Landtag von Baden-Württemberg **Drucksache 16 / 3290**

16. Wahlperiode **18. 01. 2018**

Mitteilung

des Landesbeauftragten für den Datenschutz und die Informationsfreiheit

33. Datenschutz-Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit für die Jahre 2016/2017

Schreiben des Landesbeauftragten für den Datenschutz und die Informationsfreiheit vom 18. Januar 2018:

Anbei übersende ich Ihnen meinen 33. Tätigkeitsbericht für den Datenschutz.

Dr. Brink

Eingegangen: 18. 01. 2018 / Ausgegeben: 16. 02. 2018

33. Datenschutz-Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg 2016/2017

Inhaltsverzeichnis

Vorwort

Die zwei Jahre, die der nun vorliegende Tätigkeitsbericht des Landesbeauftragten für den Datenschutz umfasst, liegen inmitten einer Zeitenwende. Entscheidende Weichenstellung war und ist die Verabschiedung der europäischen Datenschutz-Grundverordnung, die ab dem 25. Mai 2018 in der EU unmittelbar geltendes Datenschutzrecht sein wird. Rückblickend wird man noch in vielen Jahren bei der Beurteilung der Entwicklung des Datenschutzes in Deutschland und Europa die Zeit vor und die Zeit nach Inkrafttreten der Europäischen Datenschutz-Grundverordnung prinzipiell unterscheiden: In die vielleicht „gute", jedenfalls dann aber alte Zeit des deutschen Datenschutzes mit seinen Landesgesetzen (seit den 1970er Jahren) und seinem Bundesdatenschutzgesetz, mit kleinen Aufsichtsbehörden ohne nennenswerte Durchschlagskraft und mit einem Grundrecht auf informationelle Selbstbestimmung, das den deutschen Weg des Datenschutzes bahnte, aber von vielen Betroffenen wenig geschätzt wurde. Und in die neue Epoche des Datenschutzes, an deren Beginn wir jetzt stehen: mit Datenschutz-Folgenabschätzungen und Privacy by Design, mit Bußgeldern in abschreckender Höhe, Klagen von Betroffenen gegen Aufsichtsbehörden und Handlungsempfehlungen des Europäischen Datenschutz-Ausschusses.

Der Berichtszeitraum ist daher geprägt von Erwartung und Vorbereitung, die Datenschutz-Grundverordnung ist das schon im Vorhinein alles beherrschende Thema. Dass „im Schlagschatten der DS-GVO" auch ganz wesentliche Entwicklungen in Deutschland und Baden-Württemberg einsetzten, davon zeugt der nun vorgelegte Tätigkeitsbericht. Er zeichnet dabei nicht nur Sachentscheidungen nach, sondern fußt zugleich auf personellen Ereignissen, welche die Arbeit der Behörde des Landesbeauftragten prägten: Im Mai 2016 trat der langjährige Landesbeauftragte Jörg Klingbeil in den Ruhestand über. Er hat die Behörde und ihr Auftreten wesentlich geprägt und – wie sich nun zeigt – wichtige und richtige Weichenstellungen getroffen, auf denen wir heute aufbauen. Mein Kollege Klingbeil war es, der durch umsichtige und treffsichere Personalauswahl eine Verjüngung der Landesbehörde einleitete und ihre Vernetzung in die Landesregierung vorantrieb. Bis Dezember 2016 führte Volker Broo als Leitender Beamter die Behörde erfahren und sicher weiter. Seit Januar 2017 kann ich an diese Arbeit anknüpfen.

Der Berichtszeitraum war aber auch geprägt von deutlichen, zum Teil sogar harten Auseinandersetzungen um den Datenschutz: Gerade die hoheitlichen Datenverarbeiter greifen immer beherzter auf die Datenbestände und die modernen Technologien von Privatunternehmen zu und rüsten sich mit neuen Verarbeitungsbefugnissen – von der Bodycam bis zur präventiven Quellen-Telekommunikationsüberwachung.

Auch die Wirtschaftsunternehmen bereiten sich auf das neue Zeitalter vor. Sie taten dies in den zurückliegenden zwei Jahren zum Teil sehr selbstständig und engagiert, zum Teil allerdings auch angetrieben von den neuen Bußgelddrohungen. Nur wenige Unternehmen setzen weiter auf Risiko und ignorieren die neuen Datenschutzanforderungen genauso wie bereits die alten. Diese Strategie wird sich als zu riskant erweisen; wer so handelt, hat als Unternehmer bereits verloren – jedenfalls das Vertrauen seiner Kunden, Geschäftspartner und Beschäftigten.

Genau an dieser Schnittstelle setzt die Tätigkeit einer modernen Datenschutz-Aufsichtsbehörde an. Bestimmte bereits das „gute alte BDSG" in seinem § 38 Absatz 1 Satz 2: Die Aufsichtsbehörde „berät und unterstützt die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse", so verstärkt die DS-GVO diese Aufgabenzuweisung an den LfDI noch. Denn zu den Bedürfnissen der Unternehmen zählt gerade jetzt die vorbereitende Begleitung auf dem Weg in die DS-GVO. Und auch die Aufsichtsbehörden stehen vor ihrer größten Herausforderung: sich auf diesem Weg in die DS-GVO durch Orientierungshilfen, Handlungsempfehlungen und Musterentwürfe so nützlich wie nur möglich zu machen – für die Bürgerinnen und Bürger, aber ebenso für die Unternehmen und ihre betrieblichen Datenschützer; letztere sind die wahren Taktgeber des Fortschrittes beim „gelebten" Datenschutz. Und diese neue Aufgabe wartet nicht erst im Mai 2018, sie stellte sich bereits höchst intensiv im Verlauf der vergangenen zwei Jahre.

Entscheidend für die Zukunft der informationellen Selbstbestimmung der Bürgerinnen und Bürger wird aber ein anderes sein, nämlich: Welche Bedeutung messen wir als Betroffene und Grundrechtsträger zukünftig unserem Freiheitsrecht zu? Sind wir bloß willige Konsumenten, denen Annehmlichkeiten und „Dabei-

sein" wichtiger scheinen als die Chance, unsere Selbstbestimmung auch unter rasant sich ändernden technischen Bedingungen zu bewahren und nach eigenem Dafürhalten zu nutzen? Ein Grundrecht ohne Grundrechtsträger, die seine Substanz auch wertschätzen, hat keine Zukunft – auch nicht mit einer Europäischen DS-GVO.

Die Zeiten sind also an der Schwelle zur Digitalisierung unserer Lebenswelt keineswegs leicht für den Datenschutz. Aber eine ermutigende Ausstattung des LfDI durch das Landesparlament und der neue Schwung, den die DS-GVO mit sich bringt, lassen die Datenschützer gespannt und vielleicht sogar optimistisch in die Zukunft blicken. Die Grundlagen für diese Zuversicht finden sich in diesem Tätigkeitsbericht.

Mit der Vorlage dieses Tätigkeitsberichtes darf ich mich sehr herzlich nicht nur bei meinem Amtsvorgänger und meinem Stellvertreter, sondern bei allen meinen Mitarbeiterinnen und Mitarbeitern für die hervorragende Arbeit bedanken. Datenschutz ist nicht nur ein Querschnittsthema, sondern wandelt sich zugleich mit dem technologischen Fortschritt in geradezu erschreckender Eile. Datenschutz fordert uns – und manchesmal droht er uns auch zu überfordern. Hierbei die Tatkraft und den Überblick zu bewahren, ist eine große Aufgabe.

Bedanken darf ich mich an dieser Stelle aber auch bei den Abgeordneten des Landtags Baden-Württemberg, welche unsere Aufgabe maßgeblich gestalten, begleiten und fördern.

Ihr Landesbeauftragter

Dr. Stefan Brink

1. Schwerpunkte

1.1 „From kitten to tiger"? Die DS-GVO stellt uns alle vor neue Herausforderungen

Die Datenschutz-Grundverordnung (DS-GVO)[1] gilt ab dem 25.05.2018 und stellt viele verantwortliche Stellen vor umfassende Probleme. Die Ablösung des bisherigen Bundesdatenschutzgesetzes (BDSG a.F.)[2] durch die neue Verordnung, die in allen Mitgliedstaaten der Europäischen Union unmittelbare Geltung beansprucht, ist für alle Beteiligten – den LfDI selbst sowie öffentliche und private Stellen – mit größeren Umstrukturierungen verbunden. Wie muss die interne Organisation geändert werden? Welche neuen rechtlichen Vorgaben sind zu beachten? Was ändert sich mit Blick auf die Arbeitsprozesse? Dies alles sind Fragen, deren Klärung bei Aufsichtsbehörden und datenverarbeitenden Stellen viel Arbeitseinsatz erfordern. Schon im Berichtszeitraum hat sich ein großer Teil der Beratungspraxis der Dienststelle auf diese neuen Fragestellungen konzentriert. Zudem wurden wichtige Weichenstellungen im Hinblick auf die personelle Ausstattung und organisatorische Ausgestaltung des LfDI vorgenommen. Die wichtigsten strukturellen und inhaltlichen Veränderungen durch die DS-GVO sollen daher an dieser Stelle aufgegriffen werden.

1.1.1 Die zukünftige Rolle und Neuausrichtung des LfDI

Mit der Europäischen DS-GVO wurde ein unmittelbar und übergreifend geltendes, Behörden wie Unternehmen gleichermaßen erfassendes, einheitliches Rechtsregime für Europa erlassen, das ab Mai 2018 jede Verarbeitung personenbezogener Daten im europäischen Raum reguliert. An die Stelle nationaler Rechtsvorschriften und föderaler Vollzugsbehörden tritt ein einheitliches europäisches Recht, das durch „harmonisierte" Aufsichtsbehörden, zu denen auch der LfDI Baden Württemberg zählt, einheitlich umgesetzt wird. Eine neue Ära des europäischen Datenschutzes steht bevor. Hieraus ergeben sich zahlreiche Änderungen auch für den LfDI als Aufsichtsbehörde (s. näher zu den personellen und Ressort-bezogenen Änderungen das Kapitel „Aus der Dienststelle").

I. Die neue Rolle der Aufsichtsbehörde unter der DS-GVO

Die Verordnung stärkt die Rolle der nationalen Aufsichtsbehörden, welche nunmehr als Beschützer eines Europäischen Datenschutzrechts agieren. Um dieser neuen Rolle entsprechen zu können, verleiht die DS-GVO den Aufsichtsbehörden vollkommene Unabhängigkeit und schlagkräftige Vollstreckungsbefugnisse, die bei Bedarf grenzüberschreitend eingesetzt werden können. Die DS-GVO erweitert den Aufgabenbereich der Aufsichtsbehörden erheblich. Auch auf den LfDI kommt daher künftig wesentlich mehr Arbeit zu. So enthält alleine Art. 57 DS-GVO einen Aufgabenkatalog von 21 unterschiedlichen Einzelaufgaben; weitere Aufgaben aus unterschiedlichen Artikeln der DS-GVO treten hinzu. Teils finden sich in diesem Katalog Aufgaben, die schon jetzt zum Selbstverständnis der deutschen Datenschutzaufsichtsbehörden gehören. Zu nennen sind insbesondere die Aufklärung der Öffentlichkeit über die Risiken, Rechte und Garantien, die bei der Verarbeitung personenbezogener Daten ein Rolle spielen (Art. 57 Abs. 1 lit. b DS-GVO), die Unterstützung der Betroffenen bei der Wahrnehmung ihrer Betroffenenrechte, die Beratung des Parlaments und der Regierung zu datenschutzrechtlichen Fragen sowie die Sensibilisierung der verantwortlichen Stellen über ihre Pflichten im Zusammenhang mit dem Schutz personenbezogener Daten (Art. 57 Abs. 1 lit. d DS-GVO). Die Aufgabe des LfDI erschöpft sich nach der DS-GVO nicht mehr in der „bloßen" Überwachung und reaktiven Sanktionierung der Verantwortlichen, die personenbezogene Daten verarbeiten. Vielmehr sollen die Aufsichtsbehörden auch proaktiv Aufklärungs- und Sensibilisierungsarbeit leisten und den Verantwortlichen bei Fragen unterstützend zur Seite stehen.

II. Status des LfDI als oberste Landesbehörde

Zentrale Bedeutung hat die Unabhängigkeit der Aufsichtsbehörden, die in Art. 52 DS-GVO festgelegt ist. Die Aufsichtsbehörden müssen

1 Datenschutz-Grundverordnung (VO [EU] 2016/679), v. 27.04.2016, ABl.EU Nr. L 119 v. 04.05.2016, S. 1 ff.

2 Bundesdatenschutzgesetz (BDSG), v. 14.01.2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 10 Absatz 2 des Gesetzes v. 31.10.2017 (BGBl. I S. 3618).

frei von Weisungen und frei von einer Rechts- und Dienstaufsicht handeln können und dürfen daher keiner indirekten oder direkten Einflussnahme ausgesetzt sein. Eine zwingende Voraussetzung, um die Unabhängigkeit zu gewährleisten ist eine ausreichende und angemessene personelle und finanzielle Ausstattung der Aufsichtsbehörden, damit diese ihre zahlreichen Aufgaben und Befugnisse wirksam wahrnehmen können. Eine Stärkung der Unabhängigkeit der Datenschutzaufsichtsbehörden durch die DS-GVO ist organisatorisch zwingend an die Voraussetzung geknüpft, den LfDI als oberste Landesbehörde zu organisieren. Eine entsprechende gesetzliche Grundlage wird im Rahmen der anstehenden Beratungen der Anpassung des Landesdatenschutzgesetzes (LDSG) an die DS-GVO geschaffen.

III. Erhöhter Abstimmungsbedarf unter den Aufsichtsbehörden

Bislang legte jede Aufsichtsbehörde der Mitgliedstaaten – einschließlich der deutschen Aufsichtsbehörden – ihr nationales Recht aus. Ein koordiniertes Zusammenwirken fand hierbei nur vereinzelt statt. So konnten beispielsweise Unternehmen in einem Land von der dortigen unzureichenden Datenschutzkontrolle profitieren. Um eine EU-weit einheitliche Anwendung und Auslegung der DS-GVO zu gewährleisten, werden die Aufsichtsbehörden zukünftig über die Ländergrenze hinaus zur Abstimmung untereinander verpflichtet. Arbeitsintensive Abstimmungsmechanismen unter den 17 deutschen Aufsichtsbehörden und in Zukunft auch mit den anderen mitgliedstaatlichen Aufsichtsbehörden werden im Rahmen des Kohärenzverfahrens zu verbindlichen Mehrheitsentscheidungen führen. Erhöhter Abstimmungsbedarf wird zudem auch bei solchen Fällen entstehen, in denen ein Unternehmen Niederlassungen in mehreren Mitgliedstaaten besitzt. Im Kohärenzverfahren, also beim Auftreten unterschiedlicher Meinungen zu einem Beschlussvorschlag, wird zukünftig die Stellungnahme des Europäischen Datenschutzausschusses (EDSA) eingeholt werden müssen. Darüber hinaus kann jede Aufsichtsbehörde bei Angelegenheiten mit allgemeiner Geltung eine Stellungnahme des EDSA bewirken. Der Europäische Datenschutzausschuss besteht aus den Leitern der Aufsichtsbehörden, je einer pro Mitgliedstaat. Aufgrund der föderalen Struktur in Deutschland werden in Deutschland ein Vertreter der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und ein Vertreter der Aufsichtsbehörden der Länder gemeinsam von dem Stimmrecht im EDSA Gebrauch machen. Der LfDI wird eine neue Stellung im europäischen Gefüge erhalten: Durch das in der DS-GVO verankerte One-Stop-Shop-Prinzip werden neue Prozesse mit großem Abstimmungsbedarf zwischen der federführenden und den anderen betroffenen Aufsichtsbehörden unter Einhaltung kurzer Fristen zu meistern sein. Der LfDI wird sich in Zukunft in einer Vielzahl von Verfahren (Beschlüsse und Stellungnahmen) in einem mehrstufigen fristgebundenen europäischen Abstimmungsprozess befinden.

IV. Rechtliche und technische Beratungstätigkeiten als ein wesentlicher neuer Schwerpunkt

Die DS-GVO gilt unmittelbar in allen Mitgliedstaaten und hat gegenüber entsprechenden nationalen Regelungen wie dem BDSG, dem LDSG sowie den zahlreichen bereichsspezifischen Datenschutzregelungen Vorrang. Dies löst – vor allem auch mit Blick auf verbleibende nationale Regelungsbefugnisse (sog. Öffnungsklauseln), die in ihrer Reichweite und Rechtsnatur äußerst umstritten sind – nicht nur bei Unternehmen und Behörden, sondern auch bei Ministerien – erheblichen zusätzlichen Beratungsbedarf aus. Zudem wächst dem LfDI die in dieser Form und in diesem Umfang bisher nicht bestehende Befugnis zu, den Anwendungsvorrang der DS-GVO durch Anordnungen gegenüber Behörden durchzusetzen. Dies wird entsprechenden Beratungs- und auch Rechtsdurchsetzungsaufwand einschließlich der Vertretung vor Verwaltungsgerichten und der Beteiligung an Vorabentscheidungsverfahren vor dem Europäischen Gerichtshof (EuGH) auslösen. Die Beratungstätigkeiten des LfDI sind hierbei nicht nur auf rechtliche Fragestellungen begrenzt, sondern erfassen selbstredend auch technische Fragestellungen. So gestaltet die DS-GVO den sogenannten technischen Datenschutz, der durch technisch-organisatorische Maßnahmen Zielsetzungen des Datenschutzes unterstützt (vgl. § 9 BDSG a.F.), wesentlich um: Technische Maßnahmen werden in den Planungsprozess von Datenverarbeitungen vorverlagert und verbindlich gemacht (Privacy by Design/Privacy by Default). Unternehmen und Behörden haben zukünftig also auch in diesem Bereich einen rechtsverbindlichen Beratungsanspruch.

Um auf diesen Anstieg der Beratungstätigkeiten zu reagieren und insbesondere die Ein-

führung der DS-GVO inhaltlich vorzubereiten, wurde in einem ersten Schritt im Mai 2017 beim LfDI die „Stabsstelle Europa" eingerichtet. Sie ist erster Ansprechpartner und Unterstützer, wenn private und öffentliche Stellen Beratungen und Schulungen benötigen, um fit für die DS-GVO zu werden. Zudem fungiert sie im Haus als Koordinierungsstelle für sämtliche referatsübergreifende Querschnittsaufgaben mit Blick auf die DS-GVO und organisiert die Inhouse-Schulungen der Mitarbeiter.

Der LfDI steht zudem im ständigen Austausch mit den jeweiligen Akteuren, angefangen von in Baden-Württemberg ansässigen (Wirtschafts-)Unternehmen, über deren regional organisierte, branchenübergreifende Verbände, kommunale Interessenverbände bis hin zu Ministerien und öffentliche Stellen. Seit meinem Dienstbeginn wurden zahlreiche Schulungen und Einzelberatungen durchgeführt, um den Verantwortlichen Orientierung zu geben. Diese Aufgabe wird mit dem Inkrafttreten der DS-GVO im Mai 2018 natürlich nicht enden. Hier gilt dann „Nach dem Spiel ist vor dem Spiel". Unsere Beratungs- und Öffentlichkeitsarbeit werden wir im Jahr 2018 fortsetzen und intensivieren. Schon zum jetzigen Zeitpunkt ist der bei uns angemeldete Schulungsbedarf immens und dies zu recht: Wer kann schließlich besser als die Aufsichtsbehörde selbst Antworten auf die schwierigen Fragen geben, wie man sich rechtskonform auf die DS-GVO vorbereiten und die abschreckenden Sanktionen verhindern kann?

Im Sinne umfassender und innovativer Beratungsangebote fand daher Ende Oktober 2017 erstmals in Kooperation mit dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. eine Herbstkonferenz unter dem Titel „Herausforderungen der DS-GVO – Wirtschaft trifft Aufsicht" statt. Hier hatte der Landesbeauftragte die Schirmherrschaft dieser Fachtagung übernommen und sie inhaltlich wesentlich mitgestaltet. Im intensiven Austausch mit den Aufsichtsbehörden aus Baden-Württemberg, Bayern und Rheinland-Pfalz und vielen aus der Wirtschaft stammenden Referenten erhielten die teilnehmenden Unternehmen und Datenschutzbeauftragten Orientierungshilfen, Handlungsempfehlungen und Musterentwürfe, um sich optimal auf die Anforderungen, welche die DS-GVO mit sich bringt, vorzubereiten. Erstmals konnten nicht nur bundeslandübergreifende, sondern auch internationale Fachgespräche und Vorträge angeboten werden. Wir haben uns besonders über den Zuspruch und die Unterstützung durch Kollegen aus der Schweiz und Liechtenstein gefreut. Die enorme Teilnehmerzahl (mehr als 200) hat deutlich zum Ausdruck gebracht, dass mit dem erstmals angebotenen Format „Wirtschaft trifft Aufsicht" ein zukunftsweisendes Erfolgsmodell geschaffen wurde.

V. Neue weitreichende Sanktionsbefugnisse

Die DS-GVO setzt im Bereich von Rechtsverstößen auf ein massives Abschreckungskonzept (vgl. Art. 83 DS-GVO). Jede Aufsichtsbehörde der EU hat zukünftig sicher zu stellen, dass die Verhängung von Geldbußen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist (Art. 83 Abs. 1 DS-GVO). Im Vollzug kann dies – je nach Art des in der DS-GVO geregelten Verstoßes – in Geldbußen bis zu 20 Millionen Euro oder aber in einer Geldbuße bis zu 4 % des gesamten weltweit erzielten Unternehmensjahresumsatzes münden. Solche immensen Bußgeldhöhen kannte das deutsche Recht bislang vor allem im Kartellrechtsbereich. Dem Datenschutzrecht hingegen waren derartige Bußgeldhöhen fremd: Datenschutzverstöße waren innerhalb des alten BDSG auf höchstens dreihunderttausend Euro gedeckelt. Verstöße gegen die Datensicherheit (§ 9 BDSG a.F.) wurden nicht geahndet. Dies alles ändert sich nun. Mit den neuen Sanktionierungsmöglichkeiten sind auch organisatorische Änderungen verbunden. Bislang war das Regierungspräsidium Karlsruhe für die Ahndung und Verfolgung von Ordnungswidrigkeiten bei Datenschutzverstößen zuständig. Künftig kann der LfDI mit seiner neu zu schaffenden Bußgeldstelle eigenständig Geldbußen verhängen und festsetzen. Unabhängig von der Sanktionierung privatwirtschaftlicher Stellen kann der LfDI zukünftig auch gegenüber öffentlichen Stellen Anordnungen erlassen. Bislang konnten in diesem Bereich nur förmliche Beanstandungen ausgesprochen werden. Um seiner Aufgabe nach der DS-GVO gerecht werden können, wird der LfDI ab Mai 2018 daher die Fähigkeit besitzen, in Bußgeldverfahren selbst zu ermitteln und die Sanktionierung von Datenschutzverstößen vor Gericht durchzusetzen.

1.1.2. Inhaltliche Neuerungen durch die DS-GVO als Schwerpunkte in der Beratungspraxis

Die ab dem 25. Mai 2018 geltende DS-GVO bringt neben den oben beschriebenen Änderungen im strukturell-organisatorischen Bereich auch zahlreiche neue inhaltliche Vorschriften mit sich. Rechtsinstrumente, die auf den ersten Blick vermeintlich mit der alten Rechtslage übereinstimmen, sind teilweise abweichend normiert oder zumindest im Lichte des europäischen Datenschutzgrundrechts aus Art. 8 der Charta der Grundrechte der Europäischen Union (GRCh) aus europäischer Perspektive neu zu interpretieren. Aus der Vielzahl neuartiger Regelungen sind die einheitliche Normierung des Datenschutzes im öffentlichen und privaten Bereich, die neuen Einwilligungsvorschriften, bisher noch nicht implementierte Betroffenenrechte sowie die Änderungen im Bereich der Informationspflichten, Mitteilungspflichten um Datenpannen, der Auftragsdatenverarbeitung wie auch der Sanktionen hervorzuheben. Insoweit geben die folgenden Ausführungen zusammengesehen mit den oben ausgeführten Sanktionsregelungen einen ersten Überblick über das vielschichtige und umfangreiche Regelungswerk der neuen Verordnung, welches insbesondere im Jahr 2017 eine beherrschende Rolle bei der Beratung gespielt hat.

I. Datenschutz im öffentlichen und privaten Bereich

Das bis dato geltende BDSG a.F. sieht zumindest in systematischer Hinsicht die Trennung des öffentlichen und privaten Bereichs vor. Zwar besteht auch nach § 4 f Abs. 1 S. 1 BDSG a.F. für öffentliche und nicht-öffentliche Stellen die Pflicht zur Bestellung eines Datenschutzbeauftragten, der die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Im Gegensatz zu den Rechtsgrundlagen für die Datenverarbeitung von nicht-öffentlichen Stellen und öffentlich-rechtlichen Wettbewerbsunternehmen waren die Rechtsgrundlagen für die Datenverarbeitung von öffentlichen Stellen in der Vergangenheit jedoch in getrennten Abschnitten geregelt. Die DS-GVO verfolgt demgegenüber einen gesamtheitlichen Regelungsansatz, indem sie für beide Bereiche einheitliche Rechtsgrundlagen zur Verfügung stellt. Den Unterschieden von öffentlichem und privatem Bereich wird dadurch Rechnung getragen, dass den Mitgliedsstaaten über sogenannte Öffnungsklauseln, beispielsweise bei Vorliegen eines entsprechenden öffentlichen Interesses, die Möglichkeit gegeben wird, eigene Regelungen zu erlassen. Im Bereich der Öffnungsklauseln dürfen die Mitgliedstaaten somit trotz des einheitlichen Regelungsanspruches der Datenschutz-Grundverordnung eigene Gesetze auf mitgliedstaatlicher Ebene erlassen. Auf diese Weise können die Eigenheiten des jeweiligen nationalen Bereichs und die Souveränität der Mitgliedstaaten angemessen berücksichtigt werden.

II. Einwilligung

Wie auch schon das BDSG a.F. folgt die DS-GVO insbesondere in Art. 6 Abs. 1 lit. a DS-GVO dem Opt-In-Ansatz, nach dem die Verarbeitung von Daten grundsätzlich rechtmäßig ist, wenn der Betroffene seine Einwilligung für bestimmte Verarbeitungszwecke erteilt hat. Daneben sieht Art. 6 DS-GVO weitere Fälle vor, in denen die Verarbeitung von Daten rechtmäßig ist. Obwohl die Möglichkeit der Einwilligung von Art. 6 Abs. 1 DS-GVO an erster Stelle genannt wird, vermittelt eine Rechtgrundlage, die eine rechtliche Verpflichtung zur Verarbeitung aufstellt, dasselbe Maß an Rechtmäßigkeit. Die verschiedenen von der DS-GVO angebotenen Rechtmäßigkeits-Konstellationen bestehen demnach gleichwertig nebeneinander.

Die Einwilligungslösung sieht sich jedoch in verschiedenen Bereichen Problemen ausgesetzt. Laut Erwägungsgrund 32 der DS-GVO ist die zentrale Grundvoraussetzung für eine wirksame Einwilligung, dass diese freiwillig erfolgt und unmissverständlich bekundet wird. Dieser Umstand ist in einzelnen Rechtsbereichen nicht ohne weiteres umsetzbar. Überall dort, wo ein strukturelles Über-/Unterordnungsverhältnis besteht, bereitet die freiwillige Abgabe von Erklärungen Schwierigkeiten. So wird ein Arbeitgeber, dessen Arbeitsstelle zugleich seine Existenzgrundlage darstellt, bereitwilliger in Datenerhebungen einwilligen, als eine unabhängige, in keinem Weisungsverhältnis stehende Person. Noch extremer gestalten sich diese Strukturen, wenn die Betroffenen sich nicht, wie beim Arbeitsverhältnis, freiwillig in die untergeordnete Funktionsstellung begeben. Ein Beispiel für dieses Extrem ist die Stellung des Gefangenen im Justizvollzug. Wurde bereits die Grundposition nicht freiwillig eingenommen, so fällt auch die Beweisführung im Hinblick auf die Freiwilligkeit der Einwilligung selbst schwer. Insofern stellt die Anordnung der Rechtmäßigkeit der Datenverarbeitung durch eine gesetzliche

Grundlage in Fällen, in denen diese strukturellen Besonderheiten bestehen nicht nur einen der Einwilligung grundsätzlich gleichwertigen, sondern zugleich eine rechtssichereren Lösungsweg als diese dar.

Achillesferse der Rechtsfigur ist und bleibt jedoch deren Zweckbindung. Nach dieser kann die Einwilligung nur für bestimmte Zwecke erteilt werden. Diesbezüglich steht zu erwarten, dass sich die bisherigen Praxisprobleme hinsichtlich des Konkretisierungsgrades der Zweckangabe fortsetzen werden.

Zusätzlich zu den altbekannten Vorgaben ordnet die neue Vorschrift des Art. 7 Abs. 3 DS-GVO das Recht des Betroffenen auf jederzeitigen Widerruf seiner Einwilligung an. Die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Zeitpunkt des Widerrufs stattfindenden Verarbeitungen bleibt dabei im Falle eines Widerrufes unberührt. Der aus dieser Vorschrift folgende allgemeine Grundsatz der Widerrufbarkeit der Einwilligung ist auch innerhalb der nationalen Regelungen zu spiegeln, die Öffnungsklauseln in der Datenschutz-Grundverordnung umsetzen.

Auch der Gedanke des Opt-In-Grundsatzes wird von der gesamten Verordnung getragen. Demnach sind Opt-Out-Lösungen, also Anwendungen, in denen personenbezogene Daten bis zum Zeitpunkt des Widerspruchs der betroffenen Person verarbeitet werden, nicht zulässig. Ein solches Opt-Out-Modell kennt auch die grundlegende Vorschrift des Art. 6 Abs. 1 DS-GVO nicht. Dies ist konsequent, verhilft doch die Realisierung der Einwilligungslösung dem Betroffenen zu einer selbstbestimmten freiwilligen Entscheidung, wohingegen ein durch die Herbeiführung von Fakten erzwungener Widerspruch nicht dazu geeignet ist, den gleichen Grad an Autonomie zu vermitteln.

III. Betroffenenrechte

Auch die Betroffenenrechte werden durch die DS-GVO erweitert.

1. Recht auf Auskunft

Der datenschutzrechtliche Auskunftsanspruch nach § 34 BDSG bzw. Art. 15 DS-GVO ist im Hinblick auf den Schutz der personenbezogenen Daten und die konkrete Ausübung des Rechts auf informationelle Selbstbestimmung das wesentliche Instrument der Rechtsverwirklichung und hat in dem grundsätzlich zweistufigen System der Rechtsdurchsetzung eine zentrale Funktion: Nur wer in einem ersten Schritt Kenntnis der jeweils betroffenen Daten und des Umfangs von Datenverarbeitungsprozessen hat, kann in einem zweiten Schritt von seinen Betroffenenrechten des Widerspruchs etwa gegen die Verarbeitung der Daten zu Werbezwecken (§ 28 Abs. 4 BDSG bzw. Art. 21 Abs. 3 DS-GVO), der Löschung (§ 35 Abs. 2 BDSG bzw. Art. 17 DS-GVO), der Sperrung und der Berichtigung von Daten (§ 35 Abs. 1, 3 BDSG bzw. Art. 16 DS-GVO) sowie des Rechts auf Einschränkung der Verarbeitung (Art. 18 DS-GVO) Gebrauch machen oder gar Schadensersatz nach § 7 BDSG bzw. Art. 82 DS-GVO verlangen.

Neue Technologien, die Digitalisierung fast aller Lebensbereiche, Big Data und massenhafte automatisierte Datenerhebungen und -verarbeitungen machen es den Betroffenen freilich immer schwerer, überhaupt zu erkennen, ob, wie und wofür seine personenbezogenen Daten erhoben werden und wer der Verantwortliche hierfür ist.

Umso wichtiger ist es, dass die verantwortlichen Stellen den Auskunftsanspruch nach § 34 BDSG bzw. Art. 15 DS-GVO ernst nehmen, zeitnah, vollständig und richtig Auskunft erteilen und ihn nicht, wie es teilweise geschieht, nur geschäftsmäßig – und damit oberflächlich – abhandeln. Die Datenschutzaufsichtsbehörde wird hierauf ein strenges Auge werfen, schließlich eröffnet Art. 83 Abs. 5 b) DS-GVO in den Fällen unterbliebener oder unvollständiger Auskunftserteilung umfangreiche Sanktionsmöglichkeiten.

Relevant sind hier aus unserer Sicht insbesondere folgende Gesichtspunkte:

a) Inhalt und Umfang des Auskunftsanspruchs

Die Auskunft ist nach § 34 Abs. 1 BDSG

- hinsichtlich der zur Person des Auskunftsberechtigten gespeicherten Daten einschließlich der Herkunft dieser Daten,
- hinsichtlich etwaiger Empfänger oder der Kategorien von Empfängern (z.B. Adresshändler, Kreditinstitute) an die die Daten des anspruchsberechtigten weitergegeben werden sowie
- hinsichtlich des Zwecks der Speicherung zu erteilen.

Das Auskunftsrecht nach Art. 15 DS-GVO ist zweistufig aufgebaut und teilweise weitergehend. Zunächst hat der Betroffene das Recht, zu erfahren, ob der Verantwortliche im Sinne von Art. 4 Ziffer 7 DS-GVO überhaupt Daten von ihm verarbeitet (sog. „Verarbeitungsbestätigung"). Falls ja, hat der Betroffene das Recht auf Auskunft über diese personenbezogenen Daten. Neben diesen konkret verarbeiteten personenbezogenen Daten (z.B. Name, Vorname, Anschrift, Geburtsdatum, Beruf, medizinische Befunde) erstreckt sich der Auskunftsanspruch auch auf folgende weitere Informationen:

- Verarbeitungszwecke,
- Kategorien personenbezogener Daten, die verarbeitet werden (mit Gruppenbezeichnungen wie Gesundheitsdaten, Bonitätsdaten usw.),
- Empfänger bzw. Kategorien von Empfängern, die diese Daten bereits erhalten haben oder künftig noch erhalten werden,
- geplante Speicherdauer falls möglich, andernfalls die Kriterien für die Festlegung der Speicherdauer,
- Rechte auf Berichtigung, Löschung oder Einschränkung der Verarbeitung,
- Widerspruchsrecht gegen diese Verarbeitung nach Art. 21 DS-GVO,
- Beschwerderecht für die betroffene Person bei der Aufsichtsbehörde,
- Herkunft der Daten, soweit diese nicht bei der betroffenen Person selbst erhoben wurden, und
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling mit aussagekräftigen Informationen über die dabei involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen solcher Verfahren.

Im Falle der Datenübermittlung in Drittländer ist gemäß Art. 15 Abs. 2 DS-GVO über die insoweit gegebenen Garantien gemäß Art. 46 DS-GVO zu informieren (z.B. vereinbarte Standarddatenschutzklauseln, verbindliche interne Datenschutzvorschriften, d.h. Binding Corporate Rules). Keine Drittländer sind die EU-Mitgliedstaaten und die Vertragsstaaten des EWR.

Die Sinnhaftigkeit der Zweistufigkeit kann für die tägliche Praxis bezweifelt werden. Wenn Daten vorliegen, wir der Verantwortliche sicherlich auch gleich die entsprechende vollständige Auskunft erteilen und nicht nur in einem ersten Schritt mit „Ja" antworten. Nicht ausreichend ist die Nennung von Kategorien (z.B. Name, Vorname), es müssen stets die konkreten Daten beauskunftet werden, da dies bereits Art. 15 Abs. 1 2. Hs. DS-GVO verlangt. Auch die Empfänger von Daten müssen konkret benannt werden.

Entscheidend ist für den Betroffenen auch die Information, zu welchem Zweck bzw. zu welchen Zwecken seine Daten erhoben, verarbeitet und genutzt werden. Dies ist auch wichtig im Hinblick auf die grundsätzliche Zweckbindung.

In einem größeren aufsichtsrechtlichen Kontrollverfahren ist deutlich geworden, dass ein Adresshändler in seinen Beauskunftungen stets von Datenübermittlungen zum Zwecke der Werbung spricht. Nachforschungen haben aber ergeben, dass die Unternehmen, die Adressen angemietet haben, durchaus auch andere Zwecke verfolgt haben, z.B. Adressaktualisierungen und Adressberichtigungen, die Erarbeitung von Geo-Daten im Hinblick auf Scorewertberechnungen von Wirtschaftsauskunfteien, Wiederverkauf oder Ermittlung von beitragspflichtigen Kontakten durch ARD, ZDF und Deutschlandradio. Somit waren die erteilten Auskünfte – auch gegenüber der Datenschutzaufsichtsbehörde – unvollständig bzw. unrichtig und somit datenschutzwidrig.

Allerdings sind auch künftig beim Auskunftsrecht nur solche Daten mitzuteilen, die zur Person des Betroffenen gespeichert sind, also Daten, „die Angaben über persönliche oder sachliche Verhältnisse, die auf eine Person bezogen oder beziehbar sind" (vgl. Gola/Schomerus, Kommentar zum BDSG, 12. Auflage, § 34 Rn. 9), enthalten. Die Daten müssen demnach individualisierende, den Betroffenen in seinen Eigenschaften und Verhaltensweisen konkretisierende Informationen bzw. Merkmale beinhalten.

Persönliche und sachliche Verhältnisse einer Person im Sinne von Art. 4 Ziff. 1 der DS-GVO beschreibt körperliche und geistige Eigenschaften, Verhaltensweisen und berufliche, wirtschaftliche, soziale oder private Beziehungen. Erfasst werden auch alle identifizierenden Angaben wie bspw. Personenkennzeichen, Arbeitszeiten, GPS-Standortdaten, Daten in rechtlichen Analysen und biometrische sowie genetische Daten. Auf die Sensibilität oder Aussagekraft der Angaben kommt es für ihre Einordnung als personenbezogene Daten nicht

an (Plath/Schreiber in: Plath, BDSG/DS-GVO, 2. Aufl. 2016, § 3 BDSG, Rn. 8).

b) Grenzen des Auskunftsanspruchs

Ein Auskunftsanspruch besteht nicht in den Fällen des § 34 Abs. 7 BDSG. Das BDSG-neu enthält in seinem § 34 noch weitere Beschränkungen des Auskunftsrechts, insbesondere für Archivdaten und Protokollierungsdaten.

Grenzen des Auskunftsanspruchs bilden ferner z.B. Bereiche, die als echtes Geschäftsgeheimnis einzustufen sind (§ 34 Abs. 1 S. 4 BDSG). Der BGH hat dies so etwa für die konkrete Scorewert-Berechnungsformel bei Wirtschaftsauskunfteien – in einem durchaus diskussionswürdigen Urteil – entschieden (BGH, Urteil vom 28. Januar 2014 – VI ZR 156/13 –, BGHZ 200, 38-51). Ein Inkassounternehmen muss nach § 34 Absatz 7, § 33 Absatz 2 Satz 1 Nr. 7 b) BDSG Selbstauskunftsersuchen genauso wenig wie ein Rechtsanwalt beantworten, soweit es dabei die Prozesstaktik des Gläubigers offenbaren müsste.

Bei einer großen Menge von gespeicherten Informationen über die betroffene Person kann der Verantwortliche verlangen, dass präzisiert wird, auf welche Informationen oder Verarbeitungsvorgänge sich das Auskunftsersuchen konkret bezieht (EG 63 Satz 7 der DS-GVO). Das kann z.B. bei Banken, Arztpraxen oder Versicherungen mit umfangreichen und langjährigen Vertragsbeziehungen zu der betroffenen Person der Fall sein. Offenkundig unbegründete oder exzessive Anträge einer betroffenen Person können zur Ablehnung oder zu einer Kostenerstattungspflicht führen (Art. 12 Abs. 5 S. 2 DS-GVO).

c) Rechte anderer als Grenze

Art. 15 Abs. 4 und EG 63 S. 5 DS-GVO verpflichten den Verantwortlichen, die Rechte und Freiheiten anderer Personen nicht zu beeinträchtigen. An dieser Stelle ist künftig z.B. der Schutz von Geschäftsgeheimnissen zu verorten. Die Berücksichtigung gegenläufiger Rechte darf aber keinesfalls dazu führen, den Auskunftsanspruch vollständig abzulehnen oder auszuhöhlen.

d) Form der Auskunftserteilung

Die Auskunft hat gemäß § 34 Abs. 6 BDSG bzw. Art. 15 Abs. 3, 12 Abs. 1 DS-GVO grundsätzlich schriftlich im Sinne des § 126b BGB zu erfolgen, eine Übermittlung über andere Kommunikationsmedien (z.B. per E-Mail) ist bei entsprechender Antragsstellung ebenfalls zulässig. Die Auskunft ist nach Art. 12 Abs. 5 DS-GVO unentgeltlich zu erteilen. In Anlehnung an § 34 Abs. 8 BDSG sollte vom Verantwortlichen ein Entgelt gemäß Art. 15 Abs. 3 S. 2 DS-GVO erst verlangt werden können, wenn der Betroffene von ihm öfter als einmal jährlich von seinem Auskunftsrecht Gebrauch macht.

Wenn eine betroffene Person von ihrem Auskunftsrecht Gebrauch macht, sind ihr die zu erteilenden Informationen gemäß Art. 12 Abs. 3 DS-GVO unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung zu stellen. Diese Frist kann in komplexen Fällen um zwei Monate verlängert werden. Über Fristverlängerungen ist die betroffene Person unter Angabe der für die Verzögerung verantwortlichen Gründe innerhalb eines Monats nach Eingang ihres Antrags zu informieren.

2. Recht auf Berichtigung und Recht auf Löschung („Vergessenwerden")

Im Gegensatz zu § 35 BDSG kennt die DS-GVO weder Mindest- noch Höchstspeicherfristen für personenbezogene Daten. Art. 6 Abs. 1 und Art. 17 Abs. 1 DS-GVO lassen aber erkennen, dass der Verantwortliche von sich aus zu Unrecht gespeicherte Informationen grundsätzlich umgehend zu berichtigen bzw. löschen hat. Im Einzelnen gilt dazu folgendes:

- Speicherungen von personenbezogenen Daten dürfen inhaltlich nicht unzutreffend sein. Nach Art. 16 DS-GVO kann die betroffene Person den Verantwortlichen um Berichtigung bzw. Vervollständigung der über sie gespeicherten Daten ersuchen, wenn sie die Voraussetzungen dafür nachweist. Darüber hinaus kann die betroffene Person nach Art. 18 Abs. 1 lit. a) DS-GVO die „Einschränkung" der Datenverarbeitung verlangen, wenn sie besagte Angaben für unzutreffend hält. Wurde die Verarbeitung solchermaßen eingeschränkt, dürfen diese Daten – von ihrer Speicherung abgesehen – nur mit Einwilligung der betroffenen Person, zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öf-

fentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden (Art. 18 Abs. 2 DS-GVO). Gelingt es dem Verantwortlichen nicht, die Richtigkeit der Speicherung innerhalb einer angemessenen Frist zu belegen bzw. diese zu korrigieren, müssen die Angaben gelöscht werden (Art. 18 Abs. 2 DS-GVO).

- Ebenfalls zu löschen sind personenbezogene Daten, für deren Verarbeitung dem Verantwortlichen kein berechtigtes Interesse i.S. des Art. 6 Abs. 1 lit. f) DS-GVO zukommt bzw. bei denen den Grundrechten und Grundfreiheiten der betroffenen Person ein höheres Gewicht als den Interessen des Verantwortlichen beizumessen ist (Art. 17 Abs. 1 lit. c) DS-GVO). Auf einen entsprechenden Widerspruch der betroffenen Person gegen die Datenverarbeitung nach Art. 18 Abs. 1 lit. d), Art. 21 Abs. 1 DS-GVO kann der Verantwortliche allerdings die Löschung verhindern, wenn er seinerseits belegt, dass sein berechtigtes Interesse i.S. des Art. 6 Abs. 1 lit. f) DS-GVO doch höher wiegt als das der betroffenen Person (vgl. Erwägungsgrund 69). Bis zu diesem Zeitpunkt bleibt die Datenverarbeitung nach Art. 18 Abs. 2 DS-GVO „eingeschränkt".
- Personenbezogene Daten, die für die Zwecke, für die sie erhoben wurden, nicht oder nicht mehr erforderlich sind, müssen auch gelöscht werden (Art. 17 Abs. 1 lit. a) DS-GVO), es sei denn, die betroffene Person verlangt anstelle der Löschung die „Einschränkung" der Datenverarbeitung i.S. des Art.18 Abs. 2 DS-GVO, weil sie ihrerseits wegen der rechtswidrigen Speicherung Ansprüche geltend machen will und dabei u. U. beweispflichtig ist (Art. 18 Abs. 1 lit. c) DS-GVO).
- Ein weiterer Löschungsanspruch der betroffenen Person besteht, wenn ihre Daten unter Verstoß gegen datenschutzrechtliche Regelungen erhoben und weiterverarbeitet wurden (Art. 17 Abs. 1 lit. d) DS-GVO), es sei denn, die betroffene Person verlangt anstelle der Löschung nach Art. 18 Abs. 1 lit. b) DS-GVO die „Einschränkung" der Datenverarbeitung i.S. des Art. 18 Abs. 2 DS-GVO, weil sie ihrerseits wegen der rechtswidrigen Speicherung Ansprüche geltend machen will.

Insbesondere sind folgende Speicherungen zu löschen:

- Diskriminierende oder zu einer Prangerwirkung führende Angaben,
- Informationen über die Privat- und Intimsphäre einer betroffenen Person,
- Besondere Kategorien personenbezogener Daten i.S. der Art. 9 f. DS-GVO, insbesondere Gesundheitsdaten,
- Erkenntnisse, die einer besonderen Geheimhaltung unterliegen, sowie
- Angaben, die unter Umgehung der Schutzvorschrift für Kinder und Jugendliche nach Art. 8 Abs. 1 DS-GVO verarbeitet werden (Art. 17 Abs. 1 lit. f) DS-GVO).

Um zu gewährleisten, dass derartig unzulässige Speicherungen rechtzeitig gelöscht werden, schreibt der Erwägungsgrund 39 vor, dass die Verantwortlichen regelmäßige Überprüfungen ihres Datenbestandes vorzunehmen haben. Bei Auskunfteien wird dieser Zeitraum entsprechend den eigenen Vorstellungen dieser Branche mit drei Jahren als angemessen erachtet. Verantwortliche, die technisch oder organisatorisch nicht in der Lage sind, dieser Verpflichtung zu entsprechen, müssen die Angaben nach Ablauf der Prüffrist löschen.

Ungeachtet dessen steht der betroffenen Person das Recht zu, unter den genannten Voraussetzungen die Löschung der sie betreffenden Daten zu verlangen (Art. 17 Abs. 1 DS-GVO).

Darüber hinaus müssen im Fall der öffentlichen Verbreitung von Daten auch dritte Stellen über das Löschverlangen der betroffenen Person informiert werden. Dieses sog. „Recht auf Vergessen" wurde in der Rechtssache „Google Spain SL, Google Inc. vs. AEPD, Mario Costeja González" vom EuGH entwickelt und ist mittlerweile in Art. 17 Abs. 2 DS-GVO explizit normiert (s. dazu näher das Kapitel „Internet ").

Wie bereits jetzt § 35 Abs. 7 BDSG verpflichtet auch künftig Art. 19 DS-GVO den Verantwortlichen, grundsätzlich alle Empfänger, denen die Daten offenbart wurden, von der Löschung zu unterrichten, wenn die Datenverarbeitung zum Zeitpunkt der Übermittlung unzulässig war. Verlangt die betroffene Person die Erreichbarkeit der Empfänger, damit sie sich mit diesen wegen der Rechtmäßigkeit der dortigen Speicherung in Verbindung setzen kann, muss sie der Verantwortliche davon informieren. Vergleichbares gilt für jede nachträgliche Berichtigung, wenn die Daten beim Empfänger noch gespeichert sind.
Widerruft die betroffene Person ihre Einwilligung, darf keine weitere Verarbeitung der jeweiligen Daten erfolgen, es sei denn, dass dies

aufgrund einer gesetzlichen Ermächtigung zulässig ist (Art. 17 Abs. 1 lit. b) DS-GVO). Die bis zu diesem Zeitpunkt erfolgte Datenverarbeitung bleibt jedoch rechtmäßig. Die Benachrichtigungspflicht des Art. 19 DS-GVO gilt entsprechend.

Widerspricht die betroffene Person nach Art. 21 Abs. 2 f. DS-GVO der Verarbeitung ihrer Daten für die Direktwerbung, dürfen diese zu diesem Zweck nicht mehr verarbeitet werden. Ist die Verarbeitung zu anderen Zwecken rechtlich nicht zulässig, müssen die Angaben gelöscht werden. (Art. 17 Abs. 1 lit. c) 2. HS DS-GVO).

Bei Verstößen gegen die Löschungs- oder Nachberichtspflichten droht die Einleitung eines Bußgeldverfahrens nach Art. 83 Abs. 5 lit. b) DS-GVO. Außerdem setzt sich der Verantwortliche einem Haftungsrisiko nach Art. 82 DS-GVO aus.

3.) Recht auf Datenportabilität

Neu implementiert wurde das Recht auf Datenportabilität in Art. 20 DS-GVO, das dem Einzelnen eine Rechtposition einräumt, die auf die Weitergabe seiner Daten gerichtet ist. So sollen von einem Verantwortlichen im Rahmen der Datenverarbeitung erhobene Daten in Zukunft auch durch weitere Verantwortliche nutzbar sein. Relevant wird diese Rechtsposition wenn Dienstleiter gewechselt werden und die Datensätze des Kunden dabei nicht verlorengehen sollen. Dieses neu geschaffene, innovative Betroffenenrecht ruft schon jetzt besonderes Beratungsinteresse hervor – und zwar bei Betroffenen ebenso wie bei verantwortlichen Stellen. In unserer Beratungspraxis geben wir diesem die folgenden Konturen:

Nach Art. 20 Abs. 1 DS-GVO hat die betroffene Person das Recht, von dem Verantwortlichen, der gerade im Besitz ihrer personenbezogenen Daten ist, diese zu erhalten. Gemeint sind aber nur solche Angaben, die die betroffene Person selbst dem Verantwortlichen überlassen hat, sofern die Verarbeitung auf einer Einwilligung oder auf einem Vertrag zwischen dem Verantwortlichen und der betroffenen Person beruht. Hinzukommen muss, dass die Verarbeitung mithilfe eines automatisierten Verfahrens erfolgt.
Dabei kann die betroffene Person verlangen, dass ihr besagte Angaben in einem strukturierten, gängigen und maschinenlesbaren Format zugänglich gemacht werden. Die „Gängigkeit" bezieht sich auf am Markt gebräuchliche Systeme, die es der betroffenen Person ermöglichen, diese Angaben ihrerseits technisch zu verarbeiten. Häufig verwendete Formate wie XML, CSV und HTML erfüllen diese Voraussetzungen. Das Erfordernis der „Strukturiertheit" will verhindern, dass die betroffene Person keinerlei System bei den Informationen erkennen kann. Mit einem „Datensalat" kann niemand etwas anfangen! Die Verantwortlichen sind gut beraten, ihre Systeme rechtzeitig so zu konfigurieren, dass sie Anträgen auf Datenübertragung zügig entsprechen können. Werden solche Verlangen nicht rechtzeitig erfüllt, kann das empfindliche Bußgelder zur Folge haben (Art. 85 Abs. 3 lit. b) DS-GVO).

Daneben hat die betroffene Person nach Art. 20 Abs. 2 DS-GVO das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten ursprünglich bereitgestellt worden waren, zu übermitteln oder unmittelbar an einen Dritten übermitteln zu lassen, soweit dies technisch machbar ist. Mit dem Erfordernis der technischen Machbarkeit soll ausgeschlossen werden, dass der Verantwortliche nur deswegen sich ein bestimmtes Datenverarbeitungssystem beschaffen muss, um dem Übertragungswunsch der betroffenen Person entsprechen zu können.

Ob der ursprünglich Verantwortliche die Daten anlässlich der Übermittlung an den Betroffenen oder einen Dritten in seinen Beständen löschen muss, hängt davon ab, ob die betroffene Person insoweit einen Löschungsanspruch nach Art. 17 DS-GVO geltend machen kann (Art. 20 Abs. 3 DS-GVO). Insbesondere ist ein solches Löschungsbegehren nicht berechtigt, wenn die Datenverarbeitung bei dem ursprünglich Verantwortlichen für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

Auch dürfen nach Absatz 4 des Art. 20 DS-GVO grundsätzlich keine Informationen der betroffenen Person oder Dritten zufließen, die aus der persönlichen Sphäre anderer Personen herrühren, also durch die Übermittlung deren Rechte und Freiheiten beeinträchtigen würden.

IV. Informationspflichten für verantwortliche Stellen bei der Datenverarbeitung

Eines der Themen, die besonders die Unternehmen umtreiben, sind die umfangreichen Informationspflichten, die die DS-GVO der für die Datenverarbeitung verantwortlichen Stelle vorschreibt. Danach muss letztere die betroffene Person über die sie betreffende Datenverarbeitung und ihre Rechte informieren, wobei zwischen sog. Direkterhebung bei der betroffenen Person selbst (Art. 13 DS-GVO) und sog. Dritterhebung bei anderen Stellen (Art. 14 DS-GVO) unterschieden wird.
Werden die Daten unmittelbar bei der betroffenen Person erhoben, muss die für die Datenverarbeitung verantwortliche Stelle jene zum Zeitpunkt der Erhebung über folgendes informieren:

- den Namen und die Kontaktdaten des für die Datenverarbeitung Verantwortlichen sowie gegebenenfalls seines Vertreters;
- gegebenenfalls die Kontaktdaten des betrieblichen Datenschutzbeauftragten der datenverarbeitenden Stelle;
- die Zwecke, für die die Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
- gegebenenfalls die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten mit der Datenverarbeitung verfolgt werden;
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der Daten und
- gegebenenfalls ob die Daten in einem Drittland, in dem kein für EU-Verhältnisse angemessenes Datenschutzniveau gesichert ist, verarbeitet werden.

Darüber hinaus müssen für die betroffene Person zur Einsichtnahme bzw. zum Abruf folgende Hinweise bereitgehalten werden:

- die Dauer der Speicherung der Daten;
- die Rechte der betroffenen Person (Auskunftsrecht, Berichtigungsrecht, Löschungsrecht, Recht auf Einschränkung der Datenverarbeitung, Widerspruchsrecht, Recht auf Berichtigung der gespeicherten Daten, Recht auf Datenübertragbarkeit);
- Das Recht, eine Einwilligung jederzeit zu widerrufen;
- das Bestehen eines Beschwerderechts bei der zuständigen Datenschutzaufsichtsbehörde;
- ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist,
- ob die betroffene Person verpflichtet ist, die Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte, und
- im Falle einer automatisierten Entscheidungsfindung aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Datenverarbeitung.

Werden die Daten mit oder ohne Wissen der betroffenen Person bei einem Dritten erhoben, müssen diese Hinweise und eine Information über die Kategorie der erhobenen Daten spätestens innerhalb eines Monats erfolgen bzw. zugänglich gemacht werden. Verarbeitet die verantwortliche Stelle die Daten in erster Linie zum Zwecke der Übermittlung an Dritte (Auskunftei), genügt es, wenn die betroffene Person diese Informationen spätestens zum Zeitpunkt der ersten Datenweitergabe erhält.

Ändert sich der Speicherungszweck später oder sollen die Daten weiteren oder anderen Empfängern als ursprünglich angegeben zur Verfügung gestellt bzw. übermittelt werden, muss die betroffene Person auch davon informiert werden.

Die Unterrichtungspflicht durch die datenverarbeitende Stelle besteht ausnahmsweise nicht, soweit die betroffene Person bereits informiert ist, insbesondere wenn sie von einem Dritten entsprechend aufmerksam gemacht worden ist. So genügt es den gesetzlichen Vorgaben, wenn etwa ein Inkassounternehmen einen Schuldner darauf hinweist, dass er, wenn er eine Forderung unbegründet nicht rechtzeitig erfüllt, bei einer bestimmten Auskunftei eingemeldet wird, und dass diese künftige Vertragspartner der betroffenen Person zur Warnung vor Zahlungsausfällen über das Bonitätsnegativmerkmal informieren wird. Alle anderen Hinweispflichten verbleiben jedoch bei der Auskunftei. Weitere Ausnahmen sind vorgesehen, wenn sich die Erteilung dieser Informationen als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde. Die §§ 32 und 33 BDSG-neu sehen darüber hinaus u.a. Ausnahmen vor, wenn durch die Information die Geltendmachung oder Verteidigung von Ansprüchen beeinträchtigen würde oder wenn Sicherheitsgründe entgegenstehen.

Die verantwortliche Stelle hat angesichts des in Art. 5 DS-GVO vorgegebenen Transparenz-

gebotes stets den Nachweis zu erbringen, dass die Hinweise erfolgt sind. Im Falle des Verstoßes gegen die Hinweispflichten sind in Art. 83 DS-GVO hohe Bußgelder vorgesehen. Auf die Rechtmäßigkeit der Datenverarbeitung selbst hat der Pflichtenverstoß jedoch in der Regel keine Auswirkungen.

V. Mitteilungspflichten im Falle von Datenpannen

Neben den Betroffenenrechten und den Informationspflichten sind auch die Mitteilungspflichten an die Aufsichtsbehörden im Falle einer Datenpanne von den Änderungen erfasst. Der neue Art. 33 DS-GVO hat gleich der bisherigen Datenpannenregelung aus § 42 a BDSG a.F. die Meldung von Verletzungen des Schutzes personenbezogener Daten (data breach notification) zum Inhalt. Im Gegensatz zu der bisherigen Vorschrift sieht Art. 33 DS-GVO eine Meldepflicht nicht nur für besondere Kategorien von personenbezogenen Daten, sondern für jede Verletzung personenbezogener Daten vor. Zudem haben angemessene Maßnahmen zur Sicherung der betroffenen Daten keinen Vorrang vor der neuen Meldepflicht. Diese greift vielmehr „unverzüglich" nach dem Eintritt der konkreten Schutzverletzung. Auch die Sicherstellung der Strafverfolgung genießt keinen Vorrang vor der eigentlichen Meldepflicht. Diese Neuerungen betonen allesamt den Stellenwert des durch die Europäische Union implizierten Schutzes der Privatheit. In diesem Sinne kann die Information der Aufsichtsbehörde auch nicht durch eine öffentliche Mitteilung ersetzt werden. Auch das noch in § 42a S. 6 BDSG a.F. enthaltene Verwertungsverbot findet sich in der neuen Regelung nicht mehr. Gemeldete Datenschutzverletzungen können demnach grundsätzlich auch im Rahmen von Ordnungswidrigkeitsverfahren und Strafverfahren gegen den die Verletzung meldenden verwendet werden. Angesichts dessen ist es problematisch, dass die Vorschrift des § 43 Abs. 4 BDSG n.F. in diesem Bereich eine Zustimmung des Meldepflichtigen verlangt. Beachtet man, dass auch im Bereich der Regelungsspielräume der Mitgliedstaaten eine europarechtskonforme Auslegung geboten ist, so ist fraglich, ob diese neue Vorschrift des § 43 Abs. 4 BDSG n.F. in Anbetracht von Art. 33 DS-GVO überhaupt noch europarechtskonform ausgelegt werden kann, oder ob diese Vorschrift nicht vielmehr europarechtswidrig ist. Zwar besteht auch auf europäischer Ebene der Grundsatz „nemo tenetur se ipsum accusare", nach dem grundsätzlich niemand verpflichtet ist, sich selbst zu belasten. Die grundsätzlich engere Auslegung dieses Grundsatzes auf europäischer Ebene impliziert jedoch eine solche Europarechtswidrigkeit.

Inhaltlich liegt der Schwerpunkt des Art. 33 Abs. 1 DS-GVO auf einer negativen Risikoprognose. Die Meldung hat nicht zu erfolgen, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Diese negative Risikoprognose führt zur Ausdifferenzierung von Pflichten, stellt die Informationspflicht in Abhängigkeit zum potenziellen Gefahreintritt und ermöglicht eine strukturierte Risikoprüfung. Der Umfang der zu meldenden Aspekte ist in Art. 33 Abs. 3 DS-GVO geregelt. Die dort gestellten Voraussetzungen sind nur zu erfüllen, wenn die meldende Stelle ein umfassendes und nachhaltiges Datenmanagement betreibt. In diesem Zusammenhang stellt Art. 33 Abs. 5 DS-GVO weitreichende Dokumentationspflichten auf, die nicht nur die eigentliche Verletzung, sondern auch alle damit in Zusammenhang stehende Fakten mitsamt der Auswirkungen und ergriffenen Abhilfemaßnahmen erfasst. Bei Verstoß gegen die Melde- oder Dokumentationspflicht des Art. 33 Abs. 1 und 5 DS-GVO drohen gemäß Art. 83 Abs. 4 lit. a DS-GVO Bußgelder von bis zu „10.000.000 € oder im Fall eines Unternehmens 2 % des gesamten weltweit erzielten Jahresumsatzes".

VI. Auftragsdatenverarbeitung

Die Rechtsfigur der Auftragsdatenverarbeitung existierte ebenfalls bereits vor Erlass der DS-GVO. Ab dem 25. Mai 2018 stellen die Art. 28 f. DS-GVO die maßgeblichen gesetzlichen Vorschriften dar. Gleich der herkömmlichen Rechtslage können im Fall des Art. 28 Abs. 1 DS-GVO Datenverarbeitungen im Rahmen eines Auftragsverhältnisses auf einen Auftragsverarbeiter übertragen werden. Der Verantwortliche muss hierbei sicherstellen, dass „geeignete technische wie auch organisatorische Maßnahmen" durchgeführt werden, die eine Durchsetzung der Datenschutz-Grundverordnung und somit auch das dort vorgegebene Schutzniveau mit Blick auf den Schutz der Rechtspositionen der Betroffenen gewährleisten. Die Art. 28 f. DS-GVO sind insoweit spezieller als die allgemeinen Rechtsgrundlagen für die Datenverarbeitung aus Art. 6, 9 DS-GVO und gehen diesen vor. Insoweit kann man auch nach Geltung der DS-GVO von einer Privilegierung des Auftragsverarbeiters sprechen.

Die aufgezeigten Parallelen können jedoch nicht über die durch die DS-GVO ausgelösten Änderungen im Bereich der Auftragsdatenverarbeitung hinwegtäuschen. So wird die bisher anerkannte Möglichkeit der Funktionsübertragung von der DS-GVO nicht erwähnt. Nach bisheriger vorherrschender Rechtsauffassung konnte der Auftragsverarbeiter in Fällen, in denen er über Spezialwissen oder einen spezifischen Erfahrungsschatz verfügte, gesamte Funktionen auf den Auftragsverarbeiter übertragen. Einer solchen Sondergruppenbildung in Form der Funktionsübertragung stehen die von Art. 28 Abs. 1 DS-GVO aufgestellten allgemein gehaltenen, inhaltlichen Pflichten jedoch entgegen. Die europarechtliche Deutung der Auftragsdatenverarbeitung unterscheidet sich insoweit inhaltlich von dem bisher vorherrschenden nationalen Verständnis.

Die DS-GVO stellt sowohl den LfDI als auch Datenverarbeiter vor neue Herausforderungen. Schaffen Sie sich frühzeitig einen Überblick über Ihre aktuelle Situation und prüfen Sie, ob Ihr Unternehmen/ Ihre Behörde fit ist für die neuen rechtlichen Anforderungen der DS-GVO. Sprechen Sie mit uns: Wir können Sie beraten und können Rechtssicherheit schaffen!

1.2 Sicher oder frei – zwischen Skylla und Charybdis?

„Im Kampf gegen Terror ist Datenschutz das erste Opfer" – so lautete die Überschrift eines Artikels in der Online-Ausgabe der WELT vom 08.07.2016[3], der sich mit gesetzgeberischen Maßnahmen zur Stärkung der Sicherheitsbehörden befasst. Insbesondere in Zeiten erhöhter Terrorgefahr wäre es eigentlich Aufgabe der Politik, das Schiff – um im Bild zu bleiben – mit Weitsicht zwischen den Antagonisten Sicherheit und bürgerliche Freiheitsrechte in ruhige Fahrwasser zu navigieren. Wer allerdings nach dem Motto verfährt „Datenschutz ist schön, aber in Krisenzeiten wie diesen hat Sicherheit Vorrang" (so Bundesinnenmister Thomas de Maizière in den ARD-Tagesthemen am 22. März 2016)[4], läuft letztendlich Gefahr, Schiffbruch zu erleiden. Mit Sorge beobachte ich deshalb, mit welcher Frequenz der Gesetzgeber immer neue Überwachungsinstrumente einführt, mit denen das Recht des Einzelnen, selbstbestimmt über seine persönlichen Daten zu verfügen, mehr und mehr beschnitten wird. Dabei weiß der Gesetzgeber häufig die öffentliche Meinung hinter sich. So halten es gemäß einer Allensbach-Umfrage aus dem Jahr 2016 etwa 90 Prozent der Befragten für richtig, Flughäfen oder Bahnhöfe kontinuierlich mit Kameras zu überwachen. 84 Prozent unterstützen die Erfassung von Fingerabdrücken von jeder Person, die einreist. Die Hälfte der Bevölkerung befürwortet auch die flächendeckende Erfassung und Speicherung des Fingerabdrucks aller Bürger, um die Verbrechensbekämpfung zu erleichtern[5].

Die Terrorismusproblematik und die Folgewirkungen der Flüchtlingskrise prägten die Arbeit meiner Dienststelle in den vergangenen zwei Jahren. Intensiv eingebunden waren wir vor allem in einschlägige Gesetzgebungsvorhaben zur inneren Sicherheit sowohl auf Landes- wie auch auf Bundesebene auf der einen, aber auch in praktische Umsetzungsmaßnahmen und Projekte auf der anderen Seite. Den Auftakt machte dabei im Jahr 2016 das Bundesverfassungsgericht mit seinem Urteil vom 20. April 2016[6] zum Bundeskriminalamtgesetz. Darin stellte das Bundesverfassungsgericht fest, dass die Ermächtigung des Bundeskriminalamts zum Einsatz von heimlichen Überwachungsmaßnahmen zur Abwehr von Gefahren des internationalen Terrorismus zwar im Grundsatz mit den Grundrechten vereinbar sei, die derzeitige Ausgestaltung von Befugnissen aber in verschiedener Hinsicht dem Verhältnismäßigkeitsgrundsatz nicht genügt. Das führte dazu, dass verschiedene Regelungen aus dem Gesamtkomplex zu beanstanden waren. Die Entscheidung, die eine lange Rechtsprechungslinie fortführt, betrifft sowohl die Voraussetzungen für die Durchführung solcher Maßnahmen als auch die Frage der Übermittlung der Daten zu anderen Zwecken an dritte Behörden sowie schließlich erstmals auch die Anforderungen an

3 https://www.welt.de/politik/deutschland/article156894545/Im-Kampf-gegen-Terror-ist-Datenschutz-das-erste-Opfer.html
4 https://www.tagesschau.de/multimedia/sendung/tt-4351.html
5 http://www.faz.net/aktuell/politik/inland/allensbach-umfrage-zeigt-angst-um-innere-sicherheit-steigt-14073805-p2.html?printPagedArticle=true#pageIndex_1
6 Az.: 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220-378

eine Weiterleitung von Daten an ausländische Behörden.[7]

Folge dieser Rechtsprechung war zunächst eine Novellierung des Bundeskriminalamtgesetzes. Diese blieb allerdings nicht dabei stehen, die aus verfassungsrechtlichen Gründen nötige „Reparatur" vor allem der Regelungen über heimliche Überwachungsmaßnahmen vorzunehmen. Vielmehr wurde das Urteil darüber hinaus zum Anlass genommen, das bisherige System der Datenhaltung beim Bundeskriminalamt in seiner Funktion als Zentralstelle für einen Datenverbund der Polizeien des Bundes und der Länder komplett umzukrempeln. Hervorstechendstes Merkmal der neuen Regelung ist die Abkehr der Speicherung polizeilicher Personenerkenntnisse in thematisch jeweils klar umschriebenen, einzelnen Dateien hin zu einem einheitlichen Verbundsystem mit zentraler Datenhaltung, lediglich zusammengehalten durch das Kriterium einer in ihrer konkreten Ausprägung nebelhaften „Verbundrelevanz". Da die datenschutzrechtliche Verantwortung der von den Länderpolizeien einzugebenden personenbezogenen Daten nach wie vor bei den Behörden der Länder liegt, stellt dies auch meine Dienststelle vor die Frage, nach welchem Maßstab künftig beurteilt werden soll, ob eine Speicherung im Einzelfall rechtmäßig ist oder nicht. Bisher ist in sog. Errichtungsanordnungen detailliert beschrieben, welchem Zweck welche Datei dient, welche Daten dafür gespeichert werden dürfen und wer damit wie umgehen darf. Solche Errichtungsanordnungen wird es künftig nicht mehr geben. Ob die noch festzulegenden Relevanzkriterien eine sachgerechte Datenschutzprüfung überhaupt noch möglich machen, wird sich zeigen. Skepsis ist jedenfalls angebracht.

Daneben hat die Novellierung des Bundeskriminalamtgesetzes dazu geführt, dass dessen Vorschriften zur Terrorismusabwehr gewissermaßen als Blaupause für entsprechende landesrechtliche Gesetzgebungsmaßnahmen im Gefahrenabwehrrecht herangezogen wurden. Die „grüne Karte" des Bundesverfassungsgerichts, das die zahlreichen heimlichen Überwachungsmaßnahmen des bisherigen Bundeskriminalamtgesetzes als dem Grunde nach verfassungsgemäß akzeptiert hat, wird insoweit vom Landesgesetzgeber als Freifahrschein verstanden, mit dem Bund gleichzuziehen. Auch wenn letztlich nicht alle denkbaren Ermittlungsinstrumente des Bundes in das Landesrecht übernommen werden, führt das „Gesetz zur Änderung des Polizeigesetzes und des Gesetzes über die Ladenöffnung in Baden-Württemberg" (LT-Drucksache 16/2741) doch einerseits im Ergebnis zu einer deutlichen Einschränkung von Bürgerrechten, ohne andererseits die Chance zu nutzen, im Rahmen des Möglichen durch den Ausbau von Betroffenenrechten die nachteiligen Folgen sachangemessen zu kompensieren.

Mit der landesgesetzlichen Zulassung der präventivpolizeilichen Telekommunikationsüberwachung und in diesem Rahmen insbesondere auch des staatlichen Einsatzes von Schadsoftware („Staatstrojaner"), um Kommunikation an der Quelle unter Umgehung von Verschlüsselungstechniken erfassen zu können (Quellen-TKÜ"), etabliert der Landesgesetzgeber Ermittlungsmaßnahmen, die mit schwerwiegenden Eingriffen in das Fernmeldegeheimnis einhergehen. Dabei ist nicht allein die Zulassung solcher Eingriffe als solche, sondern auch die Ausweitung dieser Maßnahme bis weit in das Vorfeld konkreter Gefahren höchst bedenklich. Durch eine in ihren Konturen kaum greifbare Konstruktion des „Gefährders" bzw. der Anlassperson ist für den Einzelnen kaum noch abschätzbar, wann er zum Objekt staatlicher Überwachung werden kann. Die vom Bundesverfassungsgericht in seinem Volkszählungsurteil von 1983 beschriebenen gesamtgesellschaftlichen Gefahren, die mit einer solchen staatlich erzeugten Unsicherheit einhergehen, sind aktueller denn je.

Die gesetzliche Zulassung solcher verdeckten Eingriffsbefugnisse, welche die Freiheitsrechte der Bürgerinnen und Bürger massiv beschneiden, hat mittlerweile leider Konjunktur. Dabei ist zu konstatieren, dass der Landesgesetzgeber im Vergleich zum Bund und anderen Ländern zwar noch verhältnismäßig zurückhaltend war, indem „nur" die Telekommunikationsüberwachung, nicht aber zugleich auch noch die Online-Durchsuchung geregelt hat. Massive Vorbehalte habe ich allerdings insoweit, als diese Maßnahmen nicht auf die Abwehr terroristischer Gefahren beschränkt bleiben. Und dies, obwohl die ausdrückliche Zielsetzung des Gesetzes die Bekämpfung der vom internationalen Terrorismus ausgehenden Bedrohungen ist: „Zu diesem Zweck sollen im Polizeigesetz neue präventiv-polizeiliche Befugnisse zur Te-

7 Pressemitteilung Nr. 19/2016 vom 20. April 2016

lekommunikationsüberwachung (TKÜ) sowie zur Quellen-TKÜ geschaffen werden."[8] Mit der Möglichkeit, solche massiven Grundrechtseingriffe schon in Fällen der Allgemeinkriminalität vorzunehmen, etwa bei der „dringenden" Gefahr einer Körperverletzung, schießt der Gesetzgeber massiv übers Ziel hinaus.

In seiner Entscheidung zum Bundeskriminalamtgesetz hat das Bundesverfassungsgericht die verfassungsrechtliche Zulässigkeit solcher heimlichen Überwachungsmaßnahmen mit Blick darauf, dass es um die Abwehr terroristischer Gewalttaten geht, als gerade noch hinnehmbar bezeichnet. Die allein durch eine besondere Nähe der Gefahr („dringende" Gefahr) begrenzte Eingriffsbefugnis bei Delikten der Allgemeinkriminalität ist mit dem Grundsatz der Verhältnismäßigkeit meiner Auffassung nach nicht mehr zu vereinbaren. Das habe ich auch im Rahmen der Anhörung zum Gesetzentwurf dem Parlament gegenüber deutlich zum Ausdruck gebracht.

Selbst der Ansatz, solche Maßnahmen auf „Gefährder" bzw. Anlasspersonen zu beschränken greift zu kurz. Denn für die Erfüllung des Terrorismusbegriffs reicht es nicht aus, allein die Zielsetzungen der betroffenen Personen enger zu fassen. Es bedarf vielmehr der Beschränkung auf bestimmte schwerste Straftaten, wie sie in § 129a des Strafgesetzbuches bezeichnet sind. So ist es im neuen Bundeskriminalamtgesetz vom 1. Juni 2017 geregelt und so hat auch das Bundesverfassungsgericht dieses Begriffsverständnis seiner Entscheidung zugrunde gelegt. Wenn es Ziel des Gesetzgebers gewesen sein soll, „bis an die Grenze des verfassungsmäßig Machbaren" zu gehen, hat er mit der aktuellen Fassung des § 23b diese Grenze aus meiner Sicht deutlich überschritten.

Einer weiteren „Neuerung" wollte sich der Gesetzgeber ebenfalls nicht verschließen: der elektronischen Fußfessel. Über die Sinnhaftigkeit dieses Überwachungsinstruments streiten sich selbst Sicherheitsexperten.[9] Die jetzt zugelassene Dauerüberwachung von Personen greift tief in das Recht ein, sich frei und unbeobachtet bewegen zu können. Auch hier geht der Gesetzgeber über die Grenzen dessen hinaus, was aus Gründen der Verhältnismäßigkeit noch vertretbar ist, wenn er die Verwendung der Daten nicht nur zur Terrorismusbekämpfung, sondern etwa schon zur Abwehr drohender Körperverletzungen vorsieht.

Noch ohne Vorbild ist dagegen eine Vorschrift im Gesetz, mit welcher der „intelligenten Videoüberwachung" der Weg geebnet werden soll. Unter diesem schillernden Begriff sind algorithmenbasierte Datenerhebungen mittels Videotechnik zu verstehen, wobei des Zentrum der „Intelligenz" nicht mehr im Kopf des Polizeibeamten verortet wird, der das Geschehen an einem Monitor beobachtet, sondern im Innern einer Maschine. Der Technik wird zugetraut, polizeilich relevante Verhaltensmuster zu erkennen, um dann entsprechend Alarm zu schlagen. Damit sollen zum einen der personelle Aufwand für die Videoüberwachung als solcher und zum anderen die körperliche und geistige Beanspruchung der mit der Beobachtung der Monitore befassten Beamtinnen und Beamten verringert werden.

Ob es gelingen wird, Algorithmen zu programmieren, die in der Lage sind, polizeirelevante Verhaltensweisen zuverlässig zu erkennen, ist derzeit noch offen. Sollte dies gelingen, wäre es aus Sicht des Datenschutzes jedenfalls dann ein Gewinn, wenn im Gegenzug von der herkömmlichen Videoüberwachung, die mit einer Dauerbeobachtung samt Aufzeichnung bestimmter Bereiche und der sich darin aufhaltenden Personen verbunden ist, Abstand genommen würde. Es wäre nur noch schwer zu vermitteln, weshalb eine solche Dauerbeobachtung auch dann noch erforderlich sein sollte, wenn systemseitig sichergestellt ist, dass polizeirelevante Sachverhalte automatisiert erkannt und festgehalten werden.

Meine tendenziell positive Bewertung der aktuellen Regelung zur intelligenten Videoüberwachung darf allerdings nicht darüber hinwegtäuschen, dass damit eine Tür aufgestoßen wird, die den Weg zu Formen der Überwachung menschlichen Verhaltens öffnet, welche letztlich zu einer vollständigen Verhaltenskontrolle führen können. Zwar hat die Landesregierung einer Videotechnik (derzeit noch) eine klare Absage erteilt, mit der Gesichter eingescannt und Personen identifiziert werden; dennoch steht zu befürchten, dass die Entwicklung hier nicht stehen bleibt. So findet derzeit am

8 LT-Drs. 16/2741, A. Zielsetzung Seite 1

9 https://www.welt.de/politik/ausland/article157345443/Warum-die-Fussfessel-nicht-vor-Anschlaegen-schuetzt.html

Bahnhof Berlin-Südkreuz ein Test mit Überwachungskameras zur biometrischen Gesichtserkennung statt.[10] Ein Blick nach China zeigt die Perspektive diese Entwicklung auf: In einem Artikel der FAZ.Net vom 4. Oktober 2017 unter der Überschrift „Die wunderbare Welt der Totalüberwachung"[11] heißt es u.a.: „Chinas Bürger sind bereits heute weitflächiger Überwachung unterworfen. Der Staat und die Sicherheitsbehörden haben Zugriff auf die von Mobiltelefonen gesendeten Daten und können damit Bewegungen und Verhalten Einzelner beobachten. Überwachungskameras sind überall im Einsatz. … Jetzt aber hat eine neue Phase begonnen, in der auf Big Data und Künstliche Intelligenz wie bei der Gesichtserkennung gesetzt wird." „Künstliche Intelligenz ist schneller als die menschliche und wird die Berechenbarkeit und die Genauigkeit von gesellschaftlicher Steuerung drastisch verbessern", sagte Chinas oberster Sicherheitschef Meng Jianzhu, der Vorsitzende der mächtigen „Parteikommission für Politik und Recht", auf einer nationalen Konferenz. … In einem Beitrag im Magazin der Kommunistischen Partei, „Suche nach Wahrheit", heißt es, die allumfassende Überwachung, die frühzeitige Erkennung von Gefahren und der „Ausgleich von Konflikten" ermöglichten die Schaffung „eines friedvollen Chinas" sowie „gesellschaftliche Stabilität, Sicherheit und Harmonie"."

Einer solchen Entwicklung muss schon im Ansatz begegnet werden. Auch die Sicherheitspolitik in Baden-Württemberg wird sich künftig immer wieder der Frage stellen müssen, wie eine vernünftige und angemessene Ausstattung unserer Sicherheitsbehörden aussieht, welche gleichzeitig der Gefahr „chinesischer Verhältnisse" begegnet.

1.3 „Und Action!" – Zunahme der Videoüberwachung in allen Lebensbereichen

Wer morgens mit den öffentlichen Verkehrsmitteln zur Arbeit fährt, kennt das: Schon am Bahnhof oder an der Haltestelle wird man von Kameras, die ganz unscheinbar an Decken und Wänden installiert sind, begrüßt. Allein in den S-und U-Bahnen, Bussen sowie an den Bahnhöfen werden wir unzählige Male von einer Überwachungskamera erfasst. Wer sich auf dem Weg zur Arbeit dann noch in einem Café oder beim Bäcker einen Kaffee holt, darf auch dort noch einmal freundlich in die Kameras lächeln. Die immer günstiger werdende Videoüberwachungstechnik scheint zwischenzeitlich allgegenwärtig und ist aus unserem Alltag nicht mehr wegzudenken. Kein Wunder, vermittelt eine Kamera doch für den unbescholtenen Bürger auf den ersten Blick größtmögliche Sicherheit – geht er doch zunächst einmal davon aus, dass hinter der Kamera jemand sitzt, der die Bilder der Kamera auswertet und in Gefahrensituationen eingriffsbereit ist. Doch hält die Videoüberwachung wirklich was sie verspricht? Oder ist sie letztlich nur eine Mogelpackung, die uns eine gar nicht vorhandene Sicherheit vorgaukelt?

1.3.1 Videoüberwachung – Zauberformel zur Stärkung des allgemeinen Sicherheitsempfindens?

Geht es nach Bundesinnenminister Thomas de Maizière und einem Großteil der Bevölkerung, dann scheint die Videoüberwachung tatsächlich das Allheilmittel gegen Terror, Gewalt und eine gestiegene Kriminalitätsbelastung zu sein. Insbesondere nach den Terroranschlägen von Paris, Nizza und Berlin sowie dem Amoklauf in einem Einkaufszentrum in München 2016 wird der Ruf nach einem verstärkten Einsatz der Videoüberwachungstechnik immer lauter, was den Gesetzgeber letztlich dazu bewegt hat, die Voraussetzungen für den Einsatz von Überwachungskameras in öffentlich zugänglichen großflächigen Anlagen und im öffentlichen Personenverkehr zu erleichtern. Dass der Bürger damit immer „gläserner" wird, ein unbeobachtetes Bewegen in der Öffentlichkeit dadurch beinahe ausgeschlossen ist, scheint kaum jemanden ernsthaft zu stören. Die oftmals trotzige Rechtfertigung „Ich habe ja nichts zu verbergen" ist in diesem Zusammenhang des Öfteren zu hören.

Wirft man einen Blick auf die Anzahl der in meiner Dienststelle eingegangenen Beschwerden im Berichtszeitraum 2016/2017 so ergibt sich ein ganz anderes Bild: „Videoüberwachung ja, aber…". Nach unseren Erfahrungen wird der Einsatz von Videoüberwachung nur befürwortet, so lange man nicht unmittelbar und nicht nur vorübergehend selbst von der Überwa-

10 http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2017/08/sicherheitsbahnhof.html
11 http://plus.faz.net/politik/2017-10-04/die-wunderbare-welt-der-totalueberwachung/63343.html#offers

chung betroffen ist. Sobald aber eine Kamera auf den Arbeitsplatz gerichtet ist oder man sich im Fitnessstudio beim Training oder an der Bar in der eigenen Lieblingskneipe beobachtet fühlt, geht die Befürwortung und das Verständnis für eine Überwachung merklich zurück. Das ist auch gut so, denn jeder hat eben doch etwas zu verbergen – nämlich seine Privatsphäre – und muss eine Videoüberwachung nur im Rahmen der gesetzlichen Vorgaben der §§ 6b bzw. 28 des Bundesdatenschutzgesetzes (BDSG) hinnehmen.

Der Einsatz von Videoüberwachungskameras ist aus meiner Sicht aber noch aus einem anderen Grund zweifelhaft: Der nicht vorhandene, aber dennoch viel beschworene Sicherheitsaspekt! Politik und Wirtschaft werden nicht müde, der Videoüberwachung einen präventiven Charakter zu zuschreiben. Eine Videoüberwachung mag vielleicht Jugendliche oder Ersttäter von ihren Taten abhalten; Terroristen oder Amokläufer, die gerade die Öffentlichkeit für ihre Taten suchen, werden sie ganz bestimmt nicht an ihrem Vorhaben hindern. Hinzu tritt die Tatsache, dass Videoüberwachungsanlagen in den meisten Fällen im Rahmen eines sog. Black Box Verfahrens betrieben werden. Es werden also lediglich Aufzeichnungen gespeichert, die dann im Nachhinein, für den Fall, dass es zu einer Straftat gekommen ist, ausgewertet werden. Eine Live-Beobachtung der Videoüberwachungsanlangen im Rahmen eines sog. „Monitorings", mit welchem konkrete Gefahren und Straftaten direkt erkannt und verhindert werden könnten, ist in aller Regel zu kostenintensiv.

Die Überwachungskamera mag daher zwar auf den ersten Blick ein subjektives Sicherheitsgefühl vermitteln. Bei näherem Hinsehen wird allerdings deutlich, dass sie im Notfall regelmäßig gar nicht helfen kann.

1.3.2 Neue gesetzliche Voraussetzungen: „Videoüberwachungsverbesserungsgesetz"

Unter dem Eindruck terroristischer Anschläge im Sommer 2016 hat der Bundestag ein Gesetz zur „Erhöhung der Sicherheit in öffentlich zugänglichen großflächigen Anlagen und im öffentlichen Personennahverkehr durch optisch-elektronische Einrichtungen" beschlossen.

Das Videoüberwachungsverbesserungsgesetz vom 28. April 2017[12] ändert § 6b des Bundesdatenschutzgesetzes (BDSG) insofern, als bei der Videoüberwachung von öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs, oder Fahrzeugen und öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, „der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse gilt." Die Bundesregierung erhofft sich mit der Neuregelung eine Erhöhung des Sicherheitsniveaus in Deutschland sowie eine Verhinderung von Anschlägen, wie in München und Ansbach geschehen.[13] So sei der Einsatz von optisch-elektronischer Sicherheitstechnologie auch eine Maßnahme im öffentlichen Interesse, um die Sicherheit der Bevölkerung präventiv zu erhöhen. Dies könne erreicht werden, indem die Betreiber einer entsprechenden Videoüberwachungsanlage potenzielle Täter etwa bei der Erkundung von Örtlichkeiten im Vorfeld oder unmittelbar vor einer Tatbegehung erkennen und diese Taten vereitelt werden könnten.

Der neue Wortlaut bestimmt den Schutz von Leben, Gesundheit oder Freiheit der sich in hochfrequentierten Anlagen und Einrichtungen aufhaltenden Personen als ein besonders wichtiges Interesse. Nach der Gesetzesbegründung können diese Belange von den jeweiligen Betreibern entsprechend in die Abwägungsentscheidung nach § 6b Absatz 1 Satz 1 Nummer 3 BDSG über den Einsatz einer Videoüberwachung einbezogen und neben ihren zivilrechtlichen Verpflichtungen (z.B. Verkehrssicherungspflicht) verstärkt beachtet werden. Die Abwägungsentscheidung soll im Rahmen des § 6b BDSG nunmehr zugunsten der Zulässigkeit des Einsatzes einer Videoüberwachungsmaßnahme „geprägt" sein. Der Gesetzgeber stellt diesbezüglich auch fest, dass die aus dem grundgesetzlich abgesicherten Recht auf informationelle Selbstbestimmung herrührende Interessenabwägung nach § 6b Absatz 1 Satz 1 BDSG weiterhin notwendig bleibt.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hatte sich am 9. November 2016 mit der Entschließung „Videoüberwachungsverbesserungsge-

12 BGBl. 2017 Teil I Seite 968
13 Bundestags- Drucksache 18/10941 vom 23.01.2017

setz zurückziehen!" gegen eine Änderung des § 6b BDSG ausgesprochen. Aus Sicht der Datenschutzkonferenz ist u.a. fraglich, ob die Sicherheit in Deutschland mit privaten Videoüberwachungsanlagen tatsächlich präventiv erhöht werden kann. Um mit einer Videoüberwachung einen realen Sicherheitsgewinn im Fall eines drohenden (Selbstmord-)Anschlags zu erreichen, wäre eine sofortige bzw. frühe Reaktion des Kamerabetreibers notwendig. Private Betreiber müssten demnach in der Lage sein, terroristische Gefahren in hochfrequentierten Räumen im Vorfeld zu erkennen und diesen begegnen zu können. Diese Anforderungen dürften von Privaten nicht zu erfüllen und außerdem mit hohen Kosten verbunden sein.

1.3.3 Videoüberwachung im Beschäftigungsverhältnis

Der Bäcker, der seine Verkäuferinnen hinter der Verkaufstheke mittels Kameras überwachen lässt, oder der Eigentümer eines Einzelhandelsbetriebs, der während der Arbeitszeit immer wieder gerne auf den Monitor schaut, um zu sehen, was seine Mitarbeiter vor Ort gerade so machen – die Videoüberwachung wird auch zunehmend von Arbeitgebern zur Leistungskontrolle der eigenen Mitarbeiter eingesetzt. Dabei sind es aber nicht nur Einzelhandelsbetriebe und kleine Unternehmen, die auf die Videoüberwachung ihrer Mitarbeiter setzen. Zunehmend müssen wir feststellen, dass gerade auch größere Betriebe Kameras in ihren Produktions-und Verwaltungsräumen sowie Versandhallen installieren. Ausschlaggebend ist hier oftmals ein massives Misstrauen der Arbeitgeber gegenüber ihren Mitarbeitern. Aber auch wenn zunächst andere Zwecke für die Videoüberwachung (z.B. Wahrung des Hausrechts durch Überwachung der Ein- und Ausgänge, Schutz des Eigentums vor Diebstählen und Einbrüchen durch Überwachung der Zugänge/Rolltore etc.) genannt werden, kann dies – wenn auch unbeabsichtigt – eine datenschutzrechtlich unzulässige Mitarbeiterüberwachung in Form einer Leistungskontrolle zur Folge haben.

Ob und, wenn ja, wie eine Videoüberwachung am Arbeitsplatz zulässigerweise erfolgen kann, richtet sich nach den engen Voraussetzungen des § 32 bzw. i.V. mit § 28 des Bundesdatenschutzgesetzes (BDSG). Nach § 28 Absatz 1 Satz 1 Nummer 2 BDSG ist das Erheben und Speichern personenbezogener Daten zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Sofern sich die Videokameras jedoch in Räumlichkeiten bzw. Örtlichkeiten befinden, die grundsätzlich nur von hierzu berechtigten Mitarbeitern genutzt werden, ist die Überwachungsmaßnahme zusätzlich an § 32 BDSG zu messen. Danach dürfen zur Aufdeckung von Straftaten personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Ergänzend ist die arbeitsgerichtliche Rechtsprechung heranzuziehen.[14] Sofern angegeben wird, die Kameras dienten in aller erster Linie dem Schutz vor Eigentumsdelikten (z.B. Warendiebstählen etc.) durch die eigenen Mitarbeiter oder sich dieser Zweck aufgrund der Kameraeinstellungen ergibt, ist die Videoüberwachung diesbezüglich sogar ausschließlich an § 32 BDSG zu messen. Für Arbeitsplätze, die sich in öffentlich zugänglichen Räumen befinden (z.B. in einem großen Kaufhaus) richtet sich die Zulässigkeit hingegen nach § 32 i.V. mit § 6b BDSG.

Um die engen rechtlichen Voraussetzungen zu umgehen, setzen Arbeitgeber zunehmend auch auf die Möglichkeit der Einwilligung in die Datenerhebung. Nach § 4a Absatz 1 Satz 1 und Satz 2 BDSG kann eine Einwilligung nur wirksam erklärt werden, wenn sie auf der freien Entscheidung des Betroffenen beruht (Freiwilligkeit) und der Betroffene auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Ein-

14 vgl. z.B. BAG, Urteil vom 27.03.2003, Az. 2 AZR 51/02; Beschluss vom 29.06.2004, Az. 1 ABR 21/03; Beschluss vom 14.12.2004, Az. 1 ABR 34/03; Beschluss vom 26.08.2008, Az. 1 ABR 16/07; Urteil vom 21.06.2012, Az. 2 AZR 153/11

willigung (Informiertheit) hingewiesen wird. Trotz des bestehenden Über- und Unterordnungsverhältnisses im Arbeitsverhältnis gehen wir grundsätzlich davon aus, dass eine Einwilligung in die Datenerhebung, -verarbeitung und -nutzung im Beschäftigtenverhältnis nicht generell unzulässig ist. Aufgrund des speziellen Abhängigkeitsverhältnisses zwischen Arbeitgeber und Arbeitnehmer sind jedoch besonders hohe Anforderungen an die Prüfung zu stellen, ob in einem solchen Abhängigkeitsverhältnis eine freie Entscheidung möglich ist. Es kommt also – wie so oft – auf den konkreten Einzelfall an.

Sofern Erkenntnisse vorliegen, dass die Videoüberwachung vorrangig einer präventiven und repressiven Verhaltenskontrolle der Belegschaft dienen soll, gilt Folgendes: Die Arbeitnehmerinnen und Arbeitnehmer stehen letztlich vor der Wahl, sich entweder mit der eigenen Überwachung einverstanden zu erklären oder sich durch die Verweigerung ihrer Einwilligung als Tatverdächtige zu stigmatisieren. Verweigert ein Arbeitnehmer seine Einwilligung, ist es also nicht ausgeschlossen, dass dieser erhebliche Nachteile im Arbeitsverhältnis befürchtet oder befürchten muss. Eine echte Wahl zwischen Abgabe und Ablehnung der Einwilligungserklärung besteht somit zu keinem Zeitpunkt, was wiederum zur Folge hat, dass nicht von einer Freiwilligkeit ausgegangen werden kann.

1.3.4 Videoüberwachung im Freizeitbereich

Wie schon im Zeitraum 2014/2015 hat uns auch 2016/2017 vor allem die Videoüberwachung in Schwimmbädern beschäftigt. Unabhängig davon, ob sich Schwimmbäder in privater oder öffentlicher Trägerschaft befinden, die Videoüberwachung scheint auch dort als Wundermittel zu gelten. Dabei sind die Argumente der Schwimmbadbetreiber für eine Videoüberwachung so vielfältig wie die Standorte der Kameras: Vom Diebstahlsschutz in den Kassen- und Umkleidebereichen, über den Schutz vor Leistungserschleichungen in den Durchgangs- und Drehkreuzbereichen, bis hin zum Schutz von Leib und Leben im Bäder- bzw. Saunabereich. Für sich genommen, handelt es sich bei allen genannten Argumenten um rechtlich zulässige Zwecke. Aber schaut man genauer hin, so ist eine Videoüberwachungskamera eben doch nicht das geeignete oder erforderliche Mittel, um beispielsweise den Leistungserschleichungen in den Durchgangs- und Drehkreuzbereichen zu begegnen. Und insbesondere in den Saunen und textilfreien Bereichen muss man sich ganz besonders fragen, ob eine dem allgemeinen Lebensrisiko zurechenbare Gefährdung, wie beispielsweise ein Kreislaufzusammenbruch, den Einsatz einer Videoüberwachung, gegebenenfalls mit Aufzeichnung aller sich täglich in der Sauna aufhaltenden Personen, rechtfertigt, oder ob für solche Fälle nicht auf entsprechend geschultes Personal in den Saunen gesetzt werden sollte, die im Notfall auch unmittelbar vor Ort handeln können.

Wie verbreitet Videoüberwachungskameras darüber hinaus im Freizeitbereich sind, konnten wir anhand unserer Beschwerdeeingänge sehen: Ein großer Teil der Beschwerden richtete sich gegen Videoüberwachungskameras in Fitnessstudios. Bei der Überprüfung der Eingaben mussten wir leider feststellen, dass auch zunehmend Betreiber von Fitnessstudios Videotechnik zur Überwachung ihrer Trainings- und Kursflächen sowie ihrer Geräte einsetzen. Der genannte Zweck – Schutz von Leib und Leben der Gäste – stellt zunächst auch ein berechtigtes Interesse nach § 6b bzw. § 28 BDSG dar. Allerdings darf die Videoüberwachung nicht das qualifizierte Personal vor Ort ersetzen. Nur dieses kann im Notfall helfen und entsprechende Maßnahmen einleiten. Die Kamera, deren Bilder auf eine Black-Box übertragen werden, kann dies gerade nicht. Daneben waren aber auch die massive Überwachung in Gaststätten sowie die Implementierungen einer videoüberwachten Zugangskontrolle an einem Skilift sowie in Spielhallen zentrale Themen des Berichtsjahres.

1.3.5 Videoüberwachung in Gaststätten

Gaststättenbetreiber richten eine Videoüberwachung meistens zu dem Zweck ein, um sich vor Sachbeschädigungen, Diebstahl, Einbruch, Zechprellerei oder Überfällen zu schützen. Die Überwachung soll solche Taten verhindern und ggf. bei deren Aufklärung helfen. Dem gegenüber steht das Interesse der Gäste, sich unbeobachtet erholen, entspannen, essen und unterhalten zu können.

Bevor ein Kamerasystem in einer Gaststätte installiert wird, hat der Betreiber festzulegen, welches konkrete Ziel mit der Überwachung verfolgt werden soll. Wird die Videoüberwachung eingesetzt, um vor Einbrüchen, Diebstählen oder Sachbeschädigungen zu schützen, ist darin grundsätzlich ein berechtigtes

Interesse zu sehen. Allerdings muss in diesen Fällen eine tatsächliche Gefahr nachgewiesen werden, beispielsweise Beschädigungen oder besondere Vorkommnisse in der Vergangenheit. Weiter bedarf es des Nachweises, dass die Überwachung das geeignete und erforderliche Mittel ist, um den angestrebten Zweck zu erreichen. Deshalb ist immer zunächst zu prüfen, ob alternative Maßnahmen den Überwachungszweck ebenfalls erreichen könnten. So schützen beispielsweise Alarmanlagen, Schließsysteme und Lichtanlagen mit Bewegungsmeldern vor mutwilliger Beschädigung und vor Einbrüchen, ohne dabei in Persönlichkeitsrechte anderer einzugreifen. Versprechen solche anderen Mittel keinen Erfolg oder sind diese im Einzelfall nicht zumutbar, muss der Einsatz von Videoüberwachungstechnik jedenfalls zeitlich und räumlich auf das Notwendigste beschränkt sein. Das kann bedeuten, dass eine Videoüberwachung in der Gaststätte nur außerhalb der Öffnungszeiten erfolgen darf oder eine Kameraerfassung auf bestimmte, ausgewählte Bereiche beschränkt sein muss.

Der Betreiber einer Videoüberwachungsanlage hat nicht nur die eben genannten Grundvoraussetzungen einzuhalten, sondern darüber hinaus für jede einzelne Kameraerfassung sein Überwachungsinteresse mit den schutzwürdigen Interessen der Betroffenen abzuwägen. Bei einem Kameraeinsatz in der Gastronomie können diese Interessen – je nach überwachtem Bereich – unterschiedlich stark zu gewichten sein.

In Ein- und Ausgangsbereichen, Fluren und Treppenhäusern von Gaststätten ist die Aufenthaltsdauer von Gästen in der Regel kurz, d.h. der Eingriff in die Rechte der Gäste und Beschäftigten bleibt – je nach Ausrichtung der Kamera – überschaubar. Soll die Videoüberwachung vor Einbrechern schützen und kommt die Installation einer Alarmanlage nicht in Betracht, dürfen Kameras hier nur außerhalb der Öffnungszeiten aktiv sein.

An der Gebäudefassade darf der Erfassungsbereich der Videokameras grundsätzlich nicht über die Grundstücksgrenzen hinausgehen, d.h. eine Videoüberwachung von öffentlichen Flächen (wie Straßen und Gehwege) ist in der Regel nicht zulässig. Nur wenn es für den Überwachungszweck lage- oder situationsbedingt unvermeidbar ist, kann dies im Ausnahmefall gerechtfertigt sein, beispielsweise wenn die Fassade in der Vergangenheit mutwillig beschädigt worden ist. In solchen Fällen ist der Erfassungsbereich der Kameras räumlich auf das zwingend erforderliche Maß, d.h. auf einen Bereich, der maximal einen Meter des öffentlichen Verkehrsraums erfasst, zu beschränken. Zu prüfen ist außerdem, ob die Erfassung zeitlich begrenzt werden kann.

In den Ess- und Aufenthaltsbereichen einer Gaststätte (Sitzbereiche, Außengastronomie, Theke, Bar, etc.) halten sich Gäste typischerweise über eine längere Zeit auf, sie essen, trinken und unterhalten sich. Die Rechtsprechung ordnet dieses Verhalten dem Freizeitbereich der Gäste zu, weshalb Persönlichkeitsrechte hier besonders zu schützen sind. Eine Videoüberwachung stört die unbeeinträchtigte Kommunikation und den unbeobachteten Aufenthalt der Gaststättenbesucher und greift besonders intensiv in deren Rechte ein. Auch besteht in den Ess- und Aufenthaltsbereichen während der Öffnungszeiten keine überdurchschnittlich hohe Gefahr für das Eigentum des Gastronomen. Neben den Gästen befindet sich üblicherweise auch Personal in der Gaststätte, das bei entsprechenden Vorfällen unmittelbar die Polizei verständigen kann. Bereiche, die zum längeren Verweilen, Entspannen und Kommunizieren einladen, dürfen daher regelmäßig nicht mit Videokameras überwacht werden.

Grundsätzlich unzulässig sind Überwachungsanlagen, welche die Intimsphäre der Menschen verletzen. Die Überwachung von sensiblen Bereichen wie Toiletten, Sanitärräumen, Duschen und Umkleidekabinen ist daher nicht erlaubt. Darüber hinaus dürfen auch Pausen- oder Sozialräumen von Beschäftigten nicht videoüberwacht werden.

Lager und Tresorräume sind in einer Gaststätte üblicherweise für Gäste nicht frei zugänglich. Sie können dann überwacht werden, wenn in diesen Bereichen keine dauerhaften Arbeitsplätze eingerichtet sind, keine milderen Mittel zur Zweckerreichung zur Verfügung stehen und der Erfassungsbereich der Kamera auf das Notwendigste beschränkt ist. In Küchen dürfen Kameras nur außerhalb der Betriebszeiten aktiviert werden.

Auch der Bereich vor einer Theke darf während der Öffnungszeiten nicht videoüberwacht werden, da es sich hierbei um einen Ess- und Aufenthaltsbereich für Gäste handelt (s.o.). Dauerhafte Arbeitsbereiche von Beschäftigten hinter einer Theke sind von einer Videoüberwachung ebenfalls auszuschließen.

Die Kasse selbst kann videoüberwacht werden, wenn strafrechtlich relevante Vorfälle stattgefunden haben und diese nicht ohne den Einsatz von Videoüberwachung nachgewiesen werden können. Zudem darf es im Einzelfall keine anderen, milderen Maßnahmen zur Sicherung der Kasse geben. Solche können beispielsweise sein, die Kasse in einen geschützten Bereich innerhalb der Gaststätte zu verlegen oder das Kassensystem mit technischen Maßnahmen besonders zu sichern. Persönlichkeitsrechte von Beschäftigten sind auch in diesem Bereich zu achten, weshalb eine Kameraerfassung auf das unmittelbare Umfeld der Kasse zu begrenzen ist.

Eine Videoüberwachung von Glücksspielautomaten ist begrenzt möglich. Der Überwachungsbereich ist dabei unmittelbar auf Automatenbereich zu beschränken. Eine weiträumige Erfassung der Gaststätte ist dabei nicht erforderlich.

1.3.6 Videoüberwachung durch öffentliche Stellen

Dass die Videoüberwachung auch für öffentliche Stellen ein Schwerpunktthema ist, zeigt sich anhand der vielen Beratungsanfragen von Kommunen und Behörden, die uns im Berichtszeitraum erreicht haben. Insbesondere scheint bei den Kommunen erheblicher Bedarf an einer Videoüberwachung von Schulhöfen und kommunalbetriebenen Müllcontainerstandorten/ Wertstoffhöfen gegeben zu sein. Die Zulässigkeit einer Videoüberwachung/-beobachtung durch öffentliche Stellen richtet sich nach § 20a des Landesdatenschutzgesetzes (LDSG). Hiernach kann eine Videobeobachtung im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts zum Schutz von Leben, Gesundheit, Freiheit oder Eigentum von Personen, die sich im Bereich öffentlicher Einrichtungen, öffentlicher Verkehrsmittel, von Amtsgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen aufhalten oder zum Schutz von Kulturgütern, öffentlichen Einrichtungen, öffentlichen Verkehrsmitteln, Amtsgebäuden und sonstigen baulichen Anlagen öffentlicher Stellen zulässig sein.

Neben der Videoüberwachung von baulichen Anlagen war auch die Videoüberwachung von bzw. an Kriminalitätsschwerpunkten ein relevantes Thema im Berichtszeitraum. In Baden-Württemberg findet eine solche Videoüberwachung bereits seit 2007 im Bereich des Bahnhofvorplatzes in Mannheim statt. Im Rahmen eines Kontrollbesuchs beim Polizeipräsidium Mannheim konnten wir uns die praktische Ausgestaltung einer solchen Videoüberwachung demonstrieren lassen. Die von uns geforderte präventive Ausrichtung einer solchen polizeilichen Videoüberwachung – d.h. die Möglichkeit, bei Erkennen von Straftaten oder Delikten im Vorbereitungsstadium durch Hinzuziehen einer Streifenbesatzung entsprechend eingreifen zu können – wird dort konsequent umgesetzt. Nur ein solches konsequentes Zusammenspiel von Videoüberwachung und zeitnaher Reaktions- und Eingriffsmöglichkeit führt letztendlich zu einer Verhältnismäßigkeit und damit Zulässigkeit der Maßnahme nach § 21 des Polizeigesetzes (PolG BW).

Auch in den Justizvollzugsanstalten spielt die Videoüberwachung eine wichtige Rolle. Aus diesem Grund haben Mitarbeiter meiner Dienststelle im Berichtszeitraum in einer Justizvollzugsanstalt die Videoüberwachung des Hofbereichs und der Gebäudefassade, die unter anderem der Aufrechterhaltung der Sicherheit der Anstalt dient, und in zwei weiteren Justizvollzugsanstalten die Videoüberwachung der unmittelbaren Anstaltsumgebung, deren Zweck vor allem die Verhinderung von Mauerüberwürfen ist, kontrolliert.

1.3.7 Dashcams

Die anlasslose, dauerhafte Nutzung von Dashcams bleibt rechtswidrig und wird von Gerichten als Ordnungswidrigkeit bewertet. Entsprechend ist die datenschutzrechtliche Unzulässigkeit von Dashcam-Aufnahmen in zwei Urteilen gerichtlich festgestellt worden.

Das Verwaltungsgericht Göttingen bestätigte eine datenschutzrechtliche Anordnung der Landesbeauftragten für den Datenschutz Niedersachsen, die eine dauerhafte und anlasslose Dashcam-Nutzung an Front- und Heckscheibe eines PKW-Fahrers untersagt hatte. Der als „Knöllchen-Horst" bekannt gewordene Fahrzeugführer setzte die Kameras dazu ein, um vermeintliche oder tatsächliche Verkehrsverstöße anderer Verkehrsteilnehmer zu dokumentieren und diese gegenüber Ordnungsbehörden beweisen zu können. Das Verwaltungsgericht stellte fest, dass dieser Einsatz der Kameras datenschutzrechtlich unzulässig sei. Mit der Praxis habe der Fahrzeugführer keine eigenen schützenswerten Interessen verfolgt, sondern sei als Sachwalter öffentlicher

Interessen aufgetreten. Die öffentliche Aufgabe der Gewährleistung eines gesetzeskonformen Straßenverkehrs obliege ausschließlich den Straßenverkehrsbehörden und der Polizei, nicht aber privaten Dritten. Zudem könne ein berechtigtes Interesse wie Selbst- und Eigentumsschutz und einer diesbezüglichen Beweissicherung, den Einsatz der Kameras allenfalls in solchen Einzelfällen rechtfertigen, aber nicht die in Rede stehende anlasslose und regelmäßige Videoüberwachung des Straßenverkehrs. Ähnlich urteilte das Amtsgericht in München. Das Gericht bestätigte ein Bußgeld, bei der eine Dashcam nicht aus einem fahrenden, sondern aus einem parkenden Auto heraus seine Umgebung filmte. Eine 52-jährige Geschäftsführerin aus München wurde zu einer Geldbuße von 150 EUR verurteilt, da sie laufend Videoaufzeichnungen des vor und hinter dem geparkten Fahrzeug befindlichen öffentlichen Verkehrsraums anfertigte und speicherte. Es kam ihr darauf an, potenzielle Täter einer Sachbeschädigung an ihrem PKW ermitteln zu können. Der zuständige Richter am Amtsgericht beurteilte ihr Verhalten als vorsätzliche Ordnungswidrigkeit und führte aus, dass im vorliegenden Fall das Recht der gefilmten Personen auf informationelle Selbstbestimmung überwiege. Das Interesse der Betroffenen an der Aufdeckung einer potenziellen Straftat müsse hierbei zurückstehen. Das permanente anlasslose Filmen des vor und hinter dem geparkten Fahrzeug befindlichen Straßenraums verletze das Recht auf informationelle Selbstbestimmung schwerwiegend. Es gehe nicht an, dass 80 Millionen Bundesbürger mit Kameras herumlaufen, um irgendwelche Situationen aufnehmen zu können, die eine Straftat aufdecken könnten. Eine permanente Überwachung jeglichen öffentlichen Raums durch Privatbürger sei nicht zulässig, da dies in das Recht unbeteiligter Personen in schwerwiegender Weise eingreife.

Das Urteil verdeutlicht die geltende Rechtslage: Eine anlasslose Videoüberwachung im öffentlichen Raum erfasst eine Vielzahl völlig unbeteiligter Personen und verstößt damit gegen die Vorschriften des Bundesdatenschutzgesetzes. Der Eingriff in die Rechte der betroffenen Verkehrsteilnehmer wiegt dabei schwer, weil er heimlich und ohne Anlass erfolgt und eine große Streubreite und Eingriffstiefe erreichen kann – je nach Lage des Parkplatzes und Ausrichtung der Kamera. Das Interesse an einer effektiven Beweismittelführung in einem möglichen Unfallprozess und einer effektiven Strafverfolgung bei einer möglichen Unfallflucht des Gegners muss in diesen Fällen zurücktreten. Dieser Konflikt könnte aber mit dem Einsatz intelligenter Videosysteme, verbunden mit einer automatischen periodischen Löschung, gelöst werden. Dabei werden die aufgezeichneten Daten stets unmittelbar überschrieben, es sei denn, es wird z.B. durch Unfallsensoren eine anlassbezogene Sicherung des letzten Aufzeichnungsintervalls ausgelöst. Für die Dokumentation von Nötigungen oder Ähnlichem, nicht unfallbezogenem Verhalten, ist auch das manuelle Starten des Aufnahmevorgangs denkbar.

Auch wenn es bei der Vielzahl von Videokameras manchmal aussichtslos erscheinen mag, werde ich mich auch künftig für den Schutz des Rechts auf informationelle Selbstbestimmung einsetzen und die uns gemeldeten Videokameras in allen Lebensbereichen auf ihre datenschutzrechtliche Zulässigkeit überprüfen. Denn die Videoüberwachungstechnik ist vor allem eines nicht – ein Allheilmittel im rechtsfreien Raum!

1.4 Vom langen Nachhall eines Paukenschlags: Safe Harbor, der EuGH und der EU-U.S. Privacy Shield

In einem viel beachteten Urteil hat der Europäische Gerichtshof am 6. Oktober 2015 aufgrund einer Vorlage durch ein irisches Gericht im Klageverfahren des österreichischen Facebook-Nutzers Max Schrems gegen die irische Datenschutzaufsichtsbehörde die Angemessenheitsentscheidung der Europäischen Kommission vom 26. Juli 2000 für die Vereinigten Staaten von Amerika (sog. Safe Harbor-Entscheidung) mit sofortiger Wirkung für ungültig erklärt (Rechtssache C-362/14). Zugleich hat das Gericht festgestellt, dass die europäischen Datenschutzaufsichtsbehörden trotz des Vorliegens einer Angemessenheitsentscheidung der Kommission berechtigt und verpflichtet sind, die Angemessenheit des Datenschutzniveaus in einem Drittstaat eigenständig zu prüfen. Die unmittelbaren und mittelbaren Folgen dieses Urteils waren im Berichtszeitraum ein großes Thema nicht nur auf der Agenda des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg, sondern auch der DSK sowie der Artikel-29-Gruppe auf europäischer Ebene.

Die deutschen Datenschutzbeauftragten haben bereits seit mehreren Jahren kritisiert, dass

Safe Harbor als Selbstzertifizierungssystem keinen ausreichenden Schutz für den Transfer personenbezogener Daten in die USA biete.[15] Der EuGH hat die Kommissionsentscheidung zu Safe Harbor zum einen aufgehoben, weil er die darin vorgesehenen Hürden für eine Aussetzung oder Untersagung eines Drittstaatentransfers durch europäische Aufsichtsbehörden als unzulässigen Eingriff in die aufsichtsbehördlichen Befugnisse nach der EG-Datenschutzrichtlinie einstufte. Ein zweiter Grund für die Aufhebung der Entscheidung lag darin, dass die Kommission es nach Einschätzung des EuGH versäumt hatte, die Rechtslage und Rechtspraxis in den USA bezüglich des Schutzes personenbezogener Daten tatsächlich umfassend daraufhin zu überprüfen, ob diese ein den in der europäischen Union gültigen Vorgaben im Wesentlichen gleichwertiges und daher als angemessen anzusehendes Datenschutzniveau bieten. Im Hinblick auf die Befugnisse der Geheimdienste und Sicherheitsbehörden in den USA kam der EuGH zudem zu dem Schluss, dass insbesondere „eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des durch Artikel 7 der (EU-Grundrechte) Charta garantierten Grundrechts auf Achtung des Privatlebens verletzt" (Rdnr. 93). Außerdem verletze „eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des in Artikel 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz" (Rdnr. 95).

Als unmittelbare Folge des Urteils des EuGH vom 6. Oktober 2015 war die Übermittlung personenbezogener Daten in die USA auf der Grundlage einer Safe Harbor-Zertifizierung des Empfängers mit sofortiger Wirkung nicht mehr möglich. Dies stellte Unternehmen, die ihre Übermittlungen personenbezogener Daten an U.S.-Unternehmen auf Safe Harbor gestützt hatten, z.T. vor erhebliche Probleme, weil kurzfristig ein Ausweichen auf andere Transferinstrumente wie insbesondere Standardverträge erforderlich wurde. Erfreulicherweise haben mehrere U.S.-Unternehmen, die in großem Umfang – und in der Regel als Auftragsdatenverarbeiter – Cloud Computing-Leistungen in Europa anbieten und den Transfer bislang auf Safe Harbor gestützt hatten, ihren Auftraggebern kurzfristig nach dem 6. Oktober 2015 als Ersatz für Safe Harbor den Abschluss von Standardverträgen angeboten.

Die Europäische Kommission hat als Reaktion auf das Urteil des EuGH ihre bereits seit 2013 laufenden Verhandlungen mit U.S.-Behörden über ein Nachfolgeinstrument zu Safe Harbor intensiviert und bereits am 29. Februar 2016 unter dem Namen „EU-U.S. Privacy Shield" den Entwurf einer Angemessenheitsentscheidung nach Artikel 25 Absatz 6 der EG-Datenschutzrichtlinie als Nachfolgeinstrument für Safe Harbor vorgelegt. Die Artikel-29-Datenschutzgruppe, das Kooperationsgremium der unabhängigen Datenschutzaufsichtsbehörden der Mitgliedstaaten der Europäischen Union, hat hierzu in einer Stellungnahme am 13. April 2016 sowie einer begleitenden Pressemitteilung festgestellt, dass der erste Entwurf des Privacy Shield im Vergleich zu der vom Europäischen Gerichtshof aufgehobenen Vorgängerregelung Safe Harbor zwar eine Reihe von Verbesserungen im Hinblick auf den Schutz personenbezogener Daten enthielte, gleichzeitig aber noch signifikante Bedenken insbesondere im Hinblick auf den Umfang und die Verhältnismäßigkeit möglicher Datenzugriffe durch U.S.-Nachrichtendienste und U.S.-Sicherheitsbehörden auf aus der EU übermittelte personenbezogene Daten bestünden; denn es sei nicht hinreichend klar, ob ein massiver, anlassloser und unterschiedsloser Zugang zu personenbezogenen Daten tatsächlich ausgeschlossen werden könne. Daneben stellte die Artikel-29-Gruppe auch in Frage, ob die vom Privacy Shield als Rechtsschutzmöglichkeit für Betroffene vorgesehene neu eingerichtete sog. Ombudsperson über hinreichende Befugnisse und eine ausreichende Unabhängigkeit verfügt, um den von der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte hinsichtlich des Rechtsschutzes Betroffener im Bereich nachrichtendienstlicher Überwachung aufgestellten Anforderungen zu genügen.

Nach weiteren Nachverhandlungen mit der U.S.-Seite verabschiedete die Europäische Kommission am 12. Juli 2016 die neue Angemessenheitsentscheidung zum EU-U.S. Privacy Shield, auf deren Grundlage seit 1. August 2016 ein Transfer personenbezogener Daten in die USA möglich ist. In einer weiteren Presse-

15 vgl. 31. TB 2012/13, LT-Drs. 15/4600, Kap. 1.3.7, S. 26 f. m.w.N. sowie die Entschließung vom 19. März 2015 (abgedruckt als Anhang 22, S. 230 im 32. Tätigkeitsbericht 2014/15)

mitteilung vom 26. Juli 2016 nahm die Artikel 29-Gruppe nochmals zu der Endfassung des Privacy Shields Stellung und äußerte weiterhin Zweifel im Hinblick auf die Stellung der Ombudsperson und mögliche anlasslose und massenhafte Datenzugriffe durch U.S.-Behörden. Da es sich bei der Angemessenheitsentscheidung der Kommission vom 12. Juli 2016 allerdings um einen wirksamen Rechtsakt handelt, ist hierdurch zunächst einmal verbindlich anerkannt, dass bei U.S.-Unternehmen, die eine entsprechende Selbstzertifizierung nach dem EU-U.S. Privacy Shield vorgenommen haben, von einem angemessenen Datenschutzniveau ausgegangen werden kann.

Nach aktuellem Stand (8. November 2017) haben sich bislang 2.532 Unternehmen in die auf der Website der International Trade Administration (ITA), einer nachgeordneten Behörde des US-Handelsministeriums, veröffentlichte Liste der zertifizierten Unternehmen aufnehmen lassen.

www.privacyshield.gov/list

Ebenso wie zuvor Safe Harbor beruht der Privacy Shield auf einem System der Selbstzertifizierung. Neben einer verbindlichen Erklärung, die im Privacy Shield festgelegten Grundsätze zum Schutz personenbezogener Daten zu befolgen, müssen U.S.-Unternehmen, die dem Privacy Shield beitreten wollen, dem U.S.-Handelsministerium eine Reihe von Nachweisen vorlegen, etwa eine Datenschutz-Policy. Zu beachten ist, dass die Teilnahme am Privacy Shield nicht allen Akteuren offensteht: gemeinnützige Organisationen, Banken, Versicherungsgesellschaften und Anbieter von Telekommunikationsdiensten müssen auf alternative Transferinstrumente wie Standardverträge ausweichen. Das U.S.-Handelsministerium überprüft, ob die Selbsterklärung alle erforderlichen Angaben enthält und setzt das US-Unternehmen sodann auf die Liste. Die Zertifizierung ist zunächst für ein Jahr gültig und muss danach vom Unternehmen erneuert werden. Aus der im Internet veröffentlichten Liste ist ersichtlich, ob sich die Zertifizierung auf den Import von Beschäftigtendaten (HR, d.i. human resources) und/oder sonstige personenbezogene Daten z.B. Kundendaten (Non-HR) bezieht.

Betroffene, die der Auffassung sind, dass ihre personenbezogenen Daten von einem Privacy Shield-zertifizierten U.S.-Unternehmen unter Verletzung der Privacy Shield-Grundsätze verarbeitet werden – etwa weil ihr Recht auf Auskunft oder Berichtigung nicht erfüllt wurde –, können sich zunächst an das U.S.-Unternehmen selbst wenden, das die Anfrage binnen 45 Tagen beantworten muss. Daneben steht Betroffenen eine kostenlose Beschwerdemöglichkeit bei unabhängigen Beschwerdestellen (i.d.R. Streitschlichtungsstellen) in den USA und – in letzter Instanz – noch die Möglichkeit eines Schiedsverfahrens in den USA zur Verfügung. Selbstverständlich können sich Betroffene auch an den jeweiligen Landesbeauftragten für den Datenschutz in Deutschland wenden. Hierfür existieren zwei Beschwerdeformulare, die auf unserer Homepage zusammen mit umfangreichem weiteren Informationsmaterial zum Privacy Shield abrufbar sind.

https://www.baden-wuerttemberg.datenschutz.de/ueberblick-eu-u-s-privacy-shield/

Das eine Beschwerdeformular ist für Beschwerden wegen Verstößen gegen die Vorgaben des Privacy Shield durch das importierende U.S.-Unternehmen gedacht, während das andere bei vermuteten Datenzugriffen durch U.S.-amerikanische Geheimdienste oder Sicherheitsbehörden zum Einsatz kommen soll. Beschwerden der letzteren Art werden über ein eigens hierfür eingerichtetes Gremium der europäischen Datenschutzaufsichtsbehörden (die sog. EU-Zentralstelle) einer Ombudsperson im U.S.-Außenministerium zugeleitet, die über Möglichkeiten zur Überprüfung der Beschwerde verfügt.

Soweit sich Beschwerden darauf beziehen, dass ein zertifiziertes U.S.-Unternehmen selbst beim Umgang mit den Daten des Betroffenen gegen die Privacy Shield-Grundsätze verstoßen hat, ist danach zu unterscheiden, ob sich die Beschwerde auf Beschäftigtendaten (HR) oder sonstige personenbezogene Daten (Non-HR) bezieht. In ersterem Fall kann ein sog. informelles Gremium aus Datenschutzbehörden der EU-Mitgliedstaaten gegenüber dem zertifizierten Unternehmen verbindliche Weisungen im konkreten Einzelfall erteilen. Soweit es um sonstige personenbezogene Daten geht, sind solche Weisungen zwar nicht möglich. Dafür können die Datenschutzbehörden der EU-Mitgliedstaaten die betreffende Beschwerde an die für die Aufsicht über die zertifizierten Unternehmen zuständigen Behörden in den USA weiterleiten.

Die Artikel-29-Gruppe hat zwischenzeitlich Informationsmaterial zum Privacy Shield in Gestalt von FAQ für Betroffene sowie für EU-Unternehmen erarbeitet (Arbeitspapiere 245 und 246). Darin werden u.a. die Funktionsweise des Privacy Shield, der Ablauf der Zertifizierung und die Rechte Betroffener erläutert.

https://www.bfdi.bund.de/SharedDocs/ExterneLinks/Sachthemen/Art29DSK_Unternehmen_deutsch.html;jsessionid=6BC6C1ADFD629F315B792F5764A2A68C.1_cid329?nn=5217132

https://www.bfdi.bund.de/SharedDocs/ExterneLinks/Sachthemen/Art29DSK_B%C3%BCrger_deutsch.html;jsessionid=6BC6C1ADFD629F315B792F5764A2A68C.1_cid329?nn=5217132

Das Regelwerk zum EU-U.S.-Privacy Shield sieht vor, dass die EU-Kommission unter Beteiligung von Vertretern der Artikel-29-Gruppe, betroffener Unternehmen und interessierter NGO's den Privacy Shield jährlich daraufhin überprüft, ob er (noch) ein angemessenes Datenschutzniveau bei den Importeuren in den USA gewährleistet. Sowohl die Europäische Kommission als auch die Artikel-29-Gruppe haben von Anfang an die große Bedeutung dieser Überprüfungen für die Fortentwicklung und Verbesserung der Funktionsweise des Privacy Shields betont. Am 18. und 19. September 2017 haben sich Vertreter der Europäischen Kommission und der Artikel-29-Gruppe mit Vertretern aller betroffenen U.S.-Behörden zur Vorbereitung der ersten jährlichen Überprüfung des Privacy Shields getroffen. Mit einer Presseerklärung vom 18. Oktober 2017 hat die Kommission eine erste positive Bilanz über das Funktionieren des Datenschutz-Shields gezogen und zugleich Empfehlungen zur weiteren Verbesserung seiner Handhabung gegeben. So hat die Kommission etwa von Seiten des U.S.-Handelsministeriums regelmäßige und anlasslose Kontrollen der Einhaltung der übernommenen Pflichten durch die zertifizierten Unternehmen und eine regelmäßige Fahndung nach Unternehmen, die im Internet unrichtige Angaben über ihre Zertifizierung machen, vorgeschlagen. Zudem sollen die Bürgerinnen und Bürger der EU verstärkt über ihre Rechte aufgrund des Privacy Shields informiert und die Zusammenarbeit zwischen den Aufsichtsbehörden dies- und jenseits des Atlantiks intensiviert werden.

http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619

Über kurz oder lang werden vermutlich nicht nur der EU-U.S.-Privacy Shield, sondern auch die Standardvertragsklauseln vor dem Europäische Gerichtshof auf dem Prüfstand stehen. Man darf gespannt sein, ob der EuGH dann die im Urteil vom 6. Oktober 2015 getroffenen Aussagen zur Reichweite des Wesensgehalts der Grundrechte aus Artikeln 7 und 47 der (EU-Grundrechte)Charta im Kontext nachrichtendienstlicher Datenverarbeitung weiter konkretisiert. Die daraus zu gewinnenden Erkenntnisse könnten zugleich auch in die laufenden Verhandlungen der Europäischen Kommission mit Japan und Korea über Adäquanzentscheidungen für diese Länder einfließen.

Das Nachfolgeinstrument zu Safe-Harbor, der EU-U.S. Privacy Shield, gibt betroffenen Bürgerinnen und Bürgern vielfältige Möglichkeiten, sich für eine rechtskonforme Verarbeitung ihrer personenbezogenen Daten nach europäischem Standard auch nach einem Transfer dieser Daten in die U.S.A. stark zu machen. Jetzt kommt es darauf an, dass die Betroffenen von ihren Rechten auch tatsächlich Gebrauch machen. Die Datenschutzaufsichtsbehörden werden versuchen, auch die Praxis von U.S.-Unternehmen und -Behörden im Blick zu behalten – letztlich wird der EuGH sein Urteil über die Angemessenheit des Datenschutzniveaus in den U.S.A. und in anderen Drittstaaten sprechen.

1.5 Beschäftigtendatenschutz

Die Arbeitswelt und somit auch der Beschäftigtendatenschutz betreffen fast jeden von uns, ob auf Seiten der Wirtschaft als Arbeitgeber oder auf der anderen Seite als Arbeitnehmer. Die jährliche Arbeitszeit beträgt im Durchschnitt 1.552 Stunden. Viel Zeit, um als Arbeitnehmer eine Flut an personenbezogenen Daten zu hinterlassen und als Arbeitgeber diese persönlichen Informationen zu sammeln.

Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person gibt es in Beschäftigungsverhältnissen in Hülle und Fülle. Beispielhaft sind Adressdaten, Geburtsdaten, Bankverbindungsdaten, Familienstand, Steuer-ID, Telefonnummern und E-Mail-Adressen zu nennen, aber auch Bewerbungen, erbrach-

te Arbeitszeiten, Krankheits- und Urlaubstage sind personenbezogene Daten.

Eine bereichsspezifische Regelung zum Beschäftigtendatenschutz wäre vor diesem Hintergrund begrüßenswert, ist aber auch in diesem Berichtszeitraum nicht erreicht worden (und wird angesichts des BDSG neu in absehbarer Zeit wohl auch nicht verwirklicht werden – (1.). Sich in der täglichen Arbeit und im Umgang mit den Praxisfällen die Grundlagen der Verarbeitung zu vergegenwärtigen, kann daher hilfreich sein (2.). Insbesondere auf den Grundsatz der Erforderlichkeit wird in der Praxis immer wieder zurückgegriffen (3.). Einschnitte und besonderen Beratungsbedarf bringen insbesondere die Digitalisierung und die damit einhergehenden gestiegenen Überwachungsmöglichkeiten durch die Arbeitgeber mit sich. Hier werden durch die Rechtsprechung des Bundesarbeitsgerichts wesentliche Impulse gegeben. Diese zeigt insgesamt Licht und Schatten – aber die Richtung für mehr informationelle Selbstbestimmung der Beschäftigten stimmt (4.). Der LfDI wird diese Entwicklung in seiner täglichen Arbeit, ob als Aufsichtsbehörde oder beratende Stelle – weiter beobachten und steht jedermann/-frau mit und Tat zur Seite (5.).

1.) Kein Gesetz zum Schutz von Beschäftigtendaten

Dennoch fehlt es nach wie vor an einem spezifischen Gesetz zum Schutz von Beschäftigtendaten. Der Beschäftigtendatenschutz ist insofern ein Abbild der bestehenden Regelungen im Arbeitsrecht. Auch dort hat es der Gesetzgeber, trotz nachdrücklicher Postulate verschiedenster Lager, nicht geschafft, ein einheitliches Arbeitsrecht zu kodifizieren. Die bestehenden datenschutzrechtlichen Regelungen finden sich weit verstreut in verschiedenen Gesetzestexten. Beispielhaft ist § 39 Abs. 8 und 9 Einkommensteuergesetz, wonach der Arbeitgeber die auf der Lohnsteuerkarte enthaltenen Merkmale nur für die Einbehaltung der Lohnsteuer verwenden darf. Für die Verwendung der Sozialversicherungsnummer durch den Arbeitgeber findet sich in § 18f im Vierten Sozialgesetzbuch eine Spezialvorschrift. Da verliert man schnell den Überblick …

Wie die vergangenen Jahre gezeigt haben, war der Weg des Gesetzgebers zu einem eigenständigen Beschäftigtendatenschutz nicht gerade kurz – und er ist eigentlich noch immer nicht am Ziel angekommen. Im Jahr 1990 erließ der Bund ein novelliertes Bundesdatenschutzgesetz (BDSG). Bis 2009 hat man sich, trotz seiner großen praktischen Bedeutung, mit einer eigenständigen Regelung für den Arbeitnehmerdatenschutz Zeit gelassen – im Gegensatz zu den Datenschutzgesetzen vieler Länder (vgl. bspw. § 36 Landesdatenschutzgesetz Baden-Württemberg). Die Praxis musste solange auf die allgemeinen Regelungen des BDSG zurückgreifen.

Forderungen nach der Schaffung eines eigenständigen Beschäftigtendatenschutzgesetzes wurden erst nach dem Bekanntwerden von Datenschutzskandalen bedeutender deutscher Unternehmen erfüllt. Beschäftigte von Lidl, der Deutschen Bahn oder der Deutschen Telekom mussten erst Opfer unzulässiger Überwachungsmethoden werden, bis die Bundesregierung im Februar 2009 die Arbeit an einem Arbeitnehmerdatenschutzgesetz wieder aufnahm. Resultat war der als „Sofortmaßnahme" am 1. September 2009 in Kraft getretene § 32 BDSG.

Das in der darauffolgenden Legislaturperiode auf der Agenda stehende ausführliche „Gesetz zur Regelung des Beschäftigtendatenschutzes" scheiterte an vehementen Protesten von Arbeitgebern und Gewerkschaften.

Derzeit sieht es so aus, als ob der deutsche Gesetzgeber erneut die Möglichkeit eigenständiger und spezifischer Regelungen verstreichen lässt und so den Besonderheiten des Arbeitsverhältnisses als Nähe- und Abhängigkeitsverhältnis nicht gerecht wird. Am 25. Mai 2018 tritt bereits die EU-Datenschutz-Grundverordnung mit ihrer unmittelbaren Bindung in Kraft. Für die Datenverarbeitung im Beschäftigungskontext hat der europäische Gesetzgeber durch eine Öffnungsklausel den Weg für eigenständige nationale Regelungen geebnet. Das Gesetz zur Anpassung des Datenschutzrechts an die Datenschutz-Grundverordnung übernimmt zwar den derzeit gültigen § 32 BDSG mit wenigen Zusätzen, stellt aber nach wie vor nur einen Minimalkonsens dar. Die seit Jahrzehnten bestehenden Forderungen nach einem eigenständigen Beschäftigtendatenschutzgesetz bleiben noch immer unerfüllt.

2.) Grundlagen der Verarbeitung von Beschäftigtendaten

Für die Verwendung von Beschäftigtendaten gilt jedoch einheitlich: Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat (vgl. § 4 Abs. 1 BDSG). Die Verwendung personenbezogener (Beschäftigten-) Daten ist also grundsätzlich verboten, wenn sie nicht ausdrücklich vom Gesetz erlaubt ist oder eingewilligt wurde.

Lässt sich die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten also nicht auf eine bereichsspezifische Vorschrift oder das BDSG stützen, bleibt als Datenverarbeitungsgrundlage nur die Einwilligung, also das vorherige Einverständnis des Betroffenen in die Verwendung seiner Daten. Aber kommt eine Einwilligung im Beschäftigungsverhältnis überhaupt in Frage? Googelt man den Begriff Arbeitnehmer, spuckt die Suchmaschine Folgendes aus:

„Person, die abhängig, nämlich bei einem Arbeitgeber, beschäftigt ist."

Die wirtschaftliche Abhängigkeit einer Person legt den Schluss nahe, sie in einer Zwangslage zu sehen, die ihr eine freie Entscheidung unmöglich macht. Diese Annahme führte bei Datenschützern lange Zeit dazu, eine Einwilligung von Beschäftigten grundsätzlich nicht als Grundlage einer Datenerhebung, -verarbeitung oder -nutzung zu akzeptieren. Zu Recht hat man diesen Extremstandpunkt mittlerweile aufgegeben und den Beschäftigten ihr Recht auf informationelle Selbstbestimmung auch in einem Arbeitsverhältnis zugesprochen. Es liegt nämlich in der Hand jedes Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen – der Arbeitnehmer bestimmt ergo selbst, ob er seinem Arbeitgeber mehr von sich preisgibt, als dieser nach den gesetzlichen Vorgaben befugt wäre zu erfahren. Die Einwilligung kann auch positive Folgen für den einzelnen Arbeitnehmer haben, sodass es mit dem Sinn und Zweck des Datenschutzes nicht vereinbar wäre, die Beschäftigten pauschal der Möglichkeit einer Einwilligung zu berauben.

Das heißt jedoch nicht, dass wir als Aufsichtsbehörde gezwungen sind, Einwilligungen von Beschäftigten ungeprüft als Ermächtigung zur Datenverarbeitung anzuerkennen. Vielmehr sind wir gehalten, die Freiwilligkeit und Wirksamkeit einer jeden Einwilligung einer genauen Einzelfallprüfung zu unterziehen. Gemäß § 4a Abs. 1 Satz 1 BDSG ist eine Einwilligung nur wirksam, wenn sie auf der freien und informierten Entscheidung des Betroffenen beruht. Daneben ist der Betroffene auf den Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalls erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen.

Durch § 32 Abs. 2 BDSG (bzw. § 26 Abs. 7 BDSGneu) weitet der Gesetzgeber den Anwendungsbereich des Beschäftigtendatenschutzes erheblich aus – jede Information über Beschäftigte ist in jeder Form geschützt. Der Geltungsbereich des BDSG umfasst ja ansonsten nur den Einsatz von Datenverarbeitungsanlagen bzw. setzt die geordnete Sammlung der Daten in Dateien voraus (§ 1 Abs. 2 Nr. 3 und § 27 Abs. 1 Satz 1 BDSG). Anders beim Beschäftigtendatenschutz: Hier fallen zum Beispiel auch handschriftlich gefertigte Notizen während eines Bewerbungsgesprächs sowie die alltägliche Informationserhebung durch persönliche Befragung oder eine Übermittlung durch Telefonate in den Anwendungsbereich von § 32 BDSG. Durch die Loslösung von einer automatisierten Verarbeitung können auch die im Arbeitsrecht entwickelten zwingenden Schutzprinzipien berücksichtigt werden – etwa beim Fragerecht des Arbeitgebers und dem damit einhergehenden „Recht zur Lüge" des Beschäftigten, wenn er einem Versuch unzulässiger Informationsbeschaffung ausgesetzt ist. Auch hier hilft ihm das BDSG.

Der Abschluss von Tarifverträgen und Betriebsvereinbarungen kann das Fehlen eines eigenständigen Beschäftigtendatenschutzgesetzes in gewissem Umfang wettmachen. Gerade deshalb sollten die Vertragsparteien Tarifverträge und Betriebsvereinbarungen als Regelungsinstrument nicht ungenutzt lassen und die Datenverarbeitungen im Unternehmen entsprechend selbst regeln.

Bedauerlicherweise laufen abgeschlossene Betriebsvereinbarungen nicht selten ins Leere. Unklare oder undurchsichtige Regelungen oder ein das BDSG unterschreitendes Schutzniveau führen mitunter dazu, dass Aufsichtsbehörden eine Betriebsvereinbarung als unwirksam betrachten und auf die allgemeine Regelung des

§ 32 BDSG zurückgreifen müssen. Eine Betriebsvereinbarung kann nur dann als „besondere Rechtsvorschrift" im Sinne von § 4 Abs. 1 BDSG angesehen werden, wenn die Datenerhebung, -verarbeitung und -nutzung hinreichend präzise innerhalb des Erlaubnisumfangs gesetzlicher Bestimmungen geregelt wird und dabei das gesetzliche Schutzniveau nicht unterschritten wird. Auch können Betriebsvereinbarungen vor Begründung des Beschäftigungsverhältnisses keinen datenschutzrechtlichen Erlaubnistatbestand bereitstellen. Der Bewerber gehört dem Betrieb noch nicht an, sodass sich die Wirkung einer Betriebsvereinbarung auch nicht auf ihn erstrecken kann.

Leider führen nicht selten die fehlende Fachkunde im Datenschutz und die Besonderheit eines Arbeitsverhältnisses zu undurchsichtigen Vereinbarungen. Hier sind betriebliche Datenschutzbeauftragte und die Aufsichtsbehörden gleichermaßen gefragt. Sie können der verantwortlichen Stelle, aber auch dem Betriebsrat beratend zur Seite stehen (vgl. § 38 Abs. 1 Satz 2 BDSG). Werden Prozesse von Anfang an unter dem Gesichtspunkt datenschutzrechtlicher Vorgaben vorangetrieben, werden Entwicklungen auch nicht ausgebremst, sondern von vornherein transparent und nachhaltig gestaltet.

3.) Der Grundsatz der Erforderlichkeit

Das informationelle Selbstbestimmungsrecht des Beschäftigten ist mit dem Eigentumsrecht (Art.14 Abs. 1 und 2 Grundgesetz – GG), mit der unternehmerischen Freiheit (Art. 12 Abs. 1 GG) und der Vertragsfreiheit des Arbeitgebers (Art. 2 Abs. 1 GG) in einen schonenden Ausgleich zu bringen. Hier stehen sich also immer Grundrechte auf beiden Seiten gegenüber. Daher misst § 32 BDSG die Verwendung personenbezogener Daten am Grundsatz der Erforderlichkeit. Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten muss geeignet und zugleich das relativ mildeste Mittel sein, um die unternehmerischen Interessen und Zwecke bei der Durchführung des Beschäftigungsverhältnisses zu verwirklichen. Dementsprechend verpflichtet das Erforderlichkeitsprinzip stets zum Vergleich alternativer Handlungsformen und zwingt den Arbeitgeber zur Datenvermeidung und Datensparsamkeit, wo immer dies möglich ist. Der Beschäftigte muss seine Daten nur dann preisgeben, wenn der Arbeitgeber ohne ihre Kenntnis im konkreten Einzelfall eine legitime Aufgabe nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann. Gleichzeitig gibt der Arbeitgeber aber durch seine unternehmerische Entscheidungsfreiheit den Zweck und die konkrete Ausgestaltung des Beschäftigungsverhältnisses vor. Entscheidet sich der Arbeitgeber etwa, besonders qualitätsvolle Produkte anzubieten, so darf er das benötigte gut ausgebildete Personal entsprechend intensiver auswählen und bei der Arbeit überprüfen. Der Maßstab der Erforderlichkeit orientiert sich also in erster Linie an der unternehmerischen Entscheidungsfreiheit, die Zwecke des Beschäftigungsverhältnisses zu bestimmen.

Alles was zur Ausübung von Weisungsrechten eines Arbeitgebers oder einer Kontrolle der Leistung oder des Verhaltens seiner Beschäftigten notwendig ist und nach den Grundsätzen des Arbeitsrechts erlaubt ist, muss aus datenschutzrechtlicher Sicht als erforderlich eingestuft werden. Das heißt aber nicht, dass der Arbeitgeber seine Mitarbeiter einer Totalkontrolle unterziehen darf und sie einem ständigen Überwachungsdruck ausgesetzt sein dürfen – hiervor schützt sie ihr Recht auf informationelle Selbstbestimmung.

Der Erforderlichkeitsgrundsatz alleine soll es aber nicht gewesen sein. Der Arbeitgeber ist daneben an weitere Prinzipien des Datenschutzes gebunden. Hierzu zählt der Grundsatz der Direkterhebung (wenn der Arbeitgeber Informationen über einen bestimmten Beschäftigten haben möchte, dann muss er ihn zunächst einmal selbst befragen und darf sich nicht an Dritte wenden, vgl. § 4 Abs. 2 Satz 1 BDSG), das Gebot der Datensparsamkeit (§ 3a BDSG) und das Verbot der Vorratsdatensammlung. Besondere Bedeutung genießt der Zweckbindungsgrundsatz: Nur wenn vor der Datenerhebung, -verarbeitung und -nutzung feststeht, welcher Zweck des Arbeitgebers erreicht werden soll, lässt sich im Nachhinein beurteilen, ob in zulässiger Weise verfahren wurde. Unsere tägliche Arbeit zeigt, dass vielen Unternehmen diese Grundsätze im schlechtesten Fall völlig fremd sind oder eher als Empfehlung denn als verbindliche Vorgabe verstanden werden – ein leider weit verbreiteter Irrtum.

4.) Der Einfluss der Digitalisierung auf die Rechtsprechung des Bundesarbeitsgerichts

Der digitale Wandel bringt nicht nur Fortschritte, sondern führt auch zur Steigerung der Mög-

lichkeit von Arbeitgebern, ihre eigenen Mitarbeiter zu überwachen. Setzen sich Beschäftigte zur Wehr und suchen Rechtsschutz vor den Gerichten, enden nicht wenige vor dem Bundesarbeitsgericht. Ob und in welchem Umfang die höchstrichterliche Rechtsprechung Arbeitgebern Grenzen aufzeigt, beleuchtet der folgende Beitrag.

Wie der LfDI an den täglich eingehenden Beschwerden im Bereich des Beschäftigtendatenschutzes unschwer erkennen kann, ist die Überwachung von Arbeitnehmern durch den digitalen Wandel für viele Arbeitgeber ein Leichtes. Durch leicht zugängliche Soft- und Hardware sind viele Arbeitgeber von einer intuitiven zu einer algorithmischen Überwachung ihrer Beschäftigten übergegangen. Dass die vom Gesetz gezogenen Grenzen einer zulässigen Überwachung hierbei oft überschritten werden und Beschäftigte in ihrem Recht auf informationelle Selbstbestimmung verletzt werden, liegt auf der Hand. Zwar finden sich eine Reihe gesetzlicher Regelungen im Bereich des Beschäftigtendatenschutzes in einer Vielzahl von Spezialgesetzen verstreut, dennoch ist der Bereich immer noch unterreguliert. Nach wie vor fehlt es an einem dringend notwendig eigenständigen Beschäftigtendatenschutzgesetz. Da ist es selbstverständlich, dass das Bundesarbeitsgericht (BAG), in einer wachsenden Anzahl von Entscheidungen mit der Materie konfrontiert ist und in Konsequenz dazu die Frage der Zulässigkeit neuer Überwachungsmethoden beantworten muss – wobei eine insgesamt positive Entwicklung und damit eine Stärkung des Rechts auf informationelle Selbstbestimmung von Beschäftigten zu verzeichnen ist.

a) Soziale Medien und die Arbeitswelt

Schlagworte wie Arbeitswelt 4.0 und Big Data lassen erahnen, dass es das klassische Arbeitsverhältnis fast nicht mehr gibt. Das führt auch beim BAG zur Änderung seiner Rechtsprechungsthemen. Facebook, Google+ und Twitter werden längst nicht mehr nur von Privaten genutzt. Die Vorteile globaler Vernetzung, permanenter Erreichbarkeit und Präsenz möchten sich die meisten Unternehmen nicht entgehen lassen. Eine seriöse Facebook-Seite pflegt bestehende Geschäftskontakte und ermöglicht das Knüpfen neuer, das kann zur Gewinnsteigerung des Unternehmens beitragen.

Trotz dieser Vorteile dürfen Arbeitgeber die Risiken und mögliche Gefahren sozialer Medien nicht aus den Augen verlieren. Hierzu stellte das BAG kürzlich fest, dass der Betriebsrat in bestimmten Fällen auch ein Wort mitzureden hat (sog. Facebook-Beschluss; BAG, Beschluss vom 13.12.2016, 1 ABR 7/15).

Die Konzernmutter eines lokalen Blutspendedienstes betrieb eine Facebook-Seite, bei der die Aktivitäten aller angehörigen Unternehmen dargestellt wurden. Ein Facebook-Nutzer konnte über die Funktion „Besucher-Beiträge" einen Post zu einer seiner Meinung nach nicht ordnungsgemäßen Behandlung durch einen Mitarbeiter hinterlassen. Der Beitrag war für alle Besucher der Facebook-Seite sichtbar. Der Konzernbetriebsrat berief sich insoweit auf sein Mitbestimmungsrechts nach § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz und forderte den Arbeitgeber auf, die Facebook-Seite abzuschalten bzw. zumindest die Funktion „Besucher-Beiträge" zu deaktivieren.

Das BAG entschied, dass die Bereitstellung der Funktion „Besucher-Beiträge" der Mitbestimmung des Betriebsrats unterliege. Eine vom Arbeitgeber betriebene Facebook-Seite, die es den Nutzern von Facebook ermöglicht, über die Funktion „Besucher-Beiträge" Postings zum Verhalten und zur Leistung von Arbeitnehmern einzustellen, sei eine technische Einrichtung, die zur Überwachung der Arbeitnehmer i.S.d. § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz bestimmt sei. Ausdrücklich nicht entschieden wurde über das Bereitstellen einer offenen Kommentarfunktion.

Die Aussage des BAG muss für alle Fälle, bei denen Dritte sich auf Plattformen sozialer Medien gegenüber einer breiten Öffentlichkeit zum Verhalten oder zur Leistung einzelner Beschäftigter äußern und damit personenbezogene Daten der Beschäftigten verarbeiten können, Beachtung finden. Soziale Medien weisen im Unterschied zu herkömmlichen Kommunikationswegen eine besondere Qualität auf, sie machen Vorgänge weltweit zugänglich und sind häufig wertender Natur.

Aus datenschutzrechtlicher Sicht liegt die Verantwortung dabei zunächst bei dem Nutzer, der die entsprechenden Daten auf der jeweiligen Seite öffentlich einstellt. Inwieweit auch den Arbeitgeber eine datenschutzrechtliche Mitverantwortung trifft, ist dagegen noch nicht geklärt. Für öffentliche Stellen wird dies vom LfDI auch angesichts der Schlussanträge des Generalanwalts des EuGH im Verfahren C-210/16,

bei dem es u.a. um die datenschutzrechtliche Verantwortung bei Facebook-Fanpages geht, angenommen.
Mit seiner Entscheidung geht das BAG insoweit einen Schritt in die richtige Richtung in Sachen Beschäftigtendatenschutz.

b) Spähsoftware und Videoüberwachung: Beweisverwertungsverbot?

Im Beschäftigtendatenschutz wurde ein weiterer Meilenstein gelegt. Das BAG entschied: Mit personenbezogenen Daten aus illegaler Spähsoftware lässt sich kein Kündigungsgrund beweisen (BAG, Urteil vom 27. Juli 2017, 2 AZR 684/16).

Eine Arbeitgeberin beschloss, das gesamte Surfverhalten ihrer Beschäftigten vollständig zu überwachen und informierte die Mitarbeiter entsprechend. Auf dem Dienst-PC des Klägers wurde deswegen ein Tool (sog. Keylogger) installiert, das sämtliche Tastureingaben protokollierte und regelmäßig Bildschirmfotos (Screenshots) fertigte. Nach Auswertung der mit Hilfe des Keyloggers erstellten Dateien konnte dem Kläger nachgewiesen werden, den Dienst-PC zur Erledigung privater Angelegenheiten genutzt zu haben, weswegen er fristlos gekündigt wurde.

Der Arbeitnehmer hielt die Kündigung für rechtswidrig und das BAG gab ihm Recht. Nach Auffassung der Erfurter Richter ist der Einsatz eines Keyloggers rechtswidrig, wenn kein auf den Arbeitnehmer bezogener, durch konkrete Tatsachen begründeter Verdacht einer Straftat oder einer anderen schwerwiegenden Pflichtverletzung besteht.

Das BAG geht zu Recht von einem Beweisverwertungsverbot für die durch den Keylogger gewonnenen Erkenntnisse über die Privattätigkeit des Klägers aus. Denn die Arbeitgeberin hat das Recht auf informationelle Selbstbestimmung des Arbeitnehmers in erheblicher Weise verletzt. Die Bedingung der Datenerhebung nach § 32 Abs. 1 Satz 2 Bundesdatenschutzgesetz, nämlich ein zu dokumentierender, auf tatsächlichen Anhaltspunkten beruhender Verdacht einer im Beschäftigungsverhältnis begangenen Straftat durch einen Beschäftigten, lagen offensichtlich nicht vor. Die von der Arbeitgeberin „ins Blaue hinein" veranlasste Maßnahme war daher rechtswidrig und durfte deswegen auch nicht gerichtlich verwertet werden.

Auch wenn es im Arbeitsrecht an Vorschriften zur prozessualen Verwertbarkeit rechtswidrig erlangter Beweise mangelt, ist die Erhebung von Beweismitteln, deren Erlangung gegen das Bundesdatenschutzgesetz verstoßen, ein wichtiges Indiz dafür, dass die Verwertung des Beweismittels durch das Gericht ein nicht zu rechtfertigender Eingriff in das Grundrecht auf informationelle Selbstbestimmung sein kann. Bei der Annahme von Beweisverwertungsverboten bleibt zu hoffen, dass das BAG auch in Zukunft an seiner Linie festhält – hier gibt es nämlich durchaus eine positive Entwicklung zu verzeichnen. In einer früheren Entscheidung hatte das BAG das Vorliegen eines Beweisverwertungsverbots noch verneint und sich dazu über die Grenzen des § 32 Abs. 1 Satz 2 Bundesdatenschutzgesetz hinweggesetzt (BAG, Urteil vom 22. September 2016, 2 AZR 848/15).

Eine Arbeitgeberin, die Inventurverluste feststellte, die nur von der eigenen Belegschaft stammen konnten, installierte eine verdeckte Videokamera. Der gegen zwei bestimmte Mitarbeiterinnen gerichtete Verdacht eines Diebstahls wurde durch die Videoaufzeichnung bestätigt und brachte einen sogenannten Zufallsfund zu Tage: Die Videosequenz zeigte, wie die Klägerin einen regulären Kassiervorgang manipulierte und der Kasse Geld entnahm. Folge war die fristlose Kündigung des Arbeitsverhältnisses.

Die Kündigungsschutzklage der Klägerin hatte damals vor dem BAG keinen Erfolg. Laut BAG durften die Vorinstanzen Zeugen zum Inhalt der (inzwischen gelöschten) Videosequenz vernehmen und das Beweisergebnis verwerten. Da gegen zwei konkrete Mitarbeiterinnen der Verdacht einer Straftat bestand, sei die Videoaufzeichnung ihnen gegenüber nach § 32 Abs. 1 Satz 2 Bundesdatenschutzgesetz zulässig gewesen. Die Maßnahme sei im Verhältnis zu den von der Videoaufzeichnung betroffenen weiteren Arbeitnehmern – hier der Klägerin – auch nach § 6b Abs. 1 Nr. 3 Bundesdatenschutzgesetz rechtmäßig. Die weitere Verarbeitung und Nutzung der Videoaufzeichnung an sich sei dann wiederum für die Beendigung des Beschäftigungsverhältnisses mit der Klägerin erforderlich und somit nach § 32 Abs. 1 Satz 1 Bundesdatenschutzgesetz zulässig.

Dabei beging das BAG jedoch einen entscheidenden Fehler, ließ es doch die gesetzlichen Vorgaben aus § 32 Abs. 1 Bundesdatenschutzgesetz außer Acht. Die Ansicht, dass eine ver-

deckte Videoüberwachung zur Aufdeckung von Straftaten von Beschäftigten nicht nur dann erfolgen darf, wenn sichergestellt sei, dass von ihr ausschließlich Arbeitnehmer betroffen sind, gegen die ein dokumentierter Verdacht einer während des Beschäftigungsverhältnisses begangenen Straftat besteht, widerspricht dem eindeutigen Wortlaut von § 32 Abs. 1 Satz 2 Bundesdatenschutzgesetz: „eines" Beschäftigten, „der" Betroffene. Sieht das BAG das anders, hätte es die Entscheidung dem Bundesverfassungsgericht vorlegen müssen (vgl. Art. 100 Abs. 1 Grundgesetz).

Das Gericht hätte klären müssen, ob der Zufallsfund zu Lasten der Klägerin überhaupt entstanden wäre, wenn die Videoüberwachung zielgerichtet und verhältnismäßig auf die des Diebstahls verdächtigten Mitarbeiterinnen ausgerichtet worden wäre. Wäre das BAG von einer unzulässigen Datenerhebung ausgegangen, hätte es angesichts seiner jüngsten Entscheidung zur unzulässigen Erhebung personenbezogene Daten (BAG, Urteil vom 27. Juli 2017, 2 AZR 684/16) mithilfe illegaler Spähsoftware ein Beweisverwertungsverbot annehmen müssen. Man sieht: auch Bundesgerichte können dazulernen!

c) Kündigung für Datenerhebungsverweigerer

Mit einer weiteren Entscheidung stellt das BAG die Interessen eines Nahverkehrsunternehmens (leider) ohne überzeugende Begründung über die des Arbeitnehmers (BAG, Urteil vom 17.11.2016, 2 AZR 730/15).

Ein Busunternehmen setzte ein System ein, mit dessen Hilfe „Fahrereignisse" elektronisch ausgewertet werden können. Die abgeschlossene Betriebsvereinbarung sah die verpflichtende Teilnahme an dieser Maßnahme vor. Fährt der Busfahrer zu hochtourig, überschreitet Leerlaufzeiten, bremst zu scharf oder fährt zu schnell, weist ihn eine Warnleuchte des Systems darauf hin. Alle Daten hierzu werden aufgezeichnet und gespeichert. Die Arbeitnehmer konnten zwischen einer personalisierten und bei „guter Führung" prämienbewährten und einer „anonymisierten" Variante wählen. Der Kläger weigerte sich am System teilzunehmen, wofür er nach Ausspruch dreier Abmahnungen die fristlose Kündigung kassierte.

Das BAG bestätigte die Kündigung. Unabhängig von der Wirksamkeit der Betriebsvereinbarung sei das System nach § 32 Abs. 1 Satz 1 Bundesdatenschutzgesetz zulässig. Nach Auffassung des Gerichts handle es sich bei den erhobenen und verarbeiteten Daten zwar um personenbezogene Daten, weil die Anonymisierung ohne besonderen Aufwand aufgehoben werden könne. Die Datenerhebung und Verarbeitung sei jedoch für die Durchführung des Arbeitsverhältnisses erforderlich. Dies trifft allerdings offensichtlich nicht zu, da der Zweck des Systems, die Busfahrer zu einer vorausschauenden und sparsamen Fahrweise anzuhalten, auch durch gleich geeignete mildere Mittel hätte erreicht werden können. Schulungen oder begleiteten Kontrollfahrten wären zur Zweckerreichung ausreichend gewesen.

Im Übrigen ist es eine recht gruselige Vorstellung, dass Gerichte es für denkbar halten, der Arbeitgeber könnte mal eben „Modernisierungsverweigerer" aussortieren – eine wirklich problematische Entscheidung des BAG.

d) Der Irrweg des Betrieblichen Eingliederungsmanagement

Die Rechtsprechung zum Betrieblichen Eingliederungsmanagement (BEM) ist leider teilweise wechselhaft und sorgt somit für Diskussionen in der Praxis. 2012 entschied das BAG noch, dass es erforderlich sei, dem Betriebsrat eine Namensliste aller Arbeitnehmer zu überlassen, denen ein BEM anzubieten ist (BAG, Beschluss vom 7.2.2012, 1 ABR 46/10). Mit einer anonymisierten Unterrichtung ließen sich die aus § 84 Abs. 2 Satz 1 Neuntes Sozialgesetzbuch ergebenden Pflichten des Arbeitgebers nicht überwachen. Auf die Einwilligung des Betroffenen komme es nicht an.

Mit seiner neusten Entscheidung zur Mitbestimmung des Betriebsrats in Fragen des BEM hat das BAG von seiner früheren Rechtsprechung Abstand genommen und die Rechte des Betriebsrats geschmälert (BAG, Beschluss vom 22.3.2016, 1 ABR 14/14). Das BAG legt dem Wortlaut des § 84 Abs. 2 Satz 1 Neuntes Sozialgesetzbuch: „[…] klärt der Arbeitgeber mit der zuständigen Interessenvertretung […]" ein anderes Verständnis als in dem zuvor genannten Beschluss aus dem Jahr 2012 zu Grunde. Nun hält es die Hinzuziehung des Betriebsrats nur mit dem Einverständnis des Arbeitnehmers für zulässig. Dem ist zuzustimmen: Das Recht auf informationelle Selbstbestimmung der Betroffenen steht nur diesen selbst zu und wird

durch den Betriebsrat zwar unterstützt, aber nicht stellvertretend wahrgenommen.

5.) Die Welt des Beschäftigtendatenschutzes aus Sicht des LfDI BW

In der Regel wird der LfDI BW durch Beschwerden von Betroffenen auf unzureichenden Regelungen in Betriebsvereinbarungen aufmerksam. Praxisfälle aus der täglichen Arbeit der Aufsichtsbehörden bringen die bestehenden Defizite im Bereich des Datenschutzes ans Licht. Gerade der Bereich des Beschäftigtendatenschutzes stellt sich hier als besonders spannende Rechtsmaterie dar. Oft handelt es sich um brisante Fälle, bei deren Meldung der betroffene Arbeitnehmer Konsequenzen für sein Arbeitsverhältnis befürchtet. Vermutlich finden sich in keinem anderen Bereich des Datenschutzes so zahlreiche anonyme Beschwerden oder der Wunsch der Betroffenen, gegenüber dem Arbeitgeber unerkannt zu bleiben. Auf der anderen Seite birgt das Arbeitsverhältnis als höchstpersönliches Näheverhältnis die latente Gefahr, doch als derjenige ausfindig gemacht zu werden, der bei der Aufsichtsbehörde eine Beschwerde eingereicht hat. Bei Unternehmen mit wenigen Beschäftigten erklärt sich dies von selbst; bei Beschwerden, bei denen der Betroffenenkreis von vornherein durch den dargestellten Sachverhalt begrenzt wird, könnten Nachforschungen Rückschlüsse auf die Person des Beschwerdeführers zulassen.

Dem Wunsch der Betroffenen, ihre Beschwerde nicht gegenüber dem Arbeitgeber zu offenbaren, kommen wir als Aufsichtsbehörde selbstverständlich gerne nach. Wir sind rechtlich in der Lage, Nachfragen des Arbeitgebers zur Identität eines Beschwerdeführers zurückzuweisen. Zugleich sprechen wir aber mit dem Beschwerdeführer über die Möglichkeit des Arbeitgebers, Rückschlüsse auf seine Identität auch bei einer anonymen Vorgehensweise zu ziehen.

Die Arbeit des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg ist spannend und vielfältig. Auch wenn der Gesetzgeber uns vorrangig die Rolle einer Aufsichtsbehörde zugesprochen hat, richten wir unser besonderes Augenmerk auf die datenschutzrechtliche Beratung. Durch frühzeitige Einbindung unserer Behörde werden neue wirtschaftliche Entwicklungen im Betrieb nicht durch datenschutzrechtliche Anforderungen gehemmt, sondern langfristig und nachhaltig verbessert.

Der LfDI hat auf diesen neuen Schwerpunkt mit einer Handreichung (https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2017/07/Arbeitnehmerdatenschutz-Handreichung.pdf) reagiert, sie gibt einen Überblick über die Probleme des Beschäftigtendatenschutzes im privaten Bereich – und zwar so, wie sie an den Landesbeauftragten herangetragen werden. Der Ratgeber zeigt die zulässige Verwendung personenbezogener Daten von Beschäftigten anhand von Praxisfällen auf: echte Beratungsanfragen und eingehende Beschwerden – und echte Lösungen. Dieses neue Format in der Beratungspraxis des LfDI erfreut sich großer Beliebtheit – und wird auch 2018 fortgesetzt werden.

1.6 Neue Entwicklungen beim Datenschutz rund um das Kfz

„Das Auto als Datenkrake" und „das Auto als rollender PC" sind Schlagworte, die in den Medien breit und gegensätzlich diskutiert wurden. Das vernetzte Automobil soll Realität werden: Bereits ab 2030 werden laut der Automobilindustrie Autos alleine fahren können.

Schon in meinem letzten Tätigkeitsbericht (32. Tätigkeitsbericht 2014/2015, LT-Drs. 15/7990, S. 93ff.) habe ich auf die technischen und rechtlichen Entwicklungen bei Kraftfahrzeugen hingewiesen. Der Trend zum vernetzten und automatisierten Fahren birgt Risiken für das Recht auf informationelle Selbstbestimmung.
Im Dialog der Datenschutzbehörden von Bund und Ländern mit dem Verband der Automobilindustrie (VDA) wurde im Januar 2016 eine „Gemeinsame Erklärung" (siehe Anlage „Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA)") veröffentlicht. Diese Erklärung gibt Orientierung bei datenschutzrechtlichen Fragestellungen zu vernetzten und nicht vernetzten Fahrzeugen.

Danach können auch technische Daten, die im Fahrzeug anfallen, personenbezogene Daten sein. Dies ist etwa dann der Fall, wenn diese technischen Daten mit der Fahrzeugidentifikationsnummer oder dem Kfz-Kennzeichen verknüpft sind. Folge davon ist, dass das Bundesdatenschutzgesetz anwendbar ist.

Ein weiterer Punkt der gemeinsamen Erklärung klärt, wer die verantwortliche Stelle für

die Datenverarbeitung ist. Diese Bestimmung der verantwortlichen Stelle ist entscheidend, damit die Betroffenen wissen, bei wem sie ihre Rechte geltend machen können. Zwei Anwendungsfelder sind zu unterscheiden: Erfolgt die Speicherung der Daten im Fahrzeug („offline"), so findet (ohne im Vorhinein festgelegte Zugriffsrechte) grundsätzlich noch keine Datenerhebung durch den Automobilhersteller statt. Werden die Daten z.B. durch eine Werkstatt ausgelesen, ist diese verantwortliche Stelle i.S.d. Datenschutzrechts. Erfolgt die Übermittlung allerdings aus dem Fahrzeug heraus („online"), werden die Daten durch die Stelle erhoben, an welche die Daten übermittelt werden. Regelmäßig wird dies der Automobilhersteller sein. Der Automobilhersteller hat dann auch die Pflicht, über die durch ihn erhobenen und gespeicherten personenbezogenen Daten nach § 34 des Bundesdatenschutzgesetzes Auskunft zu erteilen. Ein allgemeines, umfassendes Auskunftsrecht gegenüber dem Automobilhersteller besteht allerdings nicht schon aufgrund dessen Gesamtverantwortung für die Gestaltung der datenspeichernden Systeme.

Damit die Datenerhebung und -verarbeitung zulässig ist, wird ggf. eine Einwilligung benötigt. In dieser muss der Hersteller die Nutzer verständlich über Datenflüsse und Funktionen des Fahrzeugs informieren. Auch wenn die Datenerhebung und -verarbeitung auf einer gesetzlichen Grundlage beruhen kann, muss der Nutzer transparent darüber informiert sein. Hier ist vor allem die Automobilindustrie gefordert, die diese Informationen auch in der Borddokumentation bereitstellt.

Um die Datenhoheit der einzelnen Nutzer sicherzustellen, streben die Automobilhersteller an, durch standardisierte Symbole im Cockpit den aktuellen Vernetzungsstatus des Fahrzeugs anzuzeigen. Gleichzeitig soll möglich sein, dass dieser Status jederzeit aktiviert bzw. deaktiviert werden kann. Jedenfalls diejenigen Daten, die der Nutzer selbst eingibt (bspw. Navigationsdaten, Sitzeinstellungen, Radiosender oder telefonische Kontaktdaten), muss er auch selbst jederzeit ändern oder zurückstellen können. Einschränkungen der Löschbarkeit bestehen bei rechtlichen Verpflichtungen oder dann, wenn entsprechende Daten im Zusammenhang mit Garantie- sowie Gewährleistungen oder der Produkthaftung von Bedeutung sind oder deren Verfügbarkeit für den sicheren Fahrzeugbetrieb erforderlich ist.

Von besonderer praktischer Bedeutung ist ein inzwischen mit dem VDA abgestimmter **Mustertext für eine allgemeine Herstellerinformation über die Verarbeitung personenbezogener Daten in Fahrzeugen**. Mit der nunmehr vorliegenden Fassung des Mustertextes werden die Kfz-Nutzer zunächst in allgemeiner Form über die Verarbeitung personenbezogener Daten im Fahrzeug aufgeklärt und sensibilisiert.
So erfolgt ein Hinweis darauf, dass in dem Fahrzeug elektronische Steuergeräte verbaut sind, welche Daten verarbeiten, die sie zum Beispiel von Fahrzeug-Sensoren empfangen, selbst generieren oder untereinander austauschen. Wichtig ist dabei auch die Unterscheidung, dass einige Steuergeräte für das sichere Funktionieren ihres Fahrzeugs erforderlich sind, weitere beim Fahren unterstützen (Fahrerassistenzsysteme) und wiederum andere Komfort- oder Infotainment-Funktionen ermöglichen.

Von zentraler Bedeutung für den Datenschutz ist die Frage des Personenbezugs dieser Daten. Da jedes Fahrzeug mit einer eindeutigen Fahrgestellnummer gekennzeichnet ist und diese Fahrzeugidentifizierungsnummer in Deutschland über eine Auskunft beim Kraftfahrtbundesamt auf den gegenwärtigen und ehemalige Halter des Fahrzeugs rückführbar ist, bestehen daran inzwischen keine Zweifel mehr. Daneben gibt es natürlich auch weitere Möglichkeiten, aus dem Fahrzeug erhobene Daten auf den Halter oder Fahrer zurückzuführen, z.B. über das Kfz-Kennzeichen. Die von Steuergeräten generierten oder verarbeiteten Daten können daher personenbezogen sein oder unter bestimmten Voraussetzungen personenbezogen werden. Je nachdem, welche Fahrzeugdaten vorliegen, sind gegebenenfalls Rückschlüsse z.B. auf das Fahrverhalten, den Standort oder die Fahrtroute bzw. auf das Nutzungsverhalten bestimmter Personen möglich.

Teil des Mustertextes werden auch Hinweise auf die Rechte der Betroffenen im Hinblick auf den Datenschutz sein. Danach steht jedermann ein unentgeltlicher und umfassender Auskunftsanspruch gegenüber dem Hersteller sowie Dritten (z.B. beauftragte Pannendienste oder Werkstätten, Anbieter von Online-Diensten im Fahrzeug) zu, sofern diese personenbezogene Daten gespeichert haben. Dabei dürfen Auskünfte darüber verlangt werden, welche Daten zur Person zu welchem Zweck gespeichert sind und woher die Daten stammen. Weitere Informationen zu den gesetzlichen Rech-

ten gegenüber dem Hersteller (beispielweise das Recht auf Löschung oder Berichtigung von Daten) finden sich im Mustertext ebenso wie in den jeweils anwendbaren Datenschutzhinweisen auf der Web-Site des Herstellers (inklusive Kontaktdaten des Herstellers und seines Datenschutzbeauftragten).
Wichtig ist auch die **Aufklärung über die konkret erhobenen und verarbeiteten Betriebsdaten im Fahrzeug**.
Dazu gehören zum Beispiel:

- Fahrzeugstatus-Informationen (z.B. Geschwindigkeit, Bewegungsverzögerung, Querbeschleunigung, Radumdrehungszahl, Anzeige geschlossener Sicherheitsgurte),
- Umgebungszustände (z.B. Temperatur, Regensensor, Abstandssensor).

In der Regel sind diese Daten flüchtig und werden nicht über die Betriebszeit hinaus gespeichert und nur im Fahrzeug selbst verarbeitet. Steuergeräte enthalten häufig Datenspeicher (unter anderem auch der Fahrzeugschlüssel). Diese werden eingesetzt, um Informationen über Fahrzeugzustand, Bauteilbeanspruchung, Wartungsbedarfe sowie technische Ereignisse und Fehler temporär oder dauerhaft dokumentieren zu können.

Gespeichert werden je nach technischer Ausstattung:

- Betriebszustände von Systemkomponenten (z.B. Füllstände, Reifendruck, Batteriestatus),
- Störungen und Defekte in wichtigen Systemkomponenten (z.B. Licht, Bremsen),
- Reaktionen der Systeme in speziellen Fahrsituationen (z.B. Auslösen eines Airbags, Einsetzen der Stabilitätsregelungssysteme),
- Informationen zu fahrzeugschädigenden Ereignissen,
- bei Elektrofahrzeugen Ladezustand der Hochvoltbatterie, geschätzte Reichweite.

Angaben im Mustertext zu Komfort- und Infotainment-Funktionen wie Einstellungen der Sitz- und Lenkradpositionen, Fahrwerks- und Klimatisierungseinstellungen, Multimediadaten, wie Musik, Filme oder Fotos zur Wiedergabe in einem integrierten Multimediasystem oder Adressbuchdaten zur Nutzung in Verbindung mit einer integrierten Freisprecheinrichtung oder einem integrierten Navigationssystem, eingegebene Navigationsziele oder Daten über die Inanspruchnahme von Internetdiensten runden die Informationslage ab. Der im Jahr 2017 fertiggestellte Mustertext wird in Kürze auch bei den Aufsichtsbehörden abrufbar sein.

Diese grundsätzlichen Auskünfte sind von den Herstellern zwingend durch konkrete Informationen über die verarbeiteten Daten, die Verarbeitungszwecke sowie über die Übermittlung von Daten an Dritte zu ergänzen, um eine ausreichende Transparenz für die Kfz-Nutzer herzustellen.

Der Dialog mit der Automobilindustrie wird weiter fortgesetzt. Ich werde mich dafür einsetzen, dass die Hoheit über die Fahrzeugdaten beim Fahrzeughalter verbleibt und die Automobilindustrie für die erforderliche Transparenz sorgt.

1.7 Digitalisierung im Gesundheitswesen

Die vielfältigen Möglichkeiten der modernen IT-Technologie prägen bereits seit einiger Zeit auch das Gesundheitswesen. Eine populäre und von einigen als Lifestyle-Phänomen bezeichnete Nutzungsmöglichkeit bieten die sog. Wearables (am Körper getragene Kleincomputer, etwa in der Gestalt von Fitnessarmbändern) und Gesundheits-Apps (auf mobilen Endgeräten installierte Anwendungsprogramme), die Daten über den körperlichen Zustand ihrer Anwender speichern und in der Regel über das Internet an Hersteller, Internetanbieter und sonstige Dritte weiterleiten. So erfreulich es ist, wenn Nutzer mit geschärftem Bewusstsein damit quasi ihre Gesundheit selbst in die Hand nehmen, zeigen solche Anwendungen aus datenschutzrechtlicher Sicht auch Schattenseiten. Die uns bekannten Technologien bergen u.a. das Risiko, dass

- die damit aufgezeichneten sensiblen und intimen Gesundheitsdaten an andere Personen oder Stellen weitergegeben werden, ohne dass die betroffenen Personen hiervon wissen oder dazu eine bewusste Entscheidung treffen,
- Unbefugte aufgrund erheblicher Sicherheitsdefizite bestimmter Angebote Zugriff auf diese Daten erhalten und
- Nutzer, etwa aufgrund massiver gesellschaftlicher, sozialer oder ökonomischer Zwänge, nicht frei über die Nutzung derartiger Technologien entscheiden können,

beispielsweise gegenüber Krankenversicherern, die verhaltens- und trackingbasierte Tarife anbieten.

Daher hat die 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder im April 2016 die Entschließung „Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen!", gefasst, die in diesem Tätigkeitsbericht als Anhang abgedruckt und im Internet unter https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2016/04/Entschliessung_Wearables.pdf abrufbar ist.
Zu den vielfältigen weiteren Möglichkeiten, die heute unter dem Begriff „E-Health" zusammengefasst werden, gehören u.a.

- Verfahren der sog. Telemedizin und Telediagnostik, z.B. in Gestalt von Videosprechstunden, in denen Patienten mit ihrem Arzt „in Echtzeit" mittels Bild- und Tonübertragung kommunizieren und so den unter Umständen nicht unerheblichen Aufwand vermeiden, der mit einem Besuch in einer Arztpraxis verbunden sein kann;
- die elektronische Vernetzung von Patienten, Ärzten, Krankenhäusern, Apotheken, Pflegeeinrichtungen und weiteren Akteuren im Rahmen einer digitalen Infrastruktur, die eine, im Verhältnis zur traditionellen Verfahrensweise unter Verwendung von papiergebundenen Arztbriefen, Entlassungsberichten u. Ä., schnellere Kommunikation ermöglicht und den Beteiligten den Zugriff auf die jeweils benötigten Daten eines einmal angelegten Datensatzes über einen bestimmten Patienten erlaubt;
- eine elektronische Gesundheitskarte, die von Patienten im Rahmen einer sog. Telematikinfrastruktur u.a. als Nachweis gegenüber Ärzten zur Berechtigung der Inanspruchnahme von Leistungen der vertrags(zahn)ärztlichen Versorgung nach dem Fünften Buch des Sozialgesetzbuches – Gesetzliche Krankenversicherung – genutzt werden kann;
- alltagsunterstützende Assistenzsysteme (auch bezeichnet als Ambient Assisted Living – AAL), die, beispielsweise durch Raumüberwachung mittels Sensoren und automatische Steuerung bestimmter Funktionen (etwa Heizung, Beleuchtung, Rollläden), eine solche technische Unterstützung im Haushalt bieten, dass kranke und pflegebedürftige Personen bei Bedarf trotz gesundheitlicher Einschränkungen weiterhin selbstbestimmt „in den eigenen vier Wänden" wohnen können, ohne auf die Versorgung und Betreuung in einem Pflegeheim angewiesen zu sein;
- den Einsatz leistungsfähiger Rechner beim Umgang mit DNA-Daten im Zusammenhang mit der sog. personalisierten Medizin.
- Diese Beispiele machen deutlich, dass die weitreichenden technischen Möglichkeiten und Chancen der Digitalisierung mit einer Vielzahl schwieriger Fragen verbunden sind. Beispielhaft seien nur die folgenden genannt:
- Darf, etwa aus ethischen Gründen, alles, was technisch machbar ist, auch in die Tat umgesetzt werden?
- Ist es mit der Vorstellung von einer medizinisch einwandfreien und individuellen Betreuung von Patienten vereinbar, wenn der unmittelbare persönliche Kontakt zwischen Patient und Arzt im Rahmen der Telemedizin und Telediagnostik gelockert oder ganz gelöst wird?
- Wer bezahlt für den Aufwand, der mit der Anschaffung, dem Betrieb und der Wartung technischer Einrichtungen, etwa in Arztpraxen, verbunden ist?
- Für welche derartigen Leistungen besteht am Markt für Gesundheits- und Pflegedienstleistungen aktuell welche Nachfrage, ggf. von wem und zu welchen Bedingungen?
- Ist es sinnvoll oder angezeigt, wenn der Bund, das Land und andere Körperschaften des öffentlichen Rechts versuchen, den Markt zu beeinflussen, beispielsweise durch die finanzielle Förderung bestimmter Projekte?
- Werden kranke Menschen, die von der Möglichkeit der freiwilligen Teilnahme an einem Telemedizin-Projekt keinen Gebrauch machen wollen, medizinisch auf traditionelle Weise weiterhin so betreut, wie sie es erwarten dürfen?
- Lassen sich die, etwa aus medizinischer, ethischer, wirtschaftlicher und politischer Sicht als wünschenswert erkannten, Ziele auf der Grundlage des geltenden Rechts umsetzen? Wie werden sich die ab Mai 2018 geltenden Vorschriften der EU-Datenschutz-Grundverordnung insofern auswirken?

Der Bundesgesetzgeber hat sich, nachdem die Einführung einer einheitlichen elektronischen Gesundheitskarte in der gesetzlichen Krankenversicherung über Jahre hinweg nur schleppend

vorangekommen war, 2015 mit dem Erlass des Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen sowie zur Änderung weiterer Gesetze (vielfach kurz als E-Health-Gesetz bezeichnet) klar positioniert: Durch entsprechende Änderungen des Fünftes Buches des Sozialgesetzbuches wurde ein Fahrplan zur Einführung einer bundesweiten Telematik-Infrastruktur und bestimmter Anwendungen der elektronischen Gesundheitskarte aufgestellt. Es bleibt u.a. abzuwarten, ob das Ziel erreicht wird, bis Ende 2018 die Voraussetzungen für eine elektronische Patientenakte zu schaffen. Da der mit dem E-Health-Gesetz vorgegebene große Rahmen noch unausgefüllt ist, haben Krankenkassen, Ärzteverbände und andere Organisationen eigenständig begonnen, quasi als Parallelstrukturen, eigene, teilweise örtlich begrenzte, digitale Netze und Plattformen zum Datenaustausch für Ärzte, Pflegeeinrichtungen, Kliniken, Apotheken und Patienten aufzubauen. In den letzten Monaten sind entsprechende Pilotprojekte in Baden-Württemberg angelaufen.

Ein gemeinsamer Nenner der uns bekannten Pilotprojekte ist die Einführung einer digital vernetzten Patientenakte, in der beispielsweise Befunde, Laborwerte, Therapieempfehlungen, Arztbriefe, Notfalldaten, Medikationspläne und Daten von Wearables, digital abgelegt sind und bei Bedarf behandelnden Ärzten und anderen Beteiligten zur Verfügung gestellt werden.

Als Vorteil solcher Vernetzungen wird u.a. genannt, dass die an der Behandlung eines Patienten beteiligten Ärzte die erforderlichen Informationen rasch und unkompliziert austauschen können, was beispielsweise auch dann von Interesse sein kann, wenn ein in Stuttgart ansässiger Arzt einen Hamburger Experten zurate ziehen möchte. Soweit eine ärztliche Behandlung dabei ausschließlich über Kommunikationsnetze durchgeführt werden soll, steht dem grundsätzlich das arztrechtliche Fernbehandlungsverbot entgegen. In Baden-Württemberg ist dieses Verbot, bislang bundesweit einmalig, durch § 7 Absatz 4 Satz 3 der Berufsordnung der Landesärztekammer Baden-Württemberg aufgehoben worden: „Modellprojekte, insbesondere zur Forschung, in denen ärztliche Behandlungen ausschließlich über Kommunikationsnetze durchgeführt werden, bedürfen der Genehmigung durch die Landesärztekammer und sind zu evaluieren."

Auch die Landesregierung hat Vorteile solcher Vernetzungen erkannt. Dem entsprechend ist die Forderung „GESUNDHEITSPARTNER STÄRKER VERNETZEN" Teil der „Digitalisierungsstrategie der Landesregierung Baden-Württemberg", Stand Juli 2017 (im Internet abrufbar unter https://www.digital-bw.de/downloads/DigitalisierungsstrategieBaWue2017.pdf). Einzelheiten finden sich in dem Dokument „Strategie zur Verbesserung der medizinischen und pflegerischen Versorgung in Baden-Württemberg (Strategie Digitalisierung in Medizin und Pflege BW)" des Ministeriums für Soziales und Integration Baden-Württemberg, das im Internet unter https://sozialministerium.baden-wuerttemberg.de/fileadmin/redaktion/m-sm/intern/downloads/Downloads_Medizinische_Versorgung/Strategie_Digitalisierung-Medizin-Pflege-BW_Feb-2017.pdf abrufbar ist. Im Mai 2017 hat das Ministerium für Soziales und Integration die „Bekanntmachung – Projektförderung im Bereich Digitalisierung in Medizin und Pflege in Baden-Württemberg" (https://sozialministerium.baden-wuerttemberg.de/fileadmin/redaktion/m-sm/intern/downloads/Foerderaufrufe/Digitalisierung-Med-Pflege_Foerderaufruf_Bekanntmachung_2017.pdf) herausgegeben, die nach Abstimmung mit unserer Dienststelle u.a. die Aussage enthält, dass bei „der Entscheidung über die Zuwendungsgewährung" als Kriterium u.a. die „Einhaltung der datenschutzrechtlichen Anforderungen einschl. Datensicherheit" berücksichtigt wird. Es ist eine Selbstverständlichkeit, dass das Land mit öffentlichen Geldern nur Projekte fördern will, die den geltenden Rechtsvorschriften, darunter auch denen des Datenschutzrechts, entsprechen. Erfreulich ist, dass dies hier klar ausgesprochen wurde.

Weniger erfreulich ist, was wir bei der näheren Betrachtung bestimmter Projekte erkennen konnten. Keines dieser Projekte war aus datenschutzrechtlicher Sicht „ohne Befund". Das Hauptproblem ist die unklare Verantwortung. Wir können ohne weiteres nachvollziehen, dass die Gestaltung eines komplexen Verfahrens mit einer Vielzahl von Beteiligten, Daten und Kommunikationswegen ein anspruchsvolles Unterfangen ist, bei dem auch die sachgerechte und rechtskonforme Zuweisung der (jeweiligen) datenschutzrechtlichen Verantwortung ein nicht unerhebliches Maß an Sorgfalt und Mühe erfordern kann. Leider mussten wir immer wieder gravierende Defizite erkennen. Wir sahen uns wiederholt veranlasst, durch entsprechen-

de intensive Beratung eine solche Sorgfalt und Mühe anzumahnen. Daran führt aus Rechtsgründen kein Weg vorbei. Zunächst schon deshalb, weil es beim Datenschutz letztlich um Grundrechtsschutz geht: Das Recht datenschutzrechtlich Betroffener, also etwa auch von Patienten im Rahmen eines digitalen Ärztenetzes, auf informationelle Selbstbestimmung ist ein Grundrecht, das auf Artikel 2 Absatz 1 des Grundgesetzes (GG) in Verbindung mit Artikel 1 Absatz 1 GG beruht. Eingriffe in dieses Grundrecht unterliegen dem Vorbehalt des Gesetzes. Soweit beispielsweise im Rahmen eines digitalen Ärztenetzes personenbezogene Daten der Patienten ohne deren Einwilligung erhoben, gespeichert, genutzt und übermittelt werden sollen, ist dafür eine gesetzliche Grundlage erforderlich. Zur Prüfung, ob es eine solche gesetzliche Grundlage gibt und um welche es sich ggf. handelt, muss auch klar sein, wer der insofern verantwortliche Akteur wäre. Es muss mit Blick auf einen bestimmten Akteur konkret geklärt werden, ob gerade diesem eine gesetzliche Regelung bestimmte Befugnisse verleiht oder Pflichten auferlegt. Öffentliche Stellen sind darüber hinaus an die Grenzen ihrer jeweiligen gesetzlichen Aufgaben gebunden.
Diese Klarheit muss auch bestehen, wenn der Umgang mit personenbezogenen Daten auf die Einwilligung der Betroffenen gestützt werden soll. Ein wesentlicher Aspekt einer datenschutzrechtlichen Einwilligung ist, dass die Betroffenen über alle relevanten Umstände hinsichtlich der beabsichtigten Datenverarbeitung informiert werden. Dazu gehört auch die Information darüber, wer für diese Datenverarbeitung verantwortlich wäre. Nur dann kann ein Patient oder sonstiger Betroffener bewusst entscheiden, ob er just diesem Verantwortlichen vertraut und seine Einwilligung erteilt.
Unabhängig davon, ob der Umgang mit personenbezogenen Daten auf gesetzlicher Grundlage oder aufgrund einer Einwilligung erfolgt, muss die datenschutzrechtliche Verantwortung klar festgelegt und den Betroffenen offengelegt werden, damit diese ggf. ihre Datenschutzrechte, etwa auf Auskunft sowie auf Berichtigung und Löschung von Daten, gezielt geltend machen können.

Ob unsere Beratung auf fruchtbaren Boden fällt, ist noch offen. Selbstverständlich behalten wir die bislang betreuten Projekte weiter im Auge. Das Forum dieses Tätigkeitsberichts nutzen wir auch dazu, an solchen Projekten Interessierte zu beraten und diesen, was hiermit geschieht, unsere Beratung anzubieten.

1.8 Digitalisierung in Schulen – Smarte Bildung

Digitales Lernen in der Schule ist ein hoch aktuelles Thema, das in unserer Gesellschaft so leidenschaftlich wie kaum ein anderes diskutiert wird. Immer wieder wird in Wahlarenen und abendlichen Talkshows die Überfälligkeit des „digitalen Klassenzimmers" betont. Es fehle den vermeintlich rückständigen Schulen nicht nur die adäquate schulische IT-Ausstattung, sondern auch das „digitale Know-how" der Lehrkräfte.

Zweifellos verändert die digitale Welt das Lernen nachhaltig. Viele Schulen haben das erkannt, aber noch nicht oder nur in Teilen in ihrem Schulalltag umgesetzt. Die meisten Lehrer und Schulleiter begrüßen zwar grundsätzlich die neuen Technologien – für einen pädagogisch sinnvollen Einsatz fehlt es jedoch allzu oft an Konzepten, Weiterbildung und Infrastruktur. Angeheizt wird die kontroverse Diskussion durch Meldungen über die nach wie vor offene Finanzierung der durch die Kultusministerkonferenz erarbeiteten Eckpunkte einer Bund-Länder-Vereinbarung zur Unterstützung der Bildung in der digitalen Welt im Bereich der Schule („DigitalPakt Schule"). Der Bund hat im Rahmen der Gespräche den Bundesländern angeboten, ihnen in Form einer Anschubfinanzierung über einen Zeitraum von fünf Jahren mit rund 5 Mrd. € unter die Arme zu greifen. Finanziert werden sollen u.a. eine schnelle Breitbandanbindung der Schulen, deren schulweite WLAN-Ausleuchtung, die Ausstattung mit standortgebundenen Endgeräten und Servern sowie sichere Cloud-Lösungen für Unterrichtsinhalte und Lehrer-Austausch. Im Gegenzug verpflichten sich die Länder zur Überprüfung und Weiterentwicklung der Bildungs- und Lehrpläne aller Bildungsgänge, Schulstufen und Fächer mit Blick auf die Anforderungen der digitalen Welt. Sie sichern weiterhin den Ausbau von Lehrerfortbildungen und Einrichtungen der Lehrerbildung zu.

Aus Sicht des LfDI ist die Digitalisierung der Schulen zu unterstützen. Dies gilt vor allem für veränderte Lehrpläne mit digitalem Lernstoff und die Fortbildung von Lehrern, aber auch für die geplante länderübergreifende Entwicklung und Implementierung einer einheitlichen Schulcloud-Lösung. Mit einer „gesamtdeutschen Lösung" könnte den Schulen endlich eine Schulcloud zur Verfügung gestellt werden,

die Datenschutz- und Datensicherheitsgarantien integriert. Dieser Schritt ist angesichts der datenschutzrechtlichen Probleme der auf dem Markt angebotenen Cloud-Lösungen überfällig.

1.8.1 Der „Aufbaukurs Informatik“ als Chance zum Erwerb von Digitalkompetenz?

In der Präambel der Bund-Länder-Vereinbarung wird die Bedeutung des Erwerbs einer „Digitalkompetenz“ hervorgehoben. Das Bildungssystem müsse die notwendigen Voraussetzungen bereitstellen, um bei den Schülerinnen und Schülern ein Bewusstsein sowohl für die Chancen als auch die Risiken der Digitalisierung zu schaffen.

Mit der Einführung des „Aufbaukurses Informatik“ in Klasse 7 im Bildungsplan Schuljahr 2017/18 einschließlich der darin definierten Standards hat Baden-Württemberg neben der Leitperspektive Medienbildung einen kleinen aber wichtigen Schritt hin zum Erwerb dieser Kernkompetenzen umgesetzt.

Bereits in den beiden zurückliegenden Tätigkeitsberichten (31. Tätigkeitsbericht 2012/2013, LT-Drs. 15/4600, S. 124, 32. Tätigkeitsbericht 2014/2015, LT-Drs. 15/7990, S. 142) hat mein Vorgänger im Amt nachdrücklich gefordert, die Bildungsplanentwürfe so zu ergänzen, dass den Schülerinnen und Schülern, über die Medienbildung hinaus, der Erwerb darauf aufbauender Kenntnisse über die Funktionsweise und die Rahmenbedingungen des Internets ermöglicht wird. Beispielhaft wurde der Einsatz von Cookies, Zählpixeln oder „Like-Buttons“ genannt, welche genutzt werden, um Informationen über das Verhalten eines „Users“ während des Surfens im Internet zu sammeln.

Die im Bildungsplan aufgezeigten Standards zum Erwerb inhaltsbezogener Kompetenzen sind zwar aktuell und geeignet. Allerdings bleibt fraglich, ob die Schulen mit der Einführung des verbindlichen „Aufbaukurses Informatik“ in Klasse 7 die geforderten Kernkompetenzen im erforderlichen Umfang überhaupt vermitteln können. Die für die unterrichtliche Umsetzung der Inhalte zur Verfügung stehende eine Wochenstunde dürfte dafür nicht ausreichen. Ähnlich verhält es sich mit dem seit dem Schuljahr 2016/17 eingeführten „Basiskurs Medienbildung“, welcher mit lediglich 35 Stunden in allen 5. Klassen unterrichtet wird. Bleibt zu hoffen, dass es trotz der knappen finanziellen Mittel im kommenden Schuljahr nicht bei den bisherigen 60 Lehrerstellen für die Aufbaukurse bleibt. Die Notwendigkeit der Gewinnung qualifizierter Fachkräfte, auch für ein künftig mögliches und eigenständiges Unterrichtsfach „Informatik“, neben den Fächern Mathematik und Physik, halte ich für unumgänglich.

1.8.2 School goes Cloud – Die Problematik der Cloud-Nutzung an öffentlichen Schulen

Auch die Schulen in Baden-Württemberg nehmen immer stärker die Möglichkeit zur Auslagerung schulischer IT und der Abbildung schulischer Software als „Service in der Wolke“ durch die Einführung moderner Cloud-Lösungen wahr. Neben einer nicht unerheblichen Einsparung von Wartungskosten bei der Schul-EDV oder von Ausgaben für diverse Softwarelizenzen bringen z.B. via Cloud zur Verfügung gestellte Produktivitätsanwendungen auch eine „digitale Innovation“ an Schulen. Die Nutzung von „Software as a Service“ (SaaS) aus der Cloud bietet nun auch im Schulbereich beispielsweise die Möglichkeit zur kollaborativen und vernetzten Arbeit zwischen Lehrern und Schülern als auch untereinander.

Eine Verarbeitung personenbezogener Daten im Auftrag der Schulen durch einen Cloud-Anbieter stellt die Schulen allerdings vor ganz neue Herausforderungen. Entscheidet sich eine Schule für eine Cloud-Lösung, besteht zwischen der Schule und dem Diensteanbieter ein sogenanntes Auftragsdatenverarbeitungsverhältnis nach § 7 des Landesdatenschutzgesetzes (LDSG). Entgegen der häufig vertretenen Auffassung bleibt die Schule – trotz der Auftragsdatenverarbeitung durch den Cloud-Anbieter – weiterhin die **verantwortliche Stelle** im datenschutzrechtlichen Sinne (vgl. § 7 Absatz 1 Satz 1 LDSG). Der Auftrag ist schriftlich zu erteilen, der Inhalt des Vertrages richtet sich nach § 7 Absatz 2 LDSG. Gerade die dort genannten Anforderungen, von der sorgfältigen Auswahl des „Auftragsverarbeiters“ bis zur Pflicht der Kontrolle seiner getroffenen technischen und organisatorischen Maßnahmen, stellen für viele Schulen, wie uns Rückfragen hierzu immer wieder zeigen, Neuland dar. Den Schulen muss jedoch klar sein, dass sie als verantwortliche Stelle, bevor sie einen Clouddienst nutzen, prüfen müssen, ob das Angebot

alle datenschutzrechtlichen Vorgaben einhält: Der Anbieter muss **sicher, verlässlich und nachprüfbar** mit den ihm anvertrauten Daten umgehen. Viele Anbieter von Cloud-Diensten erfüllen diese datenschutzrechtlichen Anforderungen nicht und können daher in Schulen auch nicht eingesetzt werden.

Dies kann dann der Fall sein, wenn der Cloud-Dienst eine Datenübermittlung in einen sog. „Drittstaat", also einen Staat außerhalb der EU und des Europäischen Wirtschaftsraumes, dessen Datenschutzniveau als bedenklich oder gar unsicher gilt, vorsieht. So existiert z.B. in den USA kein einheitlich hohes Datenschutzniveau, was einen Datentransfer dorthin zumindest erschwert. Damit dennoch personenbezogene Daten in die USA übermittelt werden dürfen, nutzen US-amerikanische Firmen u.a. den seit Juli 2016 gültigen EU-US Privacy Shield. Im Rahmen dessen verpflichten sich die Firmen durch eine Selbstzertifizierung, datenschutzrechtliche Vorgaben einzuhalten, um so ein angemessenes Datenschutzniveau zu garantieren.

Nach wie vor ungelöst ist jedoch das grundsätzliche Problem der unkontrollierten Datensammlung durch US-Nachrichtendienste, welches auch durch den neuen EU-US-Privacy Shield nicht gelöst werden kann. Der noch immer gültige „Patriot Act" ermöglicht US-amerikanischen Sicherheitsbehörden, die Cloud-Anbieter zur Herausgabe von Daten zu verpflichten. Eine solche Herausgabe erstreckt sich dann u.U. auch auf die Daten der Rechenzentren der europäischen Tochterunternehmen, solange die Muttergesellschaft des Cloud-Anbieters ihren Sitz in den USA hat.

Im Hinblick darauf sollten daher gerade Schulen eine Vorbildfunktion einnehmen und vom Einsatz eines Cloud-Anbieters außerhalb eines Mitgliedsstaates der EU und des Europäischen Wirtschaftsraumes absehen, wenn Zweifel an der Einhaltung der Datenschutzvorgaben bestehen. Auch ist, unabhängig von der Frage nach einem möglichen datenschutzkonformen Betrieb solcher Cloud-Lösungen, zunächst deren Notwendigkeit zu prüfen und gegebenenfalls der Einsatz datenschutzkonformer Alternativen in Betracht zu ziehen (vgl. § 3a BDSG, Datenvermeidung und Datensparsamkeit).

Aktuell werden auch in der Schulwelt die sog. „Treuhänderlösungen" diskutiert. Hierbei sollen die personenbezogenen Daten des Auftraggebers ausschließlich auf Servern in Deutschland und nach deutschem Recht verarbeitet werden. Der Datentreuhänder soll jeden physischen und technischen Zugriff auf die Daten des Auftraggebers überwachen und kontrollieren. Vertraglich soll der Datentreuhänder an den Auftraggeber gebunden sein und ausschließlich in dessen Auftrag handeln, weshalb eine Datenübermittlung in Drittländer nur mit dessen Einverständnis möglich sein soll. Der Datentreuhänder selbst bietet seine Dienste – im Gegensatz zu manchem Cloud-Anbieter – nur entgeltlich an.

Ob damit Datenübermittlungen in Drittländer tatsächlich ausgeschlossen sind, ist unklar – datenschutzrechtlich schwebt hier insoweit noch eine nicht akzeptable „Wolke des Nichtwissens". Derzeit befassen sich die Datenschutzaufsichtsbehörden mit der Frage der Zulässigkeit einer „Treuhänderlösung" im schulischen Umfeld. Eine abschließende datenschutzrechtliche Beurteilung war bei Redaktionsschluss noch nicht möglich.

Rückmeldungen von Schulen zeigen, dass eine mögliche „Treuhänderlösung" aus Kostengründen auf eine geringe Akzeptanz bei den Schulträgern als sächlichen Ausstattern der Schulen stößt. Die mit der „Treuhänderlösung" verbundenen Mehrkosten wiegen für Schulträger das „Mehr" an Datenschutz offenbar nicht auf.

Zusammenfassend lässt sich daher feststellen, dass die Entwicklung und Implementierung vertrauenswürdiger Cloud-Lösungen für den Schulbereich immer notwendiger wird. Die Schulen sollten hier mit datenschutzkonformen Lösungen arbeiten können, um die notwendige Rechtssicherheit bei der Verarbeitung der personenbezogenen Daten ihrer Schutzbefohlenen zu haben.

1.8.3 „Schicks doch via Messenger" – Wie private Endgeräte und „soziale Medien" die Schulwelt verändern …

Der mit dem Wunsch zum „digitalen Klassenzimmer" verbundene Einsatz von „Mobile Devices" führt zu weiteren, bisher wenig diskutierten Problemen an den Schulen. So organisieren vorrangig die „Millennials" unter den Lehrkräften längst ihren Schulalltag unter Zuhilfenahme ihrer meist privaten Smartphones oder Tablets mit den dazu passenden Apps.

Geregelt wird ein solcher Einsatz privater Datenverarbeitungsgeräte durch die Verwaltungsvorschrift zum Datenschutz an öffentlichen Schulen. Danach verpflichtet sich die Lehrkraft zur Beachtung der „Datenschutzrechtlichen Hinweise für den Gebrauch privater Datenverarbeitungsgeräte durch Lehrkräfte zur Verarbeitung personenbezogener Daten" nach Anlage 1 dieser Verwaltungsvorschrift.

Trotz der allgemeinen Formulierungen hinsichtlich der zu treffenden technischen und organisatorischen Maßnahmen in Anlage 1 zeigt sich mittlerweile die Notwendigkeit einer Anpassung der Anlage:
So steht z.B. die für den dienstlichen Gebrauch des privaten Datenverarbeitungsgerätes formulierte Voraussetzung, „das Betriebssystem durch die Installation von Updates und Patches auf dem neusten Stand zu halten", im Widerspruch mit der Updatepolitik der Hersteller von Smartphone- oder Tablet-Betriebssystemen. Ein Großteil der Smartphones und Tablets erfährt heutzutage aufgrund der schnellen Entwicklungszyklen nach schon kurzer Zeit keine regulären Updates mehr. Deshalb müsste die Lehrkraft dessen Verwendung u.U. einstellen.
An den Einsatz privater Endgeräte zur Erfüllung dienstlicher Aufgaben sind aus datenschutzrechtlicher Sicht hohe Anforderungen zu stellen. Deren Einhaltung ist insbesondere durch die Vielzahl der Systemupdates schwer zu überschauen.

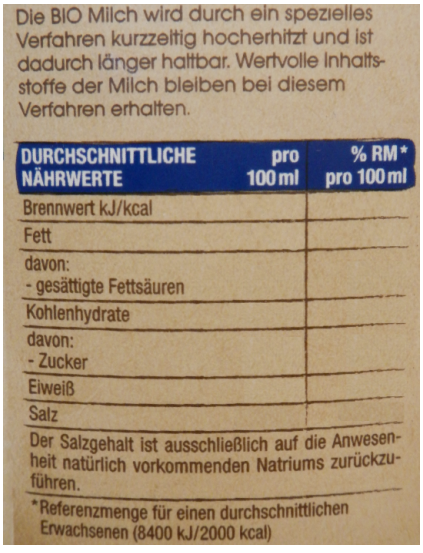
Auch die Generation der „Digital Natives" unter den Lehrkräften setzt ihr „Digitalverständnis" in ihre Arbeitswelt um, wobei häufig die Grenzziehung zwischen „privat" und „dienstlich" zu kurz kommt. Sehr deutlich wird dies beim Einsatz „sozialer Netzwerke", wie die steigende Anzahl an Eingaben hierzu zeigt. Die bereits aus dem privaten Umfeld gewohnte und in der Tat effiziente Kommunikation via Messenger ermöglicht auch im schulischen Umfeld den direkten und schnellen Weg zum Schüler, um beispielsweise einen Ausfall einer Stunde oder die Vertretungssituation zu kommunizieren. Die Lehrkraft wird aus Schülersicht so zu einem „Eintrag" im Adressbuch des Messengers, neben Freunden und der Familie, oder gar Bestandteil einer Gruppe oder eines Chats. Dass die Grenzen zwischen „privat" und „dienstlich" auf beiden Seiten unscharf werden, ist daher nicht verwunderlich. Mittlerweile wird u.a. auch die abfotografierte Krankmeldung des Schülers via Messenger ohne Weiteres akzeptiert und ausgedruckt dem Klassenbuch beigefügt.

Die Verwaltungsvorschrift zum Datenschutz an öffentlichen Schulen hierzu ist eindeutig und aktuell gültig, wenn auch gern als „unzeitgemäß" abgetan: „Die dienstliche Nutzung von sozialen Netzwerken ist für eine Kommunikation von Lehrkräften mit anderen Lehrkräften oder mit Schülerinnen und Schülern, wenn dabei personenbezogene Daten verarbeitet werden, nicht erlaubt".

Ungeachtet dessen, stellt sich – neben rechtlichen und technisch-organisatorischen Aspekten – auch in diesem Zusammenhang die Problematik einer möglichen Übermittlung in einen Drittstaat ohne angemessenes Datenschutzniveau. Handelt es sich bei dem Messenger-Dienst beispielsweise um ein US-amerikanisches Unternehmen als Betreiber, ist nicht auszuschließen, dass europäische Standards zu Datenschutz und Datensicherheit missachtet und US-amerikanische Einrichtungen und Behörden auf den Datenbestand des Unternehmens zugreifen können. Beides muss ausgeschlossen sein, wenn es um die Daten unserer Schülerinnen und Schüler, aber auch von öffentlich Bediensteten geht.

1.9 Datenschutz im Internet of Things (IoT)

Stellen Sie sich vor, bei Ihrem nächsten Einkauf wollen Sie Milch für Ihr Müslifrühstück nach Fett- und andere Nährstoffgehalten auswählen, greifen in das Regal und sehen auf der Milchtüte folgendes:



Die BIO Milch wird durch ein spezielles Verfahren kurzzeitig hocherhitzt und ist dadurch länger haltbar. Wertvolle Inhaltsstoffe der Milch bleiben bei diesem Verfahren erhalten.

DURCHSCHNITTLICHE NÄHRWERTE	pro 100 ml	% RM* pro 100 ml
Brennwert kJ/kcal		
Fett		
davon: - gesättigte Fettsäuren		
Kohlenhydrate		
davon: - Zucker		
Eiweiß		
Salz		

Der Salzgehalt ist ausschließlich auf die Anwesenheit natürlich vorkommenden Natriums zurückzuführen.

*Referenzmenge für einen durchschnittlichen Erwachsenen (8400 kJ/2000 kcal)

Würden Sie die Milchpackung kaufen? Wohl eher nicht, schließlich fehlen Ihnen die wesentlichen Informationen, um Ihre Entscheidung treffen zu können. In diesem Fall würde man von mangelhaften Produktinformationen sprechen.

Ähnlich verhält es sich beim Datenschutz. In einer Datenschutzerklärung, z.B. eines App-Anbieters, sollen die Informationen bereitgestellt werden, die es Ihnen ermöglichen, mehr über die Verarbeitung Ihrer personenbezogenen Daten durch die App in Erfahrung zu bringen: „Wie lange werden die Daten gespeichert, an wen werden sie möglicherweise weitergegeben, kann der Weitergabe oder weiteren Nutzung widersprochen werden, werden die Daten gelöscht, wenn sie nicht mehr gebraucht werden?" Eine gute Datenschutzerklärung enthält alle Informationen, um diese Fragen zu beantworten und Ihr Recht auf informationelle Selbstbestimmung ausüben zu können.

Schon im Jahr 2014 hat sich das Technik-Referat meiner Dienststelle mit der Prüfung von Datenschutzerklärung bei Smartphone-Apps befasst. Es wurden vornehmlich solche Apps evaluiert, die in Baden-Württemberg entwickelt wurden oder deren Betreiber hier ansässig sind. Damaliges Fazit: die meisten Apps ließen die notwendige Transparenz im Umgang mit personenbezogenen Daten vermissen. Hauptmanko war das Fehlen einer Datenschutzerklärung, aus der hervorgeht, warum bestimmte Daten von einer App benötigt werden. Daher konnte auch nicht nachvollzogen werden, ob die erhobenen Daten für das Funktionieren einer App tatsächlich erforderlich waren.

Mit dem Einzug von Produkten des „Internet der Dinge" bzw. „Internet of Things" (IoT) in viele Lebensbereiche unseres Alltags stellt sich die Frage nach der Transparenz und Sicherheit der Datenverarbeitung umso dringlicher. Schließlich werden immer mehr elektronische Produkte mit dem Internet verbunden – sei es die Steuerzentrale für das „Smart Home", der Fitness Tracker oder nicht zuletzt der „intelligente" interaktive Fernseher, neudeutsch Smart TV. Dank miniaturisierter Sensoren wird eine Vielzahl physikalischer oder biomedizinischer Größen durch diese „intelligenten" Geräte erfasst. Gesteuert werden sie häufig per App auf dem Smartphone. So lässt sich z.B. die Heizung im Smart Home von überall auf der Welt per App ein- und ausschalten. Auch wenn es von außen nicht ohne weiteres ersichtlich ist: Die Geräte können zahlreiche personenbezogene Daten – von der Temperatur in unserer Wohnung über unseren Gesundheitszustand bis hin zu unserem aktuellen Aufenthaltsort – erheben. Werden diese Daten zu einem Cloud-Anbieter übertragen, kann er damit umfangreiche Nutzungsprofile erstellen.

Unter dem Titel „GPEN Privacy Sweep 2016" hat im Jahr 2016 die englische Datenschutzaufsichtsbehörde eine Aktion zur Prüfung des Datenschutzes bei Produkten im Bereich des „Internet of Things" angestoßen und koordiniert. GPEN steht für „Global Privacy Enforcement Network" und ist ein informeller Zusammenschluss von Datenschutzaufsichtsbehörden auf der ganzen Welt. An der Aktion haben 25 der im GPEN aktiven Datenschutzaufsichtsbehörden teilgenommen, u.a. auch das Technik-Referat meiner Dienststelle.

Wie bei der Aktion im Jahr 2014 wurden die Datenschutzerklärungen von Produkten überprüft. Hierzu wurden auch die Datenschutzbeauftragten der Hersteller dieser Produkte kontaktiert. Sie sollten datenschutzrechtliche Fragen zu ihren Produkten beantworten.

Insgesamt erbrachte der „GPEN Privacy Sweep 2016 " folgendes Ergebnis: Mehr als 300 IoT-Geräte wurden untersucht, u.a. in den Anwendungsbereichen Smart Home, Smart Metering, Fitness und Gesundheit. Rund 60 Prozent der Nutzer werden nicht hinreichend aufgeklärt, welche personenbezogenen Daten erhoben werden und was mit diesen Daten geschieht. Insbesondere klären Unternehmen Nutzer nicht darüber auf, wie die Daten gespeichert werden und wie die Daten wieder gelöscht werden können. Außerdem beziehen sich die Datenschutzbestimmungen überwiegend nicht auf einzelne Geräte, sondern auf das gesamte Produktsortiment oder lediglich auf den Unternehmensauftritt im Web.

Was ist zu tun? Den Herstellern und Betreibern von IoT-Produkten empfehle ich sehr, auch im Hinblick auf die ab dem Jahr 2018 wirksame EU-Datenschutz-Grundverordnung, den Datenschutz bereits bei der Entwicklung der Produkte einzubeziehen und datenschutzfreundliche Produkte zu realisieren. Zudem ermutige ich die Bürgerinnen und Bürger zu kritischen Nachfragen über den Umgang mit personenbezogenen Daten bei Herstellern und Betreibern von IoT-Geräten.

2. Innere Sicherheit

2.1. JI-Richtlinie

Die Umsetzung des europäischen Datenschutzpaketes ist in Baden-Württemberg in vollem Gange. Nicht nur die DS-GVO, sondern auch die sog. JI-Richtlinie erfordern eine vollständige Prüfung, gegebenenfalls Anpassung oder Änderung bestehender polizei- und ordnungsrechtlicher Vorschriften.

Die EU-Richtlinie für den Datenschutz bei Polizei und Justiz (JI) 2016/680[1] wurde im Paket mit der europäischen Datenschutz-Grundverordnung (DS-GVO) verabschiedet und kann als „kleine Schwester" der Datenschutz-Grundverordnung für den polizeilichen und justiziellen Bereich bezeichnet werden. Die Richtlinie soll erstmalig in den Bereichen Polizei und Justiz eine datenschutzrechtliche Mindestharmonisierung herbeiführen und lässt den Mitgliedstaaten Spielräume bei der Umsetzung in nationales Recht. Im Gegensatz zu den Vorschriften der DS-GVO, welche ab 25. Mai 2018 unmittelbar anzuwenden sind, müssen bestehende Gesetze angepasst und die in der JI-Richtlinie enthaltenen Mindestvoraussetzungen spätestens bis zum 6. Mai 2018 in nationales Recht umgesetzt werden. Von diesem Anpassungsbedarf sind Bund und Länder gleichermaßen betroffen. Während der Bundesgesetzgeber diese Aufgabe für die Polizeibehörden des Bundes teilweise innerhalb des dritten Abschnitts des neuen Bundesdatenschutzgesetzes (BDSG-neu)[2] erledigt hat, steht der baden-württembergische Gesetzgeber noch am Anfang.

So stellt bereits die Frage, welche Tätigkeiten künftig der Richtlinie unterfallen und welche der DS-GVO zuzuordnen sind, den Gesetzgeber vor erhebliche Probleme. Die Abgrenzung zwischen DS-GVO und JI-Richtlinie ist komplexer, als es bei einem Blick in Art. 2 Absatz 2 lit. d DS-GVO scheinen mag. Entsprechend dieser Vorschrift findet die DS-GVO keine Anwendung auf die Datenverarbeitung bei Polizei und Justiz im Zusammenhang mit Straftaten. Dieser Bereich wird nunmehr durch die Richtlinie abgedeckt. Nach Art. 2 Absatz 1 der JI-Richtlinie findet die Richtlinie auf die Verarbeitung personenbezogener Daten durch Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit Anwendung. Sie erfasst daher sowohl die Datenverarbeitung zu präventiven als auch zu repressiven Zwecken, sodass sie den für Strafverfolgung zuständigen Bundesgesetzgeber ebenso wie die für das allgemeine Polizeirecht zuständigen Landesgesetzgeber betrifft. Die Anwendung der JI-Richtlinie stellt den Begriff der Straftat in den Fokus. Wird die Polizei z.B. zum Schutz privater Rechte und Gefahren tätig (Suizid-Fälle), so würde in dieser Konstellation ein Bezug zu einer Straftat vollends fehlen. Auf derartige bloße Gefahrenabwehrmaßnahmen der Polizei ohne Straftatbezug, ist die JI-Richtlinie folglich nicht anwendbar. Der Straftatenbegriff der Richtlinie wirft auch in anderen Bereichen Fragen auf: Was macht eine Straftat im Sinne der Richtlinie aus? Unterfallen Ordnungswidrigkeiten ebenfalls diesem Straftatenbegriff? Eine eindeutige Antwort gibt es derzeit nicht. Im deutschen Recht wird klar zwischen Straftaten einerseits und Ordnungswidrigkeit andererseits unterschieden. Eine solche Unterscheidung ist dem europäischen Recht jedoch fremd. In der Folge besteht derzeit Uneinigkeit darüber, ob die dem deutschen Recht bekannten Ordnungswidrigkeiten dem Straftatenbegriff im Sinne der Richtlinie unterfallen sollen oder vielmehr auszuklammern sind. Ungeklärt ist auch, ob die JI-Richtlinie nur für die Polizei gilt oder auch für die Gefahrenabwehr durch (Sonder-)Ordnungsbehörden. Die JI-Richtlinie klammert ausdrücklich solche Tätigkeiten von ihren sachlichen Anwendungsbereichen aus, welche nicht in den Anwendungsbereich des Unionsrechts fallen (Art. 2 Abs. 3 lit. a). Diese Einschränkung betrifft also insbesondere die den Mitgliedstaaten selbst überlassene Tätigkeit zum Schutz der nationalen Sicherheit, z.B. den Verfassungsschutz. Ein identischer

1 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

2 Artikel 1 des Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU vom 30. Juni 2017, BGBl. I S.

Bereichsausschluss findet sich auch in der DS-GVO (Art. 2 Abs. 2 lit. b).

Der baden-württembergische Gesetzgeber wird insbesondere die polizei- und strafvollstreckungsrechtlichen Vorschriften hinsichtlich des notwendigen Anpassungsbedarfs zu überprüfen haben. Zwingend sollten bestehende Gesetze auf folgen Richtlinieninhalte überprüft werden:

Artikel 6 der JI-Richtlinie verlangt, dass im Rahmen der Datenverarbeitung zwingend eine Unterscheidung zwischen den Personengruppen vorzunehmen ist. Hierbei gilt der Grundsatz, dass je weiter entfernt der Betroffene, dessen Daten verarbeitet werden, zu der im Raum stehenden Tat steht, desto höhere Maßstäbe an den Schutz seiner Daten zu stellen sind. Im Kern ist bei einer fehlenden Differenzierung nach Personengruppen vor allem die Verhältnismäßigkeit der Datenverarbeitung fragwürdig. Je nachdem, ob eine Person Verdächtiger, verurteilter Straftäter, Opfer, Zeuge oder Kontaktperson einer Straftat ist, müssen die Umsetzungsgesetze unterschiedliche Schutzniveaus mit divergierenden Rechtsfolgen vorsehen. Daher ist es zwingend, dass die Umsetzungsgesetze verschiedene Voraussetzungen für die Erhebung, Speicherung der jeweils verwendeten personenbezogenen Daten vorsehen. Gleiches gilt zudem auch für die zulässige Speicherfrist. Die Verarbeitung von Nichtverdächtigen erfordert ein erhöhtes Schutzniveau.

Effektive Polizeiarbeit ist zudem wesentlich von der Qualität der verwendeten Daten abhängig. Um die Qualität der Daten zu gewährleisten, bestimmt Art. 7 der JI-Richtlinie, dass Daten, welche auf Fakten, d.h. objektiven Tatsachen (hard data), beruhen, deutlich unterscheidbar von solchen Daten sein müssen, welche auf persönlichen Einschätzungen (soft data) beruhen. Dies kann durch eine Kennzeichnung der Daten im Aktenrückhalt oder aber durch eine explizite Kennzeichnung oder durch eine Angabe der Informationsquelle erfolgen. Unabhängig von dem gewählten Weg ist entscheidend, dass der Charakter der Daten ersichtlich ist. Ein Verzicht auf derartige Zusatzhinweise kann sich zu einem ernstzunehmenden Hindernis des polizeilichen Datenaustauschs entwickeln.

Art. 10 der Richtlinie verpflichtet den nationalen Gesetzgeber zudem, besondere gesetzliche Regelungen für besondere Kategorien personenbezogener Daten zu schaffen. Besondere personenbezogen Daten in diesem Sinne sind Daten, aus denen die rassische oder 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.

Eine weitere Neuheit der Richtlinie findet sich in Art. 25 der JI-Richtlinie: Bei Verarbeitungsvorgängen in automatisierten Verarbeitungssystemen müssen künftig Erhebung, Veränderung, Abfrage und Offenlegung einschließlich Übermittlung, Kombination und Löschung protokolliert werden. Protokolle über Abfragen und Offenlegungen müssen zudem eine Begründung, das Datum und die Uhrzeit und so weit wie möglich die Identifizierung der abfragenden oder offenlegenden Person und die Identität des Empfängers solcher personenbezogenen Daten enthalten.

Die vorstehenden Punkte vermögen nur beispielhaft aufzuzeigen, welch großer Umsetzungsbedarf mit der JI-Richtlinie verbunden ist. Selbst wenn die Richtlinie lediglich zur Umsetzung eines harmonisierten Mindestmaßes verpflichtet, sollte der Landesgesetzgeber das Momentum der Reform nicht ungenutzt lassen, ein im Vergleich zur JI-Richtlinie höheres Schutzniveau zu schaffen.

Durch die JI-Richtlinie wird der Landesgesetzgeber verpflichtet, in deren Anwendungsbereich ein datenschutzrechtliches Mindestniveau zu gewährleisten. Ein Unterschreiten des in der Richtlinie festgesetzten Mindestniveaus verbietet sich somit. Unbenommen bleibt es dem Landesgesetzgeber, ein höheres Schutzniveau im Anwendungsbereich der Richtlinie zu schaffen. Diese Möglichkeit sollte der Landesgesetzgeber nutzen!

2.2 Besondere Zeiten

Die terroristischen Anschläge in der letzten Zeit und die anhaltende Debatte in Politik und innerhalb Sicherheitsbehörden darüber, wie man dem Phänomen islamistischer Gewalttaten Herr werden könnte, hatten auch Auswirkungen auf die Arbeit meiner Dienststelle. Wiederholt ergaben sich in unterschiedlichster Weise rechtliche Fragestellungen, die in der

Praxis nicht selten so beantwortet wurden, dass bestehende Datenschutzbestimmungen bis an den Rand des Vertretbaren und zum Teil darüber hinaus gedehnt wurden. Denn eine Erkenntnis wurde wieder einmal deutlich: Der Gesetzgeber kann nicht an alles denken. Insofern kommen die Sicherheitsbehörden, gerade in turbulenten Zeiten wie diesen, immer wieder in die Situation, Maßnahmen ergreifen zu wollen, für die es rechtlich (noch) keine klare Lösung gibt und die zum „kreativen" Umgang mit den Gesetzen herausfordert. Folgendes sei hier näher dargestellt:

2.2.1 Kompetenzzentrum zur Koordinierung des Präventionsnetzwerks gegen (islamistischen) Extremismus in Baden-Württemberg (KPEBW)

Im Rahmen des im Februar 2015 von der Landesregierung beschlossenen Maßnahmenpakets zur Bekämpfung des islamistischen Terrorismus wurde die Einrichtung eines Kompetenzzentrums zur Koordinierung des Präventionsnetzwerks gegen (islamistischen) Extremismus in Baden-Württemberg (KPEBW) beschlossen. Dessen Aufgabe ist es, Maßnahmen der Präventions- und Interventionsbemühungen gegen verfassungsfeindliche Bestrebungen im Zusammenhang mit dem islamistischen Terrorismus zentral zu steuern und zu koordinieren. Darüber hinaus soll es den Informationsfluss zwischen staatlichen und nichtstaatlichen Akteuren, einschließlich der Sicherheitsbehörden, gewährleisten.

Auf operativer Ebene wurde eine landesweite zentrale Beratungsstelle eingerichtet, die von einem externen Partner, dem Violence Prevention Network e.V. (VPN) mit Sitz in Berlin, betrieben wird. Zu den Aufgaben der Beratungsstelle gehören neben Maßnahmen der schwerpunktmäßig spezifischen und allgemeinen Prävention auch die Beratung von Angehörigen und dem sozialen Umfeld von Radikalisierten, die Beratung von und die aufsuchende Arbeit mit Radikalisierten in einem frühen Stadium und der Aufbau eines Ausstiegsangebots für Radikalisierte, Ausreisewillige, Rückkehrer (z.B. Syrien-Rückkehrer) und Inhaftierte in Justizvollzugsanstalten.

Die Vertragsgestaltung sieht eine enge Zusammenarbeit von VPN auf der einen Seite und den Sicherheitsbehörden (Landeskriminalamt, Landesamt für Verfassungsschutz) auf der anderen Seite vor. Dabei stellen sich grundsätzliche Fragen des Datenschutzes, die Gegenstand zahlreicher Besprechungen und Schriftwechsel meiner Dienststelle mit (im Wesentlichen) dem Innenministerium waren, bei dem das Kompetenzzentrum organisatorisch angebunden ist.

Eine wesentliche Frage war, inwieweit VPN, der den datenschutzrechtlichen Maßgaben des Bundesdatenschutzgesetzes unterliegt, berechtigt ist, den Sicherheitsbehörden Informationen aus seiner Beratungstätigkeit mitzuteilen. Dass diese Frage zu Beginn des Projekts nicht beantwortet werden konnte, verwunderte angesichts dessen, dass VPN zu diesem Zeitpunkt bereits des Längeren in anderen Bundesländern aktiv war und an solchen Fallkonferenzen mit Sicherheitsbehörden teilnahm. Die von mir verständigte, für VPN zuständige Datenschutzaufsichtsbehörde in Berlin nahm sich der Sache an. Dabei zeigte sich, dass im Grundsatz weder eine gesetzliche Grundlage für eine Datenübermittlung besteht, noch die ins Auge gefasste Variante einer Einwilligungslösung in den meisten Fällen zum Ziel führen konnte. Während diese Frage vor allem durch meine Kollegin in Berlin endgültig zu klären war, musste ich mich einerseits mit der Frage befassen, ob und ggf. wie eine Zusammenarbeit von Polizei und Verfassungsschutz vor dem Hintergrund des sog. Trennungsgrundsatzes möglich war. In seiner Entscheidung zum Antiterrordateigesetz[3] hat das Bundesverfassungsgericht nämlich festgestellt, dass der Informationsaustausch zwischen Nachrichtendiensten und Polizeibehörden wegen der auf ihre spezifischen Aufgaben jeweils zugeschnittenen und durch sie begrenzten Datenerhebungs- und -verarbeitungsbefugnisse für den Datenschutz auch eine besondere grundrechtliche Dimension habe: „Dass Informationen zwischen den verschiedenen Sicherheitsbehörden nicht umfassend und frei ausgetauscht werden, ist nicht Ausdruck einer sachwidrigen Organisation dieser Behörden, sondern von der Verfassung durch den datenschutzrechtlichen Grundsatz der Zweckbindung grundsätzlich vorgegeben und gewollt." (informationelles Trennungsprinzip)[4]. Wie das in einer Gesprächssituation wie einer Fallkonferenz, in der Vertreter der beiden Sicherheitsbehörden zusammensitzen, praktisch umgesetzt werden soll, war und ist die

3 Urteil vom 24.03.2013 – 1 BvR 1215/07 –

4 BVerfG, Urteil vom 24. April 2013 – 1 BvR 1215/07 –, BVerfGE 133, 277-377

große Frage. Konzeptionell ist jedenfalls vorgesehen, dass sich Vertreter von Landeskriminalamt und Verfassungsschutzamt vor jeder Äußerung im Rahmen eines konkreten Falles versichern, dass sie das, was sie sagen wollen, auch tatsächlich sagen dürfen. Denn tatsächlich gibt es Regelungen in den Fachgesetzen (Polizeigesetz, Verfassungsschutzgesetz), die einen Datenaustausch unter Sicherheitsbehörden unter bestimmten Voraussetzungen zulassen. Dies mit Leben zu erfüllen dürfte für die Beteiligten eine Herausforderung darstellen. In einer Besprechung mit dem Innenministerium wurde uns versichert, dass es bisher geklappt habe und kein unzulässiger Datenaustausch stattgefunden habe. Dies zu überprüfen fällt schwer, wird doch im Zweifel dazu in den Protokollen nichts zu finden sein. Aber ich habe derzeit auch keinen Hinweis darauf, dass die Regeln nicht beachtet worden wären.

Die andere Frage war, ob und inwieweit die Sicherheitsbehörden Informationen über ihre Erkenntnisse dem privaten Verein mitteilen dürfen. Auch dazu gibt es in den einschlägigen Gesetzen Übermittlungsvorschriften, die unter ganz engen Voraussetzungen eine Weitergabe von Informationen an Private zulassen. Auch hier bleibt mir nichts übrig als darauf zu vertrauen, dass die Beteiligten verantwortungsvoll mit ihren Befugnissen umgehen. Das Innenministerium hat mir jedenfalls ausdrücklich versichert, dass man sich streng an die gesetzlichen Vorgaben halte.

2.2.2 Projekt SonAR BW

„Vertrauen ist gut, Kontrolle ist besser", mag sich das Landeskriminalamt gedacht haben und hat ein Projekt SonAR BW aufgesetzt. Ein Sonar ist ein „Verfahren zur Ortung von Gegenständen im Raum und unter Wasser mittels ausgesandter Schallimpulse"[5]. So ganz falsch liegt man mit diesem Begriffsverständnis bei der Beschreibung dessen, was das Landeskriminalamt mit der „Stelle zur operativen Analyse von Risikopersonen in Baden-Württemberg" im Sinn hatte, allerdings nicht. Denn ausgehend von der Befürchtung, den Polizeidienststellen vor Ort sei bei der Bearbeitung bestimmter Delikte durch die Lappen gegangen, dass diesen eine Gesinnung zugrunde lag, die später einmal in eine islamistisch-terroristische Gewalttat münden könnte, sollten die Dienststellen aufgefordert werden, nochmal einen zweiten Blick in ihre Unterlagen werfen - diesmal allerdings durch Spezialisten. Grundlage für diese Aktion war zunächst die Identifizierung des maßgeblichen Täterkreises. Hierzu wurde ein Kriterienkatalog entwickelt, anhand dessen dann das polizeiliche Auskunftssystem POLAS BW gescannt wurde. Die dabei gewonnenen Treffer wurden dann an die Polizeipräsidien vor Ort mit einem entsprechenden Prüfauftrag verteilt.

Meine Dienststelle wurde leider erst zu einem späten Zeitpunkt einbezogen, als das Projekt schon am Laufen war. Dies fiel auch noch in die Urlaubszeit, sodass eine kurzfristige Stellungnahme zwar möglich, eine Berücksichtigung unserer Bedenken aber nicht mehr möglich war. So blieb es im Grunde beim Austausch von Argumenten, ohne dass man letztlich zu einem klaren Ergebnis gekommen wäre.

Meine Bedenken waren folgende:
Die zunächst durchgeführte Recherche aus der Quelldatei POLAS BW anhand vorgegebener Filterkriterien stellte eine Nutzung gespeicherter Daten dar. Hierfür bedarf es grundsätzlich einer Rechtsgrundlage. In Betracht kam insoweit ersichtlich nur § 38 Absatz 1 Satz 1 des Polizeigesetzes (PolG). Danach muss eine Nutzung der POLAS-Daten „zur vorbeugenden Bekämpfung von Straftaten erforderlich" sein.

Der Begriff der „vorbeugenden Straftatenbekämpfung" war hier aus verfassungsrechtlichen Gründen im präventiven Sinne (Verhinderungsvorsorge) zu verstehen.[6] Die Datennutzung musste also erforderlich sein, um drohende Rechtsgutverletzungen von vornherein und in einem Stadium zu verhindern, in welchem es noch nicht zu strafwürdigem Unrecht gekommen ist, in der Regel also im Planungs- oder Vorbereitungsstadium[7].

Hiervon ausgehend erschien es zweifelhaft, ob die POLAS-Recherche durch das Landeskriminalamt eine Maßnahme der vorbeugenden Verbrechensbekämpfung darstellte. Zwar diente das Verfahren letztlich dem Ziel, potenzielle jihadistische Gewalttäter unter den polizeibekannten Migranten zu identifizieren, und damit präventiven Zwecken. Zum Zeitpunkt der

5 https://de.wikipedia.org/wiki/Sonar
6 Verwaltungsgerichtshof Baden-Württemberg, Urteil vom 15. Mai 2014 – 1 S 815/13 –, juris
7 Verwaltungsgerichtshof Baden-Württemberg, a.a.O.

POLAS-Recherche gab es jedoch noch keinerlei Anhaltspunkte dafür, dass die durch die Filterkriterien definierten Personen Straftaten aus politischen oder religiösen Motiven begangen hatten, geschweige denn solche planen oder vorbereiten würden. Solche Personen sollten erst in einem weiteren Schritt ermittelt werden. Mit anderen Worten, die Recherche diente damit nicht, jedenfalls nicht unmittelbar, der vorbeugenden Verbrechensbekämpfung, sie sollte vielmehr die Voraussetzungen dafür schaffen, dass in weiteren Schritten ggf. neue Ermittlungsansätze gewonnen werden konnten. Damit lag sie weit im Vorfeld konkreter Bekämpfungsmaßnahmen und damit außerhalb des ursprünglichen Verwendungszwecks. Hierzu hat das Bundesverfassungsgericht in seinem Urteil vom 20. April 2016[8] Folgendes festgestellt:
„Folglich widerspricht es nicht von vornherein dem Gebot einer dem ursprünglichen Erhebungszweck entsprechenden Verwendung, wenn die weitere Nutzung solcher Daten bei Wahrnehmung derselben Aufgabe auch unabhängig von weiteren gesetzlichen Voraussetzungen als bloßer Spurenansatz erlaubt wird. Die Behörde kann die insoweit gewonnenen Kenntnisse zum Schutz derselben Rechtsgüter und im Rahmen derselben Aufgabenstellung – allein oder in Verbindung mit anderen ihr zur Verfügung stehenden Informationen – als schlichten Ausgangspunkt für weitere Ermittlungen nutzen. Dies trägt dem Umstand Rechnung, dass sich die Generierung von Wissen – nicht zuletzt auch, wenn es um das Verstehen terroristischer Strukturen geht – nicht vollständig auf die Addition von je getrennten, nach Rechtskriterien formell ein- oder ausblendbaren Einzeldaten reduzieren lässt. In den dargelegten Grenzen erkennt das die Rechtsordnung an. Diese Grenzen gewährleisten zugleich, dass damit keine Datennutzung ins Blaue hinein eröffnet ist. Durch die Bindung an die für die Datenerhebung maßgeblichen Aufgaben und die Anforderungen des Rechtsgüterschutzes hat auch eine Verwendung der Daten als Spurenansatz einen hinreichend konkreten Ermittlungsbezug, den der Gesetzgeber nicht durch weitere einschränkende Maßgaben absichern muss."

Die merkmalbezogene Recherche (Inverssuche) im POLAS-Bestand ohne konkreten Ermittlungsbezug führte hier nicht zu unmittelbaren Spurenansätzen, die Ausgangspunkt für weitere Ermittlungen sein könnten. Sie stellte vielmehr eine „Datennutzung ins Blaue hinein" dar. Denn ob sich in dem durch die Recherche identifizierten Personenkreis tatsächlich einzelne Fälle finden konnten, die letztendlich Anlass für weitere Ermittlungen hätten bieten können, war völlig ungewiss und hing von mehreren Faktoren ab, insbesondere der sorgfältigen Dokumentation in der Ermittlungsakte und der Sorgfalt bei der Überprüfung durch die Staatsschutzdienststellen vor Ort. Das Rechercheergebnis begründete allenfalls eine vage Vermutung, dass sich im Weiteren neue Ermittlungsansätze bieten könnten. Im Ergebnis lag die Recherche im POLAS-Bestand nach meiner Auffassung damit außerhalb des rechtlich zulässigen Verwendungszwecks.

Auch eine Zweckänderung schied meines Erachtens aus. Eine ausdrückliche Regelung, welche die Nutzung der für die Verhinderung von Straftaten gemäß § 38 PolG gespeicherten Daten zu einem anderen Zweck zulässt, ist nicht erkennbar. Bei der Recherche handelte es sich vielmehr um eine besondere Form des Datenabgleichs. Regelungen hierzu finden sich in den §§ 39 und 40 PolG, die konkreten Sachverhalt allerdings nicht trafen. Selbst bei einer analogen Anwendung des § 40 PolG hätten die weiteren Voraussetzungen des § 40 Absatz 1 PolG (Erforderlichkeit zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Person) nicht vorgelegen.

Auch die Weitergabe der Rechercheergebnisse an die örtlichen Polizeidienststellen war datenschutzrechtlich nicht unproblematisch. Zwar gibt es mit § 42 Absatz 1 PolG eine entsprechende Rechtsgrundlage. Fraglich war für mich aber, ob die Unzulässigkeit der Datenverarbeitung durch das Landeskriminalamt bei der Generierung der Personengruppe nicht zu einem Verwertungs- und damit einem Übermittlungsverbot hätte führen müssen. Ein Rückgriff auf die nordamerikanische „fruit of the poisonous tree-doctrine", die vornehmlich der Disziplinierung der Polizei dient[9], ist allerdings nicht zweifelsfrei[10]. Gleichwohl erscheint es rechtsstaatlich nicht unproblematisch, die Übermittlung persönlicher Daten, die ohne hinreichen-

8 1 BvR 966/09, 1 BvR 1140/09 –, juris
9 BFH, Urteil vom 4. Oktober 2006 – VIII R 53/04 –, BFHE 215, 12, BStBl II 2007, 227
10 vgl. hierzu auch: BGH, Urteil vom 5. Juli 2017 – IV ZR 121/15 –, juris

de Rechtsgrundlage gewonnen wurden, als zur Wahrnehmung polizeilicher Aufgaben „erforderlich" zu werten. Letztlich würden damit Eingriffe in grundrechtliche Gewährleistungen perpetuiert. Trotz dieser grundsätzlichen Bedenken konnte das Vorliegen der Tatbestandsvoraussetzungen des § 42 Absatz 1 PolG von mir nicht mit letzter Sicherheit bestritten werden.

Damit aber nicht genug: Von einem Landratsamt eines anderen Bundeslandes wurde ich darüber informiert, dass dort in zwei Fällen um die Übersendung von Ausländerakten gebeten worden sei. In beiden Fällen hat das Landratsamt die Übersendung aus datenschutzrechtlichen Gründen verweigert, nachdem man sich auch bei dem dortigen Landesdatenschutzbeauftragten entsprechend rückversichert habe. Hierauf wurde dem Landratsamt geantwortet: „Man kann nur hoffen, dass explizit diese Person nie einen Anschlag begeht."

Abgesehen davon, dass solche subtilen vorweggenommenen Schuldzuweisungen an denjenigen, der sich nach sorgfältiger Prüfung der Rechtslage an gesetzliche Vorgaben halten will, aus meiner Sicht völlig fehl am Platze sind, gehe ich von folgender Rechtslage aus:

Jede Datenübermittlung setzt einerseits eine Datenerhebungsbefugnis der anfordernden Stelle und andererseits eine Datenübermittlungsbefugnis der angefragten Stelle voraus (sog. Doppeltürenmodell). Die Frage war hier, ob die Ausländerbehörden berechtigt sind, der Polizei auf Anfrage Ausländerakten zur Verfügung zu stellen. Hierfür bedürfte es einer entsprechenden Übermittlungsbefugnis, die sich nur aus dem Aufenthaltsgesetz ergeben könnte. Eine solche Befugnis sehe ich nicht.

Das Aufenthaltsgesetz (AufenthG) regelt in seinem 4. Abschnitt die Bedingungen, unter denen Ausländerbehörden personenbezogene Daten verarbeiten dürfen. Dort finden sich auch spezielle Übermittlungsvorschriften. Einziger Ansatzpunkt für eine Übermittlungsbefugnis zugunsten der Polizei ist nach unserem Dafürhalten § 89 Absatz 2 AufenthG. Danach ist „die Nutzung der nach § 49 Absatz 3 bis 5 oder Absatz 7 bis 9 erhobenen Daten zulässig zur Feststellung der Identität oder der Zuordnung von Beweismitteln im Rahmen der Strafverfolgung oder zur polizeilichen Gefahrenabwehr. Sie dürfen, soweit und solange es erforderlich ist, den für diese Maßnahmen zuständigen Behörden übermittelt oder überlassen werden."

Abgesehen davon, dass die Voraussetzungen dieser Vorschrift im Kontext des SonAR-Projekts kaum vorliegen dürften, ist die Übermittlungsbefugnis der Ausländerbehörde durch die Verweisung auf einzelne Absätze des § 49 AufenthG beschränkt auf einzelne Daten, die im Zusammenhang mit der Überprüfung, Feststellung und Sicherung der Identität eines Ausländers erhoben wurden. Damit ist zugleich ausgeschlossen, dass andere oder weitere Daten übermittelt werden dürfen. Damit besteht für die Ausländerbehörde keine Berechtigung, der Polizei komplette Ausländerakten auszuhändigen. Damit würden auch Daten offenbart, die nach § 89 Absatz 2 i.V.m. § 49 AufenthG zulässigerweise nicht übermittelt werden dürfen.

Angesichts dessen habe ich das Landeskriminalamt gebeten, die örtlichen Polizeidienststellen auf die Rechtslage hinzuweisen, damit weitere Anforderungen von Ausländerakten künftig unterbleiben.

Dieses Projekt ist auch ein Beispiel dafür, wie nach dem Motto „Der Zweck heiligt die Mittel" fehlende oder unklare Rechtsgrundlagen für eine Datenverarbeitung im Zweifel „passend gemacht" werden. Als weiteres Beispiel hierfür mag Folgendes herhalten:

2.2.3 Erhebung personenbezogener Daten unbegleiteter minderjähriger Ausländer (UMA) bei Jugendämtern

Durch Presseveröffentlichungen wurde ich darauf aufmerksam, dass es Probleme mit der Erhebung personenbezogener Daten unbegleiteter minderjähriger Ausländer, im Fachjargon UMA, durch die Polizei bei Jugendämtern gab. Einige dieser Ämter hatten Zweifel an der Berechtigung, solche Daten ohne weiteres herauszugeben. Hierzu an anderer Stelle mehr (s. Kapitel 7.9). An dieser Stelle soll nur auf die Rolle der Polizei im Rahmen dieser Aktion eingegangen werden. Dabei geht es um Folgendes:

Im Zuge des Zustroms einer großen Zahl von Flüchtlingen kam auch eine große Zahl Minderjähriger ohne elterliche Begleitung in die Bundesrepublik. Nun sieht das Aufenthaltsgesetz auch für diese Personengruppe grundsätzlich vor, dass durch erkennungsdienstliche Maßnahmen (Lichtbilder, Abnahme von Fingerabdrücken) deren Identität zu sichern ist. Fakt war aber, dass durch den unkontrollierten Zustrom niemand genau wusste, wie vie-

le dieser Minderjährigen sich im Land aufhielten. Um dem auf den Grund zu gehen, sollten die Jugendämter dem Landeskriminalamt Baden-Württemberg zu jedem ihnen bekannten Minderjährigen einen Datensatz liefern. Aufgabe des Landeskriminalamts war es dann, über das Bundeskriminalamt, das eine entsprechende Datenbank verfügt, herauszufinden, welche der gemeldeten Minderjährigen noch nicht erkennungsdienstlich behandelt worden waren. Diese wurden dann den jeweils zuständigen Ausländerbehörden gemeldet, die in der Folge zusammen mit den jeweils zuständigen Polizeipräsidien und der technischen Unterstützung des Landeskriminalamts die erkennungsdienstlichen Behandlungen nachholten.

Datenschutzrechtlich betrachtet stellte sich die Einbeziehung des Landeskriminalamts als eine Art Sammelstelle für die Daten der Jugendämter und deren Weiterverarbeitung wie folgt dar:

Nach dem sog. „Doppeltürenmodell" des Bundesverfassungsgerichts verlangt ein Datenaustausch zwischen Behörden jeweils eigene Rechtsgrundlagen für die korrespondierenden Eingriffe[11]. Für die Erfassung der sich in der Obhut der Jugendämter des Landes befindlichen unbegleiteten minderjährigen Ausländer (Datenerhebung) sowie für die weitere Verarbeitung (Erhebung, Speicherung, Übermittlung) deren personenbezogenen Daten durch das Landeskriminalamt bedurfte es deshalb einer eindeutigen gesetzlichen Grundlage.[12] Eine solche konnte ich hier nicht erkennen.

Das Aufenthaltsgesetz (AufenthG) ermächtigt in § 86 Absatz 1 Satz 1 die „mit der Ausführung dieses Gesetzes betrauten Behörden", die für die Erfüllung ihrer Aufgaben „nach diesem Gesetz und nach ausländerrechtlichen Bestimmungen in anderen Gesetzen" erforderlichen Daten zu erheben. Nach § 71 Absatz 4 Satz 1 AufenthG sind (auch) die „Polizeien der Länder" für die erforderlichen Maßnahmen nach (u.a.) § 49 Absatz 2 bis 9 AufenthG zuständig. § 49 erlaubt die Sicherung der Identität eines Ausländers durch erkennungsdienstliche Maßnahmen, sofern die jeweiligen gesetzlichen Voraussetzungen für solche Maßnahmen vorliegen.

Zwar ist „die Polizei" nach dem Wortlaut des Gesetzes demnach berechtigt, erkennungsdienstliche Maßnahmen rein tatsächlich durchzuführen. Den einschlägigen Vorschriften lässt sich dagegen nicht ohne weiteres entnehmen, dass sie auch berechtigt wäre, im Vorfeld der Abnahme von Fingerabdrücken auch den Personenkreis zu ermitteln, der möglicherweise solchen Maßnahmen zu unterwerfen ist. Der auf den jeweiligen Einzelfall bezogene Wortlaut des § 49 Absatz 3 bis 5 und 7 bis 9 AufenthG („des" bzw. „eines" Ausländers) deutet vielmehr darauf hin, dass die Personen, die einer ED-Behandlung durch die Polizei unterzogen werden sollen, bereits konkret feststehen müssen, bevor die Polizei tatsächlich ins Spiel kommt.

War von daher schon zweifelhaft, ob die Polizei überhaupt berechtigt war, die Daten aller Jugendlichen zu erheben (darunter auch von solchen, die bereits erkennungsdienstlich behandelt waren), verstärkten sich die diesbezüglichen Zweifel noch im Hinblick auf die Rolle, die das Landeskriminalamt bei dieser Aktion spielte. Zwar verweist § 71 Absatz 4 Satz 1 AufenthG undifferenziert auf die Landespolizei. Gleichwohl entspricht es datenschutzrechtlichen Grundsätzen, dass eine Datenverarbeitung nur durch die Behörde oder Organisationseinheit einer Behörde zulässig ist, die diese Daten zur Erfüllung der ihr konkret übertragenen Aufgaben tatsächlich benötigt. Denn die in den Gesetzen enthaltene Zuständigkeitsverteilung zwischen einzelnen Behörden hat eine Schutzfunktion zugunsten der Bürger auch in datenschutzrechtlicher Hinsicht; wird diese gesetzliche Zuständigkeitsordnung nicht eingehalten, begründet dies grundsätzlich einen Datenschutzverstoß.[13] Angesichts dessen stellte sich die Frage, wie das Landeskriminalamt in den Kontext ausländerrechtlicher Maßnahmen eingebunden werden durfte. Die Ausführungen des Innenministeriums auf meine Anfrage, wonach das „Landeskriminalamt Baden-Württemberg die Daten der UMA, bei denen die ED-Behandlung nachzuholen ist, an die jeweils zuständige Ausländerbehörde [übermittelt], die die betroffenen Personen zur ED-Behandlung bei der zuständigen Polizeidienststelle vorlädt" [Hervorhebungen nicht im Original] belegen meines Erachtens, dass

11 BVerfG, Nichtannahmebeschluss vom 6. März 2014 – 1 BvR 3541/13 –, juris
12 BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83 u.a., – juris, Rn. 151
13 BVerwG, Urteil vom 9. März 2005 – 6 C 3/04 –, juris, Rn 26; BVerfG, Urteil vom 24. April 2013 – 1 BvR 1215/07 –, juris, Rn. 113

auch das Innenministerium davon ausging, dass die ausländerrechtlichen Zuständigkeiten ausschließlich bei anderen Behörden, inklusive anderer Polizeidienststellen, als dem Landeskriminalamt lagen. Eine wie immer geartete normenklare Zuständigkeit des Landeskriminalamts zu der gegenständlichen Datenerhebung und -sammlung sah ich jedenfalls nicht. Ebenso wenig konnte ich erkennen, auf welcher Rechtsgrundlage das Landeskriminalamt die erhaltenen Daten daraufhin hätte überprüfen dürfen, ob sich in dem erhobenen Kreis Personen befanden, die bereits ED-behandelt worden waren. Befugnisse der Polizei für einen Datenabgleich mit polizeilichen Dateien ergeben sich regelmäßig nur aus polizeirechtlichen Bestimmungen. Solche erschienen im gegebenen Zusammenhang allerdings nicht anwendbar.

Mir ist bewusst, dass das mit den Maßnahmen verbundene Ziel durchaus legitim war und ein wichtiges öffentliches Interesse darstellte. Gleichwohl gehört es zu meinen Aufgaben, darauf zu achten habe, dass sich das staatliche Handeln streng im Rahmen des (datenschutz-) rechtlich Zulässigen hält. Hieran hatte und habe ich in diesem Fall insbesondere in Bezug auf die Rolle des Landeskriminalamts in dieser Angelegenheit erhebliche Zweifel, die auch das Innenministerium mit seiner Argumentation nicht restlos beseitigen konnte.

Nicht nur die Polizei hat allerdings hin und wieder das Problem, tatsächliches Wollen und rechtliches Dürfen sauber unter einen Hut zu bringen. Davon zeugt folgende Angelegenheit, die den Geheimdienst betrifft.

2.2.4 Die Reichsbürger und der Verfassungsschutz

Tragische oder auch nur ärgerliche Vorkommnisse im Zusammenhang mit einer Bewegung, die bislang eher ein Schattendasein geführt hatte und allenfalls unter dem Attribut „problematisch" behördlicherseits zur Kenntnis genommen wurde, ließen die der Szene der sog. „Reichsbürger" zuzurechnenden Personen verstärkt ins Blickfeld der Sicherheitsbehörden rücken. Auch wenn ich gut nachvollziehen kann, dass man den nicht unerheblichen Gefahren, die von solchen Gruppierungen ausgehen können, versucht Herr zu werden, muss ich doch auch hier darauf bestehen, dass dies nur im Rahmen des geltenden Rechts zulässig ist.

Durch Zufall erfuhr ich von einem Info-Brief des Gemeindetags Baden-Württemberg, in dem die Mitglieder auf einen „Service" des Landesamts für Verfassungsschutz Baden-Württemberg hingewiesen wurden, der es ihnen erleichtern sollte, Bürgerinnen und Bürger, die den „Reichsbürgern und Selbstverwaltern" zuzurechnen seien oder bei denen dies nicht auszuschließen sei, dem Geheimdienst zu melden. Nach der Rechtsgrundlage für solche Datenübermittlungen gefragt, stellte sich schnell heraus, dass die Sache nicht ganz so einfach war. Denn das Landesverfassungsschutzgesetz (LVSG) enthält in § 9 Absatz 1 eine Spezialregelung für die Datenübermittlung von Landesbehörden an das Verfassungsschutzamt. Die Vorschrift zählt im Einzelnen auf, welche Behörden zur Übermittlung befugt sind. Die Gemeinden werden dabei allerdings ausgenommen. Da auch die sonstigen allgemeinen Datenübermittlungsbefugnisse nach dem Landesdatenschutzgesetz aufgrund der Sondervorschrift ausgeschlossen sind, sah ich keine Berechtigung der Gemeinden, den „Service" des Verfassungsschutzes in Anspruch zu nehmen. Den Gemeindetag habe ich entsprechend informiert.

Als Reaktion hierauf bekam ich Post vom Innenministerium. Dort vertrat man die Auffassung, der Umstand, dass die Gemeinden in § 9 Absatz 1 LVSG nicht genannt seien, könne doch nur auf ein Versehen des Gesetzgebers zurückzuführen sein. Dieser habe sehr wohl die Gemeinden auch in die Übermittlungsregelung einbeziehen wollen. Dass das weder im Gesetzestext noch in der Gesetzesbegründung auch nur ansatzweise zum Ausdruck gekommen sei, sei unerheblich. Nichts deute auf eine bewusste Ausnahme der Kommunen hin. Mein Hinweis darauf, dass es rätselhaft sei, weshalb das Fehlen jeglichen Hinweises auf die Gemeinden denn ein Argument gerade dafür dienen solle, dass sie doch gemeint seien, und dass dies mit den herkömmlichen juristischen Auslegungsmethoden nicht vereinbar sei, stieß beim Innenministerium aber auf taube Ohren. Letztlich habe ich aber von weiteren Maßnahmen abgesehen, da eine Änderung des Landesverfassungsschutzgesetzes vorgesehen ist, die den rechtlichen Mangel behebt. Diese Änderung ist aber auch nötig.

Mit einer gewissen Genugtuung habe ich allerdings zur Kenntnis genommen, dass es auch Kommunen gibt, die nicht nach dem Motto „der Zweck heiligt die Mittel" vorgehen. So fragte mich eine Stadt, die um die entsprechenden

Informationen angegangen wurde, wie denn meine Meinung zu dieser Rechtslage sei; man selbst habe Zweifel an der Übermittlungsbefugnis. Ich konnte die Stadt in diesen Zweifel nur bestärken, was dazu führte, dass von einer Datenübermittlung abgesehen wurde. Mehr solcher datenschutzsensiblen Behörden würde ich mir wünschen!

2.3 Was es sonst noch gab

2.3.1 Zuverlässigkeitsüberprüfung

Regelmäßig haben meine Vorgänger im Amt in ihren Tätigkeitsberichten den Umstand beklagt, dass insbesondere bei Großveranstaltungen von denjenigen, die dort – in welcher Funktion auch immer – tätig werden sollen oder wollen, grundsätzlich verlangt wird, in die Überprüfung ihrer Zuverlässigkeit durch die Sicherheitsbehörden einzuwilligen. Schon vor mehr als zehn Jahren hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder diese allein auf eine Einwilligung gestützte Datenverarbeitung kritisiert. Denn an der Freiwilligkeit und damit Wirksamkeit solcher Einwilligungserklärungen bestehen immer wieder erhebliche Zweifel. Getan hat sich seitdem nichts. Was ursprünglich im Rahmen der Fußballweltmeisterschaft 2006 in Deutschland (angesichts der weltweiten Bedeutung dieses Ereignisses) als einmaliges Verfahren verkauft und unter dieser Voraussetzung von meinem Vorgänger akzeptiert wurde,[14] hat sich mittlerweile bundesweit in unterschiedlichen Ausprägungen als Regelverfahren etabliert. Ärgerlich ist, dass sich meine Dienststelle immer wieder aufs Neue mit dieser Problematik befassen muss, obwohl der Gesetzgeber mittlerweile mehr als genug Zeit hatte, hier für eine Klärung der Rechtslage zu sorgen. Ein Beispiel hierfür:

Mit dem Betreff „EILT! EILT! EILT!" wandte sich der Rechtsvertreter eines Konzertveranstalters an mich, weil er erhebliche datenschutzrechtliche Zweifel an der Art und Weise hatte, in der seine Mandantschaft von der Gemeinde, auf deren Gebiet das Konzert stattfinden sollte, und von der Polizei zur Durchführung einer „Akkreditierung" des vor Ort eingeplanten Personals verpflichtet wurde. Im Ergebnis konnte ich die Zweifel nur bestätigen. Zum einen betraf dies die verschlungenen Pfade, welche die erhobenen Daten nehmen sollten. Der Rechtsanwalt beschrieb das folgendermaßen: *„Das Verfahren zur Datenerhebung soll so ausgestaltet werden, dass unsere Mandantin die Daten bei ihren Subunternehmern erhebt und an die Stadt xxx weitergibt. Die Stadt xxx wiederum beabsichtigt, die Daten dann an die Polizei xxx zu übermitteln, die die eigentliche Sicherheitsüberprüfung aufgrund des Datenabgleichs vornehmen soll. Die Polizei übermittelt sodann die Ergebnisse an die Stadt xxx mit dem Vermerk, ob der Mitarbeiter akzeptiert wird oder nicht. Der Veranstalter wiederum informiert dann seine Subunternehmer.*" Nachfragen bei der Stadt und bei der Polizei ergaben keine zufriedenstellende Antwort darauf, welche Rolle der Stadt in dieser Informationskaskade eigentlich zukam. Denn niemand konnte erklären, weshalb die Subunternehmer die Daten ihrer Mitarbeiter nicht gleich direkt der Polizei hätten zuleiten können, noch was die Stadt mit den Informationen über die Zuverlässigkeit oder Unzuverlässigkeit von Mitarbeitern der Subunternehmen überhaupt hätte anfangen können. Letztlich war man sich einig, dass die Stadt hier völlig außen vor zu bleiben hatte und das Konzept entsprechend umgeschrieben werden musste. Was blieb war die aus meiner Sicht nach wie vor völlig unbefriedigende Situation, dass die polizeiliche Überprüfung des Personals ausschließlich auf der „freiwilligen" Einwilligung der jeweils betroffenen Personen beruhte. Hier von Freiwilligkeit zu sprechen, wenn der Arbeitgeber von seinen Mitarbeitern verlangt, ihre Daten an die Sicherheitsbehörden herauszugeben, damit er im Rücklauf erfährt, wen er einsetzen kann und gegen wen die Polizei Bedenken hat, erscheint mir mehr als problematisch. Daran kann auch die schönste aufklärende Datenschutzinformation nichts ändern. Die ab Mai 2018 anwendbare Datenschutz-Grundverordnung wird hier deutlich: „Es sollte nur dann davon ausgegangen werden, dass sie [die betroffene Person] ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden. … 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 … und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechts-

14 27. Tätigkeitsbericht 2006, LT-Drs. 14/650, Seite 23 ff.

grundlage liefern." Ob künftig solche Zuverlässigkeitsüberprüfungen auf der Basis individueller Einwilligungen jedenfalls im Arbeitgeber-/Arbeitnehmer-Verhältnis noch möglich sein werden, wird sich zeigen. Was mir allerdings dringend notwendig erscheint, und damit greife ich die wiederholt erhobene Forderung nachdrücklich auf, ist eine klare gesetzliche Regelung für die Polizei, welche diese nicht nur dazu ermächtigt, solche Überprüfungen überhaupt durchführen zu dürfen, sondern auch eindeutig den Rahmen absteckt, innerhalb dessen sich solche Datenverarbeitungen abspielen dürfen; angefangen vom Umfang der Überprüfung über die Frage, wer wie über das Ergebnis informiert werden darf bis hin zur Frage, wann die Daten wieder zu löschen sind. Meine diesbezüglich an das Innenministerium gerichtete Aufforderung wurde bisher leider noch nicht beantwortet.

In ganz anderem Zusammenhang traf mich das Akkreditierungsthema erneut. Anlässlich des G20-Gipfels im Juli 2017 in Hamburg wurde nämlich auch Journalisten Zugang zu beschränkten Bereichen nur gewährt, wenn sie zuvor erfolgreich ein Akkreditierungsverfahren durchlaufen hatten. Auch dabei erfolgte eine Überprüfung der Betroffenen durch die Sicherheitsbehörden „auf freiwilliger Basis". Ergebnis war, dass einzelnen Journalisten die Akkreditierung wegen Sicherheitsbedenken erst gar nicht erteilt oder nachträglich entzogen wurde. Wie sich herausstellte, beruhten einige der negativen Gefahreneinschätzung der Polizei auf Namensverwechslungen oder sie wurden auf fehlerhafter Datenbasis getroffen.

Die freie Presseberichterstattung ist ein hohes Gut. Wird diese be- oder verhindert, indem man Journalisten ausschließt, bedarf es hierfür sehr guter und belastbarer Gründe. Beruht der Ausschluss auf einer polizeilichen Gefahreneinschätzung, muss die Datenbasis hierfür aktuell sowie tatsächlich und rechtlich zutreffend sein. Ob dies in den Fällen, in denen Journalisten aus Baden-Württemberg vom Ausschluss betroffen waren, immer so war, prüfe ich gerade. Erste Stellungnahmen in diesen Fällen wurden bereits eingeholt, weitere stehen noch aus.

2.3.2 Bodycam

Der allgemein zunehmende Einsatz von Videotechnik macht auch vor der Polizei nicht halt. Ausnahmsweise aber nicht zum Schutz der Allgemeinheit oder um Straftäter zu fassen, sondern diesmal in erster Linie aus Gründen des Eigenschutzes sollten Polizeibeamtinnen und Polizeibeamte mit sogenannten Bodycams, am Körper getragene Aufnahmegeräte, ausgerüstet werden. Hintergrund ist die bedauerliche Tatsache, dass die Zahl der körperlichen Angriffe auf Polizeibeamtinnen und -beamte in den letzten Jahren kontinuierlich gestiegen ist. Die Bodycam sollte diesbezüglich deeskalierend und abschreckend wirken.

Da diese neue Form der Datenverarbeitung gesetzlich bislang so nicht vorgesehen war, war eine entsprechende Änderung des Polizeigesetzes nötig. Dabei ging man dann gleich „in die Vollen". Nicht erst dann, wenn es tatsächlich zu körperlichen Angriffen auf Polizeibeamte und Dritte kommt, sollte die filmische Dokumentation des Geschehens ermöglicht werden. Mit der – wenn auch nur flüchtigen, weil im Minutentakt immer wieder überschriebenen – Aufnahme sollte vielmehr bereits begonnen werden dürfen, wenn dies allgemein zum Schutz der genannten Personen erforderlich erschien (sog. Pre-Recording). Schließlich wurden auch noch Tonaufnahmen zugelassen. Meine Kritik richtete sich insbesondere gegen die Regelung des Pre-Recording, das angesichts der Weite seiner Anwendungsvoraussetzungen nach meiner Auffassung in keinem Verhältnis mehr zum Eingriff in die Datenschutzgrundrechte der Betroffenen stand. Wobei dabei auch ins Gewicht fiel, dass zum einen der eigentliche Gesetzeszweck, nämlich die Verhinderung von körperlichen Angriffen auf Polizeibeamtinnen und -beamte, für den Einsatz des Pre-Recording keine Rolle mehr spielen sollte, und zum anderen die bis zu 60 Sekunden langen Aufnahmen nur dann dauerhaft gespeichert werden sollen, wenn es zur eigentlichen Aufnahme infolge eines tatsächlichen Angriffs gekommen war. Da dies, wie sich bei der Evaluation später herausstellte, allerdings nur in wenigen Fällen so kam, war der Großteil der Aufnahmen überflüssig, sodass der Gedanke an eine Art der grundsätzlich unzulässigen Vorratsdatenspeicherung nahe lag. Meine im Gesetzgebungsverfahren vorgetragenen Bedenken führten tatsächlich zu einem Überdenken des Gesetzentwurfs, allerdings anders, als ich mir dies gewünscht hätte. Denn anstatt auf das aus meiner Sicht rechtlich bedenkliche Pre-Recording zu verzichten, wurde plötzlich die Voraussetzung gestrichen, dass überhaupt noch eine Gefahr für Leib oder Leben von Polizisten oder Dritten im Raum stehen musste. Pre-Recording war vielmehr nun ganz allgemein erlaubt, sobald es nur irgendwie um Gefahrenabwehr im

weitesten Sinne ging. So funktioniert manchmal Gesetzgebung!

Ein erster Bericht über die praktischen Erfahrungen der Polizei mit diesem neuen Hilfsmittel kommt erwartungsgemäß zu einem positiven Gesamturteil. Danach scheinen bei bestimmten Bevölkerungsgruppen solche Kameras tatsächlich deeskalierend zu wirken. Bei vielen Einsatzkräften hat dies den Wunsch geweckt, die Voraussetzungen für den Bodycam-Einsatz zu lockern und die Einsatzmöglichkeiten zu erweitern. Man muss kein Prophet sein um vorauszusagen, dass das letzte Kapitel in dieser Angelegenheit noch nicht geschrieben ist.

2.3.3 Prüfung der Antiterrordatei ATD

Die Antiterrordatei (ATD) ist eine gemeinsame Datenbank von 38 deutschen Sicherheitsbehörden, die auf der Rechtsgrundlage des Antiterrordateigesetzes zur Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland errichtet wurde. Neben dem Bundeskriminalamt (BKA), der Bundespolizei, dem Bundesamt für Verfassungsschutz, dem Militärischen Abschirmdienst, dem Bundesnachrichtendienst und dem Zollkriminalamt nehmen die Länderpolizeien und die Landesämter für Verfassungsschutz gleichermaßen teil.

Gemäß § 10 Absatz 2 des Antiterrordateigesetzes (ATDG) sind die Bundesbeauftragte für Datenschutz und die Landesbeauftragten für Datenschutz im Rahmen ihrer jeweiligen Prüfungszuständigkeiten verpflichtet, mindestens alle zwei Jahre die Durchführung des Datenschutzes, konkret die Rechtsmäßigkeit der in der Antiterrordatei (ATD) gespeicherten Datensätze zu kontrollieren. Bereits im letzten Tätigkeitsbericht[15] hatten wir über die Antiterrordatei berichtet. Ziel der Datei ist es, schon im Vorfeld zu erkennen, ob ein bestimmtes Verhalten typischerweise dem eines potenziellen Attentäters ähnelt. Darüber hinaus soll verhindert werden, dass jemand von einer Behörde verfolgt, von einer anderen aber geduldet oder vielleicht sogar gefördert wird. Diese sog. Verbunddatei wurde auf der Rechtsgrundlage des Antiterrordateigesetzes zur Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland errichtet und ist als Index-Datei ausgestaltet. Anhand einer vorab gebildeten Stichprobe prüften meine Mitarbeiter im Berichtszeitraum die Speicherpraxis des baden-württembergischen Landesamtes für Verfassungsschutz (LfV). Im ersten Quartal 2016 einigten sich die Landesdatenschutzbehörden und die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) darauf, ein standardisiertes Reportpaket vom BKA anzufordern, um eine bundesländerübergreifende Einheitlichkeit der Prüfpraxis der ATD zu erreichen. Entsprechend der Einigung baten wir das LfV im Vorfeld der Prüfung darum, die im Zeitraum von Oktober 2015 bis April 2016 angefallenen Protokolldaten der im LfV auf die ATD zugriffsberechtigten Personen beim Bundeskriminalamt anzufordern. Die Prüfung selbst erfolgte anhand des Aktenrückhalts der jeweiligen Einspeicherungen und durch einen zusätzlichen Abgleich mit den angeforderten Protokolldatensätzen der ATD. Auf Basis eines Zufallsprinzips wurden für die Kontrolle insgesamt zehn Einspeicherungen ausgewählt, welche zu einem Großteil erst im Jahre 2016 eingespeichert worden waren.

Grundlage für die Befüllung der ATD ist das sogenannte Nachrichtendienstliche Informationssystem (NADIS), eine Verbunddatei der Verfassungsschutzbehörden des Bundes und der Länder. NADIS wird auf der Basis des § 6 des Bundesverfassungsschutzgesetzes (BVerfSchG) geführt. Die Befüllung der ATD aus NADIS heraus erfolgt ausschließlich automatisiert. Voraussetzung hierfür ist, dass zuvor die Speicherrelevanz und die Voraussetzungen zur Einspeicherung in die ATD nach § 2 ATDG positiv festgestellt wurde. Die Nutzung der ATD durch die zugriffsberechtigten Mitarbeiter des LfV erfolgt über eine Volltextsuche. Im Falle eines Treffers werden der abfragenden Stelle in einem ersten Schritt zunächst nur sog. Grunddaten des Treffers angezeigt. Zu den Grunddaten zählen im Wesentlichen die Daten, die der Identifizierung einer Person dienen (vgl. § 3 Absatz 1 Nummer 1 lit. a ATDG). Vollen Lesezugriff auf die erweiterten Grunddaten des § 3 Absatz 1 Nummer 1 lit. b ATDG erhält das LfV erst nach einer gesondert zu stellenden Erkenntnisanfrage an die einspeichernde/verantwortliche Behörde. Letztere prüft in einem solchen Fall, ob die Voraussetzungen einer datenschutzrechtlichen Übermittlungsbefugnis gegeben sind und ob der angeforderte Datensatz für die anfragende Behörde freigegeben wer-

15 32. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Baden-Württemberg 2014/2015, Landtag von Baden-Württemberg, LT-Drs. Nr. 15/7990, S. 41f.

den kann. Erkenntnisanfragen und Freigabeverfahren erfolgen über die Nutzeroberfläche der ATD und werden stets gesondert auf dem Protokollserver das BKA protokolliert.

§ 2 Satz 1 ATDG verpflichtet die beteiligten Behörden, bereits erhobene Daten nach § 3 Absatz 1 in der Antiterrordatei zu speichern. Unsere Prüfung zeigte, dass ein überwiegende Anteil der ATD-Speicherungen im Mai 2016, das heißt nach Ankündigung unseres Kontrollbesuchs, erfolgte. Auffallend war auch, dass das LfV nur zögerlich in die ATD einspeichert. Dies entspricht den Prüfergebnissen anderer Bundesländer: Die ATD wird von den beteiligten Stellen als für die tägliche Arbeit nicht zielführend verstanden, da die Datei überwiegend vor allem der Kontaktanbahnung zu anderen Behörden dient. Unmittelbare Recherchen für operative Zwecke, das heißt ein Direktzugriff auf die in der Datei befindlichen Datensätze, sind innerhalb der ATD nur im Rahmen einer gesondert zu begründenden Eilfallregelung möglich. Auch das LfV nutzt die ATD ausschließlich zur Kontaktanbahnung. Ein tatsächlicher Austausch der Datensätze über die Kommunikationsstruktur der ATD erfolgt nicht. Dieses Ergebnis wurde auch durch Sichtung der Protokolldatensätze bestätigt: Von Oktober 2015 bis April 2016 erfolgten durch das LfV lediglich drei Suchläufe innerhalb der ATD. Darüber hinaus griff das LfV in keinem Fall auf erweiterte Grunddaten anderer Behörden zu; in keinem Fall wurde ein Eilfall mit Direktzugriffsmöglichkeiten angenommen.

Sämtliche Erkenntnisse, die durch die Mitarbeiter des LfV in die ATD eingespeichert werden, werden gesondert im dort geführten Aktenrückhalt dokumentiert. Innerhalb des LfV werden keine Personen-, sondern Sachakten geführt; dies bedeutet, dass Umstände, welche für die Bewertung der Frage, ob und welche Informationen zu einer Person vorliegen, an mehreren Stellen gefunden werden können. Der Aufwand für unsere Kontrolle war in manchem Einzelfall nur schwer zu bewältigen, da eine zusammenfassende Begründung für die Speicherung in NADIS in den Unterlagen nicht vorhanden war. Für zukünftige Kontrollen wäre es hilfreich, wenn das LfV Wege finden würde die eine Zuordnung zum Aktenrückhalt vereinfachen. Auf diese Weise wäre ein zügiges Auffinden der wesentlichen Erkenntnisse aus den mitunter vielen Ordnern zu der betreffenden Person gewährleistet. Zahlreiche, mehrbändige Sachakten mussten durchgesehen werden, um prüfen zu können, ob die personenbezogenen Voraussetzungen einer Speicherung in NADIS gegeben waren. Der zweite Prüfschritt, das heißt die Frage, ob die Überführung von NADIS in die ATD rechtmäßig erfolgte, war aufgrund des vom LfD verwendeten Formblattes deutlich einfacher zu prüfen.
Bei unserer Prüfung haben wir keinen datenschutzrechtlichen Verstoß feststellen können. Während der gesamten Prüfung haben die Mitarbeiter des LfV konstruktiv mit dem LfDI zusammengearbeitet und ihrer Pflicht zur Unterstützung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit (vgl. § 29 des Landesdatenschutzgesetzes) vollends entsprochen.

2.3.4 Kontrolle der Falldatei Rauschgift

Anlässlich einer deutschlandweit unter den Datenschutzaufsichtsbehörden abgestimmten datenschutzrechtlichen Prüfung der „Falldatei Rauschgift" (FDR) führten meine Mitarbeiter Kontrollbesuche beim Landeskriminalamt durch. Hierbei wurde anhand einer Stichprobe von 48 Datensätzen die Speicherpraxis der baden-württembergischen Polizei überprüft.

Die FDR ist Teil der beim Bundeskriminalamt geführten bundesweiten INPOL-Datenbank. Bei Verstoß gegen das Betäubungsmittelgesetz (BtMG) kann die Polizei Beschuldigte in der FDR speichern, um weitere Straftaten zu verhindern und zukünftige Ermittlungen zu erleichtern. Speicherungen in die FDR sind zulässig, wenn die Voraussetzungen des § 8 Absatz 1, 2 i.V.m. § 11 Absatz 2 Satz 3 des Bundeskriminalamtgesetzes (BKAG) vorliegen. Ein Merkblatt des Landeskriminalamtes Baden-Württemberg legt landesinterne Erfassungskriterien fest. Erfassungsgrundlage sind die „Rauschgiftsofortmeldungen", entsprechend dem „Informationsaustausch Rauschgiftkriminalität" (PDV 386), sowie die POLAS-Belege mit jenen Straftaten, welche die Erfassungskriterien erfüllen.

In Baden-Württemberg erfolgen Speicherung in und Löschung aus der FDR dezentral durch die zuständigen Dezernate der Polizeipräsidien. Diese entscheiden eigenverantwortlich über das „Ob" und die Dauer der FDR-Speicherungen. Entsprechend sind den Präsidien eigene Schreibrechte an der Verbunddatei eingeräumt. Lediglich Rauschgifttote werden zentral durch das LKA erfasst. Eine Überprüfung der Polizeipräsidien durch das LKA erfolgt insofern oberflächlich: Anhand der durch die Polizeiprä-

sidien per E-POST übermittelten Rauschgiftsofortmeldungen wird lediglich abgeglichen, ob die Mindestmengen für eine FDR-Speicherung gegeben sind. Ungeprüft bleibt, ob die Präsidien zu Recht die Voraussetzungen der § 8 Absatz 1, 2 i.V.m. § 11 Absatz 2 Satz 3 BKAG angenommen haben und ob die richtigen Speicherfristen vergeben worden sind. Für die Prüfung forderte das LKA von den Polizeipräsidien die zu der Stichprobe gehörigen, dort gespeicherten Daten, die dazugehörige Kriminalakten- und den POLAS-Bestand an.

Diese dezentrale Struktur erschwerte die Prüfung. Der Umfang des zur Prüfung vorgelegten Aktenrückhalts variierte je nach Polizeipräsidium erheblich. Während in einigen Fällen – wie notwendig – die gesamten Ermittlungsakten vorlagen, übersandten andere Präsidien nur die POLAS-Erfassungsbelege. Ein Polizeipräsidium übersandte lediglich die an die Staatsanwaltschaft übersandten Strafanzeigen, sodass in diesen Fällen der Aktenrückhalt nachgefordert werden musste. Anhand des unvollständig vorgelegten Aktenrückhalts konnte z.B. oftmals nicht nachvollzogen werden, weshalb in Fällen, in denen lediglich geringe Mengen Betäubungsmittel aufgefunden wurden, eine Einspeicherung wegen Verkaufs erfolgte. Eine umfassende Dokumentation oder Vorlage der vollständigen Akten hätte diese Lücke schließen können. In einem Fall war sogar bereits der vollständige Aktenrückhalt des Beschuldigten durch das Polizeipräsidium gelöscht worden. Ohne Aktenrückhalt kann im Prüfzeitpunkt nicht mehr nachvollzogen werden, ob der Tatvorwurf eine Einspeicherung in die FDR rechtfertigte. Die zugehörige FDR-Speicherung war daher sofort zu löschen.

Rechtswidrig war zudem auch die Speicherung zweier Kinder in die FDR, da hier mangels Strafmündigkeit bereits keine Anknüpfungsstrafbarkeit gegeben war. Bei der Kontrolle wurden zwei Speicherungen festgestellt, bei denen die Beschuldigten im Tatzeitpunkt erst 12 bzw. 13 Jahre alt – also Kinder – waren. Diese Fälle hätten nicht in die FDR aufgenommen werden dürfen.

Gemäß § 2 Absatz 1 BKAG sind in die FDR als Verbunddatei nur Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung aufzunehmen. Eine Straftat hat erheblicher Bedeutung, wenn sie mindestens dem Bereich der mittleren Kriminalität zuordenbar ist, den Rechtsfrieden empfindlich stört und dazu geeignet ist, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen. Eine konkrete Betrachtung nach Art und Schwere der Tat ist erforderlich. Problematisch sind hierbei insbesondere Bagatellfälle, bei denen nur eine „geringe Menge" im Sinne des BtMG aufgefunden wird. In einem Fall wurde ein Beschuldigter in die FDR eingespeichert, obwohl die sichergestellte Menge deutlich unter den Mindestmengen der PDV 386 lag.

Liegen die Speichervoraussetzungen des § 8 Absätze 1, 2 i.V.m. § 11 Absatz 2 Satz 3 BKAG vor, muss dies entsprechend nachvollziehbar dokumentiert wurden. § 8 Absatz 2 BKAG verpflichtet die speichernden Stellen zur Einzelfallprüfung und zur Erstellung einer dazugehörigen individuellen Negativprognose. Aus ihr muss sich zweifelsfrei ergeben, dass Grund zu der Annahme besteht, dass Strafverfahren gegen den Beschuldigten oder Tatverdächtigen zu führen sind. Der speichernden Behörde wird diesbezüglich kein Ermessen eingeräumt. Die Negativprognose ist in POLAS BW entsprechend einzelfallbezogen zu begründen und schriftlich zu dokumentieren . Diese Einzelfallbegründung darf sich nicht in der bloßen Wiederholung der Standardbegründungen der vorformulierten Auswahlmöglichkeiten erschöpfen, sondern muss u.a. auf den jeweiligen konkreten Fall und die Täterpersönlichkeit abstellen. In einer Vielzahl der Prüffälle war die Negativprognose unzureichend dokumentiert. Überwiegend fehlte die notwendige ergänzende Begründung der Wiederholungsgefahr. Individuelle Erwägungen wurden nicht festgehalten. Auch die Rechtsprechung verlangt, dass die Wiederholungsgefahr begründende Anhaltspunkte in einer auf den Einzelfall bezogenen, auf schlüssigen, verwertbaren und nachvollziehbar dokumentierten Tatsachen beruhenden Entscheidung festzuhalten sind. Ob durch den jeweiligen Sachbearbeiter überhaupt eine Prognoseentscheidung getroffen wurde und auf welcher Tatsachengrundlage bzw. aus welchen Gründen dies geschah, war nicht erkennbar.

Positiv fiel im Rahmen der Kontrolle auf, dass die Präsidien in mehreren Fällen statt der Regelspeicherfrist – bei Erwachsenen bis zu zehn Jahre, bei Jugendlichen bis zu fünf Jahre – verkürzte Speicherfristen von höchstens zwei Jahren festgelegt hatten.

Im Ergebnis zeigte sich bei dem Kontrollbesuch ein bereits bekanntes, strukturelles Dokumentationsdefizit, das nicht nur den Bereich

der FDR, sondern sämtliche INPOL-relevanten Dateien betreffen kann, welche aus POLAS BW befüllt werden. Die fehlende Dokumentation erhält vor dem Hintergrund der Fortentwicklung des Verfahrens „Polizeilicher Informations- und Analyseverbund" (PIAV) besondere Bedeutung. Als nächstes Teilmodul dieses Systems soll der Bereich „Betäubungsmittelmissbrauch" realisiert werden. Hierbei sollen die Daten der FDR in PIAV migriert werden. Aus meiner Sicht ist es daher zwingend, dass die Polizeipräsidien vor Migration der Daten sämtliche FDR-Speicherungen einer Prüfung unterziehen. Es dürfen nur solche Daten in eine bundesweite Verbunddatei gespeichert werden, die rechtmäßig in die FDR eingespeichert wurden. Der LfDI steht diesbezüglich im Austausch mit dem LKA.

2.3.5 SKB-Datenbank

Im 32. Tätigkeitsbericht 2014/2015 hatte ich bereits über die „Arbeitsdatei Szenekundige Beamte" (SKB-Datenbank) berichtet.[16] Anlass, mich mit dieser polizeilichen Datensammlung erneut zu befassen, hatte ich aufgrund mehrerer Eingaben von Bürgern, denen durch entsprechende Auskünfte seitens der Polizei bekannt wurde, dass und wie sie in dieser Datenbank gespeichert waren. In einem dieser Fälle ging es um Folgendes:

Dem Betroffenen, der nach polizeilichen Erkenntnissen der sog. Ultra-Szene eines Bundesliga-Fußballvereins zuzurechnen und in dieser Szene als „offizieller" Szene-Fotograf bekannt war, war in der SKB-Datenbank mit der Begründung, er sei als Szeneangehöriger regelmäßig im Zusammenhang mit Fußballspielen angetroffen worden, als „Störer" gespeichert worden. Auf seinen Antrag, die Eintragung zu löschen, da er nicht erkennen könne, wann und wo er über den reinen Besuch von Fußballspielen hinaus gegen die öffentliche Sicherheit und Ordnung verstoßen habe, teilte ihm das Polizeipräsidium unter Zurückweisung seines Löschungsantrags Folgendes mit: „Durch Ihre Tätigkeit als einer der offiziellen Fan-Fotografen der … Ultra-Szene begünstigen und fördern Sie die Existenz der Ultra-Szene. Aus diesem Grund sind Sie als Störer … gespeichert. Sollten Sie sich an dem Begriff „Störer" stören, wäre auch eine Speicherung als Kontakt- und Begleitperson möglich." Das war mir jetzt in der Tat neu, dass die Polizei freistellt die Personengruppe zu wählen, unter der man in ihren Dateien gespeichert werden möchte!

Zur Rechtslage: Soweit in der SKB-Datenbank personenbezogene Daten für präventivpolizeiliche Zwecke auf der Grundlage des § 37 Absatz 1 des Polizeigesetzes (PolG) gespeichert werden, muss erkennbar sein, welcher der in § 20 Absatz 2 bis 5 PolG genannten Personengruppen der Betroffene angehört. § 20 Absatz 2 PolG nennt insoweit (u.a.) den sog. Handlungsstörer im Sinne des § 6 PolG sowie nach § 20 Absatz 3 Nummer 2 PolG (u.a.) Kontakt- und Begleitpersonen von Personen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie künftig Straftaten begehen. Die Zuordnung eines Betroffenen zu einer dieser Personengruppen erfordert das Vorliegen jeweils eigener Voraussetzungen und ist nicht beliebig austauschbar. So bedarf es insbesondere für die Zuordnung zur Personengruppe des § 20 Absatz 3 Nummer 2 PolG zunächst einer Zielperson, bei der tatsächliche Anhaltspunkte dafür sprechen, dass sie straffällig werde. Bloße Vermutungen reichen nicht aus. Besteht hinsichtlich einer solchen Zielperson eine entsprechende Indizienlage, so kommt es für die Speicherung eines Betroffenen als Kontakt- und Begleitperson künftiger Straftäter darauf an, ob dieser „zu dem künftigen Straftäter persönliche oder geschäftliche Beziehungen unterhält. Flüchtige Beziehungen reichen nicht aus. Eine Begleitperson muss mit dem künftigen Straftäter wiederholt zusammengetroffen oder wenigstens einmal eine Zeit lang zusammen gewesen sein. Die Verbindung muss eine gewisse Intensität aufweisen"[17].

Vor dem Hintergrund dieser Rechtslage bezweifelte ich gegenüber dem Polizeipräsidium die Berechtigung, den Betroffenen in der SKB-Datenbank zu speichern. Nach fast sechs Monaten umfassender Prüfung teilte das Polizeipräsidium schließlich mit, dass die Speicherungsvoraussetzungen nicht ausreichend dokumentiert worden und dass die Daten deshalb gelöscht worden seien. In anderen, vergleichbaren Fällen wurde ebenso verfahren. Erneut wurde hier deutlich, dass die Speicherberechtigung in polizeilichen Dateien in vielen Fällen – möglicherweise allein - daran scheitert, dass es an der erforderlichen Dokumentation der Gründe fehlt, die für die Speicherung maßgeb-

16 Landtags-Drucksache Nr. 15/7990, Seite 55
17 VG Karlsruhe, Urteil vom 26. August 2015 – 4 K 2113/11 –, juris, Absatz-Nr. 95

lich waren. Es bleibt zu hoffen, dass sich die polizeiliche Praxis hierauf einstellt – im eigenen und allgemeinen Interesse!

2.3.6 Vergabe fünfjähriger Laufzeit bei einem Fall geringer Bedeutung

Sämtliche zur Person gespeicherten Ermittlungsverfahren mussten gelöscht werden, da im Rahmen unserer Prüfung festgestellt wurde, dass für das zuletzt gespeicherte Ermittlungsverfahren eine zu lange Speicherfrist gewählt worden und die rechtmäßige Speicherfrist bereits verstrichen war.

In einem Fall, in dem es um die Rechtmäßigkeit der Speicherung einer im Jahr 2008 durchgeführten erkennungsdienstlichen Behandlung ging, teilte uns das zuständige Polizeipräsidium auf Anfrage mit, dass der Betroffene mit insgesamt zwölf Fällen im Polizeilichen Auskunftssystem der Landespolizei (POLAS BW) einliege. Die Prüfung ergab, dass bei dem zuletzt gespeicherten Körperverletzungsdelikt aus dem Jahr 2013 zu Unrecht eine fünfjährige anstatt einer dreijährigen Löschfrist gewählt worden war. Zum Zeitpunkt des Schriftwechsels waren diese drei Jahre bereits verstrichen. Dies hatte zur Folge, dass alle zur Person des Petenten vorhandenen Datenspeicherungen zu löschen waren.

Dem liegt zugrunde, dass gem. § 5 Absatz 3 Satz 2 3. Bindestrich der Verordnung des Innenministeriums zur Durchführung des Polizeigesetzes (DVO PolG) bei vorsätzlicher Körperverletzung in einfachen und mittelschweren Fällen grundsätzlich von einem Fall von geringer Bedeutung auszugehen und deshalb lediglich eine dreijährige Speicherfrist gerechtfertigt ist. Das Polizeipräsidium vertrat zunächst die Auffassung, es liege kein Fall von geringer Bedeutung vor und begründete dies damit, dass Faktoren vorlägen, die für einen atypischen Fall sprächen; die wiederholte Begehung von Straftaten lasse nämlich eine kriminelle Neigung erkennen. Dies rechtfertige eine Speicherung mit Normalfrist (5 Jahre).

Das Polizeipräsidium wurde darauf hingewiesen, dass § 5 Absatz 3 Satz 2 DVO PolG im Zusammenhang mit § 5 Absatz 4 DVO PolG gesehen werden müsse. Die wiederholte Tatbegehung wird in Absatz 4 jedoch nicht genannt. Auch nach der Rechtsprechung ist allein die Häufung von Straftaten kein Kriterium für die Beurteilung, ob die Bedeutung der konkreten Straftat gering ist und darf aus der Vielzahl der Delikte nicht auf ihre serienmäßige Begehung geschlossen werden:

„Für die Beurteilung, ob ein geringer Unrechtsgehalt (§ 5 Abs.3 Satz 3 DVO PolG) anzunehmen ist, ist u.a. danach zu differenzieren, ob neben den vorgeworfenen Tatbeständen möglicherweise (nicht verwirklichte) besonders strafbewehrte Begehungsformen oder andere tatbestandliche Qualifikationen bestehen, die in Abgrenzung zur einfachen Begehungsweise bei der Einordnung des Unrechtsgehalts der vorgeworfenen Taten hätten berücksichtigt werden können (VG Hannover, Urt. v. 23.09.2013 – 10 A 2028/11 – <juris>). Daraus, dass bei § 5 Abs. 3 Satz 3 DVO PolG keine mit § 81 g Abs. 1 Satz 2 StPO vergleichbare Regelung enthalten ist, wonach die wiederholte Begehung sonstiger Straftaten im Unrechtsgehalt einer Straftat von erheblicher Bedeutung gleichstehen kann (Absatz 1 Satz 2), ist der Umkehrschluss gerechtfertigt, dass die wiederholte Begehung anderer Straftaten nicht generell den Unrechtsgehalt erhöht. Für dieses Verständnis spricht der Wortlaut des § 5 Abs. 4 DVO PolG, der die wiederholte Begehung anderer Straftaten nicht nennt, sondern nur Taten, die gewerbs-, gewohnheits-, serien-, bandenmäßig oder sonst organisiert begangen worden sind. Die „Fallzahl" ist […] für sich genommen kein Kriterium für die Beurteilung, ob die Bedeutung gering ist. Aus der Vielzahl der Delikte kann schließlich nicht auf ihre serienmäßige Begehung geschlossen werden. Denn diese setzt voraus, dass der Täter von vorneherein mit dem Ziel gehandelt hat, sich durch eine Vielzahl gleichmäßig begangener Taten strafbar zu machen, wobei die einzelnen Taten räumlich, zeitlich oder sonst besonders eng verschränkt sind (BGH Urt. v. 15.05.2013 – 1 StR 476/12 – u. Beschl. v. 25.09.2012 – 1 StR 407/12 – jeweils in <juris>). Diese im Strafrecht entwickelte Auslegung der serienmäßigen Begehung ist auch im Rahmen des § 5 Abs. 4 DVO PolG anzuwenden, weil es in beiden Zusammenhängen um den nicht geringen Unrechtsgehalt einer Straftat geht. […]".[18]

Das Polizeipräsidium hielt zunächst noch an seiner Ansicht fest, dass im vorliegenden Fall eine fünfjährige Speicherfrist angemessen sei und lehnte eine Einstufung des Vorgangs als Fall geringer Bedeutung weiter ab.

18 Verwaltungsgericht Karlsruhe Urteil vom 19. November 2014 - 4 K 2270/12 – ‚juris, Rn. 57

Nur auf unser beharrliches Drängen, die Entscheidung nochmals zu überdenken und die Daten zu löschen, sowie auf den Hinweis, dass andernfalls eine Beanstandung erwogen werde, lenkte das Polizeipräsidium schließlich ein und veranlasste die Löschung der Datenspeicherungen.

2.3.7 Datenlöschung aufgrund unzureichend begründeter Negativprognose[19]

Ein zum Petenten gespeichertes Ermittlungsverfahren musste, der aktuellen Rechtsprechung folgend, gelöscht werden, da in der polizeilichen Akte die angenommene Wiederholungsgefahr hinsichtlich der Begehung künftiger Straftaten nicht ausreichend begründet worden war.

In einem weiteren von uns geprüften Einzelfall wurde vom zuständigen Polizeipräsidium mitgeteilt, dass über den betroffenen Petenten Daten im Zusammenhang mit einem Ermittlungsverfahren wegen Anstiftung zum versuchten Totschlag im Ausland sowie im Zusammenhang mit einem Ermittlungsverfahren wegen Vergewaltigung/sexueller Nötigung im polizeilichen Auskunftssystem POLAS BW sowie im bundesweiten Informationssystem INPOL gespeichert seien. Erstgenanntes Verfahren sei bereits im Jahr 2005 nach § 170 Absatz 2 der Strafprozessordnung von der Staatsanwaltschaft mit der Begründung eingestellt worden, dass die weiteren Ermittlungen im Ausland wenig Erfolg versprächen. Der Akte sei kein Ergebnis des damals ins Ausland versandten Rechtshilfeersuchens zu entnehmen. Es seien auch keine sonstigen Ermittlungen dokumentiert, die einen Tatverdacht gegen den Petenten hätten erhärten und aufrechterhalten können. Zudem sei lediglich eine fünfjährige Speicherfrist festgelegt worden, welche Ende des Jahres 2004 geendet habe. Die Löschung der Daten zu diesem Ermittlungsverfahren sei durch das Polizeipräsidium bereits veranlasst worden.

Zur zweiten Datenspeicherung wurde uns mitgeteilt, dieser läge ein Ermittlungsverfahren zugrunde, in welchem die ehemalige Freundin des Petenten diesem vorgeworfen habe, sie sexuell missbraucht sowie seine beiden Kinder geschlagen zu haben. Das Ermittlungsverfahren war von der Staatsanwaltschaft nach § 170 Absatz 2 der Strafprozessordnung eingestellt worden, da ein strafbares Verhalten nicht mit der notwendigen Sicherheit nachgewiesen werden konnte. Aus der Begründung war herauszulesen, dass der Petent keine Angaben zur Sache gemacht hatte und die Aussagen der ehemaligen Freundin nicht belegt werden konnten. Die Daten zu diesem Ermittlungsverfahren seien aufgrund eines bleibenden Restverdachts gespeichert und mit einer zehnjährigen Speicherfrist versehen worden. Diese war zum Zeitpunkt unserer Anfrage zu einem Drittel verstrichen.

Gemäß § 38 Absatz 2 des Polizeigesetzes (PolG) ist die Speicherung personenbezogener Daten aus einem Ermittlungsverfahren zwar auch nach Einstellung des Verfahrens durch die Staatsanwaltschaft möglich, soweit ein Restverdacht bestehen bleibt. Sollen die Daten aber über zwei Jahre hinaus gespeichert werden, müssen nach § 38 Absatz 3 PolG tatsächliche Anhaltspunkte für eine Wiederholungsgefahr vorliegen.

Eine solche Wiederholungsgefahr war im vorliegenden Fall vom polizeilichen Sachbearbeiter auch angenommen worden. In der Akte war die vorzunehmende Einzelfallprognose jedoch nur mit den Stichworten „ja, Sexualdelikt" dokumentiert. Auch angesichts der aktuellen Rechtsprechung reicht eine derartig knappe Begründung jedoch bei weitem nicht aus. Vielmehr bedarf es einer auf den Einzelfall bezogenen, auf schlüssigen, verwertbaren und nachvollziehbar dokumentierten Tatsachen beruhenden Entscheidung.[20]

Das Fehlen einer solchen Dokumentation der Wiederholungsgefahr führt demnach zur Rechtswidrigkeit der Datenspeicherung. Unter Verweis auf diese Rechtsprechung haben wir das Polizeipräsidium deshalb aufgefordert, die Daten zu löschen. Das Polizeipräsidium schloss sich unserer Auffassung an und löschte auch die personenbezogenen Daten des Petenten im Zusammenhang mit dem zweiten Ermittlungsverfahren.

Dieser Fall zeigt erneut zwei typische Bereiche auf, mit denen wir uns immer wieder befassen. Zum einen fällt bei vielen unserer Anfragen in Bezug auf polizeiliche Datenspeicherungen auf,

19 vgl. auch 32. Tätigkeitsbericht 2014 / 2015, Landtags-Drucksache Nr. 15/7990, Seite 37 ff.
20 Verwaltungsgerichtshof Baden-Württemberg, Urteil vom 10. Februar 2015 – 1 S 554/13 –, juris

dass bereits aufgrund der damit verbundenen Überprüfung der Datenspeicherungen von der Polizei festgestellt wird, dass die Speichervoraussetzungen für einzelne Datenspeicherungen nicht mehr vorliegen und die Löschung der Daten sofort veranlasst wird. Die Datenlöschungen sehen wir durchaus positiv. Allerdings bestätigte sich auch hier wieder, dass sich unter den polizeilichen Datenspeicherungen eine Menge personenbezogener Daten befindet, die bei näherer Betrachtung nicht oder nicht mehr gespeichert werden dürften.
Zum anderen fällt – wie auch bereits bei der bundesweiten Prüfung der Falldatei Rauschgift – vermehrt auf, dass die Dokumentation der Wiederholungsgefahr vielmals nicht den Ansprüchen der aktuellen Rechtsprechung genügt und die Datenspeicherungen bei unseren Überprüfungen allein aufgrund dieses Umstandes gelöscht werden müssen, obwohl die tatsächlichen Anhaltspunkte für eine Wiederholungsgefahr oftmals sicher hätten begründet werden können. Im Rahmen der polizeilichen Sachbearbeitung sollte deshalb auf die Dokumentation der Einzelfallprognose mehr Gewicht gelegt werden.

3. Videoüberwachung

3.1 „Your Chief is watching you“ – oder „Die neue Work-Live-Balance am Arbeitsplatz“ (Einzelfälle aus dem Bereich Beschäftigtendatenschutz)

Auf die erhebliche Zunahme der Videoüberwachung am Arbeitsplatz und deren rechtlichen Voraussetzungen habe ich im Kapitel 1.3.3 bereits hingewiesen. Im Berichtszeitraum waren meine Mitarbeiter und ich allerdings mit zwei sehr massiven Fällen der Videoüberwachung am Arbeitsplatz konfrontiert:

Im ersten Fall wurden wir durch eine Beschwerde auf ein Unternehmen aufmerksam gemacht, welches insgesamt zehn Kameras zur Überwachung seiner Werkshallen und des Außenbereichs einsetzt. Dabei sind die acht Kameras im Innenbereich so ausgerichtet, dass im Wesentlichen alle Arbeitsplätze in den Werkshallen von den Kameras erfasst und aufgezeichnet werden. Die Aufnahmen werden für eine Dauer von drei Monaten gespeichert. Daneben werden die Bilder auch auf einen Monitor übertragen, welcher sowohl für die Geschäftsleitung als auch für die Mitarbeiter jederzeit einsehbar ist. Die Mitarbeiter werden somit rund um die Uhr an ihren Arbeitsplätzen videoüberwacht. Die Notwendigkeit einer Videoüberwachung wird durch den Arbeitgeber mit dem Schutz vor Einbrüchen sowie dem Schutz vor Diebstahl von Firmen- und Mitarbeitereigentum, insbesondere durch die eigenen Mitarbeiter, begründet. Entsprechende Strafanzeigen waren bisher allerdings nicht gestellt worden. Auch wurde nichts vorgetragen, was einen konkreten Diebstahlsverdacht gegen einen oder mehrere Mitarbeiter hätte begründen können.

Da es somit auf der Hand liegt, dass die Videokameras in erster Linie der Kontrolle der Beschäftigten dienen sollen, ist die Maßnahme an § 32 Absatz 1 BDSG zu messen. Danach dürfen, worauf bereits hingewiesen wurde, personenbezogene Daten eines Beschäftigten zur Aufdeckung von Straftaten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu **dokumentierende tatsächliche Anhaltspunkte** den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Ergänzend ist die arbeitsgerichtliche Rechtsprechung heranzuziehen.

Trotz mehrfacher Aufforderung wurden mir bisher keine Unterlagen vorgelegt, die den konkreten Verdacht des Diebstahls gegen einen oder mehrere Beschäftigten hätten belegen können. Es blieb vielmehr bei der pauschalen Aussage, in der Vergangenheit sei es zu Mitarbeiterdiebstählen gekommen. Damit allein lässt sich aber ein berechtigtes Interesse an einer Videoüberwachung sämtlicher Mitarbeiter nicht begründen. Abgesehen davon sind mildere, in das Persönlichkeitsrecht der Beschäftigten weniger einschneidende Mittel, wie Ausgangs- und Personenkontrollen oder Sicherung von Material und Arbeitsmittel insbesondere nach Betriebsschluss, denkbar und dem Arbeitgeber auch durchaus zumutbar.

Aber selbst dann, wenn mildere Mittel nicht in Betracht kämen, überwiegen die schutzwürdigen Interessen der Beschäftigten. Das Recht auf informationelle Selbstbestimmung schützt sie vor einer lückenlosen Überwachung am Arbeitsplatz durch Videokameras, mit der sie einem ständigen Überwachungsdruck ausgesetzt sind, dem sie sich nicht entziehen können. Sie haben selbst dann ein Recht darauf, von einer derartigen Dauerüberwachung verschont zu bleiben, wenn konkrete Straftaten festgestellt wurden. Auch in einem solchen Fall darf sich die Maßnahme nur auf einen räumlich und funktional abgrenzbaren Kreis von Arbeitnehmern beziehen und zeitlich nur beschränkt erfolgen. Eine dauerhafte Totalüberwachung unterschiedslos aller Beschäftigten wäre in keinem Fall zulässig.

Nach der Rechtsprechung des Bundesarbeitsgerichts ist eine Videoüberwachung nur als ultima ratio zulässig, wenn weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind (vgl. BAG, Urteil vom 27.03.2003, Az. 2 AZR 51/02). Der Verdacht muss in Bezug auf eine konkrete strafbare Handlung oder andere schwere Verfehlung zu Lasten des Arbeitgebers gegen einen zumindest räumlich und funktional abgrenzbaren Kreis von Arbeitnehmern bestehen. Er darf sich nicht auf die allgemeine Mutmaßung beschränken, es könnten Straftaten begangen werden (vgl. BAG, Urteil vom 21.06.2012, Az. 2 AZR 153/11). Die lediglich allgemein und ohne konkreten Anlass

geäußerte Sorge von Diebstählen genügt nicht zur Rechtfertigung einer Videoüberwachung (LAG Rheinland-Pfalz, Urteil vom 23.05.2013, Az. 2 Sa 540/12).

Dass seine bisherige Rechtsauffassung auf wackeligen Beinen steht, hat wohl auch der Arbeitgeber zwischenzeitlich eingesehen. Von einem Abbau der Videokameras hat er allerdings abgesehen und stattdessen die Einholung von Einwilligungserklärungen seiner rund 30 Mitarbeiter veranlasst, in denen sich die Beschäftigten mit der Videoüberwachung einverstanden erklären. Damit wurden die Probleme aber nur verlagert.

Nach § 4a Absatz 1 Satz 1 und Satz 2 BDSG kann eine Einwilligung nur wirksam erklärt werden, wenn sie auf der freien Entscheidung des Betroffenen beruht (Freiwilligkeit) und der Betroffene auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung (Informiertheit) hingewiesen wird.

Zwar kann nicht davon ausgegangen werden, dass eine Einwilligung in die Datenerhebung, -verarbeitung und -nutzung im Beschäftigtenverhältnis immer unzulässig ist. Aufgrund des besonderen Abhängigkeitsverhältnisses zwischen Arbeitgeber und Arbeitnehmer sind jedoch besonders hohe Anforderungen an die Prüfung zu stellen, ob in einem solchen Abhängigkeitsverhältnis eine freie Entscheidung möglich ist. Grundsätzlich ist daher eine umfassende Betrachtung der Umstände des Einzelfalls geboten.

Unabhängig davon, ob im gegebenen Fall die Beschäftigten ihre Einwilligungserklärung tatsächlich alle ohne Druck oder Zwang und damit freiwillig erteilt haben – vorhandene Zweifel könnten letztlich nur durch Einvernahme der Betroffenen ausgeräumt werden – sprechen grundsätzliche Erwägungen gegen eine Freiwilligkeit im Sinne des § 4a Absatz 1 BDSG:

Die Beschäftigten standen vor der Wahl, sich entweder mit der eigenen Überwachung einverstanden zu erklären oder sich durch die Verweigerung der Einwilligung als potenziell Diebstahlsverdächtige zu stigmatisieren. Verweigert ein Arbeitnehmer seine Einwilligung, ist es also nicht ausgeschlossen, dass er erhebliche Nachteile im Arbeitsverhältnis befürchtet oder befürchten muss. Eine echte Wahl zwischen Abgabe und Ablehnung der Einwilligungserklärung besteht somit zu keinem Zeitpunkt.

Von Freiwilligkeit kann auch deshalb nicht gesprochen werden, wenn man die Folgen der Verweigerung bzw. des Widerrufs einer erteilten Einwilligung für das Arbeitsverhältnis bedenkt. Die umfassende und dauerhafte Videoüberwachung setzt die Mitarbeiter einem Überwachungsdruck aus, dem sie sich zu keiner Zeit entziehen können, ohne dabei ihre arbeitsvertraglichen Pflichten zu verletzen, indem sie ihren Arbeitsplatz verlassen. Faktisch hat der einzelne Mitarbeiter somit keine Wahlfreiheit.

Hinzu kommt, dass sobald nur ein einziger betroffener Mitarbeiter seine Einwilligung in diese umfassende Überwachung verweigert – unter Verweis auf das dem Datenschutz immanente Verbot mit Erlaubnisvorbehalt –, keine datenschutzrechtliche Legitimationsgrundlage für diese Überwachungsmaßnahme mehr gegeben ist. Es ist daher nicht ersichtlich, wie ein Mitarbeiter sich dem sozialen Druck widersetzen könnte, wenn die Zulässigkeit der Maßnahme insgesamt mit seiner Einwilligung „steht oder fällt".

Angesichts der Tiefe des Eingriffs in das Recht auf informationelle Selbstbestimmung der Arbeitnehmer kann jedenfalls eine solche Totalüberwachung keinesfalls durch Einwilligung legitimiert werden. Anzunehmen, solche Einwilligungen kämen freiwillig zustande, hieße, die Realität zu leugnen. § 4a BDSG darf nicht das Feigenblatt sein, um derart schwerwiegende Eingriffe in das Datenschutzrecht zu legitimieren und damit insbesondere den Beschäftigtendatenschutz des § 32 BDSG auszuhebeln. Gegen den Arbeitgeber und Betreiber der Videoüberwachungsanlage habe ich daher gemäß § 38 Absatz 5 Satz 2 BDSG angeordnet, alle Kameras im Innenbereich abzuschalten und zu deinstallieren. Hiergegen hat er Klage beim Verwaltungsgericht erhoben.

Wir dürfen gespannt sein, wie das Gericht den Sachverhalt im Lichte des Beschäftigtendatenschutzes bewerten wird. Unabhängig vom tatsächlichen Ausgang des Gerichtsverfahrens wird die Entscheidung eines baden-württembergischen Verwaltungsgerichts – sowohl für die Arbeitgeber im Land als auch für uns als Aufsichtsbehörde – ein Stück Rechtsklarheit

und Rechtssicherheit in diesem komplexen und oftmals strittigen Themengebiet des Beschäftigtendatenschutzes bedeuten.

Der zweite besonders berichtenswerte Fall ist ganz ähnlich gelagert. Statt zehn Kameras wurden dort allerdings sage und schreibe 40 Kameras im Innen- und Außenbereich des Betriebs hauptsächlich zur Überwachung der eigenen Mitarbeiter eingesetzt. Neben der kompletten Überwachung des Lagers, der Büro- und Besprechungsräume wird der Außenbereich flächendeckend überwacht. Da der Arbeitgeber ausschließlich die eigenen Mitarbeiter im Verdacht hatte, für etwaige Diebstähle verantwortlich zu sein, wird die Videoüberwachung ausschließlich zum Zweck der Beschäftigtenüberwachung eingesetzt. Auch hier ist die § 32 Absatz 1 BDSG der Maßstab. Nachdem ich den Verantwortlichen in einer ersten datenschutzrechtlichen Bewertung auf die Rechtslage aufmerksam gemacht hatte, reagierte er umgehend und reduzierte die Anzahl der Kameras auf nunmehr 15 Kameras. Dies ist immer noch zu viel. Im Gegensatz zum ersten Fall bin ich hier allerdings zuversichtlich, letztlich zu einer datenschutzkonformen und vor allen Dingen mitarbeiterfreundlichen Lösung mit dem Arbeitgeber zu kommen, indem die Kameras beispielsweise nur außerhalb der Arbeitszeiten der Beschäftigten zur Durchsetzung des Hausrechts oder zum Schutze des Eigentums betrieben werden.

Der Fall zeigt damit exemplarisch, dass im Datenschutz oftmals auch Kompromisslösungen gesucht und gefunden werden können und müssen. Diese benötigen neben Bereitschaft und Engagement auf beiden Seiten vor allem eines: Zeit.

3.2 „Everywhere you go, I follow you“ – Teil I: Videoüberwachung im Freizeitbereich

3.2.1 Schwimmbäder

Zwar wurde bereits im 32. Tätigkeitsbericht[1] meiner Dienststelle ausführlich über die rechtlichen Voraussetzungen einer Videoüberwachung in Schwimmbädern berichtet. Leider war im Berichtszeitraum 2016/2017 festzustellen, dass viele Schwimmbadbetreiber nach wie vor wenig Sensibilität im Umgang mit dem Einsatz der Videoüberwachungstechnik zeigen. So erreichte uns erneut eine Vielzahl von Eingaben, die zu einer Überprüfung von sechs Schwimm- bzw. Wellnessbädern führte. Die Bäder sind dabei sowohl in privater als auch in öffentlicher Trägerschaft, sodass entweder die Voraussetzungen von § 6b BDSG oder § 20a LDSG zu prüfen waren. Als problematisch stellt sich dabei immer wieder die Videoüberwachung folgender Bereiche heraus:

a) Theken/Empfangsbereich

In aller Regel sollen die Kameras in den Empfangsbereichen und an den Empfangstheken dem Schutz des Eigentums dienen, d.h. der Verhinderung von Diebstählen, Trickdiebstählen, Betrug usw.

Sowohl nach Bundes- wie auch nach Landesrecht stellt dies grundsätzlich ein berechtigtes Interesse für eine Videoüberwachung dar. Voraussetzung ist aber, dass eine Gefahr für das Eigentum tatsächlich besteht. Hierzu muss substantiiert dargelegt werden, dass es in der Vergangenheit zu solchen Straftaten gekommen und deshalb damit zu rechnen ist, dass dies auch künftig der Fall sein wird. Eines solchen Nachweises bedarf es vor allem deshalb, da ansonsten der Kassenbereich täglich von einer Vielzahl von Personen passiert wird, die sämtlich unter einen Generalverdacht gestellt werden, ohne für eine Überwachung irgend einen Anlass gegeben zu haben. Dieser erhebliche Eingriff in das informationelle Selbstbestimmungsrecht kann nur bei schwerwiegenden Beeinträchtigungen der Rechte des Verantwortlichen gerechtfertigt sein.[2] Im Zweifel überwiegen die schutzwürdigen Interessen der Gäste, nicht gefilmt zu werden. In den meisten Fällen ist die Videoüberwachung im Rahmen der Empfangstheken auch noch aus einem anderen Grund heraus problematisch, nämlich dann, wenn es sich beim überwachten Bereich zugleich um den Arbeitsplatz von Mitarbeitern handelt.

Eine Überwachung des Empfangsbereichs ist also nur zulässig, wenn es bereits konkrete Vorfälle oder Straftaten in diesem Bereich ge-

1 https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2016/02/32._TB.pdf#, dort Kapitel 11.1.2, S. 185 f.

2 vgl. BGH, NJW 1995, 1955, 1957

geben hat oder eine belegbare Gefährdungslage gegeben ist. Um eine anlasslose Überwachung aller Gäste zu verhindern, empfehlen wir die Installation von Notfallknöpfen, die in einer konkreten Gefahrensituation eine anlassbezogene Videoüberwachung ermöglicht.

b) Durchgänge zu zusätzlich kostenpflichtigen Bereichen (beispielsweise Sauna-, Wellness- oder Gesundheitsbereiche)

In diesem Bereich stellt sich grundsätzlich die Frage der Erforderlichkeit einer Videoüberwachung. So kann der unberechtigte Zugang zu Bereichen, für die ein zusätzliches Entgelt zu entrichten ist, beispielsweise zum Saunabereich, durch andere geeignete Maßnahmen, wie hohe Drehkreuze oder Schranken, ohne unverhältnismäßigen Aufwand verhindert werden. Wer den baulichen Aufwand scheut oder aus architektonischen Gründen ablehnt, muss ggf. technisch kreativ werden. Durch den Einbau von Lichtschranken kann ein Alarmsignal bei Über- oder Unterschreiten der Schranken/ Drehkreuze ausgelöst werden, welches wiederum die Videoüberwachung aktiviert und gleichzeitig einen Mitarbeiter alarmiert, sodass der Täter „auf frischer Tat" ertappt werden kann.

c) Bereich der Umkleidekabinen

Auch wenn in den seltensten Fällen direkt in den Umkleidekabinen videoüberwacht wird, so müssen wir doch zunehmend feststellen, dass in beinahe allen überprüften Schwimmbädern zumindest die Gänge zwischen den Umkleidekabinen und Spinden von der Überwachung erfasst wurden. Damit ist die Intimsphäre der Badegäste zumindest mittelbar betroffen. Diese Intimsphäre ist unter allen Umständen zu respektieren und zu schützen. Die Kameras sind daher so auszurichten, dass lediglich der unmittelbare Bereich der Spinde erfasst wird, was entweder durch den Einsatz von Stabkameras oder durch eine Privatzonenmaskierung realisiert werden kann. Denkbar ist auch, den Aufnahmebereich der Kamera visuell sichtbar zu machen, beispielsweise durch farbliche Markierungen am Boden. Des Weiteren sollten deutlich gekennzeichnete nicht überwachte Umkleidebereiche zur Verfügung gestellt werden, damit dem Badegast eine Entscheidungsmöglichkeit verbleibt.

Auch wenn durch die Kameras letztlich auch das Eigentum der Badegäste geschützt wird und sie somit deren Interesse dienen, müssen die datenschutzrechtlichen Voraussetzungen erfüllt sein. Dazu gehört aber gerade auch die umfassende Transparenz. Nur wer überhaupt weiß, dass videoüberwacht wird und wo videoüberwacht wird, kann sich bewusst dafür entscheiden, den überwachten Bereich zu betreten. Die wenigsten Badegäste werden davon ausgehen, in den Umkleidebereichen videoüberwacht zu werden. Nur wer weiß, dass er gefilmt wird, kann sein Verhalten darauf einstellen.

d) Saunabereiche bzw. FKK-Bereiche.

Da sich die Gäste im Bereich der Sauna und in deren Außenbereich in aller Regel unbekleidet bewegen, greift die Videoüberwachung dieser Bereiche in besonderem Maß in die Intimsphäre der Badegäste ein. Eigentlich sollte es eine Selbstverständlichkeit sein, dass sich der Betreiber einer solchen Anlage hier mit der Videoüberwachung zurückhält. Leider ist die Realität eine andere, wie wir wiederholt feststellen mussten. Nicht akzeptieren können wir dabei auch das immer wieder vorgebrachte Argument, man müsse die Möglichkeit haben zu erkennen, wenn ein Saunagast gesundheitliche Probleme bekommt, etwa Kreislaufprobleme. Dass es zu solchen Problemen kommen kann, stellt ein allgemeines Lebensrisiko dar und rechtfertigt nicht zwingend den Einsatz von Überwachungskameras. Hier gibt es andere Möglichkeiten, solchen Sondersituationen zu begegnen, etwa durch den Einsatz von hilfsbereitem Personal.

Ein solch schwerwiegender rechtswidriger Eingriff in das Recht auf informationelle Selbstbestimmung kann zudem eine Straftat nach § 201a StGB (Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen) darstellen.

3.2.2 Fitnessstudios

Ein großer Teil der Beschwerden im Bereich „Freizeit" richtete sich – neben der Videoüberwachung in Schwimmbädern – gegen Videoüberwachungskameras in Fitnessstudios. Auch hier ist § 6b BDSG der rechtliche Maßstab, denn bei Fitnessstudios handelt es sich um öffentlich zugängliche Räume, da eine unbestimmte Anzahl von Personen die Räumlichkeiten betreten bzw. eine Mitgliedschaft erwerben kann.

Als Zweck der Videoüberwachung der Trainings- und Kursflächen nennen die Betreiber der Fitnessstudios, neben dem Schutz des Eigentums vor Diebstahl oder Vandalismus, regelmäßig den Schutz von Leib und Leben der Mitglieder. Das Interesse der Betreiber besteht dabei in erster Linie darin, sich im Falle eventueller Schadensersatzforderungen im Zusammenhang mit Unfällen entlasten zu können. Das vorgebliche Drittinteresse stellt somit in Wahrheit ein Eigeninteresse dar, welches zwar grundsätzlich als berechtigt anzusehen ist. Jedoch ist die Notwendigkeit dieser Überwachung zu bezweifeln. Denn jedenfalls während der Öffnungszeiten eines Fitnessstudios befindet sich – neben den Mitgliedern – regelmäßig Personal in den Räumlichkeiten. Dieses hat die Möglichkeit, im Notfall einen Arzt zu verständigen. Entsprechend ausgebildetes Personal sollte durchaus in der Lage sein, einen Überblick über die Situation im eigenen Zuständigkeitsbereich zu behalten und entsprechende Vorfälle so zeitnah zu erkennen, dass erforderliche Hilfsmaßnahmen (Notruf beim Rettungsdienst oder das Leisten von erster Hilfe) möglich sind. Eine ständige Beobachtung mittels Videoüberwachung ist hierfür nicht erforderlich. Zumal die Rechtsprechung mehrfach bestätigt hat, dass im Falle eines Unfalls die hinreichende Wahrnehmung der Verkehrssicherungspflicht nicht mit Videoaufzeichnungen nachgewiesen werden muss und der Geschädigte beweispflichtig ist.

Bei einer sportlichen Betätigung steht die freie Entfaltung der Persönlichkeit im Vordergrund. Der großflächigen und umfassenden Überwachung können sich die Mitglieder nicht entziehen. Während des Trainings werden unweigerlich das gesamte Sozialverhalten der Trainierenden und ihre Interaktion miteinander aufgezeichnet. Daher überwiegen in aller Regel die schutzwürdigen Interessen der Kunden/Mitglieder, beim Training nicht beobachtet zu werden.

Vor Installation einer Videoüberwachungsanlage empfehlen wir daher die Lektüre der Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“[3] des Düsseldorfer Kreises. Gerne stehen auch die Mitarbeiter meiner Dienststelle mit Rat und Tat zur Seite.

3.2.3 Kamera- bzw. videoüberwachte Zugangskontrollen

Die Überwachung mittels Foto- oder Videokamera findet zunehmend Verwendung in Zutrittskontrollsystemen bei Freizeitanlagen, wie beispielsweise Ski- und Sesselliften oder Seilbahnen.

Ein Fall, in dem es um Zutrittskontrollen zu einer Skiliftanlage geht, beschäftigt meine Dienststelle nun schon des Längeren. Dort werden Kunden beim Betreten der Anlage fotografiert und die so erhobenen Lichtbilder werden mit sog. Referenzfotos, welche beim Kauf etwa des Skipasses erstellt wurden, abgeglichen. Zweck ist dabei die Verhinderung von Leistungserschleichungen durch missbräuchliche Verwendung des Skipasses durch unberechtigte Dritte, die den Skipass entweder nur ausgeliehen oder durch privaten, günstigeren Weiterverkauf erworben haben. Ob ein solches Zugangskontrollsystem datenschutzrechtlich zulässig ist oder nicht, hängt von vielen Faktoren ab, insbesondere davon, wie ein solches System letztlich konkret ausgestaltet ist.

Welche Daten dürfen erhoben werden?

Sofern Fotoaufnahmen einer Person oder Gesichtsbilder aufgenommen werden, die biometrisch vermessen (biometrische Templates) und später automatisch abgeglichen werden sollen, handelt es sich um die Erhebung biometrischer Daten. Sollte die eingesetzte Software solche biometrischen Daten erfordern und speichern, so kann nach der Entschließung der 87. Datenschutzkonferenz die Erhebung, Verarbeitung und/oder Nutzung biometrischer Daten zur Gesichtserkennung zum Zweck der Erstellung eines dauerhaften biometrischen Templates nur bei Vorliegen einer wirksamen Einwilligung des Betroffenen i.S.d. § 4a BDSG rechtmäßig erfolgen. Eine solche Einwilligung muss aktiv und ausdrücklich durch den Betroffenen erteilt werden. Die Betroffenen müssen vor der Erteilung der Einwilligung über die Funktionsweise der Erstellung und Nutzung der sie möglicherweise betreffenden Templates und die damit verfolgten Zwecke und Risiken in klarer und verständiger Weise umfassend informiert werden. Die Einholung einer Einwilligung, die den hohen Anforderungen des § 4a Absatz 3 BDSG entspricht, dürfte im praktischen Alltag beim

3 https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2014/03/OH-V%C3%9C-durch-nicht-%C3%B6ffentliche-Stellen.pdf

Verkauf der Skipässe aber schlichtweg unmöglich sein.

Der Skiliftbetreiber, um dessen Anlage es aktuell geht, plant zwar keine Erhebung biometrischer Daten, allerdings stellt die Fotoaufnahme einer Person grundsätzlich ein personenbezogenes Datum dar, sodass das Zugangskontrollsystem den datenschutzrechtlichen Anforderungen genügen muss. So stellen sich insbesondere zentrale Fragen hinsichtlich der Erforderlichkeit:

- Gibt es alternative Zugangskontrollsysteme, die weniger tief in das Recht auf informationelle Selbstbestimmung eingreifen?
- Für welche Skipässe werden sog. Referenzfotos, die im System gespeichert werden und mit denen der Abgleich erfolgt, benötigt? Wie lange sollen diese Aufnahmen gespeichert bleiben?
- Wie erfolgt der konkrete Abgleich? Manuell oder durch das Computersystem? Wie lange kann der Abgleich durchgeführt werden?

Es gibt viele Stellschrauben, die letztlich darüber entscheiden, ob ein solches System datenschutzkonform ist oder nicht. Leider – so zeigt unsere Erfahrung – werden die entsprechenden Zugangskontrollsysteme oftmals ohne Rücksicht auf datenschutzrechtliche Belange erworben und eingesetzt. So können die Systeme oftmals weitaus mehr, als datenschutzrechtlich zulässig ist. Wir sehen hier einerseits die Hersteller entsprechender Systeme in der Pflicht, bereits bei der Entwicklung datenschutzrechtliche Belange in den Fokus zu rücken („privacy by design"), aber insbesondere auch die Betreiber der Freizeitanlagen, vor Installation eines Zugangskontrollsystems eine umfassende datenschutzrechtliche Vorabkontrolle durchzuführen.

Der Einsatz kameragestützter Zugangskontrollsysteme beschränkt sich aber nicht auf den sportlichen Bereich: So war meine Dienststelle im Berichtszeitraum auch mit der Überprüfung eines Einlasskontrollsystems zur Identifizierung gesperrter Spieler in Spielhallen anhand biometrischer Templates befasst. Anders als im Falle des Skiliftbetreibers, der aufgrund wirtschaftlicher Interessen ein Kontrollsystem installiert, sind Spielhallenbetreiber zudem rechtlich verpflichtet, Einlasskontrollen durchzuführen:

Die bisherige Einlasskontrolle erfolgte in aller Regel durch eine Ausweiskontrolle durch das Personal des Spielhallenbetreibers, wenn sich die Besucher der Spielhalle schon in der Spielhalle befanden. Das neue Einlasskontrollsystem soll hingegen schon im Eingangsbereich einer Spielstätte aufgestellt werden. Dieses erfasst alle Personen, die die Stätte betreten und fertigt ein Bild (biometrisches Sample) an. Aus diesen Bilddaten werden die erkennungsrelevanten biometrischen Merkmale extrahiert und mit den hinterlegten Referenzdaten (biometrische Templates) gesperrter Personen abgeglichen. Wird ein gesperrter Spieler vom System identifiziert, erfolge eine Meldung an das Personal. Die Bilddaten (Samples) nicht gesperrter Personen werden gleich wieder gelöscht. Anders läuft dies bei gesperrten Spielern. Damit das System einen gesperrten Spieler erkennt, muss vorab – am besten vor Ort – ein Foto (biometrisches Sample) von der Person gemacht werden. Aus diesem biometrischen Sample wird ein biometrisches Merkmal extrahiert. In der sich anschließenden Einlernphase (Enrollment) wird das Merkmal als biometrisches Template (Referenzmuster) dauerhaft im Erkennungssystem in digitaler Form gespeichert. In manchen Systemen können zudem weiteren personenbezogenen Daten, wie Name, Geburtsdatum, Anschrift etc. mit diesem Template verknüpft werden, um im Zweifel die Identität des gesperrten Spielers zu verifizieren. Falls nämlich das Erkennungssystem den Einlass aufgrund eines Template-Treffers in der Datenbank verweigert, kann auf Wunsch des Besuchers noch einmal ein manueller Abgleich (Verifikation) mit dem Personalausweis erfolgen.

Sowohl das Erheben der Bilddaten bei den zu sperrenden Spielern als auch die Verarbeitung dieser Bilddaten zu Templates (Enrollment), sowie das temporäre Erheben der biometrischen Samples bei sämtlichen Besuchern einer Spielhalle bedürfen nach § 4 Absatz 1 BDSG grundsätzlich einer gesetzlichen Grundlage oder einer Einwilligung der Betroffenen.

§ 6b BDSG scheidet dabei als gesetzliche Grundlage aus, da der Begriff des „Beobachtens" schon nach dem Wortsinn eine optische Erfassung über eine gewisse Dauer voraussetzt. Daher wurde die einmalige Bilderfassung, wie sie durch das System vorgenommen wird, nicht als eine Videoüberwachung bewertet. Das System war vielmehr an § 28 Absatz 1 Satz 1 Nr. 2 BDSG zu messen. Dieser ist anwendbar, soweit keine besonderen personenbezogenen Daten betroffen sind. Biometrische Daten sind für sich

genommen keine besonderen personenbezogenen Daten im Sinne des § 3 Absatz 9 BDSG. Diese Bewertung kann sich allerdings ändern, wenn die biometrischen Daten mit weiteren Daten, die Aufschluss, beispielsweise über die rassische und ethnische Herkunft geben, oder mit Daten, die Auskunft über eine existierende Spielsucht (Thematik Gesundheit) geben, verbunden werden. In solchen Fällen kann es sich dann sehr wohl um besondere Arten personenbezogener Daten im Sinne des § 3 Absatz 9 BDSG handeln. Eine solche Verknüpfung ist daher in jedem Fall auszuschließen.

Im Rahmen der datenschutzrechtlichen Prüfung stellte sich vor allem die Frage der Erforderlichkeit der Maßnahme. Insbesondere, ob das bloße Erheben von Ausweisdaten im Vergleich zu einer Erhebung von biometrischen Gesichtsdaten ein milderes Mittel darstellen kann.

Der Abgleich von Ausweisdaten erfolgt in vielen Spielhallen durch das Personal vor Ort, welches aufgrund des Geburtsdatums die Einhaltung der Jugendschutzbestimmungen und anhand des Namens, Fotos, Geburtsdatums und der Anschrift die Übereinstimmung mit der internen Sperrdatei prüfen. Der Besucher bleibt dabei also nicht „anonym", sondern wird anhand seiner Ausweisdaten vom Personal namentlich identifiziert.

Im Rahmen des Einlasskontrollsystems mittels Template-Abgleichs bleibt der Besucher – vorausgesetzt es gibt keinen Treffer in der Sperrdatei oder keine Zugangssperre aufgrund der Jugendschutzbestimmungen – gegenüber dem Personal „anonym". Dies stellt auf den ersten Blick aus Sicht des Datenschutzes eine Verbesserung dar. Allerdings wird statt dem Lesen und Erkennen durch eine natürliche Person bei der Ausweiskontrolle ein biometrisches Sample und anschließend das biometrische Merkmal erstellt, welches als eine Art „digitaler Fingerabdruck" gesehen werden kann. Ob dies datenschutzrechtlich nun ein milderes oder weitergehendes Mittel darstellt, lässt sich nicht so einfach beantworten, da es sich um völlig unterschiedliche Maßnahmen mit jeweils unterschiedlichen Eingriffen ins Persönlichkeitsrecht handelt, was einen Vergleich letztlich unmöglich macht.

Für die datenschutzrechtliche Bewertung bedeutet dies, dass im Rahmen der Erforderlichkeitsprüfung kein anderes, gleich geeignetes milderes Mittel vorliegt. Es stellt sich im Rahmen der Prüfung daher nur die Frage, ob die Maßnahme (Erstellung des Fotos, die biometrische Merkmalsextraktion, die Speicherung als Template sowie die ggf. zusätzliche Verknüpfung mit weiteren Ausweisdaten) vollständig erforderlich ist oder aber ggf. reduziert werden kann und damit ein milderes Mittel darstellt.

Durch die Erstellung des Fotos (Samples) mit anschließender biometrischer Merkmalsextraktion sowie der Speicherung des biometrischen Merkmals in Form eines Templates kann sichergestellt werden, dass einem gesperrten Spieler der Zugang zur Spielhalle verwehrt wird. Hierdurch wird also der gesetzlichen Anforderung gemäß § 43 LGlüG und somit dem berechtigten Interesse des Spielhallenbetreibers Rechnung getragen. Unstreitig ist, dass mit der Erhebung und Speicherung ein Eingriff in das Recht auf informationelle Selbstbestimmung der gesperrten bzw. zu sperrenden Spieler entsteht. U.E. hat der Eingriff aber eine geringe Persönlichkeitsrelevanz, wenn es sich um eine anonyme Erhebung und Speicherung des Templates handelt und dieses anonyme Template letztlich nur systemintern für den Zweck der Zugangskontrolle genutzt wird.

Diese Anforderungen sind dann erfüllt, wenn:

- die Bilder (Samples) sofort nach Fertigung der Templates spurenlos gelöscht werden;
- lediglich das Template des gesperrten Spielers ohne weitere Datenverknüpfungen gespeichert wird. Das System erkennt dann lediglich, dass es sich um einen gesperrten Besucher handelt;
- keine Speicherung von Zugangsdaten erfolgt, d.h. insbesondere nicht gespeichert wird, wann die Person, zu der das entsprechende Template gehört, Zugang erbeten hat;
- die technischen Voraussetzungen gegeben sind, dass die Templates verschlüsselt auf dem unternehmensinternen System gespeichert werden können und spätestens nach den gesetzlichen Fristen für die Spielersperren überprüft bzw. mit Ablauf der Spielersperren wieder gelöscht werden.

Unter diesen Voraussetzungen handelt es sich um einen Eingriff mit geringer Persönlichkeitsrelevanz, wonach ein überwiegendes berechtigtes Interesse des Spielhallenbetreibers bejaht werden kann.

Auch wenn die Erhebung und Speicherung unter den o.g. Voraussetzungen zulässig ist, halten wir für die Fallgruppe der zu sperrenden Spieler eine umfassende Information vor Erstellung der Templates für unverzichtbar. Grundsätzlich fordert auch § 4 Absatz 3 Satz 1 BDSG eine detaillierte Hinweispflicht. Eine solche umfassende Information sollte ausführlich im Formblatt „Antrag auf Selbstsperre" sowie auf den Homepages der entsprechenden Unternehmen erfolgen.

Dies bedeutet aber auch, dass eine Verknüpfung der Templates mit weiteren personenrelevanten Daten, insbesondere den Ausweisdaten, für eine wirksame Einlasskontrolle nicht erforderlich und damit datenschutzrechtlich unzulässig ist. Das System benötigt lediglich die Information „gesperrt" bzw. „nicht gesperrt", um darauf hinzuweisen, dass Anlass besteht, über den Einlass in die Spielhalle zu entscheiden. Die Spielersperre sowie die weiteren personenbezogenen Daten können an anderer Stelle gespeichert und nur für den Fall überprüft werden, wenn der Besucher trotz Einlassverweigerung weiterhin Einlass begehrt und auf die weitergehende Überprüfung besteht.

Das berechtigte Interesse der Spielhallenbetreiber an der Erhebung und Verarbeitung der biometrischen Daten und damit die Durchführung der Zugangskontrolle erstreckt sich auch auf die sonstigen Besucher der Spielhalle, da letztlich nur durch eine Kontrolle aller Besucher eine wirksame Umsetzung der Jugendschutzbestimmungen und der Suchtprävention möglich ist. Da eine Kontrolle der sonstigen Besucher in aller Regel anlasslos erfolgt, ist darauf zu achten, dass der Eingriff in das Recht auf informationelle Selbstbestimmung dieser Betroffenengruppe möglichst gering ist, d.h. die durch die Maßnahme gewonnenen Daten eine möglichst geringe Persönlichkeitsrelevanz aufweisen.

Unter Einhaltung folgender Voraussetzungen halten wir den Einsatz des Systems für sonstige Besucher nach § 28 Absatz 1 Satz 1 Nr. 2 BDSG für zulässig:

- Sofortige spurenlose Löschung der Bilder (biometrischen Samples) nach Erstellung der Templates (nach dem Enrolment). Sofortige Verschlüsselung der erhobenen Templates.
- Unverzügliche Löschung eines biometrischen Samples nach Abgleich mit den Templates (in der Sperrdatei); insbesondere Wegfall der sog. Historienfunktion.
- Keine Datenweitergabe an Dritte.
- Keine Speicherung und Auswertung von biometrischen Zusatzinformationen sowie kein Hinzuspeichern und Verknüpfen mit sonstigen Daten der Betroffenen.
- Strikte Zweckbindung bzw. keine Zweckänderung.

Ausblick DS-GVO
Fraglich ist, wie das aktuelle System nach Inkrafttreten der DS-GVO zu bewerten sein wird. Sensible Daten im Sinne der DS-GVO sind nämlich ausdrücklich auch biometrische Daten nach Art. 4 Nr. 14 DS-GVO, wonach physiologische und physische Merkmale, die die eindeutige Identifizierung einer Person ermöglichen, biometrische Daten darstellen. Liegen solche Daten vor, unterliegen diese den besonderen Verarbeitungsbeschränkungen des Art. 9 Absatz 1 DS-GVO.
Daher stellt sich insbesondere die Frage, wie der Begriff der „eindeutigen Identifizierung" künftig definiert werden muss bzw. welche Anforderungen daran gestellt werden. Nach der DS-GVO könnte es bereits ausreichen, wenn mittels Template die Person als solche wiedererkannt werden soll, auch wenn diese nicht namentlich identifiziert werden kann. Nach dem Erwägungsgrund Nummer 28 zur DS-GVO kann die Anwendung der Pseudonymisierung auf personenbezogene Daten die Risiken für die betroffenen Personen zwar senken, ob dies im Falle der Erstellung eines Templates jedoch die „eindeutige Identifizierung" einer Person ausschließt, ist fraglich.

3.3 „Everywhere you go, I follow you" – Teil II Videoüberwachung durch öffentliche Stellen

Über die allgemeine Zunahme der Videoüberwachung durch öffentliche Stellen habe ich bereits im Kapitel 1.3.6 berichtet. Insbesondere bezüglich der Überwachung von Schulhöfen und Containerstandorten (Recycling- und Wertstoffhöfe aber auch Standorte für einzelne Glascontainer) haben uns zahlreiche Anfragen aus den Kommunen erreicht.

Einschlägige Rechtsgrundlage für eine Videoüberwachung durch öffentliche Stellen ist § 20a des Landesdatenschutzgesetzes (LDSG). Hiernach kann eine Videobeobachtung im Rahmen der Erfüllung öffentlicher Aufgaben oder

in Ausübung des Hausrechts zum Schutz von Leben, Gesundheit, Freiheit oder Eigentum von Personen, die sich im Bereich öffentlicher Einrichtungen, öffentlicher Verkehrsmittel, von Amtsgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen aufhalten, oder zum Schutz von Kulturgütern, öffentlichen Einrichtungen, öffentlichen Verkehrsmitteln, Amtsgebäuden und sonstigen baulichen Anlagen öffentlicher Stellen zulässig sein. Denkbar ist der Einsatz von Videoüberwachungstechnik insbesondere, um die Begehung von Ordnungswidrigkeiten von erheblicher Bedeutung oder Straftaten zu verhindern oder deren Verfolgung oder die Geltendmachung von Rechtsansprüchen zu ermöglichen.

Als Gründe für eine Videoüberwachung in Schulhöfen werden in aller Regel Vandalismus und Sachbeschädigungen angeführt, die künftig verhindert bzw. aufgeklärt werden sollen. Bei der Überwachung von Containerstandorten spielen eher illegale Müllablagerungen, die oftmals mit einem erheblichen Entsorgungsaufwand und Kosten verbunden sind, oder Diebstähle von Wertstoffen eine Rolle für den geplanten Einsatz von Videoüberwachungstechnik.

Videoüberwachung darf allerdings nur unter strikter Beachtung des Erforderlichkeits- und Verhältnismäßigkeitsgrundsatzes erfolgen. Voraussetzung ist nach § 20a Absatz 1 Satz 2 Nr. 1 LDSG, dass Tatsachen die Annahme rechtfertigen, dass das zu schützende Rechtsgut oder Objekt gefährdet ist. Nach der Gesetzesbegründung (LT-Drs. 14/7313, S. 19) reichen bloße Indizien nicht aus. Entweder muss es in der Vergangenheit bereits zu entsprechenden Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung[4] gekommen sein oder es müssen beweiskräftige Tatsachen dafür vorliegen, dass solche in Zukunft begangen werden sollen. Dass eine Schule erfahrungsgemäß häufig Gegenstand von Vandalismus ist bzw. es an Containerstandorten regelmäßig zu illegalen Müllablagerungen kommen kann, genügt nicht. Entsprechende Vorfälle oder Hinweise sind darzulegen bzw. zu dokumentieren. Im Falle von Containerstandorten sollten die illegalen Müllablagerungen und die daraus entstehenden Folgekosten (Entsorgungskosten, Entsorgungsaufwand etc.) über einen längeren Zeitraum dokumentiert werden, um den konkreten Schaden auch beziffern zu können. Wichtig ist in diesem Zusammenhang ferner, dass es sich um Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung handeln muss. Videoüberwachung zur Verhinderung von sogenannten Fehlwürfen (beispielsweise fehlerhaft sortierte Wertstoffe) fallen nicht unter den Anwendungsbereich.

Im Rahmen der Beurteilung der Zulässigkeit der Videoüberwachung kommt es auch darauf an, ob der angestrebte Zweck auch durch mildere Maßnahmen erreicht werden kann. Grundsätzlich wären Maßnahmen, wie eine Einzäunung des Geländes, der Einsatz von Bewegungsmeldern bzw. die Einrichtung von Alarmanlagen datenschutzrechtlich mildere Mittel, da diese weit weniger in das Recht auf informationelle Selbstbestimmung eingreifen, als dies bei einer Videoüberwachung der Fall ist. Daneben sind weitere Maßnahmen zu prüfen, für Schulhöfe beispielsweise häufigere Kontrollen durch Hausmeister, einen Sicherheitsdienst oder den Einsatz der mobilen Jugendarbeit oder Polizeistreifen.

Bei Bejahung der Erforderlichkeit einer Videoüberwachung ist zu prüfen, ob schutzwürdige Interessen der Betroffenen überwiegen. Im Rahmen der Abwägung spielen die Art der geplanten Maßnahme, die überwachte Örtlichkeit und die Schwere des Eingriffs eine wesentliche Rolle. Maßgebend für die rechtliche Beurteilung der Intensität eines Eingriffs in das Recht auf informationelle Selbstbestimmung ist die Art der Beeinträchtigung. So sind insbesondere Schulhöfe während der Schulzeiten besonders sensible Bereiche, weshalb die Videoüberwachung von Schulhöfen in aller Regel immer nur außerhalb der Schulzeiten in Betracht kommen wird. In diesem Zusammenhang könnte auch geprüft werden, ob die Videoüberwachung vielleicht noch weiter eingeschränkt werden kann, nämlich auf Zeiträume, in denen die Straftaten bislang erfolgt sind, d.h. auf die Nachtstunden an den Wochenenden. Auch bei einer Überwachung der Wertstoffhöfe ist zu prüfen, ob eine zeitliche Begrenzung in Betracht kommen kann.

Videoaufzeichnungen sind ferner gemäß § 20a Absatz 5 LDSG unverzüglich zu löschen, so-

4 Straftaten im Rahmen des § 326 des Strafgesetzbuches (StGB), zumindest aber erhebliche Ordnungswidrigkeiten, z.B. nach § 61 Absatz 1 des Kreislaufwirtschafts- und Abfallgesetzes (KrW-/AbfG).

weit sie nicht zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten oder zur Geltendmachung von Rechtsansprüchen benötigt werden. In der Regel dürfte eine Speicherung von 48 Stunden, an Wochenenden und Feiertagen 72 Stunden angemessen sein. Sofern die Speicherfrist noch kürzer gewählt werden könnte, wäre dies natürlich zu begrüßen.

Insbesondere sollte auch der Transparenzgedanke bei öffentlichen Stellen im Vordergrund stehen und entsprechend früh und umfangreich auf die Videoüberwachung hingewiesen werden. Vor allem bei Schulen, die sehr sensible Bereiche darstellen, empfehlen wir eine umfangreiche Vorabinformation der Lehrer, Schüler und Eltern sowie ggf. weiterer Betroffener über den geplanten Einsatz und Umfang der angedachten Videoüberwachung. So kann insbesondere einem Überwachungsdruck vorgebeugt werden.

Vor dem erstmaligen Einsatz von Videoüberwachungstechnik hat eine schriftliche Freigabe durch die verantwortliche Stelle, also die Kommune bzw. Behörde, zu erfolgen. In der schriftlichen Freigabe sind gemäß § 20a Absatz 6 LDSG der Zweck der Videoüberwachung anzugeben, weitere wesentliche Festlegungen für das Verfahren zu treffen und das Ergebnis der Zulässigkeitsprüfung im Einzelnen darzulegen. Die inhaltlichen Anforderungen können § 20a Absatz 6 Nrn. 1 bis 8 LDSG entnommen werden.

4. Verkehr

4.1 MoveBW

Endlich nicht mehr im Stau stehen, sondern aufgrund verschiedener Mobilitätsangebote schnell und sicher unterwegs sein. Dieses Ziel verfolgt das Projekt „MoveBW" (Mobilitätsinformation und Verkehrssteuerung Baden-Württemberg), das vom Land Baden-Württemberg während der Projektlaufzeit von 18 Monaten mit rund zwei Millionen Euro gefördert wird.

Vorausgegangen war ein Wettbewerb, den ein aus sechs Teilnehmern bestehendes Konsortium gewann. Das vom Gewinner-Konsortium vorgestellte Angebot umfasst auch Parkraummanagement und verkehrsübergreifende Navigation. Verschiedene Mobilitätslösungen sollen miteinander vernetzt werden. Der Kunde kann sein Fahrtziel angeben und ihm werden verschiedene Vorschläge gemacht, wie er am besten zu seinem Ziel gelangt, er kann die ihm vorgeschlagenen Alternativen jedoch frei auswählen. In diesem System wird eine einheitliche Buchung und Abrechnung vorgegeben, sodass der Kunde nicht von verschiedenen Anbietern eine Rechnung erhält.

Am Ende des Projekts soll ein Mobilitätsassistent für die Metropolregion Stuttgart stehen, der mit Echtzeitdaten aus einer BigData-Plattform versorgt wird. Per App begleitet der Assistent Verkehrsteilnehmer in Echtzeit auf intermodalen Reisen durch Stuttgart und Umgebung. Verschiedene Transportmittel wie der öffentliche Personennahverkehr, das eigene Fahrzeug oder geliehene E-Bikes werden hierbei berücksichtigt. Bei auftretenden Störungen oder Behinderungen (z.B. Verspätungen im Nahverkehr oder Staus) schlägt die App gegebenenfalls bessere Alternativen vor. Dabei sollen die Nutzer nicht mehr für jedes Verkehrsmittel einzeln bezahlen, sondern am Monatsende eine einzige übersichtliche Mobilitätsrechnung erhalten, über die sie alle genutzten Mobilitätsangebote (inklusive Parken) abrechnen können. Mit dem Assistenten können Autofahrer auch Parkplätze der Parkraumgesellschaft Baden-Württemberg buchen. MoveBW soll damit einen wesentlichen Beitrag zum Umstieg vom Fahrzeug auf den öffentlichen Personennahverkehr und damit zur Verbesserung der Verkehrslage in der Metropolregion Stuttgart leisten.

Voraussetzung für eine erfolgreiche Abwicklung des Projekts ist, dass sich verschiedene Verkehrsträger (bspw. Gemeinden, Verkehrsunternehmen und Verkehrsverbund, Parkraumgesellschaft Baden-Württemberg) bereit erklären, an dem Projekt mitzuwirken und ihre Daten zur Verfügung stellen. So sollen die Kommunen beispielsweise in das System einpflegen, welche Strecken gesperrt sind, wo sich Baustellen befinden und wie die Umleitungen geplant sind.

Kurz nachdem bekannt war, wer den Wettbewerb gewonnen hatte, wurde meine Dienststelle eingeladen, an der Auftaktveranstaltung mit den verschiedenen Akteuren teilzunehmen. Dort wurde das Projekt intensiv vorgestellt. Im Rahmen von mehreren Gesprächen mit den Konsortialpartnern wurden Einzelheiten präsentiert und verschiedene Fragen und Problempunkte beleuchtet.

Unklar war zunächst, ob ein Austausch personenbezogener Daten zwischen den einzelnen Partnern stattfindet. Es kam in Betracht, dass einzelne Projektpartner ihre bereits vorhandenen Daten in das neue System einpflegen sollten. Hier hat sich jedoch im weiteren Verlauf gezeigt, dass Datenschutz mittlerweile bekannt ist: Von den zu verpflichtenden Projektpartnern wurde selbst vorgetragen, dass sie dies nicht könnten, da sie dazu keine Ermächtigungsgrundlage hätten und folglich Probleme mit meiner Behörde bekommen würden. Es wurde daraufhin versichert, dass kein Austausch von personenbezogenen Daten innerhalb der Projektpartner erfolgt.

Ein Teilbereich des Projekts („Incentivierung") arbeitet mit einem Belohnungssystem, damit die Bürger motiviert sind, den kommunalen Verkehrs-Strategien zu folgen. Die Bürger können Bonuspunkte für die Nutzung des öffentlichen Personennahverkehrs erhalten, die sie dann in ideelle, virtuelle und geldwerte Prämien (die von den Kommunen zur Verfügung gestellt werden) eintauschen können. Voraussetzung ist die freiwillige Registrierung und die damit verbundene Preisgabe personenbezogener Daten. Um die MoveBW-App nutzen zu können, ist die Teilnahme am Incentivierungs-Projekt allerdings nicht erforderlich.

Ein weiterer Problempunkt war, inwieweit personenbezogene Daten verwendet werden, wenn die App in Echtzeit den Verkehrsteilnehmer begleitet und somit jederzeit feststellen kann, wo er sich befindet. Hier wurde mir ver-

sichert, dass der Nutzer die App auch anonym nutzen kann. Er muss nicht seinen tatsächlichen Standort preisgeben, sondern kann einen willkürlichen Standort benennen, von dem er seine Fahrtroute berechnet haben möchte. Dass logischerweise ein nachträgliches Ändern der Route aufgrund von Verkehrsstörungen nicht möglich ist, wenn sich der Nutzer nicht dazu bereit erklärt, seinen Standort verfolgen zu lassen, versteht sich von selbst.

Insgesamt verlief und verläuft die Beteiligung meiner Dienststelle sehr erfreulich. Ich wurde über das gesamte Projekt regelmäßig informiert und meine Hinweise wurden jederzeit aufgenommen und umgesetzt.

4.2 Bodensee-Oberschwaben-Verkehrsverbund (bodo) und Landestarif BW – Einführung eines E-Ticketing-Systems

Der Ticketkauf im öffentlichen Personennahverkehr soll für den Kunden komfortabler werden: Mittels Chipkarte soll es künftig möglich sein, schneller, einfacher und ohne Suche nach einem Fahrscheinautomaten die Fahrtberechtigung zu erwerben. Datenschutzrechtliche Probleme müssen im Vorfeld erkannt und gelöst werden.

Der Bodensee-Oberschwaben Verkehrsverbund (bodo) möchte ein E-Ticketing-System stufenweise einführen.

Grundlage dieser Form des Fahrscheins ist die sogenannte VDV-Kernapplikation. Dabei handelt es sich um eine IT-Anwendung mit zentralen Komponenten, Lesegeräten und einer Chipkarte, auf der der Fahrschein gespeichert wird. Die Anforderungen an ein solches System hat der Verband Deutscher Verkehrsunternehmen (VDV) festgeschrieben. Damit soll eine einheitliche Funktionsweise innerhalb Deutschlands sichergestellt werden. Es gibt verschiedene Stufen des Systems, von denen bodo sich in der ersten Projektstufe (Gelegenheitsfahrer) für die Stufe 3a („check-in-check-out-Verfahren") entschieden hat.

In der ersten Projektstufe wird bei bodo die für den Kunden kostenlose Chipkarte für Erwachsene und Kinder (6. bis vollendetes 15. Lebensjahr) angeboten. Gelegenheitsfahrer sollen beim Ein- und Ausstieg ihre Chipkarte vor ein Lesegerät halten, der Fahrpreis wird dann automatisch ermittelt („check-in-check-out-Verfahren"). Für Kunden mit Zeitkarten (Abonnements) soll die elektronische Chipkarte erst später in einer zweiten Projektstufe eingeführt werden.

Auf der Vorderseite der Chipkarte ist die Kundennummer des Fahrgastes aufgedruckt. Ein Foto ist nicht erforderlich. Auf der Karte selbst sind die Gültigkeit der Berechtigung (Beginn und Ende), das Ausgabedatum, die Service-Klasse (1. oder 2. Klasse) sowie der Fahrgasttyp (Erwachsener bzw. Kind) gespeichert.
Im E-Ticketing existieren grundsätzlich zwei Arten von Daten: zum einen sind dies die sog. Kundenstammdaten (Kontaktdaten), zum anderen sind dies sog. Fahrdaten (die pseudonymisiert sind). Die Kundenstammdaten werden ausschließlich von der bodo-Geschäftsstelle zum Zweck der Abrechnung von Fahrten erhoben, verarbeitet und genutzt und nicht an Dritte weitergegeben. Die Kundendatenbank ist von der Fahrdatenbank getrennt. Es besteht keine Zugriffsmöglichkeit der anderen Geschäftspartner.

Bei der Überprüfung der Fahrkarte durch das Fahrpersonal kann dieses auch nicht auf die im separaten Hintergrundsystem vorhandenen Kundendaten (z.B. Name und Adresse) zugreifen, sondern nur das erkennen, was auf der Karte tatsächlich vorhanden ist.

Kunden werden über die datenschutzrechtlichen Besonderheiten des Systems auf der Homepage von bodo umfassend aufmerksam gemacht. Es besteht auch die Möglichkeit, sich direkt mit Fragen an bodo zu wenden.

Bei diesem Projekt wurde meine Dienststelle frühzeitig eingebunden. In mehreren Gesprächen wurde das Projekt ausführlich dargestellt und mit mir abgestimmt, sodass meine Anmerkungen jederzeit umgesetzt wurden.

Mit der bodo-Chipkarte soll künftig auch die Möglichkeit bestehen, den vorgesehenen Landestarif Baden-Württemberg zu nutzen. Mit diesem Tarif soll es möglich sein, innerhalb Baden-Württembergs einen einheitlichen unternehmensneutralen Tarif für die Reise zu nutzen. Kunden müssen damit nicht mehr bei Überschreiten der Tarifverbundgrenzen ein neues Ticket erwerben, sondern können bei Fahrtantritt eine durchgängige Fahrkarte lösen. Bei der Vorstellung des Landestarifs war meine Behörde eingeladen. Meine Mitarbeiter

konnten sich davon überzeugen, dass Datenschutz ein für die Verkehrsunternehmen wichtiges Thema ist. Als angedacht wurde, dass die Verkehrsunternehmen personenbezogene Daten an eine dritte Stelle übermitteln sollten, wendeten sich die Verkehrsunternehmen mit Blick auf den Datenschutz hiergegen, sodass ein Eingreifen von meiner Seite nicht erforderlich war.

4.3 Echt-Bodensee-Card

Die frühe Beteiligung meiner Behörde kann vorteilhaft sein: So kann ich schon frühzeitig auf aus vergleichbaren Projekten bekannte Risiken hinweisen und Anregungen geben, wie ein Vorgang datenschutzgerecht ausgestaltet werden kann. Leider passiert es gelegentlich, dass meine Behörde erst nach Start des Projektes hinzugezogen wird bzw. selbst auf die verantwortliche Stelle zugehen muss. Dies ist u.a. dann der Fall, wenn sich Betroffene an mich wenden und datenschutzrechtliche Verstöße anzeigen. Das macht die Zusammenarbeit mit dem Projektträger nicht einfacher ...

Schon im vergangenen Jahr erreichten mich Schreiben besorgter Gastgeber der Bodenseeregion: Es sei geplant, eine Gästekarte einzuführen, bei der umfangreiche personenbezogene Daten erhoben würden. Mir war zu diesem Zeitpunkt nicht bekannt, dass ein solches Vorhaben geplant ist und ich ging davon aus, dass das verantwortliche Unternehmen rechtzeitig auf mich zukommen werde, weil es eben auch viele kritische Stimmen im Vorfeld gab. Bedauerlicherweise war dies nicht der Fall: Die Echt-Bodensee-Card ging an den Start und die Anfragen bei meiner Behörde häuften sich. Daraufhin kündigte ich mich bei der Deutschen Bodensee Tourismus GmbH an und meldete erhebliche datenschutzrechtliche Bedenken an der Vorgehensweise an.

Die Deutsche Bodensee Tourismus GmbH stellte mir dann in einem persönlichen Gespräch das Projekt umfangreich vor. Auf der nicht übertragbaren Karte werden der codierte Vor- und Nachname gespeichert (so wird bspw. Martin Mustermann zu Mxxxxn Mxxxxxxxxn). Bei Kontrollen werde abgeglichen, ob der auf der Karte vermerkte codierte Name mit einem Ausweisdokument übereinstimmt. Damit solle vermieden werden, dass die Karte missbräuchlich genutzt wird. Des Weiteren werden die Gültigkeitsdauer (in der Regel die Dauer des Aufenthalts) sowie die Alterskategorie (Erwachsener, Kind) gespeichert. Zudem werden sog. Berechtigungs-IDs auf der Karte gespeichert. Diese seien nicht in der Person selbst oder den Eigenschaften der Person des Nutzers begründet, sondern in Eigenschaften etwa in Bezug auf seinen Urlaubsort oder die Jahreszeit. So könnten bspw. alle Gäste einer bestimmten Gemeinde einen ermäßigten Eintritt ins Strandbad erhalten.

Bei dem System müsse zwischen zwei „Datenkreisläufen" unterschieden werden. Zum einen würden die nach Bundesmeldegesetz erforderlichen Meldedaten des Gastes durch den Beherbergungsbetrieb erfasst und an die Meldebehörde weitergeleitet. Dies entspräche dem bisherigen Prozedere, es werde lediglich der Meldeschein durch ein elektronisches Verfahren ersetzt. Zugriff auf die Meldedaten hätten ausschließlich die Meldebehörde und der eingebende Gastgeber.

Zum anderen habe die Deutsche Bodensee Tourismus GmbH ein Interesse daran, ob und mit welcher Häufigkeit die Echt-Bodensee-Card ausgegeben und genutzt wird. Zu diesem Zweck solle an die Bodensee Tourismus GmbH gemeldet werden, in welcher Häufigkeit die Karte eingesetzt wird. So würden etwa die Strandbäder an die Deutsche Bodensee Tourismus GmbH melden, wie viele freie bzw. ermäßigte Eintritte erfolgten oder wie oft der öffentliche Personennahverkehr genutzt werde. Ein Personenbezug werde dabei nicht hergestellt.
Die Gastgeber selbst stellten die Karten aus. Sie codierten die Karten und übergeben diese an die Gäste. Zu Kontroll- oder Bearbeitungszwecken (etwa wenn der Gast seinen Aufenthalt verlängert) könnten die Daten vom Gastgeber ausgelesen werden. Dabei habe der Gastgeber nur Zugriff auf die von ihm erfassten Daten. Werde eine Gästekarte von einem anderen Gastgeber ausgelesen, werde diesem nur der Gültigkeitszeitraum angezeigt.

Ich habe die Deutsche Bodensee Tourismus GmbH darauf hingewiesen, dass das Konzept mit den zwei unterschiedlichen Datenbanken grundsätzlich in Ordnung sei, es aber für mich schwierig ist, das Konzept aufgrund der späten Beteiligung vollständig nachvollziehen zu können. Es müsse gewährleistet sein, dass die Meldedaten nur an die Meldebehörde gehen und nicht an Dritte, wie etwa die Deutsche Bodensee Tourismus GmbH. Die Deutsche Bodensee Tourismus GmbH hat mir versichert, dass die

Meldedaten ausschließlich an die Meldebehörde übermittelt würden und sie selbst lediglich anonymisierte Daten bzw. nur Daten aufgrund einer ausdrücklichen Einwilligung erhalte.

Weiter habe ich der Deutschen Bodensee Tourismus GmbH empfohlen, die Datenschutzbestimmungen grundlegend zu überarbeiten. Zum aktuellen Zeitpunkt sind diese missverständlich und zu allgemein formuliert. Auch mit Hinblick auf die besonderen Erfordernisse der Datenschutz-Grundverordnung herrscht hier deutlicher Überarbeitungsbedarf. Des Weiteren habe ich dringenden Aufklärungs- bzw. Schulungsbedarf bei den teilnehmenden Gemeinden, aber auch bei den teilnehmenden Gastgebern gesehen.

Zwischenzeitlich erreichte mich aus der Presse die Mitteilung, dass ein Normenkontrollverfahren bezüglich der Echt-Bodensee-Card am Verwaltungsgerichtshof anhängig sei und die Richter ernsthafte datenschutzrechtliche Bedenken hätten. Gegenstand des Verfahrens war eine Kurtaxesatzung, die von mir nicht überprüft wurde. Die Richter kamen zum Ergebnis, dass u.a. keine Verpflichtung der Gastgeber bestehe, die Echt-Bodensee-Card auszugeben. Nähere Einzelheiten des Kartenverfahrens waren nicht Gegenstand der mündlichen Verhandlung.

Es bleibt abzuwarten, ob das ganze System im Nachgang noch in Einklang mit den datenschutzrechtlichen und anderen rechtlichen Bestimmungen zu bringen ist. Dies ist meines Erachtens ein schwieriges – vielleicht sogar wenig erfolgversprechendes – Unterfangen.

4.4 Überlassung von Rohmessdaten aus Geschwindigkeitsmessungen an private Sachverständige

Bei Herausgabe von sog. Rohmessdaten ist von den Bußgeldstellen zu beachten, von wem der Auftrag zur Erstellung des Gutachtens stammt. Lediglich wenn es sich um ein Privatgutachten und nicht um ein gerichtliches Gutachten handelt, hat die Bußgeldstelle ein Ermessen, ob und in welcher Form sie die Daten herausgibt.

Ein privater Sachverständiger wandte sich mit folgendem Problem an mich: Er überprüfe als Sachverständiger für Verkehrsmesstechnik sowohl im gerichtlichen als auch im privaten Auftrag, ob die festgestellten Geschwindigkeits-, Abstands- und Rotlichtverstöße durch das eingesetzte Messgerät ordnungsgemäß gemessen wurden. Moderne Messgeräte erstellen digitale Datensätze (Original-Messdateien). Diese Datensätze beinhalten in der Regel nicht nur ein Messbild, sondern auch weitere Informationen, wie etwa den gemessenen Geschwindigkeitswert, Datum und Uhrzeit. Damit der Sachverständige bewerten kann, ob Auffälligkeiten im Messverlauf bzw. Probleme beim Messsystem auftreten, benötigt er nicht nur die jeweilige Aufnahme mit dem Betroffenen, sondern in der Regel die gesamte Messreihe. Dies bedeutet, dass der Gutachter alle bspw. an einem bestimmten Tag aufgenommenen „Verkehrssünder" erkennen kann und nicht nur denjenigen, der Beteiligter des aktuellen Verfahrens ist. Die Zentrale Bußgeldstelle beim Regierungspräsidium Karlsruhe, bei der die Datensätze aller Messungen auf Autobahnen in Baden-Württemberg aufbewahrt werden, hat nunmehr eine Erklärung zur Beweismittelanforderung verlangt, bevor die Datensätze an die Sachverständigen herausgegeben werden. Danach sollen die Sachverständigen versichern, dass sie sämtliche Daten von Dritten auch gegenüber den Verfahrensbeteiligten anonymisieren. Damit stellt sich dem Sachverständigen folgendes Problem: Treten Auffälligkeiten bei Messgeräten auf, so werden diese in der Regel erst beim Auswerten der gesamten Messreihe erkennbar. Dies bedeutet, dass die Auffälligkeit zwar bei dem aktuell Betroffenen auftreten kann, aber eben auch bei den auf der Messreihe vorhandenen Dritten. Stellt der Sachverständige eine solche Auffälligkeit bei einem Dritten fest, hat er keine Möglichkeit, dies bspw. im Rahmen einer Hauptverhandlung zu thematisieren, da er die Anonymität von Dritten zugesichert hat. Zudem wird die Originaldatei durch die Anonymisierung nachträglich manipuliert. Die ursprüngliche Falldatei kann nicht mehr angezeigt werden und somit vom Gericht im Rahmen der Beweisaufnahme nicht mehr objektiv nachvollzogen werden.

Dem Sachverständigen und dem Regierungspräsidium Karlsruhe teilte ich Folgendes mit:
Unabhängig davon ob, der Sachverständige öffentlich bestellt und vereidigt ist oder nicht, ist danach zu unterscheiden, in welcher Funktion ihm die Daten übermittelt werden.

Zum einen wird der Sachverständige im Rahmen eines Gerichtsverfahrens als gerichtlicher Sachverständige bestellt. Hierzu ergeht ein Gerichtsbeschluss, der den Gutachtenauftrag

beschreibt und auf die zur Erstellung des Gutachtens notwendigen Beweismittel eingeht. Hierbei wird in der Regel auf die sog. Originalmessdateien Bezug genommen. Liegt ein solcher Gerichtsbeschluss vor, hat die Verwaltungsbehörde keinen eigenen Entscheidungsspielraum, ob und unter welchen Voraussetzungen sie die Dateien herausgibt. Im Rahmen des gerichtlichen Gutachtenauftrags wird der Sachverständige auf die Verschwiegenheit und den korrekten Umgang mit den Daten durch das Gericht hingewiesen. Auf Seiten der Verwaltungsbehörde ist nach § 16 Absatz 2 Sätze 2 und 3 des Landesdatenschutzgesetzes (LDSG) lediglich zu prüfen, ob das Übermittlungsersuchen im Rahmen der Aufgaben der ersuchenden Stelle liegt, es sei denn, dass ein besonderer Anlass zur Prüfung der Zulässigkeit der Datenübermittlung besteht. § 49a Absatz 1 Satz 1 des Gesetzes über Ordnungswidrigkeiten (OWiG) ist hier nicht einschlägig, da dieser nur die Zulässigkeit verfahrensübergreifender Datenübermittlung regelt und nicht die Übermittlung von Daten an die im konkreten Verfahren mitwirkenden Stellen und im Instanzenzug.

Zum anderen kann ein Sachverständiger bereits schon im dem Gerichtsverfahren vorgelagerten Bußgeldverfahren durch einen Betroffenen beauftragt werden. Hier ist § 49 Absatz 1 OWiG zu beachten. Danach kann die Verwaltungsbehörde dem Betroffenen Einsicht in die Akten unter Aufsicht gewähren, soweit nicht überwiegende schutzwürdige Interessen Dritter entgegenstehen. Selbst wenn die Rohdateien unter den Begriff der Akten fallen sollten (es wird größtenteils vertreten, dass diese amtlich verwahrte Beweisstücke gem. § 147 Absatz 1 der Strafprozessordnung (StPO) darstellen, die lediglich in der Dienststelle besichtigt werden dürfen), so steht der Verwaltungsbehörde ein Ermessenspielraum zu, ob die Akteneinsicht gewährt werden kann. Dabei ist zu berücksichtigen, dass auf den Rohdateien eine Vielzahl personenbezogener Daten Dritter enthalten sind, die es zu schützen gilt. Gegen den ablehnenden Bescheid der Verwaltungsbehörde kann der Betroffene gem. § 62 Absatz 1 Satz 1 OWiG gerichtliche Entscheidung beantragen. Wenn das zuständige Gericht der Ansicht ist, dass die Akteneinsicht zu gewähren ist, hat die Verwaltungsbehörde diesem Gerichtsbeschluss Folge zu leisten und keinen weiteren eigenen Ermessensspielraum.

Die Gestaltung der Beweisaufnahme ist Sache des Gerichts, die datenschutzrechtlich durch mich nicht überprüft werden kann. Dies bedeutet, dass das Regierungspräsidium insbesondere nicht verlangen kann, dass der Sachverständige die Daten Dritter auch gegenüber Verfahrensbeteiligten anonymisiert. Die allgemeinen datenschutzrechtlichen Belehrungen, bspw. wie mit den Daten umzugehen ist (vertraulich, gesichertes System etc.), stellen meiner Ansicht nach eine Selbstverständlichkeit dar, die auch im Gutachtenbeschluss der Gerichte an die Sachverständigen zu beachten sein sollten und aus Klarstellungsgründen in der Erklärung verbleiben können.

4.5 Geschwindigkeitsmessungen bei Gemeinden durch Private

Gemeinden dürfen sich bei der Durchführung von Geschwindigkeitsmessungen unterstützen lassen. Voraussetzung dafür ist jedoch, dass die Gemeinde immer „Herrin des Ordnungswidrigkeitenverfahrens" ist.

Immer wieder erreichen mich Anfragen, inwiefern private Firmen an Geschwindigkeitsmessungen bei Gemeinden beteiligt sein dürfen. Die Gemeinden als Polizeibehörden verfolgen und ahnden Verkehrsordnungswidrigkeiten, um die Sicherheit des Straßenverkehrs zu gewährleisten. Dabei beziehen Gemeinden Privatfirmen in die Verfolgung von Ordnungswidrigkeiten ein, da sie selbst oftmals nicht über die erforderliche Technik verfügen, um die Geschwindigkeitsmessung durchführen zu können. Deshalb wird mit privaten Firmen, die diese Technik und auch die dafür erforderlichen Mitarbeiter anbieten, ein Vertrag geschlossen. Der Umfang dieses Vertrags ist verschieden ausgestaltet: Teilweise dürfen die privaten Messfirmen die Messfotos eigenständig anfertigen, teilweise ist ein Mitarbeiter der Stadt bei der eigentlichen Messung vor Ort und leitet die private Firma an. Auch der weitere Fortgang des Verfahrens ist unterschiedlich ausgestaltet. Zum Teil bereiten die privaten Firmen die Fotos nur auf und markieren solche Aufnahmen, die im Rahmen eines Ordnungswidrigkeitenverfahrens nicht verwertbar sein könnten (etwa weil das Kennzeichen nicht zu erkennen ist). Es gibt jedoch auch Ausgestaltungen dergestalt, dass die private Firma selbstständig entscheiden darf, gegen wen ein Bußgeldverfahren eingeleitet wird.

Für das Anfertigen von Messfotos ist nach dem Datenschutzrecht entweder eine gesetzliche Rechtsgrundlage oder eine Einwilligung der Betroffenen erforderlich. Dass eine Einwilligung der betroffenen Autofahrer denklogisch nicht eingeholt werden kann, versteht sich von selbst. Private Firmen, die Messfotos erstellen, haben jedoch auch keine Rechtsgrundlage, die ihnen das Anfertigen solcher Fotos erlaubt. Dies ist hoheitliche Aufgabe der Polizeibehörden, d.h. u.a. der Gemeinden. Nur diese sind berechtigt, die Verstöße gegen das Straßenverkehrsrecht zu verfolgen und zu ahnden.

Bei der Verkehrsüberwachung ist die Hinzuziehung privater Firmen möglich, solange die Ordnungsbehörde Herrin des Verfahrens bleibt. Für letzteres ist erforderlich, dass die Ordnungsbehörde die Kontrolle über die Ermittlungsdaten, die ihrer Entscheidung über die Durchführung eines Bußgeldverfahrens zu Grunde liegen, behalten muss. Dies sind in der Regel die Messdaten des Verkehrsüberwachungsgeräts. Zudem muss sie Herrin über die Entscheidung bleiben, ob und gegen wen sie ein Ermittlungsverfahren einleitet. Die beauftragte Privatfirma darf lediglich behilflich sein und etwa die erfassten Bilder aufbereiten. Eine eigene Entscheidung der privaten Firma ist nicht zulässig.

Damit private Messfirmen datenschutzgerechtlich tätig werden können, ist formell ein Auftragsdatenverarbeitungsvertrag nach § 7 Absatz 2 des Landesdatenschutzgesetzes (LDSG) erforderlich. Auf diese Weise ist sichergestellt, dass die Gemeinde verantwortliche Stelle im Sinne des Datenschutzrechts bleibt und die beauftragte Firma selbst keine personenbezogenen Daten zu eigenen Zwecken verarbeitet.

5. Justiz

5.1 Einführung der elektronischen Gerichtsakte

Im Jahr 2016 wurde bei einigen Zivilkammern des Landgerichts Mannheim und einigen Kammern des Arbeitsgerichts Stuttgart im Rahmen eines Pilotprojekts die elektronische Gerichtsakte eingeführt. Bis zum Jahr 2020 soll die Einführung der elektronischen Aktenführung – mit Ausnahme der Strafjustiz – bei allen Gerichtsbarkeiten in Baden-Württemberg abgeschlossen sein. Für Strafverfahren wird die Einführung später, jedoch spätestens zum 1. Januar 2026 erfolgen.

Die Einführung der elektronischen Gerichtsakte steht in engem Zusammenhang mit der Einführung des elektronischen Rechtsverkehrs. Ab dem 1. Januar 2018 können bei allen Gerichten und Staatsanwaltschaften in Baden-Württemberg elektronische Dokumente eingereicht werden. Die Umstellung auf die elektronische Aktenführung soll u.a. sicherstellen, dass die digitale Post innerhalb der Gerichte papierlos am Computer bearbeitet werden kann, um Medienbrüche zur Papierakte zu vermeiden.
Um sicherzustellen, dass der Schutz des informationellen Selbstbestimmungsrechts auch im Rahmen der papierlosen Gerichtsakte gewährleistet ist, sind umfangreiche technische und organisatorische Maßnahmen zu ergreifen, die komplexe Datenschutz- und Datensicherheitskonzepte erfordern.

Meine Dienststelle wurde seit dem Jahr 2016 mehrmals vom Ministerium der Justiz und für Europa mündlich und schriftlich über den Fortgang dieser Arbeiten und den Verlauf des Pilotprojekts informiert. So hatten Mitarbeiter meiner Dienststelle im Dezember 2016 die Gelegenheit, das Arbeitsplatzlabor beim Arbeitsgericht Stuttgart zu besuchen. Darüber hinaus liegen meiner Dienststelle verschiedenste, teils mehrere hundert Seiten umfassende Ausarbeitungen vor, die sich mit datenschutzrechtlich relevanten Aspekten der elektronischen Gerichtsakte befassen. Diese Papiere sind teilweise veraltet, äußerst unübersichtlich und teilweise nicht aufeinander abgestimmt und insoweit nicht geeignet, das Projekt vollständig und nachvollziehbar darzustellen. Aus diesem Grund war eine abschließende datenschutzrechtliche Prüfung und Bewertung des Projekts bislang nicht möglich. Ich habe das Ministerium der Justiz und für Europa daher aufgefordert, die von meiner Dienststelle anhand der vorliegenden Unterlagen formulierten datenschutzrechtlichen Anforderungen zeitnah in ein schlüssiges und nachvollziehbares Datenschutz- und Datensicherheitskonzept einzuarbeiten.

Die bei der Einführung der elektronischen Gerichtsakte zu berücksichtigenden datenschutzrechtlichen Anforderungen sind äußerst komplex. Ob und wie diese Anforderungen nachvollziehbar umgesetzt werden, wird meine Dienststelle auch weiterhin verfolgen.

5.2 Längerfristige verdeckte Videoüberwachung im Rahmen eines Ermittlungsverfahrens

Durch eine Eingabe hat meine Dienststelle von folgendem Vorgang Kenntnis erlangt:

In einem im Jahr 2016 geführten, zwischenzeitlich eingestellten Ermittlungsverfahren wegen des Verdachts der schweren Brandstiftung war die zuständige Staatsanwaltschaft aufgrund verschiedener Indizien davon ausgegangen, dass der oder die Täter der autonomen Szene zuzuordnen seien und es zu weiteren Straftaten kommen werde. Zur Ermittlung des Beschuldigten hatte die Staatsanwaltschaft daraufhin – ohne hierfür eine richterliche Anordnung einzuholen – die nächtliche Videoüberwachung des Haupteingangs eines Gebäudes mit zum damaligen Zeitpunkt 101 Bewohnern angeordnet, das als Wohnsitz von Angehörigen der autonomen Szene bekannt ist. Die Staatsanwaltschaft vermutete Folgetaten und hatte sich aus der Videoüberwachung Erkenntnisse hierzu erhofft, die auch zu einem Tatverdächtigen hinsichtlich der Ausgangstat führen. Die von der Videokamera bei Bewegungsauslösung aufgezeichneten Daten sind nach jeweils 24 Stunden überschrieben worden. Da es dann allerdings doch nicht zu Folgetaten kam, wurde die ursprünglich auf zwei Monate befristete Maßnahme nach rund einem Monat beendet. Nach Beendigung der Maßnahme wurden sämtliche Daten gelöscht.

Meine Dienststelle vertrat hierzu die Ansicht, dass die Videoüberwachung auf eine längerfristige Observation von Kontaktpersonen ausgerichtet war, die gemäß § 163f der Strafprozessordnung (StPO) einer richterlichen Anordnung bzw. einer richterlichen Bestätigung

bedurft hätte. Die genannte Vorschrift regelt, unter welchen Voraussetzungen ein Beschuldigter oder Personen, von denen anzunehmen ist, dass sie mit dem Täter in Verbindung stehen, entweder länger als durchgehend 24 Stunden oder zwar unterbrochen, aber an mehr als zwei Tagen beobachtet werden dürfen. Die zuständige Staatsanwaltschaft war dagegen der Meinung, dass § 163f StPO im aktuellen Fall nicht anzuwenden sei, da zu keinem Zeitpunkt ein konkreter Beschuldigter von der Maßnahme betroffen gewesen sei und sich die Maßnahme auch nicht gegen Kontaktpersonen im Sinne des § 163f StPO gerichtet habe. Es habe sich vielmehr um eine Objektüberwachung gehandelt, die von § 163f StPO nicht erfasst werde. Die Maßnahme habe daher nicht von einem Richter angeordnet oder bestätigt werden müssen.
Diese Argumentation war für meine Dienststelle nicht nachvollziehbar. Der Hauseingang des Gebäudes war überwacht worden, weil bekannt war, dass Mitglieder der autonomen Szene in dem Gebäude wohnen und vermutet wurde, dass der oder die Täter aus der autonomen Szene stammen. Die Videoüberwachung zielte damit auf diesen konkreten Personenkreis ab. Die Argumentation der Staatsanwaltschaft, dass bei Folgetaten die Erkenntnisse aus der nächtlichen Videoüberwachung zu einem Tatverdächtigen auch hinsichtlich der Ausgangstat hätte führen können, zeigt außerdem, dass vermutet wurde, dass der Täter zu den der autonomen Szene zuzuordnenden Bewohnern des Gebäudes Kontakt hat.

Da die Staatsanwaltschaft an ihrer Auffassung festhielt, hat sich meine Dienststelle in der Angelegenheit an das Ministerium der Justiz und für Europa gewandt. Dieses hat mir zum einen mitgeteilt, es teile unsere Auffassung, dass für die nächtliche Videoüberwachung des Gebäudeeingangs eine richterliche Anordnung bzw. Bestätigung erforderlich gewesen wäre und zum anderen, dass bei der für den Fall zuständigen Staatsanwaltschaft zwischenzeitlich Vorsorge dafür getroffen worden sei, dass bei vergleichbaren Konstellationen künftig eine richterliche Anordnung erwirkt werde.

5.3 Mitteilung Zeugendaten im Verfahren über Ordnungswidrigkeiten

Wie anonym ist der Zeuge im Verfahren über Ordnungswidrigkeiten zu behandeln? Darf der mutmaßliche Betroffene wissen, wer der Zeuge ist und wo er wohnt?

Mehrfach traten besorgte Bürger an mich heran, weil sie als Zeuge einer Ordnungswidrigkeit durch die Bußgeldstelle darauf hingewiesen wurden, dass sowohl ihr Name als auch ihre vollständige Adresse dem Betroffenen, gegen den sich das Bußgeldverfahren richtet, mitgeteilt werden. Dies sorgte für Ängste bei den Zeugen. Es wurde befürchtet, dass der Betroffene an sie herantrete und sich für die Anzeige rächen werde.

Die Bußgeldstellen vertraten die Auffassung, dass der Betroffene darüber informiert werden müsse, wer der Zeuge sei. Der Betroffene müsse möglichst frühzeitig einschätzen können, ob der Tatvorwurf beweisbar sei oder nicht.
Gegen diese Vorgehensweise bestehen datenschutzrechtliche Bedenken.

Soweit die bisher herrschende Auffassung zu § 66 des Gesetzes über Ordnungswidrigkeiten (OWiG) unter Hinweis auf die ältere Rechtsprechung aus der Pflicht zur Angabe der Beweismittel im Bußgeldbescheid (§ 66 Absatz 1 Nr. 4 OWiG) folgert, Zeugen seien mit Namen und Anschrift anzugeben, überzeugt dies im Hinblick auf die Änderung von § 200 der Strafprozessordnung (StPO) durch das Zweite Opferrechtsreformgesetz (vom 29. Juli 2009, BGBl. I 2280) nicht (mehr): Auch für die Anklage im Strafprozess wird nach § 200 Absatz 1 Satz 2 StPO die Angabe der Beweismittel gefordert. Die Angabe der Anschrift eines Zeugen ist indes nicht erforderlich, § 200 Absatz 1 Satz 3 StPO. Diese Regelung sollte nach dem Grundgedanken der Geltung der Strafprozessordnung für das Gesetz über Ordnungswidrigkeiten (§ 46 Absatz 1 OWiG) auch für den Bußgeldbescheid Anwendung finden. Es sind keine Gründe ersichtlich, weshalb an die Bezeichnung der Beweismittel in einem Bußgeldbescheid strengere Anforderungen zu stellen sind als in einer Anklage.

Auch im dem Bußgeldverfahren vorgelagerten Verwarnungs- bzw. Anhörungsverfahren kann nichts anderes gelten.

Über eine Verwarnung wird lediglich eine Bescheinigung erteilt (vgl. § 56 Absatz 3 OWiG), die nicht mit dem Bußgeldbescheid vergleichbar ist. Daher bedürfte es an sich nicht der Angabe von Beweismitteln im Verwarnungsverfahren, auch wenn die Kenntnis von der Art der Beweismittel sicherlich dazu geeignet sein kann, dass der Betroffene die Verwarnung eher akzeptiert.

Indes ist mit der Verwarnungsbescheinigung standardmäßig auch eine Anhörung nach § 55 OWiG verbunden für den Fall, dass der Betroffene die Verwarnung nicht akzeptiert bzw. das Verwarnungsgeld nicht rechtzeitig bezahlt. Für die Anhörung ist § 136 Absatz 2 StPO (über die Verweisung in § 46 Absatz 1 OWiG) zu beachten, wonach dem Beschuldigten durch die Vernehmung Gelegenheit zu geben ist, die gegen ihn vorliegenden Verdachtsgründe zu beseitigen und die zu seinen Gunsten sprechenden Tatsachen geltend zu machen. Dafür ist jedoch notwendig, dass ihm die wesentlichen Verdachtsgründe - und damit auch die Zeugen - genannt werden. Hierbei sind die oben ausgeführten Grundsätze zu beachten, wonach nicht die vollständige Adresse zu nennen ist.

Es erscheint mir nicht nachvollziehbar, weshalb der Betroffene die vollständige Anschrift des Zeugen benötigt, um einzuschätzen, ob der Tatvorwurf realistisch ist. Dafür ist die Angabe des Wohnortes des Zeugen ausreichend.

Die betroffenen Bußgeldstellen haben mittlerweile ihre Verwaltungspraxis dahingehend geändert und geben neben dem Namen des Zeugen lediglich noch den Wohnort und nicht mehr die vollständige Adresse an.

6. Kommunales

6.1 Einsatz von digitalen Wasserzählern mit Funkmodul

Der Einsatz von digitalen Wasserzählern, die per Funk auslesbar sind, ist auf eine normenklare Rechtsgrundlage zu stützen, soweit dabei personenbezogene Daten verarbeitet werden. Auch müssen diese Wasserzähler bestimmte Anforderungen an die Technik erfüllen.

Baden-württembergische Gemeinden bauen zunehmend digitale Wasserzähler mit Funkmodul ein. Einzelne Betroffene fühlten sich hierdurch in ihrem Grundrecht auf informationelle Selbstbestimmung verletzt und haben sich deshalb im Berichtszeitraum an meine Dienstelle gewendet. Leider war bei der Befassung mit dieser Thematik nicht immer erkennbar, dass die entsprechenden Gemeinden sich vor dem Einbau von digitalen Wasserzählern, die per Funk ausgelesen werden können, hinreichend mit den damit verbundenen datenschutzrechtlichen Anforderungen auseinandergesetzt haben (wie etwa, auf welche Rechtsgrundlage die Verarbeitung von personenbezogenen Daten insoweit gestützt werden kann).

Die in digitalen Wasserzählern gespeicherten Daten können personenbeziehbar sein (z.B. auf den Gebührenschuldner oder auf Bewohner eines Hauses). Soweit die Herstellung eines Personenbezugs möglich ist, bedarf die Verarbeitung solcher Daten einer Rechtsgrundlage. Für den Einsatz von digitalen Wasserzählern, die per Funk personenbezogene Daten übertragen, gibt es derzeit keine formell-materielle Rechtsgrundlage (also ein Parlamentsgesetz, das ausdrücklich diese Form der Datenverarbeitung regelt). Jedoch kommen als Rechtsgrundlage grundsätzlich auch kommunale Satzungen (z.B. Wasserversorgungssatzungen) in Betracht, wenn diese bestimmten datenschutzrechtlichen Anforderungen genügen.

Insbesondere muss eine kommunale Satzung klar erkennen lassen, ob und ggf. inwieweit die Verarbeitung personenbezogener Daten zulässig sein soll. Die Datenverarbeitung muss mit Blick auf den ihr zu Grunde liegenden Zweck und die Intensität des Eingriffs in das Recht auf informationelle Selbstbestimmung geeignet, erforderlich und verhältnismäßig sein. Eine Satzung, die das Verarbeiten personenbezogener Daten regelt, muss für die Betroffenen die Eingriffsintensität und den konkreten Zweck der Datenverarbeitung hinreichend deutlich erkennen lassen. Der Wortlaut der Satzung muss hinreichend klar die durch den Zweck sowie die Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit gezogenen Grenzen bestimmen, innerhalb derer das Verarbeiten personenbezogener Daten zulässig sein soll.

Wenn in einer kommunalen Satzung die Verarbeitung personenbezogener Daten mittels digitaler Wasserzähler mit Funkmodul geregelt werden soll, ist insbesondere Folgendes zu beachten:

- Ein eingesetztes Funkmodul muss deaktivierbar sein.
- Die Übertragung personenbezogener Daten per Funk ist durch technisch-organisatorische Maßnahmen gegen einen unbefugten Zugriff Dritter oder eine Beeinflussung von außen zu schützen. Insbesondere sind Datenübertragungen per Funk nach dem Stand der Technik mit einem individuellen Schlüssel zu verschlüsseln und unidirektionale Sendeeinheiten zu verwenden.
- Es dürfen nur die personenbezogenen Daten erhoben werden, die für Abrechnungszwecke erforderlich sind oder deren Verarbeitung im öffentlichen Interesse liegt.
- Ein öffentliches Interesse kann z.B. die Trinkwasserhygiene, die Leckortung oder die Überprüfung eines Manipulationsverdachts sein.
- Ggf. muss eine Gemeinde für jedes einzelne Datum, das verarbeitet wird, darlegen können, warum dies zur Aufgabenerfüllung erforderlich ist. Dabei ist der restriktive Erforderlichkeitsbegriff des Datenschutzrechts anzuwenden. Daten, die zu Abrechnungszwecken oder im öffentlichen Interesse verarbeitet werden dürfen, sind u.a. Zählernummern, Verbrauchsstände, Betriebs- und Ausfallzeiten sowie Fehlermeldungen (wie Leckage, Rohrbruch, Trocken oder Defekt).

Soweit sich Bürger beschwert fühlen, kann es sein, dass bei der rechtlichen Bewertung eines Lebenssachverhalts verschiedenen Rechtsfragen aus unterschiedlichen Rechtsgebieten Bedeutung zukommt. So ging es Betroffenen, die sich wegen des verpflichtenden Einbaus digitaler Wasserzähler mit Funkmodul an meine Dienststelle gewandt hatten, nicht immer nur um die Wahrung ihres informationellen Selbstbestimmungsrechts, sondern teilweise

auch um Aspekte außerhalb des Datenschutzrechts (wie etwa Bedenken bezüglich der Auswirkungen von Funkstrahlen oder Bedenken in Hinblick auf einen möglichen Eingriff in das Recht auf Unverletzlichkeit der Wohnung). Hier musste ich klarstellen, dass sich meine Dienststelle grundsätzlich nur mit datenschutzrechtlichen Fragestellungen näher befassen kann. Nach meiner Rechtsauffassung ist es aus datenschutzrechtlicher Sicht zwar ausreichend, wenn das Übertragen personenbezogener Daten durch digitale Wasserzähler per Funk in kommunalen Satzungen geregelt wird, soweit die o.g. Maßgaben dabei hinreichend beachtet werden. Jedoch könnte es mit Blick auf ein einvernehmliches soziales Miteinander zu erwägen sein, dass Gemeinden digitale Wasserzähler mit aktiviertem Funkmodul nur dann einsetzen, wenn die hiervon Betroffenen damit einverstanden sind.

Wenn Gemeinden die Verarbeitung personenbezogener Daten mittels digitaler Wasserzähler mit Funkmodul in einer kommunalen Satzung regeln, ist dies zulässig, solange dabei datenschutzrechtliche Belange hinreichend beachtet werden. Selbstverständlich sollte sein, dass eine kommunale Satzung in Kraft getreten sein muss, bevor auf ihrer Grundlage die Verarbeitung personenbezogener Daten erfolgen kann.

6.2 Veröffentlichung von Beratungsunterlagen und Beschlüssen von gemeindlichen Gremien

Soweit Beratungsunterlagen und Beschlüsse gemeindlicher Gremien personenbezogene Daten beinhalten und die entsprechenden Unterlagen veröffentlich werden sollen, bedarf es hierfür einer normenklaren Rechtsgrundlage, die ausdrücklich diese Form der Datenverarbeitung erlaubt (datenschutzrechtliches Verbot mit Erlaubnisvorbehalt).

Am 31. Oktober 2016 ist § 41b der Gemeindeordnung für Baden-Württemberg (GemO) in Kraft getreten, der die Veröffentlichung von Informationen durch Gemeinden regelt. Das damit verbundene Ziel, die Arbeit kommunaler Gremien für die Öffentlichkeit noch transparenter zu gestalten, begrüße ich ausdrücklich. Einige Gemeinden waren jedoch in Bezug auf Belange des Datenschutzes unsicher und haben sich deshalb an meine Dienstelle mit der Bitte um Beratung gewandt. Gegenstand von Beratungsanfragen war auch die Veröffentlichung von in öffentlicher Sitzung gefassten oder bekanntgegebenen Beschlüssen auf der gemeindlichen Internetseite.

Internetveröffentlichungen von Beratungsunterlagen mit personenbezogenen Daten

Nach § 41b Absatz 2 Satz 1 GemO sind Tagesordnung und beigefügte Beratungsunterlagen für öffentliche Gremiensitzungen im Internet zu veröffentlichen, nachdem diese den Mitgliedern des Gemeinderats zugegangen sind. Jedoch ist nach Satz 2 durch geeignete Maßnahmen sicherzustellen, dass durch eine entsprechende Internetveröffentlichung keine personenbezogenen Daten unbefugt offenbart werden. Somit ist § 41b Absatz 2 Satz 1 GemO selbst keine Vorschrift, die es einer Gemeinde erlauben würde, Beratungsunterlagen mit personenbezogenen Daten in den gemeindlichen Internetauftritt einzustellen. Auch ein Blick in die diesbezügliche Gesetzesbegründung unterstreicht dies. Ihr ist u.a. zu entnehmen, dass die mit einer Internetveröffentlichung „verbundenen weitreichenden Verletzungen des Rechts auf informationelle Selbstbestimmung […] durch geeignete Maßnahmen, z.B. eine zuverlässige Anonymisierung der zu veröffentlichen Dokumente, zu vermeiden" sind.

Der Gesetzgeber hat jedoch berücksichtigt, dass Maßnahmen, die eine unbefugte Offenbarung personenbezogener Daten verhindern sollen, mit einem erhöhten Aufwand für die Gemeinden verbunden sein können. Um zu vermeiden, dass dieser Aufwand unverhältnismäßig groß wird, hat er in § 41 Absatz 2 Satz 3 GemO geregelt, dass im Einzelfall von Veröffentlichungen abgesehen werden kann, wenn solche Maßnahmen nicht ohne erheblichen Aufwand oder ohne erhebliche Veränderungen der Beratungsunterlage möglich sind. Geeignete Maßnahmen in diesem Sinne können etwa die Löschung bzw. Schwärzung personenbezogener Daten sein. Ob solche Maßnahmen einen erheblichen Aufwand oder erhebliche Veränderungen darstellen und deshalb von einer Veröffentlichung abgesehen werden kann, ist von der Gemeinde im jeweiligen Einzelfall festzustellen. Auch ist dies eine rein kommunalrechtliche Fragestellung, mit der sich meine Dienststelle nicht näher befassen kann.

Für Gemeinden ist bedeutsam, zu erkennen, wann eine Offenbarung (Übermittlung) personenbezogener Daten aus datenschutzrechtli-

cher Sicht im Sinne von § 41b Absatz 2 Satz 2 GemO unbefugt ist. Unbefugt ist eine Offenbarung, wenn sie das Verbot mit Erlaubnisvorbehalt nicht hinreichend beachtet. Wie bereits ausgeführt stellt § 41b Absatz 2 Satz 1 GemO keine Befugnis zur Übermittlung von Beratungsunterlagen mit personenbezogenen Daten an die Internetöffentlichkeit dar. Andere Rechtsvorschriften, auf die eine Gemeinde eine Internetveröffentlichung von Beratungsunterlagen mit personenbezogenen Daten ohne Einwilligung der jeweils Betroffenen stützen könnte, sind nicht ersichtlich. So ist z.B. in § 34 Absatz 1 Satz 1 GemO zwar geregelt, dass der Bürgermeister den Gemeinderat mit angemessener Frist einberuft und diesem rechtzeitig vor dem Sitzungstag die Verhandlungsgegenstände mitteilt und dabei die für die Verhandlung erforderlichen Unterlagen beifügt, soweit dem nicht das öffentliche Wohl oder berechtigte Interessen Einzelner entgegenstehen. Erforderlich in diesem Sinne sind alle Unterlagen, die für eine hinreichende Vorbereitung der Mitglieder des Gemeinderates auf die Sitzung, die Bildung einer vorläufigen Meinung und zur Besprechung in den Fraktionen benötigt werden. Die entsprechenden Unterlagen können Informationen enthalten, die nicht für die Öffentlichkeit bestimmt sind. Dies schließt personenbezogene Daten und Betriebs- und Geschäftsgeheimnisse ein. Bedeutsam ist, dass § 34 Absatz 1 Satz 1 GemO nicht die Übermittlung von Beratungsunterlagen mit personenbezogenen Daten an die Saal- oder Internetöffentlichkeit erlaubt.

Gemeinden haben, soweit sie Beratungsunterlagen mit personenbezogenen Daten ohne Einwilligung der Betroffenen verwenden, diese vor Einstellung in das Internet zu anonymisieren. Es sei denn, sie können die Internetveröffentlichung auf eine Rechtsvorschrift stützen, die ihr diese Form der Datenverarbeitung ausdrücklich erlaubt.

Auslage von Beratungsunterlagen mit personenbezogenen Daten für Zuhörer

Auf den Punkt gebracht, gilt entsprechendes für die Auslage von Beratungsunterlagen mit personenbezogenen Daten im Sitzungsraum:

Dass Beratungsunterlagen für Zuhörer bei öffentlichen Gremiensitzungen auszulegen sind, ist in § 41 Absatz 3 Satz 1 GemO geregelt. Nach Satz 2 gilt § 41 Absatz 2 Sätze 2 und 3 GemO entsprechend. Das bedeutet, auch bei der Auslage von Beratungsunterlagen im Sitzungssaal ist durch geeignete Maßnahmen sicherzustellen, dass keine personenbezogenen Daten unbefugt offenbart werden. Der Gesetzesbegründung zu § 41b Absatz 3 GemO kann u.a. entnommen werden, dass eine Auslage von Beratungsunterlagen bei öffentliche Sitzungen nicht erfolgen muss, wenn diese wegen dem Schutz personenbezogener Daten nicht ohne erheblichen Aufwand oder erhebliche Veränderung der Sitzungsunterlagen erfolgen kann. Andere Rechtsvorschriften, die es einer Gemeinde erlauben würden, personenbezogenen Daten an die Saalöffentlichkeit durch Auslage von Beratungsunterlagen im Sitzungsraum ohne Einwilligung der jeweils Betroffenen zu veröffentlichen, sind auch hier nicht ersichtlich.

Veröffentlichung von Beschlüssen des Gemeinderats mit personenbezogenen Daten

Nach § 41b Absatz 5 GemO sind die in öffentlicher Sitzung des Gemeinderats oder des Ausschusses gefassten oder bekannt gegebenen Beschlüsse im Wortlaut oder in Form eines zusammenfassenden Berichts innerhalb einer Woche nach der Sitzung auf der Internetseite der Gemeinde zu veröffentlichen. Soweit ein Beschluss personenbezogene Daten umfasst, bedarf es dafür mindestens eines tragenden Sachgrunds. Dies vor dem Hintergrund, dass sich eine Gemeinde stets zu fragen hat, ob eine vorgesehene Verarbeitung personenbezogener Daten im strengen datenschutzrechtlichen Sinne zur gemeindlichen Aufgabenerfüllung wirklich erforderlich ist, oder ob die entsprechende Aufgabe nicht mit einem milderen Mittel erfüllt werden kann, das weniger oder gar nicht in das Grundrecht auf informationelle Selbstbestimmung der insoweit Betroffenen eingreift. Die aus Sicht des Datenschutzes wichtigen Prinzipien der Datenvermeidung und Datensparsamkeit stehen in unmittelbarem Zusammenhang mit diesem strengen Erforderlichkeitsbegriff. Ggf. müsste eine Gemeinde für jedes einzelne personenbezogene Datum nachweisen können, warum es zu ihrer Aufgabenerfüllung erforderlich ist, einen Personenbezug herzustellen und eine reine Sachverhaltsdarstellung (ohne Personenbezug) nicht ausreicht.

Gemeinden haben – unter Anwendung eines restriktiven Prüfungsmaßstabs – zu prüfen, ob es für ihre Aufgabenerfüllung wirklich erforderlich ist, dass Gremienbeschlüsse oder zusam-

menfassende Berichte mit personenbezogenen Daten im Internet veröffentlich werden. Nach meiner Kenntnis von der kommunalen Praxis dürfte dies in der überwiegenden Mehrzahl der Fälle nicht erforderlich sein. Unter der Prämisse, dass es mindestens einen tragenden Sachgrund für die Herstellung eines Personenbezugs gibt, dürfen entsprechende Gremienbeschlüsse mit personenbezogenen Daten nach Maßgabe von § 41 b Absatz 5 GemO veröffentlicht werden.

Veröffentlichung von Niederschriften über den wesentlichen Inhalt von Gemeinderatssitzungen

Im Zusammenhang mit Internetveröffentlichungen von Gremienbeschlüssen nach § 41b Absatz 5 GemO wird von kommunaler Seite immer wieder die (Internet-)Veröffentlichung von Niederschriften über den wesentlichen Inhalt von Gemeinderatssitzungen thematisiert. Dabei ist zu beachten, dass Beschlüsse des Gemeinderats i.S.v. § 41b Absatz 5 GemO von Niederschriften über den wesentlichen Inhalt der Verhandlungen des Gemeinderats nach § 38 Absatz 1 Satz 1 GemO zu unterscheiden sind. Nach § 38 Absatz 2 Satz 4 GemO ist Einwohnern die Einsichtnahme in Niederschriften über öffentliche Sitzungen gestattet. Eine (Internet-)Veröffentlichung von Niederschriften mit personenbezogenen Daten ist von dieser Regelung hingegen nicht umfasst.

Eine Publikation mit personenbezogenen Daten greift in verschiedener Hinsicht weitaus intensiver in das Recht des Betroffenen auf informationelle Selbstbestimmung ein als z.B. die Einsichtnahme von Einwohnern in Niederschriften über öffentliche Sitzungen. Dies gilt insbesondere für Internetveröffentlichungen. Während das Einsichtsrecht von Einwohnern in Niederschriften – im Einklang mit dem örtlichen Aufgaben- und Wirkungskreis der Gemeinden – regelmäßig nur einen vergleichsweise kleinen Adressatenkreis erreicht, wendet sich eine Internetveröffentlichung von Niederschriften potenziell an einen weltweiten Adressatenkreis, dessen Belange in seiner überwältigenden Mehrheit von dem jeweiligen Beratungsgegenstand in keiner Weise berührt ist. Überdies eröffnet das Internet vielfältige Verknüpfungs- und Auswertungsmöglichkeiten, die besondere Gefahren für die schutzwürdigen Interessen der Betroffenen mit sich bringen können. Deshalb ist für eine Internetveröffentlichung personenbezogener Daten eine normenklare Rechtsvorschrift erforderlich, die diese Form der Datenverarbeitung ausdrücklich erlaubt.

Einzelne Gemeinden möchten Niederschriften über Gemeinderatssitzungen als Bürgerservice und im Sinne einer besseren Transparenz des gemeindlichen Handelns zumindest mit den aus ihrer Sicht wesentlichen Äußerungen von Gemeinderatsmitgliedern im Amtsblatt und/oder im Internet veröffentlichen. Diese Beweggründe kann ich durchaus nachvollziehen. Teilweise wird ein entsprechender Wunsch auch von Mitgliedern des Gemeinderats selbst an die Gemeinden herangetragen. In diesem Zusammenhang ist jedoch zu beachten, dass auch bei Mitgliedern des Gemeinderats das Grundrecht auf informationelle Selbstbestimmung und somit das Verbot mit Erlaubnisvorbehalt beachtlich ist. Als Übermittlungsbefugnis kommt nach meiner Rechtsauffassung hier weder § 38 GemO noch eine andere Rechtsvorschrift in Betracht. Jedoch halte ich es für zulässig, wenn eine Gemeinde vor einer Veröffentlichung von Niederschriften, die personenbeziehbare Wortbeiträge von Mitgliedern des Gemeinderats enthalten, wirksame Einwilligungen der jeweils Betroffenen einholt. Dabei kann meines Erachtens eine Einwilligung für die Dauer der jeweiligen Amtszeit eingeholt werden, soweit seitens der Gemeinde auf den Einwilligungszeitraum explizit hingewiesen wird. Zu beachten ist dabei, dass entsprechende Einwilligungen stets widerruflich sind. Grundsätzlich empfehle ich, Einwilligungserklärungen schriftlich einzuholen und zu Dokumentationszwecken zu den Akten zu nehmen.

Auf der Grundlage von wirksamen Einwilligungen der jeweils betroffenen Mitglieder des Gemeinderats dürfen Niederschriften mit personenbeziehbaren Wortbeiträgen veröffentlicht werden.

Empfehlung zur Veröffentlichung von Sitzungsunterlagen, Beschlüssen und Niederschriften

Grundsätzlich empfehle ich Gemeinden, nach Möglichkeit schon in den für die Gemeinderatsmitglieder bestimmten Sitzungsunterlagen, in zu fertigenden Niederschriften über wesentliche Inhalte von Gemeinderatssitzungen sowie bei Gremienbeschlüssen jeden Personenbezug zu vermeiden, soweit dies möglich und mit der gemeindlichen Aufgabenerfüllung zu vereinbaren ist. Diese besonders datenschutzgerechte Vorgehensweise hat u.a. den Vorteil, dass ent-

sprechende Unterlagen ohne Personenbezug im Sitzungsraum für die Saalöffentlichkeit bereitgehalten und ggf. auch einer Niederschrift über eine öffentliche Sitzung als Anlage beigefügt sowie im Internet veröffentlicht werden können.

Datenschutzrechtliche Vorschriften sind nur beachtlich, wenn auch Daten von natürlichen Personen verarbeitet werden. Ein Verzicht auf die Verarbeitung von personenbezogenen Daten kann die Verfahrensökonomie fördern.

6.3 Sog. Jedermann-Einwendungen bei der Öffentlichkeitsbeteiligung im Rahmen der Bauleitplanung

Öffentliche Stellen, wie Gemeinden dürfen einen Personenbezug nur herstellen, wenn dies nach dem strengen datenschutzrechtlichen Erforderlichkeitsbegriff zur Aufgabenerfüllung erforderlich ist.

Immer wieder erreichen meine Dienststelle Beschwerden von Betroffenen, die bei der Bauleitplanung im Rahmen der Öffentlichkeitsbeteiligung nach § 3 des Baugesetzbuches gegenüber einer Gemeinde eine Stellungnahme mit Anregungen, Einwendungen und Bedenken abgegeben haben und bei denen eine Gemeinde in der Folge bei der Ermittlung und Gewichtung der für das Plangebiet erheblichen öffentlichen und privaten Belange in öffentlicher Gemeinderatssitzung einen Personenbezug hergestellt hat. Auch kam es vor, dass bei der Ergebnismitteilung Übersichten mit personenbezogenen Daten der Betroffenen an andere Personen, die gleichfalls eine Stellungnahme abgegeben hatten, übermittelt wurden. Zudem wurden teilweise solche Übersichten mit personenbezogenen Daten in den gemeindlichen Internetauftritt eingestellt.

Im Rahmen der Bauleitplanung hat eine Gemeinde nach Ermittlung und Gewichtung der für das Plangebiet erheblichen öffentlichen und privaten Belange diese gegeneinander und untereinander abzuwägen (sog. Abwägungsgebot). Zur Arbeitserleichterung erstellen viele Gemeinden Übersichten mit Namen und Adressen derjenigen, die im Rahmen der Öffentlichkeitsbeteiligung Stellungnahmen abgegeben haben, dem wesentlichen Inhalt der Stellungnahmen sowie dem jeweiligen Abwägungsergebnis (sog. Abwägungstabellen).

Für die Abwägung der öffentlichen und privaten Belange im Plangebiet ist der Gemeinderat zuständig. Soweit im Rahmen der Beratung und Beschlussfassung des Gemeinderats eine personenbezogene Zuordnung der vorgebrachten Stellungnahmen erforderlich ist, sind die entsprechenden Daten von der Gemeindeverwaltung an den Gemeinderat zu dessen Aufgabenerfüllung weiterzugeben. Beurteilungsmaßstab dabei ist, ob ein Personenbezug erforderlich ist, um den Gemeinderat in die Lage zu versetzen, sich eingehend mit den eingegangenen Stellungnahmen auseinanderzusetzen.

Wenn Stellungnahmen abgegeben werden, bei denen keine relevante Betroffenheit in eigenen Belangen gegeben ist, kann es sich um sog. Jedermann-Einwendungen handeln. Im Falle einer Jedermann-Einwendung kommt es gerade nicht auf die Person, die eine Stellungnahme abgegeben hat, und ihre persönliche Betroffenheit an. Ob eine relevante individuelle Betroffenheit einer Person vorliegt, die für eine sachgerechte Abwägung öffentlicher und privater Belange des Gemeinderats bedeutsam ist (und bei der es sich insoweit um keine sog. Jedermann-Einwendung handelt), kann nur im jeweiligen Einzelfall festgestellt werden.

Eingegangene Stellungnahmen nach § 3 BauGB sind gemäß § 35 Absatz 1 der Gemeindeordnung zwar grundsätzlich in öffentlicher Sitzung zu behandeln. Die Betroffenen müssen es zur Gewährleistung einer Verfahrenstransparenz auch grundsätzlich hinnehmen, dass ihre Stellungnahmen in öffentlicher Gemeinderatssitzung behandelt und zur Feststellung ihrer individuellen Betroffenheit ggf. auch Name und Anschrift genannt werden. Dies jedoch nur, soweit die Feststellung der individuellen Betroffenheit und eine damit verbundene Verarbeitung ihrer personenbezogenen Daten im Rahmen einer öffentlichen Gemeinderatssitzung auch zur gemeindlichen Aufgabenerfüllung erforderlich ist. Für eine entsprechende Erforderlichkeit muss mindestens ein tragender Sachgrund vorliegen. Wenn nicht, sind die entsprechenden Stellungnahmen in anonymisierter Form zu behandeln. Zudem ist zu beachten, dass, soweit die Herstellung eines Personenbezugs erforderlich ist, berechtigte Interessen Einzelner möglicherweise eine Behandlung in nichtöffentlicher Sitzung nach sich ziehen können.

Nach § 3 Absatz 2 Satz 4 BauGB sind die im Rahmen der (förmlichen) Beteiligung der Öffentlichkeit fristgemäß abgegebenen Stellungnahmen zu prüfen. Das Ergebnis der Prüfung ist denjenigen mitzuteilen, die die Stellungnahme abgegeben haben. Zweck dieser Regelung ist, dass die Gemeinde darüber informiert, ob und mit welchem Ergebnis sich der Gemeinderat mit der eigenen Stellungnahme auseinandergesetzt hat. Die Übermittlung einer Übersicht mit personenbezogenen Daten (wie etwa Namen und Adresse aller Personen, die eine Stellungnahme eingereicht haben) an Dritte ist hingegen von dieser Vorschrift nicht umfasst. Bei der Feststellung, wer Dritter in diesem Zusammenhang ist, ist auf die einzelne Stellungnahme (und nicht auf eine Übersicht in ihrer Gesamtheit) abzustellen. Jedoch kommt es immer wieder vor, dass Gemeinden personenbezogenen Daten rechtswidrig übermitteln, indem sie Übersichten mit personenbezogenen Daten allen Betroffenen zur Verfügung stellen, die eine Stellungnahme abgegeben haben und/oder diese Übersichten gar in den gemeindlichen Internetauftritt einstellen.

Um datenschutzrechtlichen Belangen hinreichend Rechnung zu tragen, können nach § 3 BauGB eingegangene Stellungnahmen unter Verwendung von nicht personenbeziehbaren Kennziffern (wie etwa fortlaufenden Nummern) in einer Übersicht (wie einer sog. Abwägungstabelle) aufbereitet werden. Dem Gemeinderat kann – soweit erforderlich – zusätzlich eine Zuordnungsliste zur Verfügung gestellt werden, in der die Kennziffern jeweils namentlich (ggf. mit Adressdaten) zugeordnet sind. Übersichten ohne personenbezogene Daten können aus Sicht des Datenschutzes auch anderen Verfahrensbeteiligten zur Verfügung gestellt, im Sitzungssaal für die sog. Saalöffentlichkeit ausgelegt oder im Internet veröffentlicht werden.

6.4 Das widerspenstige Landratsamt

Davon, dass auch innerhalb einer Organisationseinheit nicht jeder alles wissen darf, sondern dass datenschutzrechtliche Grundsätze, insbesondere der Grundsatz der Erforderlichkeit, auch behördenintern gelten und zu beachten sind, musste ich ein Landratsamt mühsam überzeugen. Worum ging es?

Anlässlich einer vom Landratsamt durchgeführten tierschutzrechtlichen Kontrolle wurde auch festgestellt, dass das Anwesen der Petentin problematische hygienische Verhältnisse aufwies. Kurzerhand informierte man hierüber sowie über die durchgeführte und eine geplante Tierschutzkontrolle den Ortsvorsteher des Stadtbezirks der Stadt, in der die Petentin ansässig war. Die Petentin sah sich dadurch in ihrem Datenschutzrecht verletzt und wandte sich an meine Dienststelle.

Das hierzu befragte Landratsamt argumentierte zunächst damit, dass der Ortsvorsteher ein für die Gefahrenabwehr zuständiges Organ der Stadt und die Mitteilung an ihn über die hygienischen Verhältnisse der Petentin deshalb zulässig gewesen sei. Trotz meines daraufhin erfolgten Hinweises, dass diese Rechtsauffassung unrichtig sei, weil selbst nach Auskunft durch die Stadt der Ortsvorsteher hier keinerlei ortspolizeilichen Befugnisse besitze (was übrigens die hierzu informatorisch befragte Kommunalaufsichtsbehörde ausdrücklich bestätigte), beharrte das Landratsamt auf seiner Meinung. Die unzulässige Datenübermittlung beanstandete ich dann mit folgender Begründung:

Die Information des Ortsvorstehers durch das Landratsamt über die persönlichen Verhältnisse der Petentin hätte einer Rechtsgrundlage bedurft. Als solche war hier § 16 Absatz 1 des Landesdatenschutzgesetzes (LDSG) in Betracht zu ziehen. Danach dürfen innerhalb des öffentlichen Bereichs personenbezogene Daten u.a. übermittelt werden, wenn dies zur Erfüllung der Aufgaben der Stelle, an die die Daten übermittelt werden, erforderlich ist (§ 16 Absatz 1 Nummer 1 2. Alternative LDSG) und zusätzlich eine der (weiteren) Voraussetzungen des § 15 Absatz 1 bis 4 LDSG vorliegt (§ 16 Absatz 1 Nummer 2 LDSG).

Die vom Landratsamt vertretene Auffassung, der Ortsvorsteher sei hier mit Aufgaben der Ortspolizeibehörde betraut gewesen, war unzutreffend.

Ortspolizeibehörde ist nach § 62 Absatz 4 Satz 1 des Polizeigesetzes (PolG) die Gemeinde. Die der Gemeinde hiernach übertragenen Aufgaben sind Pflichtaufgaben nach Weisung (§ 62 Absatz 4 Satz 2, § 65 PolG), die gemäß § 44 Absatz 3 Satz 1 1. Halbsatz der Gemeindeordnung (GemO) grundsätzlich vom Bürgermeister in eigener Zuständigkeit erledigt werden. Nach § 53 Absatz 1 Satz 1 GemO kann zwar der Bürgermeister Gemeindebedienstete auf bestimmten Aufgabengebieten mit seiner Ver-

tretung beauftragen. Eine solche Beauftragung des Ortsvorstehers des Stadtbezirks … war im konkreten Fall aber nicht erfolgt. Auch ansonsten erfolgte keine Übertragung im Einzelfall. Dies wurde durch die Stadt … ausdrücklich schriftlich bestätigt. Ebenso wenig begründen die §§ 71 und 72 GemO eine entsprechende (gesetzliche) Zuständigkeit des Ortsvorstehers. Denn die Vertretung des Bürgermeisters bei der Leitung der öffentlichen Verwaltung schließt nicht die Aufgaben nach § 44 Absatz 3 Satz 1 GemO ein. Insoweit stellt(e) Nummer 6 der (außer Kraft getretenen) VwV GemO zu § 68 fest: „Der Bürgermeister kann jedoch den Ortsvorsteher als Beamten der Gemeinde nach § 53 Abs. 1 Satz 1 mit seiner Vertretung auf bestimmten Aufgabengebieten oder in einzelnen Angelegenheiten seines Zuständigkeitsbereichs nach § 44 Abs. 2 und 3 [Anm.: § 44 Absatz 3 GemO betrifft Weisungsaufgaben, zu denen die Aufgaben der Ortspolizeibehörde gehören] beauftragen …".

Wenn eine öffentliche Stelle personenbezogene Daten auf der Grundlage des § 16 Absatz 1 LDSG übermittelt, trägt sie die Verantwortung für die Zulässigkeit der Übermittlung.[1] Sie muss insbesondere prüfen, ob die Stelle, an welche die Daten übermittelt werden sollen, sachlich zuständig ist und ob die Daten für deren Aufgabenerfüllung erforderlich sind. Sie muss im Rahmen ihrer Möglichkeiten also sicherstellen, dass die Daten nicht „in falsche Hände" gelangen. Wenn etwa klar ist, dass ein bestimmtes Amt einer Gemeinde sachlich für ein Aufgabengebiet zuständig ist, hat sich die übermittelnde Stelle unmittelbar dorthin zu wenden und darf die Daten nicht sehenden Auges an ein nicht zuständiges Amt weitergeben. Zwar wird nicht grundsätzlich zu verlangen sein, dass die innerbehördlichen Aufgabenzuweisungen bis ins Detail zu prüfen sind.[2] Ist es jedoch – wie im gegebenen Fall – aufgrund einer klaren gesetzlichen Aufgabenzuweisung offensichtlich, wer behördenintern für die Sachbearbeitung zuständig ist, handelt derjenige unverantwortlich, wer personenbezogene Daten gezielt an eine andere als die zuständige Stelle übermittelt. Dass der Ortsvorsteher hier nicht als Ortspolizeibehörde zuständig war, ergab sich meines Erachtens eindeutig aus den einschlägigen Bestimmungen des Polizeigesetzes in Verbindung mit der Gemeindeordnung. Weder die Hauptsatzung der Stadt … noch die Vereinbarung über die Eingliederung der Gemeinde … in die Stadt … legten etwas anderes nahe. Der Ortsvorsteher selbst hatte eine solche Zuständigkeit bisher auch noch nicht für sich in Anspruch genommen. Und aus dem Schriftwechsel mit meiner Dienststelle war dem Landratsamt bekannt, dass die Stadt … ausdrücklich bestätigt hatte, dass der örtlichen Verwaltung in … für Aufgaben der Ortspolizeibehörde nicht zuständig war. Vor diesem Hintergrund war es für mich nicht nachvollziehbar, dass das Landratsamt an seiner rechtsirrigen Auffassung festhielt und weiterhin unbeirrt von einer Zuständigkeit des Ortsvorstehers ausging.

Insbesondere dieses Verhalten verlieh dem Verstoß gegen das Datenschutzrecht hier besonders Gewicht. Denn es stand zu befürchten, dass das Landratsamt in vergleichbaren Fällen auch künftig personenbezogene Daten an Stellen übermitteln werde, an die mangels Zuständigkeit nicht übermittelt werden darf. Dies führte unter Abwägung aller Gesichtspunkte dazu, hier eine Beanstandung auszusprechen. Letztlich wurde zugesichert, dass man meine Rechtsauffassung künftig beachten werde.

1 Roggenkamp in: Plath (Hrsg.), BDSG/DS-GVO, 2. Aufl. 2016, § 15 Rn 11
2 Dammann in: Simitis (Hrsg.), BDSG, 8. Auflage 2014, § 14 Rn. 11

7. Gesundheit und Soziales

7.1 NAKO-Gesundheitsstudie

Die NAKO Gesundheitsstudie (NAKO) ist eine Langzeit-Bevölkerungsstudie, die zum Ziel hat, den Ursachen für die Entstehung von Volkskrankheiten, wie z.B. Krebs, Demenz, Diabetes, Infektionskrankheiten und Herzinfarkt auf den Grund zu gehen. Die Studie wird vom Verein Nationale Kohorte e.V. durchgeführt, dessen Mitglieder Institutionen deutscher Forschungseinrichtungen sind, die zur Helmholtz-Gemeinschaft, den Universitäten bzw. der Leibniz-Gemeinschaft sowie der Ressortforschung von Bund und Ländern gehören. Bundesweit werden 200.000 Männer und Frauen im Alter von 20 bis 69 Jahren in 18 regionalen Studienzentren, darunter die Studienzentren Mannheim und Freiburg, medizinisch untersucht und nach Lebensgewohnheiten (z.B. körperliche Aktivität, Rauchen, Ernährung, Beruf) befragt. Im Rahmen regelmäßig stattfindender Nachbeobachtungen und Folgeuntersuchungen werden weitere Daten zu Lebensgewohnheiten und Krankheiten erhoben. Angesichts der Sensibilität und Menge der Daten, die während eines Zeitraumes von mindestens 20 bis 30 Jahren verarbeitet, genutzt und langfristig gespeichert werden, bedarf die Studie einer kontinuierlichen datenschutzrechtlichen Begleitung. Wir haben im Berichtszeitraum das Studienzentrum Mannheim besucht und kontrolliert, ob die datenschutzrechtlichen Vorgaben beachtet werden.

Das Studienzentrum Mannheim wird vom Deutschen Krebsforschungszentrum in Kooperation mit der Universität Heidelberg betrieben. Es führt die Datenverarbeitung im Auftrag der Nationalen Kohorte e.V. durch.

Das Studienzentrum rekrutiert und untersucht insgesamt 10.000 Teilnehmer aus der Region Mannheim. Im Rahmen einer zufälligen Stichprobenziehung meldet das Einwohnermeldeamt Mannheim potenzielle Teilnehmer an das Studienzentrum. Das Studienzentrum schreibt die aus den Zufallsstichproben gezogenen Personen an und lädt sie zur Teilnahme an der Studie ein. Das im Zeitpunkt unseres Besuches verwendete Einladungsschreiben wies zwar auf die Freiwilligkeit der Teilnahme hin, dieser Hinweis wurde jedoch weder näher ausgeführt noch optisch hervorgehoben, sodass er angesichts der Fülle an Informationen, die das Schreiben enthielt, leicht übersehen oder überlesen werden konnte. Das Studienzentrum hat erfreulicherweise das Einladungsschreiben angepasst und hebt nunmehr den Hinweis optisch durch Fettschrift hervor.

Besteht Interesse an einer Teilnahme, vereinbart das Studienzentrum einen Untersuchungstermin. Zu Beginn dieses Untersuchungstermins erfolgt eine detaillierte Information über die Gesundheitsstudie, insbesondere über die Erteilung der erforderlichen Einwilligung, die Voraussetzung für eine Studienteilnahme ist. Der Teilnehmer kann sich dabei entscheiden, ob er in alle in der umfangreichen Einwilligungserklärung vorgesehenen Schritte einwilligt, und in welche nicht (z.B. Teilnahme nur an bestimmten Untersuchungen, Anforderungen von Gesundheitsdaten bei Ärzten und Krankenhäusern).

Möchte die angeschriebene Person an der Studie nicht teilnehmen, führt das Studienzentrum eine sog. Non-Responder-Befragung durch, um die Gründe für die Nichtteilnahme zu erfahren. Diese Daten werden ebenfalls in der Studiendatenbank gespeichert, obwohl der Nichtteilnehmer gerade nicht in die Studienteilnahme (und damit in eine Datenspeicherung) eingewilligt hat. Er wird dabei nicht nur nach den Gründen für seine Nichtteilnahme – der eigentliche Anlass der Befragung – gefragt. Die Mehrzahl der Fragen bezieht sich vielmehr auf den gesundheitlichen Zustand, Krankheiten, Familienstand und Schulbildung, also Informationen, deren Erforderlichkeit nicht ohne weiteres auf der Hand liegt. Das Studienzentrum hat insoweit dargelegt, dass es nicht nur darum gehe festzustellen, aus welchen Gründen eine Person an der Studie nicht teilnehmen möchte. Wichtig sei auch die Untersuchung der Merkmale, die Personen innehaben, die an der Studie nicht teilnehmen, sowie der Auswirkung der Non-Response, um ggf. Verzerrungen begegnen und die Repräsentativität der Studie gewährleisten zu können. Da das Datenschutzkonzept der NAKO dazu keine genaueren Aussagen enthält, muss sich die NAKO e.V. mit dieser Problematik erneut befassen. Für den Fall, dass die angeschriebene Person durch ihr Verhalten deutlich zum Ausdruck gebracht hat, dass sie nicht nur eine Teilnahme an der Studie ablehnt, sondern deswegen auch nicht mehr angesprochen werden möchte, hat das Studienzentrum Mannheim zugesagt, künftig keine Non-Responder Fragebögen mehr zu verschicken.

Das Studienzentrum Mannheim bietet (neben den Studienzentren Augsburg, Berlin, Essen und Neubrandenburg) 6.000 Studienteilnehmern die Möglichkeit an einer MRT-Ganzkörperuntersuchung teilzunehmen. Die MRT-Teilnehmer werden als Zufallsstichprobe aus den Studienteilnehmern des Studienzentrums Mannheim sowie den benachbarten Studienzentren Freiburg und Saarbrücken ausgewählt, die an diesen Zentren bereits das Untersuchungsprogramm absolviert haben. Zu Beginn der MRT-Untersuchung werden die Teilnehmer über diese Zusatzuntersuchung aufgeklärt. Liegen keine Ausschlusskriterien vor, sodass der Teilnehmer an der Untersuchung teilnehmen kann, erteilt dieser ggf. seine Einwilligung.

Das Studienzentrum erhebt die Daten der Teilnehmer personenbezogen. Sie werden pseudonymisiert in einer einheitlichen IT-Infrastruktur in gespiegelten zentralen Studiendatenbanken langfristig an den Standorten Greifswald (Universitätsmedizin Greifswald) und Heidelberg (Deutsches Krebsforschungszentrum) gespeichert. Der Schlüssel zur Identifizierung der Personen liegt bei der unabhängigen Treuhandstelle der Universitätsmedizin Greifswald. Im Zeitpunkt unseres Kontrollbesuches hat das Studienzentrum allerdings Daten gespeichert, die für die Erledigung eigener Aufgaben nicht mehr benötigt wurden. Grund dafür war, dass Teile der zentralen IT-Infrastruktur noch nicht voll funktionsfähig waren. Um Datenverluste zu vermeiden mussten daher Daten im Studienzentrum zwischengespeichert (z.B. Daten in medizinischen Geräten, EKG) bzw. Papierunterlagen (Einwilligungserklärungen) vorübergehend aufbewahrt werden. Die Kontrolle vor Ort ergab, dass die Papierunterlagen sicher aufbewahrt wurden und nur wenige Personen bei Bedarf auf die temporär gespeicherten Daten zugreifen konnten.

Die Nationale Kohorte e.V. hat außerdem festgelegt, dass die Erfassung von Sekundär- und Registerdaten u.a. durch das Deutsche Krebsforschungszentrum Heidelberg erfolgt. Studiendaten zu Forschungszwecken werden durch die Transferstelle an den Standorten Heidelberg (Nationale Kohorte e.V., Deutsches Krebsforschungszentrum) und Greifswald (Universitätsmedizin Greifswald) für die wissenschaftliche Nutzung zur Verfügung gestellt.

Im Ergebnis konnte festgestellt werden, dass das Studienzentrum Mannheim verantwortungsvoll mit den personenbezogenen Daten der Teilnehmer der Studie umgeht und sehr darum bemüht ist, den Anforderungen des Datenschutzes gerecht zu werden. Ich werde die NAKO weiterhin datenschutzrechtlich begleiten und bei den beteiligten baden-württembergischen Einrichtungen auf ein datenschutzgerechtes Vorgehen hinwirken.

7.2 Einschaltung eines Abrechnungszentrums durch eine Ergotherapiepraxis bei gesetzlich krankenversicherten Patienten

Die Beschwerde eines Patienten gab erneut Anlass, uns mit datenschutzrechtlichen Aspekten der Tätigkeit von Verrechnungsstellen bzw. Abrechnungszentren im Gesundheitsbereich zu befassen. In unserem 31. Tätigkeitsbericht für die Jahre 2012 und 2013 hatten wir uns unter Nummer 7.9 zu „Verrechnungsstellen und Forderungen für ärztliche Privatpatienten-Leistungen" geäußert. Diesmal ging es um den Datenschutz gesetzlich krankenversicherter Patienten.

Ein solcher hatte sich bei uns u.a. darüber beschwert, dass eine in Baden-Württemberg ansässige Abrechnungsfirma personenbezogene Daten über ihn, darunter auch sensible Diagnosedaten, ohne seine Einwilligung von seinem Ergotherapeuten erhalten habe und speichere. Da dieser Ergotherapeut in einem anderen Bundesland praktiziert und somit nicht unserer Datenschutzaufsicht untersteht, hat sich unsere Prüfung auf die unserer Aufsicht unterstehende Abrechnungsfirma beschränkt. Aus dem Vorbringen des Patienten und einer von uns eingeholten Stellungnahme dieser Firma ergab sich für uns u.a. folgender Sachverhalt:

Die Abrechnungsfirma hat vom Ergotherapeuten bestimmte Daten, darunter auch Diagnosedaten, zum Zweck der Abrechnung erhalten und beim Patienten eine von diesem zu leistende gesetzliche Zuzahlung für eine vom Ergotherapeuten erbrachte Heilbehandlung angefordert. Der Ergotherapeut hatte es versäumt, die von ihm beauftragte Abrechnungsfirma darüber zu informieren, dass der Patient diese Zuzahlung bereits in bar in der Praxis geleistet hatte. Nachdem die Abrechnungsfirma dieses Umstands gewahr wurde, hat sie die Rechnung storniert. Erst durch diese irrtümliche Anforderung der Zuzahlung hat der Patient erfahren, dass sein Ergotherapeut mit der Abrechnungsfirma zusammenarbeitet und personenbezo-

gene Daten über ihn an diese weitergegeben hat. Der Patient gelangte zu der Einschätzung, dass die Abrechnungsfirma im unrechtmäßigen Besitz seiner Daten sei. Er forderte die Firma auf, den gesamten Datensatz über seine Person sofort und vollständig zu löschen. Darauf hat die Firma dem Patienten u.a. mitgeteilt, sie habe dessen Daten gelöscht, sofern sie nicht aufgrund gesetzlicher Verpflichtungen zur weiteren Speicherung verpflichtet ist, und die danach verbleibenden Daten gesperrt, sodass die Einsicht in die übermittelte Rechnung und die darin enthaltenen Informationen nur sehr wenigen Mitarbeitern mit besonderen Zugriffsrechten möglich sei. Der Patient akzeptierte eine solchermaßen fortdauernde Speicherung seiner personenbezogenen Daten durch die Firma nicht und bekräftigte seine Forderung nach unverzüglicher Löschung.

Auch wenn demnach der Auslöser des Falles, die Anforderung der Zuzahlung, rasch als Versehen, das die Abrechnungsfirma nicht zu vertreten hat, erkannt und aufgrund der Stornierung als erledigt betrachtet werden konnte, erforderten die unterschiedlichen Auffassungen des Patienten einerseits und der Abrechnungsfirma andererseits eine vertiefte datenschutzrechtliche Prüfung. Dabei ging es insbesondere auch darum,

- auf welcher Rechtsgrundlage die Abrechnungsfirma mit den personenbezogenen Daten des Patienten, einschließlich Diagnosedaten, umgehen darf und
- ob diese Rechtsgrundlage gegebenenfalls auch eine vom Patienten zu leistende gesetzliche Zuzahlung einschließt

.

Zur Klärung dieser Fragen waren insbesondere die einschlägigen Vorschriften des Fünften Buchs des Sozialgesetzbuchs – Gesetzliche Krankenversicherung – (SGB V) heranzuziehen. Im Einzelnen:

Die Leistungen, die der Ergotherapeut dem Patienten erbracht hat, fallen unter den Begriff der Heilmittel im Sinne des § 32 SGB V i.V.m. § 124 Absatz 1 SGB V. Hinsichtlich der Abrechnung des Ergotherapeuten sind somit insbesondere die Vorschriften des § 302 SGB V zu beachten. Nach § 302 Absatz 1 Satz 1 Halbsatz 1 SGB V sind u.a. die Leistungserbringer im Bereich der Heilmittel „verpflichtet, den Krankenkassen im Wege elektronischer Datenübertragung oder maschinell verwertbar auf Datenträgern die von ihnen erbrachten Leistungen nach Art, Menge und Preis zu bezeichnen und den Tag der Leistungserbringung sowie die Arztnummer des verordnenden Arztes, die Verordnung des Arztes mit der Diagnose und den erforderlichen Angaben über den Befund und die Angaben nach § 291 Abs. 2 Nr. 1 bis 10 anzugeben" (bei den Angaben nach § 291 Absatz 2 Nr. 1 bis 10 SGB V handelt es sich um die Bezeichnung der ausstellenden Krankenkasse, einschließlich eines Kennzeichens für die Kassenärztliche Vereinigung, in deren Bezirk der Versicherte seinen Wohnsitz hat, den Familiennamen und Vornamen des Versicherten, dessen Geburtsdatum, Geschlecht, Anschrift, Krankenversichertennummer und Zuzahlungsstatus, den Versichertenstatus, für die Personengruppen nach § 264 Absatz 2 SGB V den Status der auftragsweisen Betreuung, den Tag des Beginns des Versicherungsschutzes und bei befristeter Gültigkeit der elektronischen Gesundheitskarte das Datum des Fristablaufs). Damit ist klar: Aufgrund dieser ausdrücklichen bundesgesetzlichen Regelung sind u.a. Ergotherapeuten verpflichtet, nicht nur berechtigt, zum Zweck der Abrechnung auch die „erforderlichen Angaben über den Befund", also Diagnosedaten, an Krankenkassen herauszugeben. Es ist für uns ohne weiteres nachvollziehbar, wenn Menschen, die auf größtmöglichen Datenschutz bedacht sind, dieser, nach unserer Einschätzung vom Bundesgesetzgeber wirksam angeordneten, Herausgabe von sensiblen Diagnosedaten kritisch gegenüberstehen. Entsprechendes gilt für die Regelung des § 302 Absatz 2 Satz 2 SGB V: Danach können u.a. Ergotherapeuten „zur Erfüllung ihrer Verpflichtungen Rechenzentren in Anspruch nehmen". Nach § 302 Absatz 2 Satz 3 SGB V dürfen die Rechenzentren „die Daten für im Sozialgesetzbuch bestimmte Zwecke und nur in einer auf diese Zwecke ausgerichteten Weise verarbeiten und nutzen, soweit sie dazu von einer berechtigten Stelle beauftragt worden sind; anonymisierte Daten dürfen auch für andere Zwecke verarbeitet und genutzt werden". Demnach ist es kraft ausdrücklicher bundesgesetzlicher Erlaubnis legal, wenn Ergotherapeuten zum Zweck der Abrechnung auch die „erforderlichen Angaben über den Befund" i.S.d. § 302 Absatz 1 Satz 1 Halbsatz 1 SGB V auf der Grundlage des § 302 Absatz 2 Satz 2 SGB V an Rechenzentren herausgeben und Rechenzentren solche Daten nach Maßgabe des § 302 Absatz 2 Satz 3 SGB V verarbeiten und nutzen. Im hier bearbeiteten Fall stand außer Zweifel, dass es sich bei der Abrechnungsfirma um ein Rechenzentrum i.S.d. § 302 Ab-

satz 2 Satz 2 und 3 SGB V handelt. Somit ist es aus datenschutzrechtlicher Sicht nicht zu kritisieren, wenn die Abrechnungsfirma personenbezogene Daten des Patienten, die unter die in § 302 Absatz 1 SGB V genannten Datenarten fallen, zum Zweck der Abrechnung gespeichert und genutzt hat.

Die Frage, ob dies auch hinsichtlich der vom Patienten zu leistenden gesetzlichen Zuzahlung gilt, erforderte ein noch tieferes Eintauchen in die Regelungen über die gesetzliche Krankenversicherung. Gesetzlich Krankenversicherte müssen für die Inanspruchnahme von Heilmitteln nach § 32 Absatz 2 Satz 1 SGB V i.V.m. § 61 Satz 3 SGB V Zuzahlungen leisten. Die gesetzliche Krankenversicherung ist allerdings zunächst von der Pflicht befreit, solche Zuzahlungen selbst einzuziehen. Der Bundesgesetzgeber hat mit § 43c Absatz 1 Satz 1 SGB V die Leistungserbringer verpflichtet, „Zahlungen, die Versicherte zu entrichten haben, einzuziehen und mit ihrem Vergütungsanspruch gegenüber der Krankenkasse zu verrechnen". § 43c Absatz 1 Satz 1 SGB V statuiert demnach hinsichtlich der Zuzahlungen eine weitere Rechtspflicht von Ergotherapeuten und anderen Leistungserbringern. Auch diese Rechtspflicht gehört zu den Verpflichtungen, hinsichtlich derer, wie oben dargestellt, u.a. Ergotherapeuten nach § 302 Absatz 2 Satz 2 SGB V Rechenzentren in Anspruch nehmen können. Diese Rechtsauffassung beruht u.a. auf dem Umstand, dass die zuletzt genannte Vorschrift keine bestimmten Verpflichtungen ausdrücklich nennt und somit keine derartigen Einschränkungen enthält. Wenn der Bundesgesetzgeber solche Einschränkungen gewollt hätte, beispielsweise auf die Verpflichtungen nach § 302 Absatz 1 SGB V und somit unter Ausschluss der Verpflichtungen nach § 43c Absatz 1 Satz 1 SGB V, hätte er dies normenklar zum Ausdruck bringen können, wie er dies hinsichtlich der Abrechnung der Apotheken und weiterer Stellen in § 300 Absatz 2 Satz 1 SGB V getan hat: „Die Apotheken und weitere Anbieter von Leistungen nach § 31 können zur Erfüllung ihrer Verpflichtungen nach Absatz 1 Rechenzentren in Anspruch nehmen."

Erst dann, wenn der Versicherte trotz einer gesonderten schriftlichen Aufforderung durch den Leistungserbringer nicht zahlt, hat nach § 43c Absatz 1 Satz 2 SGB V die Krankenkasse die Zahlung einzuziehen. In diesem Zusammenhang ist anzumerken, dass dies zwar im hier dargestellten Fall der Abrechnung für eine Heilmittelversorgung gilt, nicht aber mit Blick auf Hilfsmittel, wie beispielsweise Brillen, Hörgeräte, Rollstühle und Prothesen. Nach dem für Hilfsmittel geltenden § 33 Absatz 8 Satz 2 Halbsatz 2 SGB V findet § 43c Absatz 1 Satz 2 SGB V keine Anwendung.

Diese detaillierten Vorschriften über die gesetzliche Krankenversicherung machen beispielhaft deutlich, wie wichtig es generell ist, auch bei der datenschutzrechtlichen Prüfung mit der gebotenen Sorgfalt vorzugehen, die jeweils anzuwendenden Normen zu identifizieren und auch unter Beachtung knapper Halbsätze vollständig zu erfassen.

7.3 Arztpraxen im Internet

Online-Service? Aber sicher!

Viele Arztpraxen sind im Internet präsent, sei es mit einer eigenen Homepage oder in einem Verzeichnis. Diese Präsenz dient immer öfter nicht nur als reine Informationsquelle für die Patienten, sondern auch als Kommunikationsportal.

So stehen für die Patienten der Arztpraxis beispielsweise als sog. Online-Service neben dem altbekannten Kontaktformular inzwischen auch die Terminvereinbarung sowie die Bestellung von Überweisungen und Rezepten via Internet zur Verfügung.

Es liegt auf der Hand, dass dabei auch der Datenschutz eine wichtige Rolle spielt. Wenn z.B. ein Patient auf der entsprechend gestalteten Internetseite seiner Arztpraxis zur Terminvereinbarung neben seinem Namen, seinen Kontaktdaten und seinem Wunschtermin auch seine Beschwerden in einem Freitextfeld schildert, muss u.a. sichergestellt sein, dass seine sensiblen Gesundheitsdaten auf dem elektronischen Kommunikationsweg gegen unbefugte Kenntnisnahme gesichert sind. Entsprechendes gilt für eventuelle elektronische Antworten der Praxis. Der Arzt, welcher der ärztlichen Schweigepflicht (etwa nach § 9 der Berufsordnung der Landesärztekammer Baden-Württemberg) unterliegt, muss, ebenso wie z.B. bei persönlichen Terminvereinbarungen am Empfangsschalter seiner Praxis oder am Telefon, auch in der „Online-Welt" darauf achten, keine ihm in seiner Eigenschaft als Arzt anvertrauten oder bekannt gewordenen Informationen (zu den derart geschützten Informationen ge-

hört auch, dass jemand den Arzt überhaupt konsultiert hat und zum Kreis seiner Patienten gehört) unbefugt zu offenbaren. Der Arzt muss dazu, sei es bei der eigenen Gestaltung seines Internetangebots, sei es bei der Auswahl eines kommerziell angebotenen fertigen Softwareprodukts, insbesondere die wirksame Verschlüsselung der Kommunikation gewährleisten.

Leider mussten wir insofern immer wieder Mängel feststellen. Etwa derart, dass nur unverschlüsselte Verbindungen via HTTP-Protokoll angeboten werden und somit bereits die Eingabe der Daten im Klartext mitgelesen werden könnte. Oder dass die via SSL/TLS-Verschlüsselung eingegebenen Daten anschließend als unverschlüsselte E-Mail versandt werden. Wenn ein Arzt trotz fehlender Verschlüsselung eine solche elektronische Kommunikation anbietet, muss er die potenziellen Nutzer darauf hinweisen und als Alternative sichere Kommunikationswege (Besuch in der Praxis, Telefon, Fax) anbieten.

Die Forderung nach wirksamer Verschlüsselung beim Betrieb solcher elektronischer Informations- und Kommunikationsdienste ergibt sich vorrangig aus dem Telemediengesetz (TMG). Nach § 13 Absatz 7 Satz 1 TMG gilt:

Diensteanbieter haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass
1. kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und
2. diese
a) gegen Verletzungen des Schutzes personenbezogener Daten und
b) gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind,
gesichert sind.

Eine solche Maßnahme ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens (vgl. § 13 Absatz 7 Satz 3 TMG). Dabei ist der jeweilige Stand der Technik zu berücksichtigen (vgl. § 13 Absatz 7 Satz 2 TMG). Ein vorsätzlicher oder fahrlässiger Verstoß eines Arztes gegen seine Pflichten nach § 13 Absatz 7 Satz 1 Nummer 1 oder Nummer 2 Buchstabe a TMG ist nach § 16 Absatz 2 Nummer 3 TMG ordnungswidrig und kann gemäß § 16 Absatz 3 TMG mit einer Geldbuße bis zu 50.000 Euro geahndet werden.

Dabei ist allerdings zu berücksichtigen: Die Vorschriften im Abschnitt 4 des Telemediengesetzes (§§ 11 bis 15a) dienen dem Datenschutz des Nutzers solcher Dienste, hier also dem Schutz der Patienten, die mit ihrem Arzt elektronisch kommunizieren. Es ist aber nicht ausgeschlossen, dass auch die personenbezogenen Daten anderer Menschen (etwa von Familienangehörigen, Pflegern oder Betreuern des Patienten oder von Apothekern und anderen Ärzten) Gegenstand einer solchen elektronischen Kommunikation zwischen einem Patienten und einem Arzt sind. Die datenschutzrechtlichen Vorschriften, die hinsichtlich dieser anderen Betroffenen zu beachten sind, ergeben sich nicht aus dem Telemediengesetz, sondern insbesondere aus dem Bundesdatenschutzgesetz (BDSG).

Nach § 13 Absatz 1 Satz 1 TMG hat ein Arzt als Diensteanbieter den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie ggf. die Verarbeitung seiner Daten außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums in allgemein verständlicher Form zu unterrichten. Der Inhalt der Unterrichtung muss gemäß § 13 Absatz 1 Satz 3 TMG für den Nutzer jederzeit abrufbar sein. Hierfür ist auf jeder (Unter-) Seite eines Webangebotes ein gesonderter Hyperlink erforderlich, der direkt auf die Datenschutzerklärung führt und auch als solcher bezeichnet ist. „Rechtliche Hinweise" etwa wäre hierbei zu ungenau. Ein eigener Hyperlink ist auch nach § 4a Absatz 1 Satz 3 BDSG, wonach die Einwilligung besonders hervorzuheben ist, sollte sie zusammen mit anderen Erklärungen schriftlich erteilt werden, zu fordern.

Im Rahmen der Unterrichtung müssen die Nutzer auch über die etwaige Einbindung von Dienstleistern informiert werden. Dies ist immer dort der Fall, wo der Webserver nicht selbst durch die und in der Arztpraxis betrieben wird, sondern auf sog. Hosting-Provider zurückgegriffen wird. Im Kern geht es darum, die Nutzer darüber zu informieren, dass ihre personenbezogenen Daten ggf. anderen Stellen als dem Anbieter der Homepage zur Kenntnis gelangen. Von besonderer Bedeutung ist dies dann, wenn Serviceleistungen wie Terminbuchung oder Rezeptbestellung angeboten werden. Aber auch bei der Erfassung und Aus-

wertung der Zugriffe auf die Homepage bzw. dem Einsatz entsprechender Softwarelösungen wie „Google Analytics" oder „Piwik" bestehen Informationspflichten.

Aufgrund der Breite und Komplexität des Themas halte ich es für sinnvoll, wenn hier auch die Verbände ihre Mitglieder entsprechend sensibilisieren, damit zukünftig sowohl Patienten als auch Praxen auf der sicheren Seite sind.

7.4 Messenger bei Ärzten und Pflegekräften

Im Gesundheits- und Sozialwesen sehen sich Einrichtungen vermehrt mit Anfragen von Mitarbeitern konfrontiert, eigene Endgeräte (PC, Notebook, Smartphone, Mobiltelefon) auch im dienstlichen Umfeld nutzen zu können.

Insbesondere Messenger mit der Möglichkeit der Bildübermittlung wecken bei Mobiltelefonen mit Kamerafunktion und Pauschaltarif (Flatrate) große Begehrlichkeiten, sich durch deren Verwendung den Arbeitsalltag zu erleichtern (z.B. bei der Wunddokumentation).
Die Nutzung privater Endgeräte der Mitarbeiter birgt jedoch erhebliche rechtliche und sicherheitstechnische Problemstellungen. So muss insbesondere mit Blick auf die ärztliche Schweigepflicht gewährleistet sein, dass keine unautorisierten Zugriffe auf das Gerät bzw. die gespeicherten Daten erfolgen können.
Messaging bedarf bei Gesundheitsdaten als besondere Arten personenbezogener Daten mit einem hohen Schutzbedarf entsprechender technisch-organisatorischer Maßnahmen (z.B. eine durchgängige Ende-zu-Ende-Verschlüsselung). Der Einsatz von Messenger-Diensten sollte nur nach kritischer Prüfung des Funktionsumfangs (Privacy by Design) sowie der datenschutzkonformen Voreinstellung (Privacy by Default) im Vorfeld eines produktiven Einsatzes innerhalb einer Einrichtung erfolgen. Ebenso sind der Zweck und die Notwendigkeit selbstkritisch zu hinterfragen.
Problematisch sind insbesondere nachstehende Aspekte:

- Serverstandorte des Dienstleisters befinden sich außerhalb der Europäischen Union
- oder des Europäischen Wirtschaftsraumes
- unzureichende, nicht durchgängige Verschlüsselung
- Hochladen des Adressbuchs an den Diensteanbieter
- Abfrage von Statusinformationen der Nutzer
- Speicherung und Verwendung der (Protokoll)-Daten
- Datenübermittlung an Dritte

Die dienstliche Nutzung von WhatsApp ist somit in der derzeitigen Ausgestaltung des Dienstes aus datenschutzrechtlicher Sicht als unzulässig anzusehen:

Aus der Sicht des Datenschutzes handelt es sich bei einer dienstlichen Nutzung von WhatsApp um eine Datenverarbeitung im Auftrag gemäß § 11 des Bundesdatenschutzgesetzes, bei der der Auftraggeber die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung des Dienstleisters trägt. Sofern die Serverstandorte von WhatsApp sich außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraumes befinden, handelt es sich um eine Übermittlung personenbezogener Daten in ein sog. Drittland. Die Übermittlung personenbezogener Daten in ein Drittland wie die USA ist aus meiner Sicht auch durch den neuen EU-Privacy-Shield nicht befriedigend gelöst. Eine Einwilligung aller betroffenen Personen in die Datenübermittlung wird in der Regel nicht vorliegen.

Ungeachtet dessen sollte die verantwortliche Stelle vorab prüfen, ob eine Nutzung privater Endgeräte und Messenger-Dienste möglicherweise bestehenden, einrichtungsinternen Richtlinien oder Dienstvereinbarungen widerspricht. Viele Träger von Einrichtungen haben vorgegeben, dass dienstliche Tätigkeiten ausschließlich mittels firmeneigener Geräte erledigt werden dürfen. Eine private Nutzung dienstlicher IT-Kommunikation ist häufig generell verboten, ebenso die betriebliche Nutzung mitarbeitereigener Geräte.

Sofern derzeit keine entsprechenden internen Regelungen existieren, sollte die verantwortliche Stelle klar und unmissverständlich festlegen, ob und gegebenenfalls welche privaten Endgeräte der Mitarbeiter einschließlich Messenger-Diensten zu welchem Zweck und unter welchen Voraussetzungen genutzt werden dürfen.

7.5 Datenschutz in Pflegeeinrichtungen

Ein Anlass dafür, uns nach einiger Zeit wieder verstärkt mit dem Datenschutz in Pflege-

einrichtungen zu befassen, war der Umstand, dass dort vermehrt sog. Biographiegespräche mit den Heimbewohnern geführt werden, oftmals unter Verwendung von als Biographiebogen bezeichneten Vordrucken. Diese Vordrucke enthalten u.a. höchst sensible Fragen, etwa nach allgemeinen „Angaben zur Religion (z.B. Glaubensrichtung, Glaubensintensität, Wunsch nach seelsorgerischer Betreuung etc.)" und mit Blick auf besondere „Wünsche für das Lebensende (z.B. Besuch der Sitzwache, Krankensalbung, seelsorgerische Betreuung etc.)". Einen unmittelbaren Eindruck dazu sowie zu einer Vielzahl weiterer datenschutzrechtlich bedeutsamer Umstände haben wir uns durch einen Informations-, Beratungs- und Kontrollbesuch in einem Pflegeheim verschafft.

Es zeigte sich, dass das Pflegeheim, das, zusammen mit weiteren derartigen Heimen, von einer Kommune im Eigenbetrieb geführt wird, in Sachen Datenschutz relativ gut aufgestellt ist. Außer einem beim Eigenbetrieb selbst angesiedelten Datenschutzfachmann kümmern sich auch der behördliche Datenschutzbeauftragte der Kommune und seine Mitarbeiter um die Gewährleistung des erforderlichen Datenschutzes. Somit war es keine Überraschung, dass unsere Kontrolle keine gravierenden Probleme erkennen ließ. Die Bewohnerakten, die in der Regel auch höchst sensible Angaben über die Gesundheit der Bewohner enthalten, waren, soweit wir erkennen konnten, durch Aufbewahrung in einem nur für autorisiertes Personal zugänglichen verschlossenen Dienstzimmer gegen unbefugte Kenntnisnahme gesichert. Dort, wo aufgrund der besonderen räumlichen Situation in diesem Heim durch eine Glasscheibe vom Speisesaal aus Einblick in das Dienstzimmer und dort eventuell auf einem Tisch liegende Unterlagen möglich war, war bereits für einen gewissen Sichtschutz gesorgt, dessen Verbesserung uns sogleich im Rahmen unseres Besuchs zugesagt wurde.

Im Verlauf unseres Rundgangs durch das Heim fanden wir Aktenordner mit mehrere Jahre alten Anfragen nach einem Heimplatz, die nicht zum Abschluss eines Heimvertrags und zur Aufnahme in das Heim geführt hatten. Da auch das Heim davon ausging, dass diese Unterlagen zur Erledigung seiner Aufgaben nicht mehr gebraucht werden, wurden noch am Tag der Begehung die veralteten Datensammlungen entsorgt. Wir haben dies zum Anlass genommen, auf die Notwendigkeit eines durchdachten und leicht handhabbaren Systems hinzuweisen, mit dessen Hilfe alle Dokumente mit personenbezogenen Daten unter Berücksichtigung der fachlichen Notwendigkeiten sowie normativer Aufbewahrungsfristen eingeordnet, für die gebotene Zeit verwahrt und bald danach unter Umständen entsorgt werden. Durch ein solches System kann unnötiger Aufwand vermieden werden, der dadurch entsteht, dass unsystematisch und zufallsabhängig immer wieder einzelne Dokumente oder Akten in die Hand genommen und hinsichtlich der Aufbewahrungsfrist geprüft werden. Zudem kann vermieden werden, dass nicht mehr benötigte Papiere knappen und teuren Raum in Anspruch nehmen, der anderweitig und sinnvoll genutzt werden könnte.

Bei der eingehenden Prüfung und Erörterung der vom Heim verwendeten Vordrucke hat sich gezeigt, dass einige der in diesen Vordrucken vorgesehenen Informationen gar nicht erhoben werden müssen, etwa auch deshalb, weil man über die entsprechenden personenbezogenen Daten bereits verfügt, teilweise nach Erhebung mit einem anderen Vordruck. Uns wurde zugesagt, dass aufgrund unserer Beratung die Vordrucke unter Berücksichtigung der Gebote der Datensparsamkeit und der Datenvermeidung vom Heim nochmals sorgfältig und detailliert durchgesehen und „entschlackt" werden. Die Heimleitung hat uns inzwischen mitgeteilt, man habe dort die entscheidende Erkenntnis gezogen, dass im Sinne der Datensparsamkeit vieles nicht gesammelt werden muss, weshalb man nun Sorge dafür trage, dass nur die Daten erhoben werden, welche zur Erfüllung der dortigen Aufgaben notwendig sind.

Zu dem vom Heim verwendeten „Biographiebogen" wurde uns u.a. erklärt, dass man im Pflegewesen, wohl aus pflegefachlichen und -wissenschaftlichen Gründen, von solchen Vordrucken und Gesprächen in gewissem Umfang wieder abrücke. Demnach könnten sich das Thema selbst und auch dessen datenschutzrechtliche Bewertung möglicherweise von selbst erledigen. Solange dies nicht geschehen ist, sollten beim Einsatz dieser Instrumente auch datenschutzrechtliche Aspekte berücksichtigt werden. Ein Vordruck mit der Bezeichnung „Biographiebogen" und der einleitenden Aussage „Mithilfe der erhobenen Biographie können somit Ressourcen besser erkannt und Pflegeprobleme im Kontext der Lebensgeschichte besser erklärt werden." erweckt den Anschein, dass es dabei ausschließlich oder überwiegend um Informationen über die Biographie bzw. die

Lebensgeschichte von Heimbewohnern geht. Ein erster Blick auf den von uns geprüften Vordruck zeigte, dass dies nicht der Fall ist. Neben Fragen zu Eltern und Geschwistern, Familienstand, Kindern und Enkeln, Lebensphasen (untergliedert nach Kindheit und Jugend, Erwachsenenalter und Rentenalter) finden sich darin Fragen zu „Gewohnheiten/Vorlieben", etwa mit Blick auf „Lieblingsessen/Lieblingsgetränke", „Unverträglichkeiten oder Abneigungen gegen Speisen bzw. Getränke", „Essgewohnheiten", „Vorlieben und Gewohnheiten im Bereich der Körperpflege" und „Kleidung", sowie zu „Interessen/Fähigkeiten", z.B. mit Blick auf „Hobbies und Interessen", besondere „Kenntnisse/Fähigkeiten" und, wie oben bereits zitiert, auf allgemeine „Angaben zur Religion" und besondere „Wünsche für das Lebensende". Bei vielen Angaben geht es somit, jedenfalls nicht primär, um die Lebensgeschichte im eigentlichen Sinne. Es geht vielmehr um aktuelle Umstände und Befindlichkeiten, die für die Pflege und Versorgung der Heimbewohner eine bedeutende Rolle spielen und vielfach in deren Lebensgeschichte wurzeln und dadurch erklärbar sein können. Wir haben empfohlen, die Dokumente und Praxis des Heims so zu überarbeiten, dass die Dinge, die man auf freiwilliger Basis über die Heimbewohner in Erfahrung bringen möchte, im Rahmen des üblichen Wortsinns klar bezeichnet sind: Wo es tatsächlich um Biographie im Sinne von Lebensgeschichte bzw. Lebenslauf geht, können diese Begriffe beibehalten werden. Wo es (auch) um etwas anderes geht, sollte man dies unmissverständlich zum Ausdruck bringen. Unsere Erörterung mit dem Heimbetreiber förderte einen weiteren Änderungsbedarf zutage. Seitens des Heims wurde uns erklärt, dass man sich dort, genau überlegt, gar nicht unbedingt dafür interessiere, welcher Religion und Glaubensrichtung ein Heimbewohner mit welcher Intensität anhängt. Letztlich gehe es dem Heim nur darum, die sich aus Religion, Glaubensrichtung und Glaubensintensität unter Umständen ergebenden konkreten Auswirkungen auf Pflege und Versorgung des Heimbewohners zu erkennen. Wo es solche Auswirkungen nicht gebe oder geben könne und somit kein entsprechendes Erfordernis bestehe, wolle sich das Heim konsequenterweise gar nicht mit derart persönlichen und sensiblen Aspekten befassen. Uns wurde zugesagt, den Vordruck auch insofern zu überarbeiten. Zudem wurde uns versichert, dass dieser Vordruck nicht schematisch, sondern stets unter Berücksichtigung des jeweiligen Heimbewohners, seiner Persönlichkeit, seiner erkennbaren Bedürfnisse und der konkreten Situation angewandt werde.

Das von uns besuchte Heim nutzt, so wie andere vergleichbare Einrichtungen, moderne Funktechnologie, um zu verhindern, dass demenzkranke und dadurch in ihrer Orientierungsfähigkeit eingeschränkte Heimbewohner, die sich nicht mehr sicher allein außerhalb der Einrichtung bewegen können, diese verlassen und sich möglicherweise selbst in Gefahr bringen. Dieser „Weglaufschutz" funktioniert so: Betroffene Heimbewohner tragen ein Armband, in dem ein Funkchip, auch RFID (Radio Frequency Identification)-Tag genannt, untergebracht ist. Dieser Chip dient als Meldetransponder, dessen Signale von einer vom Heimpersonal betreuten Leseeinheit aufgefangen werden. Hier ist positiv anzumerken, dass die Einrichtung keine personalisierte Meldung verwendet. Das System ist so konfiguriert, dass das Pflegepersonal lediglich über eine neutrale Meldung ohne ID- oder Namensnennung erfährt, dass sich ein Bewohner im Eingangsbereich aufhält, und dann nachsehen kann, ob dieser ggf. desorientiert ist und die Einrichtung verlässt. Angesichts der Möglichkeiten, die heutige Systeme bieten (individuelle Sperrung von Türen und Aufzügen, Laufrichtungserkennung, Ortung, Erstellen von Bewegungsmustern usw.), ist dies eine erfreulich datensparsame Verwendung, da hier lediglich eine allgemeine Aufmerksamkeitsmeldung an das Personal erfolgt.

Beim Einsatz von RFID-Technik sind Pflegeeinrichtungen als verantwortliche Stellen generell aufgefordert, die Betroffenen bzw. deren sorgeberechtigte Angehörige oder Betreuer umfassend über Einsatz, Verwendungszweck und Inhalt von RFID-Chips zu informieren, RFID-Daten nur so lange zu speichern, wie es zur Erreichung des Zwecks erforderlich ist, die Vertraulichkeit der gespeicherten und der übertragenen Daten durch wirksame Authentisierung der beteiligten Geräte und durch Verschlüsselung sicherzustellen sowie ein Privacy Impact Assessment (PIA) zur Datenschutzfolgenabschätzung bei RFID-Anwendungen zu erstellen. Die Technische Richtlinie RFID des BSI (BSI TR-03126) sowie unsere Hinweise unter https://www.baden-wuerttemberg.datenschutz.de/datenschutzgerechte-nutzung-der-rfid-technik/ werden hier als Orientierungshilfe empfohlen.

Aufgrund der Vielzahl der unserer Datenschutzaufsicht unterstehenden baden-württember-

gischen Pflegeeinrichtungen ist es uns aus Kapazitätsgründen nicht möglich, auch nur einen nennenswerten Teil derselben individuell zu betreuen, etwa durch einzelne Beratungsgespräche und -besuche. Daher haben wir versucht, über einen Dachverband, der eine Vielzahl solcher Einrichtungen und Träger zu seinen Mitgliedern zählt, unsere „Streubreite" zu erhöhen. Dieser Dachverband, mit dem unsere Dienststelle auch in anderen Angelegenheiten traditionell konstruktiv zusammenarbeitet, hat uns mit vielen wertvollen Informationen unterstützt und uns im Rahmen einer Fachtagung des Verbands ein Forum gegeben, eine Vielzahl von Tagungsteilnehmern aus verschiedensten Einrichtungen und Organisationen direkt anzusprechen. Nachdem gerade auch im Pflegebereich dem Thema Datenschutz eine immer größere Bedeutung zukommt, beabsichtigen wir, insbesondere auf der Grundlage der hier eingegangenen Rückmeldungen aus der Praxis des Pflegewesens und unter Berücksichtigung der ab dem 25. Mai 2018 geltenden Vorschriften der Datenschutz-Grundverordnung der EU, einen bei Bedarf anzupassenden und fortzuschreibenden Katalog häufig gestellter Fragen („FAQs") mit den jeweiligen Antworten herausgeben.

7.6 Kontroll- und Beratungsbesuch bei einer Betriebskrankenkasse

Im Berichtszeitraum war das sog. Krankengeldfallmanagement erneut Anlass für einen Kontroll- und Beratungsbesuch meiner Dienststelle bei einer gesetzlichen Krankenkasse. Beim Krankengeldfallmanagement kam es in der Vergangenheit vor, dass einige Krankenversicherungen unzulässig detaillierte Gesundheitsdaten von Versicherten erhoben, die längere Zeit arbeitsunfähig waren oder bereits Krankengeld erhielten. Die gesetzliche Aufgabentrennung zwischen dem Medizinischen Dienst der Krankenversicherung (MDK) und den gesetzlichen Krankenversicherungen wurde dabei zu Lasten der Persönlichkeitsrechte von Versicherten häufig ignoriert. Welche datenschutzrechtlichen Probleme bei einem Krankengeldfallmanagement entstehen können und welche gesetzlichen Grenzen es zu beachten gilt, haben wir in unserem 32. Tätigkeitsbericht 2014/2015 (LT-Drucksache 15/7990, S. 120 f.) dargestellt.

Mit dem GKV-Versorgungsstärkungsgesetz wurde nunmehr mit § 44 Absatz 4 des Fünften Buches des Sozialgesetzbuches (SGB V) für Versicherte eine individuelle Beratung und Hilfestellung der Krankenkassen zur Überwindung langandauernder Arbeitsunfähigkeit eingeführt. Die Krankenkassen haben damit die Pflicht, Versicherte, die über einen längeren Zeitraum arbeitsunfähig sind, zielgerichtet und angemessen zu unterstützen und ihnen zu helfen, Krankheiten und Arbeitsunfähigkeit zu überwinden.

Den praktischen Umgang mit diesem gesetzlichen Anspruch haben wir bei einer vergleichsweise kleinen Betriebskrankenkasse in Baden-Württemberg geprüft. Ergebnis der Prüfung war, dass bei der Betriebskrankenkasse im Zusammenhang mit dem sog. Krankengeldfallmanagement keine datenschutzrechtlichen Probleme auftraten. Die Krankenkasse leistete auf Anfrage der Versicherten individuelle Beratung und Hilfestellung zur Wiederherstellung der Arbeitsfähigkeit, ohne dass dabei unzulässig personenbezogene Daten erhoben oder übermittelt wurden. Zur Erfüllung des Anspruchs aus § 44 Absatz 4 SGB V verlangte die Versicherung allerdings pauschal eine datenschutzrechtliche Einwilligungserklärung von ihren arbeitsunfähigen Versicherten. Aus Gründen der Datensparsamkeit und Datenvermeidung haben wir der Krankenkasse empfohlen, die Betroffenen in einem ersten Schritt über die Möglichkeiten einer individuellen Beratung und Hilfestellung zu informieren und erst nach einer positiven Rückmeldung des Versicherten im konkreten Einzelfall eine entsprechende Einwilligungserklärung nach § 44 Absatz 4 Satz 2 SGB V zur Datenerhebung und -verarbeitung einzuholen.

Bei der Begehung der Räumlichkeiten mussten wir feststellen, dass diese z.T. mit Videokameras überwacht wurden. Besonders auffallend waren hierbei zwei Dome-Kameras, die in den Beratungsräumen der Krankenkasse installiert waren. Die Kameras übertrugen dauerhaft ein Live-Bild an einen Monitor hinter dem Empfangstresen. Auf Nachfrage wurde uns mitgeteilt, dass die Videoüberwachungsanlage zum Schutz vor Einbrüchen und Übergriffen auf Mitarbeiter installiert worden war. Konkrete Vorfälle konnten uns auf Nachfrage nicht benannt werden. Im Alarmfall sollten die Kameras eine Aufzeichnung der Bilder auslösen.
Mit dieser Begründung konnte der Einsatz der Kameras in den Beratungsräumen nicht gerechtfertigt werden. Denn die Bilder wurden anlassunabhängig in einer besonderen Be-

ratungssituation zwischen Versichertem und Krankenversicherung erfasst. Der Betroffene vertraut sich innerhalb eines räumlich geschützten Bereichs seiner Versicherung an, teilt ihr private Dinge mit, die seine höchstpersönliche, ggf. intime Lebens-, Gesundheits- und Krankheitsgeschichte betreffen und wird dabei in einer Situation gefilmt, in der er vielleicht auch äußerlich von einer Krankheit gezeichnet ist. Die Videoüberwachung erfasste damit über einen längeren Zeitraum sensible Gesundheitsdaten der Versicherten und damit auch Daten, die besonders schützenswert sind. Diesem Umstand hatte die Krankenkasse bei ihrer eigenen Bewertung nicht ausreichend Rechnung getragen.

Besonders schwer wog der Eingriff, weil er sich auf alle Versicherten bezog, die eine Beratung in den Räumen in Anspruch nahmen. Ein konkreter Anlass für die Überwachung oder eine Ausweichmöglichkeit für die Versicherten bestand nicht. Das ungleiche Verhältnis zwischen Krankenkasse und Versichertem, wonach der Versicherte sich in einem gewissen Abhängigkeitsverhältnis befindet, spielte bei der datenschutzrechtlichen Bewertung ebenso eine Rolle, wie die übrigen Sicherheitsvorkehrungen, die bereits in anderen Bereichen der Krankenkasse zum Schutz der Mitarbeiter eingerichtet worden waren. Die Räume waren beispielsweise nicht nur ausreichend vor unbefugtem Zutritt geschützt, auch stand den Beratern im Falle eines Notfalles ein Alarmknopf in jedem Beratungsraum zur Verfügung. Zudem hätten problematische Beratungen im Voraus festgestellt und zur Sicherheit mit mehreren Personen durchgeführt werden können. Letztlich konnte die Krankenkasse auch keine konkreten Vorfälle nennen, aus denen eine konkrete Gefährdung der Mitarbeiter hervorging.
Auch wenn der Schutz der eigenen Mitarbeiter ein durchaus nachvollziehbares Interesse eines Arbeitgebers ist, war die rein subjektive Annahme einer abstrakten Gefährdungslage in diesem Fall nicht ausreichend, um einen solchen intensiven Eingriff in die Rechte der Betroffenen zu rechtfertigen. Für die Versicherten hätte zumindest eine Ausweichmöglichkeit bestehen müssen. Obwohl die Bilder zunächst nicht aufgezeichnet worden waren, überwog in diesem Fall das schutzwürdige Interesse der Betroffenen. Bei einer persönlichen Beratung bei seiner Krankenkasse muss sich ein Versicherter daher nicht anlasslos und dauerhaft überwachen lassen.

7.7 Kontrollen bei Jobcentern

Im Berichtszeitraum waren meine Mitarbeiter wieder bei zwei Jobcentern vor Ort. Dadurch wurden nun alle Jobcenter, die meiner Zuständigkeit unterliegen, von meiner Dienststelle besucht.

Wie auch schon bei früheren Kontrollbesuchen standen u.a. die folgenden Themen im Raum:

- Die korrekte Belehrung bei der Anforderung von Kontoauszügen
- Diese war bereits Gegenstand des 31. Tätigkeitsberichts (Landtags-Drucksache 15/4600, S. 112). Danach ist nach der Rechtsprechung des Bundessozialgerichts ein Hinweis auf die Möglichkeiten der Schwärzung bei besonderen Arten personenbezogener Daten (dies sind z.B. Angaben über politische Meinungen, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugungen) auf der Ausgabenseite der Kontoauszüge erforderlich.
- Aufbewahrung von Personalausweiskopien
  Auch zu dieser Thematik wurde ebenfalls im 31. Tätigkeitsbericht (S. 111 f.) und im 32. Tätigkeitsbericht (Landtags-Drucksache 15/7990, S. 133) ausgeführt. Demzufolge dürfte regelmäßig ein Vermerk darüber genügen, dass sich der Antragsteller durch Personalausweis oder sonstige Ausweispapiere ausgewiesen hat. Ggf. kann außerdem vermerkt werden, dass die im Antrag angegebenen Angaben mit denen auf dem Personalausweis übereinstimmen.
- Formulare
  Teilweise fehlten auf Formularen Hinweise auf die Freiwilligkeit bei der Erhebung von E-Mail-Adresse und Telefonnummer (vergleiche hierzu auch die Ausführungen im 31. Tätigkeitsbericht, S. 112).

  Auf einem Formular wurde zur Feststellung eines Mehrbedarfs für kostenaufwändige Ernährung die Art der Erkrankung erhoben. Dies ist, da es sich um eine Angabe über die Gesundheit handelt, ein besonders sensibles Datum. Da für unterschiedliche Krankheiten Mehrbedarf in derselben Höhe gezahlt wird, sollten meiner Auffassung nach diese Krankheiten in Krankheitsgruppen zusammengefasst werden, um zu vermeiden, dass der Betroffene seine konkrete Krankheit dem Jobcenter offenbaren muss.

Festzustellen war, dass Know-how in Sachen Sozialdatenschutz vor Ort durchaus vorhanden ist, aber – zum Zeitpunkt des Kontrollbesuchs – noch nicht immer konsequent umgesetzt wurde.

7.8 Einwilligungserklärungen bei Sozialämtern

Zum 1. Januar 2016 ist das Zweite und zum 1. Januar 2017 das Dritte Pflegestärkungsgesetz in Kraft getreten. Die beiden Gesetze haben auch die Sozialämter vor große Herausforderungen gestellt. Nichtsdestotrotz dürfen bei der Umsetzung die datenschutzrechtlichen Regeln nicht außer Acht gelassen werden.

Zum 1. Januar 2016 ist das Zweite und zum 1. Januar 2017 das Dritte Pflegestärkungsgesetz in Kraft getreten. Ein Eckpfeiler der neuen Gesetze ist die Einführung eines neuen Pflegebedürftigkeitsbegriffs, der sich – den Ausführungen der Bundesministeriums für Gesundheit zufolge – stärker an den Bedürfnissen jedes einzelnen Menschen, an seiner individuellen Lebenssituation und an seinen individuellen Beeinträchtigungen und Fähigkeiten orientiert. Fünf Pflegegrade ersetzen seit dem 1. Januar 2017 die bisherigen drei Pflegestufen.

Die gesetzlichen Änderungen haben auch die Sozialämter vor große Herausforderungen gestellt. Sozialhilfe als sogenannte „Hilfe zur Pflege" können (bei Vorliegen weiterer Voraussetzungen) pflegebedürftige Personen beziehen, die keine (soziale oder private) Pflegeversicherung haben oder bei denen die Leistungen der Pflegeversicherung nicht ausreichend sind.

Meine Dienststelle hatte im Berichtszeitraum mit einem Sozialamt zu tun, das – um die Umsetzung der Pflegestärkungsgesetze, auch im Interesse der Betroffenen, zeitnah gewährleisten zu können – Einwilligungserklärungen erstellt und verwendet hat. In einer Erklärung sollte der Betroffene (bzw. dessen gesetzlicher Betreuer) einwilligen, dass „Daten" zwischen Sozialamt und Pflegekasse ausgetauscht werden. In einer weiteren Erklärung sollte der Betroffene einwilligen, dass „Daten" zwischen dem Sozialamt und dem Pflegestützpunkt des Kreises „hinsichtlich der Umsetzung der Pflegestärkungsgesetzes" ausgetauscht werden.
Die Einwilligungserklärungen standen mit geltendem Recht nicht in Einklang: Nach der für die Sozialhilfe geltenden Vorschrift für Einwilligungen, § 67b des Zehnten Buchs des Sozialgesetzbuchs, ist der Betroffene auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Ein entsprechender Hinweis fehlte. Des Weiteren ist Voraussetzung für eine wirksame Einwilligung, dass die Einwilligung für den konkreten Fall und in Kenntnis der Sachlage erteilt wird. Dies erfordert inhaltliche Bestimmtheit. Danach muss die Einwilligungserklärung u.a. die Daten hinreichend festlegen, auf die sich die Verarbeitung oder Nutzung bezieht. In der einen Einwilligungserklärung war nur allgemein vom Austausch von „Daten" die Rede. Dies war nicht ausreichend bestimmt. Auch die Einschränkung „hinsichtlich der Umsetzung des Pflegestärkungsgesetzes" in der zweiten Einwilligungserklärung dürfte diese noch nicht ausreichend bestimmt machen.

Das betroffene Sozialamt war einsichtig.

Die Anforderungen an eine Einwilligung im Bereich der Sozialhilfe sind in § 67b des Zehnten Buchs des Sozialgesetzbuchs geregelt. Außerdem muss eine Einwilligung inhaltlich hinreichend bestimmt sein.

7.9 Übermittlung von Sozialdaten unbegleiteter minderjähriger Ausländer durch Jugendämter

In Baden-Württemberg gab es zu Beginn des Jahres 2017 ungefähr 8000 unbegleitete minderjährige Ausländer, das heißt Kinder und Jugendliche unter 18 Jahren, die ohne Begleitung eines für sie verantwortlichen Erwachsenen einreisten oder ohne Begleitung zurückgelassen wurden. Besonders im Zuge des breiten Zustroms von Schutzsuchenden in den Jahren 2015 und 2016 wurden viele Minderjährige nicht oder nicht vollständig von den Ausländerbehörden erfasst.

Um sich einen möglichst lückenlosen Überblick über die Identität dieser Minderjährigen zu verschaffen, haben sich das Ministerium für Soziales und Integration Baden-Württemberg (Sozialministerium) und das Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg im Januar 2017 an die Leiter der Jugendämter in Baden-Württemberg gewandt mit der Bitte, binnen einer Woche Angaben über alle in ihrer Zuständigkeit befindlichen unbegleiteten minderjährigen Ausländer an das Landeskriminalamt Baden-Württemberg zu übermitteln. Benötigt würden Vor- und Famili-

enname, Geburtsdatum, Staatsangehörigkeit, Wohnanschrift und ein Hinweis, ob den Behörden ausländische Pass- oder Passersatzpapiere im Original vorgelegen haben oder vorliegen. Als Rechtsgrundlage für die Datenübermittlungen der Jugendämter wurde § 87 Absatz 1 des Aufenthaltsgesetzes in Verbindung mit § 86 Satz 1 des Aufenthaltsgesetzes genannt.
Das Schreiben löste Irritationen bei den Jugendämtern aus. Daraufhin haben die Ministerien noch ein zweites Schreiben versandt, in dem als (weitere) mögliche Rechtsgrundlage für eine Datenübermittlung noch § 68 Absatz 1 Satz 1 bzw. § 71 Absatz 2 Satz 1 Nr.1 des Zehnten Buchs des Sozialgesetzbuchs genannt wurde.

Bezüglich der Rolle des Landeskriminalamts bzw. der Polizei in dieser Angelegenheit verweise ich auf die Ausführungen unter 2.4.2 im vorliegenden Tätigkeitsbericht.

In Bezug auf die Datenübermittlungen durch die Jugendämter habe ich dem Sozialministerium mitgeteilt, dass, wenn es seinen nachgeordneten Bereich (noch dazu mit kurzer Fristsetzung) zu Datenübermittlungen „drängt", die richtige Rechtsgrundlage genannt werden sollte. Dies konnte vorliegend so nicht festgestellt werden: Gemäß § 67b Absatz 1 Satz 1 des Zehnten Buchs des Sozialgesetzbuchs – auf den für die Jugendämter § 61 Absatz 1 des Achten Buchs des Sozialgesetzbuchs verweist – ist die Verarbeitung von Sozialdaten (hierzu gehört nach § 67 Absatz 6 Satz 1 des Zehnten Buchs des Sozialgesetzbuchs auch das Übermitteln) nur zulässig, soweit eine Rechtsvorschrift im Sozialgesetzbuch dies erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Eine Rechtsvorschrift im Sozialgesetzbuch wurde in dem ersten Schreiben an die Jugendämter nicht genannt. Auch bezüglich der in dem zweiten Schreiben genannten Rechtsvorschriften bestanden Zweifel, dass diese Rechtsgrundlage für die Übermittlung aller Datenarten war.

Aufgrund des akuten Handlungsbedarfs, der dem unkontrollierten Zuzug von Flüchtenden geschuldet war, habe ich keinen Grund für eine förmliche Beanstandung gesehen. Allerdings erwarte ich für die Zukunft, dass in vergleichbaren Fällen von der Möglichkeit Gebrauch gemacht wird, im Vorfeld mit meiner Dienststelle die Rechtsgrundlage abzusprechen bzw. einen Hinweis an den nachgeordneten Bereich zu geben, dass sich dieser bei Zweifeln an meine Dienststelle wenden kann. Dies hat das Sozialministerium zugesagt.

8. Schule und Hochschulen

8.1 Schlüssel ist out – Transponder ist in! Elektronische Schließanlagen an Schulen und was sie alles könn(t)en

Musste eine Lehrkraft noch vor Jahren unzählige Schlüssel für Lehrerzimmer, Unterrichtsräume, Material- und Sammlungsräume usw. mit sich führen, reduziert sich dieser Aufwand durch den Einbau von auch in Schulen immer häufiger anzutreffenden elektronischen Schließanlagen auf lediglich einen „elektronischen Schlüssel" in Form eines RFID-Transponders oder einer Chipkarte.
In welchem Umfang dabei personenbezogene Daten von Lehrern und weiteren Personen wie beispielsweise vom Hausmeister oder der Schulsekretärin verarbeitet werden und welche Funktionalitäten solche elektronischen Schließsysteme bieten, hat sich im Rahmen eines Informations- und Kontrollbesuches an einem Gymnasium gezeigt.

Elektronische Schließanlagen sind praktisch, weshalb immer mehr Schulen die herkömmlichen Schließanlagen in Schulgebäuden austauschen. Während Lehrkräfte den „zentralen Schlüssel für alles" als eine Erleichterung der täglichen Arbeit wahrnehmen, entfällt für die Schule bzw. den Schulträger der gewohnte, vergleichsweise hohe zeitliche und finanzielle Aufwand für die Verwaltung und Vergabe von herkömmlichen Schlüsseln. Die erforderlichen Schließberechtigungen für alle relevanten Schulräume werden fortan passgenau auf den Unterrichtseinsatz der Lehrkraft zugeschnitten, indem die Schließberechtigungen mittels einer Software im sogenannten Schließplan hinterlegt und anschließend via Programmiergerät auf den RFID-Transponder der Lehrkraft übertragen werden.

Hauptgrund für die Installation eines elektronischen Schließsystems in Schulgebäuden ist das einfache Handling beim Verlust oder dem Diebstahl eines Schlüssels und die damit verbundene Kostenersparnis. Führte beispielsweise das Abhandenkommen eines Generalschlüssels oder gar des gesamten Schlüsselbundes bisher dazu, dass eine Vielzahl von Schließzylindern, womöglich sogar das gesamte Schließsystem der Schule, quasi über Nacht ausgetauscht und neue Schlüssel an die Lehrkräfte ausgegeben werden mussten, genügt es bei elektronischen Schließanlagen, den abhandengekommenen RFID-Transponder per Software im Schließplan zu sperren und die Information an die Schließzylinder weiterzugeben.

Wie sich im Falle der von mir kontrollierten Schule gezeigt hat, öffnen die elektronischen Schließzylinder – im Gegensatz zu ihrem mechanischen Pendant – nicht nur Türen, sondern speichern, je nach Konfiguration, bis zu 1000 Schließvorgänge auf den darin verbauten Speicherchips. Technisch möglich ist auch eine Speicherung fehlgeschlagener und auch „erfolgreicher" Schließvorgänge auf dem RFID-Transponder. In beiden Fällen ist über die Zuordnung der Schlüssel-ID zur Lehrkraft oder anderen Schlüsselinhabern im Schließplan ein Personenbezug möglich. Bei entsprechend hoher Anzahl von Speichereinträgen lässt eine derartige Verarbeitung personenbezogener Daten auch die Erstellung eines Bewegungsprofiles des Schlüsselinhabers zu.

Datenschutzrechtlich verantwortlich für die Verarbeitung personenbezogener Daten im Rahmen des Betriebs der elektronischen Schließanlage ist vorliegend der Schulträger. Dieser ist gemäß § 48 Absatz 2 des Schulgesetzes für die äußeren Schulangelegenheiten verantwortlich, zu welchem auch der Einbau und die Erneuerung einer elektronischen Schließanlage sowie deren Betrieb zählt.

Eine Speicherung der Schließvorgänge auf den Schließzylindern oder dem RFID-Transponder ist gemäß § 4 Absatz 1 des Landesdatenschutzgesetzes nur erlaubt, wenn eine Rechtsvorschrift dies ausdrücklich erlaubt oder der Betroffene seine Einwilligung erklärt hat. Der Schulträger hat sich vorliegend zunächst auf die Einwilligung der betroffenen Personen berufen. Die mir vorgelegte Einwilligungserklärung kann die Verarbeitung personenbezogener Daten allerdings nicht rechtfertigen. Sofern der Schulträger seine Datenverarbeitungsbefugnis künftig auf eine Einwilligung stützten möchte, muss diese zwingend überarbeitet werden.

Die vom Schulträger ergänzend genannten Rechtsgrundlagen können ebenfalls nicht überzeugen: Der Schulträger argumentiert im Wesentlichen damit, dass er als sächlicher Ausstatter der Schule natürlich ein großes Interesse am Schutz seines Eigentums habe. Straftaten wie z.B. der Diebstahl oder die Beschädigung von Schulmitteln (z.B. Beamer im PC-Raum) könnten nach dessen Auffassung durch das Auslesen des Schließzylinders und die an-

schließende Auswertung der Schließvorgänge leichter und effizienter aufgeklärt werden. Die Speicherung und Auswertung personenbezogener Daten von Lehrkräften, Hausmeister und Schulsekretärin sei daher erforderlich, um seine Aufgabe – Schutz des Eigentums – erfüllen zu können.

Ich habe erhebliche Zweifel, ob die Auswertung der Aufzeichnungen und Protokolle der Schließvorgänge zu einer leichteren und effektiveren Aufklärung von Straftaten führt und dadurch das Eigentum des Schulträgers besser geschützt werden kann. Denn der Personenkreis, dessen Daten vornehmlich gespeichert werden, dürften eher nicht zum potenziellen Täterkreis zählen und deshalb allenfalls eine sehr begrenzte abschreckende Wirkung entfalten. Auch besteht die Gefahr, dass die betroffenen Personen sehr schnell grundlos verdächtigt werden, eine Straftat begangen zu haben. Schließt z.B. ein Lehrer auf die Bitte von Schülern den besagten PC-Raum auf, um diesen die Internetrecherche für ein anstehendes Referat zu ermöglichen, gerät im Falle eines Diebstahls automatisch die Lehrkraft in Verdacht, einen Gegenstand entwendet zu haben, da dessen Transponderkennung als letzter Eintrag im Speicher des Schließzylinders steht. Als potenzielle Täter kommen jedoch genauso die Schüler, eventuell sogar weitere Personen in Betracht. Immerhin ist nicht auszuschließen, dass die Schüler, die der Lehrer eingelassen hat, weiteren Personen Zugang gewährten.

Selbstverständlich muss dem Schulträger daran gelegen sein, sein Eigentum bestmöglich zu schützen. Dass dieses Ziel mit der Verarbeitung von Lehrerdaten erreicht oder besser erreicht werden kann, erschließt sich mir allerdings nicht. Ich bin nach wie vor im Gespräch mit dem Schulträger und gehe davon aus, dass gerade auch in dessen eigenem Interesse noch eine für alle Beteiligten tragbare Lösung gefunden werden kann.

Elektronische Schließanlagen bieten zweifelsohne Vorteile. Sollen dabei personenbezogene Daten verarbeitet werden, muss der Schulträger als in der Regel verantwortliche Stelle rechtzeitig vor Einbau und Inbetriebnahme des Systems prüfen, ob und unter welchen Voraussetzungen dieses datenschutzkonform betrieben werden kann.

8.2 Besuch von der Aufsicht – Kontrollbesuch an einer Schule

Mein Vorgänger im Amt hatte sich sowohl im 29. Tätigkeitsbericht 2009 (LT-Drucksache 14/5500, S. 63f.) als auch im 30. Tätigkeitsbericht 2010/2011 (LT-Drucksache 15/955, S. 87f.) mit den Entwicklungen rund um das Thema Datenschutz an Schulen befasst. Als Reaktion auf eine aus datenschutzrechtlicher Sicht ernüchternde „Bestandsaufnahme" hat das Kultusministerium in der Folge zahlreiche Maßnahmen ergriffen, mit dem Ziel, die datenschutzrechtliche Situation an öffentlichen Schulen zu verbessern. Grund genug nach Jahren der Umsetzung und Implementierung dieser Maßnahmen den aktuellen Status Quo in Sachen Datenschutz zu überprüfen.

Heute steht den öffentlichen Schulen in Baden-Württemberg in punkto Datenschutz ein vielschichtiges Angebot aus Handreichungen, Fortbildungsangeboten und weiteren Maßnahmen einschließlich kompetenter Ansprechpartner zur Verfügung. Besonders hervorzuheben ist dabei die überarbeitete Verwaltungsvorschrift zum Datenschutz an öffentlichen Schulen vom 5. Dezember 2014, welche nunmehr umfangreich die schulischen Datenschutzbelange aufgreift und regelt. Ein Bericht hierzu findet sich im 32. Tätigkeitsbericht 2014/2015 (LT-Drucksache 15/7990, S.141).

Ungeachtet dessen sehen sich die Schulleitungen mit ständig neuen und komplexen datenschutzrechtlichen Fragestellungen konfrontiert, wie sich auch im Rahmen eines Kontrollbesuchs an einer Gemeinschaftsschule gezeigt hat. So geht es beim schulischen Datenschutz längst nicht mehr nur um die klassischen Themen wie die Aufbewahrung und den Umgang mit Schüler- und Personalakten. Mittlerweile muss eine Schulleitung Antworten auf datenschutzrechtliche Fragestellungen zur Ausgestaltung der schulischen Netze, der Nutzung von Kursmanagementsystemen und Lernplattformen, zu Verfahrensverzeichnissen der schulischen Verfahren, zur dienstlichen Nutzung privater Datenverarbeitungsgeräte von Lehrkräften und zu den Rahmenbedingungen einer elektronischen Kommunikation zwischen Schule und Erziehungsberechtigten bzw. Ausbildungsbetrieben geben. Durch die Auslagerung klassischer schulischer Verfahren in eine Cloud sind ebenfalls neue, recht komplexe Szenarien entstanden, deren daten-

schutzkonforme Umsetzung Schulleitungen mitunter an ihre Grenzen führt.

In der von mir kontrollierten Gemeinschaftsschule unterstützt ein zum Datenschutzbeauftragten der Schule bestellter Lehrer die Schulleitung in datenschutzrechtlichen Belangen. Die Lehrkraft wird nach eigenen Angaben demnächst die für schulische Datenschutzbeauftragte verpflichtende zweitägige Fortbildungsveranstaltung beim zuständigen Regierungspräsidium besuchen. Die Einführung dieser Fortbildungsmaßnahme stellt eine der bereits erwähnten Maßnahmen des Kultusministeriums zur Verbesserung der Situation dar.

Aufgabe des Datenschutzbeauftragten ist u.a. die Führung des Verfahrensverzeichnisses der an der Gemeinschaftsschule eingesetzten schulischen Verfahren. Wertvolle Hilfe leistet hierbei die von Kultusministerium eingeführte Plattform „Verfahrensverzeichnis-Online-BW" – ebenfalls eine sinnvolle und notwendige Hilfestellung.

Die Schulen nehmen nach meiner Kenntnis die angebotenen Hilfestellungen gerne in Anspruch, so auch die Gemeinschaftsschule. Dies gilt insbesondere auch für die Nutzung der Mustervorlagen zur Einwilligung in die Veröffentlichung von personenbezogenen Daten und Fotos von Schülerinnen und Schülern, welche mittels des Lehrerfortbildungsservers der Landesakademie in Esslingen allen Schulen kostenfrei zur Verfügung steht.

Die Problematik der bisher noch aktivierten Möglichkeit zur E-Mailweiterleitung vom dienstlichen auf den privaten E-Mail-Account von Lehrkräften war dem schulischen Datenschutzbeauftragten der Gesamtschule durchaus bewusst. Die Abschaltung der Weiterleitungsfunktion nach einer vorausgehenden Sensibilisierung des Kollegiums steht angabegemäß vor der Umsetzung. Ebenso soll künftig die Nutzung privater Datenverarbeitungsgeräte der Lehrkräfte für dienstliche Zwecke durch das Anlagenformular der Verwaltungsvorschrift zum Datenschutz an öffentlichen Schulen geregelt werden. Auch hier wird der schulische Datenschutzbeauftragte die Umsetzung begleiten und die Schulleitung hierdurch entlasten.

Die vom Kultusministerium eingeführten unterstützenden Maßnahmen, wie z.B. die Vermittlung von datenschutzrechtlichem Fachwissen bei Schulleitungen und schulischen Datenschutzbeauftragten und das elektronische „Verfahrensverzeichnis-Online-BW", sind in der Schule angekommen und zeigen Wirkung. Der Umgang der Schulen mit personenbezogenen Daten hat sich insgesamt erheblich verbessert. So erfreulich diese Entwicklung auch ist, den Schulen sollte stets bewusst sein, dass nicht zuletzt durch die Digitalisierung und die damit einhergehenden komplexeren Verfahren und Anwendungen immer wieder neue datenschutzrechtliche Herausforderungen auf sie zukommen. Eine fachlich kompetente Beratung und Unterstützung der Schulleitung durch den schulischen Datenschutzbeauftragten ist daher wichtiger denn je. Insoweit begrüße ich es nachdrücklich, dass mit Wirksamwerden der EU-Datenschutz-Grundverordnung die Schulen verpflichtet sind, einen Datenschutzbeauftragten zu bestellen (vgl. Artikel 37 Absatz 1 lit. a). Die Vermittlung datenschutzrechtlichen Fachwissens ist und bleibt zwingend notwendig. Das geplante Aufstocken der Fortbildungsdauer und die Erweiterung der Ausbildungsinhalte der schulischen Datenschutzbeauftragten kann allerdings nur ein erster Schritt sein. Die bereits bestehende Vernetzung und der Austausch der Datenschutzbeauftragten untereinander, sowie mit den Ansprechpartnern in den Abteilungen 7 der Regierungspräsidien, muss weiter vorangetrieben werden. Damit einhergehen sollte eine Deputatsentlastung der Datenschutzbeauftragten, um ihnen die Zeit zu geben, die notwendig ist, um die anspruchsvolle Aufgabe sachgerecht erledigen zu können.

8.3 Zur Vorlage der Grundschulempfehlung an die weiterführende Schule

Seit dem laufenden Schuljahr müssen die Erziehungsberechtigten der weiterführenden Schule die Grundschulempfehlung vorlegen:

Die Grundschule erteilt eine Empfehlung, welche *weiterführende Schulart das Kind aus pädagogisch-fachlicher Sicht besuchen soll (Grundschulempfehlung). Die Erziehungsberechtigten legen als Teil der Anmeldung die Grundschulempfehlung der weiterführenden Schule vor.* (§ 5 Absatz 2 Sätze 4 und 5 des Schulgesetzes – SchulG)

Dabei entscheiden die Erziehungsberechtigten weiterhin über die weiterführende Schulart; die Grundschulempfehlung ist, wie der Begriff sagt, nicht verbindlich:

Die freie Entscheidung der Erziehungsberechtigten für eine der auf der Grundschule aufbauenden Schularten bleibt hiervon unberührt (§ 5 Absatz 2 Satz 6 SchulG).

Das Kultusministerium hatte meine Dienststelle beim Ausarbeiten dieser Vorschrift beteiligt und den Entwurf mit Begründung gesandt. Die gesetzliche Pflicht zur Vorlage der Grundschulempfehlung bei der weiterführenden Schule ist – unabhängig davon, dass die Grundschulempfehlung für die Erziehungsberechtigten nicht verbindlich ist – datenschutzrechtlich bedeutsam und greift in das Recht auf informationelle Selbstbestimmung ein, denn die weiterführende Schule erfährt so, welche weiterführende Schulart das Kind aus pädagogisch-fachlicher Sicht der Grundschule besuchen soll. Deswegen habe ich das Kultusministerium darauf hingewiesen, dass diesem Grundrechtseingriff ein legitimer Zweck zugrunde liegen und er mit Blick auf diesen Zweck und auf die Intensität des Grundrechtseingriffs geeignet, erforderlich und verhältnismäßig sein muss, und u.a. ausgeführt, dass mir das mit Blick auf die (zu) allgemeinen Ausführungen in der Begründung dazu fraglich schien. Zwar hieß es dort, dass es für die Schüler vorteilhaft sei, wenn die aufnehmende Schule die Grundschulempfehlung ihrer neuen Schüler kennt (z.B. dass „die aufnehmende Schule frühzeitig, schon zu Beginn des neuen Schuljahres, die erforderlichen organisatorischen und auch pädagogischen Entscheidungen treffen" könne, „um Kinder mit und ohne entsprechende Grundschulempfehlung von Anfang an zielgerichtet zu fördern"), allerdings blieb dabei m. E. u.a. offen, wie das konkret aussehen soll (also z.B. wer an den aufnehmenden Schulen welche organisatorischen und welche pädagogischen Entscheidungen hinsichtlich der Kinder mit und der Kinder ohne entsprechende Grundschulempfehlung treffen und was das bewirken wird). Der vorgesehene Grundrechtseingriff war somit m. E. nicht hinreichend tief begründet (eine hinreichend tiefe Begründung muss hier auch [hinreichend tiefe] pädagogische Ausführungen bzw. Erwägungen enthalten, wobei die jeweils zugrunde liegenden pädagogischen Auffassungen meiner datenschutzrechtlichen Bewertung vorgreiflich sind und außerhalb meines Aufgabenbereiches liegen). Das Kultusministerium überarbeitete auf meine Stellungnahme hin den Gesetzentwurf (vgl. LT-Drs. 16/1749, http://www.landtag-bw.de/files/live/sites/LTBW/files/dokumente/WP16/Drucksachen/1000/16_1749_D.pdf mit dem überarbeiteten Gesetzentwurf und dem Inhalt meiner Stellungnahme zum ursprünglichen Entwurf des Kultusministeriums, dort S. 20 ff.).

Nachdem der Landtag das Gesetz am 3. Mai 2017 beschlossen hat, ist es am 1. August 2017 in Kraft getreten (GBl. S. 251). Bleibt zu hoffen, dass die (Pflicht zur) Vorlage der Grundschulempfehlung den Schülern an den weiterführenden Schulen tatsächlich nützt.

8.4 Zur Vorlage der Zeugnishefte der Grundschule an die weiterführende Schule sowie zum Austausch der weiterführenden Schule und der Grundschule über Schüler

Einige Schulen verlangten am Anfang dieses Schuljahrs – zusätzlich zur ihnen ohnehin vorzulegenden Grundschulempfehlung – von allen neuen Schülern deren Zeugnishefte der Grundschulen sowie eine Einwilligung, dass sie mit der Grundschule über die Schüler sprechen dürfen.

Datenschutzrechtlich bedeutsam ist das, weil die weiterführenden Schulen

- mit den Zeugnisheften der Grundschulen personenbezogene Daten (etwa die Noten der Schüler) erheben und
- im Gespräch mit den Grundschulen personenbezogene Daten über die Schüler erheben und übermitteln.

Für Beides sahen wir nach erster Prüfung keinen Raum. Deswegen legten wir dem Kultusministerium Baden-Württemberg unsere datenschutzrechtlichen Überlegungen dazu dar mit der Bitte, uns seine Meinung mitzuteilen. Das Kultusministerium schloss sich unserer Einschätzung an, erläuterte seine Auffassung und kündigte an, die Schulen alsbald auf die Grenzen der Verarbeitung personenbezogener Daten beim Aufnahmeverfahren für die weiterführenden Schulen hinzuweisen. Das ist ein Beispiel für die seit geraumer Zeit gute Zusammenarbeit des Kultusministeriums und meiner Dienststelle.

Ausgangspunkt für die datenschutzrechtliche Bewertung der Ansinnen der Schulen ist § 4 Absatz 1 LDSG:

Die Verarbeitung personenbezogener Daten ist nur zulässig,
1. *wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder*
2. *soweit der Betroffene eingewilligt hat.*

Als solche „andere Rechtsvorschrift" kommt § 115 Absatz 3 des Schulgesetzes (SchulG) in Betracht:

Eine Schule ist berechtigt, zu schulübergreifenden Verwaltungszwecken personenbezogene Daten von Schülern, deren Erziehungsberechtigten und denjenigen, denen Erziehung oder Pflege eines Schülers anvertraut ist, bei einer anderen Schule zu erheben.

Dabei geht es nach der Gesetzesbegründung etwa darum, dass bei einem Schulwechsel die aufnehmende Schule die zu ihrer Aufgabenerfüllung notwendigen Schülerstammdaten bei der abgebenden Schule erhebt (vgl. LT-Drs. 13/4431 S. 9, http://www.landtag-bw.de/files/live/sites/LTBW/files/dokumente/WP13/Drucksachen/4000/13_4431_D.pdf). Um solche zur Aufgabenerfüllung notwendigen Schülerdaten geht es hier jedoch jeweils nicht.

Hinsichtlich der Zeugnishefte der Grundschulen ist auch Nummer 3.4.1 der „Verwaltungsvorschrift des Kultusministeriums über das Aufnahmeverfahren für die auf der Grundschule aufbauenden Schularten; Orientierungsstufe" vom 4. November 2015 (K. u. U. S. 415, ber. 2016 S. 134), geändert durch Verwaltungsvorschrift vom 22. Juni 2017 (K. u. U. S. 101), in den Blick zu nehmen:

Zum vorgesehenen Termin melden die Erziehungsberechtigten unter Vorlage der Bestätigungen der Grundschule und der Grundschulempfehlung (Anlage, Blatt 4, 5 und 7) ihr Kind bei der Werkrealschule/Hauptschule, der Realschule, dem Gymnasium oder der Gemeinschaftsschule an. Erziehungsberechtigte, deren Kinder in Baden-Württemberg schulpflichtig sind, sind nicht verpflichtet, Zeugnisse und Halbjahresinformationen bei der aufnehmenden Schule vorzulegen.

Hiervon unberührt bleiben die schulrechtlich durch Verordnung oder Schulversuchsregelungen auf der Grundlage des Schulgesetzes erfolgten Festlegungen. Danach gilt Folgendes:

- *Am Deutsch-Französischen Gymnasium kann bei der Anmeldung die Vorlage der Halbjahresinformation Klasse vier gefordert werden.*
- *An Gymnasien können, soweit die Zahl der Anmeldungen die vorhandene Kapazität übersteigt, für die Aufnahme in einen bilingualen Zug die Noten in Deutsch und Mathematik erfragt und zur Grundlage der Aufnahmeentscheidung gemacht werden.*

Die hinter dieser Regelung für den Bereich der Anmeldung an der weiterführenden Schule stehende Wertung kommt nach Mitteilung des Kultusministeriums auch nach der Aufnahme an der neuen Schule zum Tragen.

Danach besteht keine Rechtsgrundlage dafür, dass aufnehmende Schulen sich generell die Zeugnishefte der Grundschulen vorlegen lassen; die freiwillige Vorlage ist allenfalls im Einzelfall auf Grundlage einer Einwilligung zulässig.

Hinsichtlich Einwilligungen der Erziehungsberechtigten in ein Gespräch der aufbauenden Schulen mit der Grundschule über einen einzelnen Schüler ist auch Nummer 4.7.1 Sätze 1 bis 4 der genannten „Verwaltungsvorschrift des Kultusministeriums über das Aufnahmeverfahren für die auf der Grundschule aufbauenden Schularten; Orientierungsstufe" bedeutsam:

Zur Erörterung der ihre Schulen gemeinsam berührenden Fragen muss zwischen den Leiterinnen und Leitern der auf der Grundschule aufbauenden Schulen und der in deren Einzugsbereich liegenden Grundschulen mindestens ein Informationsgespräch pro Schuljahr stattfinden. Hierbei sollen vor allem Fragen der Lernmittel, der Information der Erziehungsberechtigten, der Anwendung der Regelungen für das Aufnahmeverfahren und die Orientierungsstufe, der schulartübergreifenden Kontakte der Lehrkräfte sowie der Organisation von Unterrichtshospitationen erörtert werden. Einzelne Schülerinnen und Schüler betreffende Fragen sind nicht Gegenstand dieser Informationsgespräche. Einzelfälle dürfen nur besprochen werden, wenn hierfür eine entsprechende Einwilligung der Erziehungsberechtigten vorliegt.

In den Informationsgesprächen zwischen den Leitungen der Grundschulen und der weiterführenden Schulen sollen nach Mitteilung des Kultusministeriums die diese Schulen gemeinsam berührenden Fragen erörtert werden, deren Gegenstand von der Person des einzelnen Schülers losgelöste Fragestellungen sind, etwa zu Lernmitteln, der Information der Erzie-

hungsberechtigten oder der Organisation von Unterrichtshospitationen; die Besprechung von Einzelfällen bildet nach dieser Regelung eine Ausnahme bei der Zusammenarbeit zwischen den Schularten.

Danach besteht auch für ein generelles Einholen von Einwilligungen der Erziehungsberechtigten in ein Gespräch der aufbauenden Schulen mit der Grundschule über einen einzelnen Schüler keine Rechtsgrundlage. Nur dann, wenn sich hinsichtlich einzelner Schüler tatsächlich ein solcher Gesprächsbedarf ergeben sollte, darf die aufbauende Schule die Erziehungsberechtigten auf eine solche Einwilligung ansprechen; erst dann kann sie den Erziehungsberechtigten mitteilen, um welche konkrete Angelegenheit und damit um welche Angaben im Einzelnen es gehen soll, sodass sie wissen können, in was sie ggf. einwilligen.

Schulen müssen sich vor einem Verarbeiten von Daten über Schüler (etwa bevor sie die Zeugnisse der Grundschule verlangen oder die Erziehungsberechtigten auf eine Einwilligung ansprechen) stets vergewissern, dass sie das dürfen. Dazu können sie die einschlägigen Vorschriften heranziehen oder sich an ihre Aufsichtsbehörde bei der Kultusverwaltung wenden.

8.5 Was darf die Duale Hochschule Ausbildungsstätten über Studierende mitteilen?

Ausbildungsstätten hatten die Duale Hochschule gebeten, ihnen bestimmte Daten über Studierende (etwa deren Exmatrikulation) mitzuteilen. Die Duale Hochschule kam nach interner Prüfung dieser Frage wegen Beratung auf uns zu.

Die Duale Hochschule Baden-Württemberg ist eine staatliche Hochschule. Ihr zentrales Merkmal ist ihr duales Studienkonzept mit Wechsel von Theorie- und Praxisphasen und der engen Kooperation mit den Ausbildungsstätten. Diese wählen die Studierenden selbst aus, schließen mit ihnen einen dreijährigen Vertrag und bieten ihnen über die gesamte Studiendauer hinweg eine monatliche fortlaufende Vergütung (http://www.dhbw.de/die-dhbw/wir-ueber-uns.html).

Mit ihrem Wunsch, etwa von einer Exmatrikulation zu erfahren, wollten Ausbildungsstätten u.a. sicherstellen, dass sie ihre Rechte aus dem Studien- und Ausbildungsvertrag zwischen Ausbildungsstätte und Studierendem (danach war z.B. Exmatrikulation ein Kündigungsgrund) geltend machen konnten (z.B. bei vorzeitiger Exmatrikulation, etwa wegen Verlusts des Prüfungsanspruchs, den Studien- und Ausbildungsvertrag kündigen und die Vergütung einstellen). Der Studien- und Ausbildungsvertrag enthielt keine ausdrückliche Pflicht der Studierenden, den Ausbildungsstätten z.B. eine Exmatrikulation mitzuteilen.

Nach Erörterung mit der Dualen Hochschule blieb u.a. festzuhalten, dass der Wortlaut des geltenden Landeshochschulgesetzes die Frage zur Weitergabe von Studierendendaten an Ausbildungsstätten nicht beantwortet. Wir verwiesen auf das Beispiel des § 90 Absatz 8 Satz 3 des Schulgesetzes (SchG), der vorsieht, dass die (Berufs-)Schule bestimmte Angaben über Schüler den für die Berufserziehung der Schüler Mitverantwortlichen (das sind nach § 85 Absatz 2 SchG Ausbildende, Dienstherren und Leiter von Betrieben) mitteilt, und der wie folgt lautet:

Ein zeitweiliger Ausschluss vom Unterricht, seine Androhung, ein Ausschluss aus der Schule oder seine Androhung wird den für die Berufserziehung des Schülers Mitverantwortlichen mitgeteilt.

Die Duale Hochschule wandte sich wegen dieser Frage an das Wissenschaftsministerium Baden-Württemberg. Inzwischen hat dieses uns den Entwurf eines Gesetzes zur Weiterentwicklung des Hochschulrechts mit einem neuen § 12 Absatz 2 Satz 2 des Landeshochschulgesetzes vorgelegt. Dieser lautet:

Die DHBW darf den Ausbildungsstätten nach § 65 c Daten über Studierende, die mit der jeweiligen Ausbildungsstätte einen Ausbildungsvertrag geschlossen haben, übermitteln, die den Zeitpunkt oder die Aufhebung der Immatrikulation, den Zeitraum einer Beurlaubung, die Ladung zu einer Wiederholungsprüfung, den Verlust des Prüfungsanspruchs, den Zeitpunkt der Exmatrikulation sowie gegen diesbezügliche Entscheidungen der DHBW eingelegte Rechtsbehelfe betreffen.

Dabei wäre ggf. zu verdeutlichen, um welche Daten genau es gehen soll. Zudem konnte ich der Begründung zum Entwurf nichts dazu entnehmen, ob der damit vorgesehene Eingriff in das Grundrecht der Studierenden auf infor-

mationelle Selbstbestimmung erforderlich und verhältnismäßig ist. Das habe ich dem Wissenschaftsministerium mitgeteilt und darauf hingewiesen, dass es sich empfehlen dürfte, dass es den Entwurf entsprechend ändert.

Vorschriften über das Verarbeiten personenbezogener Daten müssen u.a. erkennen lassen, inwieweit sie deren Zulässigkeit begründen oder erweitern (und so in das Recht auf informationelle Selbstbestimmung eingreifen) sollen. Der Datenverarbeitung, die zulässig sein soll, muss ein legitimer Zweck zugrunde liegen und sie muss mit Blick darauf und auf die Intensität des Eingriffs in das Recht auf informationelle Selbstbestimmung geeignet, erforderlich und verhältnismäßig sein.

8.6 Langer Weg zur Auskunft

Dem Betroffenen ist von der speichernden Stelle auf Antrag unentgeltlich über die zu seiner Person gespeicherten Daten Auskunft zu erteilen (§ 21 Absatz 1 Satz 1 Nummer 1 LDSG). Was konkret bedeutet dies, wenn Daten dezentral gespeichert werden?

Ein ehemaliger Studierender (Betroffener) hatte bei seiner Hochschule Auskunft beantragt und mitgeteilt, er erwarte einen kompletten Auszug seiner Daten. Damit hatte er Auskunft über alle bei der Hochschule zu seiner Person gespeicherten Daten beantragt. Die Hochschule teilte dem Betroffenen mit, sie speichere personenbezogene Daten dezentral. Deswegen benötige sie vom ihm zunächst Angaben dazu, um welche Bereiche und Systeme der Hochschule es ihm gehe. Sie bezog sich dabei auf § 21 Absatz 2 LDSG.

In dem Antrag soll die Art der personenbezogenen Daten näher bezeichnet werden, über die Auskunft erteilt werden soll. Sind die personenbezogenen Daten in Akten gespeichert, wird Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. (§ 21 Absatz 2 LDSG).

Der Betroffene hatte im Zusammenhang mit dem Auskunftsantrag u.a. auch Einsicht in die Bewertung einer bestimmten Arbeit beantragt. Deswegen umfasste sein Auskunftsantrag jedenfalls – ohne zusätzliche Angaben des Betroffenen nach § 21 Absatz 2 LDSG – diejenigen Daten, die im Zusammenhang mit einer solchen Arbeit und einem vorangehenden Studium regelmäßig anfallen (z.B. etwaige Daten bei der Hochschulbibliothek, dem Rechenzentrum, der/den jeweiligen Fakultät[en] beziehungsweise dem/den jeweiligen Institut[en] sowie der zentralen Studien- und Prüfungsverwaltung). Es war nichts dafür ersichtlich, dass hier die Hochschule als Voraussetzung einer Auskunft über diese Daten zunächst Angaben nach § 21 Absatz 2 LDSG fordern durfte; vielmehr hatte sie insoweit ohne solche Angaben des Betroffenen Auskunft zu erteilen.

Soweit die Hochschule darüber hinaus für eine Auskunft Angaben nach § 21 Absatz 2 LDSG benötigte, lag es jedenfalls grundsätzlich zunächst an ihr, dem Betroffenen Hinweise zu geben, die ihm diese Angaben ermöglichen: Die nähere Bezeichnung der Art der Daten ist dem Betroffenen umso eher möglich und zumutbar, je besser die verantwortliche Stelle ihn über die Systematik ihrer Datenbestände informiert. Eine Obliegenheit des Betroffenen zu solchen Angaben besteht nur insoweit, als ihm diese aufgrund seines Kenntnisstands möglich sind. Eine etwaige unzureichende Behördenorganisation schränkt den Anspruch auf Auskunft nicht zu Lasten des Betroffenen ein.

Solche Hinweise, die dem Betroffenen Angaben nach § 21 Absatz 2 LDSG ermöglichen, konnte die Hochschule etwa geben, indem sie ihm die Bereiche mitteilte, in denen sie personenbezogene Daten speichert, gegebenenfalls auch, ob das in Akten geschieht, sowie welche (weiteren) Angaben sie insoweit jeweils für eine Auskunft benötigte. Das gilt beispielsweise für Angaben, anhand derer die Hochschule ihre Datenbestände nach Daten auswerten kann, die zur Person des Betroffenen gespeichert sind.

Dass die Hochschule dem Betroffenen zunächst keine Auskunft erteilt, sondern von ihm Angaben nach § 21 Absatz 2 LDSG erwartet hatte, ohne ihm Hinweise gegeben zu haben, die ihm solche Angaben ermöglichen, habe ich beanstandet. Die Hochschule hat mir daraufhin mitgeteilt, sie habe den Auskunftsanspruch des Betroffenen durch Übersenden von Ausdrucken und Kopien in Papierform erfüllt und sei meinen Empfehlungen gefolgt.

Wenn eine Hochschule personenbezogene Daten dezentral speichert und möchte, dass der

Betroffene, der bei ihr Auskunft beantragt hat, die Art der personenbezogenen Daten näher bezeichnet, über die Auskunft erteilt werden soll, oder Angaben macht, die das Auffinden der Daten ermöglichen, dann liegt es jedenfalls grundsätzlich zunächst an der Hochschule, dem Betroffenen Hinweise zu geben, welche ihm diese Angaben ermöglichen.

9. Arbeitswelt

9.1 Der Datenschutz und seine Tücken

Es kommt nicht selten vor, dass Betroffene unter dem Mantel des Datenschutzes einen Vorteil erzielen wollen – um eine Verletzung in ihrem Recht auf informationelle Selbstbestimmung geht es da manches Mal gar nicht. Als Landesbeauftragter für den Datenschutz und die Informationsfreiheit wird man auch mal instrumentalisiert.

Erkennen wir, dass der Datenschutz nur als Vorwand dient, um etwa einem früheren Arbeitgeber Ärger zu machen, weisen wir den Betroffenen entsprechend hierauf hin. Dem einen oder anderen Betroffenen kann es dann auch mal die Sprache verschlagen, wie ein Fall unserer täglichen Praxis zeigt:

Der Betroffene bewarb sich aufgrund eines Vermittlungsvorschlags des Jobcenters bei einem Personaldienstleister. Ganz charmant wurde im Bewerbungsschreiben mitgeteilt, dass er die vorgesehene Tätigkeit nicht ausüben könne und auch nicht zur Einarbeitung bereit sei. Für den Fall, dass man ihn zu einem persönlichen Gespräch einladen möchte, behielt er sich vor, von seinem Rechtsbeistand begleitet zu werden. Zur Krönung legte er seiner Bewerbung einen „Übermittlungswiderspruch" bei, nach dem es dem Personaldienstleister untersagt sein soll, personenbezogene Daten an Dritte weiterzugeben. Hieran hielt sich der Personaldienstleister zum Nachteil des Bewerbers allerdings nicht. Die Folge war die Kürzung von Sozialleistungen durch das Jobcenter.

Entgegen der Auffassung des Beschwerdeführers durften seine personenbezogenen Daten an das Jobcenter übermittelt werden. Nach dem Sozialrecht (vgl. § 57 Zweites Sozialgesetzbuch) ist der Arbeitgeber verpflichtet, den Agenturen für Arbeit auf deren Verlangen hin Auskunft über solche Tatsachen zu geben, die für die Entscheidung über einen Anspruch auf Sozialleistungen erheblich sein können. Da das Jobcenter beim Personaldienstleister Nachfragen zur Ernsthaftigkeit der Bewerbung gestellt hat, durfte er diese auch beantworten. Der Beschwerdeführer wollte nicht auf Anhieb verstehen, dass sein als „Übermittlungswiderspruch" deklariertes Schreiben nicht die gesetzlichen Erlaubnistatbestände außer Kraft setzen kann. Datenschutz ist also auch für Beschäftigte kein Wunschkonzert.

Nicht selten erfolgen Anfragen der Bundesagentur für Arbeit zu solchen Fällen telefonisch oder per E-Mail. Das Auskunftsverlangen der Bundesagentur für Arbeit sollte zu Beweiszwecken durch den Arbeitgeber als verantwortliche Stelle entsprechend dokumentiert werden.

9.1 Betriebliches Eingliederungsmanagement datenschutzkonform gestalten

Arbeitgeber/innen, wie auch Dienstherren, sind gemäß § 84 Abs. 2 Neuntes Sozialgesetzbuch (SGB IX) verpflichtet Arbeitnehmern/innen bzw. Beamten/Beamtinnen, die innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig waren, ein betriebliches Eingliederungsmanagement (BEM) anzubieten. Welche datenschutzrechtlichen Anforderungen bei der Ausgestaltung des BEM zu beachten sind, ist vielen Arbeitgebern nicht immer klar.

Die Durchführung des BEM hat einerseits das Ziel der Wiedereingliederung des/der Betroffenen, dient andererseits aber auch der Gesundheitsprävention mit dem Zweck, das Arbeitsverhältnis bzw. Dienstverhältnis dauerhaft zu sichern.

Eine bei uns eingegangene Beschwerde, ließ mich daran zweifeln, ob der Arbeitgeber bei der Betroffenen die vorgenannten Ziele verfolgte. Der Betroffene hatte der Durchführung des BEM zugestimmt. Er führte mehrere Gespräche mit dem vom Arbeitgeber ins Leben gerufenen BEM-Team. Die Gespräche wurden protokolliert und mit weiteren im Zusammenhang stehenden Schriftverkehr zwischen den Beteiligten vollständig zur Personalakte des Betroffenen genommen. Dass dieser damit nicht einverstanden war und dem BEM nur zustimmte, weil er davon ausgegangen ist, dass seine besonderen Arten personenbezogener Daten im Sinne von § 3 Abs. 9 Bundesdatenschutzgesetz auch besonders geschützt und vertraulich behandelt würden, liegt auf der Hand.
Es liegt in der Natur der Sache, dass bei der Durchführung eines BEM gegenläufige Interessen aufeinandertreffen. Arbeitnehmer, die das Angebot ihres Arbeitgebers bzw. Dienstherren ein BEM-Verfahren durchzuführen annehmen, haben ein berechtigtes Interesse daran, dass ihre besonderen Arten personenbezogener Daten (Gesundheitsdaten) umfassend geschützt werden. Andererseits benötigen Arbeitgeber

oder deren BEM-Beauftragte aufschlussreiche Informationen, um das BEM-Verfahren so effektiv wie möglich durchführen zu können. Um eine vertrauensvolle Zusammenarbeit zu gewährleisten, empfiehlt es sich, den sensiblen Umgang mit den besonderen Arten personenbezogener Daten so genau wie möglich in einer Betriebs-/ Dienstvereinbarung zu regeln. Hier sollten insbesondere zu folgenden Punkten Vereinbarungen getroffen werden:

- Art und Umfang der Daten, die erhoben werden,
- Zweck der Datenerhebung,
- Einwilligung der Betroffenen zur Erhebung von Daten im Rahmen des BEM,
- Schweigepflicht aller Beteiligten,
- Zugangsrechte zu den sensiblen Daten,
- Aufbewahrungsdauer sowie
- Aufbewahrungsort (Trennung von BEM-Akte und Personalakte).

Die alleinige Verantwortung für den BEM-Klärungs- und Steuerungsprozess liegt beim Arbeitgeber/Dienstherren, wobei die Aufgabe auch auf einen BEM-Beauftragten oder ein BEM-Team delegiert werden kann.

Da die Durchführung des BEM-Verfahrens unter dem Vorbehalt der Freiwilligkeit steht und nicht ohne die Einwilligung des Betroffenen durchgeführt werden kann, kann es durch Widerruf der Einwilligung auch jederzeit abgebrochen werden. Voraussetzung für eine wirksame Einwilligung der Betroffenen und damit für die ordnungsgemäße Durchführung des BEM ist, dass der Betroffene ausreichend über den Ablauf des BEM-Verfahrens informiert ist. Er ist über die Ziele des BEMs sowie darauf hinzuweisen, dass er zur Offenbarung über Art, Ausmaß und Hintergründe seiner Erkrankung weder verpflichtet ist noch seine Weigerung, Gesundheitsdaten zu offenbaren, zu beruflichen Nachteilen führt. Die Dokumentation von Gesprächen im Zusammenhang mit dem BEM ist ebenso wie sonstige Aufzeichnungen über sog. Mitarbeiter- oder Personalführungsgespräche, deren Ergebnisse in einer Zielvereinbarung festgehalten werden, aufgrund ihrer Zielsetzung (Verbesserung der Führungs- und Kooperationsbeziehungen zwischen Vorgesetztem und Mitarbeiter) kein zulässiger Gegenstand der Personalakte.
Deklaratorisch sollte festgehalten werden, dass die Verwendung der erhobenen Daten datenschutzrechtlich strikt zweckgebunden zu erfolgen, d.h., dass die Datenverarbeitung ausschließlich zum Erhalt und Bestand eines gesundheitsbedingt gefährdeten Arbeitsverhältnisses stattzufinden hat. Die für die Zwecke des Verfahrens erhobenen und gespeicherten Daten dürfen insbesondere nicht ohne weiteres für sonstige arbeitsvertragsrechtliche Zwecke verwendet werden. Die Nutzung der Daten etwa für ein Kündigungsverfahren wegen der gesundheitlichen Konstitution des Beschäftigten würde eine unzulässige Zweckänderung bedeuten. Damit im Zusammenhang steht, dass datenschutzorganisatorisch die eigentliche Akte zum betrieblichen Eingliederungsmanagement von der Personalakte getrennt bleiben muss. In die Personalakte gehören nur äußere Informationen, also Nachweise für die ordnungsgemäße Durchführung des BEM, wie ein Abdruck der Einladung zu einem Gespräch hierzu, die Antwort des Beschäftigten auf diese Einladung bzw. einen Vermerk über die Nichtantwort, ein Vermerk über die Beendigung des Verfahrens oder die Ablehnung des Verfahrens durch den Beschäftigten zu Dokumentationszwecken. Die inhaltlichen Informationen sind in der Dienststelle außerhalb der Personalverwaltung zu erheben und aufzubewahren. Es empfiehlt sich dabei, die für ein BEM erforderlichen Daten von einer besonderen Organisationseinheit, einer Ad-hoc-Kommission bzw. eines BEM-Beauftragten zu erheben, der informationell abgeschottet agiert und Vertraulichkeit gewährleisten kann und muss. Diese kann aus Vertretern des Arbeitgebers und den unterschiedlichen in § 84 Abs. 2 Neuntes Sozialgesetzbuch genannten Interessenvertretungen bestehen. Von einer Beteiligung von Bediensteten aus dem Bereich der Personalverwaltung wird bereits aus Akzeptanzgründen, aber in erster Linie wegen der datenschutzorganisatorischen Probleme, das Wissen aus dem Verfahren gegenüber der Personalverwaltung geheim zu halten, abzuraten sein.

Nur so kann der Betroffene darauf vertrauen, dass die Durchführung des BEM nicht dazu genutzt werden soll, die Karriere zu stoppen oder zu beenden, sondern die Wiedereingliederung und die Aufrechterhaltung der dauerhaften Arbeitsfähigkeit des Betroffenen im Vordergrund steht.

Das betriebliche Eingliederungsmanagement verursacht in vielen Unternehmen und Dienststellen einen hohen Arbeitsaufwand. Gerade deshalb sind verbindliche und klare Regelungen für alle Beteiligten und insbesondere für den Betroffenen von besonderer Bedeutung.

Nur so kann eine vertrauensvolle Basis geschaffen werden, ohne die ein BEM-Verfahren wenig Erfolg versprechend ist. Je nachdem ob ein Betriebsrat oder Personalrat existiert, sollten Betriebs- bzw. Dienstvereinbarungen abgeschlossen werden, die insbesondere Zugriffsrechte, Verschwiegenheitsverpflichtungen und die klare Trennung der BEM-Unterlagen von der Personalakte zum Gegenstand haben. Betroffene, die befürchten müssen, dass die gemachten Angaben über Gesundheitsdaten zu ihrem Nachteil gereichen, werden nicht alles Notwendige offenbaren. Ohne diese Informationen können die Ziele des BEM aber nicht erreicht werden.

9.3 Mit alten Bewerbungsunterlagen zum neuen Job?

Ist der Kampf im Bewerbungsalltag überstanden, stellen sich viele Betroffene die Frage: Was passiert eigentlich mit meinen Bewerbungsunterlagen? Die meisten wurden vielleicht schon bei der Stellenausschreibung darauf hingewiesen, dass eine Rücksendung von postalisch eingegangenen Unterlagen aus Kostengründen nicht erfolgen wird. Werden die Bewerberstapel dann in den hintersten Kellerecken des Unternehmens aufbewahrt oder landen sie „am besten" ungeschützt in der blauen Tonne, ohne zuvor auch nur einen Aktenvernichter gesehen zu haben? Wie sieht es mit den per E-Mail eingegangenen Bewerbungen aus? Werden sie jemals gelöscht oder können sich auch alle nachfolgenden Personaler oder gar die gesamte Belegschaft problemlos ein Bild der vergangenen letzten Bewerberjahre machen?

Die richtigen Antworten auf diese Fragen hängen erst einmal entscheidend davon ab, ob sich Unternehmen und Bewerber für einander entschieden haben und ein Arbeitsverhältnis eingegangen sind oder nicht. Bei einer Einstellung werden die Bewerbungsunterlagen in der Regel Teil der Personalakte. Pauschale Übernahmen dürfen aber nicht erfolgen, sondern nur in dem zur Durchführung des Beschäftigungsverhältnisses dann erforderlichen Umfang.

Hat sich der Kandidat gegen das Unternehmen als seinen zukünftigen Arbeitgeber entschieden oder dieser die Bewerbung der einzigen Frau bevorzugt behandelt und den männlichen Mitstreitern eine Abfuhr erteilt, sind deren Bewerbungsunterlagen unwiederbringlich zu löschen bzw. zu vernichten. Mit der Entscheidung eines bestimmten Bewerbers für eine vakante Stelle ist der Zweck der übrigen Bewerbungsunterlagen – nämlich das Auswahlverfahren – weggefallen und diese sind somit zu löschen oder dem Bewerber wieder auszuhändigen. Entsprechend ist zu verfahren, wenn eine Bewerbung von sich aus zurückgezogen wird.

Fast jede negative Personalentscheidung birgt jedoch die Gefahr eines Anti-Diskriminierungsprozesses wegen Verstoßes gegen das Allgemeine Gleichbehandlungsgesetz. Um Schadensersatzforderungen erfolgversprechend abwehren zu können, benötigen Arbeitgeber häufig die Bewerbungsunterlagen. Ohne sie wird es Arbeitgebern nur schwer möglich sein nachzuweisen, dass ein Bewerber nicht aus Gründen der ethnischen Herkunft, des Geschlechts, der Religion oder Weltanschauung, einer Behinderung, des Alters oder der sexuellen Identität benachteiligt wurde (vgl. § 1 Allgemeines Gleichbehandlungsgesetz). Die Gefahr, einer Klage nach dem Allgemeinen Gleichbehandlungsgesetz ausgesetzt zu werden, besteht aber nicht ewig. Will ein Bewerber eine Benachteiligung wegen eines vom Allgemeinen Gleichbehandlungsgesetz verbotenen Merkmals geltend machen, muss er dies innerhalb der Zweimonatsfrist des § 15 Abs. 4 AGG. Ich halte eine Speicherung über drei Monate hinaus daher für nicht erforderlich.

Um die Löschfrist für Bewerbungsunterlagen abgelehnter oder nicht mehr interessierter Bewerber auf eine konkrete Stelle einzuhalten, sollten die Datenverarbeitungsprogramme so konfiguriert werden, dass eine eigenständige Löschung im entsprechenden Turnus erfolgt.

Es gibt aber auch Fälle, bei denen beide Seiten an einer längeren Speicherung bzw. Aufbewahrung der Bewerbungsunterlagen interessiert sind. Solche Konstellationen findet man insbesondere bei weltweit tätigen Konzernen, die laufend neue Stellen ausschreiben, und bei Initiativbewerbungen. Gibt ein Bewerber unmissverständlich zu verstehen, dass er auch an anderen Positionen im Unternehmen interessiert wäre und bei zukünftigen Stellenbesetzungen berücksichtigt werden möchte, dürfen seine Unterlagen auch für längere Zeit gespeichert werden. Oft stellen Unternehmen Bewerbungsportale zur Verfügung, bei denen die Bewerber ihre Unterlagen selbst hochladen und eigenständig bearbeiten und löschen können. Grundsätzlich ist dieses Format zu begrüßen, da es dem Bewerber den weitesten Spielraum

für seine Datennutzung gewährt. Voraussetzung ist aber, den Bewerber ausreichend zu informieren, wie seine personenbezogenen Daten verarbeitet werden. Hierzu gehört auch eine Mitteilung, wie die Daten übertragen werden – hoffentlich verschlüsselt!

Stellt ein Unternehmen für das Einreichen der Bewerbung eine Bewerberplattform zur Verfügung, haben die Bewerber oft auch die Wahl, in einen sogenannten Talentpool aufgenommen zu werden. Hierdurch können die Bewerber auch für zukünftig zu besetzende Stellen berücksichtigt werden.

Bei einer bei uns eingegangen Beschwerde gegen eine führende Wirtschaftsprüfungsgesellschaft hatte sich ein Bewerber mit der Aufnahme in den Talentpool einverstanden erklärt. Aber auch die Datensammlung in einen Talentpool kann nicht zeitlich unbegrenzt erfolgen. Eine wirksame Einwilligung setzt auch die Kenntnis der Speicherdauer voraus. In den Datenschutzhinweisen der Wirtschaftsprüfungsgesellschaft lasen wir, dass die Speicherdauer drei Jahre beträgt und jede Kontaktaufnahme zu einer Verlängerung um weitere drei Jahre führt. Um was für eine Kontaktaufnahme es sich handeln musste, wurde den Bewerbern nicht mitgeteilt. So könnte bspw. auch ein Löschungsbegehren nach dieser schwammigen Regelung dazu führen, dass weitere drei Jahre gespeichert wird. Solche Fallkonstellationen werden Bewerber bei der Abgabe ihrer Einwilligung mit Sicherheit nicht im Sinn gehabt haben. Durch unsere Beratung konnten wir das Unternehmen davon überzeugen, dass bereits die erstmalige Speicherung von drei Jahren für sich genommen weder im Interesse des Unternehmens noch im Interesse des Bewerbers liegen kann. Auf unsere Frage, welchen Aussagegehalt drei Jahre alte Bewerbungsunterlagen in der heutigen Zeit noch haben können, fand das Unternehmen keine überzeugende Antwort. Schließlich konnte erreicht werden, dass die Unterlagen im Talentpool für einen Zeitraum von einem Jahr gespeichert werden dürfen und nur Kontaktaufnahmen, die mit dem Eingehen eines Beschäftigungsverhältnisses im konkreten Zusammenhang stehen, zu einer Verlängerung der Speicherdauer um sechs Monate führen können.

Entscheidet sich ein Unternehmen, Bewerbungsportale zu nutzen und den Bewerbern die Aufnahme in einen Talentpool zu ermöglichen, sollten die Datenschutzhinweise konkret formuliert werden. Hierbei ist insbesondere auf die jederzeitige Widerrufsmöglichkeit der Einwilligung hinzuweisen.
Vorratsdatenspeicherungen von Bewerbungsunterlagen dürfen nicht das Ziel sein, sondern Transparenz und Seriosität. Sonst setzen sich Unternehmen dem Vorwurf aus, unwirksame Einwilligungserklärungen zu produzieren.

9.4 Die „freiwillige“ Urinprobe

Lässt sich die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nicht auf eine bereichsspezifische Vorschrift oder das BDSG stützen, bleibt als weitere Datenverarbeitungsgrundlage nur die Einwilligung, also das vorherige Einverständnis des Betroffenen in die Verwendung seiner Daten.

Aber kommt eine Einwilligung im Beschäftigungsverhältnis überhaupt in Frage? Googelt man den Begriff Arbeitnehmer, spuckt die Suchmaschine Folgendes aus:

„Person, die abhängig, nämlich bei einem Arbeitgeber, beschäftigt ist.“

Die wirtschaftliche und persönliche Abhängigkeit einer Person legt den Schluss nahe, sie in einer Zwangslage zu sehen, die ihr eine freie Entscheidung unmöglich macht. Diese Annahme führte bei Datenschützern lange Zeit dazu, eine Einwilligung von Beschäftigten grundsätzlich nicht als Grundlage einer Datenerhebung, -verarbeitung oder -nutzung zu akzeptieren. Zu Recht hat man diesen Extremstandpunkt mittlerweile aufgegeben und den Beschäftigten ihr Recht auf informationelle Selbstbestimmung auch in einem Arbeitsverhältnis zugesprochen. Die Einwilligung kann auch positive Folgen für den einzelnen Arbeitnehmer haben, sodass es mit dem Sinn und Zweck des Datenschutzes nicht vereinbar wäre, die Beschäftigten pauschal der Möglichkeit einer Einwilligung zu berauben.

Das heißt jedoch nicht, dass wir als Aufsichtsbehörde gezwungen sind, Einwilligungen von Beschäftigten ungeprüft als Ermächtigung zur Datenverarbeitung anzuerkennen. Vielmehr sind wir gehalten, die Freiwilligkeit und Wirksamkeit einer jeden Einwilligung einer genauen Einzelfallprüfung zu unterziehen, wie der nächste Praxisfall veranschaulicht.

Der minderjährige Beschwerdeführer befand sich in einem Berufsausbildungsverhältnis. Weil

sein Arbeitgeber ihn verdächtigte, Cannabis zu konsumieren, erklärte sich der Beschwerdeführer bereit, sich einem Drogentest zu unterziehen. Der Arbeitgeber sah die Einwilligung als wirksame Rechtsgrundlage zur Erhebung, Verarbeitung und Nutzung der besonderen Arten personenbezogener Daten (Gesundheitsdaten nach § 3 Abs. 9 Bundesdatenschutzgesetz) des Beschäftigten an. Wir mussten ihn jedoch vom Gegenteil überzeugen. Gegen die Wirksamkeit der Einwilligung sprach im vorliegenden Fall neben der mangelnden Freiwilligkeit der Einwilligung und der Minderjährigkeit des Beschwerdeführers auch die Beschäftigung im Berufsausbildungsverhältnis.

Gemäß § 4a Abs. 1 Satz 1 Bundesdatenschutzgesetz ist eine Einwilligung nur wirksam, wenn sie auf der freien und informierten Entscheidung des Betroffenen beruht. Daneben ist der Betroffene auf den Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalls erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Es reicht nicht aus, nur auf die Einwilligung zu verweisen. Vielmehr sind auch die Umstände, unter denen die Einwilligung abgegeben wird, einzubeziehen. Eine Einwilligung beruht auf der freien Entscheidung des Betroffenen, wenn sie ohne Zwang abgegeben wird. Sie kann als Verwendungsregulativ nur so lange akzeptiert werden, wie sich der Betroffene nicht in einer Situation befindet, die ihn faktisch dazu zwingt, sich mit dem Zugriff auf seine verlangten Daten einverstanden zu erklären.

Der Arbeitgeber konnte vorliegend nicht ernsthaft von einer zwanglosen Willenserklärung ausgehen. Allein schon die Tatsache, dass sich der Beschwerdeführer in einer Berufsausbildung befand, lässt an der Freiwilligkeit der Entscheidung zweifeln. Beschäftigte in der Berufsausbildung befinden sich gegenüber dem Arbeitgeber in einer noch unterlegeneren Position, als es ausgebildete Beschäftigte tun. Der Auszubildende ist auf die Vermittlungswilligkeit des Ausbilders angewiesen und ist daher besonders zu schützen.
Die in den Blick zu nehmenden begleitenden Umstände stritten demnach eindeutig für eine unter Zwang und Druck abgegebene Erklärung: Nach Angaben des Arbeitgebers hat der Beschwerdeführer bei der Konfrontation mit dem Verdacht des Drogenkonsums stark angefangen zu zittern und diesen mit widersprüchlichen Antworten zu zerstreuen versucht. Zum Schluss soll der Betroffene den Konsum von Cannabis sogar eingeräumt haben. Es musste auch berücksichtigt werden, dass das Gespräch im Beisein weiterer Mitarbeiter stattgefunden hat. Vermutlich wollte der Arbeitgeber sich so eine eventuell noch notwendig werdende Beweisführung sichern. Die durch die Anwesenheit weiterer Personen wachsende Drucksituation und entstehende Prangerwirkung kann nur schlecht geleugnet werden.

Eine freiwillige Entscheidungsfindung scheiterte auch an der Minderjährigkeit des Beschwerdeführers. Ob Minderjährige in die Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten wirksam einwilligen können, beurteilt sich nach dem Grad ihrer Einsichtsfähigkeit. Abstrakte Aussagen, ob ab Erreichen eines bestimmten Alters diese Einsichtsfähigkeit gegeben ist, helfen nicht weiter. Ausschlaggebend ist immer der jeweilige Verwendungszusammenhang. Er entscheidet darüber, ob die Einwilligung des Minderjährigen ausreicht oder ob sein gesetzlicher Vertreter zusätzlich einverstanden sein muss. Im zu entscheidenden Fall sprachen die Umstände des Einzelfalls dafür, neben der Einwilligung des Beschwerdeführers auch die seines gesetzlichen Vertreters als notwendig anzusehen, da die Konsequenzen insbesondere in Bezug auf den weiteren beruflichen Werdegang als gravierend anzusehen waren.

Hinzu kam noch, dass die von § 4a Abs. 3 Bundesdatenschutzgesetz gestellten Anforderungen an die Einwilligung zur Erhebung besonderer Arten personenbezogener Daten nicht erfüllt waren. Eine Einwilligung muss sich bei dieser Datenkategorie ausdrücklich hierauf beziehen.

Die Erhebung besonderer Arten personenbezogener Daten war auch nicht nach § 28 Abs. 6 Nr. 3 Bundesdatenschutzgesetz erlaubt. Diese Vorschrift knüpft die zulässige Datenverwendung, ebenso wie § 32 Bundesdatenschutzgesetz, an das Erforderlichkeitsprinzip. Dass der Arbeitgeber dieses hier grob außer Acht gelassen hat, liegt auf der Hand. Der Beschwerdeführer hatte ja seinen Cannabiskonsum selbst bestätigt; auf Nummer sicher gehen musste der Arbeitgeber daher alle mal nicht, ein weiterer Test war überflüssig.

In diesem Zusammenhang ließen wir es uns nicht nehmen, Hinweise zur Durchführung von Drogentests im Allgemeinen zu geben: Sie sind

nur zulässig, wenn Beschäftigte hierzu schriftlich wirksam eingewilligt haben. Der Test muss darauf gerichtet sein, eine Alkohol- oder Drogenabhängigkeit nachzuweisen. Es darf nicht lediglich darum gehen, den Alkohol- oder Drogenkonsum zu ermitteln. Nichts anderes macht aber ein THC-Schnelltest. Er trifft keinerlei Aussage über die physische oder psychische Verfassung des Betroffenen, die eine Drogenabhängigkeit belegen könnte. Noch wichtiger: Ein solcher Test muss erforderlich sein, um die Eignung des Arbeitnehmers für die konkret vorgesehene Tätigkeit festzustellen. Arbeitsplatzrelevantes Verhalten liegt allerdings nur vor, wenn der Mitarbeiter durch ein abhängigkeitsbedingtes Fehlverhalten sich selbst, Leben und Gesundheit Dritter oder bedeutende Sachwerte des Arbeitgebers gefährden könnte. Ob der Drogenkonsum strafbar wäre oder nicht, ist nicht die Sache des Arbeitgebers. Dem Arbeitgeber darf zudem nur das Ergebnis der Eignungsuntersuchung vom untersuchenden Arzt mitgeteilt werden, nicht eine nähere Diagnose oder einzelne Gesundheitszustände.

Die Einwilligung des Beschäftigten kann nur dann als Rechtsgrundlage für die Verwendung seiner Daten dienen, wenn die hohen gesetzlichen Anforderungen – Transparenz, Freiwilligkeit, Schriftform – eingehalten werden. Das Argument der Zwangslage und Unfreiwilligkeit kann der Arbeitgeber relativieren, indem er die Einwilligung an die Gewährung rechtlicher Vorteile knüpft, auf die der Betroffene sonst keinen Anspruch hätte.

10. Wirtschaft

10.1 Datenschutz bei Unternehmens-Newslettern – ein Kontrollbericht

Newsletter sind heute für Unternehmen ein oft genutztes Werbemittel, weil sie wenig finanziellen und zeitlichen Aufwand auf Unternehmensseite erfordern, dennoch einen großen Empfängerkreis erreichen und die Bindung an das Unternehmen fördern. Da sich die Interessierten selbst in den Newsletter eintragen, besteht auch keine Notwendigkeit der E-Mail-Adressen-Beschaffung (Kauf oder Miete). Auch wenn es sich anhört, als handle es sich hier um eine Kleinigkeit, muss doch aus datenschutzrechtlicher Sicht einiges beachtet werden. Schon im vorletzten Tätigkeitsbericht (siehe 31. Tätigkeitsbericht 2012/2013, LT-Drs. 15/4600, Kapitel 10.2, S. 131 ff.) habe ich mich mit dem Double-Opt-In-Verfahren beim Abonnieren von Newslettern befasst; im letzten Tätigkeitsbericht (siehe 32. Tätigkeitsbericht 2014/2015, LT-Drs. 15/7990, S. 151 ff.) ging es um die rechtliche Situation und die Formalien. In diesem Jahr nun wurde bei verschiedenen Unternehmen in Baden-Württemberg kontrolliert, wie die Newsletter-Praxis tatsächlich aussieht.

Der Begriff „Newsletter" ist im heutigen Sprachgebrauch – aber auch im wirtschaftlichen und gesellschaftlichen Leben – nicht mehr wegzudenken. Aber was ist unter diesem Begriff zu verstehen? Ein Newsletter ist eine periodisch versendete E-Mail, die zielgruppenspezifische Informationen enthält. Bei den Informationen handelt es sich um Neuigkeiten aus einem Unternehmen (oder Verein, Stiftung, Initiative usw.), um neue Produkte oder Dienstleistungen; aber auch über anstehende und gewesene Veranstaltungen wird berichtet.

Wie gehen speziell Unternehmen vor, wenn sie auf ihrer Internetseite die Möglichkeit anbieten, ihren Newsletter zu abonnieren? Werden dabei alle rechtlichen Vorgaben beachtet? Für diese Kontrolle wurde eine Auswahl von Unternehmen über alle Branchen hinweg getroffen. Es wurden die Newsletter von weltweit agierenden Unternehmen kontrolliert, aber auch die von mittleren und kleinen Unternehmen. Insgesamt deckten die 22 geprüften Unternehmen ein breites wirtschaftliches Spektrum ab.

Um überprüfen zu können, ob bei dem Abonnement von Newslettern alle insbesondere datenschutzrechtlichen Voraussetzungen erfüllt werden, wurde bei unserer Kontrolle der folgende **Fragenkatalog** zugrunde gelegt:

1. Verschlüsselung: Wird die Newsletter-Anmelde-Internetseite per https übertragen?
2. Wird klar und eindeutig beschrieben, wer verantwortliche Stelle ist (z.B. Abgrenzung Mutter-/Tochterkonzern) und um welchen Inhalt/welche Inhalte es bei dem Newsletter geht?
3. Wird bei der Anmeldung darauf hingewiesen, dass der Betroffene dem Newsletter-Bezug jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen (§ 7 Absatz 3 Nr. 4 UWG)?
4. Welche Daten werden als Pflichtfelder abgefragt (z.B. E-Mail-Adresse, PLZ, Wohnort, Straße und Hausnummer, Vor- und Nachname usw.)?
5. Wird die Anmeldung durch ein Double-Opt-in-Verfahren vollzogen?
6. Wenn ja: Ist die Bestätigungs-E-Mail frei von jeglicher Werbung?
7. Welche weiteren Daten werden bei der Anmeldung gespeichert (z.B. IP-Adresse, Datum/Uhrzeit)?
8. Wird der Newsletter in der Datenschutzerklärung vollständig beschrieben?
9. Wird in jedem Newsletter darauf hingewiesen, dass der Betroffene dem Newsletter-Bezug jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen (§ 7 Absatz 3 Nr. 4 UWG)?
10. Ist die Abbestellung jederzeit ohne Aufwand mit einem Klick möglich, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen (§ 7 Absatz 3 Nr. 4 UWG)?

Um das Ergebnis gleich vorwegzunehmen: Insgesamt machen die Unternehmen ihre Sache gar nicht schlecht. Positiv fiel auf, dass die Übertragung der Newsletter-Anmelde-Internetseite immerhin bei mehr als Dreiviertel aller Unternehmen verschlüsselt erfolgte, alle Unternehmen mit dem Double-Opt-In-Verfahren arbeiten und die Abmeldung vom Newsletter stets funktioniert hat.

Doch jetzt zu den Ergebnissen der einzelnen Fragen:

1. Verschlüsselung: Wird die Newsletter-Anmelde-Internetseite per https übertragen?

Positiv zu vermerken ist, dass 18 Anbieter diese Internetseite verschlüsselt übertragen. Die verbliebenen vier Anbieter sollten bedenken, dass nicht nur die E-Mail-Adresse ein personenbezogenes Datum ist, sondern sie teilweise auch Name und Vorname oder noch mehr wissen möchten. Nach § 9 BDSG haben sie bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten diejenigen technischen und organisatorischen Maßnahmen zu treffen, die notwendig sind, um die Ausführung der Vorschriften des Bundesdatenschutzgesetzes zu gewährleisten. Die Anlage zu § 9 BDSG führt hierzu aus, dass eine der Maßnahmen insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren darstellt. Dieser Anforderung kommen sie ohne Verschlüsselung nicht nach.

2. Wird klar und eindeutig beschrieben, wer verantwortliche Stelle ist (z.B. Abgrenzung Mutter-/Tochterkonzern) und um welchen Inhalt/welche Inhalte es bei dem Newsletter geht?

War die verantwortliche Stelle – wenn auch nicht wie im Impressum mit Anschrift und Verantwortlichem – stets erkennbar, so war die Angabe der Inhalte des jeweiligen Newsletters sehr breit gestreut.

Dass man sich „seinen" Newsletter durch eine individuelle Themenauswahl zusammenstellen konnte, ist auf den ersten Blick sehr kundenfreundlich. Beim zweiten Blick stellt sich dann aber die Frage nach der möglichen Profilbildung. So kommen teilweise Tracking-Programme zum Einsatz, die festhalten, wer auf welches Angebot im Newsletter klickt – das persönliche Profil ist dann gleich erstellt. Auch die Markt- und Meinungsforschung freut sich über solche Informationen. Das Unternehmen als verantwortliche Stelle muss daher gemäß § 15 Absatz 3 i.V.m. § 13 Absatz 3 Nummer 6 des Telemediengesetzes sicherstellen, dass eine Verbindung vom Kunden zum Nutzungsprofil nicht hergestellt werden kann, dieses also pseudonym bleibt. Kommt es dieser Pflicht nicht nach, so handelt es sich um ein personalisiertes Nutzungsprofil. Mit dem Bezug des Newsletters kann nicht gleichzeitig eine Einwilligung in ein personalisiertes Nutzungsprofil eingefordert werden; es fehlt an der Freiwilligkeit, die Einwilligung wäre damit unwirksam.

Ein Negativbeispiel gerade zur Erstellung von Nutzerprofilen bot ein Unternehmen: Nach der Beschreibung der Inhalte des Newsletters folgte eine zweite Seite, auf der Themen für den Newsletter ausgesucht werden konnten. Und im dritten Schritt wurde dann nach persönlichen Angaben wie bspw. vollständiger Adresse, Telefonnummer, Geburtsdatum sowie aktueller Fahrzeugmarke und -modell gefragt. Ohne das Ausfüllen dieser Angaben war die Anmeldung zum Newsletter nicht möglich. Hier geht das Unternehmen unter dem Gesichtspunkt der Datenvermeidung und Datensparsamkeit eindeutig zu weit! Bei einem solchen Vorgehen geht es eindeutig nicht mehr um die Anmeldung zu einem Newsletter, sondern ganz lapidar um die Erstellung von Nutzerprofilen. Diese Angaben sind für Beratungszwecke und Kontaktaufnahmen gut geeignet, ggf. auch für die Anforderung von Informationsmaterial, mit Newslettern haben sie dagegen nichts mehr zu tun.

3. Wird bei der Anmeldung darauf hingewiesen, dass der Betroffene dem Newsletter-Bezug jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen (§ 7 Absatz 3 Nr. 4 UWG)?

Der Hinweis auf die jederzeitige Widerspruchsmöglichkeit fehlt bei vielen Unternehmen. Gleichzeitig wird im Regelfall auf die Datenschutzerklärung hingewiesen, in der dann auf das jederzeit geltende Widerspruchsrecht hingewiesen wird. Solange der Hinweis wenigstens in der Datenschutzerklärung erfolgt und ihre Kenntnisnahme durch ein Opt-In, also ein aktives Anklicken, bestätigt werden muss, mag es noch angehen. Kritisch wird das Ganze, wenn die Datenschutzerklärung unvollständig ist oder womöglich ganz fehlt. Hier müssen die betreffenden Unternehmen noch nachbessern.

Die etwas umständlich klingende Formulierung „ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen" mag einen heutzutage mit den schon fast selbstverständlich gewordenen Flatrates etwas althergebracht anmuten, man sollte jedoch keineswegs vergessen, dass nicht jeder jederzeit einen kostenfreien Zugang zum Internet zur Verfügung hat. Wenn dann Kosten ent-

stehen, so sollten diese nicht höher ausfallen als bei der sonstigen Nutzung. Insbesondere dürfen die Unternehmen die Kündigung eines Newsletters nicht etwa durch die Notwendigkeit eines Kündigungsbriefes oder der Nutzung einer Sonder-Telefax-Nummer nicht mit zusätzlichen Gebühren o.Ä. belasten. Dieser Hinweis erschien bei 21 Unternehmen nicht.

Immerhin: Dass der Hinweis auf den jederzeit möglichen Widerspruch und der Kostenhinweis im Verlauf der Newsletter-Bestellung untergebracht werden können, hat ein Unternehmen mit Hilfe einer Fußnote gezeigt.

4. Welche Daten werden als Pflichtfelder abgefragt (z.B. E-Mail-Adresse, PLZ, Wohnort, Straße und Hausnummer, Vor- und Nachname usw.)?

Die Bandbreite war enorm: Sie reichte von der alleinigen Angabe der E-Mail-Adresse bis zur vollständigen Anschrift samt Geburtsdatum und Telefonnummer. Auch die Angabe des Arbeitgebers, also der Firma, in der der Interessent arbeitet, wurde einige Male als Pflichtfeld gefordert. Als Begründung erscheint u.U., dass die Newsletter-Abonnenten persönlich angesprochen werden sollen, was ohne Anrede und Nachname nicht möglich sei. Eine solche Begründung mag nachvollziehbar sein. Bei der Angabe von vollständigen Anschriften ist dann aber endgültig Schluss. Die Unternehmen sollten sich das Prinzip der Datenvermeidung und Datensparsamkeit (§ 3a BDSG) ins Gedächtnis rufen. Für den Versand eines Newsletters reicht die E-Mail-Adresse vollständig aus!

Quasi den Vogel abgeschossen hat ein Unternehmen, das außer den Pflichtfeldern wie Vor- und Nachname, Land, Anschrift etc. noch eine Einwilligung in die „erweiterte Nutzung" dieser Daten haben möchte, ohne zu erklären, was es genau damit meint, oder ein anderes Unternehmen, das einen bevorzugten Kommunikationskanal (telefonisch, per Mail oder per Brief) erfragt – womöglich ohne vorher nach der postalischen Anschrift in einem Pflichtfeld gefragt zu haben.

5. Wird die Anmeldung durch ein Double-Opt-in-Verfahren vollzogen?

Die Antwort auf diese Frage kann für alle Unternehmen gleich beantwortet werden: Alle nutzen das Double-Opt-In-Verfahren. Damit ist zumindest einmal die Frage der eindeutigen Einwilligung in den Erhalt des Newsletters beantwortet.

6. Wenn ja: Ist die Bestätigungs-E-Mail frei von jeglicher Werbung?

Ja, eine Werbung im landläufigen Sinne war in den E-Mails mit dem anzuklickenden Bestätigungslink nicht zu finden, dafür allerdings meistens die Links zu den jeweiligen Auftritten in den sozialen Netzwerken wie bspw. Facebook.
Nach dem Anklicken des Links wurde man bei einem Unternehmen auf eine Seite geleitet, die weitere Informationen erfragte. Solange dies aber freiwillige Angaben sind, die nicht mit dem Bezug des Newsletter gekoppelt sind, kann dies als hinnehmbar betrachtet werden.

7. Welche weiteren Daten werden bei der Anmeldung gespeichert (z.B. IP-Adresse, Datum/Uhrzeit)?

Naturgemäß werden bei der Anmeldung, die auf einer Internet-Seite des Unternehmens erfolgt, genau die gleichen Daten gespeichert wie beim Besuch anderer Seiten dieses Unternehmens. Diese Bandbreite reicht dann von der Abfrage des Referrers, des Betriebssystems oder des Browers bis zum Zugriffsstatus und auch weiter bis zur Speicherung der IP-Adresse – die Liste ließe sich beliebig ausweiten. Die manchmal ausführlichen, manchmal etwas zurückhaltenderen Angaben finden sich alle in den Datenschutzerklärungen wieder.

8. Wird der Newsletter in der Datenschutzerklärung vollständig beschrieben?

Die Antwort auf diese Frage fällt durchwachsen aus: Einige Datenschutzerklärungen enthalten eine vollständige Beschreibung des Newsletters, einige beschreiben ihn unvollständig, etliche erwähnen, dass es einen Newsletter gibt, verzichten aber auf weitere Informationen und dann gibt es noch Datenschutzerklärungen, in denen der Newsletter offenbar unter den Tisch fällt.
Gemäß § 13 Absatz 1 des Telemediengesetzes muss ein Anbieter – hier das Unternehmen – den Nutzer unterrichten, wenn und wie er dessen Daten erhebt, verarbeite oder nutzt, sofern eine solche Unterrichtung nicht bereits erfolgt ist.
Die vollständige Beschreibung des Newsletters in der Datenschutzerklärung ist folglich

ein Pflichtbestandteil, denn zu seinem Versand bzw. bei seiner Bestellung werden unterschiedliche personenbezogene Daten erhoben, verarbeitet und genutzt.

9. Wird in jedem Newsletter darauf hingewiesen, dass der Betroffene dem Newsletter-Bezug jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen (§ 7 Absatz 3 Nr. 4 UWG)?

Vollständig lautet der Hinweis auf die Übermittlungskosten:

„§ 7 Unzumutbare Belästigungen
…
(3) Abweichend von Absatz 2 Nummer 3 ist eine unzumutbare Belästigung bei einer Werbung unter Verwendung elektronischer Post nicht anzunehmen, wenn
…
4. der Kunde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen."

Die Formulierung „ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen" findet sich nur in zwei Newslettern. Einige verwenden das Adjektiv „kostenlos" oder „kostenfrei", mindestens die Hälfte lässt diesen Hinweis dagegen ganz unter den Tisch fallen.

Die Tatsache, dass es sich hier um eine Vorschrift des Gesetzes gegen den unlauteren Wettbewerb geht und daher kein Tatbestand für eine Ordnungswidrigkeit nach dem Bundesdatenschutzgesetz vorliegt, verhindert freilich nicht, dass keine Folgen eintreten. Verbraucherverbände haben nach dem Unterlassungsklagegesetz das Recht, hiergegen vorzugehen. Ich behalte mir im Rahmen der konkreten Einzelfallbearbeitung, die jedenfalls in diesen Fällen unvermeidlich ist, vor, die Verbraucherverbände zu informieren.

Ein Newsletter weist darauf hin, dass trotz Abbestellung aus technischen Gründen in einem Zeitraum von drei Tagen noch ein Newsletter versandt werden könnte. Dieser Hinweis ist für die Abonnenten besonders hilfreich, denn mich erreichen immer wieder Beschwerden, weil trotz Abbestellung kurz darauf noch Newsletter beim ehemaligen Abonnenten eingehen. Um dies nachvollziehen zu können, muss man wissen, dass der Versand jeder Information, jedes Werbemittels einen gewissen zeitlichen Vorlauf benötigt: zum einen werden solche Aktionen häufig von Externen wie bspw. Werbeagenturen organisiert und mit Inhalten gefüllt, der tatsächliche Versand an eine bestimmte Kategorie von Empfängern danach von einem Dienstleister durchgeführt. Durch die Einbindung verschiedener Externer wird schon zur Weitergabe der für den Versand notwendigen Informationen Zeit benötigt. Drei Tage erscheinen mir hier nicht zu viel; länger sollte es aber auch nicht dauern.

Immerhin ist in jedem Newsletter der Link zur Abmeldung zu finden.

10. Ist die Abbestellung jederzeit ohne Aufwand mit einem Klick möglich, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen (§ 7 Absatz 3 Nr. 4 UWG)?

Diese Frage geht von der reinen theoretischen Möglichkeit der Abbestellung des Newsletters aus Frage 9 in die Praxis über. Es zeigte sich, dass bei tatsächlich allen Unternehmen die Abbestellung ohne weitere Kosten möglich ist. Viele weisen auch in ihrer Datenschutzerklärung darauf hin, dass die Abmeldung kostenfrei möglich sei, was sich bestätigt hat.

Bei manchen Unternehmen wird man nach Anklicken des Abmelde-Links auf eine weitere Seite geleitet, in der man durch die Angabe der eigenen E-Mail-Adresse die Abmeldung bestätigen soll. Sofern hier keine Umfrage zur Kundenzufriedenheit bzw. nach den Abmeldegründen erfolgt und keine Werbung enthalten ist, ist gegen eine solche Seite zwar rechtlich nichts einzuwenden. Wenn aber schon die E-Mail-Adresse gefordert wird, sollte sie nach dem Anklicken des Abmeldelinks im Newsletter automatisch eingetragen werden.
Nach der Abmeldung versandte ein Unternehmen noch eine Bestätigung der Abmeldung. Sofern diese Bestätigung ohne Werbung und ohne Umfrage zu den Gründen der Abmeldung auskommt, ist gegen sie nichts einzuwenden. Ohne eine Bestätigung wartet man doch immer, ob die Abmeldung tatsächlich beim Unternehmen angekommen ist und auch wirklich kein Newsletter mehr kommt.

Sonstige Feststellungen

Bei meiner Kontrolle fielen mir drei weitere Punkte auf, mit denen ich eher nicht gerechnet hätte:

1. Ein Kundenkonto anlegen - warum?
Einige Unternehmen setzen vor die Bestellung eines Newsletters das Anlegen eines Kundenkontos. Die dazugehörigen Gründe sind mir nicht ersichtlich. Wenn man ein Kundenkonto anlegt, müssen regelmäßig mehr Daten angegeben werden, als beim Bezug eines Newsletters erforderlich sind. Hierzu gehören bspw. Vor- und Nachname und (Liefer-/Rechnungs-) Anschrift. Die Abfrage des Geburtsdatums ist zwar erst erforderlich, wenn das Unternehmen eine Bonitätsabfrage aufgrund der entsprechend ausgewählten Zahlungsweise (z.B. Ratenkauf, Kauf auf Rechnung) beabsichtigt, wird jedoch häufig auch beim Anlegen des Kontos erledigt. Es stellt sich auch die Frage, was mit den Daten passiert, wenn man den Newsletter abbestellt. Wird das Kundenkonto automatisch gelöscht? Muss man dies selber machen, nachdem der Newsletter abbestellt wurde?

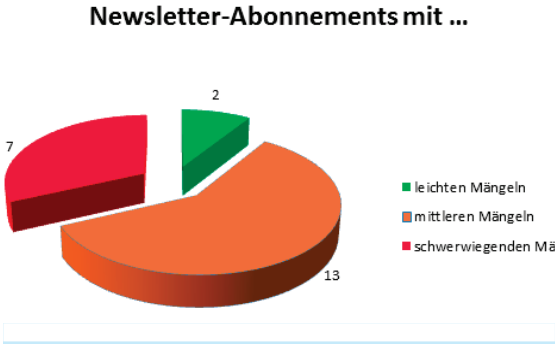
Die beiden betreffenden Unternehmen werden sich noch genau äußern müssen, warum sie das Kundenkonto – denn um nichts anderes handelt es sich – zwingend mit dem Bezug ihres Newsletters koppeln. Ich halte dies für überflüssig, nicht erforderlich und daher mit dem Datenschutz für nicht vereinbar.
Ein anderes Unternehmen verlangte das Anlegen eines Kontos speziell für den Bezug des Newsletters. Die Angabe eines Passwortes wurde gefordert, als Benutzername wurde die E-Mail-Adresse verwendet. Das Konto sollte zur Verwaltung des Newsletters eingesetzt werden: Auswahl und ggf. Änderung der Interessensgebiete, sodass der Newsletter Informationen nur dazu und nicht zu anderen Themen enthält sowie zur Abbestellung des Newsletters. Die Abbestellung konnte, wie sonst auch, im Newsletter selber durch einen Abmeldelink erledigt werden. Warum dann diese zwei Möglichkeiten zur Abmeldung? Immerhin: Nach der Abmeldung über den Link war das Konto tatsächlich gelöscht wie ein Versuch gezeigt hat.

Unternehmen sollten generell von der mit der Bestellung eines Newsletters gekoppelten Anlage eines Kundenkontos absehen, da hier viel mehr Daten erhoben, verarbeitet und genutzt werden, als zum reinen Bezug eines Newsletter erforderlich sind und damit der Grundsatz der Datenvermeidung und der Datensparsamkeit (§ 3a BDSG) verletzt wird. Zudem geht die Reichweite eines Kundenkontos weit über einen klassischen Newsletter hinaus. Allenfalls zur Interessensauswahl ist ein reines „Newsletter-Konto" denkbar.

2. Bestätigungs-Mail nicht angeklickt?
Was geschieht, wenn man nach Bestellung eines Newsletters den Link in der Bestätigungsmail nicht anklickt? Ein Unternehmen sandte nach ca. einer Woche eine Nachfrage per Mail. Sie enthielt den Text der ersten Bestätigungsmail und dazu die Bitte, den Link doch anzuklicken. Weitere Nachfragen gingen nicht ein.
Ein Hinweis des Unternehmens auf die Nachfrage war weder bei der Bestellung des Newsletters noch in der ersten Bestätigungsmail, noch in der Datenschutzerklärung oder sonst wo zu finden. Ich bin schon gespannt, was das Unternehmen dazu zu sagen hat.

3. Abmelden vom Newsletter - bei wem war ich noch mal angemeldet?
Ein Unternehmen hat es besonders „geschickt" gemacht: Mit der Bestellung seines Newsletters ist automatisch die Bestellung von zwei weiteren, anders benannten Newslettern dieses Unternehmens verbunden. Bei der Anmeldung erscheint kein Hinweis, erst bei der Abmeldung.
Diese Vorgehensweise ist mit der Rechtslage nicht vereinbar. Das Unternehmen wird hier einiges zu erklären haben.

Mein Fazit aus diesen Kontrollen:
Unternehmen gehen sehr unterschiedlich vor, wenn sie über ihre Homepage die Bestellung von Newslettern anbieten. Erstaunt hat mich vor allem, dass die größten Unternehmen, darunter sog. Global Players, auch zu denen gehören, die grundsätzliche Fehler gemacht haben. Ein Schaubild zeigt eine Verteilung unter Berücksichtigung der Mängel:



Alle Unternehmen, die in die Kontrolle einbezogen worden waren, erhalten von mir ein Feedback. Bei Problemen werde ich das datenschutzrechtliche Kontrollverfahren eröffnen müssen. Nur so kann erreicht werden, dass die betroffenen Unternehmen von ihren Fehlern erfahren und für ihren individuellen Fall umsetzbare und angemessene, rechtskonforme Lösungen entwickeln können. Es freut mich, dass das Feedback für einige Unternehmen gut ausfallen wird; auch ein Lob – und sei es für die Erfüllung nur der meisten (wenn auch nicht aller) Anforderungen meines Fragenkatalogs – darf es geben.

10.2 Teilnahme an Onlinegewinnspielen nur mit Pflicht-Einwilligung in Werbung?

Muss ich der Übersendung von Werbung zustimmen, um an einem Gewinnspiel im Internet teilnehmen zu können? Darf der Gewinnspielveranstalter diese in der Regel höchst umfangreiche Werbeeinwilligung einfach so vom Teilnehmer abpressen? Oder kann ich mich auch ohne „Gegenleistung" an einem Gewinnspiel beteiligen? Immer wieder führt diese Frage zu Unstimmigkeiten nicht nur bei den Teilnehmern der Gewinnspiele, sondern auch bei den Gewinnspielveranstaltern.

Online-Gewinnspiele sind beliebt. Beliebt bei den Teilnehmerinnen und Teilnehmern. Beliebt aber auch in der Werbe- und Adresshandelsbranche, da durch die erzwungenen Einwilligungen in Werbung – und es geht nicht um die schlichte Postwerbung, sondern um Werbung per E-Mail und Telefon – jedes Jahr Millionen von Adressen mit „sicheren Opt-ins" generiert werden können. Auch die großen Player auf dem Markt bedienen sich solcher Adressen.

Aus dem öffentlich-rechtlichen Vertragsrecht (§ 56 VwVfG) kennen wir das sog. Koppelungsverbot. Dieses Kopplungsverbot besagt, dass eine vertragliche Leistung nicht von einer artfremden Gegenleistung abhängig gemacht werden darf – andernfalls ist dieser Vertrag nichtig.

Eine entsprechende Regelung findet sich in § 28 Absatz 3b des Bundesdatenschutzgesetzes (BDSG). Dieser lautet:

„Die verantwortliche Stelle darf den Abschluss eines Vertrags nicht von einer Einwilligung des Betroffenen nach Absatz 3 Satz 1 abhängig machen, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Eine unter solchen Umständen erteilte Einwilligung ist unwirksam."

Auf Basis dieser Regelung könnte der Veranstalter eines Gewinnspiels zu dem Ergebnis gelangen, dass er sich mit der Thematik des Koppelungsverbotes gemäß § 28 Absatz 3b BDSG nicht auseinandersetzen muss, da er im Rahmen eines Gewinnspiels keine Leistungen anbietet, die auf eine Monopolstellung zurückzuführen wären. Er wird also argumentieren, dass der Betroffene frei entscheiden könne, ob er sich an dem jeweiligen Gewinnspiel beteiligen möchte – oder eben nicht. Diesem Gedankengang folgend sei die Einwilligung des Teilnehmers durchaus als freiwillige Einwilligung im Sinne von § 4a Absatz 1 BDSG zu werten und die Kopplung der Leistung Gewinnspielteilnahme im Tausch gegen die Einwilligung in Werbung daher zulässig.

Dieser Auffassung kann ich mich jedoch nicht anschließen.

Bei der Auslegung des § 28 Absatz 3b BDSG ist auch die Gesetzesbegründung (BT-Drucksache 16/12011, S. 33) heranzuziehen. Diese macht deutlich, dass sich das Koppelungsverbot insbesondere auf Unternehmen mit marktbeherrschender Stellung oder gar Monopolstellung bezieht. Auch geht es um Verträge, die auf einer Leistung mit entsprechender Gegenleistung basieren. In der Regel sind darunter Warengeschäfte und/oder Dienstleistungen gegen Geld zu verstehen. In der Begründung ist zu lesen:

„Erfasst werden soll auf diese Weise die Konstellation, dass die marktbeteiligten Unternehmen für sich genommen jeweils keine marktbeherrschende Stellung besitzen und dem Betroffenen daher ein Zugang zu gleichwertigen vertraglichen Leistungen an sich in zumutbarer Weise möglich ist, z.B. durch Absprachen unter den marktbeteiligten Unternehmen, aber marktweit immer nur, wenn er seine Einwilligung erteilt. Umgekehrt formuliert: Ein Zugang ist nicht in zumutbarer Weise möglich, wenn er nur mit Einwilligung nach Absatz 3 Satz 1 möglich ist."

Dem Schutzzweck der Regelung des § 28 Absatz 3b BDSG folgend, können Gewinnspiele

hierbei nicht eingeschlossen sein, da es sich dabei fast nie um einen Vertrag über Produkte oder Dienstleistungen gegen Geld handelt. Ganz im Gegenteil: Zumeist handelt es sich bei Gewinnspielen um kostenfreie Verlosungen im Sinne des § 661 des Bürgerlichen Gesetzbuches (BGB). Bei dieser Form des Gewinnspiels ist keine „echte" Gegenleistung des Teilnehmers erforderlich.

§ 28 Absatz 3b BDSG ist daher auf Online-Gewinnspiele gar nicht anwendbar. Maßstab für die Beantwortung der eingangs gestellten Fragen „Muss ich der Übersendung von Werbung zustimmen, um an einem Gewinnspiel teilnehmen zu können?" und „Oder kann ich mich auch ohne „Gegenleistung" an einem Gewinnspiel beteiligen?" muss daher allein § 4a Absatz 1 BDSG sein. Demzufolge muss die Einwilligung auf einer freien Entscheidung des Teilnehmers beruhen, also einer Entscheidung, die ohne Zwang oder äußeren Druck getroffen werden kann. Es muss dem Betroffenen möglich sein, selbst darüber zu entscheiden, ob und ggf. wie seine Daten erhoben, verarbeitet oder genutzt werden.

In den Fällen, in denen mit der Teilnahme an einem Gewinnspiel die Einwilligung zu Werbemaßnahmen erteilt werden muss, ist diese in § 4a Absatz 1 BDSG geforderte Freiwilligkeit also gerade nicht gegeben. In der Konsequenz ist daher diese erzwungene Einwilligung aus datenschutzrechtlicher Sicht unzulässig und damit rechtswidrig und der darauf basierende Vertrag von Anfang an nichtig.

Was wird sich im Hinblick auf die ab 25. Mai 2018 geltende Europäische Datenschutz-Grundverordnung (DS-GVO) in diesem Bereich ändern?

Artikel 7 Absatz 4 DS-GVO stellt insbesondere auf die Freiwilligkeit der Einwilligung ab.
„Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind."

Der Erwägungsgrund 43 der DS-GVO geht noch einen Schritt weiter und macht deutlich, wie schnell eine vermeintlich freiwillige Einwilligung unwirksam und damit von Anfang an nichtig werden kann.

„Die Einwilligung gilt nicht als freiwillig erteilt, […] wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist."

Für die Teilnahme und Durchführung eines Gewinnspiels ist die Einwilligung, künftig beworben zu werden, eindeutig nicht erforderlich. Es ist daher davon auszugehen, dass die im Zusammenhang mit einem Gewinnspiel geforderte Einwilligung in Werbemaßnahmen nicht als freiwillige Einwilligung zu werten ist. In der Konsequenz wäre diese Einwilligung aus datenschutzrechtlicher Sicht unzulässig und damit rechtswidrig und der darauf resultierende Vertrag von Anfang an nichtig.

Dieses aus Artikel 7 Absatz 4 DS-GVO resultierende Koppelungsverbot lässt sich nach unserer Auffassung auch nicht über Artikel 6 Absatz 1 lit. a DS-GVO entkoppeln. Diese Vorschrift regelt, dass eine Verarbeitung dann rechtmäßig ist, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten gegeben hat. So könnte das Koppelungsverbot durch eine Einwilligung sozusagen „entkoppelt" werden.

Dieser Gedanke greift vorliegend aber nicht: Nach Artikel 7 Absatz 4 DS-GVO in Verbindung mit Erwägungsgrund 43 handelt es sich bei einer Einwilligung, die erteilt werden muss, um eine gewünschte Leistung zu erhalten, diese Leistung jedoch auch ohne diese Einwilligung erbracht werden kann, nicht um eine freiwillige Einwilligung.

Schon heute halte ich die erzwungene Einwilligung in Werbung bei der Teilnahme an Online-Gewinnspielen für datenschutzwidrig, da eine Freiwilligkeit der Einwilligung nicht vorliegt und § 28 Absatz 3b BDSG in diesen Fällen nicht einschlägig ist. Die DS-GVO wird nun in diesem Sinne Rechtssicherheit schaffen: Eine der Hauptquellen für die Generierung von E-Mail-Adressen und Telefonnummern für Werbezwecke wird daher bald versiegen. Das ist eine gute Nachricht.

10.3 Ist in der (Online-)Reisebranche eine datenschutzkonforme digitale Kommunikation zwischen Reiseveranstalter und Kunden möglich?

Urlaubszeit, Reisezeit. Wo früher noch der Gang in das Reisebüro nötig war, wird heute vielfach online gebucht. Auf der Internetseite des Reiseanbieters werden alle Urlaubsdaten abgefragt und vom zukünftigen Reisegast eingegeben. Nach der erfolgreichen Buchung der Traumreise erhält der Kunde zunächst die Buchungsbestätigung zugesandt, später auch alle weiteren Reiseunterlagen, nur leider zumeist per unverschlüsselter E-Mail. So geschehen in einem Fall, der zur Beschwerde beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg geführt hat.

Problematisch wird es aus datenschutzrechtlicher Sicht immer dann, wenn Daten unverschlüsselt und damit ungeschützt durch das Netz geschickt werden. Neben den personenbezogenen Daten wie z.B. Name, Vorname, Adresse, Staatsangehörigkeit und Geburtsdatum werden oftmals auch sensible Daten wie beispielsweise die nach § 3 Absatz 9 BDSG besonders zu schützenden Gesundheitsdaten oder Angaben zu einer besonderen Art der Ernährung zwischen dem zukünftigen Reisenden und dem jeweiligen Reiseanbieter online ausgetauscht. Weitere Daten wie etwa das genaue Abreisedatum und die Reisedauer können, wenn sie in falsche Hände fallen, missbraucht werden. Es heißt nicht umsonst: Reisezeit ist Einbruchszeit.

Der technisch-organisatorische Schutz von personenbezogenen Daten ist in § 9 BDSG geregelt: Die verantwortlichen Stelle, hier also das Online-Reisebüro, muss die technischen und organisatorischen Maßnahmen treffen, die erforderlich und verhältnismäßig sind, um die jeweiligen datenschutzrechtlichen Anforderungen zu gewährleisten. Die Anlage zu § 9 BDSG führt hierzu aus, dass eine der Maßnahmen insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren darstellt.

Um den Missbrauch sensibler Daten zu verhindern, werden beispielsweise bei Banken und Versicherungen keine unverschlüsselten E-Mails an die Kunden versendet. Kontoauszüge und Versicherungsunterlagen werden stattdessen in einem über HTTPS gesicherten Dokumenten-Center zur Abholung durch den Nutzer hinterlegt oder per Ende-zu-Ende verschlüsselter E-Mail übermittelt.

Ein ähnliches Vorgehen haben wir im Rahmen der Beratung des Online-Reiseanbieters, gegen den sich die Beschwerde gerichtet hatte, empfohlen.

Der Reiseanbieter hat sich dazu bereit erklärt, in Zukunft ein per HTTPS gesichertes Dokumenten-Center auf seiner Internetseite bereit zu stellen. In diesem Dokumenten-Center sollen alle Reisebestätigungen, Reiseunterlagen und Rechnungen hinterlegt werden, die jederzeit vom Kunden – nach dem erfolgreichem Login, mit einem selbst generierten Passwort, heruntergeladen, ausgedruckt und gelesen werden können.

Mögliche Alternativvariante für einen Passwort-Login wäre beispielsweise eine Zwei-Faktoren-Authentifizierung. Diese Variante hat den Vorteil, dass der Kunde zusätzlich zu seiner Benachrichtigung über einen neuen Eingang im Dokumenten-Center über alle möglicherweise nicht legitimen Zugriffe auf sein Kundenkonto informiert werden könnte.

Mit dem Dokumenten-Center kann der Kunde zeit- und papiersparend auf Veränderungen reagieren. Unverschlüsselte E-Mails mit sensiblen personenbezogenen Daten sollten damit der Vergangenheit angehören.

Daneben soll natürlich auch der klassische Postweg zur Kommunikation zwischen Kunden und Reiseanbieter weiterhin offen stehen. Der Landebeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg wird sich anknüpfend an diesen Fall auch weiterhin für die Einhaltung der datenschutzrechtlichen Vorgaben in der Reisebranche einsetzen.

Eine sichere und datenschutzgemäße digitale Kommunikation kann durch gesicherte Dokumenten-Center auch ohne die Nutzung von E-Mail bedienungsfreundlich erfolgen. Damit die Reisezeit zur ungetrübten Erholungszeit wird!

10.4 Übermittlung von Kreditdaten durch Kreditgeber an Zahlungsdienstleister des Kreditnehmers

Der Kontoauszug ist inzwischen ein beliebtes Kommunikationsmittel für Mitteilungen der Bank an ihre Kunden geworden. Banken neigen daher bei der Formulierung des Verwendungszwecks ihrer Buchungen mitunter zu einer Ausführlichkeit, die die ohnehin hohe Datensensitivität des Kontoauszugs noch beträchtlich steigert. Auch hierbei muss jedoch der Datenschutz stets Beachtung finden.

Ein Bürger nahm bei seiner Hausbank einen Kredit auf. Die monatlichen Tilgungsraten wurden zunächst per Lastschrift von dem bei der Kreditgeberin geführten Girokonto abgebucht. Dabei gab die Bank auf dem Kontoauszug dieses Tilgungskontos im Verwendungszweck der Buchung den Darlehenszinssatz, den Zins- und Tilgungsanteil der Darlehensrate und den Restschuldbetrag an. Als der Kunde das Girokonto kündigte und die Bank nunmehr ermächtigte, die Tilgungsraten von einem anderen, bei der örtlichen Sparkasse geführten Girokonto abzubuchen, fuhr ihm bei der Lektüre des nächsten Kontoauszugs der Schreck in alle Glieder. Denn auch im Kontoauszug des Sparkassenkontos waren nun im Verwendungszweck dieselben Angaben zum Kreditgeschäft abgedruckt wie bisher. Kreditdaten, die einst ausschließlich zwischen der Kreditgeberin und dem Kunden kursiert waren, hatten nun aufgrund der elektronischen Standardeinstellungen der Kreditgeberin auch ihren Weg in die gewaltigen Datenspeicher der Sparkasse gefunden. Die Kreditgeberin war der Ansicht, der Kunde müsse auch nach dem Wechsel des Tilgungskontos mithilfe des Kontoauszugs über den aktuellen Stand des Kreditgeschäfts in gleicher Weise wie vorher unterrichtet werden.

Diese Vorgehensweise der Kreditgeberin stößt auf erhebliche datenschutzrechtliche Bedenken. Der Darlehenszinssatz, die Zusammensetzung der Darlehensrate und der Restschuldbetrag sind personenbezogene Daten des Kreditnehmers. Diese Daten werden mit der Aufnahme in den Verwendungszweck der Rateneinzugsbuchung an die kontoführende Sparkasse übermittelt. Zwar erhält die Sparkasse die Daten allein zu dem Zweck, sie ihrerseits an den betroffenen Inhaber des bei ihr geführten Girokontos weiterzugeben – und Zahlungsstromanalysen sind ohne Einwilligung des betroffenen Kunden unzulässig. Dies ändert aber nichts daran, dass die Daten mit ihrer Aufnahme in den Verwendungszweck auch dem neuen kontoführenden Kreditinstitut selbst (hier der Sparkasse) bekanntgegeben werden. Die Daten werden auf diese Weise, ebenso wie durch jede andere unnötige Weitergabe, Missbrauchs- und Vertraulichkeitsrisiken ausgesetzt. Die Datenweitergabe an die Sparkasse ist daher in Ermangelung einer Einwilligung des betroffenen Kunden nur zulässig, wenn sie zur Durchführung des Kreditvertrags erforderlich ist. Dies ist jedoch nicht der Fall. Insbesondere kann sich die Erforderlichkeit der Übermittlung nicht daraus ergeben, dass sie den Standardeinstellungen der bankseitigen IT-Systeme entspricht. Vielmehr ist bei der Konfigurierung elektronischer Zahlungsverkehrssysteme den Vorgaben des Datenschutzrechts Rechnung zu tragen.
Die kreditgebende Bank hat daher zugesagt bei Fremdeinzügen von Darlehensraten künftig auf die Übermittlung der Kreditdaten zu verzichten.

Kreditgeber sollten beim Lastschrifteinzug von Tilgungsraten von Konten anderer Kreditinstitute im Verwendungszweck keine Einzelheiten zum Darlehensgeschäft angeben.

10.5 Datenschutz hatte keine Konjunktur bei Konjunkturumfrage

Eine Handwerkskammer hatte ein Unternehmen beauftragt, Kammerzugehörige telefonisch zu befragen. Dabei ging es u.a. um die Beschäftigtenzahl, die Betriebsauslastung und den Auftragsbestand, jeweils einschließlich der bisherigen und voraussichtlichen Änderung, sowie um die bisherige und voraussichtliche Umsatzentwicklung.

Dazu baten wir die Kammer um Stellungnahme. Diese ließ wesentliche datenschutzrechtliche Fragen offen, etwa: Lag ein Auftrag zur Datenverarbeitung i.S.v. § 7 LDSG oder eine Funktionsübertragung vor? Für welche Zwecke durfte das befragende Unternehmen die Daten verwenden?

Deswegen besprach meine Dienststelle die Angelegenheit eingehend mit der Kammer. Diese überarbeitete daraufhin ihr Verfahren grundlegend. Gemäß den überarbeiteten Unterlagen, welche die Kammer uns vorgelegt hat, beauftragt sie nunmehr das befragende Unterneh-

men mit einer Datenverarbeitung i.S.v. § 7 LDSG (mit der Folge, dass ausschließlich die Kammer verantwortliche Stelle ist und – anders als bei einer Funktionsübertragung – nicht auch das befragende Unternehmen). Zudem ist nun u.a. im Vertrag zur Durchführung von Konjunktur- und Sonderumfragen zwischen der Kammer und dem befragenden Unternehmen diesem ein Verwenden der Daten für Zwecke außerhalb dieses Vertrags untersagt.

Eine Kammer, die ein Unternehmen beauftragt, Kammerzugehörige im Rahmen einer Konjunkturumfrage zu befragen, muss die Angelegenheit vorab umfassend datenschutzrechtlich prüfen und die Vereinbarungen mit dem befragenden Unternehmen klar und rechtskonform gestalten.

10.6 Internationaler Datentransfer

Verbindliche Unternehmensreglungen – erfolgreicher Abschluss des ersten europaweiten Abstimmungsverfahrens der baden-württembergischen Aufsichtsbehörde

Verbindliche Unternehmensregelungen (sog. Binding Corporate Rules, abgekürzt BCR) liegen im Trend. Immer mehr Konzerne und Unternehmensgruppen interessieren sich für dieses Instrument zur Erfüllung der Anforderungen an konzerninterne Übermittlungen personenbezogener Daten aus der EU und dem europäischen Wirtschaftsraum (EWR) in Drittstaaten. Im Berichtszeitraum waren und sind wir in mehrere BCR-Anerkennungsverfahren involviert und haben uns auf europäischer Ebene an der Weiterentwicklung der Anforderungen für BCR beteiligt.

Gemäß § 4c Absatz 2 BDSG können sich ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte Betroffener im Zusammenhang mit dem Transfer personenbezogener Daten in Drittstaaten unter anderem aus verbindlichen Unternehmensregelungen ergeben. Rund 90 Konzerne beziehungsweise Unternehmensgruppen haben inzwischen verbindliche Unternehmensregelungen eingeführt. Welche das sind, kann einer von der Artikel-29-Gruppe im Internet veröffentlichten Liste entnommen werden:

http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm

Da Konzerne heutzutage häufig nicht mehr nur in einem europäischen Mitgliedsstaat, sondern in der Regel in mehreren oder gar allen tätig sind, und das Bedürfnis nach einem koordinierten Vorgehen der einzelnen Datenschutzaufsichtsbehörden der europäischen Mitgliedstaaten daher in diesem Bereich besonders augenfällig ist, haben sich die europäischen Datenschutzaufsichtsbehörden bereits vor einigen Jahren auf ein europaweites Anerkennungsverfahren zur Prüfung von BCR mit einer federführenden Aufsichtsbehörde am Hauptsitz des Unternehmens in Europa geeinigt. Die Mehrzahl der europäischen Aufsichtsbehörden hat sich darüber hinaus verpflichtet, das Ergebnis der Prüfung durch die federführende Aufsichtsbehörde und zwei Co-prüfende Aufsichtsbehörden als für sich verbindlich anzuerkennen und auf eine eigene inhaltliche Prüfung der Unternehmensregelungen zu verzichten (sog. mutual recognition Verfahren). Auch die Frage, ob Abweichungen von den Standardvertragsklauseln der Europäischen Kommission so erheblich sind, dass ein auf die entsprechenden Vertragsklauseln gestützter Transfer einer gesonderten Genehmigung bedarf (sog. ad-hoc-Vertrag), kann seit 2014 in einem koordinierten Verfahren aller betroffener Aufsichtsbehörden, in dem diese unter der Leitung einer federführenden Behörde einen gemeinsamen Standpunkt erarbeiten, geprüft werden.

Der Landesbeauftragte hat im Berichtszeitraum als federführende Aufsichtsbehörde (lead authority) mehrere BCR-Anerkennungsverfahren geführt, von denen eines im Berichtszeitraum erfolgreich abgeschlossen werden konnte (Firma Festo, Esslingen). In einem weiteren Verfahren steht der Abschluss des Verfahrens unmittelbar bevor. Daneben haben wir auch als sog. Co-Prüfer an mehreren BCR-Anerkennungsverfahren mitgewirkt, welche von Datenschutzaufsichtsbehörden anderer EU-Mitgliedsstaaten (u.a. Großbritannien und den Niederlanden) federführend gestaltet wurden. Alle diese Verfahren betrafen BCR für Verantwortliche Stellen. Verfahren, bei denen es um BCR für Auftragsdatenverarbeiter geht, d.h. um solche BCR, die speziell für Unternehmensgruppen gedacht sind, die in erheblichem Umfang Dienste der Auftragsdatenverarbeitung für eine große Anzahl konzernfremder Auftraggeber anbieten, sind bei uns momentan noch nicht anhängig.

Die vorhandenen Regelungen zu verbindlichen Unternehmensregelungen (u.a. die Arbeitspa-

piere 204, 195, 155, 154, 153, 133, 108, 107 und 74 der Artikel-29-Gruppe) können nicht sämtliche denkbaren Fallgestaltungen abbilden und bedürfen daher der ständigen Überarbeitung und Ergänzung. Im Berichtszeitraum konnte beispielsweise geklärt werden, dass eine Übergangs- oder Einführungsfrist (sog. transition period), der zur Folge die Unternehmensgruppe ein oder zwei Jahre Zeit hat, um einzelne Forderungen der BCR umzusetzen, zur zwingenden Folge hat, dass ein Transfer personenbezogener Daten während dieser Übergangszeit nicht auf die BCR gestützt werden kann, sondern hierfür ein anderes Instrument erforderlich ist, zum Beispiel der Abschluss von Standardvertragsklauseln oder eine Einwilligung aller Betroffener.

Unterschiedliche Vorstellungen zwischen antragstellenden Unternehmen und Aufsichtsbehörden bestehen regelmäßig auch bezüglich der Zulässigkeit von Haftungsbeschränkungen, sei es in Form einer summenmäßigen Beschränkung der Haftung oder des Ausschlusses der Haftung für bestimmte Verschuldensformen (zum Beispiel einfache Fahrlässigkeit) oder bestimmte Schadensarten (zum Beispiel entgangenen Gewinn, Reputationsschäden oder jegliche Folgeschäden). Die Arbeitspapiere der Artikel-29-Gruppe äußern sich zur Zulässigkeit solcher Regelungen nicht ausdrücklich. Sie sehen vor, dass ein konzernangehöriges Unternehmen mit Sitz in der EU zugunsten aller Betroffenen die Haftung für Handlungen anderer Gruppenmitglieder außerhalb der EU übernimmt und die notwendigen Maßnahmen ergreift, um Verstößen gegen die BCR abzuhelfen und Ersatz für Schäden zu leisten, die aus einem Verstoß gegen die BCR durch ein Mitglied der Unternehmensgruppe entstanden sind. BCR sollen Betroffene nach einem Transfer ihrer Daten in einen Drittstaat so stellen, wie sie stünden, wenn ihre Daten im EWR beziehungsweise der EU verblieben wären und es dort zu einer etwaigen Datenschutzverletzung gekommen wäre. Da weder das geltende noch das künftige deutsche und europäische Datenschutzrecht (vgl. § 7 BDSG sowie Artikel 82 DS-GVO) Einschränkungen des Umfangs des zu ersetzenden Schadens über das jeweils anwendbare materielle Zivilrecht hinaus vorsehen, sind die genannten Haftungsbeschränkungen in BCR nicht möglich.

Die Abstimmung in den Anerkennungsverfahren über die BCR mit Aufsichtsbehörden anderer Mitgliedsstaaten hat nicht immer reibungslos funktioniert. Die langen Bearbeitungsfristen und die Schwierigkeit, überhaupt einen Co-Prüfer zu finden, mögen mit der hohen Arbeitsbelastung der jeweiligen Aufsichtsbehörde zu tun haben. Zudem war der enge Austausch mit Kollegen aus anderen Mitgliedsstaaten für die eine oder andere Aufsichtsbehörde sicherlich noch Neuland.

Ausblick: Was ändert sich durch die DS-GVO für BCR?
Die Datenschutz-Grundverordnung regelt BCR ausführlich in Artikel 47 DS-GVO. Durch den Verweis auf das Kohärenzverfahren werden künftig nicht nur die betroffenen sondern alle Aufsichtsbehörden in Europa in das Prüfungsverfahren einbezogen. BCR, für die das EU-weite Anerkennungsverfahren vor Mai 2018 abgeschlossen wurde, müssen danach inhaltlich an die neuen materiell-rechtlichen Vorgaben der Datenschutz-Grundverordnung angepasst werden. Eine Behandlung der Angelegenheit im Kohärenzverfahren wird hierfür aber regelmäßig nicht erforderlich sein. Vielmehr reicht es, wenn die Änderungen der BCR und der Anlagen dazu der federführenden Aufsichtsbehörde angezeigt werden. Daneben sollte die Unternehmensgruppe an alle nationalen Aufsichtsbehörden, die datenschutzaufsichtsbehördliche Genehmigungen einzelner Transfers auf der Grundlage der BCR erteilt haben, herantreten und fragen, ob eine Änderung der Genehmigung beziehungsweise die Erteilung einer neuen Genehmigung erforderlich ist. Die Arbeitspapiere der Artikel-29-Gruppe zu BCR werden derzeit überarbeitet, um sie an die Anforderungen der DS-GVO anzupassen.

11. Internet

11.1 Löschung von Ergebnissen aus Suchmaschinen (Recht auf „Vergessenwerden“)

Gemäß einem am 13. Mai 2014 ergangenen Urteil des Europäischen Gerichtshofs (Az. C-131/12) können Betroffene von Betreibern von Suchmaschinen verlangen, dass bestimmte Ergebnisse zu ihrem Namen aus den Suchergebnislisten entfernt werden. Nach Bekanntwerden dieses Urteils haben sich viele Betroffene mit dem Anliegen, entsprechende Suchergebnisse zu ihren Namen löschen zu lassen, an uns gewandt.

Voraussetzung für eine Löschung bestimmter Suchergebnisse ist, dass die Datenschutzrechte der Betroffenen schwerer wiegen als das Interesse an der Verfügbarkeit der betreffenden Suchergebnisse. Jedoch ist der Anspruch der Betroffenen auf die Entfernung von Links allein auf Suchanfragen anhand seines Namens beschränkt. Sonstige Suchanfragen, etwa zu thematischen Stichworten, sind von der Entscheidung nicht betroffen. Das heißt, dass in diesen Fällen sämtliche Links in den Suchergebnissen erscheinen dürfen – also auch zu den Internetseiten, die bei einer Suchanfrage zur Person nicht angezeigt werden dürften. Das Urteil begründet auch keine Verpflichtung, auf den verlinkten Internetseiten personenbezogene Daten des Betroffenen zu schwärzen oder gar zu löschen. Alleine das Suchergebnis, also die Verlinkung zu einer bestimmten Internetseite, ist zu entfernen.

Das Recht auf Vergessenwerden ist nunmehr auch in Art. 17 der Datenschutz-Grundverordnung (DS-GVO) geregelt. Mit Gültigkeit der DS-GVO ab dem 25. Mai 2018 ist das Recht auf Vergessenwerden somit europaweit kodifiziert. Nach Artikel 17 Absatz 1 DS-GVO sind personenbezogene Daten künftig unverzüglich zu löschen, wenn:

- Die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind
- Die betroffene Person ihre Einwilligung widerruft und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt
- Die betroffene Person Widerspruch gegen die Verarbeitung einlegt und keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen
- Die personenbezogenen Daten unrechtmäßig verarbeitet wurden
- Die Löschung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich ist
- Die personenbezogenen Daten eines Kindes wurden in Bezug auf angebotene Dienste der Informationsgesellschaft, d.h. Internetangebote, wie Medien, Webshops oder Online-Spiele, erhoben.

Dieser Anspruch ist unverzichtbar und kann durch Verhaltensregeln i.S. des Art. 40 DS-GVO nicht beschränkt werden. Allerdings muss die betroffene Person das Vorliegen dieser Voraussetzungen beweisen.

Außerdem gibt es nach Art. 17 Abs. 3 DS-GVO Ausnahmen von diesem Anspruch, nämlich

- wenn die Daten zur Ausübung des Rechts auf freie Meinungsäußerung und Information erforderlich sind;
- wenn die Angaben zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, benötigt werden, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit;
- für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke, oder
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Ein Recht auf Vergessenwerden besteht also nicht nach Belieben, sondern ist an bestimmte gesetzliche Voraussetzungen gebunden. Gerade in Fällen, in denen das allgemeine Persönlichkeitsrecht einerseits mit dem Recht auf freie Meinungsäußerung und Information andererseits kollidiert, hat durch den Suchmaschinenbetreiber eine umfassende Abwägung der widerstreitenden Interessen zu erfolgen.

In Reaktion auf das am 13. Mai 2014 ergangenen Urteil des Europäischen Gerichtshofs hat Google auf seiner Webseite ein Löschfor-

mular zur Verfügung gestellt, über das Betroffene eine entsprechende Löschung beantragen können (abrufbar unter https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=0-636294885147125291-4269928454&rd=1).

Wendet sich ein Betroffener mit der Bitte an uns, Ergebnisse zu seinem Namen aus der Suchmaschine Google löschen zu lassen, so verweisen wir den Betroffenen zunächst auf das von Google auf seiner Webseite zur Verfügung gestellte Löschformular. Außerdem verweisen wir die Betroffenen auf die für die jeweilige Suchmaschine zuständige Aufsichtsbehörde. Dies ist z.B. für Google der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit und für Bing das Bayerische Landesamt für Datenschutzaufsicht. Im Rahmen unserer aufsichtsrechtlichen Zuständigkeit können wir nur tätig werden, wenn die betreffende Suchmaschine ihren Sitz in Baden-Württemberg hat.

11.2 Unrechtmäßige Veröffentlichung von Privatinsolvenzen im Internet

Die Veröffentlichung von Insolvenzbekanntmachungen ist eigentlich Aufgabe der Amtsgerichte. In den vergangenen Monaten haben sich jedoch viele Betroffene an uns gewandt, die bei der Suche ihres Namens in gängigen Suchmaschinen Informationen über ihre Privatinsolvenz auf nicht-amtlichen Internetseiten gefunden haben. Teilweise handelt es sich um Daten aus Insolvenzverfahren, die bereits mehrere Jahre zurückliegen.

§ 9 Absatz 1 Satz 1 der Insolvenzordnung (InsO) erlaubt die öffentliche Bekanntmachung von Insolvenzdaten durch eine zentrale und länderübergreifende Veröffentlichung im Internet. Die Veröffentlichung findet auf der amtlichen Webseite www.insolvenzbekanntmachungen.de statt. Da jedermann diese Webseite ohne Eingabe eines Passwortes aufrufen und einsehen kann, sind die Insolvenzdaten während der Dauer der öffentlichen Bekanntmachung für jedermann frei zugänglich. Nach Ablauf von zwei Wochen können die Daten jedoch nur noch abgerufen werden, wenn die Abfrage neben dem Sitz des Insolvenzgerichts eine weitere Angabe i.S.d. § 2 Absatz 1 Satz 1 Nrn. 3 der Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet enthält. Dies bedeutet also, dass die Insolvenzdaten nur für einen Zeitraum von zwei Wochen öffentlich zugänglich sind.

Für die Veröffentlichung von Insolvenzdaten auf privaten Seiten gilt Folgendes: Zwar dürfen nach § 29 Absatz 1 Satz 1 Nr. 2 des Bundesdatenschutzgesetzes (BDSG) Daten aus allgemein zugänglichen Quellen erhoben und genutzt werden, jedoch ist dies nicht schrankenlos zulässig. Überwiegt das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verwendung der Daten das Interesse der verantwortlichen Stelle, so ist die Veröffentlichung unrechtmäßig. Einer Veröffentlichung von Privatinsolvenzdaten stehen regelmäßig die schutzwürdigen Interessen der betroffenen Personen entgegen. Denn die Veröffentlichung von Insolvenzdaten wirkt sich nicht nur negativ auf das allgemeine Ansehen des Betroffenen aus, sondern kann auch negative Folgen für seine Reputation haben. Die Veröffentlichung von Insolvenzdaten auf nicht-amtlichen Internetseiten sehen wir daher nach Ablauf von zwei Wochen ab der öffentlichen Bekanntmachung auf der amtlichen Webseite www.insolvenzbekanntmachungen.de als unrechtmäßig an.

Problematisch ist in den uns mitgeteilten Fällen jedoch, dass sämtliche Internetseiten aus dem nicht-europäischen Ausland betrieben wurden bzw. werden. Da sich die Zuständigkeit der datenschutzrechtlichen Aufsichtsbehörde grundsätzlich nach dem Sitzprinzip richtet, d.h., der Sitz der verantwortlichen Stelle maßgeblich für die Zuständigkeit einer Aufsichtsbehörde ist, können wir daher nicht gegen die Betreiber der Internetseiten vorgehen. Das wird sich jedoch mit der DS-GVO ändern, dann gilt das sog. Marktortprinzip und wir können auch gegen außereuropäische Anbieter vorgehen.

Wir können den Betroffenen daher derzeit nur raten, bei der entsprechenden Suchmaschine die Löschung des Links zu dem jeweiligen Eintrag zu beantragen. Dies führt zwar nicht zu einer Löschung der betreffenden Internetseite, jedoch wird die Internetseite in den Suchergebnissen nicht mehr angezeigt. Wird eine solche Löschung abgelehnt, so raten wir den Betroffenen, sich an die jeweils für den Betreiber der Suchmaschine zuständige Aufsichtsbehörde zu wenden. Dies ist z.B. für Google der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit und für Bing das Bayerische Landesamt für Datenschutzaufsicht.

11.3 Der richtige Umgang mit Spam- und Phishingmails

Fast jeder hat schon mal eine Spam- oder gar eine Phishingmail erhalten. Dies ist zwar sehr ärgerlich und lästig, jedoch aufgrund des großen Umfangs elektronischen Informationsaustausches im täglichen Leben leider nicht ganz zu vermeiden. Der Gefahr, Opfer von Spam- oder Phishingmails zu werden, kann jedoch entgegengetreten werden.

Als Spam werden unerwünschte Nachrichten bezeichnet, die dem Empfänger unverlangt zugestellt werden und häufig werbenden Inhalt enthalten. Beim Phishing hingegen werden gezielte Angriffe unternommen, um Passwörter des Opfers zu erlangen. Bei einer Phishingmail sollen Text und ggf. Bilder den Empfänger dazu verleiten, einen Anhang zu öffnen oder einen Link im Mailtext anzuklicken. Die Anhänge bestehen z.B. aus ZIP-Archiven mit ausführbaren Dateien oder aus speziell für Sicherheitslücken im Adobe Reader präparierten PDF-Dateien. Dagegen wird beim Anklicken eines Links möglicherweise eine präparierte Web-Seite im Browser geöffnet, um auf diesem Weg unbemerkt einen schädlichen Code in den PC des Opfers zu schleusen. Eine typische Phishing-Strategie ist auch, dass die verlinkte Seite das Design einer vertrauenswürdigen Seite nachahmt und den Betroffenen auf diese Weise zur Eingabe vertraulicher Daten bewegen will. Phishing ist daher als Form des Betruges einzustufen. In den uns gemeldeten Fällen von Phishing haben wir den Betroffenen daher geraten, sich an die zuständige Ermittlungsbehörde zu wenden und die Straftat zu melden. Nur die Ermittlungsbehörden – zu denen die Datenschutzaufsichtsbehörden nicht zählen – können unter Umständen den jeweiligen Inhaber einer E-Mail-Adresse ausfindig machen, von der aus die entsprechenden Nachrichten versendet werden. Bei Beschwerden wegen Spam- und Phishingmails müssen wir uns daher leider darauf beschränken, den Betroffenen allgemeine Hinweise zu geben:

Der sicherste Schutz gegen Spam- und Phishingmails ist zunächst ein verantwortungsvoller Umgang mit E-Mails und deren Anhängen. E-Mails unbekannter, aber auch bekannter Herkunft – auch wenn diese vielleicht auch auf den ersten Blick vertrauenerweckend sind – sollten mit großer Vorsicht behandelt werden. Unbekannte Anhänge sollten nicht geöffnet und unbekannten Links sollte nicht gefolgt werden. Auch wenn eine Nachricht möglicherweise neugierig macht, sollte sie trotzdem ungeöffnet direkt gelöscht werden. Dateianhänge sollten immer mit einer aktuellen Antivirensoftware geprüft werden.

Des Weiteren sollte die Weitergabe der eigenen E-Mail-Adresse an Dritte wohl überlegt sein und insbesondere nur an seriöse Geschäftspartner erfolgen. Wenn Nutzer auf einer Internetseite eine E-Mail-Adresse eingeben wollen (z.B. bei einem Internetkauf, zum Anfordern eines Newsletters oder um ein soziales Netzwerk zu nutzen), sollten in der Datenschutzerklärung dieser Seite die Passagen über die Weitergabe der E-Mail-Adresse an Dritte nachgelesen werden.

Zudem sollten sich Betroffene nicht gleich einschüchtern lassen. Gerade Phishingmails leben von einem gewissen psychologischen Moment, ohne dass die Unseriosität oft allzu offensichtlich wäre.

Vollständig ausschließen kann man die Gefahren von Spam- und Phishingmails leider nicht. Bei Beachtung vorgenannter Hinweise können die Gefahren, die von Spam- und Phishingmails ausgehen, jedoch erheblich reduziert werden.

11.4 Verantwortlichkeit von Diensteanbietern nach dem Telemediengesetz (TMG)

Häufig stolpert man in Datenschutzerklärungen von Webseiten, sozialen Netzwerken, Blogs und anderen Telemediendiensten über die Passage „Für fremde Inhalte haften wir nicht" oder „Für fremde Inhalte sind wir nicht verantwortlich". Dies ist so jedoch weder zutreffend noch kann auf diese Weise eine Haftung ausgeschlossen werden.

Telemediendienste sind elektronisch erbrachte Informations- und Kommunikationsdienste, mit denen Inhalte jeglicher Art bereitgestellt und die durch Telekommunikation übermittelt werden. Hierzu zählen neben sozialen Netzwerken u.a. Chat-Rooms, Websites und Blogs. Diensteanbieter ist nach § 2 Satz 1 Nr. 1 des Telemediengesetzes (TMG) jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt.

Als Diensteanbieter ist daher der jeweilige Betreiber der Website, des Chat-Rooms etc. nach den entsprechenden Vorschriften des Telemediengesetzes verantwortlich.

Grundsätzlich sind Diensteanbieter gemäß § 7 Absatz 1 TMG nur für eigene Informationen, die sie zur Nutzung bereithalten, verantwortlich. Aus § 10 TMG ergibt sich jedoch, dass Diensteanbieter dann für fremde Informationen, die sie für einen Nutzer speichern, verantwortlich sind, sofern sie Kenntnis von der rechtswidrigen Handlung oder Äußerung haben oder sie unverzüglich tätig geworden sind, um die Information zu entfernen oder den Zugang zu ihr zu sperren.

Fremd sind Informationen oder Äußerungen dann, wenn sie von Dritten eingestellt wurden und sich der Diensteanbieter diese Informationen nicht zu eigen macht. Von einem Zueigenmachen ist nach der Rechtsprechung des BGH aber nur dann auszugehen, wenn der Diensteanbieter nach außen erkennbar die inhaltliche Verantwortung für die auf seiner Internetseite veröffentlichten Inhalte übernommen hat.

Liegt also kein Zueigenmachen vor, so haftet der Diensteanbieter erst, sobald er Kenntnis von der Rechtsverletzung erlangt und nicht tätig wird. Kenntnis kann beispielsweise durch die Meldung eines anderen Nutzers erlangt werden oder wenn Kommentare, Forenbeiträge etc. vor der Veröffentlichung – etwa im Rahmen einer Vorabmoderation – geprüft werden. Je nach Inhalt der gemeldeten Information muss der Diensteanbieter zunächst einmal prüfen, ob tatsächlich ein Rechtsverstoß vorliegt. Unproblematisch wird dies nur in Fällen sein, in denen die Äußerung einen Straftatbestand – wie z.B. Beleidigung und üble Nachrede – erfüllt.

Schwieriger wird es jedoch, wenn die Verletzung von Persönlichkeitsrechten behauptet wird. Erfolgt hierbei ohne nähere Prüfung einfach eine Löschung der gemeldeten Äußerung, so kann das Grundrecht auf Meinungsfreiheit desjenigen, der die entsprechende Äußerung gemacht hat, sowie die Medienfreiheit des Diensteanbieters verletzt werden. In diesen Fällen muss vielmehr eine Abwägung zwischen dem allgemeinen Persönlichkeitsrecht einerseits und der Meinungs- bzw. Medienfreiheit andererseits stattfinden.

Erlangt ein Diensteanbieter Kenntnis von einer rechtswidrigen Handlung, so muss dieser prüfen, ob tatsächlich ein Verstoß vorliegt. Da diese Abwägung juristisch nicht geschulten Personen jedoch nicht ohne weiteres möglich sein wird, sollte der betreffende Inhalt zunächst von der Seite genommen und einem Rechtsanwalt zur Prüfung vorgelegt werden.

11.5 Illegales Filesharing

Das Problem des illegalen Filesharings besteht schon seit Jahren, ist aber nach wie vor aktuell. Uns erreichen immer wieder Anfragen von Betroffenen, die eine Abmahnung wegen illegalen Filesharings erhalten haben und nicht wissen, wie sie damit umgehen sollen.

Der Begriff Filesharing kommt aus dem Englischen und bedeutet wörtlich übersetzt „Dateien teilen". Unter Filesharing ist die direkte Weitergabe von Dateien zwischen Internetnutzern unter Verwendung eines Filesharing-Netzwerks zu verstehen. Eine Weitergabe erfolgt hierbei über sog. Tauschbörsen, bei denen vorwiegend Filme oder Musikdateien über spezielle Filesharing-Programme auf den eigenen Rechner heruntergeladen und anschließend über den eigenen Rechner anderen Nutzern zur Verfügung gestellt werden. Geschieht dies ohne Zustimmung des jeweiligen Rechteinhabers bzw. bestehen keine Nutzungsrechte, werden Urheberrechte verletzt.

Spezialisierte Rechtsanwaltskanzleien werden in diesen Fällen für die Film- und Musikindustrie tätig und mahnen – derzeit massenhaft – den Inhaber des Internetanschlusses, über den die Urheberrechtsverletzung erfolgt ist, ab. Der Betroffene soll dann eine sogenannte Unterlassungserklärung unterschreiben, sich also verpflichten, die Filme oder Musikdateien künftig nicht mehr illegal zu verbreiten. Außerdem soll er einen pauschalisierten Schadensersatz sowie die Anwaltskosten bezahlen.

Oftmals erfolgt jedoch der Urheberrechtsverstoß nicht durch den Anschlussinhaber, sondern durch einen Dritten. Daher stellt sich immer wieder die Frage, ob und inwieweit der Anschlussinhaber für Rechtsverletzungen, die ein Dritter über seinen Anschluss begangen hat, haftet.

Welche Sorgfaltspflichten ein Anschlussinhaber einzuhalten hat, ist gesetzlich nicht vorge-

schrieben und richtet sich daher nach der bisherigen Rechtsprechung des Bundesgerichtshofs (BGH). Danach besteht keine generelle Vermutung, dass der Anschlussinhaber auch Täter der Rechtsverletzung ist, die er widerlegen oder erschüttern müsste, nur weil er Inhaber des Anschlusses ist (Urteil vom 06.10.2016, Az. I ZR 154/15). Nutzen mehrere Personen einen Internetanschluss, so genügt es nach Ansicht des BGH, wenn der Anschlussinhaber darlegt, wer außer ihm selbst noch zeitgleich Nutzer des Anschlusses war.

Im Falle des illegalen Filesharings durch ein minderjähriges Kind hat der BGH (Urteil vom 15.11.2012, Az. I ZR 74/12) entschieden, dass Eltern ihrer Aufsichtspflicht genügen, wenn sie das Kind über die rechtswidrige Nutzung des Internetanschlusses belehren und ihm eine Teilnahme daran verbieten. Eine Verpflichtung der Eltern, die Nutzung des Internets zu überwachen, den Computer zu überprüfen oder dem Kind den Zugang zum Internet zu versperren, besteht nicht. Zu derartigen Maßnahmen sind die Eltern erst verpflichtet, wenn sie konkrete Anhaltspunkte dafür haben, dass das Kind dem Verbot zuwiderhandelt.

Bezüglich der Haftung für volljährige Familienangehörige hat der BGH (Urteil vom 08.01.2014, Az. I ZR 169/12) entschieden, dass der Anschlussinhaber grundsätzlich nicht verpflichtet ist, über die Rechtswidrigkeit einer Teilnahme an Internettauschbörsen oder über sonstige Rechtsverletzungen im Internet zu belehren. Eine Pflicht zur Belehrung ist dem Anschlussinhaber ohne konkrete Anhaltspunkte für eine bereits begangene oder bevorstehende Rechtsverletzung nicht zuzumuten, da ein Volljähriger für seine Handlungen selbst verantwortlich ist.

Im Hinblick auf volljährige Verwandte und Gäste hat der BGH (Urteil vom 12.05.2016, Az. I ZR 86/15) entschieden, dass dem Anschlussinhaber eine Belehrung über die Rechtswidrigkeit bestimmter Handlungen im Internet ohne konkrete Anhaltspunkte für eine rechtswidrige Nutzung nicht zumutbar ist. Den Anschlussinhaber, der seinen volljährigen Besuchern oder Gästen einen Zugang zu seinem Internetanschluss ermöglicht, trifft keine anlasslose Belehrungs- oder Überwachungspflicht.

Ob und inwieweit ein Anschlussinhaber die Nutzung des Internetanschlusses überwachen muss bzw. für Rechtsverletzungen durch Dritte haftet, kann daher nicht pauschal beantwortet werden. Dies ist vielmehr eine Frage, die in jedem Einzelfall konkret geprüft werden muss.

Unsere Dienststelle ist für die Thematik des illegalen Filesharings leider nicht der richtige Ansprechpartner, da es sich um keine datenschutzrechtliche Problematik, sondern um Fragen des Urheberrechts bzw. Fragen einer zivilrechtlichen Haftung handelt.

Erhalten Betroffene eine Abmahnung, so empfehlen wir diesen, sich an einen auf Abmahnungen spezialisierten Rechtsanwalt zu wenden und diesen mit der Angelegenheit zu betrauen. Bis dahin raten wir den Betroffenen, nicht in Panik zu geraten und die geforderte Summe nicht vorschnell zu bezahlen. Auch sollte ohne Rücksprache mit einem Rechtsanwalt keine Unterlassungserklärung unterschrieben werden.

11.6 Anspruch auf Löschung von Accounts und personenbezogenen Daten nach Austritt aus sozialem Netzwerk/Forum etc.

Immer wieder erreichen uns Beschwerden von Betroffenen, da Betreiber von sozialen Netzwerken, Foren etc. ihrer Aufforderung zur Löschung ihres Accounts bzw. ihrer personenbezogenen Daten nicht oder nicht vollständig nachgekommen seien. Oftmals besteht die Beschwerde auch darin, dass personenbezogene Daten von den Betreibern nicht gelöscht, sondern lediglich gesperrt wurden.

Die Pflicht zur Löschung personenbezogener Daten richtet sich nach § 35 des Bundesdatenschutzgesetzes (BDSG). Nach § 35 Absatz 2 Satz 2 BDSG sind personenbezogene Daten u.a. dann zu löschen, wenn ihre Speicherung unzulässig ist oder sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist.

Bei der Mitgliedschaft in einem sozialen Netzwerk, Forum etc. kann daher eine Löschung erst erfolgen, wenn der Betroffene entsprechend der Nutzungsbedingungen seine Mitgliedschaft beendet hat. Teilweise ist hierfür – je nach sozialem Netzwerk, Forum etc. – eine schriftliche Kündigung erforderlich. Ohne eine Beendigung der Mitgliedschaft ist der Betreiber des sozialen Netzwerks vertraglich dazu verpflichtet, den Account bereitzustellen, um somit eine Nutzung des sozialen Netzwerks zu

ermöglichen. Würde der Betreiber den Account bzw. die personenbezogenen Daten bei einem Löschbegehren einfach löschen, könnte er seine vertragliche Pflicht nicht mehr erfüllen. Eine Löschung des Accounts bzw. der personenbezogenen Daten kann daher erst erfolgen, wenn entsprechend der Nutzungsbedingungen – ggf. unter Beachtung bestimmter Fristen – eine ordnungsgemäße Beendigung der Mitgliedschaft durch den Nutzer erfolgt ist.

Aber auch nach einer Beendigung der Mitgliedschaft ist der Betreiber des sozialen Netzwerks, Forums etc. nicht immer dazu verpflichtet, die personenbezogenen Daten zu löschen. Bestehen gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen, so tritt gemäß § 35 Absatz 3 Nr. 1 BDSG an die Stelle einer Löschung eine Sperrung der Daten. Dies ist vielen Betroffenen leider nicht bekannt.

Möchte daher ein Betroffener die Löschung seiner Daten erwirken, so sollte er zunächst prüfen, wie nach den Nutzungsbedingungen des betreffenden sozialen Netzwerks, Forums etc. die Mitgliedschaft zu beenden ist. Ggf. sind diesbezüglich bestimmte Frist- und Formanforderungen einzuhalten. Auch nach einer Beendigung der Mitgliedschaft kann es jedoch sein, dass der Betroffene keine Löschung, sondern lediglich eine Sperrung seiner personenbezogenen Daten verlangen kann. Erst, wenn der Betreiber des sozialen Netzwerks, Forums etc. nach ordnungsgemäßer Beendigung der Mitgliedschaft seiner Pflicht zur Löschung bzw. Sperrung der personenbezogenen Daten nicht nachkommt, können wir aufsichtsrechtlich gegen den jeweiligen Betreiber vorgehen.

12. Technik und Medien

12.1 Online-Prüfung von baden-württembergischen Websites

Lediglich 15 % der Websites klein- und mittelständischer Unternehmen in Baden-Württemberg sind über das gesicherte HTTPS-Protokoll abrufbar, hat eine großflächig durchgeführte Online-Prüfung des LfDI BW ergeben. Sind geschäftsmäßig angebotene Telemedien nicht ausreichend gegen Verletzungen des Schutzes personenbezogener Daten abgesichert, drohen hohe Bußgelder!

Mit dem am 25. Juli 2015 in Kraft getretenen Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) wurde auch eine neue, überaus bedeutsame Regelung in das bestehende Telemediengesetz (TMG) eingeführt. Der eingeschobene neue Absatz 7 des § 13 verpflichtet (Tele-)Diensteanbieter zu Folgendem:

Diensteanbieter haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass

1. kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und
2. diese a) gegen Verletzungen des Schutzes personenbezogener Daten und b) gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind, gesichert sind. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.

Die Regelung in Satz 1 Nummer 2 Buchstabe a zielt auf die Sicherstellung des Datenschutzes, also des Schutzes personenbezogener Daten der Nutzer von Telemedien. Ohne Zweifel stellt hierbei ein als sicher anerkanntes Verschlüsselungsverfahren eine der wichtigsten Maßnahmen zum Schutz personenbezogener Daten dar.

Das Besondere an dieser neuen Forderung im TMG besteht darin, dass ein Verzicht der Nutzung eines als sicher anerkannten Verschlüsselungsverfahrens seitens des Diensteanbieters nun eine Geldbuße für diesen zur Folge haben kann. Denn, nach § 16 Absatz 2 Nummer 3 TMG handelt ordnungswidrig, wer vorsätzlich oder fahrlässig entgegen der Vorschrift des § 13 Absatz 7 Satz 1 Nummer 2 Buchstabe a TMG über eine dort genannte Pflicht zur Sicherstellung zuwiderhandelt. Die Ordnungswidrigkeit kann, nach § 16 Absatz 3 TMG, mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

Auch in der Vergangenheit hat der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW) Diensteanbieter von geschäftsmäßig angebotenen Telemedien auf § 9 Bundesdatenschutzgesetz (BDSG) hingewiesen und bei der Übermittlung besonderer Arten personenbezogener Daten gemäß § 3 BDSG bzw. bei Finanzdaten dazu aufgefordert, ein als sicher anerkanntes Verschlüsselungsverfahren einzusetzen. Der LfDI BW wird dabei nach konkreten Hinweisen und Beschwerden von Bürgern aktiv. In der Praxis sind häufig Online-Shops betroffen, die Bezahldaten unverschlüsselt übermitteln. Das Fehlen eines Ordnungswidrigkeitstatbestands bei Nichteinhaltung erschwerte bisher allerdings die Durchsetzung.

Der LfDI BW hat die Neuerung im TMG zum Anlass genommen, im Rahmen einer Massenprüfung zu ermitteln, inwieweit die Websites von in Baden-Württemberg ansässigen Unternehmen – vorwiegend mittelständischen Unternehmen aus allen Regionen und den Branchen Industrie, Handel und Dienstleistungen – über eine gesicherte Verbindung angeboten werden. Mit knapp 40.000 untersuchten Websites handelt es sich dabei um die größte Online-Prüfung, die bisher von einer deutschen Datenschutz-Aufsichtsbehörde durchgeführt wurde.

Konkret haben wir geprüft, ob die Website des Diensteanbieters über eine gesicherte HTTPS-Verbindung angeboten wird. Über HTTPS ist es möglich, eine gesicherte Verbindung zwischen dem Browser des Nutzers und dem Webserver des Diensteanbieters aufzubauen, die dem Nutzer ein sicheres Nutzen des Webangebots erlaubt. „Sicher" heißt in diesem Kontext, dass kein Dritter die übertragenen Daten mitlesen kann und sich auch kein Dritter als vermeintlich legitimer Webserver ausgeben kann (und somit Kenntnis von den nicht für ihn bestimmten Daten nehmen kann). HTTPS steht für „HTTP Secure" und basiert auf HTTP in Kombination mit dem (veralteten) „Secure So-

ckets Layer" (SSL)-Protokoll bzw. dem (aktuellen) „Transport Layer Security" (TLS)-Protokoll. TLS kann als „Standard"-Sicherheitsprotokoll im Internet angesehen werden. Es stellt (unter gewissen Voraussetzungen) u.a. eine dem Stand der Technik entsprechende technisch-organisatorische Maßnahme zur Sicherung gegen Verletzungen des Schutzes personenbezogener Daten nach § 13 Absatz 7 Satz 1 Nummer 2 Buchstabe a TMG dar. SSL/TLS gibt es in verschiedenen Versionen. Das SSL-Protokoll (Version 2 und 3) gilt heute als unsicher und sollte nicht mehr zum Einsatz kommen. Das TLS-Protokoll (Versionen 1.0, 1.1 und 1.2) gilt – bei Verwendung einer aktuellen Implementierung und einer „guten" Cipher Suite – gemeinhin als sicher. Als Anhaltspunkt für den Einsatz von TLS können etwa die „TLS/SSL Best Practices" vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herangezogen werden. Das BSI gibt strenge Vorgaben und rät selbst von der Verwendung von TLS in den Versionen 1.0 und 1.1 ab. Neben der Untersuchung auf die prinzipielle Unterstützung von HTTPS war es unser Ziel, zu ermitteln, welche SSL/TLS-Protokolle dabei jeweils zum Einsatz kommen.

Unsere Prüfung haben wir im Zeitraum von März 2016 bis September 2017 im Abstand von einigen Monaten mehrmals wiederholt, um auch eine Aussage über den Einsatz von HTTPS im zeitlichen Verlauf geben zu können. Im Jahr 2016 konnten wir keine nennenswerten Veränderungen feststellen. Lediglich 5-6 % aller aufrufbaren Websites im Untersuchungszeitraum 2016 wurden über eine „einigermaßen sichere" HTTPS-Verbindung (TLS 1.0, TLS 1.1 sowie TLS 1.2) angeboten. Auch bei einer Prüfung von knapp 2.000 Websites von Handwerksbetrieben in Baden-Württemberg konnten wir ähnliche Ergebnisse feststellen wie bei den Websites der klein- und mittelständischen Unternehmen.

Positiv aufgefallen sind hingegen die deutlichen Verbesserungen im Jahr 2017. Im Vergleich von 5,5 % HTTPS-gesicherten Websites im Juni 2016 ist dieser Wert im Juni 2017 auf einen Wert von 14,8 % gestiegen. Dies mag unterschiedliche Gründe haben. Zum einen ist in diesem Zeitraum die Zahl der erreichbaren Websites zurückgegangen – dabei könnte es sich etwa um ältere Web-Angebote handeln, die nicht über HTTPS angeboten wurden. Zum anderen hat der LfDI BW Anfang 2017 die (schlechten) Vorjahresergebnisse publiziert und im Rahmen von Vorträgen die Missstände publik gemacht und die Einhaltung der datenschutzrechtlichen Vorgaben angemahnt. Außerdem konnten wir feststellen, dass immer mehr Diensteanbieter auf die im Jahr 2015 eingerichtete Zertifizierungsstelle „Let's Encrypt" zurückgreifen. Dabei handelt es sich um eine Zertifizierungsstelle, die kostenfrei Zertifikate für Websites ausgibt und den Einrichtungsprozess von HTTPS insgesamt deutlich vereinfacht. Lag der Anteil an von der Zertifizierungsstelle Let's Encrypt ausgestellten Zertifikate an der Gesamtzahl von über HTTPS angebotenen Websites im Juni 2016 noch bei 6,7 %, so ist dieser Wert im Juni 2017 auf 25,7 % gestiegen.

Bemerkenswert war neben der insgesamt geringen Zahl von HTTPS-gesicherten Websites außerdem die Tatsache, dass die Vorgaben vom BSI (also nur TLS in der Version 1.2) im Jahr 2016 in keinem einzigen Fall eingehalten wurden. Im September 2017 erfüllten lediglich 3 Websites die BSI-Vorgaben. Insbesondere bei Diensteanbietern, die über ihre Website besondere Arten personenbezogener Daten bzw. Finanzdaten von Nutzern erheben und übermitteln, werden wir in Zukunft weiter verstärkt die Einhaltung des aktuellen Stands der Technik bei HTTPS einfordern. Hierzu weisen wir insbesondere auch auf den Artikel 32 Absatz 1 der ab Mai 2018 Anwendung findenden EU-Datenschutz-Grundverordnung (DS-GVO) hin, der Verschlüsselung als geeignete technische Maßnahme zur Einhaltung der gesetzlichen Vorschriften vorsieht. Ein Verstoß gegen diese Bestimmung kann nach Artikel 83 Absatz 4 DS-GVO mit einer Geldbuße von bis zu 10 Millionen € bzw. mit bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden.

Neben der datenschutzrechtlichen Notwendigkeit für den Einsatz von Verschlüsselung bei der Übermittlung personenbezogener Daten über das Internet sollte die Nutzung von HTTPS auch im Interesse der Diensteanbieter liegen. So wirkt sich die Nutzung von HTTPS beispielsweise auch positiv auf die Reihung einer Website bei der Google-Suche aus. Ebenso warnen aktuelle Browser Nutzer bei der Eingabe von Passwörtern auf Websites beim Fehlen einer HTTPS-Sicherung.

In Bezug auf die wirtschaftliche Zumutbarkeit lässt sich festhalten, dass die Umsetzung von HTTPS für Diensteanbieter heutzutage durch die Vielzahl an Zertifizierungsstellen kosten-

günstig möglich ist. Dank Initiativen wie „Let's Encrypt" sind entsprechende Zertifikate neuerdings auch kostenfrei zu beziehen. Diese Entwicklung begrüßt der LfDI BW.

Wir empfehlen allen Diensteanbietern in Baden-Württemberg, ihre Website über eine gesicherte HTTPS-Verbindung bereitzustellen. Der LfDI BW wird weiterhin Diensteanbieter, die über ihre Website besondere Arten von personenbezogenen Daten bzw. Finanzdaten erheben und übermitteln, auf die Einhaltung der Nutzung von HTTPS (mit aktueller TLS-Version und als sicher geltender Cipher Suite) hin überprüfen. Die Standardisierung von TLS 1.3 ist in einem fortgeschrittenen Stadium. Neben erhöhter Sicherheit bietet das Protokoll auch eine verbesserte Performance. Dies wird hoffentlich dafür sorgen, dass Diensteanbieter ein großes Interesse daran haben, möglichst schnell TLS 1.3 zu unterstützen. Dies ist außerdem ein guter Zeitpunkt, um alte Protokollversionen endgültig zu deaktivieren.

Die Ergebnisse unserer Prüfung wurden erstmals unter dem Titel „Wie sicher ist der Zugriff auf Websites im Internet?" in der Zeitschrift Datenschutz und Datensicherheit (Ausgabe 2/2017) publiziert. In diesem Beitrag wird noch detaillierter auf technische Aspekte der Prüfung und der Ergebnisse eingegangen. Der Artikel kann unter http://rdcu.be/oYVx kostenfrei gelesen werden.

12.2 Datenschutz bei Windows 10

Das neue Microsoft-Betriebssystem Windows 10 übermittelt bei einer Standard-Installation jede Menge personenbezogener Daten an Microsoft. Nutzer sollten die Datenschutzeinstellungen prüfen und gegebenenfalls anpassen!

Das neue Betriebssystem Windows 10 von Microsoft ist Ende Juli 2015 erschienen. Besitzer von Windows 7 und Windows 8 erhielten ein kostenloses Upgrade auf Windows 10. Dies sollte für eine möglichst rasche Verbreitung des neuen Betriebssystems auf den unterschiedlichsten Geräten der Nutzer sorgen – stellt Windows 10 doch einen wichtigen Übergang in die Cloud-Welt (etwa mit dem Produkt Office 365) für Microsoft dar. Gerade diese starke Verzahnung des neuen Betriebssystems mit der Microsoft Cloud und die Einführung eines neuen persönlichen Assistenten – genannt „Cortana" – brachten allerdings eine Reihe von Auswirkungen in Punkto Datenschutz mit sich. Microsoft hat sich leider gegen datenschutzfreundliche Voreinstellungen entschieden. Dies hat zur Folge, dass Nutzer selbst aktiv werden müssen, wenn sie nicht möchten, dass ihre personenbezogenen Daten an Microsoft übertragen werden.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW) hat einen Leitfaden publiziert, der Nutzern Schritt für Schritt bei der Einrichtung von Windows 10 behilflich ist und aufzeigt, wie eine möglichst datenschutzfreundliche Nutzung von Windows 10 möglich ist. Der Leitfaden ist unter https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2016/04/2016-04_leitfaden_win10.pdf# abrufbar. Der Leitfaden erfreut sich bei Nutzern bis heute großer Beliebtheit.

Ein Punkt, der für kontroverse Diskussionen sorgte ist der sogenannte „SmartScreen-Filter". Der SmartScreen-Filter untersucht besuchte Webseiten auf potenziell unsichere Inhalte und heruntergeladene Dateien auf Schadsoftware. Dazu wird beim Browsen im Web von jeder angefragten Webseite die Internetadresse (URL) an Microsoft zur Überprüfung gesendet. Bei heruntergeladenen Dateien werden Teile des Inhalts und zusätzliche Informationen über die Datei (bspw. Dateiname) an Microsoft gesendet. Befinden sich die angefragten URLs bzw. Dateien auf einer von Microsoft geführten schwarzen Liste mit bekannten Bedrohungen, so bekommt der Nutzer einen Warnhinweis angezeigt, der vor einem Besuch der Webseite bzw. einer Ausführung der Anwendung abrät. Aus Sicherheitssicht mag der SmartScreen-Filter seine Berechtigung haben. Er erlaubt einen gewissen Schutz vor bekannten Bedrohungen, insbesondere Schadsoftware und infizierte Webseiten können auf Rechnern enormen Schaden anrichten. Allerdings sieht der LfDI BW den SmartScreen-Filter aus Datenschutz-Sicht problematisch. Laut unseren Erkenntnissen wird neben den genannten Daten zudem die vollständige IP-Adresse an Microsoft übermittelt und 60 Tage lang von Microsoft gespeichert. Diese Tatsache wird von Microsoft nicht offen kommuniziert; sie findet sich nicht in den Datenschutzbestimmungen wieder. Durch die Übermittlung der IP-Adresse (als personenbezogenes Datum) ist Microsoft in der Lage, ein umfangreiches Nutzungsprofil (besuchte Webseiten und installierte Anwen-

dungen) zu bilden. Die Speicherung dieser Daten für 60 Tage erfolgt aus unserer Sicht unverhältnismäßig lange. Der LfDI BW empfiehlt aus diesem Grund das Deaktivieren des SmartScreen-Filters. In jedem Fall sollten Nutzer regelmäßig Sicherheitsupdates installieren und ein aktuelles Virenschutzprogramm einsetzen.

Der schweizerische Eidgenössiche Datenschutz- und Öffentlichkeitsbeauftragte hat Microsoft die Aufgabe mitgegeben, mit dem „Creators"-Update von Windows 10 im April 2017 einige Änderungen im Hinblick auf den Datenschutz umzusetzen. Bei der Installation des Creators Update für Windows 10 wird der Nutzer nun aufgefordert, seine Datenschutzeinstellungen zu überprüfen. Die vorzunehmenden Einstellungen ähneln im Wesentlichen jenen, die der LfDI BW in seinem Leitfaden empfiehlt. Die Übermittlung der unterschiedlichen Daten an Microsoft ist auch bei dem Creators Update nach wie vor standardmäßig eingeschaltet. Nutzer, die das nicht möchten, müssen also auch weiterhin selbst aktiv werden.

Die Niederländische Datenschutzaufsichtsbehörde hat im Oktober 2017 die vermeintlichen Verbesserungen des Creators-Updates im Hinblick auf den Datenschutz kritisiert. Microsoft informiere die Nutzer nach wie vor nicht ausreichend, welche Daten übermittelt werden und zu welchem Zweck diese verarbeitet werden. Die Niederländische Behörde bezieht sich hierbei ausschließlich auf die Windows-Versionen „Home" und „Pro", die vor allem von Privatpersonen genutzt werden. Das Bayerische Landesamt für Datenschutzaufsicht hat hingegen im September 2017 erklärt, dass im Unternehmensumfeld ein datenschutzkonformer Einsatz der Windows-Version „Enterprise" möglich ist. Hierfür müssten die Windows-Gruppenrichtlinien entsprechend geändert werden, um die Übermittlung personenbezogener Daten der Nutzer an Microsoft weitestgehend einzuschränken.

Insgesamt lässt sich festhalten, dass der Umstieg auf Windows 10 aus Sicherheits-Sicht durchaus sinnvoll ist. In diesem Bereich sind einige Verbesserungen hinzugekommen. Um möglichst wenig Daten an Microsoft zu übermitteln, empfehlen wir die Überprüfung der Datenschutz-Einstellungen. Hierbei kann Ihnen unser Leitfaden behilflich sein. Größeren Organisationen, die Windows 10 zentral administrieren, empfehlen wir die Orientierungshilfe zur datenarmen Konfiguration von Windows 10 des Arbeitskreis Informationssicherheit der deutschen Forschungseinrichtungen (AKIF) unter https://www.it-sicherheit.mpg.de/Orientierungshilfe_Windows10.pdf.

13. Datenschutz als Kulturaufgabe

Datenschutz als KULTuraufgabe oder Datenschutz 4.0

Erfahrungsgemäß haftet dem Thema Datenschutz eine Aura von Paragraphen, Verboten und Langeweile an. Viele sind auch der Meinung, dass Datenschutz nicht mehr in die heutige Zeit passt und „völlig old-fashioned" wäre – leider nur „old-fashioned", nicht „vintage". Denn wäre Datenschutz „vintage" läge er bei einigen doch wieder ziemlich im Trend….

Typische Aussagen wie „Ich habe nichts zu verbergen." machen deutlich, wie gering der Wert des Grundrechts auf informationelle Selbstbestimmung, die Grundlage für Datenschutz, von vielen bemessen wird.

Aus Sicht der Datenschützer sind diese Aussagen alarmierend, zeigen Sie doch, dass der Schutzzweck dieses Grundrechtes bisher offensichtlich zu wenig in den Alltag des Einzelnen transferiert werden konnte.

Offensichtlich ist es unumgänglich dem Thema Datenschutz schnellstmöglich ein neues Image zu verschaffen – dem Einzelnen zu vermitteln, aus welchem Grund Datenschutz an vielen Stellen Sinn macht, unerlässlich ist und ihm sogar zum Vorteil gereicht. Wir müssen dafür sorgen, dass ein offensichtlich abstraktes Gut für jeden greifbar wird, deutlich machen, welche Auswirkungen bestehender oder auch fehlender Datenschutz im persönlichen Alltag haben kann.

Der Widerspruch von Privatsphäre und stetig zunehmender Öffentlichkeit bietet dabei eine Vielfalt an spannenden Anknüpfungspunkten.
Im Sinne der Redewendung „Besondere Situationen erfordern besondere Maßnahmen" haben wir uns entschlossen ungewöhnliche Wege zu beschreiten:

Wir haben Datenschutz zur KULTuraufgabe erklärt!

Zusätzlich zur klassischen Aufgabenerfüllung einer Datenschutzaufsichtsbehörde werden wir das Thema „Datenschutz als KULTuraufgabe" im Rahmen regelmäßiger Veranstaltungen fest etablieren und gemeinsam mit verschiedenen Partnern aus ganz neuen, unkonventionellen und ungewöhnlichen Perspektiven beleuchten.

Diese andersartige Perspektive hat sich bereits als sehr erfolgreich erwiesen.
Im September 2017 haben wir in Kooperation mit den Innenstadtkinos den US-amerikanischen Science-Fiction-Thriller „The Circle" mit Tom Hanks und Emma Watson in Stuttgart präsentiert. In diesem Film vertritt Eamon Bailey (Tom Hanks) die These, dass alles, was auf der Welt passiert, öffentlich sichtbar sein muss. Nur so könnten Verantwortliche benannt und Menschenleben gerettet werden. Geheimnisse wären oft der Auslöser für Schwierigkeiten und Fehlverhalten. Ziel sei es, sämtliche Daten der User zu verknüpfen und diese mit dem Ziel völliger Transparenz in einer Online-Identität zu vereinen.

Unter dem Motto des Abends „Privatsphäre ist Diebstahl" bestand im Anschluss an die Veranstaltung für die Kino-Besucher die Möglichkeit Fragen zu stellen und die sie bewegenden Themen mit dem Landesbeauftragten und weiteren Experten in persönlicher Runde exklusiv zu diskutieren.

Das bis auf den letzten Platz ausverkaufte Haus sowie die anschließende rege Beteiligung an den Diskussionen hat gezeigt, dass dieser ungewöhnliche Ansatz ein voller Erfolg ist.

Um deutlich zu machen, wie wichtig es uns ist, das Thema Datenschutz greifbar und anschaulich zu machen haben wir Ende November 2017 dieses außergewöhnliche Format fortgesetzt und gemeinsam mit der Stadtbibliothek Stuttgart unter dem Motto „Sie sind vorsorglich festgenommen" den Dokumentarfilm PRE-CRIME gezeigt. Laut diesem Film scheint einer perfekten Welt ohne Verbrechen nichts mehr im Wege zustehen. Zukünftig werden potenzielle Verbrecher verhaftet, BEVOR sie eine Straftat begehen werden. Die Realität scheint diese Dystopie bereits eingeholt zu haben. Predictive policing und algorithmus-gestützte Polizeiarbeit, die auch in Racial Profiling münden kann, wird in vielen Großstädten bereits getestet. Welchen Preis hat die Utopie absoluter Sicherheit? Und was passiert, wenn sich der Computer irrt?

Diese beklemmenden Fragen waren Teil der an den Film anschließenden Podiumsdiskussion. Das Spannungsfeld vermeintlich absoluter Sicherheit im Tausch gegen den Verlust jeglicher Privatsphäre hat zu einer kontroversen Diskussion zwischen dem Landesbeauftragten Dr. Stefan Brink, Hanno Wagner vom Chaos

Computer Club, Nicole Weiß vom Landeskriminalamt und einem fachkundigen und interessierten Publikum geführt und eine solche kontroverse Diskussion wollten und wollen wir anstoßen.Wir werden das Format Datenschutz als KULTuraufgabe auch im neuen Jahr fortsetzen. Gleich zu Jahresbeginn haben wir geplant diesen Dokumentarfilm bei der Hochschule für Polizei Baden-Württemberg zu zeigen. Im Anschluss erwarten wir eine spannende Diskussion mit den Studierenden und den Vertretern der Polizei.

Aus der Dienststelle

I. Eingabenzahlen steigen, Beratungsbedarf wächst

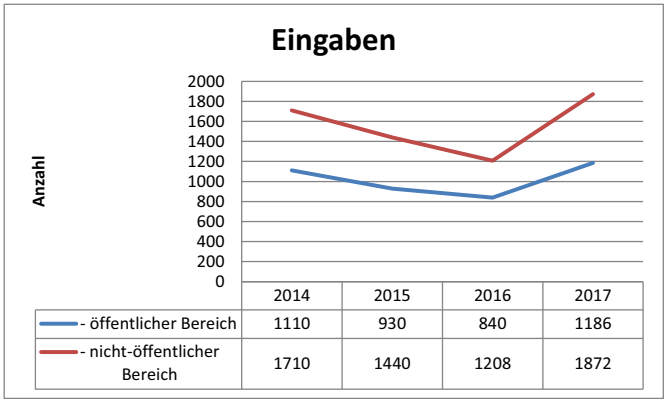
Im Berichtszeitraum 2016/2017 verzeichnete meine Dienststelle über alle Themenbereiche hinweg 5.106 Eingaben von Bürgerinnen und Bürgern. Damit bleibt der Eingang weiterhin auf einem hohen Niveau. Um die Eingabe eines Anliegens noch weiter zu erleichtern, bieten wir seit Anfang 2018 die Möglichkeit einer Online-Beschwerde an. Der Einsatz des Online-Formulars soll außerdem zu einer Beschleunigung des Bearbeitungsverfahrens beitragen. In der Planung befindet sich derzeit ein Online-Formular zur Entgegennahme von Meldungen der Datenschutzbeauftragten sowie zur Meldung von Datenpannen.

Die Entwicklung der Eingaben, Kontrollen und Beratungen zeigen die nachstehenden Übersichten.

Gesamtübersicht

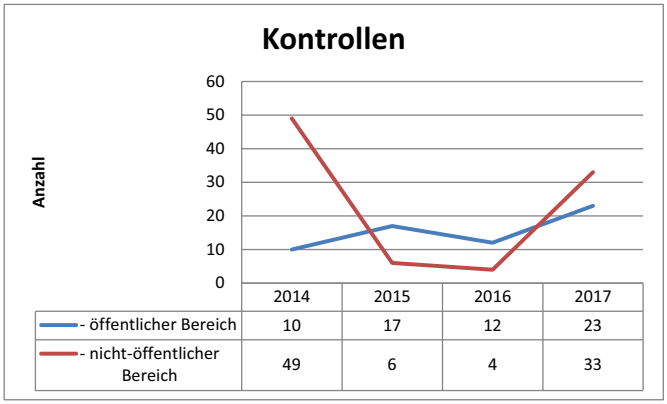
Bezeichnung	2014	2015	2016	2017
Eingaben				
- öffentlicher Bereich	1110	930	840	1186
- nicht-öffentlicher Bereich	1710	1440	1208	1872
Kontrollen				
- öffentlicher Bereich	10	17	12	23
- nicht-öffentlicher Bereich	49	6	4	32
Beratungen				
- öffentlicher Bereich	1063	788	878	991
- nicht-öffentlicher Bereich	1002	812	637	795

Eingaben



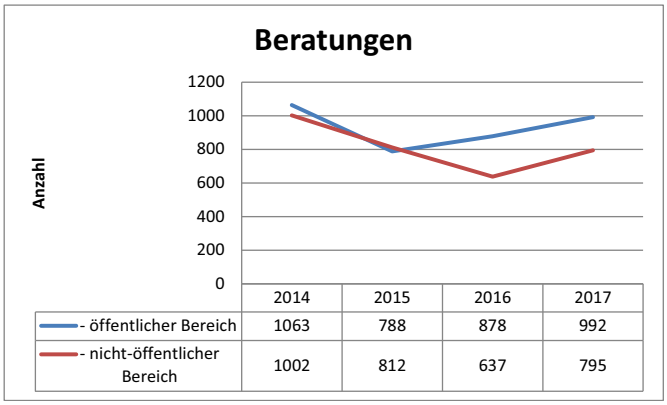
Die Zahl der bei uns eingegangenen Eingaben ist nach einem leichten Rückgang im Jahr 2016 sowohl im öffentlichen als auch nicht-öffentlichen Bereich wieder angestiegen und bleibt damit auf einem hohen Niveau. Gründe für die Steigerung innerhalb des Berichtszeitraums sind nach unserer Einschätzung unter anderem Themen wie Vorratsdatenspeicherung, Staatstrojaner, die bevorstehende europäische Datenschutz-Grundverordnung sowie unsere verstärkte Öffentlichkeitsarbeit.

Kontrollen



Zu den Kontrollmaßnahmen ist auch die arbeitsaufwändige Überprüfung von rund 1.700 Internetauftritten öffentlicher Stellen in Baden-Württemberg im Hinblick auf die Einbindung des Facebook-Like-Buttons sowie Twitter-Plugins im Jahr 2017 zu rechnen. Diese Kontrolle spiegelt sich in der Statistik nicht wider.

Beratungen



Ein wichtiger und mit hohem Arbeitsaufwand verbundener Bestandteil unserer Arbeit ist die Beratung der Landesregierung, der Ministerien, sonstigen öffentlichen Stellen sowie auch der nicht-öffentlichen Stellen im Land und ihrer betrieblichen Datenschutzbeauftragten in Datenschutzfragen.

Um den gesteigerten Informationsbedarf hinsichtlich der am 25. Mai 2018 in Kraft tretenden EU-Datenschutz-Grundverordnung (EU-DSGVO) gerecht zu werden, werden wir das Informationsangebot auf unserem Internetauftritt permanent erweitern.

Weiterhin haben wir die Öffentlichkeitsarbeit im Berichtszeitraum weiter ausgebaut. Hierzu gehört – neben einer verstärkten Presseaktivität (die Anzahl der Pressemitteilungen1 meiner Dienststelle hat sich im Jahr 2017 im Vergleich zu den Vorjahren praktisch verdreifacht) – die Durchführung von Schulungen sowie Vorträgen. Alleine im Jahr 2017 haben wir 57 Vorträge mit einem Publikum von 30 bis 500 Zuhörern sowie 17 Schulungen mit teilweise über 200 Teilnehmern gehalten.

1 https://www.baden-wuerttemberg.datenschutz.de/pressemitteilungen/

Schulungen und Vorträge 2016			
Vorträge	Publikum	**Schulungen**	Publikum
16	30 - 600	**3**	Ø 40

Schulungen und Vorträge 2017			
Vorträge	Publikum	**Schulungen**	Publikum
57	30 - 500	**17**	≤ 220

II. Neue Aufgaben

1.) Vorbereitung auf die DS-GVO

Der Übergang vom nationalen Datenschutzrecht zur Europäischen Datenschutzgrundverordnung hat auch seinen Niederschlag in der Ausstattung und Ausrichtung der Dienststelle des Landesbeauftragten. Wenn die Verordnung ab dem 25. Mai 2018 in der gesamten Europäischen Union und übergreifend für öffentliche wie auch nicht-öffentliche Stellen wirksam wird, so muss dies auch seinen Niederschlag bei den zuständigen Aufsichtsbehörden finden. Unsere Anstrengungen, dem wachsenden Beratungsbedarf von Unternehmen und Behörden gerecht zu werden, habe ich schon in ihrer gesamten Breite dargestellt. Aber auch schon vor Verabschiedung der Verordnung durch das Europäische Parlament im April 2016 hat sich meine Dienststelle auf die neuen Herausforderungen eingestellt, in dem zum Beispiel wöchentliche Englisch-Inhouse-Kurse eingeführt wurden. Seit Juli 2017 werden diese Schulungen ergänzt um Inhouse-Angebote zur Datenschutz-Grundverordnung. In einem offenen Veranstaltungsmodus unterrichten sich die Mitarbeiterinnen und Mitarbeiter des LfDI gegenseitig und nachhaltig über die anstehenden Veränderungen und entwickeln auf dieser Grundlage ein gemeinsames Verständnis dieser maßgeblichen Rechtsnorm.

2.) Das neue Landesinformationsfreiheitsgesetz

Von nicht minder großer Bedeutung für die Dienststelle ist das Gesetz zur Regelung des Zugangs zur Information in Baden-Württemberg (Landesinformationsfreiheitsgesetz – LIFG) vom 17. Dezember 2015. In Reaktion auf dieses Gesetz und die mit diesem Gesetz dem Landesbeauftragten übertragenen neuen Aufgaben der Aufklärung und Kontrolle im Bereich der Informationsfreiheit wurde im Januar 2016 eine „Stabsstelle Informationsfreiheit" beim Landesbeauftragten etabliert. Im Zusammenhang mit dem zweiten Nachtragshaushalt 2015/2016 wurden der Dienststelle bereits im Herbst 2015 zwei Stellen des höheren Dienstes für diese neuen Aufgaben zugewiesen. Seit März 2017 erfolgte die entsprechende Umbenennung der Dienststelle von „LfD" zu „LfDI"; zum Mai 2017 wurde die Stabsstelle Informationsfreiheit zu einem eigenständigen Referat des Landesbeauftragten erhoben. Die Entwicklung der Aufgaben im neuen Bereich Informationsfreiheit wird in einem eigenen (ersten) Tätigkeitsbericht für die Jahre 2016/2017 vorgestellt werden.

III. Personelles & Ressorts

Am 1. Mai 2016 trat mein Vorgänger im Amt Jörg Klingbeil in den Ruhestand. Der Landtag und seine Ausschüsse haben die hervorragende Arbeit meines Amtsvorgängers sehr positiv gewürdigt; aus den von mir im ersten Jahr meiner Tätigkeit gesammelten Erfahrungen heraus möchte auch ich mich bei Herrn Kollegen Klingbeil herzlich dafür bedanken, dass er eine in jeder Hinsicht intakte und aktive Dienststelle mit guter personeller und sachlicher Ausstattung sowie klarer thematischer Ausrichtung entwickelt hat, die alle Chancen hat, die anstehenden Herausforderungen gut zu bewältigen.

In der Zeit von Mai bis Dezember 2016 nahm mein Vertreter, Ministerialrat Volker Broo, als Leitender Beamter der Dienststelle die Geschäfte des LfD wahr; er tat dies in so umsichtiger und fachlich versierter Weise, dass der Übergang zu meinem Amtsantritt im Januar 2017 in völlig reibungsloser und konstruktiver Weise gelingen konnte.

Der Landtag Baden-Württemberg hat einen ganz erheblichen Anteil an der positiven Fortentwicklung der Landesbehörde: Mit Beschluss des Landtags vom 9. Februar 2017 gingen dem LfDI im laufenden Haushalt insgesamt acht Stellen (zwei Stellen der Besoldungsgruppe A 13 höherer Dienst, zwei Stellen der Besoldungsgruppe A 14, vier Stellen der Besoldungsgruppe A 15) sowie 48.000 Euro zusätzliche Sachmittel zu. So notwendig diese Stellenmehrung war, so war sie doch im parlamentarischen Verfahren keineswegs unumstritten. Wenn auch im Frühjahr 2017 zu befürchten stand, dass die Zeiten der fraktionsübergreifenden Anträge zum Datenschutz und der Informationsfreiheit vorbei seien und die damit verbundenen gesellschaftspolitischen Fragen nunmehr zum Gegenstand der kontroversen parlamentarischen Auseinandersetzungen werden könnten, so sehr hat das gemeinsame und fraktionsübergreifende Vorgehen im Rahmen der Beratungen des Doppelhaushalts 2018/2019 insoweit für Beruhigung gesorgt.

Mit der beschlossenen Personalaufstockung um weitere zwölf Vollzeitstellen hat sich der Personalkörper des LfDI innerhalb eines Jahres um zwanzig Stellen von 34,5 auf 54,5 Planstellen erhöht. Dies bedeutet nicht nur eine erhebliche haushaltsmäßige Anstrengung, sondern fordert von der Dienstelle selbst eine ganz erhebliche Integrationskraft. Neben Fragen der geeigneten Personalauswahl und der inhaltlichen Steuerung einer ganz erheblich angewachsenen Mitarbeiterzahl stellen sich auch große Herausforderungen im Bereich der Personalverwaltung, die nach Jahren der verwaltungsmäßig hervorragenden und sachlich äußerst zurückhaltenden Betreuung durch die Landtagsverwaltung zum 1. Juli 2017 in die Verantwortung des LfDI überführt wurde. Damit wurde zugleich eine wichtige Voraussetzung dafür geschaffen, dass dem LfDI mit dem Wirksamwerden der Datenschutz-Grundverordnung der Status einer selbständigen und unabhängigen „Obersten Landesbehörde" zugeordnet werden kann. Dieser abschließende Schritt steht von gesetzgeberischer Seite mit der Novellierung des Landesdatenschutzgesetzes zum Mai 2018 nunmehr bevor.

Diese neue Stellung des Landesbeauftragten in der Landesverwaltung hatte auch weitere Umressortierungen innerhalb des eigenen Verwaltungsaufbaus zur Folge: So übernahm Herr Ministerialrat Broo die Leitung des Referats I „Grundsatzfragen des Datenschutzes, Zentraler Service, IuK" zum 1. März 2017. Gleichzeitig wurden zwei wesentliche Grundsatzangelegenheiten (Kommunikation mit Verbänden und Einrichtungen; Presse- und Öffentlichkeitsarbeit, Medienkontakte, Veranstaltungen) direkt beim LfDI angesiedelt. Seit August 2017 wird der LfDI gerade in kommunikativen Angelegenheiten und bei Grundsatzfragen von einer persönlichen Referentin unterstützt, gleichzeitig wurde eine eigene Koordinierungs- und Pressestelle zum 1. Oktober 2017 etabliert.

IV. Beratung und Öffentlichkeitsarbeit im Fokus

1.) Veranstaltungen und Schulungen

Die Stärkung der Beratung durch die Dienststelle als Gegenentwurf zu einem Datenschutz, der nur als Bedenkenträger und Verhinderer im Nachhinein daher kommt, wurde im Berichtszeitraum vorangetrieben.

Aus der Vielzahl von Veranstaltungen, die der LfDI im Jahr 2017 durchführte, sollen nur zwei herausgehoben werden: Zum einen die Auftaktveranstaltung am 24. Februar 2017, die als „Standortbestimmung für Datenschutz und Informationsfreiheit" im Gebäude des Landtags Baden-Württemberg stattfinden konnte. Mehr als 220 Teilnehmerinnen und Teilnehmer bekundeten ihr lebhaftes Interesse an einem intensivierten und auch öffentlichkeitswirksamen Austausch über aktuelle Fragen des Datenschutzes und der Informationsfreiheit. Gleichzeitig betonten Vertreter aller Fraktionen des Landtags die wachsende Bedeutung von Datenschutz und Informationsfreiheit an der Schwelle zum digitalen Zeitalter. Besondere Nennung verdient auch die im

Oktober erstmals ausgerichtete Herbstkonferenz des Datenschutzes in Stuttgart, die unter dem programmatischen Titel „Herausforderung der DSGVO – Wirtschaft trifft Aufsicht" auf eine außergewöhnliche Resonanz stieß. Mehr als 200 Teilnehmerinnen und Teilnehmer diskutierten über zwei Tage hinweg die Herausforderungen und Lösungsansätze der neuen Ära des Datenschutzes. Neben der Datenschutz-Grundverordnung selbst wurden auch die Themen Digitalisierung, Big Data und Datenschutz durchaus kontrovers erörtert – neben dem Staatssekretär im Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg konnten auch internationale Referenten und Gäste aus der Schweiz, Liechtenstein und der Slowakei gewonnen werden. Die weiteren Aufsichtsbehörden in Deutschland waren nicht nur zahlreich vertreten, mit dem Präsidenten des Bayerischen Landesamtes für Datenschutzaufsicht Thomas Kranig konnte für das kommende Jahr zudem ein Kooperationspartner für die gemeinsam mit dem Berufsverband der Datenschutzbeauftragten BVD ausgerichtete Konferenz gewonnen werden. Mit einem gewissen Stolz erfüllt den LfDI, dass allein aus dem eigenen Haus fünf Referenten für anspruchsvolle und vielbeachtete Vortragstätigkeit gewonnen werden konnten.

2.) Twitter

Die wachsenden Anforderungen an die Tätigkeit eines Landesbeauftragten im Bereich der Kommunikation und Öffentlichkeitsarbeit spiegelt sich nicht nur in einer Vielzahl von Veranstaltungen, Schulungen und Fortbildungsangeboten bereits im Jahr 2017 wider, sondern auch bei den dazu eingesetzten Medien. Über den weiter ausgebauten Internetauftritt des LfDI hinaus nutze ich seit November 2017 den Nachrichtendienst Twitter zur Verbreitung von Informationen, Orientierungshilfen und Handlungsempfehlungen. Dieser auch aus Sicht der übrigen Datenschutzaufsichtsbehörden keineswegs unumstrittene Schritt trägt bereits erste Früchte, bereits in den ersten Wochen der Nutzung von Twitter konnte ein Kreis von mehr als 700 „Followern" aufgebaut werden und die Kommunikation mit den Datenschutzinteressierten aus allen Bereich wesentlich verbessert werden.

Das Twitter-Angebot gehört dabei als Teil der Öffentlichkeitsarbeit und -aufklärung zu den Aufgaben des LfDI. Mit ihm informiere ich zu aktuellen Themen aus der Welt des Datenschutzes, der Informationsfreiheit und der Dienststelle und erreiche mit diesem Angebot auch Zielgruppen, die über herkömmliche Instrumente wie die Homepage oder Broschüren nicht erreicht werden können. Bereits jetzt haben über 100.000 Nutzer meine 100 Tweets gesehen. Insbesondere ermöglicht der Account mir den direkten Dialog mit Bürgerinnen und Bürgern und eine unmittelbare Vernetzung mit anderen Institutionen, öffentlichen Stellen und der Datenschutz-Community. Alle Informationen rund um die Themen Datenschutz und Informationsfreiheit und alle Tweets finden sich weiterhin auf der Internetseite der Dienststelle; ebenso bleiben alle bekannten Möglichkeiten der Kontaktaufnahme erhalten. Insofern stellt der Twitter-Kanal nur eine zusätzliche Informations- und Kontaktmöglichkeit dar.

Auch nach meinem Dafürhalten sind Soziale Netzwerke aus datenschutzrechtlicher Sicht in vielen Punkten verbesserungsbedürftig. Dies ändert aber nichts daran, dass sie zur Lebenswirklichkeit vieler Nutzerinnen und Nutzer gehören und eine ganz neue Art der Kommunikation, der Transparenz und des Austausches auch für öffentliche Stellen bieten. Sich an dieser Kommunikation zu beteiligen, die Nutzung dieser Angebote durch Bürger, Unternehmen und andere öffentliche Stellen kritisch und beratend zu begleiten und diese für die jeweiligen Risiken zu sensibilisieren, anstatt der Entwicklung nur tatenlos von außen zuzusehen, stellt meines Erachtens einen sinnvollen Weg dar, der tatsächliche Veränderungen bewirken kann. Ein erster Schritt ist dabei, einen bewussten Umgang und eine bewusste, aufgeklärte Nutzung Sozialer Medien durch private Nutzer, aber insbesondere auch durch öffentliche Stellen anzuregen und anzuleiten. Diesem Ziel dient u.a. die von mir entworfene Richtlinie zur Nutzung Sozialer Medien durch öffentliche Stellen, die bereits jetzt großen Anklang bei zahlreichen öffentlichen Stellen gefunden hat. Die vielen Nachfragen und auch die Anregung eigener Projekte zeigen deutlich den Bedarf aber auch die Bereitschaft öffentlicher Stellen, sich datenschutzkonform zu verhalten und das von uns entwickelte Nutzungskonzept, die Abschätzung der Folgen der Twitternutzung in Anlehnung an die nach Art. 35 Abs. 1 DS-GVO vorzunehmende Datenschutz-Folgenabschätzung sowie die „Netiquette" als Blaupause für die eigenen Angebote zu verwenden. Auch die von uns durchge-

führten Aktionen zur Sensibilisierungen haben viele hunderte Nutzer erreicht. Diese Ergebnisse rechtfertigen den mit der Nutzung von Twitter verbundenen Nachteil, dass die Menge der Daten, die von der Twitter Inc. verwendet und ausgewertet werden, durch den Account des LfDI erhöht werden (auch, wenn die entsprechenden Daten – nämlich die Tweets und der Accountname eines Twitterers – schon öffentlich/ allgemein zugänglich/frei im Internet verfügbar sind).

Im Weiteren werde ich die Umsetzung der von uns gemachten Vorgaben kontrollieren und auf eine datenschutzfreundlichere Ausgestaltung Sozialer Medien durch die Anbieter selbst hinwirken.

3.) Neues Format „Datenschutz als Kulturaufgabe"

Schließlich hat der LfDI seinen Aufgabenzuschnitt seit dem 1. Juli 2017 um einen weiteren wichtigen Aspekt ergänzt: Unter dem Titel „Datenschutz als Kulturaufgabe" habe ich eine Veranstaltungsreihe ins Leben gerufen, die das oftmals als sperrig oder technokratisch missverstandene Thema Datenschutz mit den Mitteln von Kunst und Kultur für weitere und neue Bevölkerungskreise erschließen will. Die ersten Veranstaltungen hierzu – Filmvorführungen und (anschließende) Podiumsdiskussion – wurden äußerst interessiert und mit großer Resonanz aufgenommen; diese Reihe wird in den folgenden Jahren fortgesetzt werden und verspricht noch ganz erhebliches Potenzial.

Informationen zur Dienststelle

Aufbau der Dienststelle

Die Dienststelle des Landesbeauftragten für den Datenschutz und die Informationsfreiheit verfügt über 42,5 Planstellen und ist in sechs Referate und die Stabsstelle Europa gegliedert. Die jeweiligen Leiter/-innen und ihre Themenschwerpunkte sind der nachstehenden Übersicht zu entnehmen. Bitte wenden Sie sich bei Anfragen an unsere Telefonzentrale (0711 / 61 55 41 – 0).

Telefonzentrale: 0711 / 61 55 41 - 0
Die Telefonzentrale ist montags bis freitags in der Zeit von 9 bis 12 Uhr und montags bis donnerstags zusätzlich in der Zeit von 14 bis 15:30 Uhr besetzt.

Telefax: 0711 / 61 55 41 - 15

E-Mail: poststelle@lfdi.bwl.de

Stichwortverzeichnis