kontrollrecht des betrieblichen Datenschutzbeauftragten gegenüber dem Betriebsrat nicht besteht,[30] dürfte unter Zugrundelegung der neuen Rechtslage nicht mehr aufrechtzuerhalten sein. Dabei ist auch zu berücksichtigen, dass der behördliche Datenschutzbeauftragte gegenüber dem Verantwortlichen weisungsfrei handelt (Art. 38 Abs. 3 Satz 1 DSGVO).

Angesichts der Schweigepflicht des Personalrats sollten sowohl dieser als auch der behördliche Datenschutzbeauftragte allerdings darauf achten, dass letzterer seiner Überwachungs- und Beratungsaufgabe möglichst ohne die Nutzung personenbezogener Beschäftigtendaten nachkommt, etwa indem der Personalrat Fragestellungen in abstrakter Form – also ohne konkreten Einzelfallbezug – an den behördlichen Datenschutzbeauftragten richtet. Umgekehrt sollte der behördliche Datenschutzbeauftragte die Einhaltung technischer und organisatorischer Datenschutzanforderungen durch den Personalrat nach Möglichkeit ohne Kenntnisnahme personenbezogener Beschäftigtendaten überprüfen. Soweit der behördliche Datenschutzbeauftrage Kenntnis erlangt von Umständen, die der Schweigepflicht nach Art. 10 BayPVG unterliegen, hat er gegenüber der Dienststelle ebenfalls Stillschweigen zu bewahren (vgl. Art. 38 Abs. 5 DSGVO in Verbindung mit Art. 12 Abs. 2 BayDSG).

9.5.3.2 Technische und organisatorische Maßnahmen

Der Personalrat hat innerhalb seines Zuständigkeitsbereiches eigenverantwortlich geeignete technische und organisatorische Maßnahmen im Sinn der Art. 24 und 32 DSGVO umzusetzen. Soweit erforderlich, sollte er diesbezüglich die Beratung durch den behördlichen Datenschutzbeauftragten in Anspruch nehmen. Die Dienststelle hat den Personalrat insoweit mit den erforderlichen Sachmitteln auszustatten (Art. 44 BayPVG).

9.5.3.3 Verzeichnis der Verarbeitungstätigkeiten

Da der Personalrat selbst nicht Verantwortlicher ist, besteht für ihn keine Pflicht, ein eigenes Verzeichnis der Verarbeitungstätigkeiten (im Folgenden: Verarbeitungsverzeichnis) gemäß Art. 30 DSGVO zu führen. Allerdings muss das Verarbeitungsverzeichnis der jeweiligen öffentlichen Stelle auch die Verarbeitungstätigkeiten des Personalrats enthalten. Vor dem Hintergrund der Schweigepflicht nach Art. 10 BayPVG ist hierbei in besonderem Maße auf eine hinreichend abstrakte Beschreibung der jeweiligen Verarbeitungstätigkeit zu achten. So könnte der Zweck der Verarbeitung personenbezogener Daten durch den Personalrat etwa mit „Wahrnehmung der gesetzlich vorgesehenen Aufgaben der Personalvertretung“ umschrieben werden.

9.5.3.4 Informationspflichten und Auskunftsrecht

Informationspflichten des Personalrats nach Art. 13, 14 DSGVO bestehen nur, soweit noch keine entsprechende Information der Beschäftigten durch die Dienststelle erfolgt ist. In diesem Zusammenhang bietet es sich insbesondere an, dass die Dienststelle bei Neueinstellungen im Rahmen ihrer Informationspflicht nach Art. 13 DSGVO auch darüber informiert, in welchem Umfang die erhobenen Daten durch den Personalrat verarbeitet werden. Eine gesonderte Information der neu

[30] Vgl. Bundesarbeitsgericht, Beschluss vom 11. November 1997, 1 ABR 21/97.

eingestellten Beschäftigten unmittelbar durch den Personalrat selbst wird dann nur noch im Einzelfall erforderlich sein.

Verlangen Beschäftigte Auskunft nach Art. 15 DSGVO, ist angesichts der Schweigepflicht des Personalrats nach Art. 10 BayPVG zu unterscheiden:

— Beschränkt sich das Auskunftsersuchen auf Datenverarbeitungen durch den Personalrat, kann dieser selbstständig das entsprechende Ersuchen bearbeiten.

— Beschäftigte können ihr Auskunftsersuchen aber auch auf sämtliche Daten beziehen, welche die Dienststelle von ihnen verarbeitet. Hier sollte die Dienststelle zunächst im Wege eines konstruktiven Dialogs mit den jeweiligen Beschäftigten ermitteln, ob das Auskunftsersuchen tatsächlich auch Datenverarbeitungen durch den Personalrat umfasst. Ist dies der Fall, sollte die Dienststelle die jeweiligen Beschäftigten (nur) insoweit unmittelbar an den Personalrat verweisen. Dieser kommt dem Ersuchen dann selbstständig nach.

9.5.3.5 Regelungen zum Datenschutz im Zusammenhang mit der Personalratsarbeit

Es ist dringend zu empfehlen, dass sich Personalrat und Dienststellenleitung hinsichtlich des Vorgehens bezüglich dieser und weiterer Themen (etwa bezüglich einer Datenschutzverletzung im Bereich des Personalrats) im Wege der vertrauensvollen Zusammenarbeit (Art. 2 Abs. 1 BayPVG) gemeinsam verständigen. Entsprechende Regelungen sollten getroffen und schriftlich fixiert werden. Unabhängig hiervon sollte der Personalrat natürlich auch interne Regelungen zum Datenschutz treffen, etwa eine Aussonderungsroutine festlegen.

9.5.4 Fazit

Die besseren Argumente sprechen dafür, den Personalrat einer bayerischen öffentlichen Stelle nicht als eigenständigen Verantwortlichen im Sinn von Art. 4 Nr. 7 DSGVO anzusehen. Vielmehr bleibt – wie bislang – die jeweilige bayerische öffentliche Stelle auch für die Verarbeitung personenbezogener Daten durch den Personalrat verantwortlich. Bei der Umsetzung der datenschutzrechtlichen Pflichten des Verantwortlichen ist allerdings der besonderen Stellung des Personalrats hinreichend Rechnung zu tragen.

Die Diskussion zu dieser Thematik ist noch im Fluss. Es ist zu erwarten, dass zu gegebener Zeit auch Rechtsprechung hierzu ergehen wird. Bayerischen öffentlichen Stellen und ihren Personalräten empfehle ich daher, die weitere Entwicklung aufmerksam zu verfolgen.

9.6 Personalratsmitglied als behördlicher Datenschutzbeauftragter?

Die bayerischen öffentlichen Stellen trifft nicht nur gemäß Art. 37 Abs. 1 Buchst. a DSGVO, Art. 12 BayDSG die Pflicht, einen behördlichen Datenschutzbeauftragten zu benennen. Nach Maßgabe von Art. 12 Abs. 1 Bayerisches Personalvertretungsgesetz (BayPVG) sind bei ihnen auch Personalräte zu bilden. Gerade in kleineren Dienststellen führt dies nicht selten dazu, dass auf Grund der geringen Zahl von

Beschäftigten die Übernahme beider Funktionen durch ein und dieselbe Person als naheliegend erscheint oder sogar gewünscht wird. Bedenkt man, dass der Personalrat regelmäßig in Einzelangelegenheiten der Beschäftigten sowie in Einstellungsverfahren beteiligt wird und das Gremium dabei aus datenschutzrechtlicher Sicht Personaldaten verarbeitet, stellt sich die Frage, ob ein behördlicher Datenschutzbeauftragter zugleich Personalratsmitglied sein kann. Diese Frage ist differenziert nach der Stellung der betreffenden Person im Personalrat zu beantworten.

Hinweis: Dieser Beitrag bezieht nicht ausdrücklich zu der Frage Stellung, ob der Personalrat als von der öffentlichen Stelle gesonderter Verantwortlicher anzusehen ist (siehe dazu den Beitrag Nr. 9.5). Ihm liegt jedoch die Annahme zugrunde, dass der Personalrat datenschutzrechtlich ein besonderer Teil der öffentlichen Stelle ist, bei der er gebildet ist.

9.6.1 Vereinbarkeit der Funktionen „behördlicher Datenschutzbeauftragter“ und „einfaches Personalratsmitglied“

Aus Sicht des Datenschutzrechts ist die Vereinbarkeit der Funktionen „behördlicher Datenschutzbeauftragter“ und „einfaches Personalratsmitglied“ anhand von Art. 38 Abs. 6 DSGVO zu würdigen. Nach dieser Vorschrift kann der Datenschutzbeauftragte andere Aufgaben und Pflichten wahrnehmen; der Verantwortliche stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

Im Verhältnis der Arbeit des behördlichen Datenschutzbeauftragten auf der einen Seite zu der Arbeit des Personalrats – an der das einzelne Personalratsmitglied teilnimmt – auf der anderen Seite können Interessendivergenzen auftreten:

— Der behördliche Datenschutzbeauftragte wirkt darauf hin, dass der Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) beachtet und die den Umgang mit Personalaktendaten prägende doppelte Zugangsbeschränkung (Art. 103 Bayerisches Beamtengesetz) möglichst optimal umgesetzt wird. Der Personalrat hat demgegenüber ein Interesse daran, seine Beteiligungsrechte effektiv wahrzunehmen. Er wird daher eine Informationsbasis anstreben, die ihm ein zielführendes Gespräch mit der Dienststellenleitung ermöglicht, und in diesem Rahmen unter Umständen geneigt sein, möglichst detaillierte Informationen (auch) über einzelne Beschäftigte oder Stellenbewerber zu erlangen und über einen gewissen Zeitraum vorzuhalten.

  So kann sich für das einzelne Personalratsmitglied ein Rollenkonflikt ergeben: Drängt diese Funktion eher dazu, an der Informationsbeschaffung durch das Gremium mitzuwirken, legt die Aufgabe des behördlichen Datenschutzbeauftragten nahe, entsprechende Datenflüsse auf das personalvertretungsrechtlich unabdingbare Maß zu beschränken.

— Im Übrigen ist der Personalrat auch an der Gestaltung von Dienstvereinbarungen beteiligt, deren Gegenstand der Umgang mit Beschäftigtendaten ist. Dies gilt etwa für Vereinbarungen über die Arbeitszeiterfassung, die Nutzung von Internetzugängen oder die Verwendung von elektronischen Schließsystemen. Hier stellt zwar die Mitgliedschaft des behördlichen Datenschutzbeauftragten im Personalrat sicher, dass Datenschutzbelange in

die Verhandlungen einfließen. Allerdings besteht auch das Risiko, dass sich die in das Gremium gewählte Person eher mit dessen Interessenlage identifiziert und die ihr von der Datenschutz-Grundverordnung zugewiesene Rolle eines „neutralen" Beraters zwischen dem Verantwortlichen und seinen Beschäftigten (vgl. Art. 39 Abs. 1 Buchst. a DSGVO) verlässt.

Bei einer Gesamtbetrachtung stehen die Funktionen „behördlicher Datenschutzbeauftragter" und „einfaches Personalratsmitglied" daher in einer Spannungslage. Das Personalratsmitglied ist aber regelmäßig (vgl. Art. 16 Abs. 1 BayPVG) in ein Gremium eingebunden und kann deshalb nicht allein Entscheidungen treffen. Die Wählbarkeit zum Personalrat ist für behördliche Datenschutzbeauftragte im Übrigen nicht ausgeschlossen (vgl. Art. 14 Abs. 3, 4 BayPVG).

Aus datenschutzrechtlicher Sicht sollten Beschäftigte eine Verbindung der Funktionen „behördlicher Datenschutzbeauftragter" und „einfaches Personalratsmitglied" im eigenen Interesse möglichst vermeiden. Eine Unvereinbarkeit im Sinne von Art. 38 Abs. 6 Satz 2 DSGVO liegt aber nicht vor.

9.6.2 Vereinbarkeit der Funktionen „behördlicher Datenschutzbeauftragter" und „Personalratsvorsitzender"

Einem Personalratsvorsitzenden, der zugleich die Funktion des behördlichen Datenschutzbeauftragten ausüben soll, wird das für einfache Personalratsmitglieder skizzierte Spannungsverhältnis (noch) häufiger und intensiver erfahrbar. Der Personalratsvorsitzende führt die laufenden Geschäfte und vertritt den Personalrat im Rahmen der von diesem gefassten Beschlüsse (Art. 32 Abs. 3 Satz 1 BayPVG). Er ist insbesondere „ständiger" Gesprächs- und Verhandlungspartner für die Dienststellenleitung und die personalverwaltende Stelle. Diese hervorgehobene Position führt – insbesondere außerhalb der Sitzungen des Personalrats – zu einem regelmäßigen Auftreten von Interessenkonflikten, wenn sich der Personalratsvorsitzende jeweils entscheiden muss, welcher seiner beiden Rollen er aktuell den Vorrang geben möchte.

Aus datenschutzrechtlicher Sicht sind die Funktionen „behördlicher Datenschutzbeauftragter" und „Personalratsvorsitzender" daher regelmäßig nicht vereinbar; ihre Verbindung in einer Person steht mit der Vorgabe des Art. 38 Abs. 6 Satz 2 DSGVO nicht in Einklang.

Bayerische öffentliche Stellen sollten daher Personalratsvorsitzende grundsätzlich nicht als behördliche Datenschutzbeauftragte benennen und behördliche Datenschutzbeauftragte, die zu Vorsitzenden des Personalrats gewählt werden, von der Funktion des behördlichen Datenschutzbeauftragten entbinden. Ein Abweichen von dieser Regel erscheint im Ausnahmefall als hinnehmbar, wenn es einer öffentlichen Stelle mit nur wenigen Bediensteten nicht möglich ist, die beiden Funktionen durch verschiedene Personen zu besetzen.

9.6.3 Umgang mit Interessenkonflikten im Einzelfall

Ist ein behördlicher Datenschutzbeauftragter Mitglied oder – ausnahmsweise – Vorsitzender des Personalrats, können Situationen eintreten, in welchen die betreffende Person nicht beiden Rollen gerecht werden kann. Das ist insbesondere

dann der Fall, wenn sie in ihrer Rolle als behördlicher Datenschutzbeauftragter einen Datenschutzverstoß bei der Personalratsarbeit feststellt, oder wenn es allgemein darum geht, den von Art. 39 Abs. 1 Buchst. b DSGVO angeordneten Überwachungsauftrag gerade beim Personalrat wahrzunehmen. Für Situationen dieser Art muss der Verantwortliche im Rahmen von Art. 38 Abs. 6 Satz 2 DSGVO gewährleisten, dass anstelle eines behördlichen Datenschutzbeauftragten, der Mitglied des Personalrats ist, stets eine effektive Vertretung handeln kann.

9.6.4 Fazit

Kandidieren behördliche Datenschutzbeauftragte für den Personalrat bei einer bayerischen öffentlichen Stelle oder sollen Mitglieder des Personalrats als behördliche Datenschutzbeauftragte benannt werden, sollte die öffentliche Stelle als Verantwortlicher kritisch überprüfen, ob es dadurch zu einer Unvereinbarkeit zwischen den beiden Funktionen kommen kann. Die Freiheit eines jeden Beschäftigten, sich um ein Personalratsmandat zu bewerben oder ein solches Mandat auszuüben, sollte so wenig wie möglich beeinträchtigt werden. Allerdings muss die öffentliche Stelle sicherstellen, dass ihr ein grundsätzlich nicht in der Aufgabenwahrnehmung eingeschränkter (stellvertretender) behördlicher Datenschutzbeauftragter zur Verfügung steht.

9.7 Beschäftigtenfotos für Marketingmaßnahmen bayerischer öffentlicher Stellen

Eine bayerische öffentliche Stelle wollte mit Fotos ihrer Beschäftigten „Arbeitgebermarketing“ betreiben. Die Bilder sollten im Rahmen des Internetauftritts, in Stellenanzeigen und in Imagebroschüren verwendet werden. Ziel war die Entwicklung eines wiedererkennbaren Markenauftritts (corporate identity).

9.7.1 Einwilligung als Rechtsgrundlage für die Verwendung der Bilder

Die öffentliche Stelle ging davon aus, dass die Verwendung von Abbildungen ihrer Beschäftigten nur mit deren Einwilligung zulässig ist, war aber unsicher, nach welchen Rechtsvorschriften sich die Einwilligung richtet. Aus ihrer Sicht kam neben dem allgemeinen Datenschutzrecht auch das Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (im Folgenden: Kunsturhebergesetz, KUG) in Betracht. Beide Regelungen unterscheiden sich hinsichtlich der Voraussetzungen der Einwilligung und der Folgen ihres Widerrufs.

Anders als die Datenschutz-Grundverordnung (vgl. Art. 13 f. DSGVO) kennt das Kunsturhebergesetz keine ausdrücklichen Belehrungspflichten. Von besonderer Bedeutung ist zudem, dass das Kunsturhebergesetz selbst keinen Widerruf der Einwilligung vorsieht. Die Einwilligung nach dem Kunsturhebergesetz kann deshalb nur sehr eingeschränkt widerrufen werden. Folglich muss ein Widerrufsrecht regelmäßig ausdrücklich vereinbart werden. Wäre hier also das Kunsturhebergesetz maßgeblich, könnte die öffentliche Stelle die Bilder ihrer Beschäftigten grundsätzlich auch dann weiterverwenden, wenn diese – etwa anlässlich der Beendigung ihres Beschäftigungsverhältnisses – ihre Einwilligung widerrufen. Nach allgemeinem Datenschutzrecht ist die Einwilligung dagegen frei widerruflich (vgl. Art. 7 Abs. 3 DSGVO).

Vor diesem Hintergrund wollte die öffentliche Stelle von mir wissen, ob sie die Beschäftigten hinsichtlich ihrer Datenschutzrechte gemäß Art. 13 DSGVO informieren muss, und was gilt, wenn ein Beschäftigter zunächst in die Verwendung seiner Fotos einwilligt, diese Einwilligung später aber widerruft. Entscheidend ist damit das in der Fachwelt derzeit viel diskutierte Verhältnis von Kunsturhebergesetz und allgemeinem Datenschutzrecht.[31]

Der vorliegende Sachverhalt zeichnet sich allerdings durch zwei Besonderheiten aus. Zum einen ist eine öffentliche Stelle beteiligt und zum anderen spielt das Geschehen im Rahmen eines Beschäftigungsverhältnisses. Beide Bereiche unterliegen zahlreichen Sonderregeln. Die nachfolgenden Ausführungen lassen sich daher nicht ohne weiteres auf andere Gestaltungen übertragen.

9.7.1.1 Einwilligung nach der Datenschutz-Grundverordnung

Nach allgemeinem Datenschutzrecht gilt Folgendes: Die Veröffentlichung (und gegebenenfalls vorherige Anfertigung) von Beschäftigtenbildern ist eine Datenverarbeitung im Sinne der Datenschutz-Grundverordnung (siehe Art. 4 Nr. 2 DSGVO). Sie muss daher eine der in Art. 6 Abs. 1 DSGVO genannten Rechtsgrundlagen erfüllen. Art. 6 Abs. 1 Satz 1 UAbs. 1 Buchst. a DSGVO lautet:

Art. 6 DSGVO
Rechtmäßigkeit der Verarbeitung
(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
[…]

Aus Art. 7 Abs. 4 DSGVO ergibt sich ergänzend, dass die datenschutzrechtliche Einwilligung freiwillig erfolgen muss. Wegen des Machtungleichgewichts zwischen Dienstherrn/Arbeitgeber auf der einen Seite und Beschäftigten auf der anderen Seite ist die Freiwilligkeit der Einwilligung sorgfältig zu prüfen (vgl. Erwägungsgründe 32 und 43 DSGVO). Ergibt eine Betrachtung im Einzelfall, dass die freie Willensbildung einer oder eines Beschäftigten nicht durch ein Machtungleichgewicht beeinträchtigt ist, kann die Einwilligung in einem Dienst- oder Arbeitsverhältnis als Rechtsgrundlage einer Verarbeitung in Betracht kommen. Dies gilt auch für die Verarbeitung personenbezogener Daten zu Marketingzwecken, die der Dienstherr/Arbeitgeber verfolgt.

Wenn vorliegend also das allgemeine Datenschutzrecht maßgeblich ist, muss die öffentliche Stelle die betroffene Person gemäß Art. 13 DSGVO informieren; eine Einwilligung von Beschäftigten in die Verwendung der Fotos ist frei widerruflich.

Bis zum Zeitpunkt eines Widerrufs von der Einwilligung umfasste Verarbeitungen bleiben rechtmäßig (vgl. Art. 7 Abs. 3 Satz 2 DSGVO). Spätere Verwendungen

[31] Vor Geltung der Datenschutz-Grundverordnung war anerkannt, dass sich die Verwendung von Abbildungen in erster Linie nach den §§ 22, 23 KUG richtet, siehe etwa Bundesarbeitsgericht, Urteil vom 11. Dezember 2014, 8 AZR 1010/13, BeckRS 2015, 68087, Rn. 8 ff. für den privaten Bereich.

könnten dagegen nicht mehr im Sinne von Art. 6 Abs. 1 DSGVO auf die Einwilligung gestützt werden.

9.7.1.2 Einwilligung nach dem Kunsturhebergesetz

Fragen der Einwilligung im Zusammenhang mit der Verbreitung – nicht dem Anfertigen – von Bildern sind darüber hinaus auch in §§ 22, 23 KUG angesprochen. Die insoweit maßgebliche Regelung lautet:

§ 22 KUG
Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Die Einwilligung gilt im Zweifel als erteilt, wenn der Abgebildete dafür, daß er sich abbilden ließ, eine Entlohnung erhielt. […]

Da das Kunsturhebergesetz auf die Einwilligung in die Verbreitung von Bildnissen abstellt, dient es ebenfalls dem Schutz personenbezogener Daten der abgebildeten Person. Vor Geltung der Datenschutz-Grundverordnung war ein Vorrang der §§ 22, 23 KUG vor dem allgemeinen Datenschutzrecht anerkannt. Heute würde dies allerdings bedeuten, dass das in Art. 7 Abs. 3 DSGVO geregelte Widerrufsrecht eingeschränkt würde. Dieses Ergebnis widerspräche grundsätzlich dem Gedanken, dass Verordnungen der Europäischen Union in allen ihren Teilen verbindlich sind und in jedem Mitgliedstaat unmittelbar gelten (vgl. Art. 288 Abs. 2 Vertrag über die Arbeitsweise der Europäischen Union).

9.7.1.3 Verhältnis von Datenschutz-Grundverordnung und Kunsturhebergesetz

Vor diesem Hintergrund musste ich über das Verhältnis der Datenschutz-Grundverordnung zum Kunsturhebergesetz entscheiden. Ausgangspunkt ist der „Vorrang des Europarechts". Vorschriften der Europäischen Union setzen sich gegen widersprechende Regelungen der Mitgliedstaaten grundsätzlich durch. Deshalb gilt: Soweit das Kunsturhebergesetz der Datenschutz-Grundverordnung widerspricht, hat die Datenschutz-Grundverordnung Vorrang. Allerdings ist fraglich, ob sich beide Regeln tatsächlich widersprechen.

Die Frage nach dem Verhältnis von Datenschutz-Grundverordnung und Kunsturhebergesetz ist nicht ganz einfach zu beantworten. Hintergrund ist, dass die Datenschutz-Grundverordnung Konflikte zwischen den Datenschutzrechten der betroffenen Person und bestimmten gegenläufigen, ebenfalls schutzwürdigen Interessen anderer Personen anerkennt und dem Datenschutz nicht von vornherein einen Vorrang einräumt. Vielmehr überlässt sie es den Mitgliedstaaten, die kollidierenden Interessen angemessen auszugleichen. Unterschiedliche Regelungen bedeuten daher nicht notwendig einen problematischen Widerspruch, sondern können von einer entsprechenden Öffnungsklausel im europäischen Recht gedeckt sein. Art. 85 DSGVO bestimmt insofern:

Art. 85 DSGVO
Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit
(1) Die Mitgliedstaaten bringen durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten gemäß dieser Verordnung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken, in Einklang.

(2) Für die Verarbeitung, die zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt, sehen die Mitglied-staaten Abweichungen oder Ausnahmen von Kapitel II (Grundsätze), Kapitel III (Rechte der betroffenen Person) […] vor, wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungs-äußerung und der Informationsfreiheit in Einklang zu bringen.
[…]

Da die Regelungen über die Einwilligung (Art. 7 DSGVO) und die Informationspflichten (Art. 13 f. DSGVO) in den Kapiteln II und III enthalten sind, kann diese Vorschrift dazu führen, dass das Datenschutzrecht hinter journalistischen, künstlerischen oder literarischen Interessen oder der Meinungs- und Informationsfreiheit zurückstehen muss.

Es liegt wohl nicht ganz fern, das Kunsturhebergesetz als Regelung im Sinne des Art. 85 Abs. 1 DSGVO anzusehen, die dem Ausgleich gegenläufiger Interessen dient. Das Gesetz steht – wie sich unmittelbar aus seinem Namen ergibt – in engem Zusammenhang mit der Kunstfreiheit; aber auch für die weiter angesprochenen literarischen, journalistischen und wissenschaftlichen Freiheiten, die Meinungsäußerungs- und Informationsfreiheit hat es Bedeutung. Auf dieser Grundlage wäre es dann kein großer Schritt mehr, das Kunsturhebergesetz bei der Frage des Umgangs mit Abbildungen von Personen als vorrangig gegenüber dem allgemeinen Datenschutzrecht anzusehen.

9.7.1.4 Hier: Vorrang des allgemeinen Datenschutzrechts

Gleichwohl habe ich gegenüber der öffentlichen Stelle die Auffassung vertreten, dass die geplanten Marketingmaßnahmen und der Widerruf von Einwilligungen nach dem allgemeinen Datenschutzrecht zu beurteilen sind. Unabhängig von der Frage, ob Arbeitgebermarketing überhaupt als Betätigung der Meinungsfreiheit einschließlich der Verarbeitung zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken angesehen werden könnte, kann sich die öffentliche Stelle nach meiner Auffassung schon deshalb nicht auf das Kunsturhebergesetz berufen, weil Art. 85 DSGVO Ausnahmen vom allgemeinen Datenschutzrecht nur zulässt, soweit dies dem Ausgleich der Persönlichkeitsrechte der betroffenen Person mit den genannten Grundrechten anderer Personen dient.

Ein solcher Ausgleich kann hier aber von vornherein nicht hergestellt werden. Öffentliche Stellen können sich auf Grundrechte grundsätzlich nicht berufen. Zwar gelten die Grundrechte gemäß Art. 19 Abs. 3 Grundgesetz auch für inländische juristische Personen, soweit sie ihrem Wesen nach auf diese anwendbar sind. Von bestimmten Ausnahmen, insbesondere für Universitäten und Rundfunkanstalten, abgesehen, gilt das jedoch nicht für juristische Personen des öffentlichen Rechts. Grundrechte sollen Personen vor hoheitlichen Eingriffen schützen. Sie dienen nicht dazu, Rechte und Befugnisse öffentlicher Stellen auszuweiten. Öffentliche Stellen sind deshalb gerade nicht grundrechtsberechtigt, sondern – im Gegenteil – grundrechtsverpflichtet.

Bayerische öffentliche Stellen können einer betroffenen Person daher regelmäßig nicht die in Art. 85 DSGVO genannten Positionen entgegenhalten. Ihre Maßnahmen im Rahmen der Öffentlichkeitsarbeit bewerte ich deshalb im Ergebnis nicht als datenschutzrechtlich im Sinne von Art. 85 DSGVO privilegierte Grundrechtsausübung, sondern als bloßes öffentliches Informationshandeln.

Weil es in der vorliegenden Konstellation somit nicht um den Ausgleich kollidierender Grundrechte geht, ermöglicht Art. 85 DSGVO von vornherein nicht die Anwendung des Kunsturhebergesetzes zugunsten der öffentlichen Stelle. Die Fragen der öffentlichen Stelle sind vielmehr auf der Grundlage des allgemeinen Datenschutzrechts zu beantworten.

9.7.1.5 Folge: Freie Widerruflichkeit der Einwilligung

Art. 7 Abs. 3 DSGVO erklärt die datenschutzrechtliche Einwilligung für jederzeit widerruflich. Mitunter werden allerdings „die Wertungen der §§ 22, 23 KUG" einschließlich der eingeschränkten Widerruflichkeit der Einwilligung abgebildeter Personen auch dann berücksichtigt, wenn das Kunsturhebergesetz nicht unmittelbar anwendbar ist.

Dieser Gedanke mag in anderen Konstellationen, in denen das Kunsturhebergesetz nicht unmittelbar anwendbar ist, seine Rechtfertigung haben. Im vorliegenden Zusammenhang stehen einer Übertragung von Wertungen des Kunsturhebergesetzes, mit der die Nutzungsrechte der öffentlichen Stelle an den Bildern der Beschäftigten ausgeweitet würden, besondere Vorgaben des Beschäftigtendatenschutzes entgegen. Diese ergeben sich aus § 50 Beamtenstatusgesetz und Art. 103 ff. Bayerisches Beamtengesetz (BayBG), die gemäß Art. 145 Abs. 2 BayBG im Grundsatz auch für die nicht verbeamteten Beschäftigten bayerischer öffentlicher Stellen entsprechend gelten.

Art. 103 BayBG
Verarbeitung personenbezogener Daten
[1]Der Dienstherr darf personenbezogene Daten über Bewerber und Bewerberinnen sowie aktive und ehemalige Beamte und Beamtinnen verarbeiten, soweit dies
1. zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere zu Zwecken der Personalverwaltung oder Personalwirtschaft erforderlich ist,
2. zusätzlich bei der Verarbeitung besonderer Kategorien personenbezogener Daten Art. 8 Abs. 1 Nr. 2, 3 und 5 sowie Abs. 2 des Bayerischen Datenschutzgesetzes (BayDSG) erlaubt
und nachfolgend nichts anderes bestimmt ist. [2]Die Verarbeitung darf nur durch Beschäftigte erfolgen, die vom Dienstherrn mit der Bearbeitung von Personal-angelegenheiten betraut sind. [3]Unbeschadet der Sätze 1 und 2 dürfen Daten nach Satz 1 auch zu Zwecken der Rechnungsprüfung verarbeitet werden.

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

Zu den in Art. 103 Satz 1 BayBG genannten Zwecken ist es für eine öffentliche Stelle nicht, wie dort vorausgesetzt, „erforderlich", mit Bildern eigener Beschäftigter zu werben, insbesondere mit einer Internet-Veröffentlichung weltweite Öffentlichkeit herzustellen. Angesichts der klaren gesetzlichen Vorgaben muss vielmehr

gelten, dass eine Verarbeitung personenbezogener Daten im Beschäftigungskontext unzulässig ist, wenn die ausdrücklichen gesetzlichen Voraussetzungen nicht erfüllt sind.

9.7.1.6 Einwilligung keine dauerhaft verlässliche Rechtsgrundlage

Nach alledem kann sich eine bayerische öffentliche Stelle, sofern sie Marketingmaßnahmen der hier besprochenen Art ergreifen möchte, nicht verlässlich auf Einwilligungen ihrer Mitarbeiterinnen und Mitarbeiter stützen. Widerruft die betroffene Person ihre Einwilligung, dürfen die Fotos deshalb nur noch verwendet werden, wenn dafür eine andere Rechtsgrundlage erfüllt ist (vgl. Art. 17 Abs. 1 Buchst. b DSGVO).

9.7.2 Gesondertes Entgelt als Indiz für einen wirksamen Vertrag

Die öffentliche Stelle hatte dieses Ergebnis offenbar als möglich vorgesehen und beabsichtigt, neben der datenschutzrechtlichen Einwilligung mit den abgebildeten Beschäftigten auch Verträge über die Nutzung der Bilder abzuschließen. Datenschutzrechtlich ist damit Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO angesprochen. Diese Vorschrift erlaubt Datenverarbeitungen, die zur Erfüllung eines Vertrags erforderlich sind, dessen Partei die betroffene Person ist.

Aus datenschutzrechtlicher Sicht halte ich allerdings eine strenge Prüfung für geboten, ob Vereinbarungen des Dienstherrn/Arbeitgebers mit seinen Beschäftigten tatsächlich als Verträge im Sinne von Art. 6 Abs. 1 UAbs. 1 Buchst b DSGVO gewertet werden können. Das Beschäftigtenverhältnis ist so umfassend von Über- und Unterordnung geprägt, dass Beschäftigte erheblichem Druck unterliegen können, Vereinbarungen, die lediglich vom Dienstherrn/Arbeitgeber gewollt sind, abzuschließen.

Ob unter diesen Rahmenbedingungen echte Vertragsfreiheit ausgeübt werden kann, sollte deshalb im Einzelfall sorgfältig untersucht werden. Nicht genügen kann es nach meiner Meinung, eine Einwilligung lediglich in der äußeren Form eines Vertrags zu erklären. Gerade auch zur Abgrenzung von der Einwilligung sollte ein Vertrag im Sinne von Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO im Beschäftigungskontext eine angemessene Gegenleistung enthalten, die üblicherweise in einem Entgelt besteht, dessen Höhe das Interesse des Dienstherrn/Arbeitgebers an der Verwendung der Bedienstetenfotos widerspiegelt. Insofern sollte gelten, dass die Übertragung der Nutzungsrechte an den Bildern mit der regelmäßigen monatlichen Vergütung nicht abgegolten sein kann.

9.7.3 Sonstige Rechtsgrundlagen?

Andere Rechtsgrundlagen im Sinne von Art. 6 Abs. 1 DSGVO, die geeignet wären, die geplanten Werbemaßnahmen zu rechtfertigen, kann ich nicht erkennen.

Die gegenständlichen Maßnahmen des Arbeitgebermarketings sehe ich insbesondere nicht als erforderlich für die Wahrnehmung einer öffentlichen Aufgabe an (vgl. Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2, 3 DSGVO). Selbst wenn Marketing in einem gewissen Umfang als Informationshandeln zu den Aufgaben öffentlicher Stellen zählen kann, müssen dazu nicht Bilder der eigenen Beschäftigten verwendet werden. Insofern gelten die in Art. 103 BayBG genannten Voraussetzungen.

Auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO, der Datenverarbeitungen dann gestattet, wenn das Interesse des Verantwortlichen an der Verarbeitung das Interesse der betroffenen Person daran überwiegt, dass diese Verarbeitung unterbleibt, können sich öffentliche Stellen nach Art. 6 Abs. 1 UAbs. 2 DSGVO nicht berufen.

9.7.4 Fazit

Aus datenschutzrechtlicher Sicht stehe ich der Werbung öffentlicher Stellen mit Fotos ihrer Bediensteten reserviert gegenüber. Da eine Einwilligung regelmäßig frei widerruflich ist, kommt nach meiner Auffassung nur ein Vertrag als dauerhafte Rechtsgrundlage für die Verwendung der Bilder in Betracht, der jedenfalls ein angemessenes Entgelt für die betroffenen Personen vorsehen sollte, das zusätzlich zum monatlichen Gehalt gezahlt wird. In diesem Zusammenhang wäre allerdings auch zu klären, in welchem Umfang Beschäftigte des öffentlichen Dienstes mit ihrem Dienstherrn/Arbeitgeber zusätzliche Vergütungen vereinbaren können. Das ist jedoch in erster Linie keine datenschutzrechtliche, sondern eine dienst- und arbeitsrechtliche Frage. Für klar vorzugswürdig halte ich es jedenfalls, auf derartige Maßnahmen von vornherein zu verzichten.

10 Bildung, Wissenschaft, Kultur

10.1 Beratung bei der Änderung von Vorschriften

Im Berichtszeitraum habe ich zu Änderungen schulrechtlicher Vorschriften intensiv beraten. So wurden im Bayerischen Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG), in der Bayerischen Schulordnung (BaySchO) und in der Lehrerdienstordnung (LDO) einige datenschutzrechtlich relevante Änderungen vorgenommen. Weiterhin wurde auch eine neue Studienkollegordnung erlassen.

10.1.1 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen

Im Bayerischen Gesetz über das Erziehungs- und Unterrichtswesen sind vor allem die Einführung der Pflicht zur Vorlage eines erweiterten Führungszeugnisses für sonstiges schulisches Personal in Art. 60a BayEUG und die Verlängerung der Übergangsfrist im Hinblick auf die Verarbeitung von statistischen Daten durch die Schulen in Art. 122 Abs. 4 BayEUG hervorzuheben.

10.1.1.1 Art. 60a BayEUG

Der neue Art. 60a Abs. 2 BayEUG fordert für das sonstige schulische Personal im Sinne von Art. 60a Abs. 1 Satz 1 BayEUG – darunter fallen etwa Honorarkräfte oder Ehrenamtliche im Rahmen von Ganztagsangeboten – sowie das Verwaltungs- und Hauspersonal als Tätigkeitsvoraussetzung für den Umgang mit Schülerinnen und Schülern die **persönliche Eignung** und **Zuverlässigkeit**. Hieran fehlt es insbesondere, wenn die Person wegen einer im Katalog nach Art. 60a Abs. 2 Satz 2 Nr. 2 BayEUG genannten Straftat rechtskräftig verurteilt worden ist. Der erfasste Straftatenkatalog lehnt sich an § 72a Abs. 1 Achtes Buch Sozialgesetzbuch – Kinder- und Jugendhilfe – (SGB VIII) an. Unmittelbar datenschutzrechtlich relevanten Gehalt hat **Art. 60a Abs. 3 BayEUG**.

Die Bestimmung konstituiert eine **Nachweispflicht** vor Tätigkeitsbeginn gegenüber der Schulleitung. Diese Pflicht betrifft die persönliche Eignung im Sinne von Art. 60a Abs. 2 Satz 2 Nr. 2 BayEUG und stellt auf die Vorlage eines maximal drei Monate alten **erweiterten Führungszeugnisses** nach § 30a Abs. 1 Bundeszentralregistergesetz ab. Datenschutzrechtlich ist die Entgegennahme des erweiterten Führungszeugnisses durch die Schulleitung als eine Datenerhebung der Schule zu werten. Mithin handelt es sich bei Art. 60a Abs. 3 BayEUG um eine Regelung im Sinne von Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO.

Gegen die Einführung des Art. 60a BayEUG, insbesondere die damit verbundene Nachweispflicht mittels eines erweiterten Führungszeugnisses, habe ich angesichts des hohen Werts der hier in Rede stehenden Schutzgüter (Leben und Unversehrtheit von minderjährigen Schulkindern) keine grundsätzlichen datenschutzrechtlichen Bedenken erhoben. Allerdings konnte ich bei der konkreten Ausgestaltung des Art. 60a BayEUG einige zentrale datenschutzrechtliche Verbesserungen erwirken. So habe ich beim ursprünglichen Gesetzentwurf bemängelt, dass spezielle datenschutzrechtliche Bestimmungen fehlen, die eine spezial-

gesetzliche Rechtsgrundlage für die Datenverarbeitung im Rahmen der Ausführung des Art. 60a BayEUG regeln. Zudem vermisste ich eine gesetzliche Zweckbindung. Die infolgedessen nun erlassene Regelung greift in Art. 60a Abs. 3 Satz 2 BayEUG beide monierten Punkte auf.

Art. 60a Abs. 3 Satz 2 BayEUG lautet:

„Die Schulen dürfen die durch die Einsichtnahme in das erweiterte Führungszeugnis erhobenen Daten nur verarbeiten, soweit dies zum Ausschluss der Personen von der Tätigkeit, die Anlass zu der Einsichtnahme in das erweiterte Führungszeugnis gewesen ist, erforderlich ist."

Bei dieser Regelung handelt es sich nicht nur um eine **Zweckbindungsklausel**, sondern um eine **enge spezielle Verarbeitungsbefugnis**, die freilich auch zugleich den Verarbeitungszweck (eng) festlegt. Diese spezielle Verarbeitungsbefugnis verdrängt aufgrund ihrer Spezialität die allgemeine – ansonsten einschlägige – Verarbeitungsbefugnis des Art. 85 Abs. 1 Satz 1 BayEUG und die Zweckänderungsbefugnis des Art. 85 Abs. 2 BayEUG. Für die Rechtsanwendung und Auslegung nicht ganz unbedeutend ist auch, dass ich erreichen konnte, dass dies auch in der Begründung zum Gesetzentwurf entsprechend klargestellt wurde.

Nicht umgesetzt wurde zu meinem Bedauern mein Vorschlag, dass in der Vorschrift – entsprechend der Regelung des § 72a Abs. 5 Satz 4 und 5 SGB VIII – auch konkrete Vorgaben zur Löschung der durch die Einsichtnahme in das Führungszeugnis erhobenen personenbezogenen Daten normiert werden. Zumindest ist meinem Vorschlag insoweit Rechnung getragen worden, dass in die Begründung des Entwurfs (siehe Landtags-Drucksache 18/1481, Seite 18) insbesondere folgender Hinweis zur Löschung aufgenommen wurde:

„Aus der Zweckbindung ergibt sich auch, dass die Daten unverzüglich zu löschen sind, wenn im Anschluss an die Überprüfung keine Tätigkeit an der Schule wahrgenommen wird."

Unabhängig davon sehen – wie von mir angeregt – auch die **Verwaltungsvorschriften** konkretere Vorgaben zur Löschung vor. So stellt ein Schreiben des Bayerischen Staatsministeriums für Unterricht und Kultus an die nachgeordneten Stellen klar, dass alle durch die Einsicht in das erweiterte Führungszeugnis gewonnenen Daten zu löschen seien, wenn ihre Verarbeitung nicht mehr erforderlich ist. Nach einer positiven Entscheidung über den Einsatz der betreffenden Person sei dies unverzüglich der Fall; bei einer negativen Entscheidung nach Eintritt von deren Bestandskraft.

Damit werden der Praxis hilfreiche Hinweise an die Hand gegeben, um die allgemeine gesetzliche Vorgabe zur Löschpflicht nach Art. 17 Abs. 1 Buchst. a DSGVO umzusetzen, wonach die personenbezogenen Daten zu löschen sind, sobald sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind.

10.1.1.2 Art. 122 Abs. 4 BayEUG

Art. 113b Abs. 8 Satz 3 BayEUG bestimmt, dass die Schulen die von dieser Bestimmung geforderten statistischen Auskünfte unter Verwendung des vom Kultusministerium bereitgestellten Schulverwaltungsprogramms an das Landesamt für Statistik beziehungsweise die Statistikstellen des Kultusministeriums und des

Landesamts für Schule zu erteilen haben. Da noch nicht alle Schulen in Bayern mit dem Schulverwaltungsprogramm ASV ausgestattet sind, sah Art. 121 Abs. 4 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen in der bis zum 31. Juli 2019 geltenden Fassung (BayEUG-alt) vor, dass für Schularten, bei denen die Auskunftserteilung gemäß Art. 113b Abs. 8 BayEUG noch nicht vollumfänglich umgesetzt ist, Art. 113 Abs. 1 Satz 1 BayEUG in der bis zum Ablauf des 31. Mai 2014 geltenden Fassung gilt. Mit anderen Worten: War an Schulen noch nicht das Schulverwaltungsprogramm ASV im Einsatz, konnte aufgrund von Art. 121 Abs. 4 BayEUG-alt früheres Recht weiter angewendet werden. Diese Regelung war bisher bis zum 31. Juli 2019 befristet und wäre mithin im Berichtszeitraum ausgelaufen. Das Kultusministerium konnte mir nachvollziehbar darlegen, dass es trotz aller Anstrengungen bisher nicht möglich war, an allen rund 6.100 Schulen das Schulverwaltungsprogramm ASV einzuführen. Die Aufrechterhaltung der alten Rechtsgrundlage sei aus Datenschutzgründen erforderlich, solange auch nur eine Schule Statistikdaten im „Altverfahren" liefere. Vor diesem Hintergrund habe ich keine Einwände dagegen erhoben, diese Übergangsregelung in einem neuen Art. 122 Abs. 4 BayEUG beizubehalten. Allerdings habe ich darauf geachtet, dass auch die neue Regelung mit einem konkreten Auslaufdatum versehen ist, nämlich jetzt nach Art. 125 Satz 2 BayEUG der 31. Juli 2024. So müssen bis spätestens zu diesem Datum alle Schulen mit dem Schulverwaltungsprogramm ASV ausgestattet sein.

10.1.2 Bayerische Schulordnung

Auch in der **Bayerischen Schulordnung** (BaySchO) gab es eine zentrale datenschutzrelevante Änderung. So war mit Inkrafttreten des neuen Bayerischen Datenschutzgesetzes zum 25. Mai 2018 die Ermächtigungsgrundlage für die **Verordnung zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes** vom 23. März 2001, die sogenannte **Durchführungsverordnung**, entfallen. Die Durchführungsverordnung galt noch bis zum 31. Juli 2019.

In dieser Verordnung hatte das Kultusministerium für die öffentlichen Schulen Folgendes bestimmt. Die Bestellung behördlicher Datenschutzbeauftragter, die datenschutzrechtliche Freigabe und die Führung eines Verfahrensverzeichnisses sind nicht erforderlich, wenn die Schulen ausschließlich automatisierte Verfahren, die durch das Kultusministerium bereits generell freigegeben sind, in dem in den Anlagen zur Durchführungsverordnung aufgeführten Umfang einsetzen. Dies betraf folgende Verfahren: Verfahren der Lehrerdatei, Schülerdatei, Oberstufendatei, Stundenplanprogramm, Vertretungsplanprogramm, Notenverwaltungsprogramm, Buchausleiheprogramm, Videoaufzeichnung an Schulen, Internetauftritt von Schulen, passwortgeschützte Lernplattform und schulinterner passwortgeschützter Bereich.

In der Sache handelte es sich dabei um bestimmte Datenverarbeitungen durch automatisierte Verfahren, bei denen unter Berücksichtigung der erhobenen, verarbeiteten oder genutzten Daten eine Beeinträchtigung der Rechte und Freiheiten der Betroffenen unwahrscheinlich war. Dieser für den Datenschutz positive Umstand ist auch darauf zurückzuführen, dass ich in der Vergangenheit bei Erlass der Durchführungsverordnung und ihren Änderungen durch meine eingehende Beratung des Kultusministeriums streng auf die Wahrung des Datenschutzes, insbesondere auf den Grundsatz der Erforderlichkeit, gedrungen habe (siehe etwa mein 26. Tätigkeitsbericht 2014 unter Nr. 10.1 und mein 23. Tätigkeitsbericht 2008 unter Nr. 12.2).

Die in den Anlagen der Durchführungsverordnung geregelten detaillierten und differenzierten Vorgaben zu Zweck, Art und Umfang der einzelnen Datenverarbeitungen haben sich in der Vergangenheit in der Praxis bewährt und den Schulen eine umfangreiche Leitlinie für ein datenschutzkonformes Vorgehen an die Hand gegeben. Vor diesem Hintergrund habe ich das Kultusministerium durch intensive Beratung und Hilfe dabei unterstützt, diese bewährte und für den Datenschutz an bayerischen Schulen bedeutsame Regelung in einer dem neuen Datenschutzrecht angepassten Form beizubehalten.

Hierzu wurde in **§ 46 BaySchO** eine neue normative Verankerung geschaffen.

§ 46 BaySchO
Verarbeitungsverfahren (vergleiche Art. 85 und 89 BayEUG)
(1) [1]Schulen dürfen personenbezogene Daten in Verfahren verarbeiten, die nach Zweck, Umfang und Art den in Anlage 2 geregelten Vorgaben entsprechen. [2]Davon unberührt bleiben die Anforderungen aus anderen Gesetzen wie insbesondere der Datenschutz-Grundverordnung und dem Bayerischen Datenschutzgesetz.
(2) Abs. 1 gilt auch für Verfahren, die sich aus mehreren der in Anlage 2 genannten Verfahren zusammensetzen oder sich auf Teile dieser Verfahren beschränken, sofern die für den jeweiligen Verarbeitungszweck vorgesehenen Regelungen der einzelnen Verfahren eingehalten werden.
(3) Für die Verarbeitung von Daten, die in der Schülerakte zu führen sind, oder Daten über Leistungsnachweise gilt § 38 entsprechend.

Die in § 46 Abs. 1 Satz 1 BaySchO erwähnte **Anlage 2** übernimmt ganz überwiegend die inhaltlichen Regelungen zu den zulässigen Datensätzen der Anlage zur Durchführungsverordnung. Thematisch erfasst die Anlage 2 folgende Verfahren:

— Anlage 2 Nr. 1 Schulverwaltungsprogramm;
— Anlage 2 Nr. 2 Elektronischer Notenbogen;
— Anlage 2 Nr. 3 Klassentagebuch;
— Anlage 2 Nr. 4 Passwortgeschützte Lernplattform;
— Anlage 2 Nr. 5 Schulinterner passwortgeschützter Bereich;
— Anlage 2 Nr. 6 Videoüberwachung an Schulen.

Bei der erwähnten Überführung der Durchführungsverordnung in die Bayerische Schulordnung war es mir zugleich ein Anliegen, dafür Sorge zu tragen, dass keine Verschlechterung des Datenschutzniveaus eintritt. Denn das Kultusministerium hat die Gelegenheit der inhaltlichen Überführung der Durchführungsverordnung in die Bayerische Schulordnung zum Anlass genommen, die Regelungen inhaltlich zu konsolidieren und an mittlerweile festgestellte neue Erforderlichkeiten der Datenverarbeitung anzupassen. Daher habe ich mir bezüglich jeder Änderung und inhaltlichen Erweiterung der Datenverarbeitungsbefugnisse vom Kultusministerium darlegen lassen, dass diese unter dem Blickwinkel des Datenschutzes erforderlich und gerechtfertigt sind. Durch mein Einwirken konnte ich zahlreiche Verbesserungen für den Datenschutz erreichen. Deren einzelteilige Darstellung würde jedoch den Rahmen des Tätigkeitsberichts überschreiten, so dass ich nur einige wichtige Punkte herausgreife:

— In Anlage 2 Nr. 3 zu § 46 BaySchO habe ich erreicht, dass diese nicht nur – wie ursprünglich im Verordnungsentwurf vorgesehen – elektronische Klassentagebücher erfasst, sondern auch sogenannte analoge Klassentagebücher. Hierdurch wird auch für diese ein fester Datenkreis abgesteckt und

den Schulen Rechtssicherheit und Orientierung bei der Umsetzung datenschutzrechtlicher Vorgaben gegeben.

— Weiter konnte ich durchsetzen, dass die Anlage keine Felder (sog. Freitexteingabefelder) vorsieht, in die der Anwender nach seinem Belieben Text eingeben kann. Solche Felder sind aus Datenschutzsicht problematisch, da sie dem Anwender die Möglichkeit überlassen, freie Informationen einzutragen und dadurch das Risiko erhöht wird, dass nicht erforderliche personenbezogene Daten (etwa Eingabe der Art der Erkrankung eines Schulkinds) verarbeitet werden. Vorzugswürdig sind demgegenüber vorformulierte Auswahlfelder.

— Ich habe mich ferner erfolgreich dafür eingesetzt, dass auch die bisherige Regelung der Anlage der Durchführungsverordnung zur Videoüberwachung in die Bayerische Schuldordnung mitübernommen wird. Auf diese Weise wird den Schulen für den praktischen Vollzug eine wichtige Orientierung in diesem grundrechtssensiblen Bereich an die Hand gegeben.

— Schließlich habe ich darauf hingewirkt, dass die Regelung des § 46 Abs. 3 BaySchO getroffen wird. Danach gilt § 38 BaySchO für die Verarbeitung von Daten, die in der Schülerakte zu führen sind, oder Daten über Leistungsnachweise entsprechend. Hierdurch wird ein Wertungswiderspruch zwischen dem Datenschutz bei analogen und digitalen Daten der Schülerakte im Hinblick auf die Verwendungsmöglichkeiten vermieden. Dabei war mir besonders wichtig, dass über die Anordnung der entsprechenden Geltung des § 38 Abs. 2 Satz 1 BaySchO der schulinterne Zugriff auf Daten auf den konkreten Einzelfall beschränkt wurde. Auch an anderer Stelle in der Anlage 2 habe ich mich für die Beschränkung beziehungsweise Begrenzung des schulinternen Zugriffs auf sensible Daten, wie etwa Leistungsdaten oder verhängte Erziehungs- und Ordnungsmaßnahmen, erfolgreich eingesetzt.

Insgesamt lässt sich festhalten, dass mit der erfolgreichen Implementierung der bisherigen inhaltlichen Regelungen der Durchführungsverordnung in die Bayerische Schulordnung, genauer in **§ 46 BaySchO** in Verbindung mit **Anlage 2**, ein zentraler Baustein des bayerischen schulischen Datenschutzrechts bewahrt wurde.

10.1.3 § 14a Lehrerdienstordnung

Im Berichtszeitraum wurde auch die Lehrerdienstordnung (LDO) geändert. Bei dieser handelt es sich nicht um ein Gesetz, sondern um eine Verwaltungsvorschrift, die der Verwaltungspraxis wesentliche Hinweise für den Gesetzesvollzug liefert. Aus Datenschutzsicht relevant war die Einfügung eines neuen § 14a LDO zum Datenschutz.

§ 14a LDO
Datenschutz
(1) [1]Die Lehrkraft ist verpflichtet, an der Sicherstellung des Datenschutzes durch die Schule nach Maßgabe der Organisationsverfügungen und Weisungen der Schulleitung mitzuwirken und der Schulleitung alle hierzu erforderlichen Auskünfte zu erteilen. [2]Dies gilt auch bei der Nutzung von privaten Einrichtungen und Geräten. [3]Insbesondere unterstützt die Lehrkraft die Schulleitung bei deren Pflicht

zur Beantwortung von Anträgen auf Wahrnehmung der in der DSGVO verankerten Betroffenenrechte und bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten. [4]Datenmissbrauch oder Datenverlust (vgl. Art. 4 Nr. 12 DSGVO) sind der Schulleitung unverzüglich zu melden.
(2) [1]Die Lehrkraft darf dienstliche Aufzeichnungen und Unterlagen mit Personenbezug, auch in digitaler Form, grundsätzlich nur so lange aufbewahren, wie dies zur Aufgabenerfüllung der Schule erforderlich ist. [2]Sofern nichts anderes bestimmt ist, sind Aufzeichnungen und Unterlagen über Schülerinnen und Schüler, die nicht zu den Schülerunterlagen (§ 37 BaySchO) gehören, spätestens zwei Jahre nach Ablauf des jeweiligen Schuljahres zu löschen.
(3) Die Bekanntmachungen des Staatsministeriums zum Umgang mit Schülerunterlagen und zum Vollzug des Datenschutzrechts an Schulen sind zu beachten.

Die neue Bestimmung führt den Lehrkräften ihnen obliegende dienstliche Pflichten im Bereich des Datenschutzes klarstellend vor Augen. Hervorzuheben sind insbesondere die Mitwirkungspflicht der Lehrkräfte, wenn die Schule Betroffenenrechte nach der Datenschutz-Grundverordnung zu erfüllen hat, und die Pflicht, Datenmissbrauch oder Datenverlust der Schulleitung unverzüglich zu melden. Da Lehrkräfte – soweit dies nach den geltenden Regelungen zulässig ist – zur Verarbeitung personenbezogener Daten der Schulkinder zu schulischen Zwecken auch private Rechner einsetzen können, stellt § 14a Abs. 1 Satz 2 LDO klar, dass die datenschutzrechtlichen Pflichten der Lehrkräfte insoweit ebenfalls Geltung beanspruchen. Dies gilt freilich auch im Hinblick auf die Löschvorgaben, die in § 14a Abs. 2 LDO angesprochen sind.

Im Rahmen der Beratung des Kultusministeriums konnte ich erreichen, dass Formulierungen aus der Bestimmung entfernt wurden, die zu Fehlinterpretationen hätten führen können. Zudem konnte ich erreichen, dass ein (deklaratorischer) Hinweis in § 14a Abs. 3 LDO aufgenommen wird, wonach die Bekanntmachungen des Kultusministeriums zum Umgang mit Schülerunterlagen und zum Vollzug des Datenschutzrechts an Schulen zu beachten sind. Hierdurch wird befördert, dass diese wichtigen datenschutzrechtlichen Vorgaben – etwa im Hinblick auf Regelungen zur Nutzung privater Geräte – bei der Lektüre des § 14a LDO nicht aus dem Blick geraten.

10.1.4 Studienkollegordnung

Bisher bestanden für die zwei bayerischen Studienkollegs zwei getrennte Studienkollegordnungen, deren Inhalt im Wesentlichen identisch war. Zur Konsolidierung wurde im Berichtszeitraum eine gemeinsame Studienkollegordnung vom 16. Oktober 2019 (GVBl. S. 619) erlassen. Dabei handelt es sich um eine Rechtsverordnung, also um ein durch die Exekutive geschaffenes Normwerk. Die im Erstentwurf enthaltene Datenschutzregelung begegnete in formaler Hinsicht verfassungsrechtlichen Bedenken. Auf der Ebene der normhierarchisch unter dem Gesetz stehenden Studienkollegordnung sollten die höherrangigen datenschutzrechtlichen Vorschriften des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen für anwendbar erklärt werden. Insoweit habe ich auf die Rechtsprechung des Bundesverfassungsgerichts zum Parlamentsvorbehalt im Schulrecht hingewiesen. Diesen Bedenken ist der Gesetzgeber nun gefolgt. So hat er im neuen Art. 121 Abs. 2 Satz 2 BayEUG in der Fassung des Gesetzes zur Änderung des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen vom 24. Juli 2019 (GVBl. S. 398) selbst auf Ebene des Parlamentsgesetzes für die Stu-

dienkollegs unter anderem die entsprechende Geltung der im Schuldatenschutzrecht zentralen Norm des Art. 85 BayEUG sowie des Art. 85a BayEUG angeordnet.[32] Damit ist sowohl dem Datenschutz im Bereich der Studienkollegs ein wichtiger Dienst erwiesen als auch ein verfassungsrechtlich überzeugender Weg beschritten worden.

Im Übrigen habe ich es begrüßt, dass in § 3 Abs. 1 der Studienkollegordnung unter anderem § 24 BaySchO zu Erhebungen und insbesondere die Vorschriften der §§ 37 ff. BaySchO zu den Schülerunterlagen für entsprechend anwendbar erklärt werden. Auch dies stellt einen großen datenschutzrechtlichen Gewinn dar, da damit die im Bereich der Schulen bewährte Regelung zu den Schülerunterlagen (dazu ausführlich mein 27. Tätigkeitsbericht 2016 unter Nr. 10.1) auch für die Studienkollegs Anwendung findet.

10.2 Videoüberwachung an Schulen

Zum Thema Videoüberwachung an Schulen habe ich mich in meinen Tätigkeitsberichten bereits mehrfach geäußert (siehe 27. Tätigkeitsbericht 2016 unter Nr. 10.5, 26. Tätigkeitsbericht 2014 unter Nr. 10.9.1, 25. Tätigkeitsbericht 2012 unter Nr. 10.5 sowie 23. Tätigkeitsbericht 2008 unter Nr. 12.2.2). Die vom Bayerischen Staatsministerium für Unterricht und Kultus erlassene Verordnung zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes (einschließlich der Anlage 8 „Videoaufzeichnung an Schulen“) galt bis zum 31. Juli 2019. Seit 1. August 2019 ist die Videoüberwachung an Schulen in Anlage 2 der Schulordnung für schulartübergreifende Regelungen an Schulen in Bayern (Bayerische Schulordnung – BaySchO) unter Nr. 6 („Videoüberwachung an Schulen“) sowie in Art. 24 BayDSG (vgl. auch § 46 Abs. 1 Satz 2 BaySchO) geregelt.

10.2.1 Sachverhalt

Besorgte Eltern machten mich auf die Videoüberwachung in einer Schule aufmerksam. Meine Prüfung ergab unter anderem, dass mindestens 26 Videokameras eingesetzt und dabei auch Schulflure sowie die Aula während der Unterrichtszeit mittels Videoaufzeichnung überwacht wurden. Die verantwortliche Schule berief sich diesbezüglich zunächst allgemein auf Vorfälle wie Vandalismus, Diebstähle und Gewaltdelikte. Etwas konkreter wurde dann auf Diebstähle insbesondere von Handys Bezug genommen, die bei Stundenwechseln mit den Büchertaschen auf den Fluren abgestellt würden. Auch seien Schmierereien an Innenwänden zu verzeichnen gewesen. Zu Gewaltdelikten unterblieben konkrete Ausführungen. Eine Dokumentation zu einzelnen Vorfällen, etwa zu deren Anzahl, Datum, Uhrzeit und Ort sowie Art und Umfang von Schäden konnte mir nicht vorgelegt werden.

10.2.2 Rechtliche Bewertung

In datenschutzrechtlicher Hinsicht ist eine Videoüberwachung an bayerischen öffentlichen Schulen nur in sehr engen Grenzen zulässig. Auf Grundlage der Stellungnahme der Schule war bereits nicht erkennbar, dass die Videoüberwachung der Aula und der Schulflure die Anforderungen des Art. 24 BayDSG erfüllt hätte.

[32] Vgl. auch Landtags-Drucksache 18/1481, S. 10.

Eine anhand konkreter Vorfälle belegte Gefahrenlage konnte nicht festgestellt werden. Abstrakte Hinweise auf „Diebstähle und Schmierereien“ können hier nicht genügen. Nur eine nachvollziehbare Dokumentation etwa über Art, Häufigkeit und Schadenshöhen hätte im vorliegenden Fall eine weitere Prüfung am Maßstab des Art. 24 BayDSG überhaupt erst ermöglicht. Darüber hinaus wäre auch genau darzulegen gewesen, welche anderen – gegenüber einer Videoüberwachung milderen – Maßnahmen ergriffen wurden und warum diese nicht ausreichen, so etwa eine Aufsicht in Pausen sowie Hinweise an die Schülerschaft, insbesondere Wertgegenstände nicht unbeaufsichtigt im Flur zu belassen.

10.2.3 Vorgehen, Handlungsempfehlung und Ausblick

Nach meinen Hinweisen hat die Schule noch im ersten Halbjahr 2019 erfreulicherweise mitgeteilt, dass sie die oben beschriebene Videoüberwachung der Gänge und der Aula einstellt.

Bei dieser Gelegenheit möchte ich darauf aufmerksam machen, dass Schulen ihren behördlichen Datenschutzbeauftragten rechtzeitig vor einem beabsichtigten Einsatz einer Videoüberwachung einbinden und ihm Gelegenheit zur Stellungnahme geben müssen (vgl. Art. 24 Abs. 5 BayDSG).

11 Soziale Medien und Telemedien

11.1 Soziale Netzwerke

Bei der Nutzung Sozialer Medien durch bayerische öffentliche Stellen handelt es sich seit längerer Zeit um ein wichtiges datenschutzrechtliches Beratungsthema. Bereits mehrfach habe ich mich zu diesem Thema geäußert, zuletzt in meinem 28. Tätigkeitsbericht 2018 unter Nr. 13.1. Dabei bin ich insbesondere auf das Urteil des Europäischen Gerichtshofs vom 5. Juni 2018, C-210/16, und die Reaktion der deutschen Datenschutz-Aufsichtsbehörden auf diese Entscheidung eingegangen.

Auch im Berichtszeitraum haben mich wieder zahlreiche Beratungsanfragen bayerischer öffentlicher Stellen zur Nutzung Sozialer Medien, insbesondere Sozialer Netzwerke erreicht. Konkret handelt es sich dabei weiterhin schwerpunktmäßig um Fragen zum Betrieb von Facebook-Fanpages, die ich insbesondere auf Grundlage der vorliegenden Rechtsprechung beantwortet habe.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) hat unter meiner Mitwirkung bereits von Anfang an die Auswirkungen der Rechtsprechung des Europäischen Gerichtshofs in den Blick genommen. So bekräftigte die Datenschutzkonferenz beispielsweise in ihrem Beschluss vom 5. September 2018 auch das Erfordernis einer Vereinbarung nach Art. 26 DSGVO als eine der Voraussetzungen für einen rechtskonformen Betrieb von Fanpages. Dies führte dazu, dass Facebook sowohl eine „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“ als auch „Informationen zu Seiten-Insights“ veröffentlichte.

Ich habe mich weiterhin an der von der Datenschutzkonferenz eingerichteten Task Force Fanpages beteiligt. Diese bereitete nach Beurteilung der von Facebook veröffentlichten Informationen folgende Positionierung der Datenschutzkonferenz vor:

Positionierung zur Verantwortlichkeit und Rechenschaftspflicht
bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit
vom 1. April 2019

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat sich am 5. September 2018 zu dem (Weiter-)Betrieb von Facebook-Fanpages nach dem Urteil des EuGH vom 5. Juni 2018 geäußert.

In ihrem Beschluss hat die Konferenz deutlich gemacht, dass Fanpage-Betreiber die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und die Einhaltung der Grundsätze für die Verarbeitung

personenbezogener Daten aus Art. 5 Abs. 1 DSGVO nachweisen können müssen. Dies ergibt sich aus der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO sowie insbesondere in Bezug auf Verpflichtungen nach Art. 24, 25, 32 DSGVO.

Am 11. September 2018 veröffentlichte Facebook eine sog. „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen" sowie „Informationen zu Seiten-Insights". Diese von Facebook veröffentliche „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen" erfüllt nicht die Anforderungen an eine Vereinbarung nach Art. 26 DSGVO. Insbesondere steht es im Widerspruch zur gemeinsamen Verantwortlichkeit gemäß Art. 26 DSGVO, dass sich Facebook die alleinige Ent scheidungsmacht „hinsichtlich der Verarbeitung von Insights-Daten" einräumen lassen will. Die von Facebook veröffentlichten Informationen stellen zudem die Verarbeitungstätigkeiten, die im Zusammenhang mit Fanpages und insbesondere Seiten-Insights durchgeführt werden und der gemeinsamen Verantwortlichkeit unterfallen, nicht hinreichend transparent und konkret dar. Sie sind nicht ausreichend, um den Fanpage-Betreibern die Prüfung der Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten der Besucherinnen und Besucher ihrer Fanpage zu ermöglichen. Vor diesem Hintergrund bekräftigt die Konferenz erneut die Rechenschaftspflicht der Fanpage-Betreiber (unabhängig von dem Grad der Verantwortlichkeit) und stellt fest:

1. *Jeder Verantwortliche benötigt für die Verarbeitungstätigkeiten, die seiner Verantwortung unterliegen, eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO und – soweit besondere Kategorien personenbezogener Daten verarbeitet werden – nach Art. 9 Abs. 2 DSGVO. Dies gilt auch in den Fällen, in denen sie die Verarbeitungstätigkeiten nicht unmittelbar selbst durchführen, sondern durch andere gemeinsam mit ihnen Verantwortlichen durchführen lassen.*

2. *Ohne hinreichende Kenntnis über die Verarbeitungstätigkeiten, die der eigenen Verantwortung unterliegen, sind Verantwortliche nicht in der Lage, zu bewerten, ob die Verarbeitungstätigkeiten rechtskonform durchgeführt werden. Bestehen Zweifel, geht dies zulasten der Verantwortlichen, die es in der Hand haben, solche Verarbeitungen zu unterlassen. Der EuGH führt hierzu aus: „Der Umstand, dass ein Betreiber einer Fanpage die von Facebook eingerichtete Plattform nutzt, um die dazugehörigen Dienstleistungen in Anspruch zu nehmen, kann diesen nämlich nicht von der Beachtung seiner Verpflichtungen im Bereich des Schutzes personenbezogener Daten befreien." (EuGH, C-210/16, Rn. 40).*

3. *Im Hinblick auf die Ausführungen zur „Hauptniederlassung für die Verarbeitung von Insights-Daten für sämtliche Verantwortliche" sowie zur federführenden Aufsichtsbehörde (Punkt 4 in der „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen") weist die Konferenz darauf hin, dass sich die Zuständigkeit der jeweiligen Aufsichtsbehörden für Fanpage-Betreiber nach der DSGVO richtet. Nach Art. 55 ff. DSGVO sind die Aufsichtsbehörden für Verantwortliche (wie z. B. Fanpage-Betreiber) in ihrem Hoheitsgebiet zuständig. Dies gilt unabhängig von den durch die DSGVO vorgesehenen Kooperations- und Kohärenzmechanismen.*

Sowohl Facebook als auch die Fanpage-Betreiber müssen ihrer Rechenschaftspflicht nachkommen. Die Datenschutzkonferenz erwartet, dass Facebook entsprechend nachbessert und die Fanpage-Betreiber ihrer Verantwortlichkeit entsprechend gerecht werden. Solange diesen Pflichten nicht nachgekommen wird, ist ein datenschutzkonformer Betrieb einer Fanpage nicht möglich.

Im Ergebnis ist die Datenschutzkonferenz damit der Auffassung, dass die genannten Veröffentlichungen die Anforderungen an eine Vereinbarung nach Art. 26

DSGVO nicht erfüllten, und dass auch auf Seiten der Fanpage-Betreiber weiterhin Handlungsbedarf besteht.

Diese Positionierung habe ich noch im April erneut zum Anlass genommen, das Bayerische Staatsministerium des Innern, für Sport und Integration als das für das Datenschutzrecht federführende Ressort zeitnah auf die aktuellen Entwicklungen sowie die Haltung der Datenschutzkonferenz hinzuweisen und es gebeten, die Positionierung der Datenschutzkonferenz beim weiteren Vorgehen zu berücksichtigen. Mein Schriftwechsel mit dem Innenministerium dauert noch an.

Im September 2019 ist ein Urteil des Bundesverwaltungsgerichts ergangen[33], das dem Europäischen Gerichtshof unter anderem die Frage nach der (gemeinsamen) Verantwortlichkeit des Fanpage-Betreibers für durch Facebook vorgenommene Datenverarbeitungen zur Entscheidung vorgelegt hatte. Das Bundesverwaltungsgericht hat vor dem Hintergrund der Antworten des Europäischen Gerichtshofs das zugrundeliegende Urteil des Oberverwaltungsgerichts[34] aufgehoben und die Sache zur erneuten Verhandlung und Entscheidung an dieses zurückverwiesen. Laut Bundesverwaltungsgericht bedarf es zur Frage der Rechtswidrigkeit der beanstandeten Datenverarbeitungsvorgänge einer näheren Aufklärung der tatsächlichen Umstände durch das Oberverwaltungsgericht. So werde zu prüfen sein, welche Datenverarbeitungen bei Aufruf der Fanpages im für die Entscheidung maßgeblichen Zeitpunkt stattfanden.

Nach Veröffentlichung der Entscheidungsgründe durch das Bundesverwaltungsgericht ist es zunächst erforderlich, die entsprechenden Feststellungen des Gerichts zu analysieren und weitere Schlüsse zu ziehen – auch angesichts sich verändernder Ausgestaltungen im Zusammenhang mit dem Betrieb von Facebook-Fanpages. Aktuell beschäftigt sich unter meiner Mitwirkung unter anderem die Task Force Fanpages der Datenschutzkonferenz insbesondere mit den Auswirkungen der aktuellen Rechtsprechung.

Dies ändert jedoch nichts an meiner bereits seit Langem vertretenen Auffassung, dass der Betrieb von Fanpages durch bayerische öffentliche Stellen von diesen kritisch zu überprüfen ist.

11.2 Einbindung von Social Plugins in Internetseiten bayerischer Behörden

Im Zusammenhang mit der Nutzung von Sozialen Netzwerken wurden auch weiterhin Fragen zur Einbindung von Social Plugins in die Internetseiten bayerischer öffentlicher Stellen an mich gerichtet, etwa zum Like-Button von Facebook. Zur datenschutzrechtlichen Unzulässigkeit einer direkten Einbindung solcher Tools habe ich mich bereits in der Vergangenheit ausdrücklich positioniert, beispielsweise in meinem 25. Tätigkeitsbericht 2012 unter Nr. 1.3.2 und in meinem 26. Tätigkeitsbericht 2014 unter Nr. 12.4.3, sowie entsprechende Prüfungen durchgeführt.

33 Bundesverwaltungsgericht, Urteil vom 11. September 2019, 6 C 15.18.

34 Schleswig-Holsteinisches Oberverwaltungsgericht, Urteil vom 4. September 2014, OVG 4 LB 20/13.

In diesem Zusammenhang habe ich stets ausgeführt, dass eine Einbindung entsprechender Plugins durch bayerische öffentliche Stellen nur bei Einsatz einer Variante wie etwa der „Zwei-Klick-Lösung“ zulässig sein kann.

Der Europäische Gerichtshof hat diese Auffassung nunmehr im Ergebnis bestätigt.[35]

Der Vorlage des Oberlandesgerichts Düsseldorf an den Europäischen Gerichtshof lag eine Unterlassungsklage der Verbraucherzentrale Nordrhein-Westfalen gegen den Website-Betreiber Fashion ID zugrunde, der den „Gefällt mir“ Button von Facebook direkt in seinen Internetauftritt eingebunden hatte. Durch eine direkte Einbindung erfährt Facebook zunächst die ID-Adresse des Website-Besuchers, Daten über Browsereinstellungen und die Tatsache des Website-Aufrufes.

Der Europäische Gerichtshof hat die auf die datenschutzrechtliche Verantwortlichkeit bezogenen Vorlagefragen dahingehend beantwortet, dass der Betreiber einer Website, der ein Social Plugin einbindet, als (gemeinsam mit dem Anbieter des Plugins) verantwortlich zu betrachten ist. Die Verantwortlichkeit des Website-Betreibers bezieht sich dabei auf die Verarbeitungen, bei denen er über Zwecke und Mittel entscheidet, also auf das Erheben und Übermitteln der Daten. Zudem benötigen sowohl der Betreiber des Internetauftritts als auch der Anbieter des Plugins für diese Verarbeitungsvorgänge jeweils eine Rechtsgrundlage, die diese Vorgänge für jeden Einzelnen von ihnen rechtfertigt. Bei einer Einwilligung muss der Seitenbetreiber die Einwilligung zu den Verarbeitungsvorgängen einholen, für die er tatsächlich über Zwecke und Mittel entscheidet. Entsprechendes gilt für die Informationspflichten, die an diese Verarbeitungsvorgänge geknüpft sind.

Dies entspricht im Ergebnis meiner Einschätzung, dass die Datenübermittlung einer bayerischen öffentlichen Stelle unter Einsatz eines Social Plugins ohne Wissen und Zustimmung betroffener Personen nicht zulässig ist und die öffentliche Stelle als Betreiber der einbindenden Websites insoweit eine datenschutzrechtliche (Mit-)Verantwortlichkeit trägt.

35 Europäischer Gerichtshof, Urteil vom 29. Juli 2019, C-40/17.

12 Technik und Organisation

12.1 Künstliche Intelligenz

12.1.1 Künstliche Intelligenz im Gegensatz zu menschlichem Verstehen

Während Themen wie „Cloud“ und „Blockchain“ sich immer mehr etablieren, rückte eine im Gebiet der Informatik eigentlich schon sehr alte Technologie, die erstmals 1955 als Begriff im Rahmen eines Forschungsprojekts genannt wurde, in letzter Zeit erneut in den Fokus: Künstliche Intelligenz (KI).

Weltweit werden erhebliche Ressourcen in die Weiterentwicklung dieser Technologie investiert, die versucht, menschliche Denkprozesse zu imitieren: Mustererkennung und maschinelles Lernen werden genutzt, um einen Grad von „schlauem“ Verhalten und Leistungsfähigkeit zu erreichen, der sich mit statischen Handlungsanweisungen derzeit nicht erzielen lässt. Text- und Spracherkennung haben ihren Weg auf Smartphone, Büro und Auto gefunden. Bilderkennung ermöglicht medizinische Analysen, „Robo-Advisors“ übernehmen die Geldanlage, KI-gesteuerte Fahrzeuge fahren schon jetzt zumindest teilautonom auf den Straßen. So hat sich die Technologie aufgrund ihrer Überlegenheit bei bestimmten Aufgaben schrittweise und zum Teil unbemerkt etabliert. So wurde meist nicht ein bestehendes System in Gänze ersetzt, sondern einzelne Teilprozesse wurden aus Effizienzgründen an eine KI ausgelagert.

Als KI werden im Folgenden Systeme und digitale Verarbeitungsprozesse zusammengefasst, in denen ein oder mehrere, auf KI-Technologie basierende Teilkomponenten zum Einsatz kommen. Eine wissenschaftlich exakte Definition des Begriffs „Künstliche Intelligenz“ existiert bisher nicht. In der Bundesrat Drucksache 19/1982 wird KI aber beispielswiese wie folgt definiert:

„Künstliche Intelligenz (KI) ist ein Teilgebiet der Informatik, welches sich mit der Erforschung von Mechanismen des intelligenten menschlichen Verhaltens befasst. Dabei geht es darum, technische Systeme so zu konzipieren, dass sie Probleme eigenständig bearbeiten und sich dabei selbst auf veränderte Bedingungen einstellen können. Diese Systeme haben die Eigenschaft, aus neuen Daten zu ‚lernen‘ und mit Unsicherheiten umzugehen, statt klassisch programmiert zu werden.“

Künstliche Intelligenz unterscheidet sich

— von Algorithmen dahingehend, als dass KI Lösungswege selbst im Rahmen des Trainings entwickelt (und verbessert), während Algorithmen festgelegten Entscheidungsbäumen deterministisch folgen. Somit muss die exakte Logik eines Verarbeitungsprozesses den Entwicklerinnen und Entwicklern von Algorithmen im Voraus bekannt sein, um dann von ihnen explizit programmiert zu werden. Auf diesen (aufwändigen) Schritt kann im Fall von KI verzichtet werden. Der Ansatz hier kommt ohne das echte Verständnis der eigentlichen Logik hinter dem Prozess aus. Stattdessen wird KI mithilfe von Eingaben und gewünschten – oder nicht gewünschten – Ausgaben soweit trainiert, dass diese dann auch bei vorher unbekannten Testfällen mit hoher

Wahrscheinlichkeit (oder zumindest geringer Fehlerrate) die gewünschte Ausgabe/Entscheidung/Handlung erbringt;

— von Machine Learning (ML) insofern, als dass ML eine Grundlagentechnologie für KI darstellt;

— von Big Data insofern, als dass KI selbständig aus Daten Cluster bilden und (statistische, nicht aber logische) Zusammenhänge erkennen kann. Sie beschränkt sich nicht auf Analysen, sondern fällt auf Basis der ihr zur Verfügung stehenden Informationen autonom Entscheidungen oder setzt diese im Rahmen ihrer Möglichkeiten sogar direkt in Handlungen um. Trotzdem kann sie gegenwärtig in der Regel nur Kookkurrenzen, also mehrfaches Auftreten von Mustern oder Wörtern im selben Umfeld oder Korrelationen, also statistische Zusammenhänge finden; die zugrundeliegenden Kausalitäten und Wirkzusammenhänge „hinter" den Daten, also das „Warum" erschließen sich ihr noch nicht, das heißt, sie kann zwar ihr Verhalten auf ein Ziel hin optimieren, entwickelt aber kein „echtes" Verständnis für ihre Aufgabe und den Sinn dahinter.

Künstliche Intelligenz kann bestimmte Aufgaben mit höherer Effizienz und möglicherweise geringerer Fehlerquote erledigen als Menschen. Ohne echtes Verständnis für ihre Aufgabe, menschliches Einfühlungsvermögen, Werte und ohne „gesunden Menschenverstand" bleibt KI im Ergebnis aber momentan noch ein – wenngleich „intelligentes" – Werkzeug.

12.1.2 Strategische Förderung der KI-Entwicklung

12.1.2.1 Bayern

Mit der im April 2019 verkündeten Strategie BAYERN DIGITAL positioniert die Staatsregierung Bayern als Leitregion für Digitales. Das Programm umfasst ein Investitionsvolumen von sechs Milliarden Euro bis 2022 und wird kontinuierlich weiterentwickelt. In einer Regierungserklärung veröffentlichte der Bayerische Ministerpräsident Dr. Markus Söder im Oktober 2019 die „Hightech Agenda Bayern" mit einem Investitionsvolumen von zwei Milliarden Euro.

Davon sollen Teile in den Ausbau eines landesweiten KI-Forschungsnetzes („KI-District Bayern") und die Schaffung von 100 KI-Professuren fließen. In München soll ein KI-Zentrum von Weltrang mit dem Schwerpunkt intelligente Robotik etabliert werden, aber auch weitere KI-Spitzenzentren mit klaren Kompetenzschwerpunkten sind geplant, wie etwa in Würzburg (Data Science) oder Nürnberg (Anwendung neuer KI-Felder).

KI-Forschungskompetenzen sollen auch an regionalen Standorten gestärkt werden, so in Kempten (Pflege), Schweinfurt (Robotik), Deggendorf (Anwendungen für kleine oder mittlere Unternehmen und Landwirtschaft), Aschaffenburg (Medizin). Neben der Stärkung der Informatik als Fach an allen Hochschulen soll das Leibniz-Rechenzentrum zum informationstechnischen Kompetenzknoten für Big Data und KI ausgebaut werden.

12.1.2.2 Bundesweite KI-Strategie

Die Bundesregierung präsentierte im November 2018 eine nationale Strategie Künstliche Intelligenz[36] mit der sie die wesentlichen Rahmenbedingungen vorgibt. Die Strategie ist als „lernend" angelegt, die es kontinuierlich gemeinsam durch einen umfassenden demokratischen Prozess und Diskurs in Politik, Wissenschaft, Wirtschaft und Zivilgesellschaft zu justieren gilt. Es geht dabei um die Auseinandersetzung mit individuellen Freiheits- und Persönlichkeitsrechten, Hoffnungen und Ängsten auf der einen Seite, aber auch den Potenzialen und Erwartungen für deutsche Unternehmen, den weltweiten Wettbewerb auf der anderen Seite. So zielt sie darauf ab, „KI Made in Germany" zu einem internationalen Markenzeichen für moderne, sichere KI auf Basis des europäischen Wertekanons zu etablieren.

12.1.2.3 Datenethikkommission

Die Auswirkungen von Künstlicher Intelligenz auf Wirtschaft und Gesellschaft werden als von so grundlegender Bedeutung eingeschätzt, dass sich unter anderem auch die Datenethikkommission der Bundesregierung auf ihrer öffentlichen Tagung am 7. Februar 2019 dem Thema „Selbst- und Fremdbestimmung im Zeitalter künstlicher Intelligenz" und damit verbundenen, aktuellen technosozialen Entwicklungen widmete. Ihre wesentlichen Überlegungen hat die Datenethikkommission mittlerweile in einem Gutachten niedergelegt.[37]

12.1.3 Künstliche Intelligenz und Datenschutz

12.1.3.1 Nutzung von personenbezogenen Daten

Künstliche Intelligenz gilt als Innovationstreiber und Wachstumschance. Sie kann als sinnvolles Hilfsmittel die Arbeits- und Lebenswelt gewinnbringend verändern. Sie kann insbesondere stupide, repetitive Aufgaben übernehmen, bei Entscheidungsfindungen, Korrekturen, Einschätzungen, Recherchen oder Auswertungen unterstützen, Prozesse beschleunigen und völlig neue Unterstützungsmöglichkeiten in verschiedenen Lebensbereichen eröffnen. Dabei profitiert sie von vorausgehenden und aktuellen Entwicklungen der Digitalisierung wie etwa der zunehmenden Verbreitung vernetzter elektronischer Geräte und der Leistungssteigerung von Datenübertragung, -speicherung und -berechnung.

Wie viele andere Technologien birgt KI allerdings auch schwer einschätzbaren Risiken – sowohl direkt auf den verschiedenen Ebenen und Prozessschritten der Verarbeitung und den dadurch getroffenen Entscheidungen als auch indirekt durch möglicherweise entstehende Ungerechtigkeiten sowie soziale, wirtschaftliche und kulturelle (Seiten-)Effekte.

Umfangreiche Datenerhebungen stellen die Grundlage für statistische Erkenntnisgewinne und deren Qualität dar: Je mehr Datensätze und je größer die Stichprobe, desto verlässlichere Aussagen und Erkenntnisse können erzielt werden

[36] Bundesministerium für Bildung und Forschung, Strategie Künstliche Intelligenz der Bundesregierung, Stand 11/2018, Internet: https://www.ki-strategie-deutschland.de, Rubrik „Downloads".

[37] Datenethikkommission der Bundesregierung, Gutachten der Datenethikkommission , Stand 10/2019, Internet: https://www.bmi.bund.de, Rubrik „Themen – IT und Digitalpolitik – Datenethikkommission – Arbeitsergebnisse der Datenethikkommission".

und desto kleinere Fehlerraten sind möglich. Dieser grundsätzliche Zusammenhang gilt analog für das Training und den Einsatz Künstlicher Intelligenz. So ist es verständlich, dass bei Entwicklern und Betreibern leistungs- und konkurrenzfähiger KI-Systeme ein enormer Datenhunger besteht. Soweit personenbezogene Daten verarbeitet werden, regelt allerdings insbesondere die Datenschutz-Grundverordnung den Schutz der Betroffenen und schützt deren digitaler Bürgerrechte und Freiheiten. So kommt es vor, dass Datenschutz im KI-Umfeld als Hindernis und unnötiger Kostenfaktor wahrgenommen wird. Regulierungsgegner sprechen dann vereinzelt von „Sand im Getriebe" eines ansonsten leistungsfähigen Innovations- und Wachstumsmotors und verweisen auf den Vorsprung anderer Nationen wie etwa der Vereinigten Staaten von Amerika oder der Volksrepublik China.

Das ist aber nicht der europäische Weg. Dieser besteht in der Entwicklung von KI, die im Einklang mit den zentralen europäischen Grundwerten steht. Dazu gehört u.a. die Achtung der Menschenwürde. Diesem Weg einer menschenzentrierten KI hat sich die Staatsregierung ausdrücklich angeschlossen.

Auch die Bundesregierung betont bereits im Eckpunktepapier der Strategie Künstliche Intelligenz die Datenschutz-Grundverordnung als „einen verlässlichen gesetzlichen Rahmen für innovative Technologien und Anwendungen auch im Bereich der KI. Sie enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten"[38]. So schaffe der Datenschutz erst kontrollierte und kontrollierbare Bedingungen, unter denen KI grundsätzlich sicher und fair genutzt werden kann, ohne dass schutzwürdige Interessen, Rechte und Freiheiten verletzt oder gefährdet werden.

Hier wird Datenschutz nicht als Wettbewerbsnachteil, sondern als Qualitätsmerkmal und damit als Chance und als Wettbewerbsvorteil gesehen. „KI made in Germany" respektive „in Europa" soll als Qualitätssiegel Produkte und Dienstleistungen aufwerten. Die eventuell initial höheren Kosten für die Einhaltung des Datenschutzes bei der Verarbeitung der Daten können dabei durch das größere Vertrauen und die in der Folge zu erwartende schnellere und breitere Akzeptanz am Markt zumindest ausgeglichen werden.

So zielt der europäische Weg nicht auf ein hemmendes Gegeneinander zwischen KI-Entwicklung und Datenschutz, sondern auf ein ausgeglichenes Miteinander ab, wobei sichergestellt sein muss, dass rechtliche Regelungen eingehalten werden. Die Datenschutz-Aufsichtsbehörden in Deutschland und Europa arbeiten auf verschiedenen Ebenen und möglichst gemeinsam mit Vertretern der Wirtschaft an der Umsetzung der gesetzlichen Regelungen in konkrete technische Anforderungen für KI-Systeme.

12.1.3.2 Kernpunkte und Herausforderungen

Das Recht auf Löschung (Art. 17 DSGVO, „Recht auf Vergessenwerden") lässt sich im Fall von einmal ins Training der KI eingeflossenen personenbezogenen Daten möglicherweise kaum umsetzen, ohne die KI zurückzusetzen und neu zu trainieren, was oft nicht wirtschaftlich umsetzbar ist. Deshalb ist insbesondere Art. 5 Abs. 1 Buchst. c DSGVO („Datenminimierung") genau zu beachten, insbesondere wenn eine konkrete Verarbeitung von personenbezogener Details weder

[38] Bundesregierung, Eckpunkte der Bundesregierung für eine Strategie Künstliche Intelligenz, veröffentlicht mit Pressemitteilung des Bundesministeriums für Bildung und Forschung vom 18. Juli 2018, Internet: https://www.bmbf.de, Rubrik „Presse".

für die Erledigung der Aufgabe einer KI noch deren Training nötig ist. Beispielsweise muss eine KI für die optische Beurteilung einer Gewebeprobe auf Anzeichen für Krebs nicht zwingend sonstige personenbezogene Daten kennen. Sollte das Alter der betroffenen Person relevant für eine bessere Einschätzung der Probe sein, so ist möglicherweise das Geburtsjahr ausreichend und es muss nicht das exakte Geburtsdatum verwendet werden. Für das Training von selbstfahrenden Autos sind Videodaten erforderlich – trotzdem ist es für das Erlernen der Fahrfähigkeit nicht immer erforderlich, dass Gesichter menschlicher Verkehrsteilnehmer erkennbar sind.

Auch wenn die Trainingsdaten vorab pseudonymisiert worden sind, kann es sein, dass durch die schiere Menge an Datenpunkten derselben Person, diese wieder eindeutig zugeordnet und so die Pseudonymisierung wieder rückgängig gemacht werden kann. Darüber hinaus können selbst bei vollständiger Anonymisierung durch eine (bewusste oder unbewusste) Ungleichgewichtung bei der Auswahl der Trainingsdaten (sog. Bias) in der Folge unerwünschte oder unzulässige Diskriminierungseffekte auftreten.

Insbesondere bei Datenverarbeitungen in der öffentlichen Verwaltung ist bei Künstlicher Intelligenz des Weiteren das Recht jedes Betroffenen zu beachten, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt (Art. 22 Abs. 1 DSGVO).

Zudem hat der Betroffene nach Art. 12 DSGVO das Recht auf transparente Information und Kommunikation. Einzelentscheidungen fällt eine Künstliche Intelligenz jedoch typischerweise wie eine „Blackbox“, das heißt, es ist nicht von außen einseh- oder nachvollziehbar, wie sie zu einer Entscheidung gekommen ist, sie liefert keine Begründung oder Kommentar, sondern präsentiert nur das Ergebnis oder handelt danach. Worauf sie die Entscheidung im Einzelfall konkret stützt, lässt sich zwar aufgrund der Trainingsdaten mutmaßen , doch es gibt Fälle, bei denen KIs in zwar für Menschen als praktisch identisch wahrgenommenen Fällen völlig anders entscheiden. Gerade dann wäre eine Erklärung wünschenswert – oder sogar notwendig – wie es zu der konkreten Entscheidungsfindung gekommen ist. Nur so können Betroffene und Verantwortliche beurteilen, ob die Entscheidung auf angemessenen „Erwägungen“ beruht oder auf einer Fehlgewichtung von Faktoren, die sich letztlich auf die Betroffenen diskriminierend auswirken. Aus Gründen der Transparenz und Nachvollziehbarkeit muss daher insbesondere vermehrt an KI mit erklärbarem und nachvollziehbarem Verhalten (sog. „explainable AI“) geforscht werden.

12.1.4 Umfangreiche Gremienarbeit

Die Relevanz des Themas in Politik und Gesellschaft, der enge Bezug zum Datenschutz, wenn personenbezogene Daten verarbeitet werden, und die zukünftig wohl wachsende Verbreitung der Technologie auch im behördlichen Bereich veranlasste mich dazu, bestehende Kompetenzen in diesem Bereich auszubauen und mich sowohl beobachtend als auch konstruktiv auf mehreren Ebenen an Entwicklungen in diesem Bereich zu beteiligen.

12.1.4.1 Auf internationaler Ebene

Auf der 40. Internationalen Konferenz der Beauftragten für Datenschutz und Privatsphäre (ICDPPC) in Brüssel wurde eine Erklärung zu Ethik und Datenschutz im Bereich der Künstlichen Intelligenz verabschiedet. Diese definiert Ziele und Aufgaben einer zu bildenden, ständigen Arbeitsgruppe (ICDPPC Working Group on Artificial Intelligence), die sich mit den Herausforderungen durch die Entwicklung Künstlicher Intelligenzen befasst. Diese Arbeitsgruppe soll das Verständnis und die Einhaltung der Grundsätze dieser Entschließung durch alle an der Entwicklung von Systemen Künstlicher Intelligenz beteiligten Kreise fördern. Diese internationale Konferenz ist bestrebt, eine aktive öffentliche Debatte über digitale Ethik zu unterstützen, die auf die Schaffung einer stabilen ethischen Kultur und eines starken persönlichen Bewusstseins in diesem Bereich abzielt, weshalb ich mich an dieser Arbeitsgruppe beteiligt habe.

Nachdem im Januar 2019 die konstituierende Telefonkonferenz stattfand, nahmen bisher bis zu 19 Delegationen und Beobachter von Mitgliedern an der Arbeit der Arbeitsgruppe teil oder haben zumindest Interesse bekundet, zukünftig beizutreten.

Unter dem Vorsitz des Europäischen Datenschutzbeauftragten, der französischen Aufsichtsbehörde CNIL und des Privacy Commissioner for Personal Data Hongkong umfasste das Arbeitsprogramm der Arbeitsgruppe unter anderem:

- die Einrichtung gemeinsamer Sammlungen von Richtlinien und Grundsätzen zu KI, Datenschutz und Ethik sowie realen Fällen von Anwendungen der KI-Technologie, die für Ethik und Datenschutz relevant sind,
- die Vorbereitung von Erklärungen zum Verhältnis zwischen Ethik, Menschenrechten und Datenschutz im Bereich KI sowie über die wesentliche Notwendigkeit der Klärung von Fragen zur Rechenschaftspflicht und zu Haftungsfragen,
- die Vorbereitung einer Risikoanalyse für die Erhebung personenbezogener Daten aufgrund von Befangenheit und Diskriminierung und
- eine „Gap-Analyse“ zur Entwicklung der Kapazitäten und Fachkenntnisse der Datenschutz-Aufsichtsbehörden für die Bearbeitung ethischer und datenschutzrechtlicher Fragen bei der Anwendung von KI-Systemen.

12.1.4.2 Auf europäischer Ebene

Die europäische Kommission hat die Expertengruppe „High-Level Expert Group on Artificial Intelligence“ beauftragt, ethische Richtlinien für sog. „vertrauenswürdige“ Künstliche Intelligenz (Trustworthy AI) zu erstellen.

Diese Expertengruppe hat zur Weichenstellung der künftigen Entwicklungen und Verwendung von KI einen Entwurf dieser Richtlinien verfasst, mit dem sie die Haltung der Europäischen Union gegenüber diesem Thema begründet. Dieser Entwurf wurde Ende 2018 veröffentlicht und bis Januar 2019 der breiten Öffentlichkeit Zeit für Feedback gegeben. Der Entwurf durchläuft derzeit einen Anpassungsprozess der in ein Abschlussdokument münden und Anfang 2020 vorgestellt werden soll.

Auch wenn ich selbst nicht Teil der Expertengruppe bin, habe ich doch die Gelegenheit genutzt, den Entwurf auf Datenschutz-Aspekte hin zu prüfen und zu kommentieren. Der Entwurf befasst sich ausführlich mit erforderlichen Eigenschaften und Richtlinien für „vertrauenswürdige" Künstliche Intelligenz und behandelt dabei unter anderem die unter Nr. 12.1.3.2 genannten Kernpunkte und Herausforderungen.

12.1.4.3 Auf nationaler Ebene

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat eine Taskforce „Künstliche Intelligenz" gebildet, an der ich mich ebenfalls beteiligt habe. Diese Taskforce bündelt Ressourcen und Kompetenzen, um qualifizierte und konstruktiv kritische Sichtweisen auf diese komplexe Technologie zu erarbeiten – mit besonderem Fokus auf dem Datenschutz sowie möglichen Risiken für die Rechte und Freiheiten betroffener Personen.

Hambacher Erklärung In diesem Zusammenhang wurde die „Hambacher Erklärung zur Künstlichen Intelligenz" (siehe Anlage 1) verabschiedet. Sie nennt beispielhaft den Einsatz von KI-Systemen in der Medizin, insbesondere in der Diagnose, in der Sprachassistenz und bei der Bewertung von Bewerbungsunterlagen in der Bewerberauswahl. Aus dem geltenden Datenschutzrecht werden sieben Anforderungen für KI-Systeme abgeleitet. So muss der Einsatz von KI-Systemen nachvollziehbar und erklärbar sein, den Grundsatz der Datenminimierung enthalten, Diskriminierungen vermeiden und benötigt technische und organisatorische Standards. Die Datenschutzaufsichtsbehörden wollen die Entwicklung begleiten und fordern Wissenschaft, Politik und Anwender auf, die Entwicklung von KI im Sinne des Datenschutzes zu steuern. Im Kern geht es darum, dass am Ende Menschen und nicht Maschinen über Menschen entscheiden.

Die Erklärung wurde auf der 97. Konferenz am 3. und 4. April 2019 auf dem Hambacher Schloss vorgestellt. Der historische Ort des Kampfes um die Freiheit war insofern passend, den Willen der Datenschutz-Aufsichtsbehörden zu verdeutlichen, für einen effektiven Grundrechtsschutz einzutreten und ihren Beitrag zur Sicherung von Freiheit in der digitalen Welt zu leisten.

Positionspapier der DSK Bei der Arbeit der Taskforce und dem gemeinsamen Verfassen der Erklärung wurde insbesondere Bedarf festgestellt, die rechtlichen Vorgaben der Datenschutz-Grundverordnung in technische Anforderungen für KI-Verfahren, deren Einsatz und Entwicklung umzusetzen. So wurde nach der 2. Sitzung der Taskforce „Künstliche Intelligenz" der Arbeitskreis Technik gebeten, Vorschläge für technische und organisatorische Ansätze zu erarbeiten, mit denen ein angemessener Datenschutz gewährleistet werden kann, insbesondere hinsichtlich der Erklärbarkeit, Transparenz und Nachvollziehbarkeit, der Beherrschbarkeit und Kontrollierbarkeit sowie von Datengrundlagen, Datenminimierung und Datensparsamkeit.

Die zur Umsetzung dieses Arbeitsauftrags vom Arbeitskreis Technik eingesetzte Unterarbeitsgruppe KI befasste sich daraufhin im Detail mit den Lebenszyklen eines KI-Systems: Designs des KI-Systems, Veredelung von Rohdaten zu Trainingsdaten, Training der KI-Komponenten, Validierung der Daten und KI-Komponenten sowie des KI-Systems, Einsatz des KI-Systems und die Rückkopplung von Ergebnissen werden am Maßstab von Gewährleistungszielen untersucht.

Mit dem im November 2019 veröffentlichten Positionspapier[39] der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen soll Verantwortlichen im Umfeld von KI ein konkreter und verbindlicher Handlungsrahmen für die datenschutzrechtlichen Vorgaben an die Hand gegeben werden. Es soll verdeutlichen, dass der Einsatz von KI-Systemen und der Datenschutz vereinbar sind. Chancen und Möglichkeiten des Einsatzes von KI-Systemen werden durch Datenschutz nicht von vornherein verhindert. Damit wird Handlungssicherheit gesteigert und sichergestellt, dass das Grundrecht auf informationelle Selbstbestimmung auch in dem dynamischen, von KI-Systemen geprägten Umfeld gewahrt wird. Das Positionspapier soll auch den Dialog mit den relevanten Akteurinnen und Akteuren aus Politik, Wirtschaft, Wissenschaft und Gesellschaft wie den Verbrauchervereinigungen weiter intensivieren helfen.

12.1.5 Zusammenfassung und Ausblick

Künstliche Intelligenz beginnt sich als neue Technologie in Wirtschaft und Gesellschaft zu etablieren und ist bereits jetzt in einigen Bereichen kaum mehr wegzudenken. Aufgrund der umfangreichen Verarbeitung auch personenbezogener Daten bei Training und Einsatz von KIs und ihres steigenden Entscheidungs- und Handlungsspielraums wird der Datenschutz besonders relevant. Die Auseinandersetzung mit der Technologie offenbart jedenfalls eine Reihe von Risiken und Herausforderungen, die Fähigkeiten und Wachstumspotenziale mit geltendem (Datenschutz-)Recht in Einklang zu bringen. Daher werde ich mich auch weiterhin auf internationaler, europäischer und nationaler Ebene in Arbeitsgruppen beteiligen, um konstruktive Lösungen und Vorgaben für die Vereinbarkeit von KI und Datenschutz zu erarbeiten. Faire und sichere KI erhält so die Chance, sich als Vorbild mit dem Wettbewerbsvorteil Vertrauenswürdigkeit („Trustworthy AI“) auch über EU-Grenzen hinaus zu etablieren.

12.2 Aktuelles zur Datenschutz-Folgenabschätzung (DSFA)

Die Datenschutz-Grundverordnung richtet die vom Verantwortlichen zu treffenden technischen und organisatorischen Maßnahmen an den Risiken aus, die eine Verarbeitung für die Rechte und Freiheiten natürlicher Personen mit sich bringt. Das wird in den Bestimmungen der Art. 24 Abs. 1, Art. 25 Abs. 1 und Art. 32 Abs. 1 DSGVO deutlich. Die in Art. 35 DSGVO geregelte Datenschutz-Folgenabschätzung (DSFA, dazu bereits mein 28. Tätigkeitsbericht 2018 unter Nr. 3.1.3) ist ein Verfahren, in welchem Risiken strukturiert ermittelt und bewertet sowie Gegenmaßnahmen festgelegt werden.

Bayerische öffentliche Stellen sind grundsätzlich zur Durchführung von Datenschutz-Folgenabschätzungen verpflichtet, wenn sie Verarbeitungen personenbezogener Daten durchführen, die von der **Bayerischen Blacklist** erfasst sind.[40] Bei

[39] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, Stand: 11/2019, Internet: https://www.datenschutzkonferenz-online.de, Rubrik „Infothek – Entschließungen“.

[40] Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz-Folgenabschätzung – Bay-

anderen Verarbeitungen müssen bayerische öffentliche Stellen individuell prüfen, ob eine Datenschutz-Folgenabschätzung erforderlich ist. Über diese Prüfung sowie zum Instrument der Datenschutz-Folgenabschätzung im Allgemeinen informiert eine **Orientierungshilfe**.[41]

Die **Methodik der Datenschutz-Folgenabschätzung** ist in einem gesonderten **Arbeitspapier** näher erläutert. Hier erfahren bayerische öffentliche Stellen Näheres über die Arbeitsschritte und über Hilfsmittel, die bei einer Datenschutz-Folgenabschätzung eingesetzt werden können. Das Arbeitspapier veranschaulicht die methodische Einführung an einer Fallstudie zu der Verarbeitungstätigkeit „Personal verwalten" aus der Stadt Fiktivia.[42]

Eine Datenschutz-Folgenabschätzung (englisch: Privacy Impact Assessment – PIA) lässt sich methodisch gut mit dem sog. **PIA-Tool** durchführen, einer von der französischen Datenschutz-Aufsichtsbehörde Commission Nationale de l'Informatique et des Libertés (CNIL) bereitgestellten Software, die kontinuierlich weiterentwickelt wird.[43] Ergänzend zum PIA-Tool habe ich **weitere Werkzeuge** bereitgestellt, die einzelne Arbeitsschritte der Datenschutz-Folgenabschätzung erleichtern sollen. Der Einsatz dieser Werkzeuge ist in dem Arbeitspapier „Datenschutz-Folgenabschätzung – Methodik und Fallstudie" näher beschrieben. Es stehen jeweils Leerformulare zur Verfügung sowie Ausfüllbeispiele, die sich auf die Fallstudie aus dem Arbeitspapier beziehen.[44]

Insgesamt können bayerische öffentliche Stellen nun auf detaillierte Anleitungen und Hilfsmittel zurückgreifen, wenn sie Datenschutz-Folgenabschätzungen durchführen müssen. Das Angebot harmoniert mit dem neuen IT-Grundschutz-Baustein „CON.2 Datenschutz" des Bundesamts für Sicherheit in der Informationstechnik[45] sowie mit dem Standard-Datenschutzmodell (SDM)[46].

Zur Durchführung einer Datenschutz-Folgenabschätzung erhalte ich regelmäßig Fragen, die ich gerne beantworte. Darunter befinden sich auch einige Grundsatzfragen:

— **Falls eine Verarbeitung keine Datenschutz-Folgenabschätzung erfordert: Ist dann die gesamte DSFA-Thematik unbedeutend?**

erische Blacklist – Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DSGVO für den bayerischen öffentlichen Bereich, Internet: https://www.datenschutz-bayern.de, Rubrik „DSFA".

41 Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz-Folgenabschätzung, Orientierungshilfe, Stand 3/2019, Internet: https://www.datenschutz-bayern.de, Rubrik „DSFA".

42 Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz-Folgenabschätzung – Methodik und Fallstudie, Stand 10/2019, Internet: https://www.datenschutz-bayern.de, Rubrik „DSFA".

43 Nähere Erläuterungen und Download des PIA-Tools auf https://www.datenschutz-bayern.de, Rubrik „DSFA".

44 Einzelheiten auf https://www.datenschutz-bayern.de, Rubrik „DSFA".

45 Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutz-Baustein CON.2 Datenschutz, Internet: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompendium/bausteine/ CON/CON_2_Datenschutz.html.

46 Das Standard-Datenschutzmodell beschreibt eine Methode zur Datenschutzberatung und -prüfung auf Basis einheitlicher Gewährleistungsziele; weiterführende Informationen zu diesem Modell sind etwa auf https://www.datenschutz-mv.de in der Rubrik „Datenschutz – Standard-Datenschutzmodell zu finden.

Auch wenn eine Datenschutz-Folgenabschätzung im Einzelfall nicht erforderlich ist, muss die betrachtete Verarbeitung dennoch mit der Datenschutz-Grundverordnung in Einklang stehen. Das muss nachgewiesen werden können (Art. 5 Abs. 2 DSGVO). Die Datenschutz-Folgenabschätzung dient dem Zweck, Risiken zu erkennen, zu bewerten und zu minimieren. Wissen über die Methodik der Datenschutz-Folgenabschätzung hilft deshalb stets, Verarbeitungen sicher einzurichten.

— **Falls eine DSFA-pflichtige Verarbeitung nach wirksamer Umsetzung von geeigneten technischen und organisatorischen Maßnahmen datenschutzrechtlich sicher betrieben werden kann: Spielt dann die DSFA-Thematik keine Rolle mehr?**

Das Ausgangsrisiko der betrachteten Verarbeitung, nicht das Restrisiko ist für die Beantwortung der Frage relevant, ob „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen" besteht. Folglich ist für die Beurteilung, ob für einen bestimmten Verarbeitungsvorgang eine Datenschutz-Folgenabschätzung erforderlich ist, das Risiko der Verarbeitung zu analysieren, das besteht, bevor technische und organisatorische Maßnahmen festgelegt und umgesetzt wurden.[47]

— **Wie sollte ein Team zusammengesetzt sein, das eine Datenschutz-Folgenabschätzung durchführt?**

Festes Teammitglied ist zunächst eine **Vertreterin oder ein Vertreter des Verantwortlichen**, der die Datenschutz-Folgenabschätzung durchführt (vgl. Art. 35 Abs. 1 DSGVO). Weitere Teammitglieder sollten Fachkunde für die Themen „Prozesse der Verarbeitung", „technische Systeme und Dienste" sowie „verarbeitete personenbezogene Daten" einbringen.[48] Daher sollten vertreten sein: das **Sachgebiet**, das den betroffenen **Geschäftsprozess** inklusive der darin verarbeiteten personenbezogenen Fachdaten **verantwortet**, das **Sachgebiet**. das für die **IT-Unterstützung** des betroffenen Geschäftsprozesses **zuständig** ist, sowie gegebenenfalls ein **Sachgebiet** mit besonderer **Fachkunde im Datenschutzrecht**.

Die oder der **behördliche Datenschutzbeauftragte** kann im Einzelfall ein Mitglied des Teams sein oder bei Bedarf zugezogen werden. Dabei kann seine Beratungsleistung unterschiedlich ausgeprägt sein. Zu beachten ist, dass die oder der behördliche Datenschutzbeauftragte entsprechend seinem gesetzlichen Auftrag eine **Beratungsleistung** erbringt. Die Arbeit eines DSFA-Teams darf nicht darauf hinauslaufen, dass die oder der behördliche Datenschutzbeauftragte die für eine Datenschutz-Folgenabschätzung erforderlichen Dokumente entwirft und die übrigen Teammitglieder Meinungsäußerungen dazu abgeben. Die Datenschutz-Folgenabschätzung ist Sache des Verantwortlichen; die Mitwirkung der oder des behördlichen Datenschutzbeauftragten dient der Qualitätssicherung. Davon abge-

47 Siehe auch Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Standard-Datenschutzmodell, Version 2.0 vom 7. November 2019, S. 45 (Internet: siehe Fn. 46).

48 Standard-Datenschutzmodell (Fn. 46), S. 38 f.

sehen ist die oder der behördliche Datenschutzbeauftragte Verbindungsperson zur Datenschutz-Aufsichtsbehörde (vgl. Art. 39 Abs. 1 Buchst. d und e DSGVO).

— **Muss jede Stelle ihre eigene Datenschutz-Folgenabschätzung durchführen oder kann eine schon existierende Datenschutz-Folgenabschätzung einer anderen Stelle oder eines IT-Lieferanten verwendet werden?**

Die Nutzung von Synergieeffekten bei der DSFA-Durchführung ist nicht nur erlaubt (siehe etwa Art. 35 Abs. 1 Satz 2 DSGVO, Art. 14 Abs. 2 BayDSG), sondern aus Gründen einer datenschutzrechtlichen Standardisierung mit einhergehender höherer Qualität auch geboten.

Im Bereich der bayerischen öffentlichen Stellen gibt es zahlreiche vergleichbare oder sehr ähnliche Verarbeitungsvorgänge und damit eine Grundlage, jeweils eine Datenschutz-Folgenabschätzung als „Blaupause" zu erstellen und dann diese für mehrere Stellen zu verwenden. Da bei digitalisierten Verarbeitungsvorgängen alle drei gerade genannten SDM-Komponenten „Daten", „System" und „Prozess" für die Wiederverwendung einer Datenschutz-Folgenabschätzung hinreichend ähnlich sein müssen, wird oft noch die DSFA-Blaupause an die örtlichen Gegebenheiten der betrachteten Verarbeitung anzupassen sein. Trotzdem birgt dieses Vorgehen ein großes wirtschaftliches und qualitatives Potenzial.

Der Schlüssel für die Realisierung dieses Synergiepotenzials liegt bei den Herstellern relevanter IT-Systeme, bei den Stellen mit Federführung für die fachliche Gestaltung zentraler Fachverfahren sowie bei der koordinierten Zusammenarbeit und dem zielorientierten Austausch betroffener Stellen. Bei der Beschaffung von IT-Systemen sollten bayerische öffentliche Stellen stets prüfen, ob DSFA-Blaupausen benötigt werden. Ist dies der Fall, sollte dies bei der Formulierung der entsprechenden Ausschreibungstexte beachtet werden.

12.3 Emotet, Ransomware und andere Schadsoftware

Der Begriff Schadsoftware umfasst jegliche Art von ausführbarem Code, der unerwünschte Folgen für Nutzerinnen und Nutzer oder die von ihnen verarbeiteten Daten auslösen kann.

Während es sich bei Adware primär um ungewollte Einblendungen von Werbeanzeigen handelt, zielt Spyware bewusst auf das Entwenden von Zugangsdaten (etwa durch Passwortdiebstahl mittels Keylogger) oder andere kriminell verwertbare Daten ab. Im Sprachgebrauch am häufigsten genutzt wird der Begriff Virus, dessen Hauptziel die Infektion von Dateien und die eigene Verbreitung ist. Im Unterschied dazu versuchen Computerwürmer, sich selbst direkt über anfällige Netzwerkservices zu verbreiten. Eine Sonderform der Schadsoftware ist das Trojanische Pferd (Trojaner). Hier werden schadhafte Funktionen in einem vorgeblich nützlichen Programm oder einer unverdächtigen Datei versteckt, die das Opfer zur Ausführung oder zum Öffnen verleiten soll. Diese verdeckte, schadhafte Funktion kann eine der vorgenannten Formen haben, meist wird jedoch zuerst eine sogenannte Backdoor (Hintertür) geöffnet, die Angreifern einen oft unbemerkten Zugriff auf den Rechner ermöglicht. Über Backdoors können infizierte Rechner in

Botnetze (unbemerkter Zusammenschluss vieler infizierter Rechner unter Kontrolle eines Angreifers) integriert werden, die zu unterschiedlichen Zwecken missbraucht werden können. Beispielsweise nutzen Cryptominer die Rechenleistung, um auf Kosten der Opfer Cryptowährung zu schürfen.

Neben den genannten vielseitigen Formen von Schadsoftware wies ich bereits in meinem 27. Tätigkeitsbericht 2016 unter Nr. 2.1.2 auf die Gefahren von Ransomware hin. Dabei handelt es sich um Schadprogramme, die Daten unerwünscht verschlüsseln und so den Zugriff im Rahmen eines Erpressungsversuches verhindern. Der Name setzt sich aus den englischen Wörtern Ransom (Lösegeld) und Software zusammen.

Neben Privatpersonen und Unternehmen zählen insbesondere auch staatliche Behörden, Kommunen und deren Einrichtungen zu den Angriffszielen. Bayerische öffentliche Stellen meldeten hierzu auch im Jahr 2019 eine relevante Anzahl von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DSGVO.

Bereits 2016 machte ich darauf aufmerksam, dass die Kommunikation per E-Mail ein Haupteinfallstor eröffne. Dies bestätigen die mir gemeldeten Fälle, in denen die Einschleusung in der Regel durch infizierte E-Mail-Anhänge erfolgte. Auffällig ist, dass die Angriffe inzwischen deutlich an Qualität gewonnen haben: Die schadhaften E-Mails sind immer besser getarnt und damit zum Teil sehr schwer von „normalen" E-Mails zu unterscheiden. Als Absender sind bekannte Kommunikationspartner angegeben. Häufig werden infizierte Anhänge wie etwa fiktive Rechnungen, Bestellbestätigungen, Bewerbungen, von einem Multifunktionsdrucker eingescannte Dokumente und dergleichen verschickt. Ebenso können auch Links auf schadhafte Webseiten oder Verweise auf vermeintlich herunterzuladende Dokumente aus einem Cloud-Speicher übermittelt werden. Werden diese Anhänge oder Links geöffnet, startet im Hintergrund die Installation der Schadsoftware. Diese wird zumeist von einem Server aus dem Internet nachgeladen.

Besonders häufig erfolgten 2019 Angriffe mittels „Emotet". Diese Schadsoftware ist sehr wandelbar und zudem in der Lage, besonders authentisch aussehende schadhafte E-Mails zu verschicken. Dazu liest die Schadsoftware Empfänger und Absender von bestehenden Kommunikationsverläufen sowie deren Inhalte auf bereits infizierten Rechnern aus und verwendet diese Informationen selbständig zur Weiterverbreitung. Auf diesem Weg erhalten die noch nicht betroffenen Empfängerinnen und Empfänger fingierte E-Mails von Absenderinne und Absendern, mit denen sie bereits in Kontakt standen. Gerade wenn dieser Kontakt erst kürzlich erfolgte, senkt dies die Hürde zum ungeprüften Öffnen der E-Mail oder der Anhänge. Insbesondere dadurch ist diese Angriffsmethode besonders erfolgreich.

Ist ein Befall mit Emotet erfolgt, greift die Schadsoftware zuerst vorhandene Kontaktdaten für die Weiterverbreitung ab. Zudem können durch Nachladen weiterer Schadsoftware wie „Trickbot" Active-Directory-Benutzerdaten (zentraler Benutzer-Verzeichnisdienst) angegriffen werden, um weiteren Schaden im lokalen Netzwerk zu verursachen. Insbesondere die gesamte Benutzerauthentifizierung – nicht nur die auf dem Rechner, auf dem der Schadcode entdeckt wurde – muss dann als kompromittiert betrachtet werden.

Da der eigentliche Schadcode gegebenenfalls erst zu einem späteren Zeitpunkt nachgeladen wird, bleibt Emotet auch bei aktivem Virenscanner regelmäßig lange unentdeckt und kann sich so getarnt auf den angegriffenen Systemen dauerhaft einnisten. Auch der Versuch einer Bereinigung ist daher oft nicht erfolgreich, so

dass nur eine vollständige Neuinstallation zumindest der betroffenen Rechner eine vollständige Entfernung sicherstellt. Der nachgeladene Schadcode kann sowohl Ransomware als auch andere der genannten Schadsoftwarekategorien beinhalten.

Die folgenden Vorbeugemaßnahmen gegen Schadsoftware im Allgemeinen sollten umgesetzt werden. Sowohl Nutzerinnen und Nutzer als auch Administratorinnen und Administratoren sind hier gefordert:

- Regelmäßige Backups von Daten verhindern, dass Daten komplett verloren gehen. Der technische Zugriff auf das jeweilige Backup sollte nur zum Zeitpunkt der Erstellung bestehen, da die Schadsoftware sonst das Backup verschlüsseln, korrumpieren oder löschen kann. Backups sind regelmäßig auf Vollständigkeit zu prüfen.

- Aktuelle Betriebssystemversionen und ein regelmäßiges und zeitnahes Einspielen von Updates und Patches sind unabdingbar. Dabei muss regelmäßig überprüft werden, ob alle Updates/Patches erfolgreich eingespielt werden konnten und eventuell auftretende Probleme behoben werden. Es muss jederzeit nachweisbar sein, welchen Versionsstand die vorhandenen IT-Systeme haben.

- Ebenso wichtig sind aktuell gehaltene Virenscanner auf Clients und Servern. Dabei kann es sinnvoll sein, mehrstufiges Konzept mit unterschiedlichen Produkten zu wählen, um eine möglichst große Anzahl von Schadcode abfangen zu können. Ich weise allerdings vorsorglich darauf hin, dass auch dies keinen vollständigen Schutz darstellt, da gerade auch Emotet sehr variabel ist und unter Umständen im Antivirusprogramm noch keine aktuelle Virensignatur vorliegt.

- Nutzer sollten nur mit den minimal benötigten Rechten – und insbesondere nicht mit Administratorrechten – arbeiten.

- Eine Netzwerksegmentierung kann verhindern, dass Schadsoftware sich auf das gesamte Netzwerk ausbreiten kann.

- Wann immer möglich, sind Makros in Office-Dokumenten zu deaktivieren und nur sicherere Formate ohne Makros zu benutzten (etwa „.docx“).

- Das automatische Nachladen externer Inhalte sowie Links sollten deaktiviert werden.

- Die Standard-Einstellungen in E-Mail-Programmen sollten so gewählt sein, dass E-Mails im Nur-Text-Modus gelesen und gesendet werden (keine HTML-E-Mails).

- E-Mails sollten mit Hilfe eines Spamfilters entsprechend markiert werden.

- E-Mails mit ausführbaren Dateien im Anhang (beispielsweise „.exe“, „.scr“, „.chm“, „.bat“, „.com“, „.msi“, „.jar“, „.cmd“, „.hta“, „.pif“, „.scf“) sollten geblockt oder in Quarantäne geschoben werden. Da es aber eine Vielzahl von verschiedenen Dateiformaten gibt, kann es sinnvoll sein, stattdessen eine „White-List“ zu verwenden und nur gewünschte Dateiendungen zuzulassen.

— Der Virenscanner eines E-Mail-Servers kann verschlüsselte Anhänge nicht scannen und ist somit an dieser Stelle wirkungslos. Der Anhang muss deshalb vor dem Öffnen mit dem lokalen Virenscanner (automatisch) überprüft werden.

— Eine Erweiterung des Notfallkonzepts um das Szenario „Schadsoftwarebefall" ist empfehlenswert, um im Angriffsfall schnell und effektiv reagieren zu können. Zu einem Notfallkonzept gehört für diesen Fall auch das Bereithalten von sicheren Bootmedien.

Die vom Bundesamt für Sicherheit in der Informationstechnik gegründete Allianz für Cybersicherheit bietet eine Vorlage für eine IT-Notfallkarte mit hilfreichen Hinweisen für Endnutzerinnen und Endnutzer an, die an zentralen Orten platziert werden können.[49] Insbesondere die schnelle Verbreitung von Emotet zeigt erneut die Bedeutung einer Sensibilisierung der Beschäftigten darauf, dass auch E-Mails von bekannten Absendern nicht von vornherein als vertrauenswürdig angesehen werden dürfen.

Das Bundesamt für Sicherheit in der Informationstechnik hat auch Empfehlungen veröffentlicht, welche Maßnahmen bei einem festgestellten Schadcodebefall mit Emotet zu ergreifen sind.[50] Aus Datenschutzsicht sind dabei insbesondere folgende Punkte zu klären:

— Die Logdateien (etwa der Firewall) sind in Bezug auf die Art und den Umfang des Angriffs und insbesondere hinsichtlich des Abflusses von personenbezogenen Daten zu überprüfen.

— Versandte E-Mails sind dahingehend zu überprüfen, ob der Schadcode weiterverbreitet wurde. Kann dies nicht zweifelsfrei ausgeschlossen werden, sollten alle Kommunikationspartnerinnen und Kommunikationspartner über den Schadcodebefall und die Gefahren für ihre eigenen Systeme informiert werden.

— Zu beachten ist, dass ein Befall mit Schadsoftware eine zu meldende Verletzung des Schutzes personenbezogener Daten nach Art. 33 DSGVO sein kann. Ich verweise hierzu auf meine Orientierungshilfe „Meldepflicht und Benachrichtigungspflicht des Verantwortlichen".[51]

Nach einem Schadcodebefall müssen zudem umfassende Bereinigungsmaßnahmen ergriffen werden, und es muss ein gesicherter Wiederanlauf erfolgen. Andernfalls ist zu befürchten, dass der Schadcode nicht vollständig beseitigt ist oder noch infizierte Systeme die bereits bereinigten Systeme wieder anstecken. Auch hierzu findet sich ebenfalls Näheres in den Hinweisen des Bundesamtes für Sicherheit in der Informationstechnik, unter anderem:

49 Internet: https://www.allianz-fuer-cybersicherheit.de.

50 Internet: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/E-Mailsicherheit/emotet.html.

51 Bayerischer Landesbeauftragter für den Datenschutz, Meldepflicht und Benachrichtigungspflicht des Verantwortlichen, Stand 6/2019, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Melde- und Benachrichtigungspflicht".

- Alle Rechner im Netz sind auf Auffälligkeiten zu überprüfen.

- Befallene Rechner sind ohne Ausnahme komplett neu unter Verwendung der aktuellen Betriebssystemversionen zu installieren. Dabei müssen sichere Bootmedien verwendet werden.

- Alle Rechner müssen regelmäßig mit Updates, Patches und einem aktuellen Virenschutz versorgt werden.

- Zum Zeitpunkt der Infektion vorhandene Zugangsdaten sind als kompromittiert zu betrachten. Alle Passwörter sind umgehend zu ändern.

12.4 Cyberabwehr Bayern

Seit Geltungsbeginn der Datenschutz-Grundverordnung haben sich meine Tätigkeiten im technischen und organisatorischen Bereich des Datenschutzes fortentwickelt. Prüfungen und Beratungen fanden zuvor in den zeitlich aufeinanderfolgenden, grundsätzlich getrennten Phasen „Prüfen" – „Bewerten" – „Mängelbehebung" statt. Durch die in Art. 33 Abs. 1 DSGVO verankerte Pflicht, Verletzungen des Schutzes von personenbezogener Daten möglichst binnen 72 Stunden zu melden, verschob sich meine Tätigkeit häufig bis hin zu einer aktuellen und fortlaufenden Begleitung des täglichen administrativen EDV-Betriebs der meldenden Stellen. Insbesondere Meldungen zu Schadcodebefall mit Trojanern (siehe Nr. 12.3) erfordern von mir eine zeitnahe Beratung, vereinzelt auch die Anweisung zu konkreten Maßnahmen.

Bei einigen zum Teil sehr schwerwiegenden Fällen hat es sich gezeigt, dass die betroffenen Behörden auf Grund ihrer Meldepflichten nicht nur mit mir Kontakt hatten, sondern auch mit anderen Stellen, die gesetzliche Aufgaben im Bereich der Cybersicherheit wahrnehmen. Gerade in akuten Lagen war es für die betroffene Stelle dann aufwendig, die unterschiedlichen Ansprechpartner zu informieren, und es oblag der betroffenen Stelle, die Anfragen und Tätigkeiten zu koordinieren.

Auch wenn es vereinzelt gelang, dass sich die beteiligten Behörden beispielsweise in einer gemeinsamen Telefonkonferenz zu einem Vorfall austauschten, so wurde deutlich, dass es an konkreten Ansprechpartnerinnen und Ansprechpartnern sowie an Schnittstellen mangelte und ein koordiniertes Vorgehen jedes Mal neu gefunden werden musste.

Als Konsequenz dieser Problematik hat die Bayerische Staatsregierung am 5. November 2019 ein Konzept zur Einrichtung einer neuen zentralen Informations- und Koordinationsplattform für Behörden mit Cybersicherheitsaufgaben, der „Cyberabwehr Bayern" beschlossen.[52] Als gleichberechtigte Teilnehmer bilden das Cyber-Allianz-Zentrum Bayern im Bayerischen Landesamt für Verfassungsschutz, das Bayerische Landeskriminalamt, das Bayerische Landesamt für Sicher-

[52] Siehe dazu Bayerisches Staatsministerium des Innern, für Sport und Integration, Bayern stärkt Cyberabwehr und Digitalfunk, Aktuelle Meldung vom 5. November 2019, Internet: https://www.stmi.bayern.de/med/aktuell/archiv/2019/191105mr.

heit in der Informationstechnik, die Zentralstelle Cybercrime Bayern bei der Generalstaatsanwaltschaft Bamberg, das Bayerische Landesamt für Datenschutzaufsicht und ich seit Januar die „Cyberabwehr Bayern“.

Hauptziel ist eine bessere gegenseitige Information sowohl zu allgemeinen Gefahren im Bereich der Cybersicherheit und ein zielgerichtetes Vorgehen in konkreten Schadensfällen. Idealerweise erhalten von Cyberangriffen betroffene Stellen dadurch eine koordinierte und optimale Hilfe der einzelnen beteiligen Behörden in ihren jeweiligen Zuständigkeitsbereichen. Die Cyberabwehr Bayern ist keine neue Behörde und erhält keine neuen gesetzlichen Befugnisse oder Aufgaben. Wichtigstes Ziel für mich ist ein schneller und effizienter Austausch zwischen den beteiligten Behörden in Bayern zu cyberrelevanten Informationen, wie etwa durch regelmäßige, aber auch anlassbezogen einberufene Lagebesprechungen.

Neben der Erfüllung der Aufgaben als Datenschutz-Aufsichtsbehörde für von Cyberangriffen betroffene Stellen in meinem Zuständigkeitsbereich sehe ich mich auch als datenschutzrechtliches Kontrollorgan, das darauf achten wird, dass grundsätzlich keine personenbezogenen Daten zwischen den beteiligten Stellen im Rahmen der Cyberabwehr ausgetauscht werden und im berechtigten Einzelfall jede beteiligte Stelle nur dann personenbezogene Daten weitergibt und erhält, wenn es dafür die erforderliche Rechtsgrundlage gibt.

12.5 Anforderungen an Messenger-Dienste im Krankenhausbereich

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat am 7. November 2019 das Whitepaper „Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich“ veröffentlicht, das auch auf meiner Homepage eingesehen und heruntergeladen werden kann.[53]

Messenger-Dienste haben sich als neue Form der Kommunikation in unserer Gesellschaft inzwischen fest etabliert. Die damit einhergehenden neuen Möglichkeiten weisen auch für den Krankenhausbereich ein großes Nutzenpotenzial auf, bringen aber Risiken mit sich, wenn etwa Messenger-Dienste für die ärztliche Kommunikation eingesetzt werden. Der Austausch von Gesundheitsdaten mittels Messenger-Diensten führt in Hinsicht auf unterschiedliche Aspekte zu zahlreichen datenschutzrechtlichen Fragestellungen und Bedenken. Das neue Whitepaper der Konferenz beantwortet die aufgeworfenen Fragen und bringt Klarheit bezüglich der datenschutzrechtlichen Anforderungen für diesen Einsatzbereich von Messenger-Diensten.

Da Messenger-Dienste nur eine von zahlreichen anderen, im Krankenhausbereich bereits verwendeten oder zukünftig denkbaren IT-Anwendungen in App-Form sind, erwarte ich die Veröffentlichung entsprechender weiterer Whitepapers oder datenschutzrechtlicher Anforderungskataloge, die sich auf Fallgruppen typischer Verarbeitungen im Krankenhausbereich beziehen.

[53] Internet: https://www.datenschutz-bayern.de, Rubrik „Konferenzen – 6. und 7. November 2019“.

12.6 Überwachung des Auftragsverarbeiters bei Fernzugriff

Vor dem Hintergrund der fortschreitenden Digitalisierung bei den bayerischen öffentlichen Stellen wird bei mir immer häufiger nach datenschutzrechtlichen Anforderungen an einen Fernzugriff auf IT-Systeme gefragt, etwa im Fall von Wartungsarbeiten. Daher konkretisiere und ergänze ich nachfolgend meine bisherigen Ausführungen[54] zum Fernzugriff auf IT-Systeme, die personenbezogene Daten verarbeiten.

Der bayerische Gesetzgeber hat für bayerische öffentliche Stellen in Art. 5 Abs. 3 BayDSG die im Rahmen der Fernwartung in aller Regel nicht ausgeschlossene Möglichkeit des (Fern-)Zugriffs auf personenbezogene Daten weitgehend den Regelungen der Auftragsverarbeitung unterstellt.

Wird im Rahmen von Fernzugriffen einem Auftragsverarbeiter oder einer diesem im Wesentlichen gleichgestellten Person der Zugriff auf personenbezogene Daten des Verantwortlichen rechtmäßig gewährt und werden personenbezogene Daten während eines Fernzugriffs auch tatsächlich verarbeitet, so müssen hinsichtlich der datenschutzrechtlichen Überwachung durch den Verantwortlichen folgende zwei Konstellationen voneinander unterschieden werden:

12.6.1 Synchrone Überwachung

Falls mindestens eine beim Verantwortlichen beschäftigte, geeignete Person (im Folgenden „Beobachterin“ oder „Beobachter“ genannt) die Fernzugriffsarbeiten des Auftragsverarbeiters durchgehend überwacht, genügt es, in einem Fernzugriffsprotokoll für den einzelnen Fernzugriff den Anfang, das Ende, den Zweck, die einzelnen Arbeiten, bei denen personenbezogene Daten verarbeitet wurden, sowie alle an dem Fernzugriff beteiligten Personen mit Bezeichnung der jeweils wahrgenommenen Rolle (so etwa: fernwartende Person, IT-Administratorin/IT-Administrator, Beobachterin/Beobachter) festzuhalten. In diesem Kontext ist eine Person grundsätzlich als geeignete Beobachterin oder geeigneter Beobachter anzusehen, falls sie vor dem Fernzugriff in die relevanten datenschutzrechtlichen und technischen Aspekte eingewiesen wurde, mit geeigneter Fachkunde alle während des Fernzugriffs ausgeführten datenschutzrelevanten Aktionen des Auftragsverarbeiters nachvollziehen und abbrechen kann sowie einen klaren Überwachungsauftrag erhalten hat.

Das Fernzugriffsprotokoll muss auf die technisch dokumentierten Zugriffsdaten, die während des Fernzugriffs automatisiert erstellt wurden, eindeutig verweisen. Das Fernzugriffsprotokoll und die dazugehörenden Zugriffsdaten müssen sicher und entsprechend der jeweils geltenden Aufbewahrungsfrist[55] aufgehoben werden.

54 Siehe in meinem 20. Tätigkeitsbericht 2002 unter Nr. 17.1.9, in meinem 19. Tätigkeitsbericht 2000 unter Nr. 17.3.3 sowie in meinem 18. Tätigkeitsbericht 1998 unter Nr. 3.3.4

55 Allgemeiner Anhaltspunkt für die Dauer der Aufbewahrungsfrist ist die Wahrscheinlichkeit, dass Unregelmäßigkeiten bei der Verarbeitung noch entdeckt oder Ursachen von Unregelmäßigkeiten aufgeklärt werden können. Bei Anwendbarkeit des Bundesdatenschutzgesetzes sind solche Protokolldaten am Ende des auf deren Generierung folgenden Jahres zu löschen, siehe § 76 Abs. 4 BDSG.

12.6.2 Asynchrone Überwachung

Ist dagegen die oben beschriebene synchrone Überwachung durch eine Beobachterin oder einen Beobachter im Ausnahmefall nicht möglich, sind durch den Verantwortlichen grundsätzlich alle Zugriffe des Auftragsverarbeiters auf personenbezogene Daten technisch automatisiert zu dokumentieren. Aus dieser Dokumentation muss auch der Zeitraum der Dokumentierung hervorgehen. Zudem muss ein Fernzugriffsprotokoll mit den gleichen Inhalten wie bei der synchronen Überwachung erstellt werden.

Eine solche lückenlose technische Dokumentation kann etwa in Form von Log-Dateien erfolgen. Diese werden typischerweise durch Standardfunktionen, die ein Hersteller für sein Fachverfahren anbietet, oder durch spezielle Zusatzsoftware, die Datenzugriffe geeignet aufzeichnen kann, erstellt.

Steht eine derartige Funktion für die automatisierte Erstellung von Log-Dateien nicht zur Verfügung, kann der gesamte Dialog des Fernzugriffs – also nicht nur die einzelnen, relevanten Datenzugriffe – ersatzweise durch den Verantwortlichen aufgezeichnet werden. Hierfür können beispielsweise IT-Werkzeuge verwendet werden, die lückenlos eine ganze Fernzugriffssitzung gleichsam wie in einem Video aufzeichnen.

Bei jeder asynchronen Überwachung muss im Nachgang zum stattgefundenen Fernzugriff eine Beobachterin oder ein Beobachter die Dokumentation zum Fernzugriff in Form von Log-Dateien oder in Form der beschriebenen Dialogaufzeichnung auf ihre datenschutzrechtliche Konformität prüfen. Die Prüfung kann je nach Umfang und Sensibilität der betroffenen personenbezogenen Daten auch stichprobenartig erfolgen. Bei vorliegender Konformität bestätigt die Beobachterin oder der Beobachter den Fernzugriff als datenschutzrechtlich unbedenklich im betreffenden Fernzugriffsprotokoll. Falls jedoch Mängel bei der datenschutzrechtlichen Prüfung festgestellt werden, hat die Dienststelle die Mängel – soweit möglich – zu beseitigen und eine künftige Wiederholung dieser Mängel risikoorientiert auszuschließen. Das dabei beschrittene Vorgehen sowie dessen Ergebnis sind ebenfalls im Fernzugriffsprotokoll zu vermerken. Das Fernzugriffsprotokoll sowie die technisch automatisiert erstellte Dokumentation sind wie bei der synchronen Überwachung aufzubewahren.

Die synchrone Überwachung ist grundsätzlich zu bevorzugen, da hier das Risiko von Datenschutzverletzungen insbesondere durch die sofortige Abbruchmöglichkeit der Beobachterin oder des Beobachters deutlich geringer ist.

Ergänzend weise ich auf weitere wichtige Regeln für einen (Fern-)Zugriff hin, die ich in der Orientierungshilfe „Auftragsverarbeitung“[56] genauer dargelegt habe.

12.7 Meldungen von Datenpannen

Im Berichtszeitraum erreichten mich über tausend Meldungen nach Art. 33 DSGVO, insbesondere auch aus dem Gesundheits- und Sozialbereich.

[56] Bayerischer Landesbeauftragter für den Datenschutz, Auftragsverarbeitung, Stand 4/2019, S. 26 ff., Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Auftragsverarbeitung“.

In einer Vielzahl der gemeldeten Fälle wurden Daten versehentlich an nicht berechtigte Empfänger übermittelt. Häufige Fehlerquellen waren hier die unkorrekte Adressierung, eine fehlerhafte Zusammenstellung oder eine falsche Kuvertierung von Unterlagen, die in den betroffenen Stellen jeweils manuell ausgeführt oder angestoßen wurde. Auch die falsche Adressierung von E-Mails war ein häufiges Thema, insbesondere der Versand von Unterlagen per E-Mail an mehrere Adressatinnen und Adressaten, wobei jeweils alle Kenntnis vom Verteiler erhielten. Dies lässt sich leicht dadurch vermeiden, dass bei der Eingabe in den Header der E-Mail das „bcc"-Feld anstelle des „cc"-Feldes verwendet wird.

Bereits in mehreren früheren Tätigkeitsberichten habe ich auf die Problematik des Fehlversands durch Falscheingabe einer Telefaxnummer hingewiesen (siehe mein 27. Tätigkeitsbericht 2016 unter Nr. 5.5.3 und mein 28. Tätigkeitsbericht 2018 unter Nr. 3.1.6). Ausführliche Erläuterungen enthält zudem meine Orientierungshilfe „Datensicherheit beim Telefax-Dienst"[57]. Dennoch häuften sich zu meinem Bedauern gerade im Krankenhausbereich Meldungen unsachgemäßen Versands von vertraulichen Unterlagen an unberechtigte Empfänger per Telefax. Ich möchte nochmals hervorheben, dass gerade für die Übermittlung sensibler Daten wie Gesundheits- oder Sozialdaten der Telefaxversand nur in Ausnahmefällen, und wenn ja, dann exakt und kontrolliert genutzt werden sollte. Ferner sollte stets geprüft werden, ob nicht auch ein alternatives Kommunikationsmittel zur Verfügung steht und eine verschlüsselte elektronische Übersendung der Daten möglich ist.

In weiteren Fällen wurde ich darüber in Kenntnis gesetzt, dass dienstliche Notebooks und andere elektronische Geräte gestohlen oder vom Benutzer verloren worden waren. Diese Fälle zeigen, dass es zwingend nötig ist, sensible Daten auf mobilen Geräten verschlüsselt abzuspeichern oder sichere Lösungen über Fernzugriffe zu verwenden, bei denen die Daten zentral gehostet werden.

Aus den Meldungen ging weiterhin hervor, dass auch Behörden, Kliniken, Universitäten und andere öffentliche Stellen in größerem Umfang von Hackerangriffen, Schadsoftware oder Systemausfällen betroffen sind. So wurden mir immer wieder Fälle gemeldet, bei denen sich Schadsoftware im internen Netzwerk verbreiten konnte. Dass Schadsoftware in die Netzwerke der betroffenen Organisationen eindringen konnte, lag bedauerlicherweise oft daran, dass zu wenig Personal- und Sachmittel in die unabdingbare Gewährleistung von Basis-IT-Sicherheit investiert wurden. Es sollten in jedem Fall die Verwendung von aktuellen Betriebssystemversionen und das Einspielen von Sicherheitsupdates sowie der Einsatz von aktueller Virenschutzsoftware sichergestellt sein. Zudem müssen Maßnahmen hinsichtlich des Umgangs mit E-Mails und der Internet-Nutzung ergriffen werden.

Im Zuge der Nutzung von Telearbeit erreichten mich wiederholt Meldungen über einen unsachgemäßen Umgang mit sensiblen vertraulichen Daten durch Bearbeiterinnen und Bearbeiter sowie über die daraus resultierende Offenlegung personenbezogener Daten an nicht berechtigte Personen, entweder beim Transport von Unterlagen zum Standort der Telearbeit oder am Standort der Telearbeit selbst. In einem Fall hatte eine öffentliche Stelle den Verlust mehrerer Dutzend Patientenakten im öffentlichen Personennahverkehr zu beklagen, die ein ehrlicher Finder glücklicherweise bei der Polizei abgab. Wie in meinem 25. Tätigkeitsbericht

[57] Bayerischer Landesbeauftragter für den Datenschutz, Datensicherheit beim Telefax-Dienst, Internet: https://www.datenschutz-bayern.de, Rubrik „Veröffentlichungen – Orientierungs- und Praxishilfen – Datensicherheit beim Telefax-Dienst".

2012 unter Nr. 2.1.4 dargelegt, wird deutlich, dass es wesentlich ist, entsprechende technische und organisatorische Maßnahmen zu ergreifen, um den Aktentransport zu regeln. Insbesondere sollten personenbezogene Unterlagen ausschließlich in verschlossenen Behältnissen transportiert werden. Falls öffentliche Verkehrsmittel benutzt werden, sollte zudem Sorge getragen werden, dass diese Behältnisse nicht unbeaufsichtigt abgestellt oder ganz vergessen werden.

Im Übrigen bestand im Berichtszeitraum bei einigen Verantwortlichen Unklarheit, ob Vorfälle nach Art. 33 DSGVO meldepflichtig sind. Zudem unterbleibt nicht selten die Benachrichtigung betroffener Personen nach Art. 34 DSGVO, weil das aus einem meldepflichtigen Ereignis folgende Risiko nicht zutreffend eingeschätzt wird. Zur Information der bayerischen öffentlichen Stellen über die Meldepflicht nach Art. 33 DSGVO und die Benachrichtigungspflicht nach Art. 34 DSGVO habe ich im Berichtszeitraum eine ausführliche Orientierungshilfe veröffentlicht, die insbesondere auch zu einer strukturierten Risikobeurteilung anleitet.[58]

12.8 Beanstandungen, Sanktionen

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

12.8.1 Beanstandungen und Sanktionen bei Krankenhäusern

Im Berichtszeitraum wurden gegenüber drei öffentlichen Krankenhäusern aufgrund von massiven Verstößen gegen die Anforderungen des technisch-organisatorischen Datenschutzes Beanstandungen nach Art. 16 Abs. 4 Satz 1 BayDSG ausgesprochen.

— In einem Fall kam es bei einem Klinikum über einen längeren Zeitraum zum Fehlversand von medizinischen Daten per unverschlüsselter E-Mail. Die Daten sollten ursprünglich für fachübergreifende Tumorkonferenzen genutzt werden und ausschließlich an die an der Behandlung beteiligten Ärztinnen und Ärzte versandt werden. Wie sich herausstellte, wurden die Patientendaten jedoch auch an Ärztinnen und Ärzte versandt, die nicht an der Behandlung beteiligt waren und auch nicht dem Klinikum angehörten. Insofern wurden die E-Mails unverschlüsselt über das Internet versandt. Ich habe diese Vorgehensweise beanstandet, weil die Fähigkeit der Vertraulichkeit der Systeme auf Dauer nicht sichergestellt war (Art. 32 Abs. 1 Buchst. b DSGVO). Das Klinikum wurde aufgefordert, seine Prozesse zum E-Mail-Versand zu überprüfen und entsprechende technische und organisatorische Maßnahmen zu ergreifen.

— Ein weiteres Klinikum wurde beanstandet, da es keine ausreichenden technischen Sicherheitsmaßnahmen ergriffen hatte, um einen Schadcodebefall zu verhindern, der zu einem mehrtägigen Komplettausfall der IT geführt

[58] Bayerischer Landesbeauftragter für den Datenschutz, Meldepflicht und Benachrichtigungspflicht des Verantwortlichen, Stand 6/2019, Internet: https:www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Melde- und Benachrichtigungspflicht“.

hatte. Es handelte sich aus mehreren Gründen um eine massive Datenschutzverletzung: Die gemäß Art. 32 Abs. 1 Buchst. b und c DSGVO sicherzustellende Verfügbarkeit der elektronisch gespeicherten medizinischen Daten war über mehrere Tage hinweg nicht gegeben. Das Klinikum musste sich von der Notfallversorgung im Landkreis abmelden und die Patientenbehandlung musste auf Papier dokumentiert werden. Zudem konnte nicht vollständig ausgeschlossen werden, dass die Vertraulichkeit gemäß Art. 32 Abs. 1 Buchst. b DSGVO der Daten während des ganzen Zeitraums gegeben war und keine Daten das Krankenhaus verlassen haben. Die im entsprechenden Klinikum verbreitete Schadsoftware ist durchaus dafür bekannt, dass ihr Zweck auch das Ausspionieren von Systemen ist. Ein Hauptangriffsziel sind hierbei Passwörter und Zugangsinformationen um diese etwa für einen späteren gezielten Angriff zu nutzen. Häufig kommt es zudem zu einem E-Mail-Harvesting, das heißt, es werden die vorhandenen Kontakte genutzt, um den Virus weiter zu verbreiten. Weitere Informationen zum Thema Schadsoftware finden sich in diesem Tätigkeitsbericht unter Nr. 12.3.

Ursache des Vorfalls waren erhebliche Sicherheitsmängel beim Betrieb der IT-Systeme des Klinikums, insbesondere ein unzureichender Virenschutz und fehlende Updates für eine seit Jahren bekannte Schwachstelle im Betriebssystem sowie insgesamt die Nutzung veralteter Software. Da auch die Behebung dieser Sicherheitsmängel im Nachgang der Beanstandung eher schleppend verlieft, habe ich zudem eine Anweisung nach Art. 58 Abs. 2 Buchst. d DSGVO erlassen mit den vom Klinikum umzusetzenden technischen Sicherheitsmaßnahmen.

— In einem anderen Klinikum offenbarten sich diverse gravierende Mängel sowohl im Bereich des Faxversands als auch beim Betrieb des E-Mail-Servers, die zu einer Beanstandung geführt haben. Im diesem Klinikum waren über 150 Fax-Geräte im Einsatz, über die sensible Patientendaten an Empfänger sowohl innerhalb als auch außerhalb des Klinikums versandt wurden. Dabei kam es über einen längeren Zeitraum hinweg wiederholt zu Fehleingaben der Faxnummer, so dass sensible Daten in erheblichem Umfang bei unbeteiligten Dritten ankamen. Unter anderem aufgrund des hohen Risikos für Fehleingaben bei Faxnummern und der Risiken eines unsicheren Aufstellorts des Faxgeräts beim Empfänger eignen sich Faxgeräte nicht für die Übermittlung von vertraulichen Daten und sollten daher nur in dringenden, nicht anders zu erledigenden Ausnahmefällen verwendet werden, siehe auch Orientierungshilfe „Datensicherheit beim Telefax-Dienst“[59].

  Des Weiteren ließ dieses Haus den E-Mail-Server bei einem externen Dienstleister betreiben; außerdem war für alle Mitarbeiterinnen und Mitarbeiter des Klinikums die Möglichkeit zum Zugriff auf dienstliche E-Mails über Open Web Access von jedem beliebigen Gerät aus möglich. Wie ich schon in meinem 25. Tätigkeitsbericht unter Nr. 2.1.2 dargestellt habe, genügt der Zugriff über Open Web Access und die damit verbundene Nutzung von Privatgeräten nicht den Anforderungen des Datenschutzes. Der Betrieb des E-Mail-Servers bei einem externen Dienstleister verstößt zudem gegen Art. 27 Abs. 4 Satz 6 Bayerisches Krankenhausgesetz (BayKrG), da

[59] Bayerischer Landesbeauftragter für den Datenschutz, Orientierungshilfe Datensicherheit beim Telefax-Dienst, Internet: https://www.datenschutz-bayern.de/, Rubrik „Veröffentlichungen“.

für eine Auftragsdatenverarbeitung nur andere Krankenhäuser genutzt werden dürfen.

Ein weiterer Mangel in diesem Krankenhaus trat im Zusammenhang mit dem Krankenhausinformationssystem und dessen Berechtigungskonzept auf. So zeigte sich, dass alle Patienten seit Einführung des Krankenhausinformationssystems über die Suchfunktion jederzeit auffindbar waren, falls deren Name und Geburtsdatum bekannt waren, auch wenn sie schon seit Jahren nicht mehr im Krankenhaus behandelt wurden. Wie in der Orientierungshilfe „Krankenhausinformationssysteme (2. Fassung) der Datenschutzkonferenz (Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder)“[60] dargelegt, dürfen übergreifende Zugriffsrechte ausschließlich über einen protokollierten Sonderzugriff erfolgen, der im Klinikum zusätzlich vorhanden war, aber durch die reguläre Suchfunktion umgangen wurde.

Ferner erfolgte keine Sperrung von Patientendaten nach Entlassung, wie in meiner Orientierungshilfe gefordert. Die Daten der Patientinnen und Patienten befanden sich zwar nicht mehr im direkten Zugriff der Stationsgrafik, waren aber über die Suchfunktion jederzeit auffindbar. Somit ergab sich in diesem Fall die Möglichkeit der Offenlegung von sensiblen medizinischen Daten ohne Behandlungszusammenhang und damit eine schwerwiegende Verletzung der Vertraulichkeit dieser Patientendaten.

Seit Geltungsbeginn der Datenschutz-Grundverordnung im Mai 2018 sind neben dem Instrument der Beanstandung auch Sanktionen im Sinne des Art. 58 Abs. 2 DSGVO möglich. Zudem dürfen gegenüber einem Klinikum, das als Wettbewerbsunternehmen tätig ist, Geldbußen nach Art. 83 DSGVO verhängt werden (Art. 22 BayDSG).

12.8.2 Beanstandung des unbeabsichtigten Versands einer Excel-Datei mit Personaldaten

Eine Beanstandung musste ich aussprechen, weil eine öffentliche Stelle versehentlich eine Excel-Datei mit personenbezogenen Daten einer Gruppe von 45 Lehrerinnen und Lehrern per E-Mail unverschlüsselt an alle Gruppenmitglieder versendet hat. Beabsichtigt war, ein Arbeitsblatt mit Kontaktdaten zugänglich zu machen, um die Kommunikation unter den in vergleichbarer Funktion tätigen Lehrerinnen und Lehrern zu erleichtern. Die Excel-Datei enthielt jedoch weitere Arbeitsblätter, aus denen unter anderem eine umfassende Übersicht über die dienstlichen Beurteilungen der Jahre 2010 und 2014 (Beurteilungsprädikate) sowie Aufzeichnungen über das dienstliche Verhalten und die Amtsführung (wertende Aussagen über die Qualität von Arbeitsergebnissen, Tagungsteilnahmen und vereinzelt auch wertende Stellungnahmen anderer öffentlichen Stellen) ersichtlich waren. Diese Arbeitsblätter umfassten zudem Angaben von früheren Gruppenmitgliedern.

60 Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe Krankenhausinformationssysteme, Stand 3/2014, Internet: https://www.datenschutz-bayern.de, Rubrik „Veröffentlichungen – Orientierungs- und Praxishilfen – Krankenhausinformationssysteme (2. Fassung)“.

Unabhängig von der Frage, ob die versendete Datei Personalaktendaten im Sinne von § 50 Satz 2 Beamtenstatusgesetz (BeamtStG) enthält oder nicht, richtet sich die Zulässigkeit der Verarbeitung personenbezogener Daten der betroffenen Lehrerinnen und Lehrer nach § 50 BeamtStG und Art. 103 ff. Bayerisches Beamtengesetz (BayBG).

Gemäß Art. 103 Satz 1 Nr. 1 BayBG darf der Dienstherr personenbezogene Daten über aktive und ehemalige Beamtinnen und Beamte nur verarbeiten, soweit dies zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere zu Zwecken der Personalverwaltung oder Personalwirtschaft erforderlich ist. Nach Art. 103 Satz 2 BayBG darf die Verarbeitung nur durch solche Beschäftigte erfolgen, die vom Dienstherrn mit der Bearbeitung von Personalangelegenheiten betraut sind. Als Verarbeitung gelten gemäß Art. 4 Nr. 2 DSGVO auch die Speicherung, Verwendung und Offenlegung personenbezogener Daten. Personenbezogene Daten sind unverzüglich zu löschen, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet worden sind, nicht mehr benötigt werden (vgl. Art. 17 Abs. 1 Buchst. a DSGVO).

Das Führen einer Tabelle mit personenbezogenen Daten von mehreren Beamtinnen und Beamten (insbesondere Beurteilungsprädikate und Daten zur Vorbereitung der dienstlichen Beurteilungen im Jahr 2014), soweit sie keinem der in Art. 103 BayBG genannten Zwecke dient, und der Versand dieser Datei an eine Vielzahl nicht zugangsberechtigter Empfängerinnen und Empfänger durch die öffentliche Stelle ist mit Art. 103 Satz 1 Nr. 1 und Satz 2 BayBG nicht vereinbar.

In dem Fall hat sich ein gut bekanntes Risiko realisiert, das dem Versand einer von einem Tabellenkalkulationsprogramm erstellten Datei, die oft auch als Arbeitsmappe bezeichnet wird, innewohnt. Eine solche Datei kann mehrere unterschiedliche Tabellenbereiche besitzen, die auch Arbeitsblätter genannt werden. Typischerweise wird nach dem Öffnen der Datei nur ein Tabellenbereich angezeigt, während eventuell daneben existierende Tabellenbereiche nur über eine zusätzliche Benutzeraktion aktiviert und damit sichtbar gemacht werden können.

Diese besondere Funktionsweise führt zu folgendem Risiko: Die Versenderin oder der Versender einer solchen Datei betrachtet vor dem Versand oft nur den gerade aktivierten Tabellenbereich und übersieht dabei, dass sich in anderen Tabellenbereichen der Datei sensible Daten befinden, die nicht mit versendet werden sollen.

Eine geeignete Datenschutz-Maßnahme gegen dieses Risiko ist beispielsweise, den Tabellenbereich, der versendet werden soll, zuvor im PDF-Format abzuspeichern und dann nur noch die PDF-Datei zu versenden.

12.8.3 Beanstandungen von Kommunen

Leider kam es im Berichtszeitraum auch im Bereich der Städte und Gemeinden zu Verstößen gegen die Anforderungen des technisch-organisatorischen Datenschutzes, die in Einzelfällen auch zu Beanstandungen geführt haben.

Eine größere Stadt wurde von mir beanstandet, weil es im Rahmen ihrer Aufgabe zur Verhinderung einer Obdachlosigkeit zu einer datenschutzwidrigen Form der Kontaktaufnahme mit einem Bürger im Rahmen einer Räumungsklage kam. Da der Bürger über eine konventionelle Kontaktaufnahme per Post oder persönlichen Besuch über einen längeren Zeitraum nicht zu erreichen war, brachte eine

Mitarbeiterin des dortigen Sozialamtes ein Schreiben mit sensiblen personenbezogenen Daten, die dem Sozialgeheimnis unterliegen, offen an der Wohnungstüre des betroffenen Bürgers in einem großen Wohnkomplex mit etwa 45 Wohnungen an, obwohl der Bürger gemäß § 35 Abs. 1 Erstes Buch Sozialgesetzbuch – Allgemeiner Teil – einen Anspruch darauf gehabt hätte, dass die ihn betreffenden Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden.

Ein Absehen von einer Beanstandung schied aus, weil dieser Verstoß nicht unerheblich war. Das offene Anbringen eines persönlichen Beratungsangebotes an der Wohnungstüre ist als solches keine geeignete Maßnahme zur Kontaktaufnahme, insbesondere wenn besonders schutzwürdige Daten offenbart werden. Zudem war davon auszugehen, dass eine unberechtigte Offenbarung von personenbezogenen Daten tatsächlich erfolgt war und nicht mehr ungeschehen gemacht werden konnte.

12.9 IT-System mit voreingestellten Zugangsdaten

Heute gilt bei sicherheitskritischen digitalisierten Verarbeitungsvorgängen eine Zwei-Faktor-Authentisierung als Mindeststandard. Gleichwohl gibt es weiterhin IT-Systeme, die eine sicherheitskritische Verarbeitung unterstützen und bei denen noch eine sogenannte Ein-Faktor-Authentisierung bei der Systemanmeldung einer Benutzerin oder eines Benutzers (Login) verwendet wird. Dabei ergibt sich die genaue Anzahl der Faktoren aus der Anzahl der Komponenten „Wissen“, „Besitz“ und „Biometrie“, auf die beim Login in ein IT-System zurückgegriffen wird. Beispielsweise ist beim Login mit Hilfe einer von der Benutzerin oder dem Benutzer anzugebenden Kennung und dem dazugehörigen Passwort nur der Bereich „Wissen“ einschlägig, so dass hier von einer Ein-Faktor-Authentisierung gesprochen werden kann. Erfährt in dieser Konstellation eine Person die Benutzerkennung und das Passwort einer anderen Benutzerin oder eines anderen Benutzers, so wird regelmäßig das Risiko einer unbefugten Datenverarbeitung deutlich erhöht.

Einige IT-Systeme besitzen nach ihrer Installation beziehungsweise nach ihrer Auslieferung voreingestellte Zugangsdaten. Bei einer derartigen Werkseinstellung kann regelmäßig davon ausgegangen werden, dass die vorkonfigurierten Benutzerkennungen und die dazugehörigen vorkonfigurierten Passwörter nicht geheim sind. Denn solche für ein IT-System standardmäßig existierende Logins können oft aus den Systemdokumentationen oder aus den relevanten Austauschplattformen betroffener Systemanwenderinnen und Systemanwender entnommen werden. Sehr gut bei der Suche nach diesen Türöffnern für IT-Systeme sind Cyberkriminelle, die typischerweise bei ihren Angriffen zunächst ausprobieren, ob vergessen wurde, vorkonfigurierte Benutzerkennungen mit neuen Passwörtern zu versehen. Daher kommt das Bundesamt für Sicherheit in der Informationstechnik unter anderem auch im Prozessbaustein „Identitäts- und Berechtigungsmanagement“ seines IT-Grundschutz-Kompendiums 2019 folgerichtig zum Schluss, dass vorkonfigurierte Zugangsmittel vor dem produktiven Einsatz geändert,[61]

[61] Siehe Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kompendium, ORP.4 Identitäts- und Berechtigungsmanagement, Internet: https://www.bsi.bund.de, Rubrik „Themen – IT-Grundschutz – IT-Grundschutz-Kompendium“.

Standardpasswörter durch ausreichend starke Passwörter ersetzt und voreingestellte Logins geändert werden müssen.[62]

Die Problematik voreingestellter Zugangsdaten wird nicht selten dadurch verschärft, dass mit umfangreichen administrativen Berechtigungen ausgestattete Systemzugänge betroffen sind und auch noch IT-Systeme auf dem Markt angeboten werden, bei denen vorkonfigurierte Benutzerkennungen technisch nicht geändert werden können.

Sind ab Werk vorkonfigurierte Benutzerkennungen unveränderbar, so kommt der Absicherung dieser Benutzerkonten mit einem jeweils geeigneten Passwort die entscheidende Rolle zu, wenn es darum geht, das Risiko einer unbefugten Datenverarbeitung zu verringern. Aktuell gehaltene Hinweise für geeignete Passwörter und deren Umgang gibt unter anderen das Bundesamt für Sicherheit in der Informationstechnik.[63]

In diesem Zusammenhang ist datenschutzrechtlich Folgendes zu beachten:

Setzt eine Stelle ein IT-System ein, das personenbezogene Daten verarbeitet und das voreingestellte Zugangsdaten aufweist, so ist in der Risikoanalyse nach Art. 24, Art. 25 und Art. 32 DSGVO beziehungsweise in der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO von dieser Stelle geeignet nachzuweisen, dass wirksame Datenschutzmaßnahmen ergriffen wurden, um das von den voreingestellten Logins ausgehende datenschutzrechtliche Risiko auf ein vertretbares Maß zu reduzieren. Insbesondere muss nachvollziehbar sein, dass die vorkonfigurierten Passworte auf nur der einsetzenden Stelle bekannte Passworte gewechselt werden. Softwarehersteller sollten darauf achten, dass im Rahmen der Anforderungen von Art. 25 DSGVO nach datenschutzfreundlichen Voreinstellungen ein Passwortwechsel nach der Installation vom System angefordert wird und dieser zu jedem beliebigen Zeitpunkt einfach von der einsetzenden Stelle durchzuführen ist.

62 Siehe Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kompendium, ORP.4.A8 Regelung des Passwortgebrauchs [Benutzer, Leiter IT], Internet: https://www.bsi.bund.de, Rubrik „Themen – IT-Grundschutz – IT-Grundschutz-Kompendium".

63 Siehe etwa die Empfehlungen für Passwörter, Internet: https://www.bsi-fuer-buerger.de, Rubrik „Empfehlungen – Passwörter".

13 Datenschutzkommission

Der Datenschutzkommission beim Bayerischen Landtag gehörten am Ende des Berichtszeitraums folgende Mitglieder und stellvertretende Mitglieder an:

Aus dem Landtag:

Mitglieder:

Peter Tomaschko, CSU
Benjamin Adjei, BÜNDNIS 90/DIE GRÜNEN
Alfred Grob, CSU
Martin Hagen, FDP
Gerd Mannes, AFD
Gerald Pittner, FREIE WÄHLER
Florian Ritter, SPD

Stellvertretende Mitglieder:

Tanja Schorer-Dremel, CSU
Verena Osgyan, BÜNDNIS 90/DIE GRÜNEN
Andreas Jäckel, CSU
Matthias Fischbach FDP
Roland Magerl, AFD
Wolfgang Hauber, FREIE WÄHLER
Christian Flisek, SPD

Auf Vorschlag der Staatsregierung:

Mitglied:

Ministerialrat Michael Will, Datenschutzbeauftragter des Bayerischen Staatsministeriums des Innern, für Sport und Integration

Stellvertretendes Mitglied:

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

Auf Vorschlag der kommunalen Spitzenverbände in Bayern:

Mitglied:

Rudolf Schleyer, Vorstandsvorsitzender der Anstalt für Kommunale Datenverarbeitung in Bayern

Stellvertretendes Mitglied:

Gudrun Aschenbrenner, Mitglied des Vorstands der Anstalt für Kommunale Datenverarbeitung in Bayern

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

Mitglied:

Werner Krempl, Erster Direktor und Vorsitzender der Geschäftsführung der Deutschen Rentenversicherung Nordbayern

Stellvertretendes Mitglied:

Dr. Irmgard Stippler, Vorstandsvorsitzende der AOK Bayern – Die Gesundheitskasse

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

Mitglied:

Dr. Till Schemmann, Notar

Stellvertretendes Mitglied:

Dr. Thomas Kuhn, Rechtsanwalt

Herr Peter Tomaschko, MdL, führte den Vorsitz in der Datenschutzkommission; stellvertretender Vorsitzender war Herr Benjamin Adjei, MdL.

Die Datenschutzkommission beim Bayerischen Landtag tagte im Berichtszeitraum zwei Mal.

14 Anlagen

Anlage 1: Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3. April 2019

Hambacher Erklärung zur Künstlichen Intelligenz Sieben datenschutzrechtliche Anforderungen

Systeme der Künstlichen Intelligenz (KI) stellen eine substanzielle Herausforderung für Freiheit und Demokratie in unserer Rechtsordnung dar. Entwicklungen und Anwendungen von KI müssen in demokratisch-rechtsstaatlicher Weise den Grundrechten entsprechen. Nicht alles, was technisch möglich und ökonomisch erwünscht ist, darf in der Realität umgesetzt werden. Das gilt in besonderem Maße für den Einsatz von selbstlernenden Systemen, die massenhaft Daten verarbeiten und durch automatisierte Einzelentscheidungen in Rechte und Freiheiten Betroffener eingreifen. Die Wahrung der Grundrechte ist Aufgabe aller staatlichen Instanzen. Wesentliche Rahmenbedingungen für den Einsatz von KI sind vom Gesetzgeber vorzugeben und durch die Aufsichtsbehörden zu vollziehen. Nur wenn der Grundrechtsschutz und der Datenschutz mit dem Prozess der Digitalisierung Schritt halten, ist eine Zukunft möglich, in der am Ende Menschen und nicht Maschinen über Menschen entscheiden.

I. Künstliche Intelligenz und Datenschutz

„Künstliche Intelligenz“ (auch „KI“ oder „Artificial Intelligence“ – „AI“) wird derzeit intensiv diskutiert, da sie neue Wertschöpfung in vielen Bereichen von Wirtschaft und Gesellschaft verspricht. Die Bundesregierung hat eine KI-Strategie veröffentlicht, mit dem Ziel, Deutschland an die Weltspitze der Entwicklung von KI zu bringen. „AI made in Germany“ soll gleichzeitig dafür sorgen, dass auch bei weitreichendem Einsatz Künstlicher Intelligenz die Grundwerte und Freiheitsrechte, die in Deutschland und der EU gelten, weiterhin die prägende Rolle für unser Zusammenleben spielen. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder begrüßen diesen Ansatz der grundrechtsverträglichen Gestaltung von KI ausdrücklich.

Eine allgemein anerkannte Definition des Begriffs der Künstlichen Intelligenz existiert bisher nicht. Nach dem Verständnis der Bundesregierung geht es bei KI darum, „technische Systeme so zu konzipieren, dass sie Probleme eigenständig bearbeiten und sich dabei selbst auf veränderte Bedingungen einstellen können. Diese Systeme haben die Eigenschaft, aus neuen Daten zu „lernen“ […].“[1]

KI-Systeme werden beispielsweise bereits in der Medizin unterstützend in Forschung und Therapie eingesetzt. Schon heute sind neuronale Netze in der Lage,

[1] BT-Drs. 19/1982 zu 1. Die Datenethikkommission der Bundesregierung hebt ergänzend als wichtige Grundlagen für KI die Mustererkennung, das maschinelle Lernen und Methoden der heuristischen Suche, der Inferenz und der Handlungsplanung hervor (Empfehlungen der Datenethikkommission für die Strategie Künstliche Intelligenz der Bundesregierung, 9.10.2018).

automatisch komplexe Tumorstrukturen zu erkennen. KI-Systeme können auch genutzt werden, um Depressionserkrankungen anhand des Verhaltens in sozialen Netzwerken oder anhand der Stimmmodulation beim Bedienen von Sprachassistenten zu erkennen. In den Händen von Ärzten kann dieses Wissen dem Wohl der Erkrankten dienen. In den falschen Händen jedoch, kann es auch missbraucht werden.

Auch zur Bewertung von Bewerbungsunterlagen wurde bereits ein KI-System eingesetzt, mit dem Ziel, frei von menschlichen Vorurteilen zu entscheiden. Allerdings hatte das Unternehmen bislang überwiegend männliche Bewerber eingestellt und das KI-System mit deren erfolgreichen Bewerbungen trainiert. In der Folge bewertete das KI-System Frauen sehr viel schlechter, obwohl das Geschlecht nicht nur kein vorgegebenes Bewertungskriterium, sondern dem System sogar unbekannt war. Dies offenbart die Gefahr, dass in Trainingsdaten abgebildete Diskriminierungen nicht beseitigt, sondern verfestigt werden.

Anhand dieser Beispiele wird deutlich, dass mit KI-Systemen häufig personenbezogene Daten verarbeitet werden und diese Verarbeitung Risiken für die Rechte und Freiheiten von Menschen birgt. Sie zeigen auch, wie wichtig es ist, Entwicklung und Einsatz von KI-Systemen politisch, gesellschaftlich und rechtlich zu begleiten. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder verstehen die folgenden Anforderungen als einen konstruktiven Beitrag zu diesem zentralen gesellschaftspolitischen Projekt.

II. Datenschutzrechtliche Anforderungen an Künstliche Intelligenz

Für die Entwicklung und den Einsatz von KI-Systemen, in denen personenbezogene Daten verarbeitet werden, beinhaltet die Datenschutz-Grundverordnung (DS-GVO) wichtige rechtliche Vorgaben. Sie dienen dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen. Auch für KI-Systeme gelten die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DS-GVO). Diese Grundsätze müssen gemäß Art. 25 DS-GVO durch frühzeitig geplante technische und organisatorische Maßnahmen von den Verantwortlichen umgesetzt werden (Datenschutz durch Technikgestaltung).

1. KI darf Menschen nicht zum Objekt machen

Die Garantie der Würde des Menschen (Art. 1 Abs. 1 GG, Art. 1 GRCh) gebietet, dass insbesondere im Fall staatlichen Handelns mittels KI der Einzelne nicht zum Objekt gemacht wird. Vollständig automatisierte Entscheidungen oder Profiling durch KI-Systeme sind nur eingeschränkt zulässig. Entscheidungen mit rechtlicher Wirkung oder ähnlicher erheblicher Beeinträchtigung dürfen gemäß Art. 22 DS-GVO nicht allein der Maschine überlassen werden. Wenn der Anwendungsbereich des Art. 22 DS-GVO nicht eröffnet ist, greifen die allgemeinen Grundlagen des Art. 5 DS-GVO, die insbesondere mit den Grundsätzen der Rechtmäßigkeit, Zurechenbarkeit und Fairness die Rechte des Einzelnen schützen. Betroffene haben auch beim Einsatz von KI-Systemen den Anspruch auf das Eingreifen einer Person (Intervenierbarkeit), auf die Darlegung ihres Standpunktes und die Anfechtung einer Entscheidung.

2. KI darf nur für verfassungsrechtlich legitimierte Zwecke eingesetzt werden und das Zweckbindungsgebot nicht aufheben

Auch für KI-Systeme gilt, dass sie nur zu verfassungsrechtlich legitimierten Zwecken eingesetzt werden dürfen. Zu beachten ist auch der Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO). Zweckänderungen sind mit Art. 6 Abs. 4 DS-GVO klare Grenzen gesetzt. Auch bei KI-Systemen müssen erweiterte Verarbeitungszwecke mit dem ursprünglichen Erhebungszweck vereinbar sein. Das gilt auch für die Nutzung personenbezogener Daten zu Trainingszwecken von KI-Systemen.

3. KI muss transparent, nachvollziehbar und erklärbar sein

Personenbezogene Daten müssen in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Art. 5 Abs. 1 lit. a DS-GVO). Dies erfordert insbesondere eine transparente Verarbeitung, bei der die Informationen über den Prozess der Verarbeitung und gegebenenfalls auch über die verwendeten Trainingsdaten leicht zugänglich und verständlich sind (Art. 12 DS-GVO). Entscheidungen, die auf Grundlage des Einsatzes von KI-Systemen erfolgen, müssen nachvollziehbar und erklärbar sein. Es genügt nicht die Erklärbarkeit im Hinblick auf das Ergebnis, darüber hinaus muss die Nachvollziehbarkeit im Hinblick auf die Prozesse und das Zustandekommen von Entscheidungen gewährleistet sein. Nach der DS-GVO ist dafür auch über die involvierte Logik ausreichend aufzuklären. Diese Transparenz-Anforderungen sind fortwährend zu erfüllen, wenn KI-Systeme zur Verarbeitung von personenbezogenen Daten eingesetzt werden. Es gilt die Rechenschaftspflicht des Verantwortlichen (Art. 5 Abs. 2 DS-GVO).

4. KI muss Diskriminierungen vermeiden

Lernende Systeme sind in hohem Maße abhängig von den eingegebenen Daten. Durch unzureichende Datengrundlagen und Konzeptionen kann es zu Ergebnissen kommen, die sich als Diskriminierungen auswirken. Diskriminierende Verarbeitungen stellen eine Verletzung der Rechte und Freiheiten der betroffenen Personen dar. Sie verstoßen u.a. gegen bestimmte Anforderungen der Datenschutz-Grundverordnung, etwa den Grundsatz der Verarbeitung nach Treu und Glauben, die Bindung der Verarbeitung an legitime Zwecke oder die Angemessenheit der Verarbeitung.

Diese Diskriminierungsneigungen sind nicht immer von vornherein erkennbar. Vor dem Einsatz von KI-Systemen müssen deshalb die Risiken für die Rechte und Freiheiten von Personen mit dem Ziel bewertet werden, auch verdeckte Diskriminierungen durch Gegenmaßnahmen zuverlässig auszuschließen. Auch während der Anwendung von KI-Systemen muss eine entsprechende Risikoüberwachung erfolgen.

5. Für KI gilt der Grundsatz der Datenminimierung

Für KI-Systeme werden typischerweise große Bestände von Trainingsdaten genutzt. Für personenbezogene Daten gilt dabei auch in KI-Systemen der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO). Die Verarbeitung personenbezogener Daten muss daher stets auf das notwendige Maß beschränkt sein. Die Prüfung der Erforderlichkeit kann ergeben, dass die Verarbeitung vollständig anonymer Daten zur Erreichung des legitimen Zwecks ausreicht.

6. KI braucht Verantwortlichkeit

Die Beteiligten beim Einsatz eines KI-Systems müssen die Verantwortlichkeit ermitteln und klar kommunizieren und jeweils die notwendigen Maßnahmen treffen, um die rechtmäßige Verarbeitung, die Betroffenenrechte, die Sicherheit der Verarbeitung und die Beherrschbarkeit des KI-Systems zu gewährleisten. Der Verantwortliche muss sicherstellen, dass die Grundsätze nach Art. 5 DS-GVO eingehalten werden. Er muss seine Pflichten im Hinblick auf die Betroffenenrechte aus Art. 12 ff DS-GVO erfüllen. Der Verantwortliche muss die Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO gewährleisten und somit auch Manipulationen durch Dritte, die sich auf die Ergebnisse der Systeme auswirken, verhindern. Beim Einsatz eines KI-Systems, in dem personenbezogene Daten verarbeitet werden, wird in der Regel eine Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO erforderlich sein.

7. KI benötigt technische und organisatorische Standards

Um eine datenschutzgerechte Verarbeitung sicherzustellen, sind für Konzeption und Einsatz von KI-Systemen technische und organisatorische Maßnahmen gem. Art. 24 und 25 DS-GVO zu treffen, wie z. B. Pseudonymisierung. Diese erfolgt nicht allein dadurch, dass der Einzelne in einer großen Menge personenbezogener Daten scheinbar verschwindet. Für den datenschutzkonformen Einsatz von KI-Systemen gibt es gegenwärtig noch keine speziellen Standards oder detaillierte Anforderungen an technische und organisatorische Maßnahmen. Die Erkenntnisse in diesem Bereich zu mehren und Best-Practice-Beispiele zu entwickeln ist eine wichtige Aufgabe von Wirtschaft und Wissenschaft. Die Datenschutzaufsichtsbehörden werden diesen Prozess aktiv begleiten.

III. Die Entwicklung von KI bedarf der Steuerung

Die Datenschutzaufsichtsbehörden überwachen die Anwendung des Datenschutzrechts, setzen es durch und haben die Aufgabe, bei der Weiterentwicklung für einen effektiven Grundrechtsschutz einzutreten. Angesichts der hohen Dynamik in der Entwicklung der Technologien von künstlicher Intelligenz und der vielfältigen Einsatzfelder zeichnen sich die Grenzen der Entwicklung noch nicht ab. Gleichermaßen sind die Risiken der Verarbeitung personenbezogener Daten in KI-Systemen nicht pauschal einzuschätzen. Auch ethische Grundsätze sind zu beachten. Wissenschaft, Datenschutz-aufsichtsbehörden, die Anwender und besonders die Politik sind gefordert, die Entwicklung von KI zu begleiten und im Sinne des Datenschutzes zu steuern.

Anlage 2: Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3. April 2019

Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten!

Unternehmen haften im Rahmen von Art. 83 Datenschutz-Grundverordnung (DS-GVO) für schuldhafte Datenschutzverstöße ihrer Beschäftigten, sofern es sich nicht um einen Exzess handelt. Dabei ist nicht erforderlich, dass für die Handlung ein gesetzlicher Vertreter oder eine Leitungsperson verantwortlich ist. Zurechnungseinschränkende Regelungen im nationalen Recht würden dem widersprechen.

Diese Haftung für Mitarbeiterverschulden ergibt sich aus der Anwendung des sogenannten funktionalen Unternehmensbegriffs des europäischen Primärrechts. Der funktionale Unternehmensbegriff aus dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV) besagt, dass ein Unternehmen jede wirtschaftliche Einheit unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung ist. Erwägungsgrund 150 der DS-GVO weist für die Verhängung von Geldbußen wegen Datenschutzverstößen gegen Unternehmen klarstellend darauf hin. Nach der Rechtsprechung zum funktionalen Unternehmensbegriff haften Unternehmen für das Fehlverhalten sämtlicher ihrer Beschäftigten. Eine Kenntnis der Geschäftsführung eines Unternehmens von dem konkreten Verstoß oder eine Verletzung der Aufsichtspflicht ist für die Zuordnung der Verantwortlichkeit nicht erforderlich. Handlungen von Beschäftigten, die bei verständiger Würdigung nicht dem Kreis der jeweiligen unternehmerischen Tätigkeit zugerechnet werden können („Exzesse"), sind ausgenommen.

Die alten nationalen Haftungsregeln wurden bisher nicht europarechtskonform der neuen Rechtslage angepasst. Unzutreffend verweist § 41 Abs. 1 des neuen Bundesdatenschutzgesetzes (BDSG) auf zurechnungseinschränkende Regelungen im OWiG. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) haben bereits im Rahmen des Gesetzgebungsverfahrens zum neuen Bundesdatenschutzgesetz darauf aufmerksam gemacht, dass diese Bestimmungen den Vorgaben der DS-GVO zur Verantwortlichkeit für Datenschutzverstöße widersprechen.

Die DSK begrüßt insoweit, dass der Koalitionsvertrag vorsieht, das Sanktionsrecht für Unter-nehmen generell im deutschen Recht so zu ändern, dass „die von Fehlverhalten von Mitarbeiterinnen und Mitarbeitern profitierenden Unternehmen stärker sanktioniert werden". Diese gebotene Modernisierung des deutschen Unternehmenssanktionsrechts entspräche dann auch dem europäischen Kartellrecht und dem etablierten internationalen Standard.

Die DSK fordert den Bundesgesetzgeber daher nochmals auf, in den Beratungen des Entwurfs des Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (DS-GVO) und zur Umsetzung der Richtlinie (EU) 2016/680 die §§ 30, 130 OWiG klarstellend vom Anwendungsbereich auszunehmen und damit dem europäischen Recht anzupassen.

Anlage 3: Entschließung der 98. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 6. November 2019

Empfehlungen für eine datenschutzkonforme Gestaltung von KI-Systemen

Auf der Grundlage der Hambacher Erklärung vom 03.04.2019 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in einem Positionspapier Anforderungen an KI-Systeme erarbeitet, deren Umsetzung die DSK für eine datenschutzkonforme Gestaltung von KI-Systemen empfiehlt. Die in der Hambacher Erklärung festgelegten rechtlichen Rahmenbedingungen werden damit im Hinblick auf technische und organisatorische Maßnahmen konkretisiert, die auf die unterschiedlichen Phasen der Lebenszyklen von KI-Systemen bezogen sind.

Die Phasen des Lebenszyklus eines KI-Systems – Designs des KI-Systems, Veredelung von Rohdaten zu Trainingsdaten, Training der KI-Komponenten, Validierung der Daten und KI-Komponenten sowie des KI-Systems, Einsatz des KI-Systems und die Rückkopplung von Ergebnissen – werden am Maßstab von Gewährleistungszielen untersucht. Um aus rechtlichen Anforderungen KI-spezifische technische und organisatorische Maßnahmen abzuleiten und zu systematisieren, werden die Gewährleistungsziele Transparenz, Datenminimierung, Nichtverkettung, Intervenierbarkeit, Verfügbarkeit, Integrität und Vertraulichkeit verwendet.

Für die Verarbeitung von personenbezogenen Daten, bei der KI-Systeme zum Einsatz kommen, gelten die in der DS-GVO formulierten Grundsätze. Mit dem Positionspapier wird Verantwortlichen im Umfeld von KI ein Handlungsrahmen für die datenschutzrechtlichen Vorgaben an die Hand gegeben, an dem sie sich bei der Planung und dem Betrieb von KI-Systemen orientieren können. Das Positionspapier soll verdeutlichen, dass der Einsatz von KI-Systemen und der Datenschutz keine zwingenden Gegensätze sind. Die Chancen und neuen Möglichkeiten des Einsatzes von KI-Systemen werden durch einen modernen Datenschutz nicht verhindert. Das Positionspapier soll die Entwicklung und den Einsatz von KI auch unter Nutzung personenbezogener Daten konstruktiv begleiten. Damit wird Handlungssicherheit gesteigert und sichergestellt, dass die Grundrechte und Grundfreiheiten der betroffenen Personen, insbesondere das Recht auf informationelle Selbstbestimmung, auch in dem dynamischen, von KI-Systemen geprägten Umfeld gewahrt werden.

Die DSK legt dieses Positionspapier auch vor, um den Dialog mit den relevanten Akteuren aus Politik, Wirtschaft, Wissenschaft und Gesellschaft wie den Verbrauchervereinigungen auf dieser Grundlage weiter zu intensivieren.

Anlage: Positionspapier der DSK

Anlage 4: Entschließung der 98. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 6. November 2019

Gesundheitseinrichtungen müssen unabhängig von ihrer Größe den Schutz von Patientendaten gewährleisten

Die Datenschutzkonferenz weist nachdrücklich darauf hin, dass die Sicherheit von Patientendaten in der medizinischen Behandlung nach der Datenschutz-Grundverordnung flächendeckend gewährleistet sein muss. Der effektive Schutz von Gesundheitsdaten darf nicht von der Größe der Versorgungseinrichtung abhängen.

In der jüngeren Vergangenheit häufen sich Vorfälle, in denen der Schutz von Patientendaten in der stationären Versorgung gefährdet ist. So wurden im Juli 2019 eine Reihe von Einrichtungen eines Trägers in Rheinland-Pfalz und dem Saarland Opfer eines Befalls mit Schadsoftware. Die durch diese erfolgte Verschlüsselung von Daten im IT-Verbund der Trägergesellschaft hat zu weitreichenden Beeinträchtigungen des Krankenhausbetriebs geführt. Im September 2019 wurde bekannt, dass weltweit mehr als 16 Millionen Datensätze, darunter 13.000 von in deutschen Gesundheitseinrichtungen behandelten Patienten, offen im Internet zugänglich waren. Ursache hierfür waren nach den bislang bekannt gewordenen Informationen insbesondere unzureichende technische und organisatorische Vorkehrungen zum Schutz dieser Daten.

Der Einsatz von Informations- und Kommunikationstechnik in der Gesundheitsversorgung ist im Zeitalter der digitalisierten Medizin unabdingbar. Allerdings müssen die in diesem Zusammenhang rechtlich gebotenen und nach dem Stand der Technik angemessenen Vorkehrungen zu einem effektiven Schutz der Daten von Patientinnen und Patienten flächendeckend getroffen werden. Dazu sind alle in diesem Zusammenhang tätigen Einrichtungen unabhängig von ihrer Größe aufgrund der Datenschutz-Grundverordnung verpflichtet.

Die Datenschutzkonferenz fordert vor dem Hintergrund einer zunehmenden Digitalisierung der Gesundheitsversorgung und angesichts der damit einhergehenden Gefährdungen ausdrücklich dazu auf, auch in finanzieller Hinsicht sicherzustellen, dass alle Einrichtungen des Gesundheitswesens die zum Schutz der Patientendaten nach dem Stand der Technik gesetzlich gebotenen Vorkehrungen ergreifen können.

Anlage 5: Entschließung der 98. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 6. November 2019

Gesundheitswebseiten und Gesundheits-Apps – Keine Weitergabe sensibler Daten an unbefugte Dritte!

Mit zunehmender Sorge beobachtet die Datenschutzkonferenz, dass Betreiber von Gesundheitswebseiten und Gesundheits-Apps auch sensible personenbezogene Daten der Nutzerinnen und Nutzer ohne erkennbare Verarbeitungsgrundlage an Dritte weiterleiten. Unter anderem geschieht dies durch Tracking – und Analyse-Tools (also Programme, die das Surfverhalten beobachten und analysieren), von deren Einsatz die betroffenen Personen keine Kenntnis haben.

So wurde im September 2019 durch die Studie einer Nichtregierungsorganisation bekannt, dass zahlreiche Betreiber von Gesundheitswebseiten, die ihren Besuchern Informationen zu Depression und anderen psychischen Krankheiten anbieten, personenbezogene Nutzungsdaten ohne adäquate Einbindung der Nutzerinnen und Nutzer an andere Stellen weitergeleitet haben sollen. Teilweise soll dabei sogar die Teilnahme an Depressions-Selbsttests erfasst worden sein. Auch von 44 analysierten deutschen Webseiten besäßen weit über die Hälfte solche integrierten Bausteine, die dies ermöglicht hätten. Im Oktober 2019 wurden Recherchen veröffentlicht, wonach eine in Deutschland ansässige Diagnostik-App ebenfalls Tracking- und Analyse-Dienste nutze und in diesem Zusammenhang sensible Gesundheitsdaten wie z. B. körperliche Beschwerden ohne vorherige Information und Legitimation der Nutzer an Dritte weiterleite.

Zu den Datenempfängern gehören häufig neben sonstigen Tracking-Dienstleistern große Unternehmen wie Facebook, Google und Amazon, die vorrangig eigene Geschäftsinteressen verfolgen. Die Verknüpfung der weitergeleiteten Daten mit anderen Informationen begründet das Risiko, dass für jede Nutzerin und jeden Nutzer ein personenbezogenes Gesundheitsprofil entsteht, von dessen Existenz und Umfang die betroffenen Personen nichts wissen.

Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder prüfen im Rahmen ihrer Aufgaben und Möglichkeiten derartige Hinweise und werden Datenschutzverletzungen gegebenenfalls sanktionieren. Zugleich ist der Gesetzgeber aufgerufen, im Zusammenhang mit der bevorstehenden Einführung digitaler Gesundheitsanwendungen in die Regelversorgung den Schutz der Vertraulichkeit sensibler Gesundheitsdaten sicherzustellen. Beispielsweise wäre es nicht hinzunehmen, wenn die Nutzung einer von der Regelversorgung erfassten Gesundheits-App zwingend an gesetzlich nicht vorgesehene Weiterleitungen von Gesundheitsdaten gekoppelt würde.

Die Datenschutzkonferenz fordert die Betreiber von Gesundheitswebseiten und Gesundheits-Apps auf, die berechtigten Vertraulichkeitserwartungen ihrer Nutzerinnen und Nutzer zu respektieren. Unabhängig von den allgemeinen datenschutzrechtlichen Anforderungen an die Weitergabe personenbezogener Gesundheitsdaten sind dabei insbesondere folgende Anforderungen zu beachten:

— Leiten Betreiber von Gesundheitswebseiten und Gesundheits-Apps personenbezogene Nutzungsdaten an andere Stellen weiter, sind sie für diese

Datenweitergabe verantwortlich, selbst wenn sie – wie etwa bei der Einbindung von Social Plugins – keinen eigenen Zugriff auf die weitergeleiteten Daten haben.

— Als Verantwortliche sind Betreiber insoweit verpflichtet, die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu beachten. Die eingangs beschriebene Weiterleitung von Gesundheitsdaten kann nach Art. 9 Abs. 1, 2 Buchst. a Datenschutz-Grundverordnung ausnahmsweise nur auf Grundlage einer vor der Datenverarbeitung eingeholten ausdrücklichen Einwilligung zulässig sein, die auch den übrigen Wirksamkeitsvoraussetzungen einer datenschutzrechtlichen Einwilligung genügen muss.

— Insbesondere unterliegt die Einwilligung in die Verarbeitung von Gesundheitsdaten strengen Transparenzanforderungen: Unter anderem muss sie konkret benennen, wer für die Verarbeitung verantwortlich ist und welche Kategorien personenbezogener Daten, wie beispielsweise Gesundheitsdaten, Informationen über die sexuelle Orientierung oder zum Sexualleben verarbeitet werden. Auch die Zwecke der Datenverarbeitung und die Empfänger von weitergeleiteten Daten sind konkret zu benennen. Diese Informationen müssen die Nutzerinnen und Nutzer in die Lage versetzen, sich über die Konsequenzen ihrer erteilten Einwilligung bewusst zu werden.

— Im Rahmen der Regelversorgung wäre die einwilligungsbasierte Weiterleitung von Nutzerdaten an Tracking- oder Analyse-Dienstleister oder sonstige Dritte, die nicht Teil der Gesundheitsversorgung sind, allenfalls zulässig, wenn dies gesetzlich geregelt würde. Gegen eine solche gesetzliche Regelung bestünden allerdings im Hinblick auf das Erfordernis der freiwilligen Einwilligung erhebliche Bedenken.

Im Übrigen weist die Datenschutzkonferenz darauf hin, dass sich aus dem dargestellten Sachverhalt erneut die dringende Notwendigkeit ergibt, möglichst zeitnah eine ePrivacy-Verordnung zu verabschieden. Darin müssen die Bedürfnisse des elektronischen Datenverkehrs mit den Erfordernissen der Grundrechte auf Privatheit und auf Datenschutz in Einklang gebracht werden. Es sind insbesondere Regelungen erforderlich, die einen hohen Schutz sensibler Daten effektiv sicherstellen.

Anlage 6: Entschließung der 98. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 6. November 2019

Keine massenhafte automatisierte Aufzeichnung von Kfz-Kennzeichen für Strafverfolgungszwecke!

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

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

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

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

Die DSK lehnt Vorschläge ab, die auf die Schaffung einer neuen Rechtsgrundlage für derartige strafprozessuale Maßnahmen abzielen. Nach verfassungsgerichtlicher Rechtsprechung stellen bereits die automatisierten Kfz-Kennzeichen-Kontrollen zur Fahndung nach Personen oder Sachen einen Eingriff von erheblichem

Gewicht dar, selbst wenn die Kfz-Kennzeichen unverzüglich spurenlos gelöscht werden. Eine längerfristige Aufzeichnung sämtlicher Kennzeichen begründet demgegenüber einen deutlich schwerwiegenderen Grundrechtseingriff.

Anlage 7: Entschließung der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

Keine Abschaffung der Datenschutzbeauftragten

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) spricht sich gegen eine Abschaffung oder Verwässerung der die Datenschutzgrundverordnung ergänzenden nationalen Regelungen der Pflicht zur Benennung einer oder eines Datenschutzbeauftragten aus.

Nach § 38 Bundesdatenschutzgesetz müssen z. B. Unternehmen und Vereine Datenschutzbeauftragte benennen, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Diese Pflicht hat sich seit vielen Jahren bewährt und ist deshalb auch bei der Datenschutzreform im deutschen Recht beibehalten worden.

Die Datenschutzbeauftragten sorgen für eine kompetente datenschutzrechtliche Beratung, um Datenschutzverstöße schon im Vorfeld zu vermeiden und das Sanktionsrisiko gering zu halten. Dies hat sich ganz besonders bei der Umstellung auf die Datenschutz-Grundverordnung bewährt.

Auch beim Wegfall der nationalen Benennungspflicht von Datenschutzbeauftragten bleiben die Pflichten des Datenschutzrechts bestehen. Verantwortliche verlieren jedoch interne Beraterinnen und Berater zu Fragen des Datenschutzes. Der Wegfall mag kurzfristig als Entlastung empfunden werden. Mittelfristig geht interne Kompetenz verloren.

Eine Aufweichung dieser Benennungspflicht, insbesondere für kleinere Unternehmen und Vereine, wird diese daher nicht entlasten, sondern ihnen mittelfristig schaden.

Abkürzungsverzeichnis

ABl.	Amtsblatt der Europäischen Union
Abs.	Absatz
AFD	Alternative für Deutschland
App	Application, Anwendungsprogramm auf Smartphone
Art.	Artikel
BayDSG	Bayerisches Datenschutzgesetz
BayDSG-alt	Bayerisches Datenschutzgesetz in der bis zum 24. Mai 2018 geltenden Fassung
BeckOK	Beck'scher Online-Kommentar
BeckRS	Beck-Rechtsprechung
BDSG	Bundesdatenschutzgesetz
Buchst.	Buchstabe
CSU	Christlich-Soziale Union in Bayern
DNA	Desoxyribonuclein Acid, Träger der Erbinformation
DSFA	Datenschutzfolgenabschätzung
DSGVO	Datenschutz-Grundverordnung
EDV	Elektronische Datenverarbeitung
EU	Europäische Union
EuGH	Europäischer Gerichtshof
FDP	Freie Demokratische Partei
ff.	(nach)folgende
GVBl.	Bayerisches Gesetz- und Verordnungsblatt
https	Hyper Text Transfer Protocol Secure
IP	Internet Protocol
IT	Informationstechnik
lit.	Buchstabe
MdL	Mitglied des Landtages
m. w. N.	mit weiteren Nachweisen
Nr.	Nummer
PC	Personalcomputer
RLDSJ	Datenschutz-Richtlinie für Polizei und Strafjustiz
Rn.	Randnummer
sog.	sogenannt
SPD	Sozialdemokratische Partei Deutschlands
SSL	Secure Socket Layer
u. a.	unter anderem/und andere
UAbs.	Unterabsatz
vgl.	vergleiche
www	World Wide Web
z. B.	zum Beispiel

Stichwortverzeichnis

Der Bayerische
Landesbeauftragte
für den
Datenschutz

Wagmüllerstraße 18
80538 München
Postfach 22 12 19
80502 München
Telefon 089 21 26 72-0
Telefax 089 21 26 72-50

poststelle@datenschutz-bayern.de
www.datenschutz-bayern.de