Landtag von Baden-Württemberg **Drucksache 16 / 5000**

16. Wahlperiode **17. 01. 2019**

Mitteilung

des Landesbeauftragten für den Datenschutz und die Informationsfreiheit

34. Datenschutz-Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg für das Jahr 2018

Schreiben des Landesbeauftragten für den Datenschutz und die Informationsfreiheit vom 16. Januar 2019, Az.: C 2310/34. TB:

Anbei übersende ich Ihnen meinen 34. Tätigkeitsbericht für den Datenschutz.

Dr. Brink

Eingegangen: 17. 01. 2019 / Ausgegeben: 11. 02. 2019

34. Datenschutz-Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg 2018

Inhaltsverzeichnis

LfDI BW - 34. Tätigkeitsbericht 2018

Vorwort

2018 – Das Jahr des Datenschutzes

Mit dem nun vorgelegten ersten Tätigkeitsbericht nach Maßgabe der EU-Datenschutz-Grundverordnung (DS-GVO) findet ein Arbeitsjahr seinen Abschluss, das uns Datenschützern – und sicherlich nicht nur uns – in Erinnerung bleiben wird:
Die angekündigte Zeitenwende wurde eingeleitet durch die Verabschiedung der europäischen Datenschutz-Grundverordnung, durch intensive Vorbereitungs- und Koordinierungsarbeit auf den Stichtag 25. Mai 2018, der für alle dann doch zu früh und für nicht wenige völlig überraschend kam...

Seit diesem Datum ist die DS-GVO in der gesamten EU unmittelbar geltendes Datenschutzrecht, und es bescherte uns Datenschutz-Aufsichtsbehörden eine nie dagewesene Aufmerksamkeit: Nie zuvor wurden wir mit so vielen Eingaben, Bitten und Beschwerden überhäuft, nie zuvor war die Nachfrage nach Beratung, nach Schulung und Begleitung so intensiv, nie war das Medieninteresse so groß wie im Berichtsjahr 2018.

Wir haben uns darauf vorbereitet – und die im Bundesvergleich einmalig gute Aufstockung des Personals hat sich dabei als absolut notwendig erwiesen. Unsere Kernaufgaben (Beratung von Bürgerinnen und Bürgern als sogenannte „Betroffene" bzw. als für Datenverarbeitung „Verantwortliche" in Unternehmen, Behörden und Vereinen/Aufklärung und Sensibilisierung der Öffentlichkeit in Fragen des Datenschutzes/Aufsichtsbehördliche Durchsetzung des Datenschutzrechts mit Prüfmaßnahmen und Sanktionen) wurden ergänzt um die „europäische Dimension" des neuen Rechts: Seit dem Jahr 2018 sind wir Teil einer europäischen Datenschutzverwaltung, die sich von Portugal bis Polen, von Schweden bis Griechenland austauscht, informiert und koordiniert; und nicht ohne Stolz können wir sagen, dass Baden-Württemberg von Anfang an auf dieser neuen Ebene seinen Platz gefunden hat: als deutscher Vertreter in der einflussreichen Social Media Group des Europäischen Datenschutzausschusses, als Berichterstatter zu zentralen Fragestellungen der DS-GVO und als Gesprächspartner für international tätige Unternehmen und Medien.

Diese neuen Aufgaben und das Ausmaß unserer Inanspruchnahme hat uns 2018 an die Grenze der Belastbarkeit geführt. Keine Behörde kann eine Verdoppelung, zeitweise sogar die Verdreifachung seiner Arbeitslast einfach wegstecken. Durch organisatorische und personelle Maßnahmen passen wir uns der neuen Nachfrage laufend an und bemühen uns nach Kräften, die Antwortzeiten deutlich zu reduzieren.

Dennoch fällt mein Fazit zu Jahr 1 der DS-GVO sehr positiv aus: Mit dem Europäischen Recht haben wir eine gute Aktionsgrundlage, die wir in der praktischen Anwendung vernünftig und pragmatisch auslegen und damit bislang immer zu guten Ergebnissen gekommen sind. Gerade die exorbitanten Bußgelddrohungen der DS-GVO hatten durchaus positive Konsequenzen: Auf das „gute alte BDSG" hatte sich nach vorsichtiger Schätzung etwa ein Drittel der deutschen Unternehmen eingerichtet; die robuste europäische Ansage „Jeder Datenschutzverstoß kostet ab sofort den kompletten Jahresgewinn" hat uns das zweite Drittel der Verantwortlichen erschlossen – und die übrigen werden erkennen, dass es sich nicht auszahlt, auf Risiko zu setzen. Unsere Bußgeldstelle hat in diesem Sinne bereits die ersten Strafen verhängt, sehr fix im deutschen und europäischen Vergleich und immer mit Augenmaß (unsere Finanzministerin konnte sich 2018 über insgesamt sechsstellige Überweisungen freuen).

Im Mittelpunkt unserer Tätigkeit stand und steht weiterhin die Beratungstätigkeit: in tausenden Einzelgesprächen, auf hunderten Veranstaltungen und Seminaren, mittels dutzender Orientierungshilfen in unserem neu gestalteten Internetauftritt

(„Renner" ist unser Praxisratgeber „Datenschutz im Verein") oder via Twitter, wo wir im vergangenen Jahr über 4,5 Millionen mal Bürgerinnen und Bürger mit Datenschutzinformationen erreichten.

Das neue Recht ist nicht selbsterklärend. Es bedarf der Interpretation und Auslegung – und der selbstbewussten und umsichtigen Entscheidung, wie es richtiger Weise zu verstehen ist. Dazu sind in erster Linie die Verantwortlichen selbst berufen, aber jeder Betroffene sollte sich selbst ein Bild davon machen, ob sein Dienstleister, seine Behörde oder sein Arbeitgeber dabei verantwortungsvoll und nachvollziehbar vorgeht. Aufgabe der Aufsichtsbehörde ist es dabei, diese Entscheidungen zu begleiten und immer dann – aber auch erst dann – einzugreifen, wenn unvertretbare Datenverarbeitungen stattfinden. Das erfordert viel Sachverstand, aber auch Erfahrung und eine gewisse Gelassenheit – besonders angesichts einer teilweise überhitzten öffentlichen Debatte zum Datenschutz, die vermeintliche Fehlentwicklungen als „Datenschutz-Irrsinn" aufgreift und anprangert. Ihnen und allen wohlmeinenden Kritikern sei gesagt: Als staatliche Aufsichtsbehörde unterliegen wir und unsere Rechtspositionen nach wie vor der Rechtsbindung und dem Verhältnismäßigkeitsprinzip, die Gerichte kontrollieren unabhängig unsere Tätigkeit als unabhängige oberste Landesbehörde. Jede unserer Positionierungen, besonders auch jede Anordnung oder Sanktion, müssen wir eingehend und überzeugend begründen und am Maßstab des Gesetzes rechtfertigen. Wer immer also meint, beim Datenschutz handele es sich um eine bürokratische, technisch komplexe und letztlich nicht nachvollziehbare Pflichtübung, dem sagen wir:

Wenn es nicht vernünftig ist, dann ist es kein Datenschutz!

Am Ende entscheidet aber nicht die Aufsichtsbehörde, wie es um die Zukunft des Datenschutzes bestellt ist – diese Entscheidung treffen alle von der Digitalisierung betroffenen Bürgerinnen und Bürger: Welche Bedeutung messen wir als Betroffene und Grundrechtsträger zukünftig unserem Freiheitsrecht auf informationelle Selbstbestimmung zu? Sind wir bloß willige Konsumenten, denen Annehmlichkeiten und „Dabeisein" wichtiger scheinen als die Chance, selbstbestimmt ins digitale Zeitalter zu schreiten?
Ein Grundrecht ohne Grundrechtsträger, die seine Substanz auch wertschätzen, hat keine Zukunft – auch nicht mit einer Europäischen DS-GVO.

Den neuen Schwung der DS-GVO nehmen wir Datenschützer jedenfalls optimistisch auf – die Grundlagen für diese Zuversicht finden sich in diesem Tätigkeitsbericht. Wiederum gilt mein Dank nicht nur meinen Amtsvorgängern und meinem Stellvertreter, der mich hervorragend unterstützt, sondern allen meinen Mitarbeiterinnen und Mitarbeitern für ihre intensive Arbeit, die in vielen Bereichen weit über das „geforderte Maß" hinausgeht und Beleg dafür ist, dass wir Datenschützer auch immer „Überzeugungstäter" sind und bleiben werden. Bedanken darf ich mich an dieser Stelle aber auch bei den Abgeordneten des Landtags Baden-Württemberg, welche unsere Aufgabe auch im Jahr 2018 maßgeblich gestaltet, begleitet und gefördert haben.

Ihr Landesbeauftragter

Dr. Stefan Brink

1. Schwerpunkte

1.1 Der LfDI hilft weiter: beraten, schulen, sensibilisieren

Eine wesentliche Aufgabe aller Datenschutz-Aufsichtsbehörden ist nach der Datenschutz-Grundverordnung (DS-GVO, Art. 57) die Sensibilisierung der Datenverarbeiter (sog. verantwortliche Stellen), der betrieblichen und behördlichen Datenschutzbeauftragten und natürlich aller Bürgerinnen und Bürger (sog. Betroffene) für die aus der Verordnung entstehenden Rechte und Pflichten. In umfangreichem Maße kam die Dienststelle des LfDI diesem gesetzlichen Auftrag nach und führte für Unternehmen, Einzelhändler, Handwerker und Vereine sowie für Behörden und ihre Mitarbeiter im ganzen Land Schulungen und Beratungen durch.

1.1.1 Stabsstelle Europa on Tour

Das Jahr 2018 stand vollends im Lichte der Datenschutz-Grundverordnung (DS-GVO). Die Anzahl der Nachfragen und der Bedarf an Schulungen waren enorm, sodass sich baden-württembergweit innerhalb des Berichtszeitraums etwa 9.000 Teilnehmerinnen und Teilnehmer in rund 80 Veranstaltungen der Stabsstelle Europa des Landesbeauftragten zu vielfältigen datenschutzrechtlichen Themen schulen und sensibilisieren ließen.
Diese Schulungen wurden so gut angenommen, dass wir im wahrsten Sinne des Wortes ganze Stadthallen füllten. Dies alles mit dem Ziel, eine solide Grundlage für datenschutz- und DS-GVO-konformes Handeln sowohl in Landesbehörden und kommunalen Verwaltungen als auch in Konzernen, kleinen und mittelständischen Unternehmen und Vereinen mit Sitz in Baden-Württemberg zu schaffen und die Verantwortlichen bei ihren jeweiligen Anpassungs- und Umsetzungsprozessen an den neuen europäischen Rechtsrahmen zu befähigen, effektive Lösungen und Prozesse zu entwickeln.
Themeninhalte der DS-GVO-Veranstaltungen waren u. a.:

- Anpassungsbedarfe identifizieren
- Action-Plan und Last-Minute-Maßnahmen
- Rechenschaftspflicht effektiv umsetzen
- Informationspflichten
- Betroffenenrechte
- Umgang mit Datenpannen
- Neue Arbeitsweisen der Aufsichtsbehörden

Schnell kristallisierte sich eines heraus: Während die großen Unternehmen und Konzerne die zweijährige Umsetzungs- und Schonzeit bis zur Geltung der DS-GVO von 2016 bis 2018 gut genutzt haben, um Projektteams zu bilden und erforderliche Prozesse einzurichten und damit grundsätzlich in der Lage waren, einen nahtlosen Übergang zwischen altem und neuem Recht zu garantierten, ergab sich insbesondere bei kleinen und mittelständischen Unternehmen und bei Handwerksbetrieben sowie Vereinen ein gänzlich anderes Bild. Hier herrschten spätestens seit April 2018 Verunsicherung, Verwirrung, teilweise gar Panik. Vermutlich die Anfang Mai in vielen Medien geschürte Angst vor millionenhohen DS-GVO-Bußgeldern schuf dort nicht nur das Problembewusstsein für den notwendigen Anpassungsbedarf, sondern sorgte für Kurzschlussreaktionen wie das Herunterfahren von Webseiten oder für die überstürzte Beauftragung von „Dienstleistern" ohne jede fachliche Qualität. Die „kleinen Verarbeiter" begannen meist erst kurz vor dem 25. Mai, tätig zu werden. Selbst wenn aber rechtzeitig mit der Umsetzung der neuen Vorgaben begonnen wurde, fehlte es im Umsetzungsprozess der DS-GVO-Vorgaben zumeist an personellen und finanziellen Mitteln.
Und so hieß es für die Stabsstelle insbesondere in den finalen Wochen vor dem 25. Mai und in den darauf folgenden Monaten, die Schockstarre dieser Stellen durch zahlreiche Schulungen, Handreichungen, Mustervorlagen und vor allem durch die

Entwicklung und Vorstellung praxisnaher Lösungen entsprechend abzufedern. Hier kooperierten wir bewusst mit Multiplikatoren (u. a. zahlreichen Berufs- und Fachverbänden, IHKs und Handwerkskammern), um eine möglichst hohe Anzahl von Verantwortlichen zu erreichen.

Neben den auf eine Großzahl an Teilnehmern ausgerichteten Schulungsformaten wurden zahlreiche Einzel- und Gruppen-Beratungstermine durchgeführt. Im Beratungssektor konnten allgemeine Hilfestellungen zur Umsetzung der Datenschutz-Grundverordnung, aber auch konkrete projektbezogene Beratungen durchgeführt werden. So begleiteten wir beispielsweise den Entwurf von DS-GVO-konformen Einwilligungen, Vereinbarungen sowie Informationserklärungen, die Entwicklung von Online-Schulung-Tools oder die Entwicklung von elektronischen Datenschutz-Managementsystemen. Aber auch bei anderen Projekten, wie Forschungsvorhaben oder konkreten Produktentwicklungen konnte unbürokratisch und pragmatisch auf die Vereinbarkeit mit den neuen Datenschutzregeln – insbesondere mit dem Grundsatz „privacy by design" – hingewirkt werden.

1.1.2 Schulungen für den kommunalen Bereich

Die Datenschutz-Grundverordnung beschäftigt in hohem Maße auch die Gemeinden und Landkreise in Baden-Württemberg. Nicht nur inhaltliche Veränderungen kamen dabei auf die rund 1100 Kommunen und 44 Stadt- und Landkreise im Land zu. Vielmehr mussten und müssen vor Ort auch Strukturen und Prozesse geschaffen werden, um die Anforderungen des europäischen Datenschutzrechts erfüllen zu können.

„Mit der Datenschutz-Grundverordnung stehen wir datenschutzrechtlich an einer Zeitenwende. Die Aufgabe der Aufsichtsbehörden ist an dieser Stelle nicht nur zu sagen, was nicht geht. Sie sollen auch die verantwortlichen Stellen dabei beraten, wie es geht und wie es besser geht. Wir wollen als Partner der Kommunen diese dabei unterstützen, dass Datenschutz zum echten Anliegen wird." Mit diesem Zitat des LfDI Dr. Brink begannen etliche Schulungen im kommunalen Bereich.

Vor diesem Hintergrund setzten wir im kommunalen Bereich seit Anfang des Jahres 2018 konsequent den Schwerpunkt auf Schulungen und Beratungen. So wurde in Kooperation mit der Verwaltungsschule Baden-Württemberg und der Württembergischen Verwaltungs- und Wirtschafts-Akademie (VWA) Schulungsreihen für Kommunen und behördliche Datenschutzbeauftragte angeboten. Erläutert wurden die wesentlichen Grundzüge des neuen Datenschutzrechts, ergänzt um praktische Tipps und Empfehlungen für die Umsetzung vor Ort sowie Erläuterungen der Rechtsauffassungen der Dienststelle. Neben den Gemeinden und Landratsämtern nutzten auch andere öffentliche Stellen das Schulungsangebot des LfDI.

Dabei gebe der LfDI eine echte Orientierung, so eine Teilnehmerin, die von diversen Schulungen berichten konnte, die im Moment angeboten werden. „Gut strukturiert, somit waren viele Informationen möglich, und obwohl nicht immer einfach, konnten Sie auf alle Fragen eingehen. Würde mich freuen, wenn es mehr dieser Art von Ihnen und unserer Aufsichtsbehörde gäbe", so die positive Rückmeldung eines Teilnehmers.

Die Anzahl von bisher über 1350 Teilnehmerinnen und Teilnehmern aus Gemeinden und Landkreisen zeigt, dass der Bedarf an verlässlicher Orientierung in der kommunalen Praxis hoch ist und Beratungs- und Schulungsangebote von Seiten der Aufsichtsbehörde auch als solche wahrgenommen und nachgefragt werden.

Obwohl die Anzahl der Eingaben seit dem Wirksamwerden der DS-GVO deutlich gestiegen ist, wurden nicht nur die Beratungs- und Schulungsangebote intensiviert, son-

dern auch der regelmäßige Austausch mit den kommunalen Landesverbänden zum Thema Datenschutz institutionalisiert. „Unser Ziel ist es, durch ein abgestimmtes Vorgehen mit den kommunalen Landesverbänden den Städten, Gemeinden und Landkreisen in Baden-Württemberg ein höheres Maß an Sicherheit im Bereich ihrer datenschutzrechtlichen Verantwortlichkeiten zu geben", so der LfDI. Nachgehalten werden die Beratungen durch eine strukturierte Veröffentlichung häufig gestellter Fragen in Form einer FAQ-Liste und weiteren Informationen, wie etwa Kurzpapieren der Datenschutzkonferenz oder eigenen Handreichungen und Mustervorlagen auf der Internetseite des LfDI, welche laufend aktualisiert werden.

1.1.3 Veranstaltungen und Hinweise

Unserem gesetzlichen Auftrag folgend haben wir nicht nur zahlreiche Informationsveranstaltungen organisiert und durchgeführt, aber auch umfangreiche Hinweise in gedruckter und elektronischer Form verfasst und bereitgestellt.

Hervorzuheben sind insbesondere neben vielen anderen drei Projekte:

- Im Januar 2018 haben wir sämtliche in Baden-Württemberg ansässigen Wirtschaftsauskunfteien und Inkassounternehmen zusammen mit der Verbraucherzentrale zu einem Vortrag eingeladen, bei dem die Auswirkungen der EU-Datenschutzgrundverordung für das Inkassowesen und die Speicherung und Beauskunftung von Kriterien, die für die Bewertung der Kreditwürdigkeit von Unternehmen und Einzelpersonen maßgeblich sind, erläutert wurden. Das betrifft insbesondere die Ermittlungstätigkeit der Inkassounternehmen bei der Geltendmachung einer Forderung, die Einmeldung von säumigen Schuldnern bei Auskunfteien, die Berechtigung, dort etwa vor der Vergabe von Kredit Bonitätsabfragen vornehmen zu dürfen, sowie die Problematik, wann besagte Informationen zu löschen sind. Die dabei zu beachtenden, aber nicht ganz einfach zu überschauenden Regelungen wurden in einem Hinweispapier zusammengefasst und den betroffenen Unternehmen, der Anwaltschaft, aber auch interessierten Bürgerinnen und Bürgern zur Verfügung gestellt.
- Besonderes Kopfzerbrechen scheint die EU-Datenschutzgrundverordnung den Vereinen zu bereiten (siehe auch unser Praxisratgeber für Vereine). Müssen jetzt alle Mitglieder eine Einwilligung in die Verarbeitung ihrer Daten durch den Verein abgeben? Wann dürfen Daten von Mitgliedern an Dachorganisationen übermittelt oder gar für Werbezwecke genutzt werden. Was darf der Presse in personenbezogener Form über Vereinsmitglieder offenbart werden? Solche und noch viele andere Fragen wurden an uns herangetragen mit der Folge, dass wird nicht nur umfassende Informationen über die datenschutzrechtlichen Rahmenbedingungen beim Umgang mit personenbezogenen Daten in der Vereinsarbeit erarbeiten und zur Verfügung stellen mussten, sondern auch zu einer Vielzahl von Vorträgen bei Vereinen als Redner eingeladen wurden.
- Im Sommer 2018 trat die IHK Region Mittlerer Neckar an uns heran, um gemeinsam mit uns eine Hinweisbroschüre herauszugeben, was diese bei der Verarbeitung personenbezogener Daten von Kunden und Geschäftspartnern entsprechend der Datenschutzgrundverordnung zu beachten haben. Interessant ist, welche Themen von den Geschäftsleuten als für sie interessant und wichtig benannt wurden, nämlich Datenschutz bei der Video-Überwachung, Auftragsverarbeitung, Datenschutz-Folgenabschätzung, Meldung von Datenpannen sowie der Beschäftigtendatenschutz. Auch der Datenschutz bei der Werbung und die Bestellung von betrieblichen Datenschutzbeauftragten sollte thematisiert werden. Aber eine

Problematik stand auch hier wieder im Vordergrund: wie müssen Datenschutzerklärungen bei Internetauftritten gestaltet sein, damit sie dem Datenschutzrecht genügen und der Betreiber der jeweiligen Homepage nicht Opfer von Abmahnanwälten wird.

Im Übrigen gibt es zahlreiche FAQs, Orientierungshilfen und Merkblätter zu nahezu allen relevanten datenschutzrechtlichen Themen. Sie können in Papierform bei unserer Behörde bezogen oder auf unserer Homepage abgerufen werden.

Wir hoffen, mit unserem Informationsangebot den Bürgerinnen und Bürgern den „Einstieg" in die EU-Datenschutzgrundverordnung erleichtert zu haben. Allerdings müssen wir unsere Bemühungen, stets aktuell zu sein, angesichts der rasanten Entwicklung in der Informationstechnologie unbedingt fortsetzen.

Die „Mammut-Aufgabe DS-GVO" kann nur gemeinsam mit den privaten und öffentlichen Verantwortlichen gelöst werden. Der LfDI nimmt hier seine Aufgabe als Berater und Informationsstelle immer umfangreicher wahr – und wird diesen Ansatz eines „gestaltenden Datenschutzes" auch in den kommenden Jahren weiter ausbauen.

1.2 Beratungspraxis zur Umsetzung der DS-GVO – Hauptfragen aus der Wirtschaft

Gegen Ende des Jahres 2017 stieg die Anzahl der Anfragen zur Umsetzung der DS-GVO sprunghaft an. Insbesondere kleine Familienbetriebe, Freiberufler und Selbständige traten mit sehr grundsätzlichen Fragen hinsichtlich der DS-GVO an den LfDI heran. Nicht selten ging es darum, was von diesem Regelwerk für kleine und mittlere Unternehmen überhaupt gelten würde. Oft wurde auch gefragt, was an Werbung künftig noch möglich sei. Zu einer gewissen Ratlosigkeit führten wohl auch die vielen teils unterschiedlichen Meinungen und Interpretationen bei Recherchen im Internet. Nicht immer zielführende Informationen von fachspezifischen Verbänden und Interessenvertretungen haben Unklarheiten leider eher noch verstärkt.

a) Was muss ich überhaupt aus der DS-GVO umsetzen?"

Sehr häufig hatten die Anfragen den Inhalt, in Erfahrung zu bringen, ob wirklich alles, was in der DS-GVO steht, für alle Stellen, hier insbesondere Unternehmen, gelten würde. Manche der Anfragen ließen leider auch den Eindruck zu, dass der Datenschutz vor dem Wirksamwerden der DS-GVO am 25. Mai 2018 eher ein Schattendasein geführt hat, sprich, dass der Datenschutz zu diesem Datum erst neu aufgestellt und organisatorisch eingeführt werden musste.

Die DS-GVO unterscheidet grundsätzlich nicht zwischen einem milliardenschweren, im Dax gelisteten Weltunternehmen und einer Fünf-Zimmer-Pension im Schwarzwald. Lediglich die Verarbeitung personenbezogener Daten für ausschließlich persönliche oder familiäre Tätigkeiten fällt nicht in den Anwendungsbereich der DS-GVO. Auch die Art der verarbeiteten Daten oder die Anzahl der verarbeiteten Datensätze spielen keine große Rolle.
Dies bedeutet, dass alle Stellen (Unternehmen, Selbständige, Behörden, Vereine usw.), die personenbezogene Daten verarbeiten, nach der DS-GVO ein Grundgerüst an Datenschutz und Datenschutzorganisation umsetzen müssen.

Hierzu gehören insbesondere folgende Punkte:

- Implementierung des Datenschutzes in die Organisation des Unternehmens
- Datenverarbeitung nur bei entsprechender Rechtsgrundlage oder Einwilligung des Kunden/Betroffenen
- Erarbeitung eines Verarbeitungsverzeichnisses nach Art. 30 DS-GVO

- Umsetzung der Informationspflichten nach Art. 13, 14 DS-GVO
- Prüfung, ob eine Datenschutz-Folgenabschätzung erforderlich ist
- Konzept hinsichtlich des Umgangs mit Datenpannen einschließlich der Meldepflicht gegenüber der Aufsichtsbehörde
- Umsetzung der Betroffenenrechte (z. B. Auskunft, Löschung, Berichtigung, Einschränkung der Verarbeitung, Werbewiderspruch)
- Management hinsichtlich des Umgangs mit Datenschutzbeschwerden
- Sicherheit der Datenverarbeitung
- Prüfung, ob ein Datenschutzbeauftragter zu benennen ist

Die wesentlichsten Themen werden nachfolgend noch genauer erläutert.

b) Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO

Wer muss ein Verzeichnis führen?
Prinzipiell muss jede Stelle, die personenbezogene Daten verarbeitet, ein Verarbeitungsverzeichnis führen. Die neue Regelung in Art. 30 DS-GVO verpflichtet nicht nur jeden Verantwortlichen im Sinne von Art. 4 Nr. 7 DS-GVO (hierzu zählen sowohl Behörden als auch z. B. Unternehmen, Freiberufler, Vereine), sondern nun auch die Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DS-GVO, ein Verzeichnis von Verarbeitungstätigkeiten, welche sie im Auftrag durchführen, zu erstellen und zu führen.
Gemäß Art. 30 Abs. 5 DS-GVO besteht eine Ausnahme für Stellen mit weniger als 250 Personen, sofern die Verarbeitung nur gelegentlich erfolgt. Praktisch sind uns jedoch bisher keine Unternehmen bekannt, die personenbezogene Daten nur gelegentlich verarbeiten. Allein die Personalverwaltung stellt – selbst bei kleinsten Unternehmen – bereits eine regelmäßige Verarbeitung dar. Auch die Verarbeitung von Kundendaten dürfte selbst in kleinsten Unternehmen regelmäßig vorkommen.

Was ist ein Verzeichnis von Verarbeitungstätigkeiten?
Gemäß Artikel 30 DS-GVO müssen alle Stellen, die personenbezogene Daten verarbeiten, ein Verzeichnis ihrer Verarbeitungstätigkeiten führen. In diesem werden die jeweiligen Verarbeitungstätigkeiten und weitere Informationen zusammengetragen und dargestellt. Das Verzeichnis von Verarbeitungstätigkeiten dient als wesentliche Grundlage für eine strukturierte Datenschutzdokumentation und hilft dem Verantwortlichen dabei, gemäß Art. 5 Abs. 2 DS-GVO nachzuweisen, dass die Vorgaben aus der DS-GVO eingehalten werden (Rechenschaftspflicht).

Was ist eine Verarbeitungstätigkeit?
Dieses Verzeichnis betrifft sämtliche ganz oder teilweise automatisierte Verarbeitungen sowie nicht-automatisierte Verarbeitungen personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Für jede einzelne Verarbeitungstätigkeit ist eine Beschreibung nach Maßgabe des Art. 30 DS-GVO anzufertigen. Als Verarbeitungstätigkeit wird im Allgemeinen ein spezieller, eigenständiger Geschäftsprozess verstanden. Es ist ein strenger Maßstab anzulegen, so dass jeder neue Zweck der Verarbeitung eine eigene Verarbeitungstätigkeit darstellt. Was konkret eine Verarbeitungstätigkeit ist, hängt vom jeweiligen Unternehmen ab. In einem kleinen Unternehmen mit wenigen Mitarbeitern kann z. B. die gesamte Personalverwaltung (inkl. Bewerbungsverfahren und Lohnabrechnung) als eine einzige Verarbeitungstätigkeit gesehen werden. Bei einem mittleren Unternehmen sollte eine stärkere Untergliederung stattfinden, z. B. in Personalgewinnung, Personaleinstellung, Verwaltung des aktuellen Personals, Beendigung der Arbeitsverhältnisse und ähnliche Verarbeitungstätigkeiten. In einem großen Unternehmen können allein in der Personalabteilung dutzende oder gar hunderte Verarbeitungstätigkeiten vorliegen, wenn z. B. unterschiedliche Bewerbungsverfahren für Ferienjobber, Werkstudierende, Auszubildende, mittlere

Angestellte, Führungskräfte und Top-Manager bestehen.

Wozu dient ein Verzeichnis der Verarbeitungstätigkeiten?
Das Verzeichnis der Verarbeitungstätigkeiten dient einerseits dazu, der verantwortlichen Stelle einen Überblick über die eigene Datenverarbeitung zu geben. Dadurch soll verhindert werden, dass personenbezogene Daten in einer Weise verarbeitet werden, die rechtswidrig ist oder u. U. schlicht nicht im Interesse der jeweiligen Stelle liegt. Durch die strukturierte Erhebung des Ist-Zustandes können auch mögliche Probleme (z. B. fehlende Sicherungsmaßnahmen) besser erkannt werden. Das Verzeichnis dient so dem dokumentierten Überblick über die eigene Datenverarbeitungstätigkeit.

Andererseits stellt das Verzeichnis im Falle einer Kontrolle einen ersten Überblick für die Aufsichtsbehörden dar. Auch bei Gerichtsverfahren kann es zur Entlastung beitragen.

Außerdem erleichtert ein genau geführtes Verzeichnis die Erstellung von Hinweisen nach Art. 13 und 14 DS-GVO ungemein, da viele Informationen im Verarbeitungsverzeichnis auch in diesen Datenschutzhinweisen dargestellt werden müssen.

Wie soll das Verzeichnis geführt werden?
Ein Verarbeitungsverzeichnis muss schriftlich geführt werden. Dies kann elektronisch oder auf Papier geschehen. Auf der Internetseite des LfDI ist ein Muster für eine Loseblattsammlung veröffentlicht, das verwendet werden kann. Auch eine tabellarische Auflistung der Verarbeitungstätigkeiten ist denkbar.

Welche Inhalte sind wichtig?
Die Informationen, die für jede Verarbeitungstätigkeit erhoben werden müssen, sind in Artikel 30 Abs. 1 und 2 DS-GVO aufgeführt. Sie sind auch aus dem o. g. Muster erkennbar. Wenn sich Informationen wiederholen, sollten diese gesondert dargestellt werden. Das wäre z. B. bei einem IT-Sicherheitskonzept der Fall, das ja alle elektronisch verarbeiteten Daten betrifft. Art. 30 Abs. 1 Buchstabe g und Art. 30 Abs. 2 Buchstabe d DS-GVO geben vor, dass das Verzeichnis, wenn möglich, auch eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DS-GVO enthalten soll. Wie detailliert diese Beschreibung sein muss, lässt sich der DS-GVO nicht unmittelbar entnehmen.

Und was soll man dann mit dem Verzeichnis machen?
Wenn das Verarbeitungsverzeichnis fertiggestellt ist, können aus ihm die Informationspflichten nach Art. 13 und 14 DS-GVO erarbeitet werden. Die Inhalte im Verzeichnis und in den Datenschutzhinweisen sind in weiten Teilen deckungsgleich.
In der Folge ist es sinnvoll, das Verarbeitungsverzeichnis zumindest einmal jährlich zu überprüfen und ggf. zu aktualisieren.

c) Informationspflichten nach Art. 13, 14 DS-GVO
Durch die Artikel 13 und 14 DS-GVO sind verantwortliche Stellen verpflichtet, die betroffene Person (z. B. den Kunden) über die Art und Weise ihrer Datenverarbeitung zu informieren. Derartige Informationen kennt man bereits von den bisherigen Datenschutzerklärungen auf Internetseiten, wo über Cookies, Analyse- und Trackingprogramme, Social-Media-Plugins und ähnliches informiert wird. Nach der DS-GVO sind ähnliche Informationen nun jedoch auch über „analoge" Datenverarbeitungen zur Verfügung zu stellen. Diese Informationen werden „Datenschutzhinweise" genannt. Adressaten dieser Informationen sind beispielsweise Kundinnen und Kunden oder Mitarbeiterinnen und Mitarbeiter von Unternehmen. Während für kleine Unternehmen eine einzige Information für alle Adressaten sinnvoll sein kann, sollten größere Unternehmen auf unterschiedliche Gruppen angepasste Informationen bereitstellen.

Grundsätzliche Regelungen
Die DS-GVO stellt in Artikel 12 grundsätzlich dar, dass Personen, deren personenbezogene Daten verarbeitet werden, über diese Verarbeitung informiert werden müssen. Damit soll verhindert werden, dass „hinter dem Rücken der Betroffenen" Daten verarbeitet werden und die betroffene Person deshalb nichts dagegen unternehmen kann. Der Verordnungstext fordert eine Information in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache". Jede Person soll verstehen, was mit ihren Daten geschieht.

Diese hohen Anforderungen an die Information werden in Artikel 13 und 14 DS-GVO im Hinblick auf die Datenschutzhinweise konkretisiert. Sie sollen den Betroffenen in eine informierte Situation versetzen, in der er nachvollziehen kann, wer seine Daten wann, wo, für welche Art und Weise der Verarbeitung und für welche Zwecke erhoben hat. Durch diese Kenntnis wird der Betroffene dazu befähigt, seine Betroffenenrechte auszuüben. Wird der Schutz seiner personenbezogenen Daten verletzt, kann er in dieser informierten Lage gezielt um Rechtsschutz ersuchen.

Artikel 13 und 14 DS-GVO gelten für Online-Datenverarbeitungen (z. B. auf Internetseiten) ebenso wie für analoge Datenverarbeitungen.

Da es unzählige, unterschiedlich ausgestaltete Konstellationen gibt, in denen der Betroffene informiert werden muss, gibt es kein allgemeines, standardisiertes Informationsblatt, durch das diese Hinweispflichten in allen denkbaren Fällen erfüllt werden können. Auch bei gleichgelagerten Fällen wie beispielsweise der Information des Betroffenen auf einer Internetseite kann je nach konkret eingebundenen Applikationen wie Cookies oder Trackingtools von mehreren verantwortlichen Stellen über unterschiedliche Punkte zu informieren sein. Die konkrete Ausgestaltung der Informationen muss daher von jeder verantwortlichen Stelle für den konkreten Anwendungsfall geprüft werden.

Hierfür sind die relevanten Datenverarbeitungsprozesse für personenbezogene Daten im Unternehmen zu sichten und im Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DS-GVO zu erfassen. Im nächsten Schritt sind die Anwendungsfälle in den unternehmerischen Prozessen zu erfassen, in denen standardisiert personenbezogene Daten verarbeitet werden. Ein solcher Anwendungsfall ist beispielsweise die Beantwortung von Kundenanfragen nach Angeboten. Die Bestandteile der Hinweise nach Art. 13 und 14 DS-GVO überschneiden sich in weiten Teilen mit den im Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DS-GVO aufgeführten Punkten.

Direkte und indirekte Datenerhebung
Die Frage, ob nach Artikel 13 oder nach Artikel 14 DS-GVO informiert werden muss, richtet sich nach der Art, wie (bzw. wo) die Daten erhoben werden.

Wenn die Daten direkt beim Betroffenen erhoben werden (etwa im Rahmen eines Kauf-, Werk- oder Dienstleistungsvertrags; z. B. indem der Kunde selbst ein Formular ausfüllt), muss nach Artikel 13 DS-GVO informiert werden.

Wenn die Daten jedoch bei einer dritten Stelle erhoben werden, muss nach Artikel 14 DS-GVO informiert werden. Eine dritte Stelle ist z. B. ein Adresshändler, der eine Adresse an ein anderes Unternehmen vermietet. In einem solchen Fall erfährt der Betroffene normalerweise erst durch die Information von der Speicherung seiner Daten bei der verarbeitenden Stelle. Daher fordert Artikel 14 DS-GVO auch mehr Informationen als Artikel 13 DS-GVO. Eine Datenerhebung über eine Suche im Internet fällt auch unter Art. 14 DS-GVO.

Zeitpunkt und Art der Information
Nach Art. 13 DS-GVO ist der Betroffene im Zeitpunkt der Datenerhebung zu informieren. Dies kann z. B. durch einen Aufdruck auf dem Formular, in das die Daten

eingetragen werden, geschehen. Sofern kein Formular verwendet wird, sollte dem Betroffenen ein schriftlicher Ausdruck der Datenschutzhinweise angeboten werden. In Geschäftsräumen kommt auch ein Aushang an geeigneter Stelle in Betracht.

Wenn die Daten nicht direkt bei dem Betroffenen erhoben werden, ist nach Art. 14 DS-GVO ebenfalls eine Information vorgeschrieben. Diese muss nach Art. 14 Abs. 3 DS-GVO möglichst schnell, spätestens aber innerhalb eines Monats geschehen. Wenn der Betroffene bereits vor Ablauf der Frist kontaktiert wird oder die Daten an einen weiteren Empfänger weitergegeben werden sollen, muss die Information entsprechend früher erfolgen.

Es ist u.U. möglich, dass die Daten zu einem anderen Zweck verarbeitet werden sollen als zu dem, für den sie ursprünglich erhoben wurden (Zweckänderung). In einem solchen Fall muss vor der neuen Verarbeitung ebenfalls über diese Zweckänderung informiert werden.

Die Information muss in jedem Fall leicht zugänglich und verständlich erteilt werden. Wenn der Betroffene die jeweiligen Informationen bereits erhalten hat (z. B. weil er sie bei seinem letzten Besuch gelesen hat), kann eine erneute Information entfallen.
Der Betroffene muss die Information auch nicht unterschreiben oder anerkennen. Es ist jedoch Aufgabe der verantwortlichen Stelle, nachzuweisen bzw. zu dokumentieren, dass der Betroffene zumindest die Möglichkeit hatte, die Informationen zu erhalten. Auch ist es nicht zulässig, dass in den Informationen bestimmte „Freibriefe" für eine weitergehende Datenverarbeitung versteckt werden.

Medienbrüche sind grundsätzlich zulässig. Ein Medienbruch entsteht immer dann, wenn die Datenerhebung in einer anderen Form durchgeführt wird als die Übermittlung der Datenschutzhinweise. Bspw. können Daten telefonisch erhoben werden, die Informationen dann aber im Anschluss per Brief zugeschickt werden. Es ist aber wichtig, dass durch den Medienbruch keine Informations-Barriere entsteht. Dies wäre der Fall, wenn die betroffene Person spezielle technische Geräte benötigt, um die Information einzusehen. Auch der in der Briefpost enthaltene Verweis auf eine Internetseite kann im Zweifel zu einer Erschwernis führen. Wird in elektronischen Dokumenten auf eine Internetseite verlinkt, ist dies hingegen unbedenklich.

Beispiele

Fall 1 / Messekontakte:
Ein Unternehmen bedient einen Stand auf einer Wirtschaftsmesse. Gemäß dem üblichen Geschäftsgebaren hinterlassen Besucher des Standes in einer dort aufgestellten Box ihre Visitenkarten, um weitere Informationen über Produkte des Unternehmens zu erhalten. Die auf den Visitenkarten enthaltenen Informationen werden unternehmensintern in eine Geschäftskontakteliste eingepflegt.

- Fall der Direkterhebung, Art. 13 DS-GVO.
- Die Rechtsgrundlage der Datenverarbeitung ergibt sich hier aus der (freiwilligen) Herausgabe der Visitenkarte als eindeutig und schlüssig in die Datenverarbeitung einwilligendes Verhalten.
- In diesem Fall sind dem Betroffenen die relevanten Informationen weitgehend bekannt, da er mit dem Geschäftsgebaren vertraut ist. Die Führung der unternehmensinternen Kontaktlisten ist allgemein bekannt.
- Die Datenschutzhinweise sollte der Verantwortliche durch Aushänge am Messestand an der Stelle, an der die Visitenkarten abgegeben werden, geben.

Fall 2 / Bewerberakquise auf Firmenmessen:
Auf einer Firmenmesse werden potentielle Bewerber angesprochen und nach ihren persönlichen Daten und ihrem Lebenslauf gefragt. Die Daten dieser Personen werden in eine Firmendatenbank der Personalabteilung eingepflegt.

- Fall der Direkterhebung, Art. 13 DS-GVO.
- Bezüglich der Rechtsgrundlage ist auf eine informierte ausdrückliche Einwilligung zu achten. Aus Nachweisgründen sollte diese schriftlich erfolgen.
- Die betroffene Person ist hier umfassend zu informieren. Dies kann durch ein standardisiertes ausführliches Informationsblatt geschehen, da allen potentiellen Bewerbern die gleiche Behandlung zuteil wird.
- Hierbei ist wichtig, dass auch das Löschkonzept des Verantwortlichen in der Erklärung zum Ausdruck kommt. Die Daten sollten spätestens ein Jahr nach Aufnahme wieder aus der Firmendatenbank entfernt werden.

Fall 3 / Zuliefererlisten:
Ein Unternehmen benötigt für die Herstellung seiner Produkte eine bestimmte Art von Sensoren. Um in jedem möglichen Fall mit den notwendigen Bestandteilen für das zu erstellende Produkt versorgt zu sein, speichert sich das Unternehmen alle potentiellen Zulieferer in einer Liste ab. Neben den Kontaktdaten des Unternehmens stehen auch konkrete Ansprechpartner (= Personenbezug) auf diesen Listen. Die Listen ergänzt das Unternehmen um öffentlich im Internet zugängliche Daten.

- Fall der Dritterhebung, Art. 14 DS-GVO.
- Information kann nachgelagert im Zeitpunkt der ersten Kontaktaufnahme erfolgen, Art. 14 Abs. 3 Buchstabe b DS-GVO, aber spätestens nach einem Monat.
- Es empfiehlt sich für die Kontaktaufnahme mit Kontakten von dieser Liste, ein entsprechendes Briefpapier oder eine E-Mail-Vorlage mit entsprechenden Datenschutzhinweisen zu verwenden.

Fall 4 / Informationen im Bewerbungsverfahren:
Eine Mitarbeiterstelle wird elektronisch durch ein entsprechendes Inserat ausgeschrieben. Es besteht ein Online-Kontaktformular, in das der Bewerber seine Daten eintragen kann.

- Fall der Direkterhebung, Art. 13 DS-GVO
- Auch bei der Eintragung von Daten in ein elektronisches Kontaktformular ist trotz der Mitwirkung der betroffenen Person ein Erheben gegeben.
- Während des gesamten Eintragungsprozesses sollte die Datenschutzerklärung mit den Informationen nach Art. 13 DS-GVO optisch sichtbar und beispielsweise durch einen speziellen Button aufrufbar sein.
- Hinweis: Auch ohne das Bestehen des elektronischen Kontaktformulars wäre die betroffene Person im Zeitpunkt der Stellenausschreibung gemäß Art. 13 DS-GVO zu informieren.

Fall 5 / Allgemeine Information auf Internetseiten:
Ein Blogger betreibt eine Website. Welche speziellen Informationsangaben muss er neben den allgemein durch Art. 13 DS-GVO vorgegebenen Angaben im Zweifelsfall machen?

- Fall der Direkterhebung, Art. 13 DS-GVO.
- Zusätzlich zu den auch in anderen Anwendungsfällen erforderlichen Informationen an den Betroffenen über die Umstände der Datenverarbeitung ist in diesem speziellen Fall je nach Ausgestaltung der Website und der Verwendung von weiteren Anwendungen über folgende Punkte zu informieren:
  * Einbindung von Cookies (auch Drittanbieter!)
  * Analyseprogramme (z. B. Einbindung von Google Analytics)
  * Einbindung von Social-Media-Plugins – Doppel-Klick-Lösung / Sichere Einbindung!
  * Weitergabe von Daten im Fall von Werbung

Fall 6 / Ungefragte Zusendung von Angebotsanfragen:
Ein potentieller Kunde schickt einem Unternehmen (ohne vorher mit diesem Kontakt gehabt zu haben) die Bitte um ein Angebot. Das Unternehmen nimmt den Kontakt

zu seinem Kundenbestand und versendet ein entsprechendes Angebot auf elektronischem Weg.

- Fall der Direkterhebung, Art. 13 DS-GVO.
- Sobald die Anfrage in das System aufgenommen wird, gilt sie als erhoben.
- Es empfiehlt sich, für die ausgehende Antwort mit dem konkreten Angebotsinhalt ein entsprechendes Briefpapier oder eine E-Mail-Vorlage mit Hinweisen auf die Informationspflichten zu verwenden. Die Mitarbeiter sind in einem solchen Fall anzuweisen, nur diese Vorlagen zu benutzen.

Fall 7 / Telefonanruf:
Ein möglicher Kunde ruft bei einem Unternehmen an. Der den Anruf annehmende Mitarbeiter pflegt personenbezogene Daten in die automatisierte Kundendatenbank ein.

- Fall der Direkterhebung, Art. 13 DS-GVO.
- Im Fall einer Telefonhotline kann mit standardisierten Bandansagen gearbeitet werden, die die entsprechenden Informationen auf Wunsch (per Eingabe einer bestimmten Ziffer, auf die zuvor hingewiesen wurde) ermöglichen.
- Ansonsten ist auf die automatisierte Datenverarbeitung mündlich hinzuweisen, soweit dem Betroffenen die Umstände im konkreten Fall nicht bereits bekannt sind. Ein mündlicher Verweis auf ausführliche Informationspflichten auf der Homepage ist möglich.

d) Identifizierung der betroffenen Person bei der Geltendmachung des Auskunftsanspruchs nach Art. 15 DS-GVO

Die DS-GVO sieht ein Auskunftsrecht für betroffene Personen vor. So ist in Artikel 15 geregelt, dass jede betroffene Person das Recht hat, vom Verantwortlichen eine Bestätigung zu erhalten, ob und wenn ja, welche ihrer personenbezogenen Daten verarbeitet werden. Welche Art von Daten ihr mitgeteilt werden müssen und weitere Einzelheiten sind in diesem Artikel ebenfalls geregelt. Ein wesentliches Problem dabei: Woher weiß bei solchen Anfragen der Verantwortliche, dass die anfragende Person tatsächlich die betroffene ist?

Das Recht auf Auskunft betrifft nur die eigenen personenbezogenen Daten (sog. Recht auf Selbstauskunft). Hierzu wendet sich der Anfragende an den Verantwortlichen und stellt einen Antrag nach Artikel 15 DS-GVO. In einem ersten Schritt muss der Verantwortliche prüfen, ob bei ihm überhaupt personenbezogene Daten des Anfragenden gespeichert sind; trifft dies zu, so muss er im zweiten Schritt dem Anfragenden eine Reihe von Informationen geben, die in diesem Artikel abschließend aufgezählt werden (sog. zweistufiges Verfahren).

Schon vor der Prüfung, ob Daten des Anfragenden verarbeitet werden, muss sich der Verantwortliche vergewissern, dass der Anfragende auch der Betroffene ist. Denn nur diesem gegenüber muss und darf der Verantwortliche Auskunft geben. Das bedeutet umgekehrt: Der Anfragende muss dem Verantwortlichen gegenüber belegen, dass er berechtigt ist, diese Daten zu erhalten, er muss sich also identifizieren. Hat der Verantwortliche begründete Zweifel an der Identität, so kann er zusätzliche Informationen anfordern, die zur Bestätigung der Identität des Anfragenden erforderlich sind (Artikel 12 Absatz 6 DS-GVO).

Der Anspruch auf Auskunft ergibt sich aus dem Grundsatz der Transparenz (Artikel 5 Absatz 1 Buchst. a DS-GVO und dazugehöriger ErwGr. 39 DS-GVO), wonach betroffene Personen jederzeit erfahren können sollen, welche ihrer personenbezogenen Daten wie verarbeitet wurden und (zukünftig) werden, ob sie und ggf. an wen weitergegeben werden (sollen) oder wurden. Diese Informationen müssen leicht zugänglich sowie verständlich und in klarer und einfacher Sprache abgefasst sein (vgl. hierzu auch Artikel 12 Absatz 1 DS-GVO).

Je nachdem, auf welchem Weg bzw. in welcher Konstellation die Anfrage nach Art. 15 DS-GVO erfolgt, ergeben sich unterschiedliche Möglichkeiten der Identitätsprüfung:

1. **Bislang keinerlei (Vor-)Kontakt**
   Dies ist oberflächlich betrachtet die einfachste Fallgestaltung, denn wenn keine personenbezogenen Daten verarbeitet werden, können auch keine Angaben zu gespeicherten Daten gemacht werden. Der Verantwortliche ist hier aber genauso wie im umgekehrten Fall verpflichtet, sorgfältig zu prüfen, ob Daten des Anfragenden gespeichert sind. Ist er im Zweifel, kann er vom Anfragenden verlangen, dass dieser „präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich" (ErwGr. 63 DS-GVO) sein Auskunftsersuchen bezieht. Der Verantwortliche muss sicherstellen, dass der Anfragende auch der Auskunftsberechtigte ist. Hat der Verantwortliche begründete Zweifel an der Identität, so kann er zusätzliche Informationen anfordern, die zur Bestätigung der Identität des Anfragenden erforderlich sind (Artikel 12 Absatz 6 DS-GVO). Dazu kann der Betroffene eine Ausweiskopie übersenden; er ist darauf hinzuweisen, dass nicht benötigte Einträge in der Kopie geschwärzt werden sollten; erforderlich sind in jedem Fall folgende Angaben: Vorname, Name und vollständige Anschrift. Ist die Identität eindeutig festgestellt worden und sind keinerlei personenbezogene Daten des Anfragenden aufzufinden, so muss sodann eine sog. „Negativauskunft" gegeben werden (vgl. Artikel 15 Absatz 1 Satz 1 DS-GVO: „... zu verlangen, ob … personenbezogene Daten verarbeitet werden. …"), also bestätigt werden, dass keine personenbezogenen Daten des Anfragenden verarbeitet werden.

2. **Auskunftsbegehren per Brief**
   Die Situation ist hier recht unkompliziert zu handhaben: Der Antragsteller gibt in seinem Schreiben die komplette Adresse an. Damit ist im Regelfall ein Vergleich mit den gespeicherten Daten möglich; bei Übereinstimmung der Anschrift kann davon ausgegangen werden, dass der Anfragende die betroffene Person ist. Falls möglich, kann der Verantwortliche die Angabe der Kundennummer, des Aktenzeichens, einer Referenznummer, ein Buchungszeichen o. Ä. verlangen. In Zweifelsfällen könnte noch das Geburtsdatum erfragt werden. Ist bei den gespeicherten Daten eine Telefonnummer hinterlegt, wäre auch dies eine weitere Möglichkeit der Identifizierung, wenn auch nicht die einzige. Eine weitere Möglichkeit ist das PostIdent-Verfahren, in dessen Verlauf die Identität durch Vorlage eines Personalausweises oder Reisepasses nachgewiesen wird. Die Auskunft sollte schriftlich gegeben werden, um die Gefahr von Fehlsendungen zu verringern. Als Adresse wäre die bekannte, also die beim Verantwortlichen gespeicherte zu verwenden; die sicherste Versandart sind Einschreiben eigenhändig oder Schreiben per Postzustellungsurkunde.

3. **Auskunftsbegehren per E-Mail**
   Wurde bereits zuvor Kontakt per E-Mail gepflegt, so kann die Überprüfung der E-Mail-Adresse bereits einen Hinweis auf die Identität des Anfragenden geben. Bei der Bearbeitung einer solchen Anfrage ist zu beachten, dass die Auskunft nur dann elektronisch erteilt werden darf, wenn die anfragende Person belegt, dass sie berechtigt ist, über die angegebene E-Mail-Adresse für sie bestimmte Informationen zu empfangen. Möglich ist das z. B. mittels eines elektronischen Vertrauensdienstes nach der eIDAS-Verordnung. In Frage kommende Vertrauensdienste sind etwa die qualifizierte elektronische Signatur, De-Mail bzw. die eID-Funktion des elektronischen Personalausweises. Eine Alternative für den Nachweis, Inhaber des Auskunftsanspruchs zu sein, wäre die Übermittlung eines gescannten amtlichen Ausweises auf elektronischem Wege. Hierbei muss allerdings sichergestellt sein, dass die betroffene Person die Möglichkeit

hat, den Scan des amtlichen Ausweises über eine gesicherte Verbindung (z. B. per E-Mail-Verschlüsselung oder über eine HTTPS-gesicherte Website) zu übermitteln. Auch hier gilt: Nicht benötigte Daten auf dem Scan sollten vom Betroffenen geschwärzt werden. Bei einem hohen Schutzbedarf der Daten in der Selbstauskunft sind ebenfalls entsprechende Maßnahmen zur Wahrung der Vertraulichkeit und Integrität der Daten beim elektronischen Versand an die betroffene Person zu treffen. In Frage kommt etwa die Bereitstellung über ein zugangsgesichertes Online-Portal oder die Übermittlung als verschlüsseltes PDF-Dokument. Das Passwort zum Einloggen bzw. Öffnen der Datei sollte über einen unabhängigen Kanal, etwa telefonisch, mitgeteilt werden.

4. Auskunftsbegehren per Telefon…

- … im unmittelbaren Anschluss an z. B. eine Bestellung oder ein Telefonat in einer anderen, konkreten Angelegenheit: Erscheint es dem Verantwortlichen anhand des vorangegangenen Telefonats plausibel, dass der Anrufende berechtigt ist, die gewünschten Informationen zu erhalten, so können sie telefonisch gegeben werden. Dies sollte allerdings der Ausnahmefall sein. Die gegebene Auskunft muss schriftlich dokumentiert werden, da ansonsten kein Nachweis möglich ist.
- … eines gut bekannten Kunden: Auch hier muss die Identität geprüft werden. Ist z. B. die Telefonnummer des Kunden bereits bekannt, so kann dies anhand der Rufnummernanzeige am Telefon oder durch einen Rückruf des Verantwortlichen beim Kunden geschehen. Ausnahmsweise kann diese Art der Identitätsprüfung ausreichen. Die Prüfung samt Ergebnis, die Tatsache, dass Auskunft erteilt wurde, sowie die Inhalte der Auskunftserteilung muss der Verantwortliche als Nachweis dokumentieren.
- … ohne weiteren Zusammenhang: Eine Identifizierung am Telefon ist noch schwieriger als bei einer E-Mail. Der Anfragende sollte daher auf den Postweg verwiesen werden. Auf diese Weise ist auch der Nachweis über die gegebene Auskunft leichter zu führen.

Auskunftsersuchen telefonisch zu beantworten, stellt den Verantwortlichen schon allein aufgrund der vielen Informationen, die er nach Artikel 15 DS-GVO zu geben hat, vor Probleme; andererseits stellt die Fülle an Informationen auch für den Anfragenden eine große Herausforderung dar, muss er sich doch alles merken und hat keine Gelegenheit, nochmals in aller Ruhe alles nachzulesen. Die telefonische Auskunftserteilung sollte aus diesen Gründen nur eine Ausnahme sein. Es bleibt dem Verantwortlichen unbenommen, die Auskunft nach dem Telefonat zusätzlich schriftlich zu geben.

5. Auskunftsbegehren per persönlichem Erscheinen

Ist der Anfragende bereits persönlich bekannt, so ist eine Identitätsprüfung nicht mehr erforderlich. Ist der Anfragende nicht persönlich bekannt, so kann er sich durch Vorlage seines Personalausweises bzw. Reisepasses oder eines anderen geeigneten Dokuments identifizieren. In beiden Fällen muss die Auskunftserteilung vom Verantwortlichen schriftlich dokumentiert werden, wobei die Tatsache „persönlich bekannt" bzw. „ausgewiesen durch …" festgehalten werden muss. Die Anfertigung einer Ausweiskopie für Dokumentationszwecke ist weder erforderlich noch zulässig. Es genügt, in der Dokumentation Teile der Ausweisnummer (etwa die vier letzten Buchstaben/Ziffern) zu notieren. Die Auskunft kann auch – zusätzlich zur mündlich erteilten – im Nachgang schriftlich erfolgen.

Allgemeines

Des Weiteren sind die folgenden Punkte zu beachten:

- Handelt es sich bei den gespeicherten Daten um besonders sensible Daten

(z. B. nach Art. 9 DS-GVO), so muss die Anforderung an eine fehlerfreie Identifizierung so hoch gelegt werden, wie der Aufwand hierzu noch vertretbar ist. Im gegenteiligen Fall, wenn es z. B. im Fall von Adresshändlern „nur" um gespeicherte Anschriften geht, genügen postalische Anfragen mit Angabe der vollständigen Anschrift; der Maßstab ist hier niedriger anzulegen.

- Handelt es sich um personenbezogene Daten, die im Rahmen eines Onlineshops gespeichert wurden, kann als ein Identifizierungsmerkmal auch das Pseudonym, unter dem sich der Anfragende angemeldet hat, oder der Benutzername erfragt werden (niemals jedoch das Passwort!).
- Eine Kopie des Personalausweises oder Reisepasses war bis vor kurzem nur eingeschränkt zulässig. Eine Änderung des Personalausweisgesetzes (§ 20 Absatz 2) bzw. des Passgesetzes (§ 18 Absatz 3) ermöglicht jetzt jedoch, dass der Inhaber selbst Kopien fertigen und weitergeben darf. Zu beachten ist in jedem Fall: Die Kopie muss eindeutig und dauerhaft als Kopie gekennzeichnet sein. Sie muss im Einzelfall erforderlich sein, häufig genügt es, zum Nachweis der Vorlage des Ausweises Teile der Ausweisnummer (etwa die vier letzten Buchstaben/Ziffern) zu notieren. Der Verantwortliche darf sie nur zur Identitätsprüfung verwenden und muss sie sofort danach vernichten, darf sie also keineswegs speichern. Nicht benötigte Angaben müssen geschwärzt sein; hierauf muss der Verantwortliche hinweisen.

  Die Kopie der Vor- und Rückseite könnte beispielsweise so aussehen:

Quelle: https://de.wikipedia.org/wiki/Personalausweis_(Deutschland)

- Bleiben begründete Zweifel über die Identität bestehen und wird deshalb keine Auskunft gegeben, so muss dies der Verantwortliche dokumentieren, um später nachweisen zu können, warum keine Auskunft erteilt wurde.
- Der Verantwortliche ist nach Artikel 5 Absatz 2 DS-GVO verpflichtet, nachzuweisen, dass er alle datenschutzrechtlichen Vorschriften einhält. Aus dieser Verpflichtung rührt z. B. die Führung des Verarbeitungsverzeichnisses oder eben auch der Nachweis darüber, dass und wie, mit welchem Ergebnis das zweistufige Verfahren zur Auskunftserteilung durchgeführt wurde.
- Der Verantwortliche muss bei jeder Auskunft im Rahmen der Möglichkeiten und nach Sensibilität der gespeicherten Daten handeln. Eine falsch oder unvollständig erteilte oder eine verfristete (Artikel 12 Absatz 3 DS-GVO) Auskunft kann genauso wie eine zu Unrecht nicht erteilte oder an die falsche Person erteilte Auskunft nach Artikel 83 Absatz 5 Buchst. b DS-GVO zu einem bußgeldbewehrten Ordnungswidrigkeitenverfahren führen.

Der Anfragende muss belegen, dass es sich bei seiner Anfrage um „seine" personenbezogenen Daten handelt. Der Verantwortliche muss seinerseits alle vertretbaren Mittel nutzen, um die Identität des Anfragenden sicher festzustellen.

Erfahrungsgemäß sind die Angabe von Vorname, Name, vollständiger Anschrift, falls vorhanden der Kundenummer o. Ä. in den meisten Fällen ausreichend. Nur

als ultima ratio kann eine Kopie des Personalausweises angefordert werden; der Anfragende muss in diesem Fall allerdings darauf hingewiesen werden, dass er nicht benötigte Angaben schwärzen sollte. Lässt sich die Identität nicht zweifelsfrei belegen, so muss die Auskunftserteilung mit einer entsprechenden Begründung abgelehnt werden.

e) Werbung

Mit der DS-GVO sind alle detaillierten Regelungen des bisherigen Bundesdatenschutzgesetzes (BDSG) zur Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung weggefallen (siehe bisher insbesondere § 28 Abs. 3 und 4 sowie § 29 BDSG-alt).

Eine werbliche Ansprache ist seit dem 25. Mai 2018 datenschutzrechtlich zulässig, wenn

- eine konkrete und informierte Einwilligung des Beworbenen (Kunden) nach Art. 6 Abs. 1 Satz 1 Buchstabe a DS-GVO in die konkrete Werbung vorliegt oder
- eine Interessenabwägung nach Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO – auch unter Einbeziehung der Regelungen von § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG) – zugunsten des Werbenden ausgeht.

1. Einwilligung

Die Einwilligung ist als eine Rechtmäßigkeitsvoraussetzung für die Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 Satz 1 Buchstabe a DS-GVO nur wirksam, wenn sie freiwillig und – bezogen auf einen bestimmten Fall – informiert abgegeben wird. Informiert setzt voraus, dass auch die Art der beabsichtigten Werbung (Brief, E-Mail/SMS, Telefon, Fax), die Produkte oder Dienstleistungen, für die geworben werden soll, und die werbenden Unternehmen genannt werden, um den Transparenzanforderungen von Art. 12 Abs. 1 und Art. 13 Abs. 1 Buchstabe c DS-GVO sowie der bisher insoweit ergangenen Rechtsprechung zu genügen. Erforderlich ist nach Art. 4 Nr. 11 und Art. 7 Abs. 2 DS-GVO eine unmissverständlich abgegebene Willensbekundung in Form einer Erklärung in einer klaren und einfachen Sprache oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person ihr Einverständnis zur Verarbeitung der sie betreffenden Daten erteilt.

Die Schriftform für datenschutzrechtliche Einwilligungen sieht die DS-GVO nicht als Regelfall vor.

Verantwortliche haben allerdings gemäß Art. 5 Abs. 2 DS-GVO die Einhaltung der Rechtmäßigkeitsvoraussetzungen der Datenverarbeitung und gemäß Art. 7 Abs. 1 DS-GVO auch speziell das Vorliegen einer Einwilligung nachzuweisen. Um dieser Verpflichtung nachkommen zu können, ist den Verantwortlichen anzuraten, sich regelmäßig um eine Einwilligung in Schriftform mit handschriftlicher Unterschrift oder mindestens in Textform (z. B. E-Mail) zu bemühen.

Für Einwilligungen ist ein gesonderter Text oder Textabschnitt ohne weiteren anderen Inhalt zu verwenden. Soll sie zusammen mit anderen Erklärungen (insbesondere vertraglichen Erklärungen) schriftlich oder in einem elektronischen Format erteilt werden, so ist die datenschutzrechtliche Einwilligungserklärung gemäß Art. 7 Abs. 2 Satz 1 DS-GVO in einer von anderen Sachverhalten klar unterscheidbaren Weise darzustellen.

Für das elektronische Erklären einer Einwilligung ist – zur Verifizierung der Willenserklärung der betroffenen Person – das Double-Opt-In-Verfahren geboten (je nach konkreter Art des Kontaktes: E-Mail oder SMS), wobei die Nachweis-Anforderungen des Art. 5 Abs. 2 DS-GVO und des BGH (Urteil vom 10. Februar 2011, I ZR 164/09) bei der Protokollierung zu berücksichtigen sind. Das bloße Abspeichern der IP-Adressen von Anschlussinhabern und die Behauptung, dass von diesen eine Einwilligung vorliege, genügen dem

BGH nicht. Der Nachweis der Einwilligung erfordert mehr, z. B. die Protokollierung des gesamten Opt-In-Verfahrens und des Inhalts der Einwilligung.

2. Interessenabwägung

Nach Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO muss die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich sein, sofern nicht die Interessen der betroffenen Person überwiegen (sog. Interessenabwägung).
Um die Verarbeitung personenbezogener Daten auf ein berechtigtes Interesse stützen zu können, müssen drei Voraussetzungen gegeben sein:

- Der für die Verarbeitung der personenbezogenen Daten Verantwortliche oder ein Dritter haben ein berechtigtes Interesse an der Datenverarbeitung.
- Die Verarbeitung ist zur Wahrung des berechtigten Interesses erforderlich.
- Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen nicht.
- Wenn diese drei Voraussetzungen kumulativ vorliegen, kann eine Verarbeitung auf Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO gestützt werden.

Anhaltspunkte für die hier zu treffende Abwägungsentscheidung enthält Erwägungsgrund 47 DS-GVO, der u. a. ausführt: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden."

Die DS-GVO verlangt eine Abwägung im konkreten Einzelfall sowohl im Hinblick auf die Interessen der Verantwortlichen bzw. Dritten als auch der betroffenen Person. Ein bloßes Abstellen auf abstrakte oder auf vergleichbare Fälle ohne Betrachtung des Einzelfalls genügt den Anforderungen der DS-GVO nicht. Insoweit ergibt sich für die Interessenabwägung u. a. aus ErwGr. 47 dass die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen sind. Damit ist auch auf die subjektiven Erwartungen der betroffenen Person im Einzelfall abzustellen. Neben diesen ist aber auch zu fragen, was objektiv vernünftigerweise erwartet werden kann und darf. Entscheidend ist daher auch, ob die Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung in bestimmten Bereichen der Sozialsphäre typischerweise akzeptiert oder abgelehnt wird.

Die Erwartungen der betroffenen Person werden bei Maßnahmen zur Direktwerbung auch durch die Informationen nach Art. 13 und 14 DS-GVO zu den Zwecken der Datenverarbeitung bestimmt. Informiert der Verantwortliche transparent und umfassend über eine vorgesehene Verarbeitung von Daten für Zwecke der Direktwerbung, geht die Erwartung der betroffenen Person in aller Regel auch dahin, dass ihre Kundendaten entsprechend genutzt werden. Allerdings kann durch Transparenz der gesetzliche Abwägungstatbestand nach Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO nicht beliebig erweitert werden, da die Erwartungen an dem objektiven Maßstab der Vernunft gemessen werden müssen.
Die Datenverarbeitung muss ferner insgesamt im Hinblick auf die berechtigten Interessen erforderlich sein. Auch die Erstellung eines Profils unter Verwendung externer Datenquellen (z. B. Informationen aus sozialen Netzwerken) für Zwecke der Direktwerbung (Werbescores) wird in der Regel zu einem Überwiegen der schutzwürdigen Interessen der betroffenen Person führen.
Hinsichtlich der Übermittlung von Daten für Werbezwecke an Dritte sowie der Nutzung von Fremdadressen ist zu prüfen, ob den Interessen der betroffenen Person ein höherer Stellenwert einzuräumen ist als dem Interesse des Verantwortlichen an der Übermittlung sowie des Dritten zur Nutzung von Fremdadressen zur Werbung. Insoweit erläutert ErwGr. 47, dass die Erwartungshaltung des Betroffenen auch davon bestimmt wird, ob eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z. B. wenn diese Kunde des

Verantwortlichen ist. Die Vorgaben des Art. 6 Abs. 4 DS-GVO sind ggf. zu beachten.
Zudem sind bei der Interessenabwägung die ohnehin geltenden allgemeinen Grundsätze aus Art. 5 Abs. 1 DS-GVO zu berücksichtigen, also insbesondere:

- faire Verfahrensweise,
- dem Verarbeitungszweck angemessen,
- in einer für die betroffene Person nachvollziehbaren Weise (insbesondere Nennung der Quelle der Daten, wenn Fremddaten verarbeitet werden).
- Für die verschiedenen Kommunikationskanäle bedeutet dies:

a) Postalische Werbung
Schutzwürdige Interessen dürften in der Regel nicht überwiegen, wenn im Nachgang zu einer Bestellung allen Kunden (ohne Selektion) postalisch ein Werbekatalog oder ein Werbeschreiben zum Kauf weiterer Produkte des Verantwortlichen zugesendet wird. Sofern es anhand eines Selektionskriteriums zu einer Einteilung in Werbegruppen kommt und sich kein zusätzlicher Erkenntnisgewinn aus der Selektion ergibt, wird die Interessenabwägung in der Regel ebenfalls zugunsten des Verantwortlichen ausfallen.

Eingriffsintensivere Maßnahmen wie automatisierte Selektionsverfahren zur Erstellung detaillierter Profile, Verhaltensprognosen bzw. Analysen, die zu zusätzlichen Erkenntnissen führen, sprechen hingegen dafür, dass ein Interesse der betroffenen Person am Ausschluss der Datenverarbeitung überwiegt. In diesen Fällen handelt es sich um Profiling, das nicht mehr auf Art. 6 Abs. 1 Buchstabe f DS-GVO gestützt werden kann und damit die Einholung einer Einwilligung vor der Datenverarbeitung erforderlich macht. Das Widerspruchsrecht des Art. 21 DS-GVO reicht dann nicht aus.

b) E-Mail-Werbung
E-Mail-Adressen, die unmittelbar von den betroffenen Personen im Rahmen einer Geschäftsbeziehung (Bestandskunden) erhoben wurden, können grundsätzlich für E-Mail-Werbung genutzt werden, wenn dieser Zweck entsprechend Art. 13 Abs. 1 Buchstabe c DS-GVO den betroffenen Personen bei der Datenerhebung transparent dargelegt worden ist. Überwiegende schutzwürdige Interessen der betroffenen Person nach Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO sind insbesondere dann nicht gegeben, wenn die in § 7 Abs. 3 UWG enthaltenen Vorgaben für elektronische Werbung eingehalten werden.

c) Telefonwerbung
Für Anrufe bei Verbrauchern zu Zwecken der Direktwerbung (B2C) sieht das UWG (§ 7 Abs. 2 Nr. 2) keine Ausnahme vom Einwilligungserfordernis vor, sodass ein solches Nutzen von Telefonnummern ohne vorherige Einwilligung wegen der besonderen Auswirkungen dieser Werbeform (stärkere Belästigung/Störung) datenschutzrechtlich an den überwiegenden schutzwürdigen Interessen der betroffenen Personen gemäß Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO scheitert.

Bei Werbung mit einem Telefonanruf gegenüber einem sonstigen Marktteilnehmer (B2B) kommt es für die Zulässigkeit gemäß § 7 Abs. 2 Nr. 2 UWG darauf an, dass von dessen zumindest mutmaßlicher Einwilligung ausgegangen werden kann. Im B2B-Bereich stehen deshalb bei einem Nutzen von Telefonnummern für Werbeanrufe datenschutzrechtlich nicht von vorne herein überwiegende schutzwürdige Interessen der telefonisch anzusprechenden Gewerbetreibenden nach Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO entgegen. Nach bisheriger Rechtsprechung ist aber ein geschäftlicher Vorkontakt Voraussetzung für den Werbeanruf. Sog. „Cold Calls" sind daher auch im B2B-Bereich unzulässig.

3. Informationspflichten bei Werbung
Werden personenbezogene Daten unmittelbar bei der betroffenen Person erhoben, z. B. für Kauf- und Dienstleistungsverträge, Prospektanforderungen oder Gewinnspiele, ist diese umfassend nach Art. 13 Abs. 1 und 2 DS-GVO u. a. über die Zwecke der Verarbeitung der Daten zu unterrich-

ten. Eine schon geplante oder in Betracht kommende Verarbeitung oder Nutzung der Daten für Zwecke der Direktwerbung ist daher der betroffenen Person von Anfang an transparent darzulegen.

Bei einer nachträglichen Änderung der Verarbeitung auch für Zwecke der Direktwerbung schreibt Art. 13 Abs. 3 DS-GVO eine vorherige Information vor. Diese Information ist mit einem Hinweis auf das Werbewiderspruchsrecht (Art. 21 Abs. 4 DS-GVO) zu versehen.

Grundsätzlich ist vom Verantwortlichen zum Zeitpunkt der Datenerhebung über alle Themen nach Art. 13 Abs. 1 und 2 DS-GVO zu informieren. Allerdings besteht schon rein praktisch nicht immer die Möglichkeit, der betroffenen Person alle Informationen aus Art. 13 Abs. 1 und 2 DS-GVO sofort vollständig zu geben, z. B. bei Bestell-Postkarten als Zeitschriften-Beilage, bei Bestellungen am Telefon oder bei Kaufverträgen an Automaten. Die Aufsichtsbehörden unterstützen daher den Vorschlag der früheren Artikel 29-Gruppe (WP 260, S. 17) für ein zweistufiges Informationsmodell.
Aus den Informationspflichten nach Art. 13 Abs. 1 und 2 DS-GVO ergeben sich in der Regel folgende grundsätzliche Mindestanforderungen (entscheidend ist aber stets der Informationsbedarf im Einzelfall), die regelmäßig auf einer ersten Stufe umgesetzt werden müssen:

- Identität des für die Verarbeitung Verantwortlichen (Name einschließlich Kontaktdaten);
- Kontaktdaten (Anschrift, Telefonnummer, E-Mail-Adresse) des betrieblichen Datenschutzbeauftragten (soweit benannt);
- Verarbeitungszwecke und Rechtsgrundlage in Schlagworten;
- Angabe des berechtigten Interesses, soweit die Verarbeitung darauf beruht;
- Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
- Übermittlung in Drittstaaten;
- Widerspruchsrecht nach Art. 21 DS-GVO;
- Hinweis auf Zugang zu den weiteren Pflichtinformationen gemäß Art. 13 Abs. 1 und 2 DS-GVO (wie Auskunftsrecht, Beschwerderecht), z. B. auch mittels Internet-Link.

Information des Bestandes („Altfälle")
Art. 13 und 14 DS-GVO stellen für die Informationspflichten vom Wortlaut her gesehen zunächst auf Datenerhebungen nach Wirksamwerden der DS-GVO ab („Werden personenbezogene Daten … erhoben …"). Die frühere Artikel 29-Gruppe geht jedoch im Hinblick auf ErwGr. 171 Satz 2 („Verarbeitungen, die zum Zeitpunkt der Anwendung dieser Verordnung bereits begonnen haben, sollten innerhalb von zwei Jahren nach dem Inkrafttreten dieser Verordnung mit ihr in Einklang gebracht werden.") und der Grundsätze aus Art. 5 Abs. 1 Buchstabe a DS-GVO zur Transparenz (vgl. WP 260) davon aus, dass bei den künftigen Kontakten mit den betroffenen Personen die neuen Informationspflichten in angemessener Weise umzusetzen bzw. nachzureichen sind.

Achtung: Auch Werbung im B2B-Bereich fällt zumeist unter die o. g. Regelungen. Fälschlicherweise wird häufig dargelegt, dass Adressen im B2B-Werbebereich keinen Personenbezug aufweisen würden. Dies ist aber häufig der Fall: Die oft als Zusatzinformationen enthaltenen Ansprechpartner gelten natürlich als personenbezogene Daten und auch Handynummern von selbständigen Unternehmern, die sowohl geschäftlich als auch privat genutzt werden, oder personalisierte E-Mail-Adressen haben Personenbezug.

Die DS-GVO setzt allgemein gültige Standards innerhalb der Europäischen Union, was auch für die Wirtschaftsunternehmen zu einem faireren Wettbewerb führen wird. Dabei hat die DS-GVO den Datenschutz nicht völlig neu erfunden. Viele Regelungen des „alten" BDSG finden sich auch in der DS-GVO wieder. Daher ist manches Wehklagen über das neue Datenschutzrecht gerade auch von Wirtschaftsverbänden nur

sehr eingeschränkt nachvollziehbar. Transparenz, Information und Dokumentation sind drei wichtige Grundpfeiler des neuen Rechts. Mit dem Informationsmaterial der Datenschutzaufsichtsbehörden sollten auch kleinere Betriebe und Selbständige diese datenschutzrechtlichen Aufgaben meistern können.

1.3 Zertifizierung, Akkreditierung

Verantwortliche und Auftragsverarbeiter erhalten künftig die Möglichkeit, die Einhaltung der DS-GVO bei der Verarbeitung personenbezogener Daten im Rahmen von Prozessen, Dienstleistungen und Produkten zertifizieren zu lassen (Art. 42 DS-GVO).

„Eine Zertifizierung (…) mindert nicht die Verantwortung des Verantwortlichen oder des Auftragsverarbeiters für die Einhaltung dieser Verordnung und berührt nicht die Aufgaben und Befugnisse der Aufsichtsbehörden (…)" (Art. 42 Abs. 4 DS-GVO).

Eine Person oder Institution kann nicht insgesamt nach der DS-GVO zertifiziert werden: zertifiziert werden nur konkrete Prozesse, Dienstleistungen oder Produkte. Zertifizierung nach der DS-GVO kann durch die zuständige Datenschutz-Aufsichtsbehörde oder durch akkreditierte Zertifizierungsstellen erfolgen.
Der LfDI Baden-Württemberg sieht derzeit grundsätzlich davon ab, selbst zu zertifizieren.

Die Akkreditierung von Zertifizierungsstellen erfolgt gemäß Akkreditierungsstellengesetz durch die Deutsche Akkreditierungsstelle (DAkkS), Berlin. Die Datenschutz-Aufsichtsbehörden, also auch der LfDI Baden-Württemberg, wirken an diesem Verfahren mit.

Auf Grundlage einer erfolgreichen Akkreditierung kann die Datenschutz-Aufsichtsbehörde dem antragstellenden Unternehmen die Befugnis erteilen, als Zertifizierungsstelle tätig zu werden. Dies erfolgt in einem eigenständigen Verwaltungsverfahren (§ 39 BDSG).

Akkreditierungs-Anträge werden, sobald Akkreditierungs-Verfahren durchgeführt werden können, an die DAkkS zu richten sein. Sie wird sie an die jeweils zuständige Datenschutz-Aufsichtsbehörde weiterleiten.

Zertifizierungsstellen benötigen ein Programm, nach dem sie ihre Kunden prüfen. Dieses Konformitätsbewertungsprogramm kann von ihnen selbst oder einem anderen Programmeigner ausgearbeitet worden sein.

Derzeit finden unter Mitwirkung des LfDI Baden-Württemberg Abstimmungen mit den anderen Datenschutz-Aufsichtsbehörden und der DAkkS statt, u. a., um die Anforderungen an zu akkreditierende Zertifizierungsstellen, an Konformitätsbewertungsprogramme und die Zusammenarbeit der Datenschutz-Aufsichtsbehörden und der DAkkS näher zu konkretisieren. Einige der zu erarbeitenden Dokumente werden sodann dem Europäischen Datenschutz-Ausschuss vorgelegt.

Aufgrund dieser notwendigen Vorbereitungs- und Abstimmungsprozesse können Akkreditierungs-Verfahren derzeit noch nicht durchgeführt werden. Wir informieren Sie u. a. auf unseren Internetseiten (https://www.baden-wuerttemberg.datenschutz.de) über den aktuellen Stand.

1.4 Betrieblicher Datenschutzbeauftragter

Zahlreiche Anfragen betrafen das Thema Datenschutzbeauftragter. Die teils neuen Regelungen zur Benennungspflicht mit ihren unbestimmten Rechtsbegriffen sind nur schwer verständlich und haben daher zu großer Verunsicherung bei Unternehmen, Selbständigen und Vereinen geführt.

Neue Rechtsgrundlagen
Die Voraussetzungen, die zur Pflicht führen, einen betrieblichen oder behördlichen Datenschutzbeauftragten (DSB) zu benennen, sind seit dem 25. Mai 2018 in zwei Vorschriften geregelt: In Art. 37 Abs. 1 der EU-Datenschutz-Grundverordnung (DS-GVO) sowie in § 38 des Bundesdatenschutzgesetzes (BDSG).

Die Pflicht trifft – beim Vorliegen der jeweiligen gesetzlichen Voraussetzungen – den Verantwortlichen und den Auftragsverarbeiter.

Sechs Fallkonstellationen, welche die Pflicht begründen, einen behördlichen oder betrieblichen Datenschutzbeauftragte zu benennen:

1. Verantwortlicher ist **eine öffentliche Stelle oder Behörde** (Art. 37 Abs. 1 Buchst. a DS-GVO)

   Hier muss immer ein Datenschutzbeauftragter benannt werden.

2. Die **Kerntätigkeit** besteht in der **umfangreichen oder systematischen Überwachung** von betroffenen Personen (Art. 37 Abs. 1 Buchst. b DS-GVO).

   Achtung: Überwachung meint nicht nur Videoüberwachung, Detekteien und private Sicherheitsunternehmen, sondern z. B. auch die Nachverfolgung des Surfverhaltens im Internet oder des Kaufverhaltens durch ein Treueprogramm.

3. Die **Kerntätigkeit** umfasst die u**mfangreiche Verarbeitung besonderer Kategorien von Daten oder strafrechtlicher Verurteilungen** (Art. 37 Abs. 1 Buchst. c DS-GVO).

4. Regelmäßig sind **mindestens zehn Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt (§ 38 Abs. 1 S. 1 BDSG).

   Bitte beachten: Die Leitung des Verantwortlichen (Geschäftsführer/in, Chef/Chefin, Inhaber/-in, Partner usw.) bzw. des Auftragsverarbeiters wird hierbei immer hinzugerechnet.

5. Es ist eine **Datenschutz-Folgenabschätzung** durchzuführen (§ 38 Abs. 1 S. 2 1. HS BDSG in Verbindung mit Art. 35 DS-GVO).

6. Es werden personenbezogene **Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung** verarbeitet (§ 38 Abs. 1 S. 2 2. HS BDSG).

   In diese Gruppe gehören insbesondere Wirtschaftsauskunfteien, Adresshändler sowie Markt- und Meinungsforschungsinstitute.

1. Hauptanwendungsfälle

a) Die Kerntätigkeit umfasst die umfangreiche Verarbeitung besonderer Kategorien von Daten oder strafrechtlicher Verurteilungen (Art. 37 Abs. 1 Buchst. c DS-GVO).

Besondere Kategorien von Daten nach Art. 9 Absatz 1 DS-GVO sind u. a.: Gesundheits- und Patientendaten, Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder eine Gewerkschaftszugehörigkeit hervorgeht sowie genetische Daten oder Daten zum Sexualleben oder zur sexuellen Orientierung. Hinzu kommen nach Art. 10 DS-GVO Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln.

Zum Begriff der „Kerntätigkeit" führt Erwägungsgrund 97 S. 2 der DS-GVO aus:

*„Im privaten Sektor bezieht sich die Kerntätigkeit eines Verantwortlichen auf seine **Haupttätigkeiten** und nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit."*

Demnach muss hier eine Haupttätigkeit des Verantwortlichen in der Verarbeitung besonderer Datenkategorien liegen. Eine dem eigentlichen Geschäftszweck völlig untergeordnete reine Neben- bzw. Hilfstätigkeit oder die Durchführung reiner Verwaltungs- und Erhaltungsaufgaben (soweit diese überhaupt Personenbezug haben, so z. B. unternehmensinterne Personalverwaltung einschließlich der Entlohnung, das Führen eines Zeiterfassungssystems bei den Beschäftigten, der Betrieb eines hausinternen IT-Systems) sind hier unbeachtlich.

Der Begriff der Kerntätigkeit steht aber immer in Wechselwirkung zum Umfang der Tätigkeiten insgesamt, sodass stets eine Gesamtbetrachtung anzustellen ist: Macht eine Hilfstätigkeit 55 % der Gesamttätigkeit eines Unternehmens aus, ist sie eben keine Hilfs- oder Nebentätigkeit mehr. Die Kerntätigkeit muss also die verantwortliche Stelle qualitativ und quantitativ prägen.

Als „Kerntätigkeit" lassen sich die wichtigsten Arbeitsabläufe betrachten, die zur Erreichung der Ziele des Verantwortlichen oder des Auftragsverarbeiters (Geschäfts- / Unternehmenszweck bzw. Unternehmensstrategie) erforderlich sind, also alle Maßnahmen, die den Geschäftszweck unmittelbar fördern, die wesentlich oder maßgeblich zum Gesamtwertschöpfungsprozess des Verantwortlichen beitragen.
Wenn die Frage nach dem Vorliegen einer solchen Kerntätigkeit mit „nein" beantwortet wird, ist die Prüfung beendet. Eine Pflicht zur Benennung eines Datenschutzbeauftragten nach Artikel 37 Abs. 1 Buchst. c DS-GVO besteht dann nicht. Auf weitere Fragen, etwa nach dem Vorliegen einer umfangreichen Bearbeitung, kommt es nicht mehr an.

Beispiel:
Ein Versicherungsmakler, der neben den „gängigen" Versicherungen wie Hausrats-, Rechtsschutz- oder Haftpflichtversicherungen auch Versicherungen im Gesundheitsbereich (z. B. Kranken-, Zahnzusatz- und Berufsunfähigkeitsversicherungen) vermittelt und dabei Gesundheitsdaten seiner Kunden verarbeitet, muss keinen Datenschutzbeauftragten bestellen, da diese Datenverarbeitung nicht seine Kerntätigkeit darstellt.

b) Es sind regelmäßig mindestens zehn Personen ständig mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt (§ 38 Abs. 1 S. 1 BDSG).
Das Wort „Personen" soll deutlich machen, dass aus datenschutzrechtlicher Sicht allein die Anzahl der mit der automatisierten Verarbeitung personenbezogener Daten beschäftigten Personen – unabhängig von ihrem arbeitsrechtlichen Status als Arbeitnehmer, freie Mitarbeiter oder Auszubildende – entscheidend ist.

Es sind also beispielsweise hinzuzurechnen: Voll- und Teilzeitkräfte, Leiharbeitnehmer, Auszubildende, Volontäre und Praktikanten sowie Beschäftigte in Telearbeit.

„In der Regel" soll unterstreichen, dass gewisse Schwankungen in der Anzahl der Personen, die automatisiert Daten verarbeiten, unbeachtlich sind, wenn „in der Regel" die Anzahl unter 10 Personen bleibt. Dadurch soll vermieden werden, dass Unternehmen nur deshalb einer anderen Kategorie (DSB-Bestellpflicht) zugeordnet werden, weil sie die maßgebliche Personengrenze für die Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz kurzzeitig überschreiten. Entscheidend ist der auf ein Jahr zu betrachtende, durchschnittliche Personalbestand.

„Ständig" soll klarstellen, dass Personen, die nur gelegentlich, z. B. als Urlaubsvertretung, beschäftigt sind und dabei personenbezogene Daten automatisiert verarbeiten, nicht mitzuzählen sind.

Es sind aber nur die Personen hinzuzuzählen, die im Unternehmen (Verein usw.) automatisiert Daten verarbeiten. Eine automatisierte Datenverarbeitung liegt vor, wenn für die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten von der Person Datenverarbeitungsanlagen wie z. B. PCs, Tablets oder Smartphones eingesetzt werden. Das BDSG schränkt Art. 4 Nr. 2 DS-GVO diesbezüglich ein, da es dem BDSG nur auf die automatisierte Datenverarbeitung ankommt.

Personen (Beschäftigte), die mit anderen (z. B. technischen/handwerklichen) Aufgaben betraut sind und keine automatisierte Datenverarbeitung durchführen, sind nicht zu berücksichtigen. Nicht hinzuzuzählen sind damit z. B. angestellte Handwerker, Reinigungskräfte, LKW-Fahrer, Monteure, Lager-Mitarbeiter, Arbeiter an Produktionsstätten und auf Baustellen etc., die ihre Aufträge intern nur auf Papier bekommen und nicht automatisiert personenbezogene Daten verarbeiten.

2. Person des Datenschutzbeauftragten

Mit der Aufgabe des Datenschutzbeauftragten kann gemäß Art. 37 Abs. 6 DS-GVO sowohl ein Beschäftigter des Verantwortlichen oder ein Beschäftigter des Auftragsverarbeiters – aber wegen möglicher Interessenkollisionen nicht gegenseitig – (sog. interner Datenschutzbeauftragter) als auch eine (natürliche) Person außerhalb des Verantwortlichen betraut werden (sog. externer Datenschutzbeauftragter, mit entsprechendem Dienstleistungsvertrag). Juristische Personen können nicht Beauftragter sein, da die Regelungen auf eine natürliche Person zugeschnitten sind.

Zum Beauftragten für den Datenschutz darf nach Art. 37 Abs. 5, 38 Abs. 6 DS-GVO nur benannt werden, wer

- die zur Erfüllung seiner Aufgaben erforderliche berufliche Qualifikation,
- insbesondere das Fachwissens auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis (Recht, Technik, Organisation),
- die Fähigkeit zur Erfüllung seiner Aufgaben nach Art. 39 DS-GVO sowie
- die nötige Zuverlässigkeit besitzt.

a) Fachwissen

Unabhängig von Branche und Größe der verantwortlichen Stelle müssen die Datenschutzbeauftragten über Grundkenntnisse zu den verfassungsrechtlich garantierten Persönlichkeitsrechten der Betroffenen und der Beschäftigten der verantwortlichen Stelle sowie umfassende Kenntnisse der einschlägigen Regelungen der DS-GVO, des Bundesdatenschutzgesetzes und anderer datenschutzrechtlicher Bestimmungen verfügen. Branchenkenntnis und Vertrautheit mit der Organisationsstruktur evtl. eingeschalteter Auftragsverarbeiter sind ebenfalls von Nutzen. Darüber hinaus sind Kenntnisse der einschlägigen technischen Vorschriften (IT), der Datenschutzprinzipien und der Datensicherheitsanforderungen insbesondere nach Art. 24 f. DS-GVO erforderlich.

Einrichtungsspezifisch sind des Weiteren Kenntnisse

- der spezialgesetzlichen datenschutzrelevanten Vorschriften,
- der Informations- und Telekommunikationstechnologie und der Datensicherheit (Funktionsweise moderner Informations- und Kommunikationstechnologien wie Internet, E-Mail, Cloud-Dienste; Sicherheitsrisiken (z. B. Phishing und Malware wie z. B. Viren, Trojaner, Spyware, Ransomware); IT-Grundschutz, Informationssicherheits-Managementsysteme und Informationssicherheitsmaßnahmen),
- betriebswirtschaftlicher Zusammenhänge,
- der technischen und organisatorischen Struktur sowie deren Wechselwirkung in der zu betreuenden verantwortlichen Stelle sowie
- im praktischen Datenschutzmanagement der verantwortlichen Stelle notwendig.

Das Berufsbild Datenschutzbeauftragter ist staatlich nicht reglementiert. Folglich

macht der Staat keinerlei Vorgaben im Hinblick auf die Aus- und Fortbildung eines DSB. Das erforderliche Fachwissen kann man sich somit frei aneignen, das Vorhandensein spezieller Zertifikate oder Abschlüsse wird seitens der Datenschutzaufsichtsbehörde nicht gefordert.

b) Keine dienstlichen oder familiären Interessenkonflikte

Die Person muss in der Lage sein, die Aufgaben eines DSB zu erfüllen (Art. 37 Abs. 5 DS-GVO). Nach Art. 38 Abs. 6 DS-GVO können DSB „andere Aufgaben und Pflichten wahrnehmen". Der Verantwortliche bzw. Auftragsverarbeiter hat allerdings dafür Sorge zu tragen, dass „derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen", also keine Unvereinbarkeiten bzw. Befangenheit vorliegen. In der Person des Datenschutzbeauftragten darf es also keine Interessenkonflikte geben, die persönliche Integrität muss sichergestellt sein. Dies bedeutet bei internen DSB z. B., dass das Grund-Beschäftigungsverhältnis mit der Funktion des DSB keine Zielkonflikte oder Interessenkonflikte aufweisen darf. Bei einer externen Bestellung darf das Unternehmen, das die Dienstleistung Datenschutzbeauftragter anbietet, ebenso wenig „befangen" sein.

Für eine korrekte Erfüllung der Aufgaben des DSB ist vielmehr eine weitestgehende Distanz gegenüber der zu kontrollierenden Stelle unerlässlich, denn eine effektive Kontrolle ist dann zu bezweifeln, wenn der Kontrolleur sich selbst kontrollieren muss, wenn etwa eine enge familiäre Verbindung zur Leitungsebene besteht bzw. wenn die Frage zu stellen ist, „welchen Hut der DSB gerade aufhat".

Betriebliche/behördliche Interessenkonflikte

Das Fehlen eines Interessenkonflikts ist eng mit dem Erfordernis einer unabhängigen Tätigkeit verknüpft; das BDSG-alt sprach hier von der notwendigen Zuverlässigkeit. DSB dürfen zwar auch andere Funktionen wahrnehmen, aber nur mit Aufgaben und Pflichten betraut werden, die zu keinen Interessenkonflikten mit ihrer Tätigkeit als DSB führen. Dies bedeutet insbesondere, dass der DSB keine Position innehaben kann, bei der er die Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegt. Dies ist immer fallweise zu betrachten.

Als Grundregel lassen sich zu den mit Interessenkonflikten einhergehenden Positionen innerhalb der Stelle im Überblick benennen:

Leitungs-, Chef- und Inhaberebene

Beispiele:
Inhaber, Leiter, Partner, Chef, Manager, Vorstandsvorsitzender, Geschäftsführer, Vorstand oder sonstiger gesetzlich oder verfassungsmäßig berufener Leiter des Unternehmens/der Behörde/des Vereins.

Nachgeordnete Positionen mit Führungsaufgaben und Entscheidungskompetenz über die Festlegung von Zwecken und Mitteln der Datenverarbeitung (IT)

Bei diesen Personen steht das Interesse an einer wirtschaftlichen Führung des Unternehmens im Vordergrund, das mit dem Interesse des Datenschutzbeauftragten, ungeachtet der betrieblichen Auswirkungen die datenschutzrechtlichen Vorschriften einzuhalten und umzusetzen, kollidiert.

Beispiele:
Leiter oder Verantwortlicher IT, Leiter des operativen Geschäftsbereichs, Finanzvorstand, leitender medizinischer Direktor, Leiter der Marketingabteilung, Leiter der Personalabteilung, Betriebsleiter), jedoch auch hierarchisch nachgeordnete Positionen, wenn die betreffenden Funktionen oder Aufgabenfelder ähnliche Interessenkonflikte mit sich bringen.

Durch ihre Nähe zur Geschäftsleitung und ihre leitende Position sind auch Prokuristen als Datenschutzbeauftragte ungeeignet. Bei ihnen besteht die Gefahr, dass sie sich mit den Geschäftszwecken und Zielen des Verantwortlichen bzw. Auftragsverar-

beiters so weitgehend identifizieren, dass dadurch die Erfüllung einer unabhängigen Kontrollfunktion als Datenschutzbeauftragter beeinträchtigt ist. Schließlich ist ein betrieblicher Datenschutzbeauftragter verpflichtet, unter Umständen auch gegen die Interessen der Geschäfts- oder Behördenleitung zu handeln. Das Gleiche gilt in der Regel für Abteilungsleiter und deren Mitarbeiter, wenn sie selbst personenbezogene Daten verarbeiten, wie beispielsweise in der EDV, im Personalbereich, aber auch im Marketing oder im Vertrieb. Als Datenschutzbeauftragte müssten sie sich ebenfalls selbst kontrollieren.

Eine gleichzeitige Tätigkeit als DSB und Geheimschutz- oder Geldwäschebeauftragter scheidet ebenfalls aus. Auch können Interessenkonflikte auftreten, wenn z. B. ein externer DSB aufgefordert wird, den Verantwortlichen oder den Auftragsverarbeiter in datenschutzrelevanten Rechtssachen vor Gericht zu vertreten. Auch ist es unzulässig, wenn ein Unternehmen, das den Verantwortlichen bzw. Auftragsverarbeiter im Bereich der IT nennenswert betreut, bei diesem betreuten Unternehmen gleichzeitig auch die Dienstleistung externer Datenschutzbeauftragter wahrnimmt (auch wenn dies ein anderer Mitarbeiter übernehmen würde).

Fallgruppen ohne Interessenkonflikte
Nach der Rechtsprechung des Bundesarbeitsgerichts (Urteil vom 23. März 2011, Az.10 AZR 562/09, RDV 2012, S. 237) besteht keine generelle Unvereinbarkeit zwischen dem Amt des betrieblichen Datenschutzbeauftragten und einer Betriebsratsmitgliedschaft. Dass der betriebliche Datenschutzbeauftragte Kontroll- und Überwachungsbefugnisse gegenüber dem Arbeitgeber hat, macht ein Betriebsratsmitglied nicht generell für diesen Aufgabenbereich ungeeignet. Auch als Mitglied des Betriebsrats kann ein Datenschutzbeauftragter Beaufsichtigungs- und Kontrollbefugnisse ordnungsgemäß wahrnehmen.

Als Datenschutzbeauftragte sind somit im Ergebnis alle Mitarbeiter eines Unternehmens geeignet, die wenig mit dem Datenbedarf des Unternehmens zu tun haben und die gebotene Distanz zur Unternehmensleitung aufweisen. Möglich ist in der Regel eine Kombination mit den Bereichen Organisation oder Recht, auch die gleichzeitige Aufgabe als IT-Sicherheitsbeauftragter ist regelmäßig unschädlich. Bei einer gleichzeitigen Mitarbeit in der Rechtsabteilung kann es jedoch unter Umständen ebenfalls zu einer Interessenkollision kommen, insbesondere wenn der Datenschutzbeauftragte als Mitarbeiter der Rechtsabteilung auch in Gerichtsprozessen gegen Mitarbeiter auftritt.

Familiäre Interessenkonflikte
Auch familiäre Bindungen bzw. Beziehungen zwischen dem Verantwortlichen bzw. Auftragsverarbeiter und dem DSB können zu Interessenkonflikten führen und damit die notwendige Unabhängigkeit nach Art. 38 Abs. 3 DS-GVO und Fähigkeit im Sinne des Art. 37 Abs. 5 DS-GVO negativ beeinflussen.

Beispiele:

- Wie kritisch und bestimmt tritt man als DSB auf, wenn die Unternehmenschefin/Behördenleiterin die eigene Ehefrau ist?
- Besteht für Beschäftigte nicht eine größere Hemmschwelle, sich an den DSB zu wenden, wenn dieser der Sohn des Unternehmenschefs/Behördenleiters ist?
- Wird die Tochter als DSB eher auf Seiten ihrer Mutter als Unternehmenschefin stehen oder auf Seiten des sich beschwerenden Kunden?

Im Hinblick auf den Unternehmenschef / den Behördenchef / einen Partner können Mitglieder der erweiterten Kernfamilie (Vater, Mutter, Sohn, Tochter, Schwiegersohn, Schwiegertochter, Großvater, Großmutter) daher nicht als DSB benannt werden, unabhängig davon, ob diese Angehörigen im Unternehmen / in der Behörde beschäftigt sind.

Es war lange Zeit politisch umstritten, ob es in der DS-GVO überhaupt (verbindliche)

Regelungen zum Datenschutzbeauftragten geben würde – zu unterschiedlich war die bisherige Praxis in den Mitgliedstaaten. Letztlich wurde der Datenschutzbeauftragte in die VO aufgenommen und daher das bei uns bewährte Modell bewahrt. Die Benennungspflicht ist weitgehend abhängig von den verarbeiteten Datenarten und dem damit verbundenen Risiko für die Betroffenen. Die bisherigen Regelungen des „alten" BDSG finden sich weitgehend unverändert auch im neuen BDSG wieder.

1.5 Wir sind im Bild! Filmen und Fotografieren unter der DS-GVO

Rund um den 25. Mai 2018, dem Zeitpunkt der Geltung der Datenschutz-Grundverordnung (DS-GVO), brach tsunamiartig eine Welle von Anfragen zum Thema filmen und fotografieren über meine Dienststelle herein. Horrormeldungen über das Wegbrechen ganzer Berufszweige sowie medienwirksame Berichte über Aufnahmen von Kindergartengruppen, auf denen die Gesichter durch Schwärzen unkenntlich gemacht wurden, waren der Auslöser. Die Datenschutz-Grundverordnung war plötzlich zum Sargnagel der privaten wie der beruflichen Fotografie erklärt. Verwundern musste dies, denn im Vergleich zur alten Rechtslage hat sich eigentlich nur wenig geändert. Das Problem lag wohl eher darin begründet, dass man vor der Geltung der Datenschutz-Grundverordnung das Fotografieren selten, wenn nicht gar nicht mit Datenschutz in Verbindung gebracht hatte. Insbesondere die hohen Bußgeldandrohungen hatten anscheinend einen sensibilisierenden Effekt und führten zur Frage, ob das mit dem Aufnehmen von Personen und dem Veröffentlichen dieser Aufnahmen womöglich auch in fremde Rechte eingreift und ob dies so ohne Weiteres möglich ist.

Angesichts der zahllosen Anfragen, die zunächst auch alle – soweit dies möglich war – zeitnah abgearbeitet wurden, zeigte sich schnell, dass hier eine allgemeine Information der Öffentlichkeit notwendig war. Wir entschlossen uns deshalb, das Thema anhand einer FAQ-Liste anzugehen, die in unser Internetangebot eingestellt wurde. Nicht zuletzt dies scheint Grund dafür zu sein, dass sich die Situation mittlerweile offenbar beruhigt hat, Eingaben zu dieser Thematik sind jedenfalls kaum noch zu verzeichnen.

Gleichwohl, um nochmal einen kurzen Überblick zu geben, folgende Hinweise:
Bei Bildaufnahmen natürlicher Personen handelt es sich um personenbezogene Daten. Hierzu reicht es aus, dass die abgebildeten Personen direkt oder indirekt – durch Heranziehung zusätzlicher Informationen – identifiziert werden können (Artikel 4 Nummer 1 DS-GVO).

Wer natürliche Personen fotografiert und wer Fotografien natürlicher Personen der Öffentlichkeit zugänglich macht, hat hierbei die datenschutzrechtlichen Rahmenbedingungen zu beachten. Schon an dieser Stelle ist darauf hinzuweisen, dass die §§ 22 und 23 des Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KunstUrhG) nach ihrem Wortlaut zusammen mit der Strafvorschrift des § 33 KunstUrhG nur das Verbreiten und das öffentliche Zur-Schau-Stellen erfassen, nicht jedoch das Herstellen von Abbildungen.

Ausnahmsweise ist das Datenschutzrecht dann unbeachtlich, wenn die Fotografien ausschließlich für den privaten Gebrauch bestimmt sind (Artikel 2 Absatz 2 Buchstabe c DS-GVO) und den eigenen Haushaltsbereich nicht verlassen.

Jegliche Verwendung (Artikel 4 Nummer 2 DS-GVO) personenbezogener Daten setzt datenschutzrechtlich eine dahingehende Berechtigung voraus. Sowohl für das Fotografieren als solches (**Datenerhebung**) als auch für den weiteren Umgang mit den Fotografien, insbesondere die Veröffentlichung (**Offenlegung**), muss (mindes-

tens) eine der in Artikel 6 Absatz 1 Satz 1 DS-GVO geregelten Voraussetzungen vorliegen. Im Wesentlichen in Betracht kommen dabei die Einwilligung (Buchstabe a in Verbindung mit Artikel 7 DS-GVO), der Vertrag (Buchstabe b) sowie das berechtigte Interesse (Buchstabe f). Dabei ist die Einwilligung gegenüber den beiden anderen Rechtsgrundlagen zwar nicht subsidiär; wenn sich jedoch die Berechtigung zur Datenverarbeitung aus einem Vertrag oder aus einem berechtigten Interesse, das im konkreten Fall entgegenstehende Interessen der Betroffenen überwiegt, herleiten lässt, kommt es auf eine Einwilligung nicht mehr an.

Anfertigung von Fotoaufnahmen (Datenerhebung)

Vertragliche Befugnisse zur Anfertigung von Fotografien (Fall des Artikel 6 Absatz 1 Satz 1 Buchstabe b DS-GVO) ergeben sich meist in Zwei-Personen-Verhältnissen. Wer etwa ins Fotostudio geht, um Pass- oder Bewerbungsfotos machen zu lassen, geht einen Werkvertrag ein. Dessen Hauptzweck ist gerade die Verarbeitung personenbezogener Daten. Hier bedarf es seitens des Fotografen lediglich noch der Erfüllung der Informationspflichten nach Artikel 13 DS-GVO, um (datenschutzrechtlich) rechtssicher zu handeln.

Sollen Personengruppen aufgenommen werden (Phase der Datenerhebung), kann danach differenziert werden, ob es sich um eine geschlossene Gesellschaft (bestimmbarer Kreis von Betroffenen) oder um einen unbestimmbaren, nicht abgrenzbaren Kreis Betroffener handelt. Zunächst kann in beiden Fällen Artikel 6 Absatz Satz 1 Buchstabe f DS-GVO als Rechtsgrundlage dienen. Ein berechtigtes (künstlerisches, gewerbliches) Interesse wird regelmäßig begründbar sein. Dabei kann es sich um das Eigeninteresse des Fotografen oder, soweit er im Auftrag eines Dritten tätig wird, um das Interesse eines Dritten, des Auftraggebers, handeln. In jedem Fall hängt die Zulässigkeit der Aufnahmen vom Ergebnis der Interessenabwägung ab.

Bei dieser Interessenabwägung kann in Rechnung gestellt werden, dass es jedenfalls bei geschlossenen Gesellschaften durchaus üblich ist und es in der Regel auch den „vernünftigen Erwartungen" (Erwägungsgrund 47 Satz 1 der DS-GVO) der Betroffenen entspricht, dass solche Veranstaltungen auch bildlich dokumentiert werden. Von daher werden Fotoaufnahmen in solchen Fällen regelmäßig ohne explizite Einwilligung der Betroffenen zulässig sein. Ausnahmen gelten allenfalls, soweit es um die Ablichtung von Kindern geht, die einem besonderen Schutz unterliegen. Hier bedarf es grundsätzlich der Einwilligung der (aller) Personensorgeberechtigten.

Zur Erfüllung der auch in diesen Fällen erforderlichen Informationspflichten sollte an der Veranstaltungsörtlichkeit gut sichtbar auf die nach Artikel 13 DS-GVO maßgeblichen Punkte hingewiesen werden, wobei die Möglichkeit erwähnt werden sollte, dass man sich gegebenenfalls aus dem Erfassungsbereich der Kamera(s) entfernen und/oder den Fotografen darauf aufmerksam machen kann, dass man nicht abgelichtet werden will. Da die Informationspflichten vom (datenschutzrechtlich) Verantwortlichen zu erfüllen sind, treffen sie entweder den Fotografen oder, soweit dieser als Auftragsverarbeiter gemäß Artikel 28 DS-GVO tätig wird, den Auftraggeber.

Sollen Fotografien an Örtlichkeiten hergestellt werden, die räumlich nicht abgegrenzt sind und in denen ein unbestimmbarer Kreis von Personen betroffen ist (Menschen kommen und gehen, z. B. Landschaftsfotografie, Straßenfotografie etc.), bildet Artikel 6 Absatz 1 Satz 1 Buchstabe f DS-GVO ebenfalls die Rechtsgrundlage. Im Rahmen der Abwägung dürften Erwartungen der Betroffenen dahingehend, dass sie bildlich erfasst werden, zwar weniger zum Tragen kommen. Soweit es nicht um Aufnahmen für rein private Zwecke geht, für die das Datenschutzrecht nicht gilt, dürfte dabei zugunsten des Fotografen zu berücksichtigen sein, dass er sich bei seiner Tätigkeit ebenfalls auf Grundrechte nach der

Charta der Grundrechte der Europäischen Union berufen kann (Artikel 13/Kunstfreiheit, Artikel 15/Berufsfreiheit; nach Auffassung des Europäischen Gerichtshofs ist ein angemessenes Gleichgewicht zwischen den miteinander in Einklang zu bringenden Grundrechten zu gewährleisten, Urteil vom 20. Oktober 2018, Az.: C 149/17), dass zufällig in der Öffentlichkeit aufgezeichnete Personen tendenziell weniger tief in ihrem informationellen Selbstbestimmungsrecht betroffen sind und dass auch unter Heranziehung des Rechtsgedankens des Artikel 11 Absatz 1 DS-GVO die Forderung nach Einholung individueller Einwilligungen nicht nur faktisch unmöglich, sondern auch datenschutzrechtlich untunlich wäre. Gleichfalls entfallen dürfte die Pflicht zur Information, wobei hier, da es sich faktisch um verdeckte Datenerhebungen handelt, Artikel 14 DS-GVO einschlägig wäre. Nach Artikel 14 Absatz 5 Buchstabe b DS-GVO entfällt die Pflicht zur Information, wenn sich deren Erteilung als unmöglich oder unverhältnismäßig erweist, was in den gegebenen Fallkonstellation regelmäßig so sein wird.

Veröffentlichung von Fotoaufnahmen (Datenübermittlung)

Die Veröffentlichung von Fotoaufnahmen stellt eine weitere, neue Verarbeitungsmaßnahme dar. Auch für diese ist eine Rechtsgrundlage erforderlich. Ob vor dem Hintergrund der DS-GVO hierfür aber weiterhin die §§ 22 und 23 KunstUrhG in Frage kommen, ist streitig. Soweit man sich der Auffassung anschließt, das KunstUrhG trete hinter die DS-GVO zurück, kommt Artikel 6 Absatz 1 Satz 1 Buchstabe f DS-GVO als Rechtsgrundlage auch für die Bildveröffentlichung in Frage. Auch hier wird sich die Frage einer Berechtigung zur Veröffentlichung in aller Regel aus dem Ergebnis einer Abwägung der jeweils betroffenen Interessen ergeben. Geht man davon aus, dass §§ 22 und 23 KunstUrhG nicht mehr fortgelten, kann im Rahmen der Interessenabwägung gleichwohl auf das abgestufte Schutzkonzept der §§ 22, 23 KunstUrhG zurückgegriffen werden. Das Bildnis einer Person, das deren äußere Erscheinung in einer für Dritte erkennbaren Weise wiedergibt, darf danach grundsätzlich nur mit deren Einwilligung verbreitet werden. Die nicht von der Einwilligung der abgebildeten Person gedeckte Verbreitung eines Bildes ist nur zulässig, wenn dieses dem Bereich der Zeitgeschichte oder einem der weiteren Ausnahmetatbestände des § 23 Absatz 1 KunstUrhG zuzuordnen ist und berechtigte Interessen der abgebildeten Person nicht verletzt werden (§ 23 Absatz 2 KunstUrhG). Die Ausnahmetatbestände des § 23 Absatz 1 Nummer 2 und 3 KunstUrhG betreffen Bilder (im Gegensatz zu den Bildnissen), auf denen natürliche Personen quasi als Beiwerk mit erfasst werden. Bezogen auf die Eigenheiten der Straßenfotografie hat das Bundesverfassungsgerichts jüngst (Nichtannahmebeschluss vom 8. Februar 2018 – 1 BvR 2112/15 –) in Abwägung zwischen Kunstfreiheit und allgemeinem Persönlichkeitsrecht die hervorgehobene Präsentation einzelner Personen zum zentralen Punkt seiner Abwägung gemacht. Dies kann grundsätzlich der Maßstab sein: je individueller eine Person in den Vordergrund tritt, umso eher wird eine Einwilligung in die Veröffentlichung erforderlich sein. Je mehr sie in der Masse aufgeht, desto weniger bedarf es einer Einwilligung. Ein genereller Maßstab lässt sich hierbei nicht bestimmen.

Ist eine Einwilligung erforderlich, ist diese freiwillig, gut informiert und mit Widerrufsbelehrung versehen einzuholen (Artikel 7 DS-GVO), es gelten die Informationspflichten gemäß Artikel 13 DS-GVO. Dabei ist insbesondere anzugeben, in welchem Medium die Veröffentlichung beabsichtigt ist (Homepage, Presse, Internet, soziales Netzwerk, etc.), wobei den Betroffenen eine Differenzierung zu ermöglichen ist, etwa dahingehend, dass nur der Veröffentlichung in bestimmten Medien zugestimmt wird.

1.6 Beschäftigtendatenschutz

1.6.1 Grundfragen

Zwar hat die DS-GVO in vielen Bereichen Umstrukturierungsprozesse in Gang gesetzt, im Bereich des Beschäftigtendatenschutzes haben sich auf den ersten Blick jedoch keine bahnbrechenden Veränderungen ergeben. Hierbei vergessen Verantwortliche leider, dass die weitreichenden Informationspflichten und Betroffenenrechte nach Art. 12 ff. DS-GVO nicht nur den Kunden, sondern auch der eigenen Belegschaft zustehen. Eine weitere oft diskutierte Frage ist die Notwendigkeit der Anpassung von bestehenden Betriebsvereinbarungen an die Vorgaben der DS-GVO.

Wie bereits im letzten Tätigkeitsbericht kritisiert, fehlt es im Bereich des Beschäftigtendatenschutzes trotz entsprechender Bestrebungen des deutschen Gesetzgebers auch weiterhin an einem nationalen „Gesetz zur Regelung des Beschäftigtendatenschutzes", das mit eigenständigen und spezifischen Regelungen die Besonderheiten des Arbeitsverhältnisses als Nähe- und Abhängigkeitsverhältnis beachtet. Die seit dem 25. Mai 2018 unmittelbar anzuwendende DS-GVO überlässt den Mitgliedsstaaten der Europäischen Union die Entscheidung, ob sie durch Rechtsvorschriften spezifischere Vorschriften im Bereich des Beschäftigtendatenschutzes erlassen oder nicht. Für die Datenverarbeitung im Beschäftigungskontext hat der europäische Gesetzgeber in Art. 88 DS-GVO im Wege einer Öffnungsklausel ganz konkret die Möglichkeit für eigenständige nationale Regelungen geschaffen, die jedoch nicht zu einer absoluten Zersplitterung in diesem Bereich führen dürfen. Das neue BDSG übernimmt zwar in seinem § 26 den bislang gültigen § 32 BDSG der alten Fassung mit wenigen Zusätzen, stellt aber nach wie vor nur einen Minimalkonsens dar. Die in unserem 33. Tätigkeitsbericht gegebenen Hinweise zum Beschäftigtendatenschutz haben mit Anwendung der DS-GVO daher nicht an Aktualität verloren.

Auch unter der DS-GVO bleibt das allgemeine Prinzip des Verbots mit Erlaubnisvorbehalt bestehen. Die Verarbeitung personenbezogener (Beschäftigten-)Daten ist demnach grundsätzlich verboten, wenn nicht eine bestimmte gesetzliche Erlaubnis oder eine wirksame Einwilligung vorliegt. Im Beschäftigtendatenschutz liegt die zentrale Rechtsgrundlage in § 26 Abs. 1 Satz 1 BDSG, demzufolge personenbezogene Daten von Beschäftigten vom Arbeitgeber für Zwecke des Beschäftigungsverhältnisses verarbeitet werden dürfen, wenn dies für die Entscheidung über die Begründung, die Durchführung oder die Beendigung des Beschäftigungsverhältnisses erforderlich ist oder zur Erfüllung der sich aus dem Gesetz bzw. einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten erforderlich ist. Der Schutz der eigenen Daten und damit der informationellen Selbstbestimmung der betroffenen Personen ist gerade im Beschäftigungsverhältnis von hoher Relevanz. Ein gutes Datenschutzmanagement kann ein Unternehmen so als attraktiven Arbeitgeber auszeichnen und wie beim korrekten Umgang mit Kundendaten zu einem Wettbewerbsvorteil führen.

1. Erfüllung der Informationspflichten gegenüber den Beschäftigten

Wo dem BDSG kein eigenständiger Regelungsgehalt zukommt, kommt es zur alleinigen Anwendung der DS-GVO, wo das BDSG die in der DS-GVO vorgesehen Öffnungsklauseln nutzt zu einem Nebeneinander von europäischem und nationalem Recht. So auch im Bereich der Informationspflichten.

Ein Grund, warum die DS-GVO zur Mammutaufgabe für die meisten Unternehmen wurde, sind die erhöhten Anforderungen an die Erfüllung der Informationspflichten, auch wenn diese nicht ganz neu sind: Auch nach altem Recht musste der Verantwortliche die Betroffenen über die Verarbei-

tung ihrer Daten benachrichtigen (vgl. § 4 Abs. 3 und § 33 BDSG-alt). Vermutlich hat die Angst vor hohen Bußgeldern die Unternehmen dazu bewogen, ihre Informationspflichten mit Anwendung der DS-GVO seit dem 25. Mai 2018 zukünftig ernster zu nehmen. Im Vergleich zur alten Rechtslage ist der Umfang der Informationspflichten gestiegen. Welche Informationen die betroffene Person erhält, bestimmt sich danach, ob der Verantwortliche die Daten beim Betroffen selbst (Art. 13 DS-GVO) oder von einem Dritten (Art. 14 DS-GVO) erhoben hat. Denken Verantwortliche an die Erfüllung ihrer Informationspflichten, zeigt unsere Erfahrung, dass Unternehmen erst nach und nach realisieren, wie weitgehende Informationspflichten nicht nur den Kunden, sondern auch den eigenen Beschäftigten gegenüber bestehen.

In den meisten Fallkonstellationen des Beschäftigtendatenschutzes richtet sich der Inhalt der Informationspflicht nach Art. 13 DS-GVO. Hiernach muss die betroffene Person, wie bislang auch, über die Identität des Verantwortlichen informiert werden (vgl. Art. 13 Abs. 1 lit. a) DS-GVO). Wer das ist, scheint im Bereich des Beschäftigtendatenschutzes ganz eindeutig zu sein. Ganz so leicht ist es insbesondere bei Konzernunternehmen oder bei Bereichen, die vom Verantwortlichen nicht im Wege der Auftragsverarbeitung, sondern im Wege der altbekannten Funktionsübertragung ausgelagert wurden, aber nicht immer. Auch die Beschäftigten sind über die Kontaktdaten des Datenschutzbeauftragten zu informieren, sofern ein solcher bestellt wurde. Wie auch bisher muss über die Zwecke der Verarbeitung unterrichtet werden. Neu ist – und gerade das dürfte den einen oder anderen Verantwortlichen vor gewisse Herausforderungen stellen –, dass auch die Rechtsgrundlage für die Verarbeitung benannt werden muss (vgl. Art. 13 Abs. 1 lit. c) DS-GVO). Zwar gibt es im Bereich des Beschäftigtendatenschutzes wie eingangs erwähnt leider noch immer kein eigenständiges Beschäftigtendatenschutzgesetz und damit nur die allgemeine Vorschrift des § 26 BDSG, so dass man denken könnte, die richtige Rechtsgrundlage sei schnell gefunden. Die Fallstricke des Beschäftigtendatenschutzes zeigen aber, dass nicht selten das Gegenteil der Fall ist. Im Bereich des Beschäftigtendatenschutzes gibt es zahlreiche Spezialvorschriften. Beispielhaft ist § 39 Abs. 8 und 9 Einkommenssteuergesetz, der die Verarbeitung von auf der Lohnsteuerkarte enthaltenen Merkmalen regelt. Daneben können auch in Betriebsvereinbarungen eigenständige Erlaubnisnormen zur Verarbeitung personenbezogener Daten durch die Betriebsparteien geschaffen werden. Welche Rechtsgrundlage bei der Erfüllung der Informationspflichten anzugeben ist, kann somit sehr unterschiedlich ausfallen. Im Gegensatz zum BDSG macht die DS-GVO keine Einschränkung hinsichtlich der Verpflichtung zur Mitteilung über die Empfänger oder Kategorien von Empfängern personenbezogener Daten, wenn bereits bei der Erhebung feststeht, dass diese personenbezogene Daten erhalten sollen (vgl. Art. 13 Abs. 1 lit. e) DS-GVO). Es kommt auch nicht mehr darauf an, ob der Betroffene nach den Umständen des Einzelfalls mit einer Übermittlung seiner Daten rechnen musste (vgl. § 4 Abs. 3 Satz 1 Nr. 3 BDSG-alt). Die DS-GVO geht noch einen Schritt weiter und verpflichtet auch zur Mitteilung über eine Übermittlung personenbezogener Daten über den Geltungsbereich der DS-GVO hinaus (vgl. Art. 13 Abs. 1 lit. f) DS-GVO.

Wie aber erfüllen Arbeitgeber diese weitreichenden Informationspflichten? Nach der Verordnung müssen die in Art. 13 oder Art. 14 DS-GVO aufgelisteten Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache gegeben werden (vgl. Art. 12 Abs. 1 DS-GVO). Im Bereich des Beschäftigtendatenschutzes empfiehlt der LfDI BW den Arbeitgebern die Informationspflichten gegenüber den Mitarbeitern in einer Form vorzunehmen, die es den Beschäftigten jederzeit ermöglicht, die Information abzurufen. Hierfür können die im Unternehmen üblicherweise zur Verfügung stehenden Kanäle genutzt werden,

wie zum Beispiel Veröffentlichungen im Intranet, ein zentraler Aushang am Schwarzen Brett oder eine entsprechende E-Mail an alle Mitarbeiter. Es ist nicht notwendig, jedem Mitarbeiter ein persönliches Schreiben mit den nach der DS-GVO vorgesehen Informationen auszuhändigen und sich den Empfang des Schreibens bestätigen zu lassen. Ob der Mitarbeiter die ihm überlassenen Informationen zur Kenntnis nimmt, liegt ganz bei ihm. Keinesfalls sollten Unternehmen – wie die tägliche Arbeit des LfDI BW zeigt – das absurde Vorgehen an den Tag legen, den Mitarbeiter bei Nichtbestätigung des Erhalts des Informationsschreibens mit der Kündigung zu drohen!

Verantwortliche dürfen nicht übersehen, dass die Informationspflichten auch gegenüber ihren eigenen Beschäftigten bestehen. Gerade in diesem Bereich bieten sich die im Unternehmen üblicherweise genutzten Kanäle zur Informationserteilung, wie das Intranet oder das schwarze Brett, an.

2. Betriebsvereinbarung als datenschutzrechtliche Erlaubnisnorm

Wie Art. 88 Abs. 1 DS-GVO klarstellt, können auch Kollektivvereinbarungen, also neben Tarifverträgen auch Betriebsvereinbarungen, eine Rechtsgrundlage für die Verarbeitung personenbezogener Beschäftigtendaten darstellen. Diese Klarstellung findet sich auch explizit in § 26 Abs. 4 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. Wie aber erfüllen die Betriebsparteien die hohen Anforderungen aus Art. 88 Abs. 2 DS-GVO, denen eine Betriebsvereinbarung standhalten muss? Danach muss eine Betriebsvereinbarung angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person umfassen. Dies gilt insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb eines Unternehmensverbunds und die Überwachungssysteme am Arbeitsplatz.

Im Zuge der Umstellung auf die DS-GVO zeigt die aufsichtsrechtliche Erfahrung, dass viele Unternehmen notwendige Anpassungen von Betriebsvereinbarungen recht spät auf dem Schirm hatten. Da kommt eine Rahmenbetriebsvereinbarung als Rettung aller bisher abgeschlossenen Betriebsvereinbarungen natürlich sehr entgegen. Wenn Unternehmen jedoch denken, dass es mit einer solchen Rahmenbetriebsvereinbarung getan ist und man die einzelnen Betriebsvereinbarungen dann nicht mehr anpassen müsste, täuschen sie sich in der Regel. Nur die wenigsten bereits abgeschlossenen Betriebsvereinbarungen werden den Anforderungen aus Art. 88 Abs. 2 DS-GVO gerecht und beinhalten z. B. konkrete Zweckfestsetzungen der zu verarbeitenden Daten, ein entsprechend der Zweckbestimmung definiertes Löschkonzept oder konkrete Zugriffsberechtigungen. Wie der Name der „Rahmen"-Betriebsvereinbarung schon vermuten lässt, kann diese nur den Rahmen für die allgemeinen Anforderungen an Betriebsvereinbarungen vorgeben. Alles was so vor die Klammer gezogen werden kann und für jede bestehende und zukünftig abzuschließende Betriebsvereinbarung gilt, kann und sollte in einer Rahmenbetriebsvereinbarung geregelt werden. Konkrete Regelungen und Ausgestaltungen hingegen müssen sich in den spezifischen Betriebsvereinbarungen finden. Sicherlich können z. B. allgemeine Kriterien zur Löschkonzeption in einer Rahmenbetriebsvereinbarung getroffen werden. Damit ist jedoch nichts darüber gesagt, wie lange personenbezogene Daten aus einer Videoüberwachung von Beschäftigten, die ihre Rechtsgrundlage in einer spezifischen Betriebsvereinbarung haben, gespeichert werden dürfen. Sinn und Zweck von Betriebsvereinbarungen ist der Ausgleich zwi-

schen den betrieblichen Belangen und den Interessen der Beschäftigten, die stellvertretend durch den Betriebsrat wahrgenommen werden. Die Betriebsparteien wissen am besten, warum sie welche Daten für welchen Zweck und wie lange brauchen. Lediglich allgemeine Ausführungen in einer Rahmenbetriebsvereinbarung helfen da nicht weiter. Daher werden die Betriebsparteien nicht drum herumkommen, auch bereits bestehende Betriebsvereinbarungen anzupacken – hierzu können sie sich in der Rahmenbetriebsvereinbarung verpflichten. Die Aufsichtsbehörden sehen so, dass der Handlungsbedarf zur Anpassung und Umsetzung der DS-GVO auch in diesem Bereich erkannt wurde.

Rahmenbetriebsvereinbarungen sind nach Ansicht des LfDI BW also ein sinnvoller Weg. So können beispielsweise die Datenschutzgrundsätze aus Art. 5 DS-GVO in einer einfachen und für die Beschäftigten transparenten Art und Weise erläutert werden. Die Betriebsparteien müssen die Datenschutzgrundsätze nämlich beim Abschluss jeder zukünftigen und auch jeder bisher abgeschlossenen Betriebsvereinbarung beachten. Ein weiterer erfolgversprechender Faktor kann die Einigung über Grundsätzliches zur Erfüllung von Betroffenenrechten sein. Hier könnten die Betriebsparteien beispielsweise festlegen, wie den Beschäftigten die Erfüllung ihrer Betroffenenrechte konkret erleichtert werden könnte (vgl. Art. 12 Abs. 2 DS-GVO). Eine Möglichkeit wäre die Zurverfügungstellung von Mustervorlagen zur Durchsetzung von Auskunfts- oder Löschungsansprüchen.

Betriebsparteien sollten die ihnen eröffneten Möglichkeiten von Betriebsvereinbarungen nutzen und so eigenständige Verarbeitungsbefugnisse schaffen, die auf die betriebsinternen Gegebenheiten abgestimmt sind. Der Abschluss einer für alle Betriebsvereinbarungen vor die Klammer gezogenen Rahmenbetriebsvereinbarung ist sinnvoll, erspart in der Regel jedoch nicht die notwendigen Anpassungen spezifischer Betriebsvereinbarungen.

3. Betriebsrat – eigener Verantwortlicher im Sinne der DS-GVO? Ja!

Eine zurzeit heiß diskutierte Frage ist, welche Rolle der Betriebsrat im Sinne des Datenschutzes im Unternehmen überhaupt einnimmt. Ungeklärt ist, ob neben den möglichen anderen Akteuren, wie bspw. konzernangehörigen Tochterunternehmen, auch der Betriebsrat als eigener Verantwortlicher im Sinne der DS-GVO in Betracht kommt oder ob er entsprechend der langjährigen Rechtsprechung des BAG (vgl. BAG NZA 1998, 385) weiterhin dem Arbeitgeber als Verantwortlichem zuzurechnen ist. Adressat der Datenschutzgrundverordnung ist der Verantwortliche, also die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (vgl. Art. 4 Nr. 7 DS-GVO). Wie bereits bei den Informationspflichten erläutert, ist nicht zwangsläufig der Arbeitgeber der Verantwortliche im Sinne des Datenschutzes. Die Beantwortung der Frage nach der Eigenverantwortlichkeit von Betriebsräten ergibt sich nach Auffassung des LfDI BW aus der DS-GVO selbst: Entscheidet der Betriebsrat selbst über die Zwecke und Mittel der Verarbeitung personenbezogener Daten, ist er als eigener Verantwortlicher anzusehen.

Es gibt jedoch Stimmen, welche die Auffassung vertreten, dass die Mittel der Verarbeitung in der Regel durch den Arbeitgeber vorgegeben werden. Dieser würde über die im Unternehmen bestehende Infrastruktur (z. B. Telefonanschluss, Internetzugang, die auf den PCs aufgespielte Software) entscheiden. Auch wenn dies zutreffen mag, zeigt die aufsichtsrechtliche Erfahrung, dass die Frage, welches Mittel ein Betriebsrat zur Erfüllung seiner Aufgaben nutzt, in der Regel durch diesen selbst bestimmt wird. Der Betriebsrat entscheidet selbst, ob er bspw. eine Excel-Liste oder eine handschriftliche Liste von Mitarbeiterdaten anlegt oder wie er Vorgänge, die ihm von den Beschäftigten des Unternehmens gemeldet werden, dokumentiert, verwal-

tet oder ablegt. Nach Auffassung des LfDI BW sprechen somit die gewichtigeren Argumente dafür, dass der Betriebsrat selbst über die konkreten Mittel der Verarbeitung personenbezogener Daten entscheidet.

Auch bzgl. der weiteren Voraussetzung, über die Zwecke der Verarbeitung personenbezogener Daten zu entscheiden, werden unterschiedliche Meinungen vertreten. Die eine Seite ist der Auffassung, dass sich die Zwecke der Verarbeitung aus der betriebsverfassungsrechtlichen Stellung und der dem Betriebsrat durch das Betriebsverfassungsgesetz zugewiesenen Aufgaben ergeben und er damit nicht selbst über die Zwecke der Verarbeitung entscheiden würde. Gegen diese Ansicht spricht jedoch, dass sich auch in zahlreichen anderen Fallkonstellationen die Zwecke der Verarbeitung aus gesetzlichen Vorgaben ergeben. Verarbeitet ein Verantwortlicher personenbezogene Daten zu Zwecken, die gesetzlich vorgegeben werden (vgl. Art. 6 Abs. 1 Buchstabe c, Abs. 2 DS-GVO), vermag dies nichts an seiner datenschutzrechtlichen Verantwortlichkeit zu ändern. Somit sprechen gute Gründe dafür, dass der Betriebsrat auch dann über die Zwecke der Verarbeitung entscheidet, wenn ihm diese abstrakt vom Betriebsverfassungsgesetz vorgegebenen werden.

Weitere Argumente, weshalb dem Betriebsrat die Verantwortlichkeit im Sinne von Art. 4 Nr. 7 DS-GVO abgesprochen werden soll, konnten den LfDI BW bisher nicht überzeugen, da sie offensichtlich alleine von den (nicht erwünschten) Konsequenzen her gedacht sind. Insbesondere die Folge, dass der Betriebsrat beim Vorliegen der entsprechenden Voraussetzungen einen eigenen Datenschutzbeauftragten benennen müsse, wird als Begründung gegen die Verantwortlichkeit angeführt, da dem Arbeitgeber sonst zu hohe Kosten entstehen würden. Ergebnisse können jedoch nicht allein aus Praktikabilitätsgründen getroffen werden. Liegen die gesetzlichen Tatbestandsvoraussetzungen vor, muss das Resultat hieraus folgen und nicht aus Kostenerwägungen.

Welche Konsequenzen hat aber die Einstufung des Betriebsrats als eigener Verantwortlicher? Selbst für die Datenverarbeitung verantwortlich zu sein bedeutet auch, den von der DS-GVO auferlegten Pflichten als Verantwortlicher nachzukommen. Somit müssen auch Betriebsräte bspw. Auskunftsansprüche und Löschverpflichtungen erfüllen. Wie aber sieht es mit der Verhängung von Bußgeldern aus? Normadressat von Bußgeldern sind in aller Regel die Verantwortlichen. Somit kommen auch Bußgelder gegen Betriebsräte in Betracht. Problematisch ist, inwieweit der Betriebsrat nach nationalem Recht rechts- und vermögensfähig ist. Die Beantwortung dieser Frage wurde in der Vergangenheit von der Rechtsprechung unterschiedlich beantwortet. In einem Fall hat der Bundesgerichtshof dem Betriebsrat jedoch zumindest eine begrenzte Rechtsfähigkeit zugesprochen (vgl. BGH, Urteil v. 25.10.2012, III ZR 266/11). Es bleibt daher abzuwarten, wie sich die Thematik in Zukunft entwickelt. Möglich bleibt immer die Haftung des handelnden Betriebsratsmitglieds.

Dem LfDI BW ist die umstrittene Rechtslage durchaus bewusst. Welche Meinung sich zukünftig auch durchsetzt, jedenfalls haben Betriebsräte auf die Einhaltung der datenschutzrechtlichen Anforderungen hinzuwirken. Betriebsräte sollten sich daher nicht scheuen, weiterhin auf das Beratungsangebot unserer Behörde zurückzugreifen.

1.6.2 „Your Chief is watching you“ – Die Fortsetzung

In meinem letzten Tätigkeitsbericht hatte ich einen interessanten Fall aus dem Bereich des Beschäftigtendatenschutzes vorgestellt, in dem der Arbeitgeber insgesamt zehn Kameras zur Überwachung seiner Werkshallen und des Außenbereichs einsetzt hatte. Acht dieser Kameras erfassten dabei so gut wie alle Arbeitsplätze. Die Aufnahmen wurden auf einen Monitor übertragen, welcher sowohl für die Ge-

schäftsleitung als auch für die Mitarbeiter jederzeit einsehbar war. Zudem wurden die Aufnahmen für eine Dauer von drei Monaten gespeichert. Faktisch fand damit eine Dauerüberwachung der Mitarbeiter statt. Die Notwendigkeit der Videoüberwachung wurde 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, die einen Anhaltspunkt dafür hätten geben können, dass es sich hier nicht nur um eine Schutzbehauptung handelte, waren allerdings nicht gestellt worden. Auch wurde nichts vorgetragen, was einen konkreten Diebstahlsverdacht gegen einen oder mehrere Mitarbeiter hätte begründen können. Wir sahen die Videoüberwachung daher als unzulässig an, woraufhin der Arbeitgeber bei allen beschäftigten Arbeitnehmern Einwilligungserklärungen eingeholt hatte, wonach sich diese mit der lückenlosen Überwachung durch die Kameras am Arbeitsplatz einverstanden erklärten. Anders als der Arbeitgeber, der davon ausging, die Videoüberwachung sei nun von der Einwilligung gedeckt und damit zulässig, haben wir die freie Entscheidungsmöglichkeit der Mitarbeiter und damit die Freiwilligkeit der Einwilligungserklärungen jedoch in Zweifel gezogen. Aufgrund der ständigen Überwachung am Arbeitsplatz bzw. in der gesamten Produktionsstätte des Arbeitgebers war ein unbeobachtetes Arbeiten gar nicht mehr möglich. Hätten die Mitarbeiter die Einwilligung also widerrufen oder erst gar nicht erteilt, hätten sie dort überhaupt nicht mehr arbeiten können. Von Freiwilligkeit konnte daher keine Rede mehr sein.

Gegen den Arbeitgeber und Betreiber der Videoüberwachungsanlage habe ich daher gemäß § 38 Absatz 5 Satz 2 des Bundesdatenschutzgesetzes (noch in der alten Fassung) angeordnet, alle Kameras im Innenbereich abzuschalten und zu deinstallieren. Hiergegen erhob dieser Klage beim Verwaltungsgericht Stuttgart (VG Stuttgart), über welche am 12. Juli 2018 per Urteil entschieden wurde (Az.: 11 K 6401/16). Entgegen einem allgemeinen Trend bei vielen Arbeits- und Verwaltungsgerichten, datenschutzrechtliche Fragestellungen im Zusammenhang mit einer Videoüberwachung am Arbeitsplatz nur am Rande zu prüfen oder gar zugunsten der Arbeitgeber zu entscheiden, hat das VG Stuttgart eine Lanze für den Beschäftigtendatenschutz gebrochen. So argumentiert das Gericht, dass sich der Arbeitgeber im konkreten Fall weder auf die Möglichkeit der Einwilligung gemäß § 26 Absatz 2 des Bundesdatenschutzgesetzes (BDSG) stützen kann noch die Videoüberwachung nach § 26 Absatz 1 Satz 2 BDSG rechtmäßig sei. Im Einzelnen:

a) Wirksamkeit der Einwilligungserklärungen

Vor Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) bzw. des neuen Bundesdatenschutzgesetzes war unklar, ob im Rahmen von Beschäftigtenverhältnissen überhaupt in Datenverarbeitungsvorgänge wirksam eingewilligt werden kann. § 26 Absatz 2 BDSG beendet diese Diskussion, indem er die Einwilligung im Beschäftigungsverhältnis eindeutig zulässt, sie mit Blick auf das Merkmal der Freiwilligkeit aber an ganz besondere Voraussetzungen knüpft. So sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder der Arbeitgeber und die beschäftigte Person gleichgelagerte Interessen verfolgen. Das VG Stuttgart führt hierzu aus, dass soweit die Videoüberwachung dazu dienen solle, Straftaten – auch innerhalb der Belegschaft – zu verhindern, dies durchaus ein gleichgelagertes Interesse darstellen könne. Auch könne es sich für die Mitarbeiter als rechtlicher oder tatsächlicher Vorteil erweisen, dass sich durch die Videoüberwachung und –aufzeichnung der Verdacht von Straftaten ausräumen sowie eine darauf gestützte Verdachtskün-

digung verhindern lasse. Letzteres ist meiner Meinung nach allerdings nur dann der Fall, wenn den Mitarbeitern in solchen Fällen auch konkret Zugriff auf die relevanten Videodaten eingeräumt wird, sodass diese sich dann auch tatsächlich entlasten könnten. Ansonsten verbleibt die Entscheidung über die tatsächliche Verwendung der Daten beim Arbeitgeber, was diesem letztlich wieder einen einseitigen Vorteil verschafft. Das VG Stuttgart führt weiter aus, dass in den Fällen des § 26 Absatz 2 Satz 2 BDSG die Freiwilligkeit nicht von Gesetzes wegen anzunehmen sei, vielmehr sei die Prüfung unter Berücksichtigung von § 26 Absatz 2 Satz 1 BDSG und den allgemeinen Kriterien zur Beurteilung der Freiwilligkeit nach Art. 7 Absatz 4 DS-GVO gerade nicht entbehrlich. Vielmehr hebe der Gesetzgeber durch eine Art Regelbeispiel hervor, in welchen Fällen die Freiwilligkeit vorliegen könne (so das VG Stuttgart mit Verweis auf BeckOK Wolff/Brink DatenschutzR/Riesenhuber BDSG 2018 § 26 Rn. 47). Sieht man sich hierzu die Gesetzesbegründung näher an, so fällt auf, dass diese Regelbeispiele zwar Eingriffe in das Recht auf informationelle Selbstbestimmung bzw. den Schutz personenbezogener Daten darstellen, die Eingriffe aber lediglich eine geringe Eingriffstiefe aufweisen. So werden beispielsweise genannt: Die Einführung eines betrieblichen Gesundheitsmanagements zur Gesundheitsförderung oder die Erlaubnis zur Privatnutzung von betrieblichen IT-Systemen, die Aufnahme von Name und Geburtsdatum in eine Geburtstagsliste oder die Nutzung von Fotos für das Intranet (vgl. BT Drucksache 18/11325 vom 24.02.2017). Eine dauerhafte Videoüberwachung am Arbeitsplatz ist damit definitiv nicht zu vergleichen.

Im zu entscheidenden Fall war darüber hinaus aufgrund mehrerer Umstände nicht von einer Freiwilligkeit auszugehen. So stellt das VG Stuttgart zum einen auf den Zeitpunkt der Abgabe der Einwilligungserklärung ab. Die betroffenen Mitarbeiter der Klägerin hätten diese zu einem Zeitpunkt abgegeben, als die Videokameras schon installiert waren. Damit wäre für die Mitarbeiter ersichtlich gewesen, dass der Arbeitgeber bereits Aufwendungen getätigt und ein Interesse daran hatte, die Überwachung auch durchzuführen. Mit Vorlage der Einwilligungserklärungen zur Unterschrift hätte man die Mitarbeiter in die Lage versetzt, sich durch eine etwaige Verweigerung der Unterschrift den Plänen ihres Arbeitgebers entgegenzustellen. Dies stelle eine Einwirkung auf die innere Freiheit der Willensentscheidung dar, welche noch durch einen gewissen Gruppenzwang – die Erklärungen wurden ja allen Mitarbeitern vorgelegt – verstärkt worden sei. Jeder Mitarbeiter hätte, so das VG Stuttgart in seiner Entscheidung weiter, damit rechnen müssen, dass die Durchführung der Videoüberwachung allein aufgrund seiner Verweigerung nicht oder nur teilweise zu realisieren sein würde.

Diesen Ausführungen des VG Stuttgart ist vorbehaltlos zuzustimmen. Dabei spielt aber noch ein weiterer Gesichtspunkt eine wichtige Rolle: Von Freiwilligkeit kann nämlich auch dann nicht gesprochen werden, wenn man die Folgen der Verweigerung bzw. des Widerrufs einer erteilten Einwilligung für das konkrete 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. Im konkreten Fall wäre ein Arbeiten am überwachten Standort nämlich gar nicht mehr möglich gewesen, wurden doch alle Bereiche der Werkshallen systematisch von den Kameras erfasst. Selbst wenn der eigentliche Arbeitsplatz in einen „nicht unmittelbar überwachten Bereich" verlegt worden wäre, wäre der Mitarbeiter doch bei vielen anderen Arbeitsschritten überwacht worden. Kurzum: Der Dauerüberwachung hätte man sich nicht entziehen können, vielmehr hätte es dem Arbeitsverhältnis die Grundlage entzogen. Faktisch hatte der einzelne Mitarbeiter somit keine Wahlfreiheit.

Indem das VG Stuttgart bei der Beurteilung der Freiwilligkeit der Willensentscheidung auf objektive Kriterien abgestellt hat, war für ein Einvernehmen der Beschäftigten im konkreten Fall kein Raum. Das Gericht hat in der mündlichen Verhandlung auch deutlich gemacht, dass es davon ausgeht, dass § 26 Absatz 2 BDSG nicht zwingend einer subjektiven Komponente bedarf, die Freiwilligkeit aufgrund des Aufbaus der Norm vielmehr anhand objektiver Kriterien im Einzelfall bestimmt werden kann. Dem kann nur zugestimmt werden. Wenn der Mitarbeiter schon bei der Abgabe der Einwilligungserklärung nicht wirklich freiwillig entscheiden kann, wie „frei"(willig) soll er dann vor Gericht aussagen? Das Abstellen auf objektive Kriterien stellt somit letztlich den einzelnen Mitarbeiter unter Schutz.

b) Keine Rechtmäßigkeit der Videoüberwachung nach § 26 Absatz 1 Satz 2 BDSG

Im Weiteren setzt sich das VG Stuttgart auch mit der Erlaubnisnorm des § 26 Absatz 1 Satz 2 BDSG auseinander. Danach dürfen zur Aufdeckung von Straftaten personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Auch wenn das VG Stuttgart nur knapp argumentiert, dass es bereits deshalb an den Voraussetzungen der Norm fehle, weil die Klägerin schon keine Person innerhalb ihrer Belegschaft benannt habe, gegenüber welcher der Verdacht der Straftat bestünde und eine Datenerhebung dann ohnehin auch nur hinsichtlich dieser Person erfolgen könne, so ist die (alleinige) Prüfung des § 26 Absatz 1 Satz 2 BDSG ein erhebliches Indiz dafür, dass das Gericht im Falle einer Videoüberwachung, die konkret nur den eigenen Beschäftigten gilt, weil sie beispielsweise im nicht öffentlich zugänglichen Bereich stattfindet, § 26 Absatz 1 Satz 2 als lex specialis im Verhältnis zu Satz 1 sieht. Das ist absolut folgerichtig, können doch bei Vorliegen eines konkreten Straftatverdachts keine höheren Anforderungen gestellt werden als bei abstrakten Verdächtigungen bzw. einer deutlich niedrigeren Deliktsschwelle. Umso mehr haben verschiedene Urteile im Zusammenhang mit Videoüberwachung im Beschäftigungsverhältnis verwundert, in denen – insbesondere in nicht öffentlich zugänglichen Bereichen – lediglich § 26 Absatz 1 Satz 1 BDSG als Rechtsgrundlage geprüft wurde, somit eine Videoüberwachung „pauschal" und „auf Vorrat" gegenüber den eigenen Beschäftigten eingesetzt werden durfte (zuletzt BAG, Urteil vom 23.08.2018, Az. 2 AZR 133/18, OVG des Saarlands, Urteil vom 14.12.2017, Az. 2 A 662/17) und daher im Ergebnis letztlich die besondere Schutzbedürftigkeit des Arbeitsverhältnisses bei einer Videoüberwachung gar nicht oder nur sehr eingeschränkt berücksichtigt wurde.

Mit der (alleinigen) Prüfung des § 26 Absatz 1 Satz 2 BDSG wird auch klar, dass Videoüberwachung am Arbeitsplatz immer nur das letzte Mittel sein kann – d. h. nur als ultima ratio zulässig ist. Der Arbeitgeber darf also gerade nicht „vorbeugend" Daten sammeln, um eventuelle zukünftige Straftaten zu dokumentieren. Vielmehr darf die Videoüberwachung nur und erst dann eingesetzt werden, wenn der konkrete Verdacht einer strafbaren Handlung gegenüber einem bestimmten Arbeitnehmer oder einem zumindest individuell eingrenzbaren Personenkreis besteht. Und auch dann muss der Arbeitgeber zuvor alle anderen, gleich effektiven Maßnahmen erfolglos eingesetzt haben bzw. deren Verwendung geprüft und nachvollziehbar verworfen haben.

Mein Rat an die Arbeitgeber: Das tiefe Misstrauen gegenüber den eigenen Mitarbeitern, das sich in einer Videoüberwachung auf „Vorrat" ausdrückt, sollte einer offenen Unternehmenskultur weichen, in der den

Mitarbeitern Vertrauen entgegengebracht wird. Das bedeutet nicht, dass Unternehmen Diebstähle oder andere Straftaten ihrer Mitarbeiter tolerieren müssten. Aber es bedeutet, nur ein solches Kontrollsystem zu etablieren, dass bei strafrechtlichen Auffälligkeiten Maßnahmen in Gang setzt, die im Hinblick auf ihre Eingriffstiefe gestaffelt aufeinander aufbauen und eine Dokumentation der einzelnen Maßnahmen vorsieht. Am Ende kann und darf dann auch eine zulässige Videoüberwachung auf Grundlage des § 26 Absatz 1 Satz 2 BDSG stehen.

In unserem geschilderten Fall ist leider noch nicht das letzte Wort gesprochen. Grund: Der Arbeitgeber hat Berufung gegen das o. g. Urteil des VG Stuttgart eingelegt. Es bleibt also abzuwarten, wie der VGH Baden-Württemberg entscheiden wird.

1.6.3 Der überfürsorgliche Datenschutzverstoß

Die übertrieben verstandene Fürsorgepflicht einer Personalleiterin kann auch mal schnell zu einem Datenschutzverstoß führen und möglicherweise ein Bußgeldverfahren nach sich ziehen. Es gilt daher: Fürsorge schön und gut, aber nicht um den Preis des Beschäftigtendatenschutzes!

Eine Beschäftigte der Verwaltung eines Krankenhauses hat sich an uns gewandt und uns Folgendes mitgeteilt: Sie ließ sich aufgrund einer Krebserkrankung im Krankenhaus ihres Arbeitgebers behandeln und fiel krankheitsbedingt für mehrere Monate aus. Nach Rückkehr aus dem Krankenstand nahm die Personalleiterin Einsicht in ihre Patientenakte, um angebliche Zweifel an der Leistungsfähigkeit zu beseitigen.

Eine Einsichtnahme in die Patientenakte, aufgrund der Fürsorgepflicht der Personalleiterin ist nach Art. 88 DS-GVO i. V. m. § 26 Abs. 3 BDSG für Zwecke des Beschäftigungsverhältnisses nur dann zulässig, wenn es zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Beschäftigten an der Vertraulichkeit ihrer Patientendaten überwiegt.

Liegen Anhaltspunkte für die Gefährdung der Gesundheit des Beschäftigten vor, besteht für den Arbeitgeber zweifellos eine Fürsorgepflicht gegenüber seinem Beschäftigten. Die Einsicht in die Patientenakte ohne das Einverständnis des Beschäftigten stellt allerdings einen erheblichen Eingriff in die Persönlichkeitssphäre des Beschäftigten dar, da es sich bei Daten zum Gesundheitszustand einer Person um besondere Arten personenbezogener Daten handelt, die entsprechend vor dem Zugriff Dritter zu schützen sind (vgl. Art. 4 Nr. 15 i. V. m. Art 9 DS-GVO). Da der Zweck der Fürsorgepflicht auch durch gleich geeignete mildere Mittel, wie vorsichtiges Nachfragen beim Beschäftigten zu seiner Arbeitsfähigkeit, das Führen eines offiziellen Mitarbeitergespräches oder die Aufforderung, die Leistungsfähigkeit durch den Betriebsarzt klären zu lassen, hätte erreicht werden können, ist die Einsichtnahme in die Patientenakte des Beschäftigten unverhältnismäßig und stellt damit einen datenschutzrechtlichen Verstoß dar.

Eine Einsichtnahme durch die Personalleiterin als Nichtzugriffsberechtigte ist vom Arbeitgeber durch geeignete technisch-organisatorische Maßnahmen zu verhindern. Das Beschwerdeverfahren wurde daher an die Bußgeldstelle weitergeleitet. Diese wird die Notwendigkeit der Einleitung eines Bußgeldverfahrens gegen die Personalleiterin bzw. das Krankenhaus prüfen.

1.6.4 Wenn das Foto weg muss

Unternehmen zeigen in der heutigen digitalen Zeit immer mehr Präsenz via Internet und wollen mit einer aussagekräftigen Homepage den ersten Kontakt zu ihren Kunden herstellen. Dazu sollen neben den allgemeinen Kontaktdaten des Ar-

beitnehmers häufig auch Mitarbeiterfotos veröffentlicht werden. Die Aufnahme und Bereitstellung von Fotos der Angestellten auf einer öffentlich zugänglichen Internetseite, aber auch im Intranet oder bei einem betriebsinternen Aushang, muss aber besonderen rechtlichen Anforderungen genügen, welche Arbeitgeber kennen und beachten müssen.

Lichtbilder sind personenbezogene Daten gemäß Art. 4 Nr. 1 der DS-GVO, weil sie die Identifikation des Betroffenen ermöglichen. Nach dem Grundsatz des Verbots mit Erlaubnisvorbehalt bedarf es für ihre Verarbeitung demnach einer rechtlichen Grundlage. Die für den Beschäftigungskontext spezielle Norm des § 26 BDSG kann hierbei nicht angewendet werden, da eine Erforderlichkeit der Datenverarbeitung „Nutzung eines Fotos" für die Durchführung des Beschäftigungsverhältnisses in der Regel nicht angenommen werden kann – anders mag es sich beispielsweise bei einem Pressesprecher verhalten. Entsprechendes gilt im Bereich des Beschäftigtendatenschutzes für eine mögliche Rechtfertigung nach Art. 6 Abs. 1 f) DS-GVO, welcher die Datenverarbeitung bei Vorliegen eines überwiegenden Interesses seitens des Verantwortlichen ermöglicht. Zwar wird man ein kundenorientiertes Erscheinungsbild grundsätzlich als berechtigtes Interesse eines Arbeitgebers anerkennen können. Es darf aber nicht vergessen werden, dass eine Veröffentlichung von personenbezogenen Daten im Internet von jedermann global abrufbar ist und die gefundenen Informationen zu einer Person problemlos mit weiteren im Netz vorhandenen Daten zu Persönlichkeitsprofilen zusammengeführt werden können. Schon die Veröffentlichung der allgemeinen Kontaktdaten des Beschäftigten im Internet ist deshalb nur gerechtfertigt, wenn die vertragliche Tätigkeit auch Beziehungen zu Außenkontakten mit sich bringt und der Beschäftigte als direkter Ansprechpartner fungieren soll. Will ein Unternehmen darüber hinaus der Öffentlichkeit auch ein Foto des Mitarbeiters präsentieren, führt kein Weg an der Einwilligung des Abgebildeten vorbei. Damit die Einwilligung wirksam ist, muss sie zwingend vor – und nicht erst nach – der Aufnahme und ihrer Veröffentlichung eingeholt werden. Weiterhin sind die strengen Voraussetzungen für eine Einwilligungserklärung zur Informiertheit, Bestimmtheit und Transparenz zu beachten (vgl. Art. 7 DS-GVO). Werden diese erfüllt, spricht bezüglich der Verarbeitung von Mitarbeiter-Fotos auch nichts dagegen, die Einwilligung in Form einer Generalerklärung einzuholen, die sich allgemein auf sämtliche Fotoaufnahmen bei internen Veranstaltungen und die entsprechenden Zwecke der Verarbeitung bezieht. Lediglich, wenn sich der beabsichtigte Zweck der Verarbeitung der Fotografie nachträglich ändert, ist erneut eine separate Einwilligungserklärung notwendig.

Wie mit den Mitarbeiterfotos zu verfahren ist, wenn das Arbeitsverhältnis beendet worden ist, soll der folgende Fall aus unserer Praxis zeigen:

Auf einem Gruppenfoto der Belegschaft war auch ein ehemaliger Arbeitnehmer unter ca. einem Dutzend anderer Kollegen abgebildet. Über diese im Netz veröffentlichte Nutzung beschwerte sich nun der ehemaliger Arbeitnehmer. Er verlangte, dass sein Foto heruntergenommen wird. Statt einer Löschung wurde nun aber auf dem Foto sein Kopf heraus- und der einer anderen Person per Foto-Retusche hineingeschnitten.

Vom ursprünglichen Vorliegen der erforderlichen Einwilligung konnten wir im vorliegenden Fall ausgehen. Diese wurde vom ehemaligen Beschäftigten aber widerrufen, was möglich und wirksam ist (vgl. Art. 7 Abs. 3 Satz 1 DS-GVO). Ein Widerruf verpflichtet das Unternehmen zur Löschung. Andererseits führt das Ende des Arbeitsverhältnisses nicht automatisch zum Erlöschen des Rechts des Arbeitgebers an der Verwendung von Mitarbeiterfotos. Es darf nicht übersehen werden, dass es – auch finanziell – sehr aufwändig wäre, wenn der Arbeitgeber jedes Mal, wenn jemand aus dem Unternehmen ausscheidet, sämtliche

Belegschaftsfotos erneuern oder die Person unkenntlich machen müsste. Da es sich bei den Bildern auf der Internetseite nicht um die Aufnahmen einzelner Personen handelte, denen eine Identität klar zugeordnet werden konnte, sondern um solche von größeren Gruppen, durch die jeweils alle Mitarbeiter gezeigt wurden, kamen wir zu dem Ergebnis, dass es dem Unternehmen bei der Verwendung der Bilder augenscheinlich um eine allgemeine Darstellung des Unternehmens ging. Einzelne Personen und Persönlichkeiten der Arbeitnehmer wurden nicht hervorgehoben, ihre Namen nicht genannt und die Identität ihrer Person auch sonst nicht herausgestellt. Zudem entstand beim Betrachter nicht zwingend der Eindruck, es handele sich zweifelsohne um die vollständige aktuelle Belegschaft. Durch die Demontage des Kopfes des Betroffenen und das Einsetzen des Kopfes einer anderen Person auf den Fotos konnte der Anspruch des Betroffenen, nicht mehr hinreichend erkennbar bzw. identifizierbar zu sein, deshalb ausreichend erfüllt werden, sodass kein Recht auf vollumfängliche Löschung bestand.

Widerruft der Beschäftigte seine Einwilligung, bleibt dem Arbeitgeber mangels anderer Rechtsgrundlage, auf die er die Verarbeitung stützen könnte, keine andere Wahl: Das Foto muss weg oder zumindest retuschiert werden, um eine Identifizierung auszuschließen.

1.6.5 Immer auf dem neuesten Stand der Technik – oder?

Auch Arbeitgeber müssen als Verantwortliche unter Berücksichtigung des Stands der Technik geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DS-GVO treffen, um bei der Verarbeitung von Beschäftigtendaten ein angemessenes Schutzniveau für die Rechte und Freiheiten der betroffenen Personen zu gewährleisten. Im digitalen Zeitalter sind solche Schutzmaßnahmen unerlässlich.

Für ein Unternehmen kann die (zusätzliche) Bereitstellung eines Bewerbungsformulars auf der Firmen-Homepage den Prozess der Suche nach neuen Arbeitnehmern enorm erleichtern. Indem interessierte Kandidaten ihre Bewerbungsunterlagen direkt über das Formular in digitaler Form zur Verfügung stellen, können diese ganz einfach abgespeichert und bei Bedarf abgerufen werden. Es besteht nicht mehr die Notwendigkeit, Stapel von Bewerbungsmappen mit zahlreichen Dokumenten wie Lebensläufen und Zeugnissen durchzugehen. Dass bei solcher Vorgehensweise ganz besondere Vorsicht geboten ist, zeigt der folgende Fall:

Durch eine Beschwerde wurden wir auf die Internetseite eines Bäckerei-Unternehmens aufmerksam gemacht, die sehr tief blicken ließ. Über die bloße Eingabe des Firmennamens in Kombination mit einem entsprechenden Schlagwort wie „Lebenslauf" oder „Bewerbung" in die gängigen Internet-Suchmaschinen gelangte man zu Einträgen, deren Überschriften bereits häufig in Reinschrift Name, Anschrift, Geburtsdatum oder E-Mail-Adresse von Bewerbern der letzten Jahre wiedergaben, ohne dass auch nur ein weiterer Klick notwendig war. Ebenso erhielten wir den Hinweis auf ein ungeschütztes Verzeichnis der Homepage, in dem verschiedene Unterlagen der Bewerber des Unternehmens zu finden waren. Zu allen Dokumenten und Daten in den Suchergebnissen sowie in dem Verzeichnis war der offene Zugang von außen möglich, ohne jede Zugriffsbeschränkung, Abfrage eines Passworts oder eine sonstige Form der Authentifizierung. So konnten ohne weiteres neben Bewerbungsanschreiben, Lebensläufen und Zeugnissen sogar auch sensibelste Daten wie Personalausweis-Kopien eingesehen werden. Der Ursprung des Übels war schnell gefunden: Die Kontakt- und Bewerbungsformulare auf der Website wurden nicht über eine verschlüsselte Verbindung angeboten, die Übertragung der dort gemachten Angaben mit den hochgeladenen Unterlagen erfolgte also vollkommen ungesichert – ebenso die Speicherung auf dem Webserver. Und

das über einen Zeitraum von etwa neun Monaten hinweg.
Dieser eklatante Datenschutzverstoß musste nach Bekanntwerden selbstverständlich dringend behoben werden. Der Verantwortliche wurde umgehend kontaktiert und über die mangelhafte Konfiguration der Homepage in Kenntnis gesetzt. Gleichzeitig forderten wir ihn dazu auf, die Bewerbungsunterlagen sofort zu löschen oder zumindest ein sicheres Zugangskonzept mit Passwort-Abfrage zu implementieren, um den unberechtigten Zugriff von Dritten auf die Bewerberdaten zu unterbinden. Die Umsetzung dieser Forderungen erfolgte glücklicherweise prompt, das Unternehmen gestand die gemachten Fehler allesamt ein und zeigte ehrliches Bedauern des Vorfalls. Die Dokumente wurden von dem Server gelöscht und sowohl das Bewerberportal als auch die Kontaktformulare gesperrt bzw. von der Website genommen. Bei den Betreibern der Internet-Suchmaschinen (insbesondere Google) wurde die Löschung der Links beantragt, die zu den Bewerberdaten führten. Außerdem zog die Homepage auf einen neuen Server um und wird nun mit TLS-Verschlüsselung betrieben. Nach entsprechender Absprache mit uns sind auch die Formulare auf der Internetseite wieder online, die durch eine verschlüsselte Auslieferung nunmehr ebenfalls den Sicherheitsstandards entsprechen.

Wie dieses Fallbeispiel deutlich macht, sind besonders die von Art. 32 Abs. 1 lit. a) und b) DS-GVO geforderten technischen Maßnahmen zur Verschlüsselung bzw. zur dauerhaften Sicherstellung der Vertraulichkeit der Systeme und Dienste von zentraler Bedeutung im Umgang mit Online-Bewerberdaten. Arbeitgeber sind gehalten, sich stets über den Stand der Technik und eine entsprechende Umsetzung – gerade auch durch eingeschaltete Dienstleister – auf dem Laufenden zu halten, um selbst den Datenschutzvorgaben jederzeit entsprechen zu können. Ist ein solches Wissen nicht vorhanden, kann es dem Arbeitgeber wie im vorliegenden Fall schnell passieren, dass von ihm unbemerkt (schwerwiegende) Verstöße gegen das Datenschutzrecht passieren, für die er als Verantwortlicher geradestehen muss. Dies explizit auch vor dem Hintergrund der möglichen Verhängung eines empfindlichen Bußgeldes nach Art. 83 DS-GVO. Ob die Einleitung eines Bußgeldverfahrens gegen das hier verantwortliche Bäckerei-Unternehmen notwendig und geboten ist, wird derzeit von der Bußgeldstelle geprüft.

1.6.6 Wenn die Kollegen Bescheid wissen

Wie die Vielzahl an Datenpannen im Berichtszeitraum zeigt, bleiben auch im Bereich des Beschäftigtendatenschutzes Meldungen nach Art. 33 Abs. 1 DS-GVO an die Aufsichtsbehörden nicht aus. Geht das Unternehmen zusätzlich von einem hohen Risiko für die persönlichen Rechte und Freiheiten der Beschäftigten aus, sind auch diese über Verletzung des Schutzes ihrer personenbezogenen Daten zu informieren (vgl. Art. 34 DS-GVO).

Einer Anfrage eines Beschäftigten ging eine solche Meldung nach Art. 34 DS-GVO seines Arbeitgebers voraus. Der Arbeitgeber informierte den Beschäftigten darüber, dass seine Entgeltabrechnung einer überschaubaren Anzahl an Kollegen durch eine Fehleinstellung an der Kuvertiermaschine zugeschickt wurde. Die Gehaltsabrechnung enthielt die üblichen personenbezogenen Daten, insbesondere Angaben über die Höhe der Vergütung sowie Art und Höhe von Zuschlägen und Zulagen. Natürlich waren auch die Art und Höhe der Abzüge aufgelistet. Die Mitteilung über die Datenpanne reichte dem Beschäftigten jedoch nicht aus. Er wollte wissen welche Kollegen genau über sein gezahltes Gehalt und seine Abzüge im Bilde sind und machte von seinem Auskunftsanspruch aus Art. 15 DS-GVO gegenüber seinem Arbeitgeber Gebrauch. Das Auskunftsersuchen über die einzelnen Empfänger wurde vom Arbeitgeber jedoch mit dem Verweis abgelehnt, dass Art. 34 DS-GVO die Mitteilung solcher Informa-

tionen nicht vorsehe. Der Beschäftigte bat uns daher um unsere Einschätzung: In der Tat sieht Art. 34 DS-GVO nicht vor, dass das Opfer einer Datenpanne über die einzelnen Empfänger unterrichtet wird. Macht die betroffene Person jedoch einen Auskunftsanspruch nach Art. 15 DS-GVO geltend, ist der Auskunftsersuchende auch über die Empfänger oder Kategorien von Empfängern, gegenüber denen personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden sollen, zu beauskunften.

In der bisherigen Rechtsprechung wurde dem Verantwortlichen ein Wahlrecht hinsichtlich der Mitteilung über die Empfänger oder die Kategorien von Empfängern zugestanden (vgl. AG München, Urteil vom 08. August 2017 – 172 C 1891/17 –, juris, Rn. 68). Diese Rechtsprechung ist jedoch noch zur alten Rechtslage ergangen und hat lediglich nationale Vorschriften, insbesondere § 34 BDSG-alt, in Bezug genommen. Eine Übertragung ist daher nicht ohne weiteres auf die durch die DS-GVO geänderte Rechtslage möglich. Bei der DS-GVO handelt es sich um eine europäische Verordnung die als solche unmittelbare Wirkung in allen Mitgliedsstaaten entfaltet und unmittelbar anwendbares Recht ist. Die Karten wurden also neu gemischt.

Nach Auffassung des LfDI BW steht dem Auskunftsersuchenden und nicht dem Verantwortlichen das Wahlrecht über die Nennung der konkreten Empfänger oder die Kategorien von Empfängern zu. Möchte dieser lediglich die Kategorien von Empfängern erfragen, muss der Verantwortliche auch nur diese beauskunften. Möchte die betroffene Person jedoch auch Auskunft über die einzelnen Empfänger, muss der Verantwortliche ihm diese grundsätzlich mitteilen, soweit er sie noch kennt. Hat der Verantwortliche sie nicht gespeichert, ist er nicht verpflichtet weitere Anstrengungen zu unternehmen, um die einzelnen Empfänger herauszufinden. Zu berücksichtigen ist jedoch, dass der Verantwortliche im Rahmen der Auskunftserteilung nicht nur die Grundrechte des Auskunftsersuchenden, sondern auch die Grundrechte derjenigen Personen nicht verletzen darf, deren personenbezogene Daten durch die Auskunftserteilung offenbart werden würden. Insoweit bedarf es einer grundrechtskonformen Auslegung von Art. 15 DS-GVO. Ereignet sich also eine Datenpanne nach Art. 33 DS-GVO, bei der Beschäftigten personenbezogene Daten von Kollegen unrechtmäßiger Weise offenbart werden, müssen die verschiedenen Grundrechtspositionen in einen schonenden Ausgleich zueinander gebracht werden. Je nachdem, welches Grundrecht stärker zu gewichten ist, hat der Verantwortliche zu entscheiden, ob die Auskunftserteilung lediglich die Kategorien von Empfängern oder die Empfänger selbst umfasst. In dem zu beurteilenden Fall, stuften wir das Interesse des Beschäftigten an der Offenlegung der einzelnen Kollegen höher ein. Zu einer gegenteiligen Auffassung hätte man gelangen können, wenn konkrete Anhaltspunkte dafür bestehen würden, dass den Kollegen durch diese Information an den Betroffenen konkrete Schäden drohen.

Selbstverständlich haben Unternehmen kein Interesse an Datenpannen. Diese verursachen nicht nur administrativen Aufwand gegenüber den Aufsichtsbehörden, sondern möglicherweise auch gegenüber den von der Datenpanne betroffenen Personen. Werden hieraufhin Betroffenenrechte – wie Auskunftsansprüche– geltend gemacht, kann der Verursacher sich nicht ohne weiteres aus der Affäre ziehen. Ein Grund mehr, seine Systeme durch routinemäßige Checks noch sicherer zu machen und Datenpannen vorzubeugen.

1.7 G 20-Gipfel 2017

Der G 20-Gipfel am 7. und 8. Juni 2017 in Hamburg war nicht nur überschattet von Gewaltexzessen einzelner Gruppen von Gipfelgegnern. Als bekannt wurde, dass 32 Medienvertretern die Akkreditierung wegen angeblicher Sicherheitsbedenken entzogen worden waren, löste dies ebenfalls ein heftiges öffentliches Echo aus.

Kurz nach Bekanntwerden der Vorwürfe, dies sei auf fehlerhafte Datenspeicherungen und -übermittlungen von Sicherheitsbehörden zurückzuführen, habe ich eine Untersuchung der Vorgänge angeordnet, soweit baden-württembergische Behörden und Journalisten, die aus Baden-Württemberg stammen oder hier arbeiten, betroffen waren. Über das Ergebnis habe ich dem Innenausschuss des Landtags von Baden-Württemberg im September 2018 berichtet. Kurz zusammengefasst kann Folgendes festgestellt werden:

Seit etlichen Jahren erfolgen Zuverlässigkeitsüberprüfungen als Voraussetzung für die Zulassung zu Großveranstaltungen jeder Art ohne gesetzliche Grundlage, einzig und allein auf der Basis einer „freiwilligen" Einwilligung. Was ursprünglich einmal als singuläres Verfahren (Fußball-Weltmeisterschaft 2006) von einem meiner Vorgänger als gerade noch hinnehmbar akzeptiert worden war, nämlich die massenhafte sicherheitsbehördliche Durchleuchtung ohne gesetzliche Grundlage von Bürgern, die als freiwillige Helfer, als Dienstleister oder auch als Journalisten Zutritt zu Veranstaltungsorten bekommen sollten, hat sich im Lauf der Jahre leider als Standard verselbständigt. Dem Begriff „Sommermärchen" kommt damit eine völlig neue Bedeutung zu.

Meine Kritik an diesem seit Jahren bestehenden und schon von meinen Vorgängern wiederholt beklagten datenschutzrechtlichen Missstand scheint nun endlich auf Gehör gestoßen zu sein. Sowohl findet sich im neuen Landesdatenschutzgesetz eine, wenn auch nur rudimentäre, Regelung zur Zuverlässigkeitsüberprüfung; auch das in Arbeit befindliche Polizeigesetz soll die Rahmenbedingungen für diese intensiven Eingriffe in das informationelle Selbtsbestimmungsrecht der Betroffenen vorgeben.

Inhaltlich war zu prüfen, ob die für die Feststellung, dass gegen die betroffenen Journalisten Sicherheitsbedenken bestehen, herangezogenen Daten der Polizei und des Verfassungsschutzes in den jeweiligen Auskunftssystemen zulässigerweise gespeichert werden durften.

Die Prüfung beim Landesamt für Verfassungsschutz ergab zwar keine Mängel hinsichtlich der gespeicherten Daten. Die hieraus gezogenen Schlussfolgerungen, wonach bei den vom Bundesamt für Verfassungsschutz angefragten Journalisten sicherheitsbehördliche Bedenken bestanden, waren auch nachvollziehbar. Eine nähere rechtliche Prüfung war mir jedoch deshalb nicht möglich, weil in keinem der Fälle die Gründe für die Entscheidungen dokumentiert worden waren. Auch das für die Letztentscheidung zuständige Bundesamt für Verfassungsschutz konnte insoweit nur das nicht näher begründete Votum zur Kenntnis nehmen und musste auf dieser Grundlage über die Zulassung oder die Ablehnung befinden. Angesichts dessen, dass insbesondere mit dem Ausschluss von Journalisten aus solchen Veranstaltungen tief in das Grundrecht auf freie Presseberichterstattung eingegriffen wird, halte ich eine Verfahrensweise, die mangels Dokumentation der entscheidungserheblichen Erwägungen eine echte Überprüfung nicht ermöglicht, für inakzeptabel.

Die Prüfung der Datenlage bei der Polizei bestätigte erneut, was sich schon bei früheren Prüfungen gezeigt hat: Eindeutig gesetzeswidrig in der Sache war keine der Speicherungen. Vielfach fehlte es aber an einer nachvollziehbaren Dokumentation der Gründe für das Vorliegen einer Wiederholungsgefahr. Diese ist Voraussetzung dafür, dass Daten überhaupt bzw. für einen bestimmten Zeitraum ge-

speichert werden dürfen. Häufig wird hier lediglich mit Schlagworten gearbeitet, deren Konkretisierung sich zwar mühsam aus den Akten herleiten lässt, die aber nicht wirklich erkennen lassen, welche Gründe der Prognose tatsächlich zugrunde lagen. Ebenfalls fehlte es meist an einer Dokumentation der Gründe, die der Annahme einer länderübergreifenden Bedeutung von Straftaten zugrunde lagen und diese belegen konnten. Dies ist Voraussetzung dafür, dass solche Sachverhalte im bundesweiten polizeilichen Auskunftssystem INPOL gespeichert werden dürfen. Und schließlich fiel auf, dass die Polizei geneigt zu sein scheint, bei der Vergabe von Löschfristen eher an die oberste Grenze des Zulässigen zu gehen, anstatt jeweils einzelfallbezogen angemessene Fristen zu bestimmen.

Mein Fazit der Prüfung lautete: Der im Mittelpunkt der medialen Wahrnehmung stehende Vorwurf, im Zusammenhang mit dem G20-Gipfel seien Journalisten zu Unrecht Akkreditierungen entzogen worden, weil Polizei- und Verfassungsschutzbehörden Daten der Betroffenen zu Unrecht speichern würden, hat sich zwar in der Gesamtbetrachtung nicht belegen lassen, ließ sich aber mangels verwertbarer Dokumentationen auch nicht in jedem Fall ausräumen. Zu kritisieren bleibt darüber hinaus erneut die Praxis der polizeilichen Speicherungen.

1.8 Ärzte und DS-GVO (Datenschutzerklärung)

Es mag verwundern, dass wir ausgerechnet den Ärzten mit Blick auf die Schwierigkeiten bei der Anpassung an die zum 25. Mai 2018 wirksam gewordene Datenschutz-Grundverordnung (DS-GVO) hier einen eigenen Beitrag widmen, und nicht beispielsweise auch Angehörigen anderer Berufe. Schließlich hatten alle, einschließlich der Datenschutzaufsichtsbehörden, ihre mehr oder weniger großen Probleme, die neuen Datenschutzvorschriften der DS-GVO richtig zu verstehen und anzuwenden. Die Gründe hierfür sind:

Durch eine Vielzahl hier eingegangener Anfragen und Beschwerden wurde deutlich, dass nicht wenige Ärzte im Land, etwa unter dem Eindruck irreführender Schulungsveranstaltungen oder von einigen Organisationen verbreiteter fehlerhafter Vordrucke, wesentliche Regelungen der DS-GVO, insbesondere über datenschutzrechtliche Einwilligungen ihrer Patienten, gründlich missverstanden haben. Immer wieder wurde uns mitgeteilt, Ärzte würden ihre (potentiellen) Patienten mit der Aussage unter Druck setzen, diese müssten Vordrucke für datenschutzrechtliche Einwilligungen unterschreiben, andernfalls hätten sie ohne ärztliche Behandlung oder sonstige Betreuung die Arztpraxis zu verlassen. Natürlich kann es auch für Besucher eines Friseursalons oder einer Spielhalle unerfreulich sein, bei Verweigerung der Unterschrift unter solch einen Vordruck gezwungenermaßen auf den gewünschten Service zu verzichten. Es bedarf aber sicher keiner Erläuterung, dass etwa für einen Schmerzpatienten mit vereitertem Backenzahn die Abweisung durch „seinen" Zahnarzt in der Regel eine gravierendere Bedeutung haben dürfte als ein verweigerter Haarschnitt oder versagter Spielspaß.

Ärztliche Behandlung nur nach datenschutzrechtlicher Einwilligung?
Nein.
Eine Quelle des Übels war die, beispielsweise bei Informationsveranstaltungen

und im Internet verbreitete, falsche bzw. falsch verstandene Botschaft, Ärzte dürften unter der Geltung der DS-GVO personenbezogene Daten ihrer Patienten generell, also bereits hinsichtlich des Erhebens beim Patienten, der Speicherung und der Verwendung, nur noch mit deren schriftlicher Einwilligung verarbeiten. Bekräftigt wurde dieser Gedanke vielfach mit der Sorge, dass Ärzte, die kein entsprechendes Schriftstück vorweisen können, im Rahmen von Abmahnungen zur Kasse gebeten werden oder auch in Konflikt mit Vorschriften des Ordnungswidrigkeiten- oder gar Strafrechts geraten könnten. Nicht wenige kamen auf der Grundlage dieses falschen Verständnisses zu der Einschätzung, dass es sich bei der DS-GVO um ein „Bürokratie-Monster" der EU handele, das hinsichtlich der Einholung schriftlicher Einwilligungen bisher unbekannten Aufwand erzwingen würde. Manche Kritik, die gegen die DS-GVO vorgebracht wurde, mag ganz oder teilweise nachvollziehbar sein. Diese ist es nicht.

Ausgangspunkt für das richtige datenschutzrechtliche Verständnis ist der Behandlungsvertrag (vergleiche dazu die Regelungen der Paragrafen 630 a ff. des Bürgerlichen Gesetzbuchs – BGB), den ein Arzt traditionell mit seinem Patienten schließt, unter Umständen auch durch schlüssiges Verhalten, beispielsweise wenn der Arzt den unter akuten Schmerzen leidenden Praxisbesucher zur sofortigen Behandlung in sein Behandlungszimmer „durchwinkt". Der nächste Schritt der datenschutzrechtlichen Prüfung ist die Frage: Ergibt sich aus der DS-GVO eine normative Grundlage für das Erheben, die Speicherung und die Verwendung personenbezogener Daten des Patienten durch seinen Arzt, die mit einer ärztlichen Behandlung üblicherweise einhergeht? Die Antwort ist natürlich „ja": Die datenschutzrechtliche Grundlage dafür ergibt sich aus dem jeweiligen Behandlungsvertrag in Verbindung mit Artikel 6 Absatz 1 Buchstabe b DS-GVO, soweit es etwa um Gesundheitsdaten oder genetische Daten geht, zusätzlich aus Artikel 9 Absatz 2 Buchstabe h, Absatz 3 DS-GVO.

Artikel 6 Absatz 1 Buchstabe b DS-GVO hat folgenden Wortlaut: „Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist: die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen." Nach Artikel 9 Absatz 1 DS-GVO ist u. a. die Verarbeitung von Gesundheitsdaten und genetischen Daten untersagt. Diese Untersagung gilt nach Artikel 9 Absatz 2 Buchstabe h DS-GVO in folgenden Fällen nicht: „die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich." Nach Artikel 9 Absatz 3 DS-GVO gilt: „Die in Absatz 1 genannten personenbezogenen Daten dürfen zu den in Absatz 2 Buchstabe h genannten Zwecken verarbeitet werden, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt."

Demnach ist ein Arzt durch datenschutzrechtliche Vorschriften (selbstverständlich!) nicht gehindert, Patienten, ebenso wie vor dem Wirksamwerden der DS-GVO, ohne vorherige Einholung von deren da-

tenschutzrechtlicher Einwilligung zu behandeln, dabei deren dafür nötige personenbezogene Daten einschließlich der sensiblen Gesundheitsdaten und gegebenenfalls auch genetischer Daten zu erheben, im Rahmen der von ihm zu leistenden Dokumentation (vergleiche dazu § 630 f BGB und § 10 Absatz 1 der Berufsordnung der Landesärztekammer Baden-Württemberg) zu speichern und zu verwenden.

Nach § 630 f BGB gilt:
„(1) Der Behandelnde ist verpflichtet, zum Zweck der Dokumentation in unmittelbarem zeitlichen Zusammenhang mit der Behandlung eine Patientenakte in Papierform oder elektronisch zu führen. Berichtigungen und Änderungen von Eintragungen in der Patientenakte sind nur zulässig, wenn neben dem ursprünglichen Inhalt erkennbar bleibt, wann sie vorgenommen worden sind. Dies ist auch für elektronisch geführte Patientenakten sicherzustellen. (2) Der Behandelnde ist verpflichtet, in der Patientenakte sämtliche aus fachlicher Sicht für die derzeitige und künftige Behandlung wesentlichen Maßnahmen und deren Ergebnisse aufzuzeichnen, insbesondere die Anamnese, Diagnosen, Untersuchungen, Untersuchungsergebnisse, Befunde, Therapien und ihre Wirkungen, Eingriffe und ihre Wirkungen, Einwilligungen und Aufklärungen. Arztbriefe sind in die Patientenakte aufzunehmen. (3) Der Behandelnde hat die Patientenakte für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach anderen Vorschriften andere Aufbewahrungsfristen bestehen."
Baden-württembergische Ärzte unterliegen zudem der Dokumentationspflicht nach § 10 Absatz 1 der Berufsordnung der Landesärztekammer Baden-Württemberg: „Ärztinnen und Ärzte haben über die in Ausübung ihres Berufes gemachten Feststellungen und getroffenen Maßnahmen die erforderlichen Aufzeichnungen zu machen. Diese sind nicht nur Gedächtnisstützen, sie dienen auch dem Interesse der Patientinnen und Patienten an einer ordnungsgemäßen Dokumentation."

Der Versuch, für solche normativ erlaubten Datenverarbeitungen Einwilligungen einzuholen, ist nicht nur überflüssig und unpraktisch, sondern auch irreführend: Den Patienten wird der falsche Eindruck vermittelt, dass es für das Erheben, die Speicherung und die Verwendung bestimmter Daten auf ihre Einwilligung ankomme und sie demnach die Rechtsgrundlage durch den Widerruf ihrer Einwilligung beseitigen könnten. Dass ein Arzt die Irreführung seiner Patienten nach Kräften zu vermeiden hat, bedarf keiner Diskussion.

Wenn ein Arzt personenbezogene Daten über seine Patienten an eine privatärztliche Verrechnungsstelle oder einen vergleichbaren Empfänger herausgeben will, bedarf er dafür, wie vor dem Wirksamwerden der DS-GVO, der datenschutzrechtlichen Einwilligung seines Patienten. Soweit es um die Herausgabe personenbezogener Patientendaten durch einen behandelnden Arzt an einen externen Laborarzt geht, verweisen wir auf die Ausführungen in dem Beitrag Nummer 7.9.2 „Laborauftrag durch behandelnden Arzt" in unserem 32. Tätigkeitsbericht zum Datenschutz 2014/2015:

„Beauftragt der behandelnde Arzt als Stellvertreter des Patienten einen externen Laborarzt, dann benötigt der behandelnde Arzt für die damit verbundene Weitergabe personenbezogener Daten über den Patienten keine datenschutzrechtliche Einwilligung."

Zur flächendeckenden und effizienten Ausräumung bestehender Missverständnisse haben wir die FAQ-Liste „Datenschutz in der Arztpraxis" in unser Internetangebot aufgenommen, mit vollständigem Text im Anhang und die strategische Zusammenarbeit mit der Landesärztekammer und Landeszahnärztekammer Baden-Württemberg, der Kassenärztlichen und der Kassenzahnärztlichen Vereinigung Baden-Württemberg sowie mit anderen bedeutenden und einflussreichen Akteuren im baden-württembergischen Gesundheitswesen gesucht und gefunden.

Für einige Patienten, die sich nach ihrer Verweigerung datenschutzrechtlicher Einwilligungen und nach Abweisung durch ihren Arzt mit einer Anfrage oder Beschwerde an unsere Dienststelle wandten, war von entscheidender Bedeutung, von ihrem Arzt weiter behandelt zu werden, etwa weil sie diesem in Hinblick auf dessen Heilkunst besonderes Vertrauen entgegenbringen. Als Datenschutzaufsichtsbehörde sind wir u. a. dafür zuständig, einen Arzt bei Bedarf zur Beachtung datenschutzrechtlicher Vorschriften anzuhalten. Einen Arzt gegebenenfalls zu veranlassen, einen von ihm geschlossenen Behandlungsvertrag zu erfüllen oder eine ärztliche Behandlung vorzunehmen, liegt allerdings außerhalb unserer gesetzlichen Zuständigkeit. Für den Fall, dass Ärzte trotz unserer Beratung einem (potentiellen) Patienten, der keine datenschutzrechtliche Einwilligung erklärt hat, die ärztliche Behandlung verweigern, haben wir mit der Landesärztekammer Baden-Württemberg vereinbart: Patienten, denen es darum geht, (weiter) behandelt zu werden, können sich an die zuständige Bezirksärztekammer in Baden-Württemberg wenden, damit diese den Arzt unter Erinnerung an seine standes- und berufsrechtlichen Pflichten zur ärztlichen Behandlung veranlasst. Aufgrund der Rückmeldungen, die wir dazu erhalten haben, gehen wir davon aus, dass sich dieses Verfahren bewährt hat.

Sind Patienten rechtlich verpflichtet, datenschutzrechtliche Einwilligungen zu erklären?
Nein.
Eine Vielzahl von Patienten beklagte sich bei uns darüber, ihnen sei in ihrer Arztpraxis ein Vordruck für datenschutzrechtliche Einwilligungen mit der Aussage präsentiert worden, dass sie diese unterschreiben müssten. Auch dieses Missverständnis galt es auszuräumen. Ein „Müssen" gibt es insofern nicht. Ein Wesensmerkmal der datenschutzrechtlichen Einwilligung ist die Freiwilligkeit.

Nach Artikel 4 Nummer 11 DS-GVO bezeichnet der Ausdruck „Einwilligung" der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Müssen notwendige datenschutzrechtliche Einwilligungen vom Patienten schriftlich erklärt werden?
In bestimmten Fällen braucht der Arzt also die Einwilligung des Patienten, etwa wenn er dessen personenbezogene Daten an eine privatärztliche Verrechnungsstelle oder einen vergleichbaren Empfänger herausgeben will. Muss diese Erklärung vom Patienten schriftlich abgegeben werden? Die soeben zitierte Regelung zeigt, dass es nach Artikel 4 Nummer 11 DS-GVO kein Schriftformerfordernis, also kein „Müssen" hinsichtlich der Schriftlichkeit gibt. Ein Patient oder sonstiger datenschutzrechtlich Betroffener kann eine solche Einwilligung in wirksamer Weise etwa auch mündlich oder durch entsprechende Gestik erklären. Natürlich ist aus der Sicht von Ärzten und anderen datenschutzrechtlich Verantwortlichen eine schriftliche Einwilligung, etwa durch Unterschrift eines Patienten auf einem Vordruck, wünschenswert. Schließlich unterliegen sie nach Artikel 7 Absatz 1 DS-GVO der Nachweispflicht:

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

Diese Nachweispflicht ist eine Ausprägung der Rechenschaftspflicht nach Artikel 5 Absatz 2 DS-GVO:

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

Der demnach erforderliche Nachweis kann durch Vorlage eines unterschriebenen Dokuments auf besonders einfache und aussagekräftige Weise geführt werden. Daher dürfen Ärzte und andere Verantwortliche natürlich geeignete Vordrucke verwenden und die Betroffenen um schriftliche Bestätigung bzw. Unterschrift bitten. Einen Anspruch auf Schriftlichkeit bzw. Unterschrift haben sie gegenüber den Betroffenen aber nicht. Gegebenenfalls können sie den Nachweis auf andere Weise zu führen versuchen, beispielsweise durch einen entsprechend aussagekräftigen Vermerk in der Patientenakte.

Zu beachten ist, dass der deutsche Gesetzgeber unter Nutzung der entsprechenden Öffnungsklausel der DS-GVO ein Schriftformerfordernis statuieren kann, wie es sich beispielsweise aus § 73 Absatz 1b Satz 1 SGB V ergibt:

„Ein Hausarzt darf mit schriftlicher Einwilligung des Versicherten, die widerrufen werden kann, bei Leistungserbringern, die einen seiner Patienten behandeln, die den Versicherten betreffenden Behandlungsdaten und Befunde zum Zwecke der Dokumentation und der weiteren Behandlung erheben."

Sind Pauschaleinwilligungen zulässig?
Nein.
Ein weiteres gravierendes Problem war, dass von verschiedener Seite Vordrucke für Einwilligungen verbreitet wurden, die pauschale Einwilligungen für nicht näher eingegrenzte Übermittlungen personenbezogener Daten an einen nicht oder kaum eingrenzten Empfängerkreis vorsehen. Es ist nachvollziehbar, dass Ärzte durch die einmalige Einholung eines solchen Blankoschecks ihren Aufwand gering halten wollen. Dem geltenden Datenschutzrecht entspricht eine solche Praxis aber nicht. Denn, wie weiter oben in diesem Beitrag zitiert, ist die Einwilligung im Sinne des Artikels 4 Nummer 11 DS-GVO eine „für den bestimmten Fall" abgegebene Willensbekundung. Aus datenschutzrechtlicher Sicht wünschenswert sind somit möglichst konkret gefasste und etwa durch Ankreuzen und Freitextfelder (weiter) konkretisierbare Vordrucke, mit denen, je nach aktuellem, insbesondere im Sinne des Patientenwohls und Behandlungserfolgs definierbarem Bedarf, gezielt und mit Bedacht zum Ausdruck gebracht werden kann, welche personenbezogenen Daten (etwa die komplette Patientenakte, einschließlich der Daten über die vom Arzt festgestellte HIV-Infektion? Oder nur der jüngste Bericht über die Behandlung der Fußpilzerkrankung?) an wen (mit konkreter Benennung des Empfängers) herausgegeben werden dürfen. Nur auf der Grundlage einer solch konkreten Nennung des Empfängers kann sich der Patient sinnvoll mit der Frage befassen, ob er den potentiellen Empfänger eventuell kennt und ihm vertraut, gegebenenfalls inwieweit.
Die Problematik der datenschutzkonformen Gestaltung von Vordrucken für Einwilligungen haben wir bereits Anfang Juni 2018 mit der Kassenärztlichen Vereinigung Baden-Württemberg (KVBW) erörtert und im November 2018 eine Rückmeldung erhalten. Die Zusammenarbeit mit der KVBW ist insofern für uns von besonderer Bedeutung, als die KVBW insofern die besondere Aufmerksamkeit der Ärzteschaft genießt. Die Zusammenarbeit mit der KVBW sowie mit den genannten anderen strategischen Gesprächspartnern ist anspruchsvoll, aber durchaus lohnenswert und bei Redaktionsschluss für diesen Tätigkeitsbericht noch im Gange.

Müssen Patienten mit ihrer Unterschrift den Empfang der Datenschutzinformation einer Arztpraxis quittieren?
Nein.
Die DS-GVO statuiert keine solche Rechtspflicht der Patienten. Einer Rechtspflicht unterworfen sind insofern die Ärzte als datenschutzrechtlich Verantwortliche. Sie müssen ihre Informationspflicht nach Artikel 13 DS-GVO erfüllen. Genauer gesagt: Sie müssen die geforderten Informationen zur zumutbaren Kenntnisnahme anbieten, etwa durch Auslegen entsprechender Pa-

piere an der Empfangstheke der Praxis. Ob die jeweiligen Praxisbesucher von diesem Angebot Gebrauch machen, ist allein diesen überlassen. Wenn dem bereits oben beispielhaft genannten Schmerzpatienten mit vereitertem Backenzahn nicht danach zumute wäre, sich mit Datenschutzinformationen zu befassen, wäre dies, auch ungeachtet datenschutzrechtlicher Überlegungen, bereits bei praktischer und lebensnaher Betrachtung ohne Weiteres nachvollziehbar. Der Arzt genügt seiner Informations- und Dokumentationspflicht, wenn er die notwendigen Informationen anbietet und darüber einen kurzen Vermerk („DS-Info am 22.11.18 am Empfang angeboten", gez. Arzthelfer X) anlegt oder dies in seinem elektronischen Patienten-Informationssystem markiert.

1.9 Technisch-Organisatorische Maßnahmen

Die Datenschutz-Grundverordnung stellt erhöhte Anforderungen an die IT-Sicherheit. Die rechtlichen Grundlagen zur IT-Sicherheit verteilen sich auf mehrere Artikel. Zentral ist dabei vor allem Artikel 32 DS-GVO, der Vorgaben zur Sicherheit der Verarbeitung macht.

So wird als wichtige und bisher in der Praxis häufig vernachlässigte Maßnahme die Verschlüsselung aufgeführt (vgl. Art. 32, Abs. 1 lit. a DS-GVO). Ebenso ist die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen vorgeschrieben (Art. 32, Abs. 1 lit. b DS-GVO). Ähnlich wie bereits aus dem BSI Grundschutz bekannt sind Risiken der Datenverarbeitung zu beurteilen und Maßnahmen zur Eindämmung des Risikos vorzunehmen (vgl. Art. 32, Abs. 2, Art. 25 Abs. 1 DS-GVO). Die DS-GVO macht dabei kaum konkrete Vorgaben, sondern verweist auf den zu berücksichtigenden Stand der Technik. Die Verwendung dieses unbestimmten Begriffs zeigt, dass es keine feste Definition gibt, sondern diese sich im Laufe der Zeit verändert. Verantwortliche müssen also regelmäßig ihre verwendeten Maßnahmen kontrollieren und so justieren, dass mindestens solche fortschrittlichen Verfahren zum Schutz personenbezogener Daten zum Einsatz kommen, die ein hohes Schutzniveau leisten und in der Praxis erprobt sind. Der Stand der Technik steht damit zwischen den allgemein anerkannten Regeln der Technik am unteren und dem Stand der Wissenschaft am oberen Ende. Das bedeutet, dass üblicherweise nicht die allerneusten wissenschaftlichen Erkenntnisse umgesetzt werden müssen, sondern etablierte Techniken, wie sie etwa in Internet-Standards festgeschrieben sind – RFC 4880 (OpenPGP) und RFC 3156 (PGP/MIME) für die Verschlüsselung von E-Mails wäre ein Beispiel. Die Einhaltung des Stands der Technik setzt aber auch voraus, dass Verantwortliche regelmäßig ihre Maßnahmen überprüfen und so schnell auf Schwachstellen oder Sicherheitslücken reagieren.

Die folgenden zwei Kapitel zeigen beispielhaft Anforderungen, Maßnahmen und Methoden nach dem Stand der Technik, um den Schutz personenbezogener Daten sicherzustellen.

Mehr Sicherheit und Datenschutz durch Datenträgerverschlüsselung

Eine der häufigsten Datenpannen, bei denen personenbezogene Daten in fremde Hände gelangen, ist der Verlust von USB-Sticks, Speicherkarten, externen Festplatten, Laptops oder ganzer PCs. Diese werden bei Einbrüchen gestohlen, im Zug vergessen oder gehen anderweitig verloren. Teilweise sind auf den Geräten besondere Daten nach Artikel 9 DS-GVO wie Medizindaten gespeichert, z. B. beim Diebstahl von PCs aus Arztpraxen. Aber es wurden auch schon PCs aus Geldautomaten gestohlen. Wie können sich Verantwortliche nun davor schützen, dass daraus nicht auch noch eine große Datenpanne wird?

Die wichtigste Maßnahme zur Vorsorge ist relativ einfach umzusetzen: Verschlüsselung der Datenträger! Um den Zugriff auf sensible Daten zu verhindern, sollte dabei die gesamte Festplatte oder der gesamte Datenträger mittels „Full Disk Encryption" verschlüsselt und per Passwort oder vergleichbarem Zugriffsschutz gesichert werden. Entsprechende Verfahren sind seit vielen Jahren Stand der Technik, aber die Hersteller konnten sich bisher nur bei Smartphones und Tablets dazu durchringen, sie standardmäßig zu aktivieren.

Datenträgerverschlüsselung ist in verschiedenen Sicherheitsstufen unter allen gängigen Desktop- und Server-Betriebssystemen verfügbar: Windows (BitLocker oder extern via VeraCrypt), macOS (FileVault), Linux (dm-crypt, LUKS), *BSD (GELI, CGD, …), AIX (EFS), Solaris (encrypted ZFS) bringen entsprechende Verfahren seit Jahren mit. Es empfiehlt sich grundsätzlich – auch bei wenig sensiblen Daten – Festplatten zu verschlüsseln. Dies gilt insbesondere für Laptops, externe Festplatten, USB-Sticks und ähnlichem, da bei diesen ein erhöhtes Risiko des Verlusts besteht. Neben der Auswahl einer sicheren Verschlüsselungs-Software ist darauf zu achten, dass sichere Algorithmen und eine ausreichende Schlüssellänge sowie sichere Passwörter gewählt werden.

Um Verantwortlichen eine Hilfestellung bei der Einrichtung von Datenträgerverschlüsselung zu geben haben wir eine Kurzanleitung veröffentlicht, die die Einrichtung bei gängigen Betriebssystemen beschreibt. Das Dokument kann auf unserer Internetseite kostenlos heruntergeladen werden.

Hinweise zum Umgang mit Passwörtern

Passwortsicherheit ist ein zentrales Thema bei technisch-organisatorischen Maßnahmen. Passwörter sind immer noch ein zentrales Element zur Authentifizierung von Nutzern. Aus diesem Grund haben wir aktualisierte Hinweise zum Umgang mit Passwörtern veröffentlicht, die sowohl Nutzern eine Hilfestellung bei der Auswahl von sicheren Passwörtern als auch Entwicklern und Administratoren Hinweise für die Aufstellung von Passwort-Richtlinien und die Speicherung von Passwörtern in Anwendungen bieten.

Die Anmeldung mittels Nutzername und Passwort stellt bei der Anmeldung an Computern, bei Web-Diensten, Internet-of-Things-Geräten und vielem anderen das gängigste Verfahren zur Authentifizierung dar. Sie sind damit oftmals das wesentliche oder gar einzige Sicherheitselement, das vor dem Zugriff durch Unbefugte schützt.

Ein großes Risiko ist dabei, dass Passwörter von Dritten erraten werden können. Daher sind einerseits die Nutzer selbst in der Pflicht, starke Passwörter auszuwählen, andererseits müssen aber auch Hersteller und Administratoren sinnvolle und sichere Vorgaben machen. Dafür haben sich eine Reihe von Regeln etabliert:

1. **Starke Passwörter wählen**
   Es sollten immer starke Passwörter verwendet werden, die aus zwölf oder mehr Zeichen bestehen. Sie sollten sowohl Klein- als auch Großbuchstaben und Ziffern enthalten. Auf kompliziert einzugebende Sonderzeichen sollte verzichtet werden, da diese u. U. auf verschiedenen Tastaturen unterschiedlich eingegeben werden müssen.
2. **Passwörter niemals doppelt verwenden**
   Angreifer haben in den letzten Jahren eine große Menge an Passwörtern gesammelt, oftmals indem sie die Passwortdatenbanken großer Web-Portale aufgrund von Sicherheitslücken kopieren konnten. Über fünf Milliarden Passwörter sind daher bekannt. Angreifer nutzen diese, um sich unrechtmäßig bei anderen Diensten anzumelden oder weitere Passwörter (die nur minimal geändert wurden) zu knacken.

3. **Keine Wörter aus Wörterbüchern verwenden**
   Angreifer können heutzutage – insbesondere wenn sie Zugriff auf Datenbanken mit verschlüsselten Passwörtern haben – in kurzer Zeit automatisiert sehr viele Kombinationen durchprobieren. Gute Passwörter sollten daher weder Begriffe oder Begriffskombinationen aus Wörterbüchern enthalten („Sommer2018") noch solche wiederverwenden. Die einzige Ausnahme sind wirklich sehr lange Passwörter, die aus einer Reihe zufälliger und nicht zusammenhängender Wörter bestehen.
4. **Passwörter nicht weitergeben**
   Passwörter sollen grundsätzlich nicht an Dritte weitergegeben werden. Ebenso wenig sollen sie nicht per unverschlüsselter E-Mail verschickt oder in unverschlüsselten Dokumenten gespeichert werden.
5. **Passwort-Safe verwenden**
   Niemand kann sich Hunderte Passwörter merken. Daher ist es sinnvoll, Passwörter in einem Passwort-Safe zu speichern. Entsprechende Programme gibt es als Freie- und Open-Source-Software kostenlos, bei einigen Betriebssystemen werden auch bereits welche mitgeliefert (z. B. der Schlüsselbund unter macOS). Viele Web-Browser unterstützen die Speicherung von Passwörtern – diese sollten aber mit einem Master-Passwort abgesichert werden.
6. **Nur bei Kompromittierung ändern**
   Früher wurde empfohlen, Passwörter in regelmäßigen Abständen zu ändern. Diese Empfehlung gilt heutzutage als überholt, da sie nicht zu mehr Sicherheit führt – sondern nur dazu, dass Nutzer sich diese im Klartext notieren, einfache Passwörter wählen, eine Zahl hochzählen oder ähnliches. Daher sollten Administratoren die Nutzer nicht mehr zwingen, Passwörter in regelmäßigen Abständen zu ändern. Nur wenn es Anzeichen dafür gibt, dass Passwörter oder Passwort-Hashes in fremde Hände gelangt sind, sollten Nutzer diese ändern bzw. zu einer Änderung aufgefordert werden.
7. **Software-Entwickler dürfen Passwörter keinesfalls im Klartext speichern**
   Entwickler von Anwendungen, Web-Portalen, Apps oder ähnlichem müssen zum Vergleich die Zugangsdaten der Nutzer speichern. Dabei dürfen sie die Passwörter auf keinen Fall im Klartext speichern, sondern müssen stattdessen moderne Verfahren wie Argon2 nutzen. Üblicherweise sollten dafür existierende Software-Bibliotheken verwendet werden.
8. **Sichere Passwörter auch auf Smartphones**
   Auch wenn Passwörter auf Smartphones oder Tablets schwieriger einzugeben sind, sollten hier sichere und lange Passwörter gewählt werden. Vierstellige PINs oder Wischgesten sind in der Regel nicht ausreichend. Aufgrund der meist vorhandenen biometrischen Authentifizierung sind Passwörter nur relativ selten einzugeben und daher auch zumutbar.
9. **Standard-Passwörter immer ändern**
   Standard-Passwörter, die z. B. von Internet-of-Things-Geräten, Fernwartungseinheiten, Software-Paketen und ähnlichem vergeben werden, sind oftmals nicht zufällig sondern bei allen Geräten gleich. Daher müssen diese bei Inbetriebnahme sofort geändert werden.

Details und weitere Hinweise – inklusive Tipps, wie man sich sichere Passwörter einfach merken kann – sind in unseren Hinweisen zum Umgang mit Passwörtern enthalten, die kostenlos auf unserer Webseite heruntergeladen werden können. Dort finden sowohl Nutzer als auch Administratoren und Software-Entwickler ausführliche Hinweise.

Datenpannen – Verlust von Speichermedien

Die Miniaturisierung von Flash-Speichermedien von SD über miniSD bis zu microSD mit großer Speicherkapazität bei sinkenden Preisen führt dazu, dass man nicht

nur bei Smartphones und Digitalkameras große Mengen von Daten mit sich herumträgt, sondern diese Medien auch gerne zum Transport von Daten zwischen zwei Rechnern oder zwei Standorten verwendet werden. Entweder mit USB-Adapter oder gleich als USB-Stick.

Durch die geringen Abmessung und das geringe Gewicht werden diese Medien gerne auch beim Postversand verwendet, gehen aber auch leichter verloren – was die Verlustmeldungen zeigen.

Es gibt somit einiges zu beachten. Als wichtigste Empfehlung gilt immer die Verschlüsselung der Speichermedien gemäß Stand der Technik. Dies hat den Vorteil, das Risiko bei Verlust oder Diebstahl ggf. auf ein vertretbares Maß reduziert zu haben.

Nicht substantiiert ist jedoch die Argumentation einer Verlustmeldung, das Risiko für die Betroffenen sei gering, da es sich um Ministicks handele und deren Auffinden eher unwahrscheinlich sei.

Um bei einem Verlust dem Finder/Fundbüro bzw. der Nachforschungsstelle die Rückgabe zu erleichtern, sollte man das Speichermedium eindeutig markieren und – sofern möglich – auch neutrale Kontaktdaten aufbringen.

Bei vielen vermeintlichen Diebstählen auf dem Postweg ist die Briefsortieranlage der Übeltäter. Der Grund dafür ist, dass Sortiermaschinen für Standardbriefe mit Erhebungen in dünnen Briefumschlägen nicht gut zurechtkommen. Standard- und Kompaktbriefe werden mit Transportbändern und -rollen sortiert. Lose eingelegte Gegenstände werden bei der schnellen, maschinellen Sortierung mit hohen Fliehkräften aus einem einfachen Papierumschlag herausgeschossen. Maschinen für Großbriefe ab DIN A5 können dagegen mit Erhebungen umgehen. Idealerweise verwendet man für den Versand stabile Versandtaschen/Luftpolsterumschläge. Auch sollte das Speichermedium fixiert sein bspw. mit Klebeband, um nicht umherwandern zu können.

1.10 Steuerberater und Lohnbuchhaltung

Die Frage, wie die Übertragung der laufenden Lohn- und Gehaltsabrechnung an einen Steuerberater datenschutzrechtlich zu beurteilen ist, ist seit Jahren hoch umstritten. Ohne erkennbaren Anlass rückte diese Frage mit Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO) aber unvermittelt wieder in den Blickpunkt des Interesses, wovon eine Vielzahl von Eingaben, sowohl von Steuerberatern als auch von potenziellen Auftraggebern, zeugt. Während Steuerberater und ihre berufsständischen Vertretungen hier bisher klar die Position vertreten, dass die Leistung des Steuerberaters immer eine eigenverantwortlich erbrachte fachliche Beratung sei und der Steuerberater, gleich, welchen Auftrag er übernimmt, grundsätzlich keine weisungsabhängige Tätigkeit ausübe, wird dies jedenfalls von einzelnen Datenschutzaufsichtsbehörden genau anders bewertet. Auch ich bin diesbezüglich dezidiert anderer Auffassung. Danach kommt für die Beauftragung des Steuerberaters mit der laufenden Lohn- und Gehaltsabrechnung datenschutzrechtlich nur eine Auftragsverarbeitung im Sinne des Artikels 28 DS-GVO in Betracht. Hierfür spricht Folgendes:

Seit dem Beschluss des Bundesverfassungsgerichts vom 27. Januar 1982 (1 BvR 807/80 –, BStBl II 1982, 281, BVerfGE 59, 302-329) steht fest, dass das Buchführungsprivileg für steuerberatende Berufe (§ 5 Absatz 1 des Steuerberatungsgesetzes) nicht für die laufende Lohnbuchhaltung gilt. Begründet wird dies damit, dass es sich bei der laufenden Lohnbuchhaltung um reine Routinearbeiten handelt, die „sich als eine nicht durch besondere rechtliche Erwägungen geprägte schematisierte Subsumtion von Lohnzahlungsvorgängen unter die amtlichen Lohnsteuertabellen und das betriebliche Lohnkonto darstellt".

Folgerichtig wurde das Steuerberatungsgesetz angepasst; nach § 6 Nummer 4 des Steuerberatungsgesetzes gilt das Verbot der unbefugten Hilfeleistung in Steuersachen (u. a.) nicht für die laufende Lohnabrechnung. Für die Frage, ob der Steuerberater solche Arbeiten als Verantwortlicher im Sinne des Artikels 4 Nummer 7 DS-GVO oder als Auftragsverarbeiter im Sinne des Artikel 4 Nummer 8 DS-GVO erledigt, kommt diesem Umstand, dass es sich bei der laufenden Lohnbuchhaltung um rein mechanische Verarbeitungsvorgänge handelt, die keine besondere Qualifikation der steuerberatenden Berufe erfordert, entscheidende Bedeutung zu. Denn dies hat zur Folge, dass der für die Mitarbeiterdaten Verantwortliche die Befugnis behält, Zwecke und Mittel der Verarbeitung zu bestimmen. Dem steht auch nicht entgegen, dass der Steuerberater ansonsten, soweit er dem Steuerberaterprivileg unterfallende Arbeiten erledigt, zweifelsfrei als Verantwortlicher tätig wird. Denn es ist anerkannt, dass je nach konkreter Tätigkeit und Zusammenhang dieselbe Organisation hinsichtlich bestimmter Verarbeitungen als Verantwortlicher und hinsichtlich anderer Verarbeitungen als Auftragsverarbeiter handeln kann (Hartung, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 2. Auflage 2018, Art. 4 Nr. 8 DS-GVO Rn. 7; ebenso: Arbeitspapier Nr. 169 der Artikel-29-Datenschutzgruppe, Seite 35: ein Dienstleister ist nur dann als Verantwortlicher einzustufen, wenn seine Fachkompetenz die entscheidende Rolle spielt und der Auftrag schwerpunktmäßig nicht in der Verarbeitung der Daten liegt, sondern die Daten nur Grundlage einer höherwertigen Dienstleistung sind).

Soll die Lohnbuchhaltung durch den Steuerberater nicht im Rahmen eines Auftragsverhältnisses nach Artikel 28 DS-GVO erfolgen, sondern tritt der er selbst als datenschutzrechtlich Verantwortlicher auf, bedarf es einer Rechtsgrundlage, die den Auftraggeber berechtigt, die personenbezogenen Daten seiner Beschäftigten dem Steuerberater zu übermitteln, und gleichzeitig bedarf es einer Rechtsgrundlage, die den Steuerberater zur (eigenverantwortlichen) Verarbeitung der Beschäftigtendaten berechtigt. Soweit es um die Verarbeitung personenbezogener Daten durch den Steuerberater für Zwecke der laufenden Lohnabrechnung geht, kann als Rechtsgrundlage jedenfalls nicht auf § 11 des Steuerberatungsgesetzes abgestellt werden, da es sich insoweit nicht um Daten handelt, die der „Erfüllung der Aufgaben nach diesem Gesetz" (Hilfe in Steuersachen) dienen. Hinzu kommt, dass die Lohnbuchhaltung auch die Verarbeitung besonderer Kategorien personenbezogener Daten, sog. sensitiver Daten, beinhaltet, wie etwa Gesundheitsdaten oder Daten, aus denen religiöse oder weltanschauliche Überzeugungen hervorgehen. Sensitive Daten dürfen nur unter den (zusätzlichen) Voraussetzungen des Artikels 9 Absatz 2 DS-GVO verarbeitet werden. Die Verarbeitung solcher Daten durch den Steuerberater als (Eigen-)Verantwortlichen lässt sich indes unter keinen dieser Ausnahmetatbestände des Artikels 9 Absatz 2 DS-GVO subsumieren. Auch die Ausnahmeregelung des § 26 Absatz 3 des Bundesdatenschutzgesetzes (BDSG) hilft hier nicht weiter. Denn weder verarbeitet der Steuerberater die sensitiven Daten „für Zwecke des Beschäftigungsverhältnisses", noch ist die Verarbeitung „zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich". Fehlt es somit an der Berechtigung, solche Daten zu verarbeiten, schließt dies insgesamt eine Lohnbuchhaltung als Verantwortlicher aus. Dagegen ist die Weitergabe auch sensitiver Daten im Rahmen eines Auftragsverhältnisses nach Artikel 28 DS-GVO grundsätzlich unproblematisch.

Schließlich überzeugt es auch nicht, eine inhaltlich identische Dienstleistung datenschutzrechtlich nach unterschiedlichen Grundsätzen zu behandeln, je nachdem, ob der Dienstleister Kaufmann oder Steuerberater ist. Ein wirklich stichhaltiger Grund, Steuerberater einzig und allein aufgrund ihres Berufsstands auch bezogen

auf solche Leistungen zu privilegieren, die grundsätzlich keinerlei Bezug zur eigentlich privilegierten Tätigkeit aufweisen, ist nicht erkennbar.

Auch das Kurzpapier Nummer 13 der Datenschutzkonferenz steht dieser Auffassung entgegen anderslautender Behauptung nicht entgegen. Wenn dort in Anhang B die Tätigkeit von Berufsgeheimnisträgern pauschal von der Auftragsverarbeitung ausgeschlossen wird, ist dies jedenfalls nicht so zu verstehen, dass dies grundsätzlich auch für solche zusätzlich übernommenen Hilfstätigkeiten gilt, die keinen unmittelbaren Bezug zur Kerntätigkeit des Geheimnisträgers haben.

Übernimmt ein Steuerberater neben seiner eigentlichen Steuerberatertätigkeit (Hilfe in Steuersachen) zusätzlich weitere Aufgaben, handelt es sich um Auftragsverarbeitung im Sinne des Artikels 28 DS-GVO und bedarf einer entsprechenden Vereinbarung mit dem datenschutzrechtlich verantwortlichen Auftraggeber.

1.11 Datenschutz in der Pflege

Die Misere der Pflegebranche ist kein neues Problem, jedoch ist sie im Berichtszeitraum verstärkt in den Mittelpunkt der Aufmerksamkeit gerückt. Kaum ein Tag vergeht, an dem die Presse nicht vom sogenannten „Pflegenotstand" berichtet. Auch Bundesgesundheitsminister Spahn wird zitiert mit den Worten „Wir haben verstanden." Der Mangel an qualifizierten Pflegekräften und die damit einhergehende Arbeitsüberlastung stellt die ambulante und stationäre Pflege vor erhebliche Herausforderungen. Angesichts der vielfältigen aktuellen Probleme, mit denen sich Pflegeeinrichtungen deshalb konfrontiert sehen, warfen wir in unserer Pressemitteilung vom 27. März 2018 die Frage auf, ob diese Einrichtungen überhaupt noch Zeit haben, sich vernünftig um die überaus sensiblen Daten der ihnen anvertrauten Pflegebedürftigen zu kümmern.

1.11.1 Datenschutz in Pflegeeinrichtungen – ein Thema in Zeiten des Pflegenotstands?

War das Jahr 2018 vor dem Hintergrund des allgegenwärtigen Pflegenotstands der richtige Zeitpunkt, um die Pflegebranche mit dem Thema Datenschutz zu konfrontieren?

„Ja, gerade dann!" lautete die Antwort des Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI). Die Erfahrung lehrt, dass sich – besonders in Phasen, in denen die Akteure unter großer Spannung stehen – eine solche Spannung nicht selten über den Datenschutz „entlädt". Zu unseren Aufgaben gehört es auch, in solchen Situationen bereits im Vorfeld möglicher Datenschutzverstöße und Beschwerden die Verantwortlichen zu beraten und für ihre datenschutzrechtlichen Pflichten zu sensibilisieren. Geschieht erst eine Datenpanne, dann ist es oft zu spät, um Schaden noch abzuwenden. Unsere Aufklärung und Beratung war dieses Jahr zudem umso wichtiger, als unter den Beteiligten große Verunsicherung herrschte, welche Anforderungen die am 25. Mai 2018 wirksam gewordene Datenschutz-Grundverordnung (DS-GVO) für die Pflege mit sich brachte.

Aus diesen Gründen entschlossen wir uns, so wie im 33. Tätigkeitsbericht 2016/2017 unter 7.5 am Ende angekündigt, die in der Pflege tätigen Personen mit einem Katalog häufig gestellter Fragen („FAQ") für die Anforderungen des Datenschutzes zu rüsten. Um den Fragenkatalog möglichst praxisnah auszugestalten, haben wir uns zunächst ein möglichst umfassendes Bild zu machen versucht: Wir baten die Beteiligten mit Pressemitteilung vom 27. März 2018 darum, uns ihre konkreten datenschutzrechtlichen Fragen einzusenden. Um eine große Streubreite zu erwirken und so möglichst viele Pflegeeinrichtungen im Land zu erreichen, banden wir die verschiedenen baden-württembergischen Pflegeverbände als Multiplikatoren ein, welche ihre

Mitglieder über unsere Pressemitteilung informierten. Auch die baden-württembergische Landesregierung machte in ihrem Newsletter vom 27. März 2018 auf unsere Pressemitteilung aufmerksam.

In der Folge erhielten wir zahlreiche Rückmeldungen unterschiedlicher Beteiligter der Pflegebranche. Es meldeten sich sowohl Pflegebedürftige, deren Angehörige, Heimleitungen von Pflegeeinrichtungen als auch Pflegeverbände zu Wort. Wir beantworteten die an uns gerichteten Fragen und gingen den uns berichteten Problemen auf den Grund.

1.11.2 Warum ist der Datenschutz in der Pflege eigentlich so wichtig?

Der Bereich der Pflege ist im wahrsten Sinne des Wortes ein „sensibler" Bereich, das gilt auch für die Belange des Datenschutzes: Unvermeidlich erlangen die Mitarbeiter der Pflegeeinrichtungen auch Kenntnis über die Gesundheit und die teilweise sehr persönlichen oder intimen Lebensumstände der Pflegebedürftigen sowie ggf. auch von deren Angehörigen. Dabei sind gerade Menschen in einer Pflegesituation in besonderem Maße davon abhängig, dass die Personen, welche sie pflegen, sorgfältig mit ihren Daten umgehen. Hinzu kommt, dass durch die stetig anwachsende Zahl von pflegebedürftigen Menschen hierzulande auch das Thema des Datenschutzes in der Pflege eine zunehmend größere Bedeutung einnimmt.

Schon beim Abschluss eines Pflegevertrages müssen Menschen mit Pflegebedarf eine Vielzahl hoch sensibler Informationen über sich preisgeben. Nur so können Heime, Pflegedienste und deren Mitarbeiterinnen und Mitarbeitern individuell angepasste Hilfe anbieten. Im sogenannten Aufnahmebogen werden beispielsweise nicht nur umfassende Informationen über die gesundheitliche Situation des künftigen Heimbewohners abgefragt, sondern in der Regel werden vom biografischen Hintergrund bis hin zu Vermögensverhältnissen und dem religiösen Bekenntnis eine Vielzahl von personenbezogenen Daten erhoben, welche in hohem Maße schutzwürdig sind. Die Einhaltung des Datenschutzes ist nicht nur eine gesetzliche Verpflichtung, sondern auch eine wichtige Voraussetzung für das Vertrauen der Pflegebedürftigen und deren Angehörigen in die Pflegeeinrichtung.

1.11.3 Welches sind die typischen datenschutzrechtlichen Probleme in Pflegeeinrichtungen?

Stellvertretend für die vielfältigen datenschutzrechtlichen Probleme, mit denen wir uns während des Berichtszeitraums beschäftigt haben, möchten wir einige Beispiele herausgreifen:

Im Kontakt mit dem Geschäftsführer einer Pflegeeinrichtung, welche als privatrechtliche GmbH organisiert war, stießen wir darauf, dass dieser gleichzeitig die Funktion als betrieblicher Datenschutzbeauftragter innehatte. Wir wiesen ihn darauf hin, dass er als Geschäftsführer der GmbH nicht gleichzeitig betrieblicher Datenschutzbeauftragter sein könne. Die Datenschutzgesetze fordern, dass der betriebliche Datenschutzbeauftragte in seiner Stellung von dem Leiter der verantwortlichen Stelle unabhängig und weisungsfrei sein muss. Diese Voraussetzung ist nur dann erfüllt, wenn der betriebliche Datenschutzbeauftragte nicht in einem Interessenskonflikt mit dem Verantwortlichen steht. Als Geschäftsführer der GmbH ist er verantwortlich für die betriebswirtschaftlichen Geschicke des Unternehmens. Diese Ziele sind nicht notwendig deckungsgleich mit den Zielen eines betrieblichen Datenschutzbeauftragten, sie stehen vielmehr häufig in einem Konflikt miteinander.

Jener Geschäftsführer stellte allerdings selbst fest – nicht zuletzt aufgrund des Wirksamwerdens der DS-GVO – dass ihm

neben seinen Aufgaben als Geschäftsführer schlicht die erforderlichen zeitlichen Ressourcen fehlen würden, um den gesetzlichen Anforderungen an einen Datenschutzbeauftragten gerecht zu werden.

Bis zum 25. Mai 2018 galt Folgendes: Der Datenschutzbeauftragte musste gemäß § 4f Abs. 3 Satz 2 BDSG a. F. in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei sein, um die gesetzlich geforderte Unabhängigkeit zu gewährleisten. Sie mussten in der Lage sein, ihre Verpflichtungen ohne Interessenkonflikte erfüllen zu können. Diese rechtlichen Voraussetzungen gelten auch unter dem Regime der DS-GVO seit dem 25. Mai 2018 fort: Art. 38 Absatz 3 Satz 1 DS-GVO verlangt, dass der Datenschutzbeauftragte keine Anweisungen bezüglich der Ausübung seiner Aufgaben erhält. Art. 38 Absatz 6 DS-GVO normiert, dass der Verantwortliche sicherstellt, dass die Aufgaben und Pflichten des Datenschutzbeauftragten nicht zu einem Interessenkonflikt führen.

Der Geschäftsführer der Pflegeeinrichtung benannte kurze Zeit später einen externen Datenschutzbeauftragten für die GmbH und aktualisierte die Datenschutzerklärung auf der Homepage der Pflegeeinrichtung entsprechend.

Weitere Probleme im Hinblick auf Datenschutz sowie Datensicherheit offenbarten unseren Erfahrungen im Berichtszeitraum zufolge auch folgende Situationen:

Eine Pflegeeinrichtung hatte in ihrer Eingangshalle gut sichtbar einen digitalen Fotorahmen angebracht, auf dem Fotos von Heimbewohnern gezeigt werden. Es stellte sich heraus, dass die Pflegeeinrichtung nicht daran gedacht hatte, auch für das Abspielen der Fotos auf diesem Medium von den Bewohnern zuvor eine ausdrückliche Einwilligung einzuholen. Auch die Anlage zum Heimvertrag, welche die Pflegeeinrichtungen gewöhnlich für die Einwilligung zur Veröffentlichung von Fotoaufnahmen verwenden, entspricht nach unseren Erfahrungen oft nicht den datenschutzrechtlichen Anforderungen. Wir wiesen in diesem Zusammenhang darauf hin, dass Pflegeeinrichtungen für jedes einzelne Medium, in welchem sie Fotos der Bewohner abbilden möchte (z. B. Heimzeitung, Aushang am Schwarzen Brett, Internetseite des Heimträgers, Werbeprospekt), eine separate Einwilligung von dem Bewohner benötigen. Praktisch umsetzbar ist dies etwa, indem man für jedes Medium eigenständige Kästchen vorsieht, welche man entweder bei „Ja" oder „Nein" ankreuzen kann.

Im Zusammenhang mit einer in der Nähe des Eingangsbereichs einer Pflegeeinrichtung angebrachten Attrappe einer Videokamera, welche auf die Eingangstüre der Pflegeeinrichtung gerichtet war, klärten wir den Verantwortlichen darüber auf, dass auch eine bloße Attrappe datenschutzrechtlich unzulässig sein kann.

Die Installation einer Kameraattrappe ist dann zulässig, wenn die Pflegeeinrichtung nur ihr eigenes Grundstück überwacht. Ist diese Attrappe hingegen z. B. auf öffentliche Wege gerichtet, so ist zwar das Bundesdatenschutzgesetz (BDSG) bei Kameraattrappen nicht unmittelbar anwendbar, da tatsächlich keine ja keine Daten erhoben werden, jedoch berührt eine Attrappe dennoch schutzwürdige Interessen der Betroffenen in gleicher Weise, weil die Betroffenen nicht erkennen können, dass es sich um eine Attrappe handelt. Ebenso wie bei echten Kameras können die Betroffenen sich beobachtet fühlen (der BGH spricht von sog. „Überwachungsdruck") . Aus diesem Grund ist eine Attrappe, die auf Passanten gerichtet ist, ebenso unzulässig.

Bei der Prüfung von Vertragsunterlagen verschiedener Pflegeeinrichtungen ist uns aufgefallen, dass darin oftmals Angaben vom zukünftigen Bewohner abgefragt werden, welche im datenschutzrechtlichen Sinn nicht erforderlich sind für die Erfüllung des Behandlungsvertrags, z. B. die Frage nach der Konfession und der Staatsange-

hörigkeit. Dieses Thema hatte uns bereits im letzten Tätigkeitsbericht beschäftigt (vgl. 33. Tätigkeitsbericht 2016/2017, 7.5, S. 98 f.). Pflegeeinrichtungen wie Pflegeverbände argumentierten uns gegenüber, dass diese Angaben aus ihrer Sicht erforderlich seien für die von ihnen geforderte Biographiearbeit und nannte ein Beispiel: Aufgrund bestimmter Kriegserfahrungen einer Pflegebedürftigen hatte es sich auf die Behandlung ungünstig ausgewirkt, dass dieser eine polnische Pflegekraft zugeteilt war.

Wir stellten in diesem Zusammenhang sowohl in unseren FAQs als auch in Beratungsgesprächen nochmals klar: Zur Erhebung der unmittelbar pflegerelevanten personenbezogenen Daten ist die Pflegeeinrichtung aufgrund des geschlossenen Behandlungsvertrags datenschutzrechtlich befugt. Geht es hingegen nur um zusätzliche Informationen über die Bewohner, die für die Pflegeeinrichtung zwar nicht unbedingt erforderlich sind zu erfahren, aber regelmäßig nützlich oder dienlich sind, damit die Pflege besser und gezielter erfolgen kann, so empfehlen wir Folgendes: In die Vertragsvordrucke kann man einen Hinweis aufnehmen, dass der Bewohner nicht verpflichtet ist zur Angabe dieser Informationen, sondern die Preisgabe dieser Information vielmehr freiwillig erfolge. Wir raten dazu, die Vertragsvordrucke im Hinblick auf diese Punkte zu verändern. Was das Beispiel mit der polnischen Pflegekraft angeht, so ergab sich im Laufe unseres Gespräches, dass es sich hierbei um Einzelfälle handeln würde. Angesichts dessen gaben wir zu bedenken, dass bei vereinzelt relevanten Informationen eine pauschale Abfrage in Vertragsvordrucken „auf Verdacht" aus unserer Sicht nicht erforderlich sei und rieten dazu, die Vertragsunterlagen insoweit abzuspecken.

Ferner stellte sich heraus, dass das Gros dieser Art von zusätzlichen, oft biographischen Informationen in der Regel ohnehin nicht allesamt bereits bei Vertragsschluss erhoben würden, sondern dass diese Daten vielmehr erst im Rahmen von persönlichen Gesprächen der Pflegekräfte mit dem Bewohner erhoben und dann in der Pflegedokumentation notiert würden. Gibt ein Bewohner diese Informationen der Pflegekraft im Gespräch freiwillig preis, so willigt der Bewohner konkludent darin ein, dass seine Daten erhoben werden dürfen. Wird er zusätzlich noch danach gefragt, ob er damit einverstanden ist, dass diese Informationen auch in seiner Pflegedokumentation notiert werden, ist dieses Vorgehen nicht zu beanstanden.

Überdies waren wir mit der Frage konfrontiert, ob Heimvertragsunterlagen datenschutzrechtlich zulässig seien, welche wie folgt gestaltet würden: Statt bei jeder erforderlichen Einwilligung jeweils eine Ja- und Nein-Ankreuz-Möglichkeit vorzusehen, war der Vertragstext so vorformuliert, dass der Bewohner mit den Datenverarbeitungen einverstanden ist, es sei denn, er kreuzt bei der jeweiligen Datenverarbeitung „Nein" an. Hintergrund eines solchen Vertragstextes sei die Erfahrung der Pflegeeinrichtungen, dass viele Bewohner mit einer Gestaltung, bei der jedes Mal aktiv ein „Ja" oder „Nein" angekreuzt werden muss, überfordert seien. In diesem Zusammenhang wiesen wir darauf hin, dass die beabsichtigte Gestaltung mit der bloßen Option, ein Nein-Kästchen anzukreuzen (sog. „Opt-out-Lösung"), nach der DS-GVO nicht mehr zulässig ist. Ebenso ist es zulässig, wenn die Kreuzchen durch das Heim vorausgefüllt würden. Im Übrigen können Pflegebedürftige auch mit dem Opt-out-Verfahren überfordert sein.

Gem. Artikel 4 Nr. 11 der DS-GVO muss eine Einwilligung u. a. die Voraussetzung erfüllen, dass sie in Form einer unmissverständlichen Willenserklärung und mit einer eindeutig bestätigenden Handlung abgegeben wird. Die betroffene Person muss mit dieser Erklärung zu verstehen geben, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist (sog. „Opt-in-Lösung").

Schließlich fiel uns bei der Durchsicht der Vertragsunterlagen ebenso auf, dass die

Einwilligungen nicht immer den seit Geltung des Artikels 9 Absatz 2 lit. a) DS-GVO erforderlichen ausdrücklichen Hinweis enthalten, dass bei der Datenverarbeitung in Form von Gesundheitsdaten besonders sensible personenbezogene Daten verarbeitet werden. Ein solcher Hinweis könnte wie folgt lauten: „Wir informieren Sie darüber, dass vorliegend auch Gesundheitsdaten verarbeitet werden. Bei Gesundheitsdaten handelt es sich um besonders sensible Daten."

1.11.4 Die häufigsten Fragen der Pflegeeinrichtungen („FAQs")

Sämtliche dieser Erfahrungen, welche wir im Berichtszeitraum aus dem Kontakt mit den Akteuren der Pflegebranche gesammelt hatten, ließen wir schließlich in unsere Zusammenstellung häufig gestellter Fragen („FAQ") einfließen. Die FAQs veröffentlichten wir schließlich im Juni 2018 auf unserer Homepage.

Den Frage-Antworten-Katalog haben wir wie folgt aufgebaut: Wir behandeln darin zunächst grundlegende Fragen des Datenschutzes in der Pflege und gehen dann darauf ein, welche Verarbeitungen personenbezogener Daten in den verschiedenen Situationen zulässig sind. Sodann beschäftigen wir uns mit der Reichweite des Einsichtsrechts in die Pflegedokumentation und nehmen auch „Dauerbrenner" wie das Anfertigen von Fotografien und die Benennung eines Datenschutzbeauftragten mit auf. Schließlich thematisieren wir, wie sich die neuen Regelungen der DS-GVO auf die Pflegeeinrichtungen auswirken.

Um auch diesmal wieder möglichst viele Pflegeeinrichtungen zu erreichen, haben wir die verschiedenen Pflegeverbände kontaktiert und sie gebeten, diese FAQs unter ihren Mitgliedern zu streuen. Inzwischen hat uns der Dachverband, mit dem unsere Dienststelle auch in anderen Angelegenheiten regelmäßig konstruktiv zusammenarbeitet, anlässlich eines Treffens in unserer Dienststelle ein wertvolles und informatives Feedback zu unseren FAQs gegeben, welches auf den einzelnen Rückmeldungen der Mitglieds-Pflegeeinrichtungen basiert.

Im Rahmen dieses Schwerpunktthemas haben sich auch andere Pflegeverbände zu Wort gemeldet und jüngst eine Frage an uns herangetragen, welche sie aktuell besonders beschäftigt und auf die sie noch keine Antwort in unseren FAQs gefunden haben: Sie möchten wissen, ob die stationären Pflegeeinrichtungen tatsächlich verpflichtet sind, anlässlich von Prüfungen durch die Heimaufsicht die personenbezogenen Personallisten ihrer Beschäftigten in nicht-anonymisierter Form der Heimaufsicht offenzulegen. Hintergrund ist, dass den Heimaufsichtsbehörden die Prüfung obliegt, ob die in einer stationären Einrichtung Beschäftigten persönlich und fachlich geeignet sind für die von ihnen zu leistende Tätigkeit. Sofern die Beschäftigten nicht die erforderliche Eignung besitzen, etwa aufgrund einer strafrechtlichen Verurteilung wegen einer vorsätzlichen Körperverletzung zu einer Freiheitsstrafe, kann die zuständige Behörde ein Beschäftigungsverbot erlassen. Offenbar handelt es sich hierbei um keine neue datenschutzrechtliche Frage, jedoch sind die Pflegeeinrichtungen stark verunsichert, ob sie im Falle einer Offenlegung ihrer Beschäftigtendaten gegen die verschärften Vorschriften der DS-GVO verstoßen und fürchten mit hohen Bußgeldern sanktioniert zu werden. Der LfDI ist derzeit noch damit beschäftigt, zu untersuchen, ob die Offenlegung der Personallisten tatsächlich erforderlich ist. Sobald diese Frage geklärt ist, werden wir unsere FAQs um diese Thematik ergänzen und auf unserer Homepage unter der Rubrik „FAQs" veröffentlichen.

Es bleibt abzuwarten, ob politische Maßnahmen wie das „Sofortprogramm Pflege" des Bundesgesundheitsministers Jens Spahn den Pflegenotstand lindern werden. Solange die in der Pflege tätigen Personen unter derart schwierigen Bedingungen arbeiten, wird auch der Datenschutz in

diesem Bereich weiterhin ein schwieriges Thema sein, für das häufig zu wenig Zeit aufgewendet wird. Daher sind wir auch in Zukunft stets offen für Rückmeldungen aus der Praxis zum Thema Datenschutz in der Pflege: Konstruktive Kommentierungen sowie Fragen des Datenschutzes von allgemeinem Interesse nehmen wir gerne unter poststelle@lfdi.bwl.de entgegen.

1.12 Die telemedizinische Sprechstunde DocDirekt – Modellversuch „im Ländle“ als Vorbild fürs ganze Land?

Deutschlands Gesundheitsbranche blickt derzeit gespannt auf Baden-Württemberg und beobachtet interessiert, wie sich die erste telemedizinische Sprechstunde für gesetzlich Versicherte hierzulande entwickelt. Sofern das Pilotprojekt DocDirekt der Kassenärztlichen Vereinigung Baden-Württemberg (KVBW) gut anläuft, könnte der hiesige Modellversuch zum Vorbild für telemedizinische Sprechstunden auch in vielen anderen Ländern werden. Doch so laut viele Stimmen nach der Etablierung einer digitalen ärztlichen Sprechstunde auch rufen mögen: Mein Amt hat dafür zu sorgen, dass ein solches Angebot der Telemedizin auch den Anforderungen des Datenschutzes und der Datensicherheit entspricht. Der folgende Beitrag beleuchtet die datenschutzrechtlichen Aspekte des Pilotprojekts im Zusammenhang mit den jüngsten Entwicklungen im Bereich der Digitalisierung im Gesundheitswesen.

1.12.1 Digitalisierung im Gesundheitswesen – Die deutsche Politik erwacht aus ihrem Dornröschenschlaf

Im Einsatz digitaler Technologien, insbesondere der medizinischen Online-Beratung, sehen manche im deutschen Gesundheitswesen ein hohes Einsparpotenzial. Gleichzeitig rutscht Deutschland einem Bericht der EU-Kommission zufolge bei der Digitalisierung im Gesundheitswesen im Vergleich der europäischen Länder auf Platz 21 (im Internet abrufbar unter: https://ec.europa.eu/digital-single-market/en/desi; Stand: Juli 2018). Dieses Ergebnis ist nachvollziehbar vor dem Hintergrund, dass die Entwicklung der Telematik-Infrastruktur sowie der elektronischen Gesundheitskarte in Deutschland inzwischen fast 15 Jahre lang andauert.

Kein Wunder also, dass sowohl die Bundes- als auch die baden-württembergische Landespolitik die Digitalisierung im Gesundheitswesen zuletzt noch stärker als bisher in den Fokus genommen haben und mit großem Nachdruck vorantreiben wollen. Die Bundespolitik hat sich mit der sog. „E-Health-Initiative“ auf die Fahnen geschrieben, Telemedizin fördern zu wollen und daran zu arbeiten, dass telemedizinische Anwendungen schneller eingeführt werden. So sollen beispielsweise erfolgreiche Pilotprojekte besser in die allgemeine Gesundheitsversorgung integriert werden (im Internet abrufbar unter: https://www.bundesgesundheitsministerium.de/e-health-initiative.html; Stand Oktober 2018). Auch die Landesregierung Baden-Württemberg verfolgt mit ihrer Strategie „Digitalisierung in Medizin und Pflege in Baden-Württemberg“ diese Ziele. Das Ministerium für Soziales und Integration fördert einzelne Projekte in diesem Bereich. In diesem Jahr hat mein Amt einige dieser Projekte intensiv beraten, betreut und begleitet.

Eines dieser Pilotprojekte, welches das Ministerium für Soziales und Integration im Rahmen seiner Digitalisierungsstrategie mit rund 1 Million EUR fördert, ist die von der KVBW initiierte medizinische Fernsprechstunde DocDirekt. Mit diesem Callcenter sollen Teleärzte Patienten zeitnah beraten, auf freie Praxistermine verteilen und so davon abhalten, vorschnell die Krankenhaus-Notaufnahme aufzusuchen, so die Grundidee der KVBW.

1.12.2 Die telemedizinische Sprechstunde – bisher die Ausnahme in Deutschland

Die Idee einer telemedizinischen Sprechstunde ist nicht vollkommen neu: In der Schweiz etwa bietet ein Unternehmen seit dem Jahr 2000 rund um die Uhr ärztliche Beratungen per Telefon oder Video an und stellt auch Rezepte aus. Der schweizerische Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) weist darauf hin, schweizerische private Krankenversicherungen würden demjenigen Versicherten einen günstigeren, erschwinglichen Versicherungstarif anbieten, der sich verpflichtet, das Callcenter des Unternehmens stets zuerst zu konsultieren, bevor er persönlich einen Arzt aufsucht. Diese Tarife seien in der Schweiz inzwischen sehr weit verbreitet. Die Krankenversicherungslandschaft in der Schweiz ist jedoch, anders als in Deutschland, durch privatrechtliche Unternehmen geprägt. Der Versicherte kann deshalb in die Datenverarbeitung durch das Unternehmen einwilligen. Der EDÖB vertritt die Auffassung, dass die Datenverarbeitung durch dieses Unternehmen nach schweizerischem Recht datenschutzrechtlich nicht zu beanstanden ist.

Der Grund dafür, warum die telemedizinische Sprechstunde hingegen hierzulande bislang die große Ausnahme ist, sind enge rechtliche Grenzen. Zwar brachte das 2015 verabschiedete „Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen" (E-Health-Gesetz) eine punktuelle Öffnung für telemedizinische Sprechstunden. Es erachtete in bestimmten medizinischen Konstellationen eine telemedizinische Sprechstunde für zulässig; im Jahr 2017 wurden medizinische Fernsprechstunden schrittweise zunächst bei der Distanz-Befundbeurteilung von Röntgenaufnahmen zugelassen und dann bei vertragsärztlicher Versorgung, wenn der Fokus jeweils auf Nachsorge- und Kontrollterminen lag. Eine rein digitale Behandlung ohne vorherigen persönlichen Kontakt zwischen Arzt und Patienten, eine sogenannte ausschließliche Fernbehandlung, sieht jedoch auch das E-Health-Gesetz nicht vor.

Die Muster-Berufsordnung für Ärzte (MBO-Ä) regelte dieses ausschließliche Fernbehandlungsverbot in § 7 Absatz 4 bis vor kurzem wie folgt: „Ärztinnen und Ärzte dürfen individuelle ärztliche Behandlung, insbesondere auch Beratung, nicht ausschließlich über Print- und Kommunikationsmedien durchführen." Damit ist eine ausschließlich digitale Behandlung ausgeschlossen, es muss zumindest vorher ein persönlicher Arzt-Kontakt mit einer direkten Untersuchung stattgefunden haben.

1.12.3 Die Lockerung des ärztlichen Fernbehandlungsverbots – der Dammbruch in Baden-Württemberg

Die Landesärztekammer Baden-Württemberg hat im Jahr 2016 mit der Lockerung des ausschließlichen Fernbehandlungsverbots den Dammbruch ausgelöst, indem sie die ausschließliche ärztliche Fernbehandlung im Rahmen von Modellprojekten ermöglicht hat.

Der Wortlaut des § 7 Absatz 4 baden-württembergische Berufsordnung – Ärzte lautet: „Ärztinnen und Ärzte dürfen individuelle ärztliche Behandlung, insbesondere auch Beratung, nicht ausschließlich über Print- und Kommunikationsmedien durchführen. Auch bei telemedizinischen Verfahren ist zu gewährleisten, dass eine Ärztin oder ein Arzt die Patientin oder den Patienten unmittelbar behandelt. Modellprojekte, insbesondere zur Forschung, in denen ärztliche Behandlungen ausschließlich über Kommunikationsnetze durchgeführt werden, bedürfen der Genehmigung durch die Landesärztekammer und sind zu evaluieren."

Ein Jahr später, im Oktober 2017, genehmigte die Landesärztekammer Baden-Württemberg das bundesweit erste

Modellprojekt zur ausschließlichen Fernbehandlung von Privatversicherten: Bei diesem Projekt bieten zwei private Krankenversicherungen ihren Versicherten nach dem schweizerischen Vorbild an, dass sie sich ausschließlich via telemedizinischer Sprechstunde beraten und behandeln lassen können.

Private Krankenversicherungen verarbeiten die besonderen Kategorien personenbezogener Daten (z. B. Gesundheitsdaten) ihrer Versicherten in der Regel auf der Grundlage von deren Einwilligung. Sofern die Einwilligung allen datenschutzrechtlichen Anforderungen genügt, ist dies grundsätzlich nicht zu beanstanden.

1.12.4 Die telemedizinische Sprechstunde DocDirekt – der smarte Weg zum Arzt?

Mit dem telemedizinischen Modellvorhaben DocDirekt betrat die KVBW im April 2018 absolutes Neuland: Als bundesweit erste Kassenärztliche Vereinigung bot sie von nun an erstmals auch gesetzlich Krankenversicherten an, sich über das von ihr betriebene Callcenter von kooperierenden Telemedizinern aus der Ferne beraten zu lassen. Dies ist insofern bemerkenswert, als dies das erste telemedizinische Versorgungsangebot ist, welches von einer Kassenärztlichen Vereinigung in ihrer Funktion als Körperschaft des öffentlichen Rechts angeboten wird.

Körperschaften des öffentlichen Rechts sind wie Behörden an den Grundsatz der Gesetzmäßigkeit der Verwaltung gebunden. Sie dürfen Sozial- bzw. Gesundheitsdaten nur in engen Grenzen verarbeiten, nämlich nur insoweit, als diese Verarbeitung für die Erfüllung einer ihrer gesetzlich normierten Aufgaben erforderlich ist. Im Fall der Kassenärztlichen Vereinigungen legt § 285 SGB V den abschließenden Aufgabenkatalog fest, im Rahmen derer die Verarbeitung von Sozialdaten erlaubt ist.

Das Angebot telemedizinischen Sprechstunde DocDirekt funktioniert nach Aussagen der KVBW wie folgt: Eine bei der KVBW angestellte Medizinisch-Technische-Assistentin (MTA) nimmt den Telefon-, Chat- oder Video-Anruf des Versicherten entgegen und fragt zunächst dessen Beschwerdebild ab. Bei Notfällen wird der Anrufer sofort an die 112 weitergeleitet; liegt kein Notfall vor, so wird der Anrufer binnen 30 Minuten von einem kooperierenden Telearzt zurückgerufen. Wird hingegen anhand der Beschwerden deutlich, dass der Anrufer noch am gleichen Tag einen Arzt aufsuchen sollte, kann der Telearzt anhand einer Software sehen, bei welchem Vertragsarzt ein Termin zur Behandlung vor Ort frei ist.

Die KVBW selbst verarbeitet in dem Moment, wenn die KVBW-eigenen MTAs das Beschwerdebild des Versicherten am Telefon aufnehmen und schriftlich erfassen, Sozialdaten der Versicherten, die oftmals auch gleichzeitig Gesundheitsdaten sind. Bei diesen Kategorien handelt es sich jeweils um besonders sensible Daten, denen der deutsche wie europäische Gesetzgeber jeweils ein besonders hohes Schutzniveau zugeordnet hat. An die Verarbeitung von Gesundheitsdaten und deren Schutz werden dementsprechend hohe Ansprüche gestellt.

Siehe dazu Artikel 9 DS-GVO – „Verarbeitung besonderer Kategorien personenbezogener Daten" (bzw. § 46 Nr. 14 BDSG) – wobei nach Artikel 4 Nr. 15 DS-GVO (bzw. § 46 Nr. 13 BDSG) „Begriffsbestimmungen" Gesundheitsdaten personenbezogene Daten sind, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

Erwägungsgrund 35 der DS-GVO spezifiziert die Definition der Gesundheitsdaten weiter:

– Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese natürliche Person für gesund-

heitliche Zwecke eindeutig zu identifizieren, – Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, auch aus genetischen Daten und biologischen Proben, abgeleitet wurden, und – Informationen über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person unabhängig von der Herkunft der Daten, ob sie nun von einem Arzt oder sonstigem Angehörigen eines Gesundheitsberufes, einem Krankenhaus, einem Medizinprodukt oder einem In-Vitro-Diagnostikum stammen.

Und Erwägungsgrund 53 der DS-GVO (zur „Verarbeitung sensibler Daten im Gesundheits- und Sozialbereich") führt im Satz 1 weiter aus: Besondere Kategorien personenbezogener Daten, die eines höheren Schutzes verdienen, sollten nur dann für gesundheitsbezogene Zwecke verarbeitet werden, wenn dies für das Erreichen dieser Zwecke im Interesse einzelner natürlicher Personen und der Gesellschaft insgesamt erforderlich ist, insbesondere im Zusammenhang mit der Verwaltung der Dienste und Systeme des Gesundheits- oder Sozialbereichs, einschließlich der Verarbeitung dieser Daten durch die Verwaltung und die zentralen nationalen Gesundheitsbehörden zwecks Qualitätskontrolle, Verwaltungsinformationen und der allgemeinen nationalen und lokalen Überwachung des Gesundheitssystems oder des Sozialsystems und zwecks Gewährleistung der Kontinuität der Gesundheits- und Sozialfürsorge und der grenzüberschreitenden Gesundheitsversorgung oder Sicherstellung und Überwachung der Gesundheit und Gesundheitswarnungen oder für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken, die auf Rechtsvorschriften der Union oder der Mitgliedstaaten beruhen, die einem im öffentlichen Interesse liegenden Ziel dienen müssen, sowie für Studien, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden. Durch das hohe Schutzniveau von Gesundheitsdaten ist nach der DS-GVO die Durchführung einer Datenschutz-Folgenabschätzung notwendig und die Liste des LfDI nach Artikel 35 DS-GVO Absatz 4 benennt explizit auch den Einsatz von Telemedizin-Lösungen zur detaillierten Bearbeitung von Krankheitsdaten. Nach Artikel 32 Absatz 1 DS-GVO hat der Verantwortliche (und ggf. vorhandene Auftragsverarbeiter) unter Berücksichtigung des Stands der Technik geeignete technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten zu treffen. Als Maßnahme wird bspw. die Verschlüsselung personenbezogener Daten genannt.

Die Daten der Patienten werden angabegemäß dreifach gesichert und sollen auf Servern in Ehningen und Frankfurt, aber auch bei der KVBW selbst auf Servern gespeichert werden. Die Aussagen der beteiligten Dienstleister, wenn es um die Sicherheit der Daten geht, stimmen optimistisch: „TeleClinic bietet maximale Datensicherheit und verhindert Missbrauch auf jeder Ebene. Ein vierstufiges Sicherheitssystem bietet die höchste Datensicherheit Deutschlands. Die Hoheit des Nutzers über seine Daten ist das höchste Gebot für TeleClinic." Oder „Bei der medizinischen Beratung und Behandlung genießen Datensicherheit und Datenschutz oberste Priorität. Die Datenverarbeitung findet ausschließlich im Gebiet der Bundesrepublik Deutschland statt. Alle Daten werden verschlüsselt übertragen und verschlüsselt auf Datenbankservern in zertifizierten deutschen Rechenzentren abgelegt."

An diesen Aussagen muss sich die konkrete technisch-organisatorische Ausgestaltung des Modellvorhabens messen lassen. Auch die Datenschutz-Folgenabschätzung wird damit zur spannenden Lektüre.

Das Produkt „docdirekt Powered by TeleClinic" (https://www.docdirekt.de/impressum/) hat nicht nur eine, sondern gleich zwei Datenschutzerklärungen parat.

Unter https://www.docdirekt.de/datenschutz/ (Stand Oktober 2018) erhält man

die erste Datenschutzerklärung und erfährt, dass diese Erklärung nur für die Website www.docdirekt.de gilt. Sie gilt nicht für Websites, auf die diese Homepage verlinkt.

„Details zur Erhebung, Speicherung, Verarbeitung und Nutzung von personenbezogenen Daten bei einer Anmeldung zur Nutzung von docdirekt entnehmen Sie bitte der datenschutzrechtlichen Einwilligungserklärung: Datenschutzbestimmungen docdirekt" und dort erhält man offenbar auch die Antwort auf die Frage: „Wer erhält Zugriff auf die im docdirekt-System gespeicherten Daten?":

„[…] Auf die über Sie im docdirekt-System gespeicherten Daten können zugreifen

- die Beschäftigten der KVBW, die mit der Sie betreffenden Betreuung im Rahmen von docdirekt und der Abrechnung der ärztlichen Leistungen befasst sind,
- die Sie behandelnden Teleärzte,
- der Sie behandelnde Arzt einer gegebenenfalls eingeschalteten PEP-Praxis und
- Beschäftigte der TeleClinic GmbH im Rahmen des Betriebs und der Wartung der Software.
- Eine Weitergabe Ihrer personenbezogenen Daten an Dritte erfolgt nur soweit die gesetzlichen Rahmenbedingungen dies erlauben. […]"

Gekoppelt mit einer dort ebenfalls verorteten „Einwilligungserklärung und Entbindung von der Schweigepflicht". Diese führt weiter aus:

„[…] Ich willige in folgende Datenverarbeitung ein und entbinde damit auch die Beschäftigten der KVBW sowie die in meine Behandlung eingeschalteten Teleärzte und Ärzte der PEP-Praxen insoweit von ihrer Schweigepflicht:

Die KVBW darf die im Rahmen meiner Anmeldung sowie der Nutzung von docdirekt erhobenen Daten, insbesondere meinen Vor- und Nachnamen, Anschrift, Telefonnummer (Festnetz und/oder mobil) und E-Mail-Adresse, die administrativen Versichertendaten auf meiner elektronischen Gesundheitskarte (§ 291 SGB V) sowie die von mir mitgeteilten Beschwerden speichern und an die in meine Behandlung eingebundenen Teleärzte weiterleiten.

Die in meine Behandlung über docdirekt eingebundenen Teleärzte dürfen die von ihnen erhobenen Behandlungsdaten und Befunde an die KVBW und eine PEP-Praxis weiterleiten.

Ebenso darf eine mir genannte PEP-Praxis der KVBW mitteilen, ob ich diese aufgesucht habe oder nicht. […]"
(Quellen: https://www.docdirekt.de/fileadmin/user_upload/dokumente/datenschutzbestimmungen_docdirekt.pdf, https://www.medical-tribune.de/praxis-und-wirtschaft/ehealth/artikel/kv-projekt-docdirekt-mit-tele-aerzten-geht-online/)
Zum Einloggen geht es nun zu einer verlinkten Seite https://docdirekt.teleclinic.com/login.
Hierbei fällt auf, dass die nun verwendete IP-Adresse von der vorherigen deutlich abweicht und zum Adressbereich der Fa. Cloudflare, Inc. (Hauptsitz San Francisco, USA) gehört. Cloudflare „reinigt und beschleunigt" den Webdatenverkehr. Und weiter: „Wenn Sie Cloudflare verwenden, müssen wir die Daten auf unserem Edge entschlüsseln, um schlechten Datenverkehr zwischenspeichern und filtern zu können. […] Schon vor der Übermittlung Ihrer Website wird das Cloudflare Rechenzentrum Besucher auf eventuelle Bedrohungen scannen. Dabei berücksichtigt es beispielsweise die IP-Adresse des Besuchers, welche Ressourcen angefordert werden, welche Nutzlast sie angeben, und wie oft sie Anfragen ausführen. Zusammen genommen können wir anhand dieser Merkmale Websites vor bösartigen Besuchern schützen, indem wir sie noch vor Ihrem Webserver stoppen.[…]"

(Quellen: https://support.cloudflare.com/hc/de/articles/205177068-Schritt-1-Wie

-funktioniert-Cloudflare-, https://www.cloudflare.com/de-de/network/)

Auf die Fa. Cloudflare erfolgte bisher aber kein sichtbarer Hinweis. Auch weichen nun die zweiten Datenschutzhinweise unter https://www.teleclinic.com/datenschutz (Stand Oktober 2018) deutlich von den ersten Hinweisen bei DocDirekt ab.

Das Produkt verwendet unter anderem „die Technologie der Mixpanel, Inc. (Hauptsitz San Francisco, USA) um statistische Auswertungen durchzuführen, die es TeleClinic ermöglichen, Produktfunktionen zu optimieren und ansprechender zu gestalten." Es wird an dieser Stelle auch auf eine Opt-out-Möglichkeit hingewiesen. Von den Patienten wird also erwartet, vor der eigentlichen Nutzung sämtliche Hinweise gründlich zu studieren und zuallererst die Privacy-Einstellungen vorzunehmen, die ihnen genehm sind.

Sollten die Patienten auf einem Smartphone die docdirekt-App nutzen, sind ebenfalls Tracking- und Analysemodule in Verwendung. Und dies offenbar, bevor überhaupt explizit eine Einwilligung erteilt werden kann. (Quelle: https://www.kuketz-blog.de/gesundheits-app-docdirekt-weitere-datenschutz-bruchlandung/)

Das Modellvorhaben hat also Nachbesserungsbedarf und die Verantwortlichen und Auftragsverarbeiter sollten vor Einführung weiterer Module wie dem Elektronischen Rezept und weiterer Expansion nochmals selbstkritisch über dessen gesamte technisch-organisatorische Ausgestaltung nachdenken.

1.12.5 DocDirekt und die besondere Rolle der KVBW

Bei den vielen Beratungen der KVBW, welche meine Dienststelle anlässlich von DocDirekt durchgeführt hatte, stand aus datenschutzrechtlicher Perspektive vor allem die Frage nach der Rechtsgrundlage im Mittelpunkt: Kann die KVBW sich auf eine gesetzliche Ermächtigungsgrundlage aus ihrem Aufgabenkatalog des § 285 SGB V berufen? Oder kann sie sich als Körperschaft des öffentlichen Rechts auf die (konkludente) Einwilligung der Versicherten stützen?

Die Kassenärztlichen Vereinigungen haben, vergleichbar mit den gesetzlichen Krankenkassen, einen gesetzlich sehr eng gefassten und klar umgrenzten Bereich, innerhalb dessen sie befugt sind, personenbezogene Daten der Versicherten zu verarbeiten. Insbesondere dürfen sie diese Daten – im Gegensatz zu den privaten Krankenversicherungen – in der Regel nicht auf Grundlage einer Einwilligung verarbeiten.

Kassenärztliche Vereinigungen bzw. gesetzliche Krankenkassen verarbeiten die besonderen Kategorien personenbezogener Daten (z. B. Gesundheitsdaten) auf gesetzlicher Grundlage im Rahmen ihres jeweiligen gesetzlichen Aufgabenkatalogs (§§ 284 ff. SGB V). Eine Datenverarbeitung dürfen sie regelmäßig nicht mit einer Einwilligung rechtfertigen, da diese in ihrer Eigenschaft als Körperschaften öffentlichen Rechts in Grundrechte wie das der informationellen Selbstbestimmung nur in den gesetzlich normierten Fällen eingreifen können (Grundsatz der Gesetzmäßigkeit der Verwaltung, Art. 30 Absatz 3 GG i. V. m. § 30 SGB IV). Andernfalls könnten Behörden mit Hilfe einer Einwilligung ihren gesetzlichen Handlungsspielraum beliebig erweitern.

Ferner versperren die als abschließend zu verstehenden bereichsspezifischen Regelungen des Sozialdatenschutzes – hier der Aufgabenkatalog der Kassenärztlichen Vereinigungen des § 285 SGB V – einen Rückgriff auf allgemeinere Regelungen des Datenschutzrechts, welche auch die Möglichkeit einer Einwilligung enthalten.

Schließlich lehnt die Rechtsprechung die Einwilligung wegen des bestehenden Ungleichgewichts zwischen Sozialversicherungsträgern und Versicherten

ab, da es infolgedessen an der Freiwilligkeit der Datenverarbeitung fehle (Urteil des Bundessozialgerichts vom 10.12.2008 – Az B 6 KA 37/07 R).

Auch der europäische Gesetzgeber weist im Zusammenhang mit der Freiwilligkeit der Einwilligung im Erwägungsgrund 43 der DS-GVO ausdrücklich darauf hin, dass eine Einwilligung keine gültige Rechtsgrundlage liefern sollte, wenn es sich bei dem Verantwortlichen um eine Behörde handelt und zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht herrscht.

Vor dem Hintergrund dieser Rechtslage hat mein Amt die KVBW dahingehend beraten, dass die Einwilligung als Rechtsgrundlage für Datenverarbeitungen, welche die KVBW im Rahmen von DocDirekt beabsichtigt selbst vorzunehmen, nicht in Betracht kommt; allenfalls könnten die Datenverarbeitungen der KVBW mit ihrer gesetzlichen Aufgabe des sog. Sicherstellungsauftrags, also mit einer normativen Ermächtigungsgrundlage, begründet werden.

§ 285 Absatz 2 i.V.m. Absatz 1 Nr. 2 SGB V regelt u. a., dass die Kassenärztlichen Vereinigungen Einzelangaben über die persönlichen und sachlichen Verhältnisse der Versicherten nur erheben und speichern dürfen, soweit dies zur Erfüllung der in Absatz 1 Nummer 2 SGB V genannten Aufgaben erforderlich ist. Nummer 2 benennt als eine Aufgabe der Kassenärztlichen Vereinigungen die Sicherstellung der vertragsärztlichen Versorgung auf (sog. Sicherstellungsauftrag). Die Vorschriften der § 75 i.V.m. § 73 Absatz 2 sowie § 105 SGB V gestalten den Sicherstellungsauftrag nach Inhalt und Reichweite näher aus und umfassen auch Maßnahmen der Kassenärztlichen Vereinigungen, welche die Sicherstellung der vertragsärztlichen Versorgung gewährleisten, verbessern oder fördern.

Wir haben der KVBW bei dem Versuch, die Datenverarbeitung auf die Rechtsgrundlage des Sicherstellungsauftrags zu stützen, konkrete Gestaltungsmöglichkeiten und konstruktive Vorschläge unterbreitet.

Gleichwohl war die KVBW nicht bereit, die Datenerhebung, welche sie durch ihre MTAs bei der Aufnahme des Beschwerdebilds plante und inzwischen praktiziert, auf den aus unserer Sicht erforderlichen Umfang zu begrenzen. Die MTA sollte nach dem Willen der KVBW uneingeschränkt „alle für eine effektive erste Anamnese" erforderliche Daten erheben. Nach Auffassung des LfDI ist eine derart unbestimmte und umfangreiche Erhebung von Daten durch die KVBW aus datenschutzrechtlicher Hinsicht unzulässig: Sie verstößt gegen die Grundsätze der Datensparsamkeit und -transparenz.

Die KVBW begründet ihre Verfahrensweise u. a. mit dem Argument, mit DocDirekt die Patientensteuerung verbessern zu wollen, um unnötige Arztbesuche möglichst zu verhindern und Notfallambulanzen zu entlasten. Dasselbe Ziel könnte aber nach unserer Auffassung auch erreicht werden, wenn die KVBW ihre Versicherten anhand einer nur groben Triage mittels eines klar definierten Fragenkatalogs an einen passenden Telearzt vermitteln würde. Wir unterbreiteten insoweit konkrete Vorschläge für einen solchen möglichen Fragenkatalog. Es ist gerade nicht erforderlich, dass eine MTA der KVBW die komplette Anamnese eines Patienten aufnimmt. Überdies ist nicht ersichtlich, warum es für das Ziel Sicherstellung der vertragsärztlichen Versorgung erforderlich sein soll, dass die KVBW selbst in Form von eigenen Mitarbeitern hochsensible Gesundheits-/Sozialdaten der Versicherten verarbeitet und sich nicht auf eine bloße Vermittlung der Versicherten an Teleärzte beschränkt.
Aus datenschutzrechtlicher Sicht haben wir zudem darauf hingewiesen, dass der Gesetzgeber für die sog. Terminservicestellen der Kassenärztlichen Vereinigungen eigenständige gesetzliche Regelungen geschaffen hat.

Terminservicestellen gibt es in Deutschland seit dem Jahr 2016. Sie dienen der

zeitnahen Vermittlung von Terminen bei niedergelassenen Fachärzten und Psychotherapeuten bei Vorliegen einer Überweisung. Sie werden von den Kassenärztlichen Vereinigungen betrieben. Ihre Einrichtung wurde durch das GKV-Versorgungsstärkungsgesetz gesetzlich in § 75 Absatz 1 a SGB V verankert.

Daraus lässt sich ableiten, dass der Gesetzgeber bereits für die Vermittlung von Terminen eine eindeutige gesetzliche Regelung für erforderlich hält, weil diese Aufgabe von dem Sicherstellungsauftrag nicht umfasst ist. Festzuhalten ist, dass nach Auffassung des LfDI jedenfalls Vermittlungen durch die Kassenärztlichen Vereinigungen, die inhaltlich weit über die Patientenvermittlung in Form einer groben Triage, so wie bei DocDirekt beabsichtigt, hinausgehen, nicht vom Sicherstellungsauftrag gedeckt sind.

Auch die Möglichkeit des § 105 Absatz 1 Satz 2 SGB V, welcher den Kassenärztlichen Vereinigungen den Betrieb von Eigeneinrichtungen und auch die Anstellung von Ärzten erlaubt, hilft hier nicht weiter. Diese Norm erlaubt den Kassenärztlichen Vereinigungen nicht, selbst Zugriff auf die Inhalte der Daten zuzugreifen, welche von ihnen angestellte Ärzte erheben. Vorliegend hat die KVBW jedoch keine Ärzte angestellt, sondern MTA.

Trotz datenschutzrechtlicher Bedenken ging die KVBW mit diesem Modellprojekt im April 2018 an den Start. Unter den Beteiligten bestand schließlich Einvernehmen, dass Änderungen der bundesgesetzlichen Rechtslage erforderlich sind, um eine datenschutzkonforme Umsetzung entsprechender Vorhaben zu gewährleisten.

Tatsächlich plant der Bundesgesetzgeber laut dem vorliegenden Gesetzentwurf zum Terminservice- und Versorgungsgesetz (TSVG) eine relevante Neuerung in § 105 SGB V (Im Internet abrufbar unter: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/T/Kabinettvorlage_Gesetzesentwurf_TSVG.pdf; Stand: 31.10.2018). Der Sicherstellungsauftrag soll danach erweitert werden: Kassenärztliche Vereinigungen sollen u. a. die Möglichkeit bekommen, im Rahmen des Sicherstellungsauftrags den Versicherten sog. „telemedizinische Versorgungsangebotsformen" anzubieten. Wir nahmen insoweit die Gelegenheit wahr, unsere Position klar zu machen, indem wir dem Ministerium für Soziales und Integration gegenüber mehrfach Stellung genommen haben zu den geplanten gesetzlichen Änderungen. Würden die Änderungen so beschlossen werden wie aktuell im Gesetzentwurf vorgesehen, so würde dies zwar den Sicherstellungsauftrag inhaltlich erweitern, jedoch ist auch hiervon nach unserer Auffassung noch nicht die Befugnis der Kassenärztlichen Vereinigung umfasst, Sozial- bzw. Gesundheitsdaten ihrer Versicherten auch selbst zu verarbeiten (Stand: 31. Oktober 2018).
Die KVBW hat in der Zwischenzeit bereits angekündigt, DocDirekt bis Ende des Jahres 2018 von den ursprünglichen Modellregionen Stuttgart und Tuttlingen auf ganz Baden-Württemberg ausweiten zu wollen. Bis Frühjahr 2019 soll es auch die Möglichkeit der Ausstellung eines elektronischen Rezepts geben. Dies ist insofern bemerkenswert, als es auch für die Ausstellung von Rezepten auf Grundlage einer ausschließlichen Fernbehandlung noch hohe rechtliche Hürden gibt.

Nach § 48 Absatz 1 Satz 2 Arzneimittelgesetz ist die Verordnung eines Arzneimittels ohne „offenkundigen" Arzt-Patienten-Kontakt grundsätzlich verboten. Nach § 31 Bundesmantelvertrag – Ärzte in Verbindung mit der Arbeitsunfähigkeits-Richtlinie des Gemeinsamen Bundesausschusses erfordern die Beurteilung der Arbeitsunfähigkeit und ihre voraussichtliche Dauer sowie die Ausstellung einer entsprechenden Bescheinigung eine ärztliche Untersuchung.

Zweifellos besteht der starke politische Wille, telemedizinische Versorgungsangebote zu fördern, um die ärztliche Versorgung zu optimieren und die Chancen,

welche die Digitalisierung der Gesundheitsbranche hierfür bietet, nicht alleine privaten Unternehmen zu überlassen. Inzwischen ist sogar die Skepsis großer Teile der Ärzteschaft, die jahrelang vehement zumindest einen persönlichen Erstkontakt zwischen Medizinern und Patienten eingefordert hatten, gegenüber der ausschließlich telemedizinischen Behandlung gewichen, sodass auf dem 121. Ärztetag im Mai 2018 bundesweit das berufsrechtliche Verbot der ausschließlichen Fernbehandlung gelockert worden ist. Das ist eine Zeitenwende und bedeutende Veränderung für das deutsche Gesundheitswesen. Jedoch sollte der Zeit- und Innovationsdruck, der durch die jahrelangen Versäumnisse an Kraft gewonnen hat, nicht dazu führen, dass telemedizinisch unausgereifte Angebote unkontrolliert auf den Gesundheitsmarkt drängen. Ein solches Szenario ginge zulasten der Entwicklung von Angeboten, die einen qualitativ hochwertigen und datenschutzrechtlich einwandfreien Standard gewährleisten. Gerade im Bereich der gesetzlichen Sozialversicherung, wo hochsensible Daten verarbeitet werden, sollten die bereits entwickelten Standards zum Datenschutz und zur Datensicherheit nicht einfach untergraben werden.

Als Datenschutzaufsichtsbehörde werden wir die die Entwicklungen in diesem Spannungsfeld weiterhin im Auge behalten und konstruktiv begleiten, datenschutzrechtlich thematisieren und notwendige gesetzgeberische Fortschritte ebenso anmahnen wie wir Datenschutzverstöße ggf. aufgreifen werden.

1.13 Bußgelder

Mit dem Wirksamwerden der DS-GVO zum 25. Mai 2018 wurden die Datenschutzaufsichtsbehörden ermächtigt, gemäß Art. 58 Abs. 2 lit. j DS-GVO in Verbindung mit Art. 83 DS-GVO bei Datenschutzverstößen Bußgelder gegen verantwortliche Stellen oder Auftragsverarbeiter zu verhängen. Am 06. Juni 2018 verabschiedete der Landtag von Baden Württemberg das neue Landesdatenschutzgesetz, welches am 21. Juni 2018 in Kraft trat. Gemäß § 25 Abs. 2 dieses Gesetzes übt der Landesbeauftragte für den Datenschutz die Befugnisse gemäß Art. 58 DS-GVO aus. Infolge der benannten Regelungen werden datenschutzrechtliche Bußgeldverfahren seit dem 25.Mai 2018 von meiner Dienststelle bearbeitet. Hierzu wurde eine Bußgeldstelle eingerichtet, die selbständig datenschutzrelevante Vorgänge untersucht und Bußgeldverfahren durchführt. Kenntnis von bußgeldrelevanten Vorgängen erhält die Bußgeldstelle durch Anzeigen von Staatsanwaltschaften und Polizei sowie durch Eingaben von Bürgern und durch Vorlagen der Fachreferate meiner Dienststelle.

1.13.1 Arbeitsweise der Bußgeldstelle

Gemäß § 41 Abs. 1 BDSG gilt bei Verstößen, die mit einem Bußgeld gemäß Art. 83 Abs. 4 bis 6 DS-GVO geahndet werden sollen, grundsätzlich das Gesetz über Ordnungswidrigkeiten (OWiG). Über § 46 Abs. 1 OWiG findet überdies die Strafprozessordnung (StPO) entsprechende Anwendung. Die Bußgeldstelle hat damit gemäß § 46 Abs. 2 OWiG als Verfolgungsbehörde im Bußgeldverfahren im Wesentlichen dieselben Rechte und Pflichten wie die Staatsanwaltschaft bei der Verfolgung von Straftaten. Hierzu zählen unter anderem die Vernehmung von Zeugen, die auch zwangsweise durchgesetzt werden kann, sowie die Erwirkung und der Vollzug von Durchsuchungs- und Beschlagnahmebe-

schlüssen mit Amtshilfe durch die Polizei. In datenschutzrechtlichen Bußgeldverfahren gelten zudem dieselben Prinzipien wie in jedem anderen Bußgeldverfahren.

1.13.2 Kriterien für die Einleitung eines Bußgeldverfahrens

Zur Verbesserung von Datenschutz und Datensicherheit stellen Bußgeldverfahren nur eine von vielen möglichen Maßnahmen dar. Insbesondere bei Verstößen, bei denen die/der Verantwortliche uneinsichtig ist und bei Verstößen, die aufgrund der nachfolgenden Kriterien als schwerwiegend einzustufen sind, ist die Einleitung eines Bußgeldverfahrens alternativ oder zusätzlich zu weiteren aufsichtsbehördlichen Maßnahmen wahrscheinlich. Diese Kriterien sind insbesondere:

1.13.3 Anzahl der Bußgeldverfahren

Innerhalb der ersten Monate nach Wirksamwerden der DS-GVO blieb die Zahl der monatlichen Eingänge auf einem stabilen Niveau. Unter Berücksichtigung der Altfälle, welche meine Dienststelle vom Regierungspräsidium Karlsruhe übernommen hat, wurden von Anfang Juni bis Ende Oktober 2018 rund 120 Bußgeldverfahren durchgeführt. Manche davon wurden einer Einstellung, sei es aus Rechtsgründen oder aus Opportunitätsgründen, zugeführt.

In einer Vielzahl von Fällen dauern die Ermittlungen noch an. Einige dieser Verfahren sind alsbald abschlussreif.

Mit einem ersten Bußgeldbescheid unter der DS-GVO wurde am 21. November 2018 eine Geldbuße in Höhe von 20.000,- Euro zzgl. einer Verfahrensgebühr von 1.000,- Euro gegen einen baden-württembergischen Social-Media-Dienstleister festgesetzt. Das Unternehmen hatte die Passwörter ihrer Nutzer im Klartext, also unverschlüsselt und unverfremdet gespeichert, um mittels eines sog. Passwortfilters zum Schutz der eigenen Nutzer die Übermittlung von Passwörtern an unberechtigte Dritte zu verhindern. Das Unternehmen war Opfer eines Hackerangriffs geworden, durch den unter anderem die Klartext-Passwörter von 330.000 Nutzern entwendet und später online veröffentlicht wurden. Nach Meldung dieser Datenpanne und Information der eigenen Nutzer arbeitete das Unternehmen in vorbildlicher Weise offen und transparent mit meiner Dienststelle zusammen. Meine Vorgaben wurden dabei bereitwillig und zügig umgesetzt, sodass in sehr kurzer Zeit eine deutliche Verbesserung der Sicherheit der Nutzerdaten erreicht werden konnte. Vor diesem Hintergrund genügte es, die Geldbuße im unteren Bereich des Bußgeldrahmens anzusetzen. Dabei wurde

berücksichtigt, dass das Unternehmen unter Einbeziehung der aufgewendeten und avisierten Maßnahmen für IT-Sicherheit einschließlich der Geldbuße einen Gesamtbetrag im sechsstelligen Euro-Bereich zu tragen hat.

Mit einem zweiten Bußgeldbescheid wurde am 06. Dezember 2018 eine Geldbuße von 80.000 Euro zzgl. einer Verfahrensgebühr von 4.000,- Euro gegen einen Verantwortlichen verhängt. Dieser hatte bei einer digitalen Publikation aufgrund unzureichender interner Kontrollmechanismen Gesundheitsdaten veröffentlicht, die versehentlich personenbezogene Daten enthielten. Der Verantwortliche wirkte bereitwillig und transparent bei der Aufklärung des Sachverhalts mit, sodass zügig die Datenschutzlücken identifiziert und geschlossen werden konnten. Für die Verbesserung der internen Kontrollmechanismen wendete der Verantwortliche dabei erhebliche Personal- und Sachmittel auf, die das Bußgeld bei Weitem überstiegen. Eine Reihe weiterer Bußgeldbescheide werden innerhalb der nächsten Monate folgen. Angesichts der Vielzahl an Beschwerden und Eingaben, die meine Dienststelle seit Wirksamwerden der DS-GVO erreicht haben, ist künftig von einem Anstieg der Bußgeldverfahren auszugehen.

1.13.4 Höhe der Geldbußen

Der Bußgeldrahmen wurde mit Wirksamwerden der DS-GVO deutlich erhöht. Konnten nach BDSG a. F. nur Bußgelder bis zu einer Höhe von maximal 300.000 Euro verhängt werden, wurde der Rahmen nun auf bis zu 20 Millionen Euro bzw. 4 % des weltweiten Konzernumsatzes eines Unternehmens angehoben. Die neue Bußgeldobergrenze liegt damit um ein Vielfaches über der bisherigen Grenze. Der Wunsch des europäischen Verordnungsgebers nach höheren Bußgeldern ist somit unmissverständlich und muss von allen europäischen Datenschutzaufsichtsbehörden umgesetzt werden, wie sich unter anderem aus Art. 83 Abs. 1 DS-GVO ergibt. Denn danach hat jede Aufsichtsbehörde sicherzustellen, dass „die Verhängung von Geldbußen… wirksam, verhältnismäßig und abschreckend ist." Es besteht jedoch weder eine Umrechnungsformel von Verstößen gemäß BDSG a.F. zur DS-GVO, noch existiert bislang ein europäischer Bußgeldkatalog. Allerdings arbeitet die Bußgeldstelle meiner Dienststelle gemeinsam mit der Bußgeldstelle der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), sowie den Datenschutzaufsichtsbehörden der Länder Rheinland-Pfalz und Hessen an der Erstellung von bundeseinheitlichen Richtlinien für die Verhängung von Geldbußen. Daneben findet unter Beteiligung der BfDI eine Abstimmung auf europäischer Ebene in der sog. „Task Force Fining" statt, die bislang aber noch keine Ergebnisse zur europäischen Vereinheitlichung der Bußgeldpraxis erbracht hat.

In der Bußgeldstelle meiner Dienststelle sind derzeit einige Verfahren anhängig, die nach vorläufiger Bewertung des derzeitigen Ermittlungsstandes die Festsetzung eines Bußgeldes im fünfstelligen Euro-Bereich erfordern. Daneben sind einzelne Verfahren anhängig, die nach vorläufiger Bewertung mit der Verhängung eines sechsstelligen Bußgeldes abgeschlossen werden. Verfahren, die die Verhängung einer Geldbuße im Millionen-Euro-Bereich erwarten lassen, sind derzeit nicht anhängig.

Auch in Zukunft wird nicht jeder Datenschutzverstoß mit einem Bußgeld geahndet werden müssen. Im Mittelpunkt der Arbeit meiner Dienststelle steht nach wie vor die Verbesserung des Datenschutzes und der Datensicherheit durch Aufklärung und Beratung. Wegen der gestiegenen Anzahl von Beschwerden ist jedoch insgesamt mit einem Anstieg der Bußgeldverfahren zu rechnen. Sofern Bußgelder verhängt werden müssen, werden diese in aller Regel deutlich höher ausfallen, als es in der Vergangenheit der Fall war. Der obere Bereich des Bußgeldrahmens wird dabei aber nur im Ausnahmefall erreicht werden.

2. Polizei und Kommunen

2.1 Kontrolle der Vergabe des ermittlungsunterstützenden Hinweises „HWAO“

Eine Kontrolle der Vergabepraxis des ermittlungsunterstützenden Hinweises „wechselt häufig Aufenthaltsort (HWAO)“ bei der Polizei Baden-Württemberg konnte den Verdacht, Personen der Volksgruppe der Sinti und Roma würden durch die Vergabe des Hinweises zielgerichtet erfasst und stigmatisiert, nicht bestätigen. Allerdings wurden wir bei der Kontrolle auf andere Mängel, insbesondere in Bezug auf die Festlegung und Einhaltung der rechtlichen Speicherfristen, aufmerksam.

Nach einem Gespräch mit dem Verband Deutscher Sinti und Roma e. V., Landesverband Baden-Württemberg, in welchem uns gegenüber der Verdacht geäußert wurde, dass die Polizei mittels der Vergabe des ermittlungsunterstützenden Hinweises (EHW) „wechselt häufig Aufenthaltsort (HWAO)“ eine zentrale Datei führe, in der systematisch alle bekannt gewordenen Angehörigen der Volksgruppe der Sinti und Roma gespeichert und stigmatisiert würden, entschieden wir uns zur Durchführung einer Kontrolle hinsichtlich der Vergabepraxis dieses Hinweises.

EHWs sind laut des vom Bundeskriminalamt erstellten EHW-Leitfadens „Hinweise auf Besonderheiten einer natürlichen Person, die primär dazu geeignet sind, einen polizeilichen Kontext zu verdeutlichen, polizeiliches Handeln zielgerichteter zu steuern bzw. zu unterstützen, oder die dem Schutz Dritter dienen. Sie sind darüber hinaus auch geeignet, Datenbestände für Ermittlungen zu kennzeichnen bzw. zu selektieren. Sekundär kann ein EHW auch dem Schutz der Betroffenen und der eingesetzten Polizeibediensteten dienen.“ Der EHW „wechselt häufig Aufenthaltsort“ ist ein landesspezifischer Hinweis und durfte nach dem Leitfaden in der Fassung der Polizei Baden-Württemberg mit landesspezifischen Ergänzungen (Stand: 17.03.2016) nur vergeben werden, wenn der Betroffene keine ständige Bindung an einen festen Wohnort oder einen häufig wechselnden Aufenthaltsort hatte. Die Rechtsgrundlage für die Vergabe dieses landesspezifischen EHW bildete § 38 Absatz 1 des Polizeigesetzes (PolG). Demnach kann der Polizeivollzugsdienst personenbezogene Daten, die ihm im Rahmen von Ermittlungsverfahren bekannt geworden sind, speichern, verändern und nutzen, soweit und solange dies zur Abwehr einer Gefahr oder zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. Die Gewinnung von Ermittlungshinweisen setzt voraus, dass auch Anhaltspunkte dafür bestehen, dass die betroffene Person zukünftig eine Straftat begehen wird (vgl. § 38 Absatz 3 PolG). Eine Speicherung ist deshalb nur i. V. mit der Annahme einer Wiederholungsgefahr möglich.

Noch vor Beginn unserer Kontrolle erfuhren wir, dass im Rahmen einer Prüfung des Innenministeriums der Verwendung von Minderheitenkennzeichnungen im Informationssystem der Landespolizei POLAS festgestellt wurde, dass der EHW „HWAO“ in seiner Aussagekraft eingeschränkt ist, da er nur in den Bundesländern Sachsen und Baden-Württemberg verwendet wurde. Vor dem Hintergrund des allgemeinen Diskriminierungsverbots wurde deshalb entschieden, dass der EHW seit 20. Juli 2018 nicht mehr vergeben werden darf.

An unserer Prüfung hielten wir dennoch fest. Eine Anfrage beim Landeskriminalamt Baden-Württemberg im April 2018 hatte einen Bestand von über 14.000 Personen ergeben, denen der EHW „HWAO“ im polizeilichen Informationssystem POLAS zugespeichert war. Unsere Prüfung führten wir anhand von Stichproben durch, die anhand verschiedener Kriterien ausgewählt wurden. In die Prüfung einbezogen wurden Fälle, in denen der EHW Personen zugespeichert wurde, die lediglich mit einem einzigen Delikt in POLAS einliegen

und deren Speicherung bereits mindestens fünf Jahre zurück liegt. Zur weiteren Eingrenzung der Fallzahlen wurden alphabetisch pro Anfangsbuchstabe des Familiennamens jeweils nur die beiden ältesten Speicherungen berücksichtigt. Anhand dieser Kriterien wurde uns durch das Landeskriminalamt eine Liste mit insgesamt 49 Personen übersandt, wobei zwei Personen doppelt erfasst waren. Die Akten wurden durch das Landeskriminalamt bei insgesamt zehn verschiedenen Polizeipräsidien angefordert. Zu drei Personen waren die Akten jedoch aufgrund abgelaufener Speicherfristen zwischenzeitlich gelöscht worden. Zur Prüfung standen uns somit insgesamt 44 Akten zur Verfügung.

Wir konnten feststellen, dass in den meisten Fällen die Vergabe des EHW Personen betraf, die keinen festen Wohnsitz hatten. Bei anderen erschien die Vergabe aufgrund wechselnder Aufenthaltsorte berechtigt. In sieben Fällen war eine Aussage zur Rechtmäßigkeit der Vergabe anhand der übersandten Aktenbestände nicht sicher möglich. Der Hinweis „HWAO" wurde in diesen Fällen an Personen vergeben, die einen festen Wohnsitz in Deutschland hatten. In diesen Fällen wurden die Ermittlungsakten (E-Akten) nachgefordert. In fünf Fällen wurden uns diese zeitnah übersandt und wir konnten feststellen, dass die Vergabe berechtigt war. In zwei Fällen teilten die Polizeipräsidien mit, dass die E-Akten bereits ausgesondert seien. In einem dieser Fälle hatte uns bislang lediglich eine unvollständige Kopie der Erfassungsbelege vorgelegen. Anhand der nun vollständig übersandten Erfassungsbelege konnte dem Sachverhalt bereits die Rechtmäßigkeit der Vergabe des EHW entnommen werden. In zwei weiteren Fällen, in denen uns die Akten bei der Prüfung bereits vollständig vorlagen, wurde jedoch festgestellt, dass die Voraussetzungen zur Vergabe des Hinweises nicht vorgelegen hatten. Im einen Fall handelte es sich um einen Deutschen, der sich im Ausland während eines Urlaubsaufenthalts strafbar gemacht, jedoch in Deutschland einen festen Wohnsitz hatte. Im anderen Fall wurde eine ausländische Betroffene mit festem Wohnsitz in Deutschland zur Anzeige gebracht. Der Akte war weder ein Hinweise auf häufig wechselnde Aufenthaltsorte noch darauf zu entnehmen, dass sie keine feste Bindung an den bekannten Wohnort hatte. Die Vergabe des Hinweises „HWAO" war deshalb in beiden Fällen nicht nachvollziehbar.

Bei den geprüften Vorgängen wurde der Hinweis „HWAO" an Angehörige insgesamt 15 verschiedener Staaten sowie einen Staatenlosen vergeben. In einem Fall fand sich in der Akte ein Hinweis, dass die Betroffene einer Gruppe von „Landfahrern" angehören soll. Dieser Verdacht wurde von der Geschädigten in der Vernehmung geäußert. Bei der Betroffenen handelte es sich um eine serbische Staatsangehörige ohne festen Wohnsitz in Deutschland. In einem anderen Fall wurde vermerkt, dass es sich bei dem Betroffenen um einen Angehörigen einer Gruppe „Sinti" handle, welche zur Tatzeit am Tatort in Wohnwagen campiert hatten. Die Ermittlungen ergaben, dass der Betroffene von der bekannten Wohnanschrift bereits seit längerer Zeit nach Unbekannt verzogen war. In beiden Fällen ist deshalb nichts gegen die Vergabe des Hinweises einzuwenden.

Die Prüfung der uns übersandten Akten bzw. Aktenbestände ergab, dass der EHW „HWAO" in den meisten Fällen berechtigt vergeben worden war. Anhaltspunkte dafür, dass der Hinweis zielgerichtet für die polizeiliche Speicherung bestimmter Volksgruppen genutzt wird, ergaben sich aus den geprüften Akten nicht.

Bei unserer Prüfung stießen wir allerdings auf andere Probleme in Bezug auf die polizeiliche Speicherpraxis in POLAS:

So wurde in mehreren Fällen mitgeteilt, dass die E-Akten zu den in POLAS gespeicherten Fällen bereits vernichtet worden seien. Weshalb lediglich die Papierakte, nicht aber die POLAS-Speicherung gelöscht wurde, ist nicht nachvollziehbar. Eine Speicherung ohne Aktenrückhalt ist

nicht zulässig. Die Vorgänge sind deshalb aus POLAS zu löschen.

Weiter wurde festgestellt, dass die für POLAS festgelegten Speicherfristen in vielen der geprüften Fälle bereits abgelaufen waren. Ein Polizeipräsidium erklärte diesen Umstand damit, dass bei Fällen, welche als INPOL-relevant markiert und damit im bundesweiten polizeilichen Informationsverbund INPOL gespeichert wurden, die automatische Löschung unterblieben sei, da sich die Laufzeiten dann nach den in INPOL festgelegten längeren Speicherfristen gerichtet hätten. Es ist zu vermuten, dass diese Problematik auch bei Fällen anderer Polizeipräsidien zugrunde liegen könnte. Zumindest in einem weiteren Fall fand sich ein Vermerk in der Akte, wonach eine Fristverlängerung aufgrund längerer Speicherfristen des INPOL-Bestands der betroffenen Person festgelegt wurde. In anderen Fällen befanden sich INPOL-Fahndungsnotierungen oder INPOL-Auszüge in der Akte, die diese Vermutung ebenfalls nahe legen.

Abgesehen davon, dass es nach § 38 Absatz 5 Satz 4 PolG einer schriftlichen Begründung der Erforderlichkeit bedarf, wenn die Daten über die festgesetzten Fristen weiter gespeichert bleiben sollen, stellt sich hier die Frage, ob es rechtmäßig sein kann, dass Vorgänge im landesweiten POLAS-System aufgrund von Erkenntnissen anderer Bundesländer über die festgelegten Speicherfristen hinaus gespeichert werden. Gerade weil es sich um ein landesweites Dateisystem handelt, in dem bewusst nur Fälle aus Baden-Württemberg und keine bundesweiten Vorgänge gespeichert werden, ist es unzulässig, die Löschfristen in POLAS durch Erkenntnisse anderer Bundesländer in bundesweiten Dateien auszuhebeln und die in POLAS gespeicherten Vorgänge über die zulässigen landesrechtlichen (Höchst-) Fristen hinaus zu speichern (siehe auch Nr. 2.4 dieses Berichts).

Ein ähnliches Problem, fand sich regelmäßig bei Vorgängen, die als relevant zur Erfassung in der Verbunddatei „Kriminalaktennachweis" (KAN) markiert wurden. Die Erfassung in KAN dient dem Nachweis von Kriminalakten, die bei Bund und Ländern angelegt sind, bei schweren oder überregional bedeutsamen Straftaten oder Straftaten bei denen gemäß § 81 g Absatz 1 der Strafprozessordnung (StPO) die Voraussetzungen zur Speicherung eines DNA-Identifizierungsmusters vorliegen. In der Regel war diese Kategorisierung mit der Vergabe einer zehnjährigen (Höchst-) Speicherfrist verbunden, obwohl für die Vorgänge oftmals nach §38 PolG i. V. m. § 5 Absatz 1 der Verordnung des Innenministeriums zur Durchführung des Polizeigesetzes (DVO PolG) nur eine Laufzeit von fünf Jahren oder nach § 5 Absatz 3 DVO PolG (als Fälle geringer Bedeutung) sogar nur eine dreijährige Speicherfrist gerechtfertigt gewesen wäre. Hier stellt sich die Frage, wie diese Vorschriften tatsächlich anzuwenden sind, wenn gleichzeitig auch ein Kriterium zur KAN-Vergabe mit der Möglichkeit deutlich längerer Speicherfristen greift. Die Aussonderungsprüffristen für KAN betragen nach § 77 Abs. 1 des Bundeskriminalamtgesetzes (BKAG) bei Erwachsenen höchstens zehn Jahre, bei Jugendlichen fünf Jahre und bei Kindern zwei Jahre, wobei nach Zweck der Speicherung sowie Art und Schwere des Sachverhalts zu unterscheiden ist. Bezüglich der zulässigen Speicherfristen für KAN heißt es in der Errichtungsanordnung, dass jede eingebende Stelle für sich im Rahmen einer Einzelfallprüfung die Aussonderungs- und Prüffristen festlegt. Auch dies unterstreicht, dass die landesrechtlichen Regelungen des § 38 PolG i. V. m. § 5 DVO PolG beachtet werden und somit auch Anwendung finden müssen. Nur so kann die Speicherung dem Verhältnismäßigkeitsgrundsatz gerecht werden. Dies wird auch im Zusammenhang mit der Einführung des Polizeilichen Informations- und Analyseverbunds (PIAV) verdeutlicht. PIAV ist als Verbundanwendung auf Bundesebene Teil des Informationssystems der Deutschen Polizei (INPOL) und stellt zur länderübergreifenden Kriminalitätsanalyse unverzüglich ausgewählte Personen-, Sach- und

Falldaten aus Vorgangs- und Fallsystemen des Bundeskriminalamts, der Länderpolizeien, der Bundespolizei, des Zolls sowie der Polizei beim Deutschen Bundestag bereit. In der Bund-Länder-Zusammenarbeitsrichtlinie heißt es im Zusammenhang mit der Aussonderungsprüfung „Kürzere Aussonderungsprüffristen können sich aus landes- bzw. bundesrechtlichen Vorschriften ergeben".

Eine weitere Problematik, die uns bei der Prüfung der Fälle vermehrt begegnet ist, ist Folgende: Häufig wurden in den Erfassungsbelegen bei der Prognose für die Annahme der Wiederholungsgefahr Kriterien ausgewählt, die nicht nachvollziehbar und in der Akte nicht weiter begründet waren. Die entsprechenden Bedeutungen der Begrifflichkeiten wurden dabei offensichtlich häufig nicht beachtet. So wurden zum Beispiel Betroffene als „Überzeugungstäter" gekennzeichnet oder ihnen „fehlendes Unrechtsbewusstsein" unterstellt, obwohl sie laut Akte keinerlei Angaben gemacht und sich laut Akte keinerlei sonstigen Hinweise ergeben hatten, die eine solche Feststellung stützen würden. Es ist deshalb fraglich, wie die entsprechenden Beurteilungen überhaupt getroffen werden konnten. Teilweise wurde bei Sachverhalten, die als Fälle geringer Bedeutung gem. § 5 DVO PolG anzusehen waren, den Betroffenen „hohe kriminelle Energie" unterstellt, ohne weiter in der Akte auf diese Annahme einzugehen. Auch die Kriterien „Gewohnheits-, Serien-, Gewerbs-, Bandenmäßigkeit" wurden vielfach gewählt, ohne dass diese begründet erscheinen. Zur Frage, ob eines dieser Kriterien vorliegt, müssen gewisse, bereits durch die Rechtsprechungen häufig definierte, Voraussetzungen erfüllt sein. So wird „Gewohnheitsmäßigkeit allgemein als durch Übung, insbesondere wiederholte Tatbegehung erworbener, eingewurzelter und selbständig fortwirkender Hang verstanden, als psychischer Zustand, der gerade dadurch gekennzeichnet ist, dass der Täter sich seiner beim Handeln nicht bewusst ist und der sich im täglichen Leben in den Fällen äußert, in denen ein Handeln auch dann noch wiederholt wird, wenn sich die dieses Handeln rechtfertigenden Umstände längst geändert haben." (OLG Köln, Beschluss vom 10. November 2015 – 1 RVs 209/15 , Rn.11, -juris). Nach aktueller Rechtsprechung handelt gewerbsmäßig „wer sich durch wiederholte Tatbegehung eine nicht nur vorübergehende Einnahmequelle von einigem Umfang und einiger Dauer verschaffen will. (Festhaltung BGH, 17. Juni 2004, 3 StR 344/03, BGHSt 49, 177)" (BGH, Urteil vom 09. Juli 2013 – 5 StR 181/13 –, juris). Auch „Bandenmäßigkeit" lässt sich nicht allein dadurch schon begründen, dass mehrere Personen gemeinsam eine Straftat begehen. „Als Indizien, ob eine Tat bandenmäßig begangen wurde, kommen insbesondere in Betracht: Eingebundensein in eine bandenmäßige Organisation, geschäftsmäßige Auftragsverwaltung, gemeinsame Buchführung, arbeitsteilige und gleichberechtigte Akquisition, Vermittlungstätigkeit und Forderungseinziehung, gegenseitige Kontrolle und Schutz, gemeinsame Kasse oder die Beteiligung an den gemeinsam erwirtschafteten Gewinnen und Verlusten. (BGH, Urteil vom 19. Mai 1999 – 2 StR 650/98 –, juris)

In Bezug auf die Wiederholungsgefahr stellten wir außerdem fest, dass die Dokumentation der angenommenen Wiederholungsgefahr für die Begehung künftiger Straftaten des Betroffenen oftmals nicht den rechtlichen Anforderungen entspricht. Nach § 38 Absatz 3 PolG wird für eine über zwei Jahre andauernde Speicherung das Vorliegen tatsächlicher Anhaltspunkte für die Annahme, die betroffene Person werde zukünftig eine Straftat begehen, gefordert. Diese Annahme lag offensichtlich allen geprüften Vorgängen zugrunde, jedoch wurde diese in vielen Fällen gar nicht oder nicht ausreichend begründet. Die aktuelle Rechtsprechung fordert: „Die die Wiederholungsgefahr nach § 38 Abs 1 S 2, 3 PolG a. F. (juris: PolG BW 1992) begründenden Anhaltspunkte sind in einer auf den Einzelfall bezogenen, auf schlüssigen, verwertbaren und nachvollziehbar dokumentierten Tatsachen beruhenden Entscheidung festzuhalten. Fehlt es an einer solchen

Dokumentation der Wiederholungsgefahr, ist die Datenspeicherung rechtswidrig." (Verwaltungsgerichtshof Baden-Württemberg, Urteil vom 10. Februar 2015 – 1 S 554/13 –, juris) In vielen Fällen wurde im Erfassungsbeleg zwar eine Auswahl der vorgegebenen Stichworte getroffen, diese in dem dafür vorgesehenen Freitextfeld zur Einzelfallbegründung für die Wiederholungsgefahr aber nicht näher erläutert. Die Ausführungen beschränkten sich dabei überwiegend auf die Wiederholung ausgewählter Stichworte bzw. von Synonymen. Teilweise fanden sich wenig aussagekräftige und im Vorgang ebenfalls nicht weiter erläuterte Formulierungen wie z. B. "Gesamtumstände der Tat" oder „besteht aufgrund des persönlichen Umfelds".

Im Rahmen unserer Prüfung stellten wir zudem fest, dass teilweise Fälle gespeichert waren, die allein aufgrund der vorliegenden Einstellungsverfügung der Staatsanwaltschaft hätten gelöscht werden müssen. So ging in einem Fall aus der Einstellungsverfügung hervor, dass der Straftatbestand gar nicht erfüllt und das Verhalten strafrechtlich nicht zu beanstanden war. In einer anderen Mitteilung hieß es „Die Überprüfung durch die Ermittlungsbehörde ergab bislang keine greifbaren Anhaltspunkte für Straftaten. (..)" In einer anderen Mitteilung der Staatsanwaltschaft, über fünf Jahre nach einem begangenen Diebstahl, wurde mitgeteilt, dass die Tat bereits verjährt und die Ahndung der Tat deshalb ausgeschlossen sei. Bei diesem Hinweis hätte eigentlich auffallen müssen, dass auch die festgesetzte fünfjährige Laufzeit für die POLAS-Speicherung abgelaufen war.

Das Ergebnis unserer Kontrolle zeigt, dass in Bezug auf die Einhaltung rechtlicher Vorgaben bei den polizeilichen Speicherungen in vielerlei Hinsicht Mängel bestehen. Die uns zur Prüfung vorgelegten Akten wurden alle in den Jahren 2007 bis 2011 in POLAS erfasst. Die Frage ist, ob sich in den vergangenen Jahren an den festgestellten Problemen etwas verändert hat. Wir haben deshalb beim Landeskriminalamt bezüglich der aktuellen Regelungen zum Löschverfahren in POLAS sowie der aktuellen Eingabemodalitäten hinsichtlich der Speicherfristenauswahl bei gleichzeitiger KAN-Relevanz um Auskunft ersucht. Die Antwort steht noch aus. Die Problematik bei fehlender Dokumentation der Wiederholungsgefahr im Hinblick auf die Rechtmäßigkeit der Datenspeicherungen in POLAS hatten wir bereits im Rahmen unserer Kontrolle der „Falldatei Rauschgift" im Jahr 2016 angesprochen. Wir gehen davon aus, dass die rechtlichen Anforderungen zwischenzeitlich bis auf die Sachbearbeiterebene umgesetzt wurden und bei der Erfassung in POLAS auch Beachtung finden. Die Polizei ist gefordert, technische sowie didaktische Maßnahmen zu finden, um die Rechtmäßigkeit polizeilicher Speicherungen für die Zukunft zu garantieren und Missstände bei bestehenden Speicherungen zu beheben.

2.2 Gebrochene Zusage

Man sollte doch meinen, dass man sich auf das Wort der Polizei verlassen kann. Schließlich nimmt sie in regelmäßigen Umfragen über die Vertrauenswürdigkeit von Institutionen regelmäßig einen Spitzenplatz ein. Leider zeigt die Realität manches Mal ein anderes Bild. So im Fall einer Petentin, dem Folgendes zugrunde lag:

Im Jahr 2015 wandte sich die Petentin an meine Dienststelle, weil sie auf ein Auskunftsersuchen hin erfahren hatte, was die Polizei so alles über sie speichert. Die Zahl der gespeicherten Verfahren war tatsächlich beeindruckend, sie reichten fast 20 Jahre zurück. Um hier aber keinen falschen Eindruck entstehen zu lassen: Es ging durchweg um Bagatelldelikte, die allerdings in „schöner" Regelmäßigkeit wiederkehrten.

In mühevoller Kleinarbeit gelang es uns, dabei auch tatkräftig durch das Landeskriminalamt unterstützt, die Rechtmäßigkeit oder Unrechtmäßigkeit der einzelnen

Speicherungen jeweils herauszuarbeiten. Hieran schloss sich der Versuch an, die Polizeidienststellen, welche die Speicherungen im polizeilichen Informationssystem jeweils zu verantworten hatten, von unserer Rechtsauffassung zu überzeugen. In einigen Fällen gelang dies schnell, etwa die Speicherung einer Sachbeschädigung: Hier war der Petentin vorgeworfen worden, im Rahmen einer Aktion, bei der mit Sprühkreide Punkte auf einem Parkplatz aufgesprüht worden waren (Schaden ca. 30 Euro), die Deckel der Sprühdosen in ihrem Rucksack bei sich geführt zu haben. In anderen Fällen ging es um die Reduzierung von Speicherfristen, hier wurden zum Teil Maximalfristen vergeben, die aus unserer Sicht nicht berechtigt waren, und die den Effekt hatten, alle vorherigen Speicherfristen mitzuziehen, bis die letzte Frist abgelaufen war.

Das Ganze führte im Ergebnis dazu, dass das Landeskriminalamt im Januar 2017 abschließend mitteilte, wenn nichts neues mehr dazu komme, würden die Daten Ende Juli 2017 komplett gelöscht werden. Freudig teilten wir dieses gute Ergebnis der Petentin mit, allerdings mit dem Rat, zu gegebener Zeit sicherheitshalber nochmal nachzufragen, ob die Ankündigung auch vollzogen sei. Die Überraschung folgte auf den Fuß: Nach einem Auskunftsantrag vom Herbst 2017 wurde der Petentin im Dezember 2017 mitgeteilt, es sei alles noch beim Alten. Obwohl sich die Petentin in Baden-Württemberg über Jahre nichts mehr hatte zuschulden kommen lassen, befand sich der vollständige Datenbestand noch immer im Auskunftssystem. Als Löschtermin war das Frühjahr 2023 vorgesehen. Die erstaunliche Begründung dafür war, dass die Bundespolizei mittlerweile ein Ermittlungsverfahren in das bundesweite, beim Bundeskriminalamt geführte Informationssystem INPOL eingestellt habe. Aus einer Dienstanweisung zum Landesinformationssystem POLAS ergebe sich, dass in solchen Fällen der Landesbestand mitgezogen werde. Auf eine solche Begründung waren wir nicht gefasst! Postwendend teilten wir dem Landeskriminalamt sowie betroffenen Polizeipräsidien unsere Rechtsauffassung wie folgt mit:

Die Frage, ob und für welchen Zeitraum die Polizei des Landes personenbezogene Daten von Bürgern in ihren Dateien speichern darf, bestimmt sich einzig und allein nach Gesetz. Eine Dienstanweisung als rein polizeiinterne Vorgabe kann Grundrechtseingriffe dagegen nicht legitimieren. Die für die Polizei des Landes allein maßgeblichen Speicherungsvoraussetzungen ergeben sich aus § 38 des Polizeigesetzes (PolG) in Verbindung mit § 5 der Verordnung des Innenministeriums zur Durchführung des Polizeigesetzes (DVO PolG). Nach diesen Vorschriften ist eine weitere Speicherung der Daten der Petentin in dem Auskunftssystem POLAS nach dem 31. Juli 2017 nicht mehr zulässig. Etwas anderes würde nur gelten, wenn die weitere Speicherung erforderlich und dies entsprechend dokumentiert wäre (§ 38 Absatz 5 Satz 4 PolG), was hier allerdings nicht der Fall war. Auch aus dem Bundeskriminalamtgesetz (BKAG) kann hier keine (weitere) Speicherberechtigung hergeleitet werden, etwa durch Anwendung des §77 Absatz 3 Satz 1 BKAG. Denn der Bund ist nicht berechtigt, auf Länderdateien bezogene landesgesetzliche Speicherfristen durch abweichendes Bundesgesetz auszuhebeln. § 77 BKAG gilt ausschließlich für Speicherungen im polizeilichen Informationsverbund INPOL. Diese Speicherungen sind akzessorisch zu den Speicherungen im Landesbestand. Speicherungen, die im Landesbestand nach Landesrecht zu löschen sind, sind demgemäß auch im Bundesbestand zu löschen (§ 29 Absatz 5 Satz 1, § 31 Absatz 2 Satz 1 BKAG). Der „Mitzieheffekt" des § 77 Absatz 3 Satz 1 BKAG bedeutet nicht, dass nach Landesrecht zu löschender Landesbestand allein deshalb weiterzuführen wäre, weil die Polizei eines anderen Verbundteilnehmers nach jeweils eigenem Recht zur Speicherung berechtigt wäre. Wobei, auch darauf muss hingewiesen werden, die Polizei in diesen Fällen nicht in der Lage ist, die Speicherungen durch Polizeidienststellen anderer Länder oder des Bundes auf ihre

Rechtmäßigkeit zu prüfen. Um es deutlich zu sagen: Es kann nicht sein, dass die Polizei Bürgerinnen und Bürger allein im blinden Vertrauen darauf speichert, dass Polizeibehörden anderer Länder schon alles richtig gemacht haben werden, obwohl die eigenen rechtlichen Grundlagen eine Speicherung verbieten.

Vor diesem Hintergrund baten wir das Landeskriminalamt, die Daten aus dem Bundesbestand zu löschen, und die betroffenen Dienststellen, ihrerseits den Landesbestand zu bereinigen.

Beim Landeskriminalamt führte dies dann tatsächlich zum Umdenken. Das Amt löschte die Daten, für die es originär zuständig war, umgehend aus dem Auskunftssystem. Für die Daten aber, für die es keine Verantwortung trug, waren ihm allerdings die Hände gebunden. Hier waren die örtlichen Polizeidienststellen am Zug. Das klappte nicht in jedem Fall ganz reibungslos. Insbesondere ein Polizeipräsidium teilte erst nach Wochen auf telefonische Nachfrage mit, dass unsere Rechtsauffassung wohl zutreffe, man wolle sich aber erst noch an höherer Stelle rückversichern. Unabhängig davon werde man aber die Speicherungen zur Petentin in POLAS löschen. Das ist mittlerweile auch geschehen. Endlich!

2.3 Datenschutz bei der Waffenbehörde

Man sollte meinen, dass das Thema Datenschutz mittlerweile auch in der kleinsten Behörde angekommen ist. Deshalb erstaunt es immer wieder, wenn man durch Beschwerden feststellen muss, dass die Bedeutung dieser grundrechtlichen Gewährleistung doch noch nicht in allen Köpfen angekommen zu sein scheint. Als Beispiel dafür mag folgender Fall herhalten:

Ein Petent wandte sich an uns, weil er nicht damit einverstanden war, dass die Waffenbehörde eines Landratsamts Daten über seinen Gesundheitszustand bei seinem Arbeitgeber abgerufen hatte. Dem lag zugrunde, dass der Arbeitgeber des Petenten, ein Bewachungsunternehmen, bei der Waffenbehörde um Zustimmung ersucht hatte, dem Petenten eine Waffe zu überlassen. Geregelt ist dies in § 28 Absatz 3 des Waffengesetzes (WaffG). Die Waffenbehörde muss hierbei prüfen, ob die Person, der die Waffe überlassen werden soll, die erforderliche Zuverlässigkeit besitzt und auch persönlich geeignet ist. Bestehen Bedenken hinsichtlich der persönlichen Eignung, etwa wegen physischer oder psychischer Einschränkungen, muss die Behörde dem nachgehen.

Hier war es so, dass der Arbeitgeber schon bei der Antragstellung darauf hingewiesen hatte, dass der Petent in den zurückliegenden Jahren über längere Zeiträume arbeitsunfähig krank gewesen sei und dass dem möglicherweise psychische Probleme zugrunde gelegen hätten. Er sei jedenfalls in entsprechenden Fachkliniken behandelt worden. Aufgrund dieser Informationen sah sich die Behörde zu Recht verpflichtet, der Sache auf den Grund zu gehen. Anstatt sich allerdings mit weiteren Nachfragen zunächst an den Betroffenen selbst zu wenden, wozu sie rechtlich verpflichtet gewesen wäre, wandte sie sich an den Arbeitgeber und bat diesen um eine Aufstellung der Fachrichtung der Ärzte, welche die Arbeitsunfähigkeitsbescheinigungen des Betroffenen erteilt hatten. Diese erhielt sie dann auch postwendend.

Nachdem wir die Behörde zunächst darauf hingewiesen hatten, dass nach § 13 Absatz 2 des Landesdatenschutzgesetzes (LDSG) in seiner damals geltenden Fassung zunächst der Betroffene selbst hätte gefragt werden müssen, bevor man Erkundigungen über ihn bei Dritten hätte einholen dürfen (sog. Direkterhebungsgrundsatz), entspann sich ein lebhafter Schriftwechsel. Zunächst sah man keine schutzwürdigen Interessen des Betroffenen, die gegen eine Datenerhebung bei Dritten gesprochen hätten. Zudem wurde behauptet, die zu erfüllende Aufgabe habe „ihrer Art nach" eine Datenerhebung bei Dritten erforder-

lich gemacht. Auf unsere Frage, worin den diese „Art" bestehe, ob eine Interessenabwägung stattgefunden habe und was überhaupt dagegen gesprochen hätte, den Betroffenen zunächst selbst zu befragen, wurde zunächst die Bedeutung der erhobenen Daten (Gesundheitsdaten!) bagatellisiert. Weiter wurde behauptet, man habe ja beim Arbeitgeber nur nachgehakt, um feststellen zu können, ob die persönliche Eignung des Petenten überhaupt in Frage zu stellen wäre. Merkwürdig, denn die bereits vorliegenden Informationen hatten gerade schon solche Bedenken hervorgerufen, sie waren schließlich Grund für die erneute Datenerhebung. Auf unser erneutes Schreiben, in dem wir auf diesen Widerspruch hinwiesen und erneut aufforderten zu begründen, weshalb im konkreten Fall die Datenerhebung beim Arbeitgeber „ihrer Art nach" geboten gewesen sei, wurde es interessant. Ausführlich wurde uns nämlich zunächst dargelegt, wie wichtig es sei, nur Personen eine Waffe in die Hand zu geben, bei der sichergestellt sei, dass sie kein Risiko für die Allgemeinheit darstellen; das hatten wir mit keinem Wort in Frage gestellt. Sodann wurde wir über die weitere Praxis der Behörde wie folgt informiert: „Sofern Sie weiterhin Zweifel an der datenschutzkonformen Erhebung der Daten haben, wird die Sachbearbeiterin … insbesondere vor dem Hintergrund des Amoklaufs in … eine datenschutzrechtliche Rüge akzeptieren." Mit anderen Worten, es wurde zum Ausdruck gebracht, dass man sich auch künftig aus vermeintlich übergeordneten Gründen nicht an datenschutzrechtliche Vorschriften zu halten gedenke! Dass wir das nicht akzeptieren konnten, liegt auf der Hand.

In einem Schreiben an den Landrat stellten wir den Vorgang nochmals dar und brachten zum Ausdruck, dass wir die Behandlung der Angelegenheit durch die Behörde in der Sache für falsch und im Ton unserer Behörde gegenüber für inakzeptabel hielten. Hier komme ein Fehlen jeglichen Verständnisses für den Datenschutz zum Ausdruck. In seiner Antwort teilte uns der Landrat mit, er teile unsere Rechtsauffassung und habe die betroffenen Mitarbeiter angewiesen, den Datenschutz künftig zu beachten. Das ist auch zwingend geboten.

Den Bürger in seinen Rechten ernst zu nehmen heißt auch, ihn grundsätzlich dann einzubeziehen, wenn es um seine Daten geht. Eine Verarbeitung seiner Daten nach Treu und Glauben und in einer für ihn nachvollziehbaren Weise (so einer der Grundsätze für die Verarbeitung personenbezogener Daten nach Artikel 5 der Datenschutz-Grundverordnung) verpflichtet dazu, sich insbesondere bei der Erhebung seiner Daten vorrangig an ihn zu wenden, es sei denn, ein Gesetz berechtigt oder verpflichtet zu etwas Anderem oder es liegt ein zwingender Grund dafür vor, von diesem Grundsatz abzuweichen. Eine gewisse Sensibilität im Umgang mit Bürgerrechten sollte auch in sicherheitsempfindlichen Bereichen selbstverständlich sein.

2.4 Datenschutz und Bauleitplanung

Das Verfahren zum Erlass von Bauleitplänen ist aufwändig und kompliziert. Kein Wunder, dass Kommunen peinlich darauf bedacht sind, jeden erdenklichen Verfahrensfehler auszuschließen, der letztlich das Projekt zum Scheitern bringen könnte. Dem lag auch die verständliche und lobenswerte Absicht einer Stadt zugrunde, um deren Fall es im Folgenden ging:

Eine Stadt beabsichtigte, ein Gewerbegebiet zu entwickeln. Zu diesem Zweck leitete sie ein Bebauungsplanverfahren ein. Im Rahmen der Öffentlichkeitsbeteiligung äußerten sich zahlreiche Bürger zu dem Vorhaben. Mit den Planunterlagen stellte die Stadt diese Stellungnahmen dann einschließlich Namen und Adressen, teilweise sogar mit E-Mail-Adresse, auf ihre Homepage ins Internet. Einzelne Betroffene beschwerten sich daraufhin bei uns und meinten, die Stellungnahmen hätten zumindest auch ohne die Identifikationsdaten veröffentlicht werden können. Das sahen wir auch so.

Schriftlich wandten wir uns an die Stadt und legten unsere Rechtsauffassung dar, wonach eine personenbezogene Veröffentlichung der Stellungnahmen datenschutzrechtlich unzulässig sei. Wir begründeten dies wie folgt:

„Zweifelsfrei stellt die Veröffentlichung personenbezogener Daten durch die Stadt Weinheim eine Verarbeitung im Sinne des Artikels 4 Nummer 2 der Datenschutz-Grundverordnung (DS-GVO) dar. Sie wäre nur zulässig, wenn es hierfür eine eindeutige Rechtsgrundlage gäbe. Eine solche müsste gemäß Artikel 6 Absatz 1 Satz 1 Buchstabe c und e DS-GVO Bundes- oder Landesrecht entnommen werden können. Naheliegend wäre hier, eine solche Rechtsgrundlage im Baugesetzbuch (BauGB) zu finden. Dies ist indes nicht der Fall. Der aus unserer Sicht allein in Betracht kommende § 3 BauGB sieht jedenfalls keine solche namensbezogene Veröffentlichungsbefugnis privater Stellungnahmen vor, wie dies etwa in § 73 Absatz 1 des Landesverwaltungsverfahrensgesetzes geregelt ist. Diesbezüglich weisen wir auch auf die Rechtsprechung des Bundesverfassungsgerichts hin (Kammerbeschluss vom 24. Juli 1990 – 1 BvR 1244/87 –, juris; ebenso: VG Neustadt (Weinstraße), Urteil vom 16. November 2015 – 4 K 1000/14.NW –, juris), wonach die Wiedergabe persönlicher Daten der Einwender gegen das Recht auf informationelle Selbstbestimmung verstößt (BVerfG: „Bei der Entscheidung darüber, ob und in welchem Umfang personenbezogene und nichtanonymisierte Daten der Beschwerdeführer in den Planfeststellungsbeschluss … aufzunehmen und mit diesem öffentlich zu verbreiten waren, musste deshalb dem Gehalt, der Bedeutung und der Tragweite des Rechts auf informationelle Selbstbestimmung Rechnung getragen werden. … Bei einer solchen Bekanntmachung, die die intensivste Form einer Übermittlung personenbezogener Daten darstellt, handelt es sich datenschutzrechtlich um eine Datenübermittlung „auf Vorrat“."). Für den Bereich der Bauleitplanung gilt dies entsprechend."

Die Stadt hielt dem entgegen, Datenschutz habe gegenüber den – auch europarechtlich vorgegebenen – Transparenzerfordernissen in der Bauleitplanung zurückzutreten. Die der Öffentlichkeit zur Verfügung gestellten Unterlagen müssten eine umfängliche inhaltliche Auseinandersetzung und Würdigung der Stellungnahmen zulassen. Insbesondere dürfe eine Anonymisierung nicht zur Qualitätsminderung vorliegender Umweltinformationen führen, weil lediglich erkennbar sei, was geäußert wurde, aber nicht durch wen und mit welchem räumlichen Bezug. Es müsse vermieden werden, dass eine „überschießende Beachtung des Datenschutzes" zu Verfahrensfehlern führe.

Abgesehen davon, dass eine umfängliche inhaltliche Auseinandersetzung und Würdigung der Stellungnahmen ausschließlich Sache des Trägers der Bauleitplanung ist, überzeugt die Auffassung der Stadt jedenfalls nicht, soweit es um Stellungnahmen von Privatpersonen geht. Nach der Argumentation der Stadt müsste der Öffentlichkeit Gelegenheit gegeben werden, private Stellungnahmen zu kommentieren. Aus § 3 Absatz 2 BauGB lässt sich das kaum herauslesen. Zudem reicht es für das von § 3 Absatz 2 BauGB bezweckte Bewirken eines Anstoßes aus, wenn diejenigen Umweltinformationen, die in den verfügbaren Stellungnahmen behandelt werden, schlagwortartig so zusammengefasst und charakterisiert werden, dass interessierten Bürgern eine umfassende Information darüber gegeben wird, welche Umweltauswirkungen die Realisierung des aufgelegten Bebauungsplans haben kann (OVG Berlin-Brandenburg, Urteil vom 13. April 2016 – OVG 10 A 9.13 –, juris).

Da der gegenständliche Fall ein Problem betrifft, das von allgemeinem Interesse ist, haben wir das Wirtschaftsministerium Baden-Württemberg als oberste Baurechtsbehörde des Landes um seine Meinung ersucht. Im Ergebnis wurde unsere Rechtsauffassung vollumfänglich bestätigt. Auch das Wirtschaftsministerium sieht die Gemeinden weder verpflichtet noch be-

rechtigt, die Stellungnahmen von Bürgerinnen und Bürgern namensbezogen und mit Adresse oder gar weiterer persönlicher Daten im Internet einzustellen. Es sei insbesondere nicht ersichtlich, inwiefern die personenbezogene Veröffentlichung der Stellungnahmen die Qualität des Abwägungsergebnisses vermindern könnte.

Mit diesem Ergebnis haben wir uns erneut an die Stadt gewandt und sie aufgefordert, künftig auf die personenbezogene Veröffentlichung von Stellungnahmen privater Personen im Rahmen eines Bauleitplanverfahrens abzusehen.

Auch in Planungsverfahren ist der Datenschutz zu beachten. Planungsrechtliche Vorschriften stehen grundsätzlich nicht über den Schutzvorschriften der Datenschutz-Grundverordnung. Der Geltungsvorrang des europäischen Rechts entfällt allenfalls dann, wenn aufgrund entsprechender Öffnungsklauseln europarechts- und verfassungskonform Abweichendes geregelt ist. Das Baugesetzbuch enthält für das Bauleitplanverfahren keine diesbezüglichen ausdrücklichen Regelungen.

2.5 Online-Prüfung von baden-württembergischen Behörden-Websites

Lediglich 19 % der Behörden-Websites in Baden-Württemberg sind über das gesicherte HTTPS-Protokoll abrufbar, wie eine großflächig durchgeführte Online-Prüfung des LfDI BW ergeben hat. Zumindest an einigen Stellen sind aber auch positive Entwicklungen zu verzeichnen.

Im letzten Tätigkeitsbericht (2016/2017) haben wir über unsere Online-Prüfung von baden-württembergischen Unternehmens-Websites berichtet: lediglich 15 % der Unternehmens-Websites waren 2017 per HTTPS gesichert, wie wir festgestellt hatten (2016 waren es lediglich 5 %). Bis Anfang 2018 ist dieser Wert nun immerhin auf 22 % gestiegen. In der Zwischenzeit haben wir auch die baden-württembergischen Behörden-Websites in unsere Online-Prüfung aufgenommen – hierauf wollen wir in diesem Beitrag näher eingehen.

Zur Wahrung der Sicherheit der Datenverarbeitung fordert Artikel 32 DS-GVO:

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

Das HTTP Secure (HTTPS)-Protokoll stellt die Standard-Maßnahme dar, um Sicherheit (insbesondere Vertraulichkeit, Authentizität und Integrität) der Kommunikation im Web zu gewährleisten und ist damit eine geeignete technische Maßnahme im Sinne von Artikel 32 DS-GVO.

In unserer aktuellen Online-Prüfung haben wir untersucht, inwieweit die Websites von Behörden in Baden-Württemberg über HTTPS gesichert sind. Da gerade die Websites von Städten und Gemeinden für viele Bürger die erste Anlaufstelle für (zurzeit immer noch recht einfache) E-Government-Anwendungen darstellen, haben wir den Fokus auf diese Websites gelegt.

Zum Ergebnis

Von den untersuchten 1.754 Behörden-Websites wurden Anfang 2017 13 % über eine HTTPS-Verbindung angeboten. Bis Anfang 2018 hat sich dieser Wert auf 19 % erhöht. Die folgende Tabelle zeigt die Werte heruntergebrochen auf die unterschiedlichen Behörden.

Behörde	Anzahl Websites	HTTPS (2017)	HTTPS (2018)
Hochbauamt	25	4 %	8 %
Notariat	317	0 %	0 %
Landratsamt	35	31 %	43 %
Ministerium	11	64 %	64 %
Stadt/ Gemeinde	1.054	11 %	28 %
Amtsgericht	108	0 %	0 %
Arbeitsgericht	17	0 %	0 %
Finanzamt	82	0 %	0 %

In der Tabelle können wir einen deutlichen Anstieg an per HTTPS angebotenen Websites von Städten und Gemeinden erkennen. Wenn wir die Ergebnisse bei den Websites von Städten und Gemeinden jedoch im Detail betrachten, so lässt sich feststellen, dass der Einsatz von HTTPS sehr stark mit der Einwohnerzahl einer Gemeinde/Stadt korreliert. Von den 743 Websites von Gemeinden sind lediglich 20 % per HTTPS gesichert; von den 311 Websites von Städten sind es hingegen 43 %. Die folgende Tabelle schlüsselt die Ergebnisse weiter auf.

Einwohnerzahl	Anzahl Websites	HTTPS (2018)	Bevölk.
< 2.000	187	9 %	222.073
2.000 – 5.000	403	21 %	1.356.508
5.000 – 20.000	412	34 %	3.819.913
20.000 – 50.000	78	53 %	2.406.106
50.000 – 100.000	13	62 %	902.132
100.000 – 500.000	8	100 %	1.459.920
> 500.000	1	100 %	615.862

Es ist deutlich erkennbar, dass, je größer eine Gemeinde/Stadt ist, desto eher wird die Website dieser Gemeinde/Stadt per HTTPS angeboten. In einem Flächenland wie Baden-Württemberg, in dem sehr viele Menschen auch in kleineren Gemeinden und Städten leben, sind demnach auch sehr viele Bürger von nicht gesicherten Websites ihrer Gemeinden und Städte betroffen. Darüber gibt die 4. Spalte Auskunft. In Gemeinden mit unter 20.000 Einwohnern leben immerhin 5.398.494 Menschen; dabei sind unter 50 % der Websites über HTTPS gesichert. Im Gegensatz dazu sind mehr als 50 % der Websites von Städten mit mehr als 20.000 Einwohnern über HTTPS gesichert. Davon profitieren insgesamt 5.384.020 Einwohner (und damit weniger Menschen als von nicht-gesicherten Websites Betroffenen in kleineren Gemeinden und Städten).

Die in der Online-Prüfung gewonnene Erkenntnis, dass das Datenschutzniveau (zumindest in Bezug auf den Einsatz von HTTPS) auf Websites mit der Größe einer Gemeinde/Stadt (in Bezug auf die Einwohnerzahl) korreliert, bestätigt unsere Beobachtung, dass kleinere Gemeinden eher weniger Ressourcen für den Datenschutz aufwenden (können). Im Hinblick auf den Einsatz von HTTPS gilt aber zumindest der Kostenaspekt nicht als Ausrede. Die nötigen TLS-Zertifikate sind dank der Initiative „Let's Encrypt" inzwischen kostenfrei erhältlich. Lediglich 10 Städte und 14 Gemeinden nutzen allerdings bisher von Let's Encrypt ausgestellte Zertifikate. Im Vergleich dazu sind von Let's Encrypt ausgestellte Zertifikate bei Unternehmen im Ländle beliebter und weitaus häufiger im Einsatz, nämlich inzwischen bei 30 % der über HTTPS-gesicherten Websites von Unternehmen.

Nicht alle (untersuchten) Behörden-Websites erheben personenbezogene Daten von Nutzern. Streng genommen müssten diese Websites nicht über HTTPS angeboten werden. Allerdings lassen unter Umständen auch diese Websites Rückschlüsse auf deren Besucher zu, etwa für welche Sozialleistungen sich ein Bürger interessiert. Außerdem sind ungesicherte Websites anfällig für Manipulationen durch Angreifer. Aus diesem Grund ist eine möglichst flächendeckende Nutzung von HTTPS aus Datenschutz- und IT-Sicherheitssicht wünschenswert. Der LfDI BW wird weiterhin dafür eintreten, dass sich der Anteil an HTTPS-gesicherten Unternehmens- und Behörden-Websites im Ländle weiter verbessert.

Wie bereits im letzten Tätigkeitsbericht erwähnt, empfehlen wir allen Website-Betreibern in Baden-Württemberg, ihre Website über eine gesicherte HTTPS-Verbindung bereitzustellen. Der LfDI BW wird weiterhin Website-Betreiber, die über ihre Website personenbezogene Daten erheben, auf die Einhaltung der Nutzung von HTTPS (mit aktueller TLS-Version und als sicher geltender Cipher Suite) hin überprüfen und auffordern – falls nötig werden wir im Unternehmensbereich hier auch Bußgelder verhängen.

Die Ergebnisse der aktuellen Prüfung wurden erstmals unter dem Titel „HTTPS im Lichte der DSGVO" in der Zeitschrift Datenschutz und Datensicherheit (Ausgabe 11/2018) publiziert. In dem Beitrag wird noch detaillierter auf technische Aspekte der Prüfung und der Ergebnisse eingegangen.

3. Videoüberwachung

3.1 BGH Urteil zu Dashcams – Datenschutz durch Technikgestaltung

Dashcams sind kleine Videokameras, die in einem Auto befestigt werden und aus der Perspektive des Fahrers das Verkehrsgeschehen aufzeichnen. Im Regelfall sollen sie den Hergang von Unfällen und andere Ereignisse im Straßenverkehr zum späteren Nachweis festhalten.

Im Mai 2018 urteilte der Bundesgerichtshof (BGH, Urteil vom 15. Mai 2018 – VI ZR 233/17), dass die permanente und anlasslose Aufzeichnung des Verkehrsgeschehens mit den datenschutzrechtlichen Regelungen des Bundesdatenschutzgesetzes nicht vereinbar ist. Nach einer Güterabwägung im Einzelfall erkannte das Gericht Dashcam-Aufzeichnungen aber als zulässiges und verwertbares Beweismittel im Unfallhaftpflichtprozess an. Der Entscheidung lag ein Sachverhalt zugrunde, bei dem eine Kamera im Fahrzeug des Klägers den öffentlichen Raum regelmäßig über einen Zeitraum von ca. vier Stunden ohne konkreten Anlass filmte. Mit den Aufnahmen sollten für den Fall eines Verkehrsunfalls Beweismittel gesichert werden.

An mehreren Stellen betont der BGH, dass der Betreiber einer Dashcam technische Möglichkeiten nutzen müsse, um eine dauerhafte Aufzeichnung der Bilder zu vermeiden. Lediglich die kurzzeitige anlassbezogene Speicherung im Zusammenhang mit einem Unfallgeschehen soll zulässig sein. Eine Güterabwägung zugunsten des Dashcambetreibers komme überhaupt nur in Betracht, wenn eine Dashcam bestimmte (Daten-)Schutzmechanismen aufweise. Die Risiken für Persönlichkeitsrechte Dritter seien demnach durch Datenminimierung (Artikel 5 Absatz 1 Buchstabe c DS-GVO) und durch Technikgestaltung (Art. 25 DS-GVO – Privacy by Design) zu minimieren. Der Eingriff in das informationelle Selbstbestimmungsrecht der Verkehrsteilnehmer solle durch kurzzeitige, anlassbezogene Aufzeichnungen begrenzt werden, die erst bei Kollision oder starker Verzögerung des Fahrzeugs durch einen Bewegungssensor ausgelöst werden, ggf. durch Verpixelung der Personen, automatisiertes und dem Eingriff des Verwenders entzogenes Löschen. Als zentrale Voraussetzungen einer datenschutzrechtlichen Zulässigkeit von Dashcam-Aufnahmen sieht der BGH eine Verkürzung der Aufzeichnungsdauer und eine Verknüpfung der Speicherung mit einem konkreten Aufzeichnungsanlass.

Entsprechend ist mit einem angepassten technischen System, das eine automatische periodische Löschung beinhaltet, ein datenschutzkonformer Dashcam-Einsatz grundsätzlich möglich (siehe bereits Pressemitteilung des LfDI Baden-Württemberg vom 10. Oktober 2017). Nach den nunmehr geltenden Vorschriften der Datenschutz-Grundverordnung und des neuen Bundesdatenschutzgesetzes ergibt sich hier keine andere Bewertung. Wesentlich ist dabei, dass die aufgezeichneten Daten stets unmittelbar überschrieben werden. Im Falle einer Kollision oder starken Verzögerung des Fahrzeugs kann durch Unfallsensoren aber eine anlassbezogene Sicherung des letzten Aufzeichnungsintervalls ausgelöst werden. Für die Dokumentation von Nötigungen oder Ähnlichem, nicht unfallbezogenen Verhalten, ist auch das manuelle Starten des Aufnahmevorgangs denkbar.

3.2 Ungesicherte Netzwerkkameras – Das Tor zur Welt

Fühlen Sie sich beobachtet, wenn sie die Parklücke vor ihrem Haus auch nach dem achten Anlauf nicht richtig ansteuern? Wenn Sie tänzelnd und beschwingt Ihre Auffahrt kehren? Oder wenn Sie nur im Bademantel bekleidet den Müll in die Tonne vor ihrem Haus werfen? Vielleicht

sind Sie – ohne es zu Wissen – am anderen Ende der Welt schon längst eine Internetberühmtheit? Betreibt Ihr Nachbar eine Netzwerkkamera an seiner Haustür oder an seinem Gebäude und nimmt er es dabei mit dem Datenschutz und der Datensicherheit nicht so genau, steigen Ihre Chancen auf unfreiwilligen internationalen Ruhm ganz erheblich.

Netzwerkkameras oder IP-Kameras können kabellos mit einem Netzwerk verbunden und dadurch beliebig in Funkreichweite installiert werden. Im Gegensatz zu früheren Kameras bestehen sie aus einem Rechner, der digitale Videobilder und Tonspuren unmittelbar als Web- und Streamingserver ausgeben und die Aufnahmen selbst speichern kann. Ist das Gerät über das Internet erreichbar, kann mittels Browser über die kameraeigene Software auf das Kamerabild und den Speicher des Geräts zugegriffen werden – natürlich weltweit per Smartphone oder Tablet. Die kabellosen Systeme sind bequem und einfach einzurichten, günstig in der Anschaffung und entsprechend weit verbreitet. Dabei legen die Hersteller selten Wert auf eine sichere Software, weshalb die Geräte oft erhebliche Risiken bergen. Verpasst man ein wichtiges Update oder wird der Support für das Gerät eingestellt, können Kameras die über das Internet erreichbar sind, leicht angegriffen und kompromittiert werden. Gerade IP-Kameras sind häufig Ziel massenhaft verbreiteter Schadsoftware. Verliert man erst einmal die Kontrolle über seine Kamera, können Fremde unbeschränkt auf die Kamerafunktionen und -bilder zugreifen, diese vervielfältigen und verbreiten, die Kamera steuern oder das Gerät für eigene kriminelle Zwecke als Teil eines sogenannten Botnetzes (beispielsweise „Mirai" oder „Persirai") missbrauchen. Neben Sicherheitslücken in der Software ist mangelnder Passwortschutz ein Hauptrisiko. Ist ein voreingestelltes Passwort nicht abgeändert oder wird ein unsicheres Standard-Passwort verwendet, sind IP-Kameras besonders leicht zu übernehmen und ein attraktives Ziel für automatisierte Angriffe aus dem Internet.

Im vergangenen Jahr mussten wir mehrere Betreiber von Netzwerkkameras darauf hinweisen, dass sie ihre Kameras datenschutzwidrig betreiben. Ein Passwortschutz war für die Weboberfläche der IP-Kameras erst gar nicht eingerichtet, weshalb die Kamerabilder über das Internet frei erreichbar und damit weltweit abrufbar waren. Auch den Zugriff auf Kamerafunktionen und Kameraspeicher hatten die Betreiber nicht beschränkt. Im Live-Stream übertrugen die Kameras zum Teil weiträumig den öffentlichen Straßenraum und erfassten die Nachbargebäude im jeweiligen Wohngebiet. In einem Fall setzte der Betreiber eine sogenannte digitale Türkamera ein, die ein Live-Überwachungsbild der unmittelbaren Nachbarschaft zeigte und darüber hinaus Bilder aller klingelnden Gäste über mehrere Jahre archivierte. Hierbei handelte es sich nicht nur um Freunde und Verwandte, sondern auch um Postboten, Lieferanten und Handwerker. Die smarte Türkamera verfügte außerdem über die Funktion „Open-Door". Ob diese tatsächlich mit dem Türöffner verbunden war, hat (zumindest) die Aufsichtsbehörde nicht überprüft. Der Betreiber wurde über die Sicherheitslücke informiert. Die Einleitung eines Bußgeldverfahrens war in diesem Fall nicht zu vermeiden, da über einen langen Zeitraum eine nach Art und Umfang erhebliche Überwachung des öffentlichen Raumes vorlag.

Der Einsatz einer digitalen Tür- oder Klingelkamera ist unter bestimmten Voraussetzungen durchaus zulässig. Eine dauerhafte und anlasslose Bildübertragung öffentlich-zugänglicher Bereiche muss aber in jedem Fall ausgeschlossen sein. Eine anlasslose Aufzeichnung der Audiospur kann sogar eine Straftat darstellen (vgl. § 201 des Strafgesetzbuchs). In öffentlich zugänglichen Bereichen kann eine Klingelkamera eingesetzt werden, wenn eine Bildübertragung nach Betätigung der Klingel, d. h. anlassbezogen erfolgt, eine dauerhafte Speicherung der Aufnahmen ausgeschlossen ist, das System nicht mehr abbildet als ein Blick durch den Türspion gewähren würde und die Übertragung

nach einigen Sekunden automatisch unterbrochen wird. (Sicherheits-)Kameras, die manuell oder durch Bewegung aktiviert werden und ein Pre-Recording einsetzen, erfüllen diese Voraussetzungen nicht. Ein duales System, das in Wohnbereichen gleichzeitig als Überwachungs- und Klingelkamera genutzt wird und dabei den öffentlichen Raum filmt, kann die rechtlichen Anforderungen an eine Videoüberwachung öffentlich zugänglicher Räume in der Regel nicht erfüllen.

Beim Betrieb von Netzwerk- oder IP-Kameras ist besonders darauf zu achten, dass diese datenschutzkonform konfiguriert und ausgerichtet sind. Sicherheitshinweise der Hersteller sollten unbedingt beachtet, die Software regelmäßig aktualisiert und ein sicheres Zugangspasswort vergeben werden.

3.3 Von wegen „I'm dancing on my own" – Videoüberwachung in Tanzschulen

Wie schon in den letzten Jahren, richtete sich ein Großteil der Beschwerden im Bereich „Freizeit" wieder gegen die Videoüberwachung in Schwimmbädern und Fitnessstudios. Im Berichtszeitraum 2018 stach zudem allerdings eine ganz neue Zielgruppe heraus – die Tanzschulen.

Aufgrund einer Beschwerde wurden wir auf eine Tanzschule aufmerksam, die neben dem Ein- bzw. Ausgangsbereich sämtliche öffentlich zugänglichen Räumlichkeiten, d. h. die Garderoben, den Gastrobereich, die Flure, Spinde und vor allem die Tanzsäle videoüberwachte. Zur Begründung wurde angeführt, dass es insbesondere in den Garderoben und im Gastrobereich regelmäßig zu Diebstählen und Sachbeschädigungen komme und im Übrigen alle Tanzschulen „das so machen würden". Das mit dem „so machen" wollten wir schließlich genauer wissen und haben verschiedene Tanzschulen in Baden-Württemberg stichprobenartig aufgesucht und überprüft. Um das Ergebnis vorweg zu nehmen: Das mit dem „so machen" hat sich leider überwiegend bestätigt! Dies bedeutet aber nicht, dass die Videoüberwachung auch rechtmäßig ist: Grundsätzlich handelt es sich bei Tanzschulen um öffentlich zugänglichen Räumlichkeiten. Datenschutzrechtlich beurteilt sich die Videoüberwachung somit nach § 6b des Bundesdatenschutzgesetzes in seiner alten Fassung bzw. seit dem 25. Mai dieses Jahres nach Art. 6 Absatz 1 Satz 1 Buchstabe f der Datenschutz-Grundverordnung (DS-GVO) in Verbindung mit § 4 des Bundesdatenschutzgesetzes. Danach ist die Videoüberwachung nur zulässig, soweit sie zur Aufgabenerfüllung öffentlicher Stellen (1), zur Wahrnehmung des Hausrechts (2) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (3) erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Wenn es sich bei den überwachten Räumen gleichzeitig um Arbeitsplätze von Beschäftigten handelt, sind zudem deren schutzwürdige Interessen in besonderer Weise zu berücksichtigen. Dies gilt vor allem dann, wenn sie sich im Rahmen ihrer Arbeitstätigkeit in den überwachten Bereichen dauerhaft aufhalten und der Überwachung mithin nicht entgehen können.

a) Überwachung der Eingangsbereiche

Bei unseren Kontrollen mussten wir feststellen, dass fast alle überprüften Tanzschulen ihre Eingangsbereiche videoüberwachen. Dies ist oftmals durch die Lage der Tanzschulen bedingt, die sich beispielsweise auf mehrere Etagen erstrecken und sich daher die Eingangsbereiche auf anderen Stockwerken befinden als die restlichen Räumlichkeiten. Die mittels der Kameras durchgeführte Zugangskontrolle dient der Durchsetzung des Hausrechts und ist grundsätzlich ein zulässiger Zweck bzw. stellt ein berechtigtes Interesse der Kamera- bzw. Tanzschulbetreiber dar.

In aller Regel wird aber ein Monitoring (d. h. eine Übertragung der Kameradaten auf einen Monitor ohne zusätzliche Aufzeichnung der Daten) zur Zweckerreichung ausreichen. Dies ermöglicht ein unmittelbares Einschreiten, wenn beispielsweise eine unberechtigte Person das Gebäude betritt. Eine zusätzliche Speicherung der Kameraaufnahmen ist zur unmittelbaren Umsetzung des Hausrechts nicht erforderlich bzw. überwiegen in diesen Fällen die schutzwürdigen Interessen der Tanzschulgäste, beim Besuch einer Freizeiteinrichtung nicht anlasslos einer Datenspeicherung ausgesetzt zu werden. Bei der Ausrichtung der Kamera ist insbesondere darauf zu achten, dass nur das eigene Grundstück bzw. der eigene Hauseingang überwacht wird und sich die Kameraüberwachung nicht auf Nachbargebäude/-grundstücke oder gar den öffentlichen Verkehrsraum erstreckt. Sind im Gebäude zugleich andere Eigentümer/Mieter untergebracht, wird in der Regel sogar ein Monitoring ausscheiden. Hier bleibt letztlich dann nur der Rückgriff auf eine sogenannte Klingelkamera, bei der nur für einen kurzen Zeitraum die Aufnahme der Person, die das Gebäude betreten möchte, übertragen wird. Sinn und Zweck ist es dabei, die Kamera mit einer Schließanlage zu verbinden und somit nur berechtigten Personen Zugang zum Gebäude zu verschaffen.

b) Überwachung der Garderoben/ Spinde

Zweck der Videoüberwachung dieser Bereiche ist in aller Regel die Verhinderung und Aufklärung von Diebstählen zu Lasten der Gäste der Tanzschulen. Grundsätzlich sehen wir auch den Schutz vor Diebstählen zu Lasten Dritter (d. h. der Tanzschüler/Kunden) als ein berechtigtes Interesse (Drittinteresse) an, welches vom Betreiber einer Videoüberwachungsanlage verfolgt werden kann. Rechtlich noch nicht geklärt ist dabei allerdings, ob es sich bei diesem Zweck um ein unmittelbares Drittinteresse handelt, da Art. 4 Nr. 10 DS-GVO eigentlich vorsieht, dass ein Betroffener (und Tanzschüler/Kunden werden nun mal eben gerade von der Kamera erfasst und sind damit „Betroffene") nicht gleichzeitig Dritter sein kann. Damit fragt sich, ob letztlich ein mittelbares eigenes Interesse der Tanzschulbetreiber vorliegt. Gleichgültig ob Eigen- oder Drittinteresse – Diebstähle und Sachbeschädigungen sind in jedem Fall konkret nachzuweisen. Leider werden diese oft nur „behauptet" oder vorgetragen, ohne jedoch konkrete Beweise wie beispielsweise Mitteilungen an die Polizei, Strafanzeigen etc. vorlegen zu können.

Geht es also um die Verhinderung und Aufklärung von Straftaten wie Diebstähle oder Sachbeschädigungen, sind diese konkret nachzuweisen. Zwar kann in ganz bestimmten Einzelfällen auch einmal eine abstrakte Gefahrenlage bejaht werden, so dass dann keine konkreten Nachweise gefordert werden. Dies beschränkt sich aber auf spezielle Rechtsgüter/Objekte, bei denen aufgrund der allgemeinen Lebensanschauung davon auszugehen ist, dass diese häufig Ziel von Straftaten sind. Die Kamerabetreiber sind daher aufgefordert, Straftaten sorgfältig zu dokumentieren.

Wie bei jeder Videoüberwachung ist zudem zu prüfen, ob es nicht noch andere Maßnahmen gibt, die weniger tief in das Recht auf den Schutz personenbezogener Daten eingreifen – beispielsweise regelmäßige Kontrollen durch das Personal oder der Einbau abschließbarer Spinde. Selbstverständlich müssen sich diese Maßnahmen in den Tanzschulablauf integrieren lassen, um als gleich geeignet zu gelten.

Leider mussten wir immer wieder feststellen, dass – selbst wenn alle genannten Punkte erfüllt wurden – die Videoüberwachung zu exzessiv betrieben wurde. So wurden neben den Garderoben gleich noch die Eingänge zu den Umkleidebereichen oder am besten gleich der komplette Tanzsaal mit überwacht. Ein solch weitgehender Erfassungsbereich der Kameras ist schlichtweg nicht erforderlich, um Straftaten wie Diebstähle von Jacken oder Taschen aus den Garderoben zu dokumentieren. Der

Erfassungsbereich ist daher unmittelbar auf die Garderoben zu beschränken. Damit haben in aller Regel auch die Tanzschüler/Kunden, die nicht von einer Kamera gefilmt werden möchten, die Möglichkeit, der Kameraüberwachung zu entgehen.

Generell sollten Kamerabetreiber – auch bei einer zulässigen Videoüberwachung – Alternativangebote für Kunden und Gäste, die besonderen Wert auf Schutz ihrer personenbezogenen Daten legen, zur Verfügung stellen. Dies können beispielsweise Garderoben/Spinde sein, die bewusst von einer Überwachung ausgenommen werden. Die dadurch entstehende Wahlmöglichkeit für die betroffenen Kunden und Gäste führt letztlich zu einer positiveren Bewertung im Rahmen der Abwägung der schutzwürdigen Interessen.

c) Überwachung der Gastrobereiche

Viele Tanzschulen bieten neben dem klassischen Tanzunterricht auch Tanzveranstaltungen und sonstige Events an, so dass in vielen Schulen – entweder im Tanzsaal oder in den anderen Räumlichkeiten – Gastro- oder Barbereiche zu finden sind, wo Speisen und Getränke konsumiert werden können. Wie in normalen Gaststätten mussten wir auch in diesen Gastrobereichen eine starke Tendenz zum Einsatz von Videoüberwachungskameras feststellen. Zur Zulässigkeit von Videoüberwachungskameras in Gaststätten habe ich in meinem letzten Tätigkeitsbericht ausführlich Stellung genommen. Daher an dieser Stelle nur noch einmal grundlegend zur Erinnerung: Bereiche, die zum längeren Verweilen, Entspannen und Kommunizieren einladen – hierzu zählen gerade auch die Gastrobereiche in den Tanzschulen – dürfen regelmäßig nicht mit Videokameras überwacht werden. Hier überwiegt eindeutig das Recht auf Schutz der personenbezogenen Daten der Tanzschüler/Kunden, im Rahmen einer Freizeitaktivität nicht von Kameras beobachtet und dauerhaft aufgezeichnet zu werden.

Damit soll nicht gesagt werden Tanzschulbetreiber dürften sich nicht vor einem unzulässigen Griff in die Kasse im Bereich der Bar/Theke schützen oder müssen untätig zusehen, wie Gäste sich während der Abwesenheit des Personals hinter der Bar an den Getränken bedienen. Solche Taten – sofern konkret nachweisbar, d. h. dokumentiert – dürfen sehr wohl mittels Kamera verhindert bzw. aufgeklärt werden. Dazu muss aber nicht der komplette Gastrobereich überwacht werden. Vielmehr ist es ausreichend, die Kasse selbst oder aber den Bereich hinter der Bar per Kamera zu überwachen.

Bei einer eingeschränkten Videoüberwachung der Kasse oder des hinteren Bar-/Thekenbereichs dürfen die eigenen Mitarbeiter nicht vergessen werden. Diese haben ebenfalls ein Recht auf Schutz ihrer personenbezogenen Daten.

d) Überwachung der Tanzsäle

Wie bereits erwähnt, mussten wir bei vielen Tanzschulen eine Videoüberwachung der kompletten Tanzsäle feststellen. Auf die Frage, warum eigentlich sämtliche Tanzschüler bei ihren teilweise mehr oder weniger erfolgreichen Tanzkünsten beobachtet werden müssen, haben wir von keiner der überprüften Tanzschulen eine befriedigende Antwort erhalten. Teilweise wurde argumentiert, es fänden auch innerhalb der Tanzsäle Diebstähle und Sachbeschädigungen statt. Allerdings wurden diese nicht nachgewiesen. Auch die allgemeine Lebenserfahrung spricht dagegen, dass während der Öffnungszeiten eine überdurchschnittlich hohe Gefahr für das Eigentum des Tanzschulbetreibers besteht, befindet sich neben den (anderen) Tanzschülern/Kunden doch üblicherweise auch Personal in der Tanzsälen, das bei entsprechenden Vorfällen unmittelbar eingreifen kann. Letztlich mag auch das Argument, die Mitarbeiter wünschten eine Überwachung der Tanzsäle, um sich gegenüber unberechtigten Vorwürfen von Eltern, sie hätten junge Tanzschüler (Kinder) nicht ordnungsgemäß behandelt, nicht zu über-

zeugen. Gerade Kinder und Jugendliche sind besonders schutzwürdig und daher von jeder Videoüberwachung auszunehmen.

Eine Videoüberwachung der Tanzsäle während der Öffnungszeiten ist daher grundsätzlich unzulässig. Bei einer Teilnahme an Tanzkursen oder Tanzevents steht die freie Entfaltung der Persönlichkeit im Vordergrund. Der Freizeitbereich ist daher besonders schutzwürdig, so dass im Zweifel die schutzwürdigen Interessen der betroffenen Tanzschüler/Kunden überwiegen.

Vor Installation einer Videoüberwachungsanlage empfehlen wir daher die Lektüre der Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen" auf unserer Homepage. Gerne stehen auch die Mitarbeiter meiner Dienststelle mit Rat und Tat zur Seite.

4. Verkehr

4.1 Autonomes Fahren

Die hier ansässigen Automobilhersteller und auch die in Baden-Württemberg tätigen Zulieferbetriebe für die Automobilindustrie arbeiten fieberhaft an der Entwicklung des autonomen Fahrens. Autonomes Fahren verspricht mehr Reisekomfort, mehr Sicherheit im Verkehr, bessere Umweltverträglichkeit — sprich ein ganz anders Mobilitätserlebnis. Baden-Württemberg mit seiner leistungsstarken Kraftfahrzeugindustrie ist ein ganz herausragender Standort für Innovation und Entwicklung auf diesem Gebiet. Insofern ist es mir ein wichtiges Anliegen, diese Prozesse im Hinblick auf eine datenschutzgerechte Umsetzung zu begleiten.

Auch schon jetzt wird in den modernen Fahrzeugen eine Fülle an Daten generiert. Dabei geht es um Diagnose- und Servicedaten, die von der Werkstatt ausgelesen werden können und müssen und dann unter Umständen auch an die Herstellerfirmen weitergeleitet werden. Kommunikations- und Kontaktdaten der Nutzer des Fahrzeugs werden über die Infotainmentprodukte im Fahrzeug gesammelt und gespeichert. Über eingebaute SIM-Karten wird ein ständiger Kontakt der Fahrzeuge mit dem Backend der Herstellerfirma hergestellt. Die Standortdaten des Fahrzeugs müssen nicht zuletzt aufgrund gesetzlicher Regelungen für das I-Call Notrufsystem jederzeit übermittelt werden.
Schon heute gibt es teilautonomes Fahren über die Fahrassistenzsysteme, man denke da nur an Spurhalte-, und Abstandsassistenten und Einparksysteme.
Beim autonomen Fahren kommt noch zwangsläufig hinzu, dass das Auto durch seine Sensoren die gesamte Umgebung erfasst, um sich mit künstlicher Intelligenz durch die Straßen zu bewegen. Dabei werden andere Verkehrsteilnehmer, Gebäude, Passanten etc. erfasst und verarbeitet.

Notwendigerweise müssen sich auch die autonomen Fahrzeuge untereinander unterhalten können. Damit verbunden ist ein Datenaustausch über Umgebungsdaten und Standortdaten, man spricht dabei vom vernetzten Fahren.

All diese von den Fahrzeugen generierten Daten, die dem Nutzer statt reinem Fahrerlebnis auch Mobilitätserlebnisse ermöglichen sollen, bergen jedoch ein nicht ganz unbeträchtliches Risiko für die informationelle Selbstbestimmung. Werden die Mobilitätsdaten mit der Fahrzeugidentifikationsnummer oder dem Kennzeichen, zusammengeführt und verknüpft, entstehen personenbezogene Daten. Da diese Datenverarbeitung laufend und automatisch erfolgt, kann der Nutzer nicht mehr ohne weiteres erkennen, wann er beim Fahren welche Daten wem Preis gibt. Dazu, sich Begehrlichkeiten von Werkstätten, Herstellern, Versicherungsunternehmen, Strafverfolgungsbehörden etc. auf diese Daten vorzustellen, braucht man nicht allzu viel Phantasie. Für einen Versicherer zu wissen, ob das Drehzahlmoment des Motors signifikant erhöht ist und deshalb von einer aggressiv/dynamischen Fahrweise ausgegangen werden kann, mag für die Tarifgestaltung oder die Schadensregulierung äußerst hilfreich sein.

Autonomes Fahren ohne die Generierung und Verarbeitung einer Vielzahl von Daten ist nicht möglich. Es kann jedoch niemand wollen, dass wir die Freiheit, die wir durch autonomes Fahren gewinnen, mit unseren Daten bezahlen müssen.

Regelungen über den Umgang mit den personenbezogenen Daten sind vorhanden. Gerade durch die Einführung der Datenschutz-Grundverordnung (DS-GVO) haben die Informationspflichten eine herausragende Stellung erhalten. Ziel muss es sein, dass der Nutzer jederzeit weiß, welche Daten sein Fahrzeug generiert und ob und gegebenenfalls wie er diese Daten so weit wie möglich selbst verwalten kann. Auch die Grundsätze des Datenschutzes durch Technikgestaltung und durch daten-

schutzfreundliche Einstellungen (privacy by design und privacy by default), welche in der DS-GVO explizit festgeschrieben wurden, geben den Rahmen vor, in dem diese Technologie datenschutzgerecht gelingen kann. Wichtig ist es dabei, dass meine Behörde früh in die Entwicklungsprozesse eingebunden wird, um diese zu begleiten.

Für die Entwicklung der Sensoren für das autonomen Fahrens ist es unablässig, dass die Systeme erst einmal mit Daten gefüttert werden. Dafür müssen insbesondere die Umgebung, der Verkehr sowie die Reaktion der anderen Verkehrsteilnehmer von den Systemen erfasst werden. Diese sind sogenannte „selbstlernende Systeme". Ereignisse, menschliche Verhaltensweisen, straßenrechtliche Vorgaben und vor allem die unmittelbare Umgebung müssen vom System erfasst und in einen Algorithmus überführt werden. Dazu bedarf es einer präzisen Erkennung anderer Verkehrsteilnehmer und verschiedener Objekte. Das Instrument der Datenschutzfolgeabschätzung gibt einen guten Rahmen für die Entwickler dieser Systeme vor, um sich der datenschutzrechtlichen Relevanz der Technik bewusst zu werden und die Datenvermeidung und Datensparsamkeit in die Entwicklung der Systeme von vornherein zu implementieren.

Wenn sich alle Beteiligten wie Hersteller, Entwickler und auch die Nutzer über die Herausforderungen hinsichtlich des Datenschutzes bewusst sind und schon in der Entwicklung ein Augenmerk auf datenschutzfreundliche Lösungen gelegt wird, dann kann das autonome Fahren auch aus Sicht des Datenschutzes gelingen.

4.2 Ergebnisse der Prüfung der Einhaltung datenschutzrechtlicher Voraussetzungen durch die Autowerkstatt

Moderne Kraftfahrzeuge generieren immer mehr Daten. Viele davon werden in der Werkstatt für die Inspektion oder die Reparatur benötigt. Auch rein technische Daten sind personenbeziehbare Daten, wenn sie mit der Fahrgestellnummer oder den Kundendaten verknüpft werden.

Im Juni 2017 startete dazu eine bundesweite Befragung von Autowerkstätten durch sechs Aufsichtsbehörden, um die Verarbeitung von Fahrzeugdaten nachzuvollziehen und auf die datenschutzrechtliche Relevanz und Vereinbarkeit zu untersuchen.

Von meiner Dienststelle wurden die Vertragswerkstätten eines in Baden-Württemberg ansässigen Automobil-Herstellers angeschrieben.

Dabei wurden die Werkstätten befragt, welche personenbezogenen Daten aus dem Fahrzeug bei einem Werkstattbesuch ausgelesen werden und in dem Datenverarbeitungssystem der Werkstatt gespeichert. Zentrale Themen der Befragung waren die Rechtsgrundlage für die Datenverarbeitung, die Weitergabe der Daten an den Hersteller oder an andere Dritte wie beispielsweise Versicherungen und die Information der Kunden über eine Datenverarbeitung Ihrer Kraftfahrtzeug-Daten.

Die Antworten der Werkstätten aller teilnehmenden Bundesländer wurden anonymisiert ausgewertet.

Das Ergebnis zeigte, dass die Datenverarbeitung der zwingend für Reparatur, Service und Wartung erforderlichen Daten, inklusive Datenübermittlung an den Hersteller, gem. Artikel 6 Absatz 1 Buchstabe b der Datenschutz-Grundverordnung (DS-GVO) möglich ist. Für eine Einwilligung in die Datenverarbeitung besteht dann keine Notwendigkeit mehr. Einige Werkstätten hatten trotzdem eine Einwilligung für eine Datenverarbeitung vorgelegt, die jedoch so weit gefasst war, dass pauschal in jedwede Datenverarbeitung eingewilligt werden sollte. Diese Einwilligung war auch verknüpft mit der Auftragsannahme. Diese Vorgehensweise verstößt jedoch gegen

die datenschutzrechtlichen Regelungen. Zum einen muss die Einwilligung in die Datenverarbeitung zweckgebunden sein. Es muss aus der Erklärung ersichtlich sein, welche Daten, zu welchem Zweck erhoben werden und wie sie verarbeitet werden. Zum anderen muss die Abgabe einer Einwilligung freiwillig sein, sie darf also an keine nachteiligen Folgen gekoppelt werden, die Annahme des Kraftfahrzeugs zur Reparatur darf nicht davon abhängig gemacht werden, ob der Kunde die Einwilligung unterschreibt.

Die Datenschutz-Grundverordnung schreibt vor, dass der Kunde in präziser, transparenter, verständlicher und leicht zugänglicher Art und Weise Informationen bekommt, die sich auf die Verarbeitung beziehen. Die Werkstätten gaben an, dass Informationen zur Datenverarbeitung entweder in den Betriebsanleitungen oder in den Einwilligungserklärungen vorhanden seien oder die Kunden durch Servicemitarbeiter aufgeklärt werden. Ich empfehle den Werkstätten, ein Informationsblatt an die Kunden mit dem Inhalt gem. Artikel 12, 13 DS-GVO beizulegen oder auf den Auftrag mit aufzudrucken.

Schwieriger zu beantworten war die Frage, nach welchen rechtlichen Grundlagen die Verknüpfung der technischen Daten mit dem Namen des Kunden oder mit der Fahrzeugidentifikationsnummer übermittelt werden darf. Viele der Übermittlungen erfolgen aufgrund der Vertragserfüllung im Rahmen des Werkstattvertrages gem. Artikel 6 Absatz 1 Buchstabe b DS-GVO. Darunter fällt beispielsweise bei Garantie-, Gewährleistungs- und Kulanzfällen die Prüfung der Leistungserstattung durch die Hersteller und bei konkreten Reparaturdurchführungen wie Fahrzeugdiagnosen die Rückkoppelung mit dem Hersteller.

Die datenschutzrechtliche Grundlage für die Datenverarbeitung der erforderlichen Fahrzeugdaten für die Produktüberwachung/Produktbeobachtung und für eventuelle Rückrufaktionen ist Artikel 6 Absatz 1 Buchstabe c DS-GVO. Es liegt hier die Erfüllung einer rechtlichen Verpflichtung des Automobilherstellers aus dem Produkthaftungsgesetz vor. Da hier sowohl die Werkstatt als auch der Hersteller die Daten der Kunden für die erwähnten Zwecke verarbeiten, wäre eine gemeinsame Verarbeitung gem. Artikel 26 DS-GVO denkbar mit der Konsequenz, dass die Werkstätten und die Hersteller in einer gemeinsamen Vereinbarung festlegen, wer welchen Informationspflichten nachkommt.

Für eine Datenverarbeitung zu Zwecken der Produkt/Qualitätsverbesserungen und Produktfortentwicklungen kann Artikel 6 Absatz 1 Buchstabe f DS-GVO heran gezogen werden. Gleiches gilt für Datenverarbeitungen im Kontext von Marketingaktionen und Kundenzufriedenheitsbefragungen. Diese könnte jedoch auch anonymisiert verarbeitet werden.

Demgegenüber kann die zentrale Führung einer elektronischen Wartungs- und Reparaturhistorie beim Automobilhersteller (digitaler Servicenachweis) nur mit expliziter Einwilligung des Halters durchgeführt werden. Gleiches gilt für die Teilnahme an Vergütungs- und Bonusprogrammen der Kunden.

Die Werkstätten sind sich kaum bewusst, welche Daten sie für welche Zwecke erheben. Die Datenverarbeitung für eigene Zwecke und für Zwecke, die dem Hersteller dienen, werden als nicht getrennt voneinander wahrgenommen. Somit fehlt es auch oftmals an einer ordnungsgemäßen Information der Kunden und an einer ordnungsgemäßen Vereinbarung zwischen Werkstätten und Herstellern.

5. Justiz und Recht

5.1 Umsetzung der Richtlinie (EU) 2016/680 im Justizbereich …

Die in verschiedensten Beiträgen meines Tätigkeitsberichts angesprochene Datenschutz-Grundverordnung gilt für strafrechtliche und ordnungswidrigkeitenrechtliche Verfahren nicht. Auch im Bereich des Justizvollzugs findet sie grundsätzlich keine Anwendung. Für diese Bereiche enthält die Richtlinie (EU) 2016/680 datenschutzrechtliche Vorgaben, die zwar inhaltlich in weiten Teilen der Datenschutz-Grundverordnung entsprechen. Anders als die unmittelbar anwendbare Datenschutz-Grundverordnung muss die Richtlinie jedoch durch nationales Recht umgesetzt werden. Soweit dies nicht im Bundesrecht erfolgt, etwa in der Strafprozessordnung oder dem Gesetz über Ordnungswidrigkeiten, geschieht dies im Landesrecht. Das Ministerium der Justiz und für Europa hat hierzu einen umfangreichen Entwurf für ein „Gesetz zur Anpassung des besonderen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 für den Geschäftsbereich des Justizministeriums sowie für die zur Ahndung von Ordnungswidrigkeiten zuständigen Behörden" erarbeitet. Wie bereits dem Namen zu entnehmen ist, enthält dieser Entwurf Anpassungen an die Datenschutz-Grundverordnung. Vor allem aber dient er der Umsetzung der Richtlinie (EU) 2016/680. Neben einer Vielzahl von Einzelgesetzen, die an die unionsrechtlichen Vorgaben angepasst werden sollen, wie z. B. das Justizvollzugsgesetzbuch, enthält der Gesetzentwurf auch ein neues Landesdatenschutzgesetz für Justiz- und Bußgeldbehörden.

5.1.1 … durch Schaffung eines Landesdatenschutzgesetzes für Justiz- und Bußgeldbehörden

Das Landesdatenschutzgesetz vom 12. Juni 2018 enthält ergänzende Regelungen zur Durchführung der Datenschutz-Grundverordnung, aber keine Regelungen zur Umsetzung der Richtlinie (EU) 2016/680. Für die Justiz- und Bußgeldbehörden soll die Richtlinie, soweit erforderlich, durch ein Landesdatenschutzgesetz für Justiz- und Bußgeldbehörden umgesetzt werden. Dieses soll für die Datenverarbeitung der ordentlichen Gerichte in Strafsachen, der Staatsanwaltschaften, aber auch für die Verarbeitung personenbezogener Daten zur Ahndung von Ordnungswidrigkeiten und zur Vollstreckung von Bußgeldern durch alle hierfür zuständigen öffentlichen Stellen des Landes gelten. Außerdem sollen in diesem Gesetz die Aufgaben und Befugnisse meiner Dienststelle in diesem Bereich festgelegt werden. Schließlich enthält der Gesetzentwurf eine Sondervorschrift für die Videoüberwachung in Gefangenen-Vorführbereichen von Gerichtsgebäuden und eine Rechtsgrundlage, die es im Außendienst tätigen Justizbediensteten erlaubt, in Gefahrensituationen Geräte mit einer so genannten Mithörfunktion zu benutzen.

Ich habe zu dem Entwurf des Landesdatenschutzgesetzes für Justiz- und Bußgeldbehörden mehrmals Stellung genommen. Meine schwerwiegendsten Bedenken richteten sich dabei nicht gegen die Vorschriften, die der unmittelbaren Umsetzung der Richtlinie (EU) 2016/680 dienen. Vielmehr bezogen sich diese auf die Regelungen über die Videoüberwachung in Gefangenen-Vorführbereichen von Gerichtsgebäuden und die Rechtsgrundlage für verdeckte Tonaufnahmen durch im Außendienst tätige Justizbedienstete.

Die Möglichkeit, mittels Videotechnik inhaftierte Personen zu überwachen, die wegen einer Verhandlung vom Gefangenentransporter der Justizvollzugsanstalt in die

Vorführzelle des Gerichts, von dort zum Gerichtssaal und wieder zurück gebracht werden müssen, soll die Sicherheit und Ordnung in den Gerichten gewährleisten; etwa durch frühzeitiges Erkennen von Angriffen inhaftierter Personen auf das Vorführpersonal oder durch die Verhinderung von Suizidversuchen inhaftierter Personen in der Vorführzelle. Der mir vorgelegte erste Referentenentwurf vom Mai 2018 sah hierzu z. B. vor, dass auch öffentliche oder behördenöffentliche Bereiche des Gerichtsgebäudes mittels Videotechnik beobachtet und auch Aufzeichnungen gefertigt werden können, soweit Tatsachen die Annahme rechtfertigen, dass dort Straftaten begangen werden sollen, durch die Personen, Gebäude oder darin befindliche Sachen gefährdet sind.

Eine derartige Regelung würde dazu führen, dass außer den Gefangenen und den Vorführbeamten auch andere Beschäftigte des Gerichts, aber auch Zeugen, Rechtsanwälte und die Öffentlichkeit von dieser Videobeobachtung und -aufzeichnung erfasst würden. Hierdurch würde massiv in die Grundrechte der Betroffenen eingegriffen werden. Dennoch war eine Güterabwägung zwischen den Interessen der Unbeteiligten und dem Sicherheitsbedürfnis der Gerichte im ersten Referentenentwurf nicht vorgesehen. In meiner Stellungnahme habe ich darauf hingewiesen, dass ich die vorgesehenen Regelungen für europarechtswidrig halte.

Meinen Bedenken ist insofern Rechnung getragen worden, als in der überarbeiteten Entwurfsfassung vom Juli 2018 der für die Videoüberwachung vorgesehene Vorführbereich auf die Vorführzellen und den nicht für die Öffentlichkeit zugänglichen Bereich des Gerichts beschränkt wurde. Außerdem ist eine Interessenabwägung zwischen den Interessen der – auch unbeteiligten – Betroffenen und dem Sicherheitsbedürfnis der Gerichte aufgenommen worden.

Im September 2018 wurde ich wegen einer Ergänzung des Gesetzentwurfs noch einmal angehört. Dabei ging es um eine Rechtsgrundlage für den Einsatz einer Mithörfunktion bei mobilen Alarmgeräten. In dieser ist vorgesehen, dass im Außendienst tätige Justizbedienstete (etwa Gerichtsvollzieher oder Betreuungsrichter) in Gefahrensituationen zu ihrem Schutz mittels geeigneter Geräte heimlich Tonaufnahmen anfertigen und an eine Leitstelle übermitteln können. Die Leitstelle soll diese Tonaufnahmen speichern können und an die Polizei sowie an die Dienststellen der Justizbediensteten, die die Tonaufnahmen angefertigt haben, übermitteln. Als alleiniger Zweck dieser Maßnahmen, also z. B. auch der Weiterleitung der Aufnahmen von der Leitstelle an die Dienststelle des Justizbediensteten, ist der Schutz des tätigen Justizbediensteten bei Gefahr genannt.

Aus dem Entwurf ergibt sich außerdem, dass auch die Justizbediensteten, die die Tonaufnahmen angefertigt haben, und deren Dienststellen die Tonaufnahmen speichern.

Gegen die vorgesehenen Regelungen, die auch in Wohnungen heimliche Tonaufnahmen erlauben würden, obwohl diese durch Artikel 13 des Grundgesetzes besonders geschützt sind, bestehen schwerwiegende datenschutzrechtliche Bedenken.

So ist bereits nicht nachvollziehbar, weshalb ausgerechnet heimliche Tonaufnahmen dem Schutz von im Außendienst tätigen Justizbediensteten dienen sollen. Vielmehr ist zu vermuten, dass die Kenntnis eines Betroffenen davon, dass seine Äußerungen aufgezeichnet werden, zur Deeskalation einer Gefahrensituation beitragen würde. Darüber hinaus halte ich es für fraglich, ob die vorgesehene Vorgehensweise bei einer akut vorliegenden Gefahrensituation überhaupt zu einem rechtzeitigen Eingreifen der Polizei führen würde, zumal die Aufnahme zunächst der Leitstelle übermittelt werden soll, die dann ihrerseits über die Weiterleitung an die Polizei entscheidet. Auch bei anderen im Entwurf vorgesehenen Datenverarbeitungsmaßnahmen ist nicht ersichtlich, inwiefern diese dem Schutz des Justizbediensteten

dienen. Dies gilt z. B. für die Übermittlung der Aufnahmen durch die Leitstelle an die Dienststelle des Justizbediensteten. Die genannten Maßnahmen, die zu schwerwiegenden Eingriffen in das informationelle Selbstbestimmungsrecht der Betroffenen führen würden, sind zur Erreichung des angestrebten Zwecks weder geeignet noch erforderlich und aus datenschutzrechtlicher Sicht daher abzulehnen.
Darüber hinaus ist dem Entwurf nicht zu entnehmen, zu welchem Zweck die Tonaufnahmen von verschiedenen Stellen, also mehrfach, gespeichert werden sollen und weshalb dies für nötig gehalten wird. Auch dies ist aus datenschutzrechtlichen Gründen inakzeptabel.

5.1.2 ... durch Änderung des Justizvollzugsgesetzbuchs

Auf den Justizvollzug findet grundsätzlich die Richtlinie (EU) 2016/680 Anwendung. Diese enthält Bestimmungen 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, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Der Justizvollzug, einschließlich der Sicherungsverwahrung, des Jugendarrests, der Untersuchungshaft und der ihr gleichgestellten Freiheitsentziehungen erfolgt entweder zu Zwecken der Strafvollstreckung und/oder zum Schutz vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Obwohl der Justizvollzug den vorgenannten Zwecken dient, auf die die Richtlinie (EU) 2016/680 Anwendung findet, kommt es vereinzelt vor, dass Justizvollzugsanstalten auch zu anderen Zwecken personenbezogene Daten verarbeiten. In diesen seltenen Fällen ist die Datenschutz-Grundverordnung anwendbar. Mit dem mir vorgelegten Gesetzentwurf zur Änderung des Justizvollzugsgesetzbuchs soll daher zum einen die Richtlinie (EU) 2016/680 umgesetzt werden. Zum anderen soll, soweit ausnahmsweise die Datenschutz-Grundverordnung Anwendung findet, eine Anpassung an diese erfolgen.
Die von mir zum Referentenentwurf vom Mai 2018 vorgelegte Stellungnahme wurde bei der Überarbeitung des Entwurfs zu großen Teilen berücksichtigt. Keine Berücksichtigung fanden meine Anmerkungen zu den Vorschriften über die Einwilligung.
Im Ersten Buch des Justizvollzugsgesetzbuchs ist eine Vorschrift vorgesehen, die regelt, dass die Justizvollzugsanstalt personenbezogene Daten verarbeiten darf, wenn das Justizvollzugsgesetzbuch oder eine andere Rechtsvorschrift dies erlaubt oder die betroffene Person eingewilligt hat. Diese Vorschrift entspricht bzgl. der Einwilligung nicht den Anforderungen der Richtlinie (EU) 2016/680 an eine Rechtsgrundlage für eine Datenverarbeitung. Darüber hinaus ist den Erwägungsgründen der Richtlinie zu entnehmen, dass die Einwilligung allein als Rechtsgrundlage für eine Datenverarbeitung äußerst kritisch gesehen wird. Denn im Anwendungsbereich der Richtlinie hat der Betroffene, z. B. ein Strafgefangener, der sich mit einer ihn betreffenden Datenverarbeitung einverstanden erklären soll, regelmäßig keine echte Wahlfreiheit. In diesen Fällen kann seine Äußerung daher nicht als freiwillig abgegebene Willensbekundung betrachtet werden. Es fehlt damit an der für eine Einwilligung erforderlichen Freiwilligkeit.

Ob und in welcher Form meine Anmerkungen und Bedenken im weiteren Verfahren berücksichtigt wurden, war mir bei Redaktionsschluss für den Tätigkeitsbericht noch nicht bekannt. Nach meiner Kenntnis soll das Gesetz zur Anpassung des besonderen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 für den Geschäftsbereich des Justizministeriums sowie für die zur Ahndung von Ordnungswidrigkeiten zuständigen Behörden im Januar 2019 verabschiedet werden.

5.2 Datenschutz bei Rechtsanwälten

Zahlreiche Beschwerden über die Verarbeitung personenbezogener Daten durch Rechtsanwälte waren auch in diesem Berichtsjahr zu bearbeiten. Schwerpunkte waren dabei die Themen Auskunftspflicht, Verschlüsselung von E-Mails und sog. Gegnerlisten.

Das Verhältnis der Rechtsanwälte zur Datenschutzaufsicht war noch nie ganz unproblematisch. Der Rechtsanwalt ist ein unabhängiges Organ der Rechtspflege (§ 1 der Bundesrechtsanwaltsordnung). Schon von daher fällt es einzelnen Vertretern dieser Berufsgruppe schwer zu akzeptieren, dass sie der Kontrolle einer staatlichen Aufsichtsbehörde unterliegen sollen. Hinzu kommt, dass die Rechtsanwaltskammern die standesrechtliche Aufsicht wahrnehmen und insoweit gewissermaßen in Konkurrenz zur Datenschutzaufsicht treten. Gleichwohl ist nicht ernsthaft zu bestreiten, dass auch die Datenverarbeitung durch Rechtsanwälte grundsätzlich der Datenschutz-Grundverordnung unterfällt und damit grundsätzlich auch der Kontrolle durch die Aufsichtsbehörde unterliegt. Lediglich im Rahmen des § 29 des Bundesdatenschutzgesetzes (BDSG) gelten dabei gewisse Ausnahmen.

§ 29 Absatz 1 BDSG privilegiert (u. a.) Rechtsanwälte insoweit, als sie von bestimmten Pflichten, denen Verantwortliche gegenüber betroffenen Personen unterliegen, freigestellt sind. Insbesondere betrifft dies etwa die Pflicht, darüber Verfahrens- oder Prozessgegnern Auskunft zu geben, welche Daten sie im Rahmen des Mandatsverhältnisses verarbeiten und woher diese Daten stammen (Artikel 15 DS-GVO). Darüber hinaus schränkt § 29 Absatz 3 BDSG die Handlungsmöglichkeiten der Aufsichtsbehörde gegenüber Rechtsanwälten insoweit ein, als der physische Zugang zu den Kanzleiräumen und zu den dort gespeicherten Daten ausgeschlossen wird, soweit dadurch eine Verletzung der Geheimhaltungspflicht zu befürchten wäre.

Ob diese Vorschriften des BDSG Bestand haben werden – was wir sehr bezweifeln –, wird der Europäische Gerichtshof entscheiden. In der täglichen Praxis bedeutsam war bisher vor allem die Einschränkung der Betroffenenrechte. Viele Beschwerden über Rechtsanwälte richteten sich gegen die verweigerte Auskunft über die Daten, die der Anwalt speichert und insbesondere, aus welcher Quelle sie stammen. Damit hatten die Betroffenen aber wegen der genannten Ausnahmebestimmung regelmäßig keinen Erfolg. Dabei muss allerdings darauf hingewiesen werden, dass schon nach altem Recht die anwaltliche Schweigepflicht zur Folge hatte, dass Rechtsanwälte über alles, was sie im Zusammenhang mit der Wahrnehmung eines Mandats erfahren hatten, gegenüber Dritten schweigen durften und schweigen mussten. Etliche Gerichtsentscheidungen hatten dies bestätigt. Angesichts dessen mussten wir die Beschwerdeführer in ihrer Erwartung, wir könnten sie in ihrem Anliegen unterstützen, regelmäßig enttäuschen. Eine ganz andere Frage ist die, ob der Mandant selbst berechtigt ist, von seinem Anwalt zu erfahren, welche Daten er über ihn speichert. Eine Berufung auf das Mandatsgeheimnis und damit auf § 29 BDSG geht hier fehl. Jedenfalls dürften entsprechende Ansprüche aus der vertraglichen Beziehung (Geschäftsbesorgungsvertrag) herzuleiten sein. Konkrete Beschwerden hierzu gab es bisher allerdings nicht.

Eine häufige Beschwerde betraf die Kommunikation durch Rechtsanwälte per unverschlüsselter E-Mail. Hier haben offensichtlich die wiederholten Warnungen vor den Risiken dieser Form der Kontaktaufnahme ohne entsprechende Schutzvorkehrung gegen unbefugte Kenntnisnahme durch Dritte zu einem gesteigerten Datenschutzbewusstsein geführt. Dass gerade Rechtsanwälte, die ansonsten regelmäßig – und angesichts drohender Strafbarkeit bei Verletzung zu Recht – auf ihre anwaltliche Schweigepflicht pochen, sich in dieser Frage verhältnismäßig unbedarft, um nicht zu sagen leichtfertig verhalten, darf schon verwundern.

Unbeschadet sonstiger rechtlicher Geheimhaltungspflichten gelten der Datenschutzgrundsatz der Integrität und Vertraulichkeit (Artikel 5 Absatz 1 Buchstabe f DS-GVO) sowie die Verpflichtung auf die Sicherheit der Verarbeitung (Artikel 32 DS-GVO) auch für Rechtsanwälte. Danach ist die Vertraulichkeit der Verarbeitung zu gewährleisten, was insbesondere auch bedeutet, dass personenbezogene Daten vor unbefugter oder unrechtmäßiger Verarbeitung zu schützen sind. Für die E-Mail-Kommunikation, die bekanntlich Möglichkeiten der unbefugten Kenntnisnahme eröffnet (verschiedentlich wird die unverschlüsselte E-Mail mit einer Postkarte verglichen), bedeutet dies, dass grundsätzlich eine Pflicht zur Ende-zu-Ende-Verschlüsselung besteht. Da dies von vielen Rechtsanwälten schlicht ignoriert wird, haben wir uns an die Rechtsanwaltskammern gewandt, in der Hoffnung, von dort Unterstützung zu erhalten. Die Antwort steht noch aus. Je nach Ergebnis werden wir prüfen müssen, ob wir in geeigneten Fällen aufsichtsrechtliche Maßnahmen in die Wege leiten.

Wen würde es nicht stören, wenn er im Internet in einem Atemzug mit Rechtsbrechern angeprangert würde? Unvorstellbar? Weit gefehlt! Sogenannte Gegnerlisten sind Gang und Gäbe. Dabei handelt es sich um anwaltliche Werbemaßnahmen, mit deren Hilfe Rechtsanwälte anhand der Zahl der gewonnen Verfahren auf ihre Fachkompetenz hinweisen wollen. Zwar hat das Bundesverfassungsgericht in einem Beschluss vom 12. Dezember 2007 (1 BvR 1625/06) solche Methoden der Eigenwerbung grundsätzlich für zulässig erklärt. Etliche instanzgerichtliche Urteile haben diese Berechtigung jedoch insoweit eingeschränkt, als die namentliche Nennung von Privatpersonen in solchen Listen als unzulässiger Eingriff in das Persönlichkeitsrecht der Betroffenen gewertet wurde. Auch vor dem Hintergrund der durch die Datenschutz-Grundverordnung mittlerweile geänderten datenschutzrechtlichen Rahmenbedingungen ist Eingriffen in das Datenschutzgrundrecht (Artikel 8 der Grundrechte der Charta der Europäischen Union) im Verhältnis zu nationalem Recht aktuell größere Bedeutung zuzumessen. Rechtsanwälten ist deshalb zu raten, bei Werbemaßnahmen in eigener Sache künftig sensibler mit persönlichen Daten ehemaliger Prozessgegner umzugehen.

6. Kommunales

6.1 Gemeinderatssitzungen im Internet – neue Wege der Transparenz in den Kommunen

Was vor einigen Jahren als Pilotprojekt in einigen wenigen Kommunen begann, wird immer öfter Gegenstand von Überlegungen einzelner Gemeinderats-Fraktionen oder der Kommunalverwaltung. Eine Gemeinderatssitzung oder auch die Kandidatenvorstellung einer Bürgermeisterwahl live oder als Podcast im Internet zu übertragen, bietet für die Kommunen den Vorteil, interessierten Mitbürgerinnen und Mitbürgern einen niedrigschwelligen und bürgernahen Zugang zu gemeindlichen Entscheidungsprozessen zu geben.

Mit der Bild- und Tonaufnahme der Personen, die von der Kamera erfasst werden, stellt sich die Frage nach der Rechtsgrundlage dieser Form der Datenverarbeitung.

Mangels einer gesetzlichen Regelung kann die Verarbeitung von personenbezogenen Daten im Zusammenhang mit Gemeinderatssitzungen somit nur auf eine wirksame Einwilligung der jeweils Betroffenen gemäß Artikel 6 Absatz 1 Satz 1 Buchstabe a DS-GVO gestützt werden. Nach Artikel 4 Nummer 11 DS-GVO muss diese Willensbekundung „freiwillig" erteilt worden sein. Eine Einwilligung ist dann freiwillig, wenn die betroffene Person „eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden" (Erwägungsgrund 42, letzter Satz). Arbeiten Behörden mit Einwilligungen als Rechtsgrundlage für ihre Datenverarbeitung, ist das Merkmal der Freiwilligkeit besonders sorgfältig zu prüfen. Denn im Verhältnis Behörde – Bürger liegt ein strukturelles Ungleichgewicht vor, welches die Freiwilligkeit einer Willensbekundung des Bürgers grundsätzlich in Frage stellt (Erwägungsgrund 43).

Da die von der Datenverarbeitung (in Form der Internetübertragung) möglicherweise betroffenen Personen keine homogene Gruppe darstellen, kann für eine erste Annäherung an das Merkmal der Freiwilligkeit eine Unterscheidung nach Betroffenengruppen hilfreich sein:

- **Gemeinderatsmitglieder**
  Bei Mitgliedern des Gemeinderats sollte das Merkmal der Freiwilligkeit grundsätzlich gegeben sein. Möglich ist auch eine Einwilligungserklärung, welche die gesamte Amtszeit umfasst.

- **Gemeindebedienstete**
  Hier ist das Vorliegen des Merkmals der Freiwilligkeit besonders sorgfältig zu prüfen. Bei Leitungs- und Führungsfunktion (wie etwa Amts-, Abteilungsleitungen) kann Freiwilligkeit vorliegen. Bei anderen kommunalen Bediensteten ist regelmäßig davon auszugehen, dass aufgrund des Über- und Unterordnungsverhältnisses ein deutliches Ungleichgewicht und somit keine wirklich freie Wahlmöglichkeit der Bediensteten besteht. In diesen Fällen kann keine wirksame Einwilligung eingeholt werden. Hier ist dafür Sorge zu tragen, das die Bediensteten außerhalb des Aufnahmebereichs der Kameras arbeiten.

- **Vertreter kommunaler Gesellschaften und Bedienstete von anderen öffentlichen Stellen**
  Grundsätzlich gilt das Gleiche wie bei Bediensteten von Gemeindeverwaltungen, also wird eine Einwilligung regelmäßig nicht freiwillig sein. Unter diese Betroffenengruppe können unter anderem Revierförster oder Polizeibeamte subsumiert werden. Bei Leitungs- und Führungsfunktion (wie etwa Geschäftsführern kommunaler Gesellschaften) kann von Freiwilligkeit ausgegangen werden.

- **Externe Gutachter und Projektentwickler**
  Eine freie Wahlmöglichkeit von externen Gutachtern und Projektentwicklern im Sinne der DS-GVO kann beispielsweise

dann gegeben sein, wenn eine Auftragserteilung aufgrund eines vorgeschalteten Vergabeverfahrens und somit nach den restriktiven Vorgaben des Vergaberechts erfolgte und deshalb davon ausgegangen werden kann, dass kein deutliches Ungleichgewicht vorliegt.

- **Saalöffentlichkeit**
  Eine Internetübertragung von Zuhörern in Bild und Ton ist in Hinblick auf die Anforderungen an eine Einwilligungserklärung datenschutzrechtlich besonders problematisch. Deshalb sollte hiervon Abstand genommen werden. Auch kann grundsätzlich nicht ausgeschlossen werden, dass eine Internetübertragung mit einem Abschreckungseffekt für Zuhörer verbunden ist und diese deshalb nicht an Gemeinderatssitzungen teilnehmen. Insbesondere kann eine laufende Kamera für Bürger eine Hemmschwelle darstellen, sich in sog. Bürgerfragestunden zu äußern.

Grundsätzlich besteht bei der Übertragung von Gemeinderatssitzungen im Internet ein Spannungsfeld zwischen der Transparenz öffentlichen Handelns und dem Schutz personenbezogener Daten der Menschen, die in Bild und Ton aufgenommen werden. Bei Vorliegen der oben ausgeführten Voraussetzungen ist eine Wahrung des informationellen Selbstbestimmungsrechts der betroffenen Personen möglich, hier hilft eine freiwillig abgegebene Einwilligung weiter. Einzig die Übertragung der Personen aus der Saalöffentlichkeit ist grundsätzlich zu vermeiden, um Abschreckungseffekte zu vermeiden.

6.2 Fotos, Fotos, Fotos …

Die Kommunen als verantwortliche Stellen veröffentlichen in erheblichem Umfang Fotos, auf denen Personen abgebildet sind – sei es auf der eigenen Homepage, in einer Tourismus-Broschüre oder im Amtsblatt, welches meistens auch in einer Online-Version geführt wird. Eine Veröffentlichung dieser Fotos im Internet ermöglicht einer Weltöffentlichkeit den Zugang zu personenbezogenen Daten aus dem regionalen Bereich. Entsprechend sorgfältig müssen die Kommunen in diesem Zusammenhang das Vorliegen einer Rechtsgrundlage prüfen.

Die Öffentlichkeitsarbeit öffentlicher Stellen gehört nach unserer Rechtsauffassung zu den Kommunen zugewiesenen Aufgaben. Sowohl das Fotografieren (= Erheben) als auch die Veröffentlichung von Lichtbildern richten sich nach § 4 des Landesdatenschutzgesetzes (LDSG). Wir halten es für vertretbar, im Rahmen einer Erforderlichkeitsprüfung den § 23 Absatz 1 Nummer 2 oder 3 des Kunsturhebergesetzes (KUG) jedenfalls entsprechend anzuwenden. Je eher sich eine Vielzahl von Personen als „Beiwerk" oder im Rahmen von Übersichtsaufnahmen auf dem Bild befindet, desto eher wird eine Veröffentlichung ohne Einwilligung zulässig sein. Je eher einzelne Personen hervorgehoben präsentiert werden, desto eher bedarf es einer Einwilligung der Betroffenen. In besonderem Maß gilt dies, wenn es sich um Abbildungen von Kindern handelt. Im Zweifel sollte die öffentliche Stelle Personen entweder um Einwilligung bitten oder sie unkenntlich machen (z. B. verpixeln).

Werden Fotos aufgrund einer Einwilligung veröffentlicht und die darauf abgebildete Person widerruft diese, erstreckt sich dieser Widerruf nur auf zukünftige Datenverarbeitungen. Folgen aus der erlaubten seitherigen Veröffentlichung von Bildern sind grundsätzlich nicht zu beseitigen. Wird beispielsweise die Einwilligung zur Veröffentlichung für Fotos in einer Tourismus-Broschüre der Kommune widerrufen, dürfen keine neuen Broschüren mit den konkreten Fotos gedruckt werden. Bereits gedruckte Broschüren müssen aus datenschutzrechtlichen Gründen nicht zurückgeholt werden. Allerdings sind Fotos auf der Homepage der Kommune zu entfernen oder die Betroffenen zu verpixeln.

Da das Fotografieren eine Datenerhebung darstellt, ist die Informationspflicht gemäß Artikel 13 DS-GVO zu beachten.

6.3 Die Abgrenzung von DS-GVO und JI-Richtlinie in der kommunalen Praxis

Wiederholt wurde an meine Dienststelle die Frage herangetragen, ob die DS-GVO für Behörden anwendbar sei, die im Bereich der Gefahrenabwehr tätig sind. Insbesondere stellt sich diese Frage, wenn in einer Behörde Datenverarbeitungen nicht ausschließlich „zum Zwecke der Gefahrenabwehr" durchgeführt werden, zum Beispiel in einer Straßenverkehrsbehörde.

Gemäß Artikel 2 Absatz 2 Buchstabe d DS-GVO wird die Verarbeitung personenbezogener Daten durch zuständige Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung vom Anwendungsbereich der Datenschutz-Grundverordnung ausgenommen, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt. In Erwägungsgrund 19 der DS-GVO ist dazu ausgeführt, dass der Schutz natürlicher Personen bei der Verarbeitung solcher Daten durch die zuständigen Behörden sowie der freie Verkehr dieser Daten in einem eigenen EU-Rechtsinstrument geregelt sind. Mit dieser Vorschrift wird also der klassische Bereich der polizeilichen Gefahrenabwehr vom Geltungsbereich der Datenschutz-Grundverordnung ausgenommen.

Insofern unterfallen öffentlichen Stellen, unter anderem auch Sonderordnungsbehörden, dem Anwendungsbereich der JI-Richtlinie, wenn die Verarbeitung zu Zwecken der Gefahrenabwehr oder der repressiven Strafverfolgung erfolgt. Die Legaldefinition in Artikel 3 Nummer 7 der Richtlinie (EU) 2016/680 (kurz: JI-Richtlinie) bestimmt, dass „zuständige Behörde" im Sinne der JI-Richtlinie zum einen

a) eine staatliche Stelle ist, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zuständig ist,

oder

b) eine andere Stelle oder Einrichtung ist, der durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, übertragen wurde.

Exkurs: Eine Straßenverkehrsbehörde ist keine eigene verantwortliche Stelle, sondern wird als untergeordnete Organisationseinheit der Kommune tätig. Verantwortliche Stelle ist die Gemeinde als Gebietskörperschaft mit all ihren Organen und organisatorischen Untergliederungen, vertreten durch den (Ober-)Bürgermeister oder die (Ober-)Bürgermeisterin.

Gerade in größeren behördlichen Einheiten kann sich die Frage der Verantwortlichkeit bezüglich einer konkreten Datenverarbeitung stellen. Dies kann sich zum Beispiel (wie hier) im Hinblick auf den Anwendungsbereich oder beim Erstellen des Verarbeitungsverzeichnisses ergeben. Für die Frage, ob DS-GVO oder JI-Richtlinie anzuwenden sind, ist dabei entscheidend, in welchem Aufgabenbereich die fragliche Datenverarbeitung stattfindet.

Erfasst wird also die Gefahrenabwehr (nur) im Zusammenhang mit drohenden oder begangenen Straftaten oder Ordnungswidrigkeiten. Der Begriff der Ordnungswidrigkeiten ist zwar nicht explizit in Artikel 2 Absatz 2 Buchstabe d DS-GVO enthalten. Er ist europarechtskonform aber als Straftat einzuordnen.

Bei der Frage der Anwendbarkeit der DS-GVO oder der JI-Richtlinie bezüglich einer konkreten Datenverarbeitung ist innerhalb einer Behörde (z. B. der Straßenverkehrsbehörde) entscheidend, in welchem Aufgabenbereich die fragliche Datenver-

arbeitung stattfindet. Die Bußgeldstelle innerhalb einer größeren Behördeneinheit unterliegt demnach der JI-Richtlinie, die reine Verwaltungsabteilung dagegen der DS-GVO.

7. Gesundheit und Soziales

7.1 Diskretion in der Arztpraxis

Die Sicherstellung von Diskretion in einer Arztpraxis ist Teil der ärztlichen Schweigepflicht und bildet die Grundlage des Vertrauensverhältnisses zwischen Arzt und Patient. Die Anforderungen bestehen auch nicht erst seit der Datenschutzgrundverordnung. Gesundheitsdaten des Patienten waren bereits laut Bundesdatenschutzgesetz als sog. besondere Arten personenbezogener Daten mit hohem Schutzbedarf durch technisch-organisatorische Maßnahmen gemäß Stand der Technik zu schützen.

Manchmal herrscht am Empfangstresen aber Stau und Praxispersonal gibt dabei personenbezogene Gesundheitsdaten im Gespräch oder am Telefon derart laut preis, dass Dritte im Wartebereich mithören und daher ggf. über Patienten und deren Diagnose informiert werden.

Schallschutztechnische Mindestanforderungen nach DIN orientieren sich an der geplanten Nutzung. Für Arztpraxen wird gemäß Norm ein erhöhter Schallschutz – Schallschutzklasse II – gefordert. Innerhalb der Praxis betrifft dies z. B. die Trennwände zwischen Behandlungsräumen, sowie zwischen Behandlungsräumen und Fluren. Diese sind in Qualität und Detail so auszuführen, dass eine akustische Beeinträchtigung durch benachbarte Räume vermieden wird. Gleiches gilt auch für die Qualität der Raumtüren.

Idealerweise befindet sich zwischen Rezeption und Warteraum ebenfalls eine Raumtür. Eine akustische Abschirmung des Empfangs bei offener Raumfolge zum Wartebereich ist aber auch durch Raumteiler und bei denkmalgeschützten Räumlichkeiten mit eingeschränkten baulichen Veränderungsmöglichkeiten durch gezielte Diskretionsbeschallung realisierbar. Entspricht das angepasste Hintergrundgeräusch dem diskreten Geräuschpegel im Empfangsbereich, kann das menschliche Ohr dem Patientengespräch nicht folgen.

Telefone mit mobilem Empfangsteil sind nicht ortsgebunden und das Personal kann den Empfang für vertrauliche Telefonate verlassen. Die Möglichkeit der zusätzlichen Verwendung von sog. Headsets ermöglicht leisere Telefonate. Telefonate, die an der Rezeption zwingend am Empfang im Beisein Dritter stattfinden, sollten nur mit Headset und ohne Informationen über die Krankheitsgeschichte in Verbindung mit Namensnennung erfolgen.

Eine Kontrolle der akustischen Gegebenheiten im Wartebereich und der Diskretionszone um den Empfang sollte in Eigenverantwortung periodisch geprüft werden. Ebenso sollte das Praxisteam trainieren, die Nennung von Diagnosen und Patientennamen bei Anwesenheit Dritter strikt zu vermeiden.

7.2 Verletzung der Informationspflicht durch Sozialleistungsträger

Mit Geltung der Datenschutz-Grundverordnung (DS-GVO) haben Verantwortliche bei Datenerhebungen eine weitreichende Informationspflicht. Für die Erhebung von personenbezogenen Daten bei der betroffenen Person ist die Informationspflicht in Artikel 13 DS-GVO geregelt. Dieser Pflicht kommen Sozialleistungsträger (z. B. Sozialamt, Jobcenter, Jugendamt) bislang nicht immer nach.

Artikel 13 DS-GVO lautet wie folgt: (1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;

b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;

c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;

e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und

f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

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

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

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

d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

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

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

(3) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

(4) Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

Ergänzende Regelungen zur Informationspflicht sieht (für den Bereich der Sozialleistungen) § 82 des Zehnten Buchs des Sozialgesetzbuchs vor.

Im Rahmen unserer Tätigkeit haben wir festgestellt, dass die erforderlichen Informationen (bislang) nicht immer erteilt wer-

den. In diesem Zusammenhang weisen wir auch darauf hin, dass bestimmte Informationen (z. B. Art. 13 Absatz 1 Buchstaben c und e, Absatz 2 Buchstaben a und e DS-GVO) nicht für das gesamte Landratsamt bzw. die gesamte Stadt einheitlich sein dürften, sondern in jedem Amt unterschiedlich sein können – und sogar innerhalb eines Amts können bei Datenerhebungen zu verschiedenen Zwecken unterschiedliche Informationen erforderlich sein.

Wir bitten um Beachtung. Erläuterungen zur Informationspflicht können Sie dem Kurzpapier Nr. 10 der Datenschutzkonferenz „Informationspflichten bei Dritt- und Direkterhebung" entnehmen (auf unserer Internetseite abrufbar unter www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2017/08/DSK_KPNr_10_Informationspflichten.pdf).

7.3 Vorlage des Personalausweises und Anforderung von Kontoauszügen beim Sozialamt

Sozialhilfeträger dürfen zur Überprüfung der Identität die Vorlage des Personalausweises verlangen. Des Weiteren ist davon auszugehen, dass sie zur Überprüfung der Einkommens- und Vermögensverhältnisse die Kontoauszüge jedenfalls der letzten drei Monate auch ohne konkreten Verdacht des Leistungsmissbrauchs anfordern dürfen. Hierbei ist jedoch Folgendes zu beachten:

- Bei Anträgen auf Sozialhilfeleistungen müssen dem Sozialamt die erforderlichen Unterlagen vorgelegt werden, um das Vorliegen der Anspruchsvoraussetzungen feststellen zu können. Dies schließt die Überprüfung der Identität ein. Zur Kontrolle der Personalien können Mitarbeiter des Sozialamts daher die Vorlage eines gültigen Passes oder Personalausweises verlangen. Zur Identifizierung und zur Aufgabenerfüllung des Sozialamts ist eine Kopie des Dokuments in der Akte aber grundsätzlich nicht erforderlich. Vielmehr dürfte regelmäßig ein dort oder auf dem Antragsformular anzubringender 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.

- Das Bundessozialgericht hat sich in zwei Urteilen (Urteil vom 19. September 2008, Az. B 14 AS 45/07 R, und Urteil vom 19. Februar 2009, Az. B 4 AS 10/08 R) zu der lange Zeit umstrittenen Frage der Zulässigkeit der Anforderung von Kontoauszügen geäußert. Danach ist die Anforderung der Kontoauszüge jedenfalls der letzten drei Monate bei der Beantragung von Leistungen nach dem Zweiten Buch des Sozialgesetzbuchs auch ohne konkreten Verdacht des Leistungsmissbrauchs zulässig.

  Dies dürfte grundsätzlich auch für den Bereich der Sozialhilfe gelten.

  Die Obliegenheit, Kontoauszüge vorzulegen, gilt allerdings nicht in vollem Umfang für die Ausgabenseite, das heißt für die Frage, wofür der Leistungsbezieher seine Mittel verwendet. Eine Einschränkung ergibt sich hier für besondere Arten personenbezogener Daten (inzwischen besondere Kategorien personenbezogener Daten gemäß Artikel 9 der Datenschutz-Grundverordnung). Dies sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben (inzwischen außerdem genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person und Daten der sexuellen Orientierung einer natürlichen Person). Geschützt ist die Geheimhaltung des Verwendungszwecks bzw. des Empfängers der Überweisung. Dementsprechend dürfen etwa Angaben

über Gewerkschaftsbeiträge, Spenden an Kirchen oder an politische Parteien hinsichtlich des Empfängers, nicht aber der Höhe, geschwärzt werden. Lediglich für den Fall, dass sich aus den insoweit geschwärzten Kontoauszügen eines Leistungsbeziehers ergibt, dass in auffälliger Häufung oder Höhe Beträge überwiesen werden, ist nach Auffassung des Bundessozialgerichts im Einzelfall zu entscheiden, inwieweit ausnahmsweise doch eine Offenlegung auch des bislang geschwärzten Adressaten gefordert werden kann.

Die Jobcenter müssen auf die Möglichkeiten der Schwärzung der Adressaten auf der Ausgabenseite der Kontoauszüge bereits bei ihrem Mitwirkungsbegehren hinweisen.

Dies gilt unseres Erachtens auch für die Sozialämter.

Die Sozialämter in Baden-Württemberg sollten ihre Verwaltungspraxis (z. B. ihre Formulare) den obigen rechtlichen Vorgaben zeitnah anpassen.

8. Schule und Hochschulen

8.1 Datenschutzbeauftragte an öffentlichen Schulen in BW – wie „gemeinsam“ darf es denn sein?

Das Ministerium für Kultus, Jugend und Sport strebt mit seiner Regelung zur verpflichtenden Benennung schulischer Datenschutzbeauftragter an öffentlichen Schulen durch die europäische Datenschutz-Grundverordnung eine aus seiner Sicht ressourceneffektive und kostenneutrale Lösung an.

Mit Blick auf die praktische Umsetzbarkeit sowie die generelle Rechtskonformität der Lösung bleiben jedoch Fragen offen.

Mit Geltung der Datenschutz-Grundverordnung (DS-GVO) seit dem 25. Mai 2018 besteht nun auch für öffentliche Schulen, wie für alle anderen öffentlichen Stellen, die Pflicht zur Benennung eines Datenschutzbeauftragten (DSB).
Entgegen der Regelungen verschiedener anderer Länder (wie z. B. Hessen) war die Benennung schulischer DSBs in Baden-Württemberg noch vor der DS-GVO gemäß § 10 LDSG a. F. eine „kann“-Regelung und erfolgte schriftlich durch die Schulleitung unter Mitbestimmung des schulischen Personalrates.

Mit Blick auf die Zahl von rund 5000 Bildungseinrichtungen in Baden-Württemberg stellt Artikel 37 Absatz 1 Buchstabe a DS-GVO, bezogen auf die öffentlichen Schulen, die Kultusverwaltung vor die Herkulesaufgabe einer verordnungskonformen Umsetzung der Bestellpflicht. Auch hier kämpft man mit der Frage nach dem „woher?“ der dafür erforderlichen Ressourcen, welche sich bisher an öffentlichen Schulen fast ausschließlich aus ambitionierten und engagierten Lehrkräften rekrutierten.

Das Stimmungsbild der bis dahin schon benannten schulischen DSBs hat sich nun aber mit den gestiegenen Anforderungen durch die DS-GVO spürbar getrübt wie meinem Fachreferat in Beratungsgesprächen vielfach rückgemeldet wurde.

Immer wieder schlägt im Dialog mit etablierten und erfahrenen schulischen DSBs die Frage nach einer möglichen persönlichen Haftung durch, welche viele der Funktionsträger noch immer umtreibt. Außerdem stellt sich nach wie vor beim Thema der Anerkennung im Vergleich mit anderen Funktionsträgern im Schulbereich eine gewisse Ernüchterung ein. Während beispielsweise eine Lehrkraft, welche das Schulnetzwerk betreut, sich über einen Deputatsnachlass freuen darf, geht der schulische DSB bei der Wahrnehmung seiner Aufgaben noch immer „leer“ aus und erhält im besten Fall eine der wenigen Poolstunden über die die Schulen ggf. verfügen.

Als Konsequenz haben bereits erste schulische DSBs schon vor dem 25. Mai 2018 „vorsorglich“ ihre Aufgabe „zurückgegeben“, wie mir aus Rückmeldungen bekannt wurde.

Die Lösung des Problems der fehlenden personellen und finanziellen Ressourcen bei der Bestellpflicht schulischer DSBs scheint das Kultusministerium in der großzügigen Auslegung des Wortlautes des Artikels 37 Absatz 3 DS-GVO gefunden zu haben: Hiernach können mehrere öffentliche Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe einen gemeinsamen Datenschutzbeauftragten benennen.

Basierend hierauf, bat das Kultusministerium in einem Schreiben vom Februar 2018 um die landesweite Umsetzung der Regelung, wonach jeweils zwei Personen in jeder Abteilung 7 der vier Regierungspräsidien und jeweils eine Person in jedem Staatlichen Schulamt bestimmt werden sollen, welche dann als DSB für die ihrer direkten Aufsicht unterliegenden Schu-

len benannt werden. Die für die jeweilige Schule als DSB benannte Person solle dann den Schulen mitgeteilt werden, damit diese deren Kontaktdaten gemäß Artikel 37 Absatz 7 DS-GVO veröffentlicht und der Aufsichtsbehörde mitteilt.
Bereits bestellte DSBs an den Schulen könnten entsprechend berücksichtigt werden. Dem Schreiben ist weiter zu entnehmen, dass die bestimmten Personen über ihre Aufgabe als DSB durch die Behörde noch zu informieren seien.

Diese Regelung scheint mir schon bei der Benennung eines Mitarbeiters der Schulaufsicht als schulischem DSB fraglich, ergibt sich doch hier ein möglicher Interessenkonflikt, welchen es gemäß Artikel 38 Absatz 6 DS-GVO zu verhindern gilt. Die Weisungsbefugnis und ggf. Durchsetzungskraft der Schulaufsicht gegenüber der Schulleitung steht hier dem ausschließlich beratenden Charakter des DSB gegenüber. Auch fordern die Regularien der DS-GVO in Bezug auf die Benennung eines DSBs durch Artikel 37 Absatz 5 DS-GVO eine berufliche Qualifikation und Fachwissen auf dem Gebiet des Datenschutzrechts. Da in der besagten Regelung des Ministeriums keinerlei Aussagen über die fachliche Qualifikation der zu bestimmenden Personen getroffen wurde, bleibt es fraglich ob und wodurch eine solche Qualifikation verifiziert wurde.

Erste Rückfragen verschiedener benannter DSBs bei den Staatlichen Schulämtern an meine Dienststelle zeichnen hier das Bild eines nur dürftigen Know-How der Funktionsträger. Wie wichtig aber die Fachkunde der schulischen DSBs ist, zeigt sich alleine schon beim Thema der Datenschutz-Folgenabschätzung (DSFA), zu welcher der DSB beratend hinzugezogen werden kann und deren Prozess er begleitet.

Es ist ohnehin fraglich, ob sich regelungsbedingt nun noch die eigentliche Kernaufgabe des schulischen DSB, die Unterrichtung und Beratung der Schulleitung, durch die herbeigeführte räumliche Trennung zur Schule wahrnehmen lässt. Letztlich kommen an den verschiedenen Schulen verschiedene Verfahren zur Verarbeitung personenbezogener Daten zum Einsatz, die ein DSB „vor Ort" deutlich besser kennt.

Die Erfüllung einer weiteren bedeutsamen Aufgabe des schulischen DSB kommt durch diese Regelung meines Erachtens ebenfalls weitgehend zu kurz: Gemäß Artikel 37 Absatz 1 Buchstabe b DS-GVO obliegt auch dem schulischen DSB die Sensibilisierung und Schulung der Lehrkräfte und ggf. des weiteren Schulpersonals, wie z. B. der Schulsekretärin oder des Hausmeisters. Beispielhaft sei hier eine gemeldete Datenpanne erwähnt. Am Ende der Beratung dazu empfahl meine Dienststelle eine Sensibilisierung in Form eines Vortrages des schulischen DSB auf einer Schulkonferenz. Eine solche Maßnahme lässt sich bei einer solchen Vielzahl von Schulen, für welche sich ein DSB dank dieser Regelung nun verantwortlich zeichnet, nur schwer stemmen.

Leider beschreitet das Kultusministerium durch die getroffene Regelung zur Umsetzung der verpflichtenden Benennung schulischer DSBs durch die DS-GVO nun einen vordergründig einfachen Weg. Anstatt den schulischen DSB „vor Ort" nun fest in der Schulstruktur zu etablieren, lagert man diese Aufgabe nun zentral an die Schulaufsicht aus. Neben einem möglichen Interessenskonflikt durch die Benennung von Mitarbeitern der Schulaufsicht zu schulischen DSBs scheint mir die durch diese Regelung gegebene fehlende Nähe zur Schule wesentlich gravierender. Eine angemessene Unterstützung der Schulleitung bei datenschutzrechtlichen Fragen und Vorhaben gelingt nur durch einen ansässigen DSB und dessen Kenntnis der Strukturen und des Umfelds der Schule. Dies gilt auch für die in Artikel 37 Absatz 1 Buchstabe b DS-GVO vorgesehenen Sensibilisierungs- und Schulungsmaßnahmen aller an den Verarbeitungsvorgängen beteiligten Mitarbeiter der Schule, die sich bei einer Zuständigkeit des DSBs im schlimmsten Fall für mehr als hundert Schulen nicht umsetzen lässt. Zu dieser in meinen Augen fraglichen

Umsetzung der Bestellpflicht schulischer DSB habe ich das Kultusministerium in einem Schreiben um Stellungnahme gebeten. Hierbei habe ich der Kultusverwaltung auch meine Unterstützung beim Finden einer adäquaten Lösung angeboten, welcher es mit Blick auf die gestiegenen Beratungsanfragen durch Schulen an meine Dienststelle dringend bedarf.

Update: Entsprechende Stellen wurden im Nachtragshaushalt bewilligt. Ich hoffe, dass dies zu einer besseren Aufgabenwahrnehmung beitragen wird.

8.2 Auskunftsrecht gegenüber Schulen

Auskunft über die Daten zur eigenen Person ist ein wesentliches Recht der betroffenen Person, auch unter der DS-GVO (vgl. deren Artikel 15).

In meinem 33. Tätigkeitsbericht 2016/2017 habe ich mich damit befasst, dass ein ehemaliger Studierender Auskunft bei der Hochschule beantragt hatte (dort Nummer 8.6 „Langer Weg zur Auskunft", S. 111 f.; LT-Drs. Nr. 16/3290). Hier geht es um Auskunft von einer öffentlichen Schule.

Im Rahmen des Beschwerdeverfahrens hat meine Dienststelle die Schule als Verantwortliche u. a. auf folgende wesentlichen Punkte hingewiesen:

„Negativauskunft"

Die Pflicht zur Auskunft umfasst wie bisher auch eine „Negativauskunft". Der Verantwortliche muss also dem Antragsteller mitteilen, wenn keine diesen betreffenden personenbezogenen Daten verarbeitet werden. Das ergibt sich aus Artikel 15 Absatz 1 Halbsatz 1 DS-GVO.

Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden (Artikel 15 Absatz 1 Halbsatz 1 DS-GVO).

Auskunft über die Empfänger der Daten

Die betroffene Person hat nach Artikel 15 Absatz 1 Halbsatz 2 Buchstabe c DS-GVO ein Recht auf Auskunft über die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden.

Im Sinne der Datenschutz-Grundverordnung bezeichnet der Ausdruck „Empfänger" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. (Artikel 4 Nummer 9 Satz 1 DS-GVO)

Wenn es keine Empfänger von den Antragsteller betreffenden personenbezogenen Daten gibt, besteht die o. g. Pflicht zur „Negativauskunft" auch insoweit.

Zeitrahmen

Der Verantwortliche hat der betroffenen Person die Auskunft unverzüglich zu erteilen, grundsätzlich jedenfalls innerhalb eines Monats nach Eingang des Antrags, oder die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags, über die Ablehnung des Antrags zu unterrichten.

Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag gemäß den Artikeln 15 bis 22 DS-GVO ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Verantwortliche unterrichtet die betroffene Person innerhalb eines Monats nach Eingang

des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung. (Artikel 12 Absatz 3 Sätze 1 bis 3 DS-GVO)

Wird der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen. (Artikel 12 Absatz 4 DS-GVO)

Artikel 12 Absatz 3 Satz 1 DS-GVO bezieht sich auch auf das Erteilen der Auskunft. Artikel 12 Absatz 4 DS-GVO bezieht sich auch auf eine Ablehnung des Antrags (auf Auskunft). Dafür spricht auch Erwägungsgrund 59 Satz 3 der DS-GVO, wonach der Verantwortliche verpflichtet werden sollte, den Antrag der betroffenen Person unverzüglich, spätestens aber innerhalb eines Monats zu beantworten und ggf. zu begründen, warum er den Antrag ablehnt.

Die Verantwortlichen müssen Auskunftsanträge betroffener Personen unverzüglich und auch inhaltlich rechtmäßig bearbeiten.

9. Privater Datenschutz

9.1 Wie mein Name an der Tür? – Offenlegung der Bewohnernamen auf Klingelschildern

Viele Wohnungsnutzer betrachten es als freundlichen Service, wenn Ihr Vermieter oder Hausverwalter an der Klingel ein Klingelschild mit ihrem Namen anbringt. Spätestens, wenn der Bewohner dies nicht wünscht, stellt sich jedoch die Frage, ob im Anbringen der Klingelschilder eine rechtswidrige Datenverarbeitung liegt.

9.1.1 Das Klingelschild als Datenverarbeitung

Zunächst bleibt festzuhalten, dass das Anbringen von Klingelschildern mit den Namen der Bewohner in der Regel in den sachlichen Anwendungsbereich der Datenschutz-Grundverordnung fällt.

Die Datenschutz-Grundverordnung gilt nach ihrem Artikel 2 Absatz 1 „für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen". Der Ausdruck Dateisystem bezeichnet nach Artikel 4 Nr. 6 DS-GVO „jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geographischen Gesichtspunkten geordnet geführt wird".

Unabhängig davon, ob ein Klingelschild aus einer an ein Rechnersystem angeschlossenen elektronischen Anzeige oder nur aus einem von hinten beleuchteten Stück Papier besteht, wird jedenfalls bei größeren Wohneinheiten gelten, dass die Namen der Bewohner der Mieterkartei des Vermieters oder einer entsprechenden Datensammlung der Hausverwaltung entnommen sind. Wenn diese Sammlung z. B. nach der Wohnungsnummer oder alphabetisch nach den Namen der Mieter sortiert ist und ein Mindestmaß an Strukturierung aufweist, ist sie als Dateisystem im Sinne der Datenschutz-Grundverordnung anzusehen. Die so gespeicherten Namen werden durch ihre Wiedergabe auf den Klingelschildern allen Passanten und Besuchern des Hauses offengelegt und somit in nichtautomatisierter Weise verarbeitet. Also gilt dafür die DS-GVO.

Als Rechtsgrundlage dieser Verarbeitung personenbezogener Daten wird häufig die Interessenabwägungsklausel aus Artikel 6 Absatz 1 Unterabsatz 1 lit. f DS-GVO einschlägig sein. Hiernach ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Ein berechtigtes Interesse des Vermieters oder der Hausverwaltung, das die Namensangabe auf dem Klingelschild erforderlich macht, dürfte in der Regel fehlen. Diese Stellen haben Kenntnis von der jeweiligen Wohnungsnummer, sodass deren Angabe auf dem Klingelschild für die Wahrung ihrer Interessen ausreicht. Artikel 6 Absatz 1 Unterabsatz 1 lit. f DS-GVO schützt allerdings auch berechtigte Interessen Dritter. Z. B. können Paketzusteller und unangemeldete Besucher ohne kriminelle Absichten und Kenntnis der Wohnungsnummer ein berechtigtes Interesse daran haben, die Klingel eines bestimmten Bewohners zu finden. Wünscht der Bewohner jedoch nicht, dass sein Name auf dem Klingelschild erscheint und selbst für Passanten ohne Besuchsabsichten sichtbar ist, so dürfte sein Interesse an der Wahrung seiner Privatsphäre in aller Regel überwiegen. Wenn dies dazu führt, dass ein Postdienst-

leister ein Paket oder ein Übergabeeinschreiben nicht zustellen kann, so ist dies in erster Linie Sache des Bewohners (denn ihn alleine treffen die möglichen negativen Folgen).

Einem im Notfall verständigten Rettungsdienst kann durch Mitteilung der Wohnungsnummer ein schnelles Eingreifen ermöglicht werden. Für die Praktikabilität eines solchen Vorgehens spricht auch, dass es in mehreren europäischen Ländern üblich ist, Klingelschilder nur mit Wohnungsnummern zu versehen.

9.1.2 Das Klingelschild als Datenschutzverstoß?

Der für die Beschriftung der Klingelschilder verantwortliche Vermieter oder Hausverwalter hat, bevor er zur Tat schreitet, die Interessenabwägung gem. Artikel 6 Absatz 1 Unterabsatz 1 lit. f DS-GVO zu treffen. Vor Inkrafttreten der Datenschutz-Grundverordnung genügte es hierfür nach § 28 Absatz 2 Nr. 2 BDSG a.F. zu prüfen, ob Grund zu der Annahme eines schutzwürdigen Geginteresses des betroffenen Bewohners besteht. Da mit Namen versehene Klingelschilder in Deutschland bislang allgemein üblich sind, durfte der Verantwortliche davon ausgehen, dass die Namensnennung auf dem Klingelschild auch im Interesse des Bewohners ist. Entsprechende Klingelschilder aus dieser Zeit brauchen nicht entfernt zu werden, solange der betroffene Bewohner der Namensnennung auf seinem Klingelschild nicht widerspricht (vgl. Art. 21 DS-GVO).

Nach Artikel 6 Absatz 1 Unterabsatz 1 lit. f DS-GVO muss der Vermieter oder Hausverwalter seit dem 25.5.2018 die Interessenlage in Neufällen genauer prüfen. Ein der Namensnennung entgegenstehender Wille des betroffenen Bewohners ist von Anfang an auch dann beachtlich, wenn dafür zunächst keine Anhaltspunkte bestehen. Vermieter und Hausverwalter sollten die Bewohner daher vor ihrem Einzug wählen lassen, ob sie ein Klingelschild mit ihrem Namen oder mit einer bloßen Wohnungsnummer wünschen. Der Bewohner kann jederzeit und ohne Angabe besonderer Gründe die Entfernung seines Namens vom Klingelschild verlangen.

9.2 Der Adresshandel – künftig nur noch mit Einwilligung

Die DS-GVO enthält – im Gegensatz zum BDSG-alt – keine ausdrückliche Regelung zum Adresshandel mehr: Das sog. „Listenprivileg", die transparente Übermittlung sowie die transparente Nutzung des § 28 BDSG-alt sowie die Spezialregelungen des § 29 BDSG-alt sind weggefallen. Der Adresshandel wurde somit weiter eingeschränkt. Stimmen vor allem aus der Werbewirtschaft, wonach sich mit dem Wirksamwerden der DS-GVO rechtlich mehr oder weniger nichts verändert habe, können daher getrost als Märchen oder bestenfalls als Wunschdenken bezeichnet werden. Die Zulässigkeit der Verarbeitung personenbezogener Daten zum Zwecke des Adresshandels richtet sich in der DS-GVO demnach mangels Spezialregelung nach den allgemeinen Vorschriften.

Definition des Adresshandels

Oftmals wird unter Adresshandel nur die Generierung und Vermarktung von Daten (Name, Adresse) verstanden, die für die Kontaktaufnahme mit einer Person – in der Regel zur werblichen Ansprache per Post – erforderlich sind (gilt auch für den Handel mit Unternehmensdaten, wenn diese Daten einen konkreten Ansprechpartner beinhalten). Unerheblich ist dabei, ob die Daten verkauft, vermietet oder in sonstiger Form einem Dritten überlassen werden.

„Moderner" Adresshandel ist aber viel, viel mehr – und die Kunden sind längst nicht mehr nur Werbetreibende. Es geht zum Beispiel um crossmediale Kommunikati-

onsstrategien (einschließlich Online Behavioral Advertising), Zielgruppenanalysen, Adressverifizierung und Datenbereinigung, Profiling, in enger Zusammenarbeit mit Wirtschaftsauskunfteien im Rahmen von Adressbewertungen um die wirtschaftliche Einstufung von Wohngegenden (wichtig für Scoring und Bonitätsauskünfte). Adresshändler wissen viel über die Menschen, die hinter den Adressdaten stehen. Die hinzugespeicherten Zusatzinformationen – Profiling, Werbe- oder Adress-Scoring – (z. B. durch Kundenbindungs- und Treueprogramme) sind das, was den Wert von Adressdaten ausmacht. Adresshändler handeln also eher mit Subjektdaten, die dann zu Objekten u. a. von Werbetreibenden werden. Es geht um Beeinflussung, Prognosen hinsichtlich des Kaufverhaltens, ja, vielleicht sogar häufig um Manipulation.

So bietet ein großer deutscher Adresshändler (mit dem gelben Posthorn im Logo) u. a. folgende Dienstleistung an: „microdialog finance – Informationen zum Verhalten von Privatkunden im Versicherungs-, Banken- und Finanzmarkt" – der Übergang vom Adresshändler zur Wirtschaftsauskunftei ist offensichtlich fließend.

Was ist datenschutzrechtlich erlaubt?

Die Einwilligung. Unproblematisch ist die Datenverarbeitung, wenn der Betroffene nach Art. 6 Abs. 1 Satz 1 Buchstabe a DS-GVO vorher ausdrücklich und informiert in den Adresshandel eingewilligt hat. Sehr beliebt sind hier bei allen renommierten Adresshandels- und Marketingunternehmen nach wie vor Gewinnspiele, vor allem Online-Gewinnspiele, wobei die Gewinnspiel-Veranstalter gerne im Ausland sitzen, vor allen in Großbritannien. In einem Fall konnten wir nun herausfinden, dass es den Veranstalter gar nicht gibt. Es ist auch davon auszugehen, dass die vorgelegten Double-Opt-in`s oft frei erfunden sind. Wir bewegen uns hier also nicht selten im kriminellen Bereich. Weitere, intensive Untersuchungen der Aufsichtsbehörde werden folgen.

Unter „Einwilligung" versteht die DS-GVO entsprechend ihrem Art. 4 Nr. 11 jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutig bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Maßgeblich sind die Art. 7 f. DS-GVO, die Erwägungsgründe 32, 33, 38, 42, 43, 65 und 171 sowie §§ 27, 51 BDSG.

Eine Einwilligung ist demnach nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht, der 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 hinzuweisen ist (so bereits zum BDSG-alt: OLG Frankfurt am Main, 24.01.2018 – 13 U 165/16). Die Einwilligung muss also stets für den konkreten Fall und in Kenntnis der Sachlage erteilt werden (BGH, Urt. v. 25.10.2012, I ZR 169/10, juris Rn. 24; zum alten Recht). Insbesondere muss klar sein, welche Produkte oder Dienstleistungen welcher Unternehmen sie konkret erfasst (BGH, a. a. O.) und auf welchem Kommunikationsweg (z. B. Post, E-Mail, Telefon, Telefax) die werbliche Ansprache erfolgen soll.

Soll die Einwilligung auf weitere Unternehmen erstreckt werden, so müssen diese in der Einwilligungserklärung mit Namen und Adresse aufgeführt sein, weil sonst – gerade bei einer Vielzahl von begünstigten Unternehmen – die Möglichkeit des jederzeitigen Widerrufs der Einwilligung gegenüber dem Werbenden unangemessen beschränkt wird (OLG Koblenz, Urt. v. 26.3.2014, 9 U 1116/13, juris Rn. 39 m. w. N.; zum alten Recht). Pauschale Einwilligungserklärungen genügen diesen Anforderungen jedenfalls nicht. Wenn neben dem Adresshandel auch andere Zwecke verfolgt werden (siehe oben in der Definition), müssen diese selbstverständlich

aufgeführt werden, nur dann umfasst die erteilte Einwilligung auch diese Zwecke.

Die Interessenabwägung. Fraglich ist, ob der Adresshandel auch im Rahmen einer Interessenabwägung nach Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO zulässig sein kann.
Um die Verarbeitung personenbezogener Daten auf ein berechtigtes Interesse stützen zu können, müssen drei Voraussetzungen gegeben sein.

1. Der für die Verarbeitung der personenbezogenen Daten Verantwortliche oder ein Dritter haben ein berechtigtes Interesse (dieses kann rechtlich, wirtschaftlich, tatsächlich oder ideell sein) an der Datenverarbeitung.
2. Die Verarbeitung ist zur Wahrung des berechtigten Interesses erforderlich.
3. Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen nicht.

Erst wenn diese drei Voraussetzungen kumulativ vorliegen, kann eine Verarbeitung auf Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO und damit das berechtigte Interesse gestützt werden.

Der gerade von der Werbewirtschaft geäußerte Hinweis der gewissen „Privilegierung" auch des Adresshandels als berechtigtes Interesse durch ErwG 47 greift hier nicht: Dort ist nur von der Direktwerbung die Rede, nicht auch vom Adresshandel. Und der Adresshandel ist kein Unterfall der Direktwerbung, sondern etwas Anderes. Eine Aktivität, die als Adresshandel zu werten ist, kann nicht zugleich Werbung sein. Umgekehrt gilt dasselbe (Simitis, Bundesdatenschutzgesetz, 8. Aufl., Rn. 75 zu § 29 BDSG-alt). Auch das Widerspruchsrecht nach Art. 21 Abs. 2 DS-GVO betrifft einzig die Direktwerbung, nicht auch den Adresshandel. Dass es sich hierbei um unterschiedliche Nutzungszwecke handelt und nicht etwa der Adresshandel als Unterfall der Werbung anzusehen ist, hatte auch § 28 Abs. 3 Satz 1 BDSG-alt klargestellt.

Gleichwohl wird man den klassischen Adresshandel als berechtigtes wirtschaftliches Interesse des Adresshandelsunternehmens bejahen können, ebenso des Dritten, also des Unternehmens, das die Adressdaten z. B. für eine Werbekampagne anmietet. Auch eine Erforderlichkeit könnte gegeben sein, wobei dem Adresshändler auch der Weg über eine Einwilligung offen steht. Die Tatsache, dass der Verantwortliche oder ein Dritter ein solches berechtigte Interesse an der Datenverarbeitung geltend machen kann, bedeutet aber noch nicht, dass die Verarbeitung auch zulässig ist.

Entscheidend ist nun die Interessenabwägung: Die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person dürfen nicht überwiegen; dabei sind die vernünftigen Erwartungen der betroffenen Personen, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen. Insbesondere dann, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss, könnten die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen überwiegen (ErwG 47).

So wird es regelmäßig beim Adresshandel sein: Der Betroffene geht gerade nicht davon aus, dass ein Unternehmen, mit dem er geschäftlichen Kontakt hat, ungefragt seine Kundendaten an andere, ihm völlig fremde Unternehmen verkauft oder vermietet und er von dort plötzlich unerwünschte Werbung bekommt. Zudem hat der Betroffene – das zeigt die jahrelange Praxis der Datenschutzaufsichtsbehörde – ein sehr starkes Interesse daran, dass seine Kundendaten nicht zu einer grenzenlos gehandelten Ware verkommen, auf die er keinerlei Einfluss mehr hat. Der Betroffene hat auch aus dem Gesichtspunkt der Transparenz (Art. 5 Abs. 1 Buchstabe a DS-GVO) heraus ein überwiegendes Interesse daran, Herr (oder Frau) seiner Daten zu bleiben. Dies gilt umso mehr bei angereicherten Adressdaten, die regelmä-

ßig ein ziemlich konkretes Persönlichkeitsprofil des Betroffenen abbilden: Der Handel mit diesen Daten stellt einen schweren Persönlichkeitseingriff dar, auch hier geht die Interessenabwägung zu Gunsten des Betroffenen aus.

Aufgrund dieser Sachlage wird nun teilweise versucht, verschiedene Formen des Adresshandels in die Datenschutzhinweise nach Art. 13, 14 DS-GVO aufzunehmen, um die Betroffenen sozusagen „bösgläubig" zu machen, weil sie ja mit dieser Datenverarbeitung dann rechnen müssen. Dieser Weg ist abwegig und unzulässig: Die Datenschutzhinweise nach Art. 13, 14 DS-GVO sind nicht dafür gedacht, zusätzliche Erlaubnisnormen für Datenverarbeitungen zu schaffen oder gar das Ergebnis einer Interessenabwägung nach Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO vorwegzunehmen (bzw. vollendete Tatsachen zu schaffen).

Die Abwägung beim Adresshandel geht also zu Gunsten der schützenswerten Interessen sowie Grundrechte und Grundfreiheiten des Betroffenen aus. Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO scheidet als Rechtsgrundlage für den Adresshandel folglich regelmäßig aus.

Grundsätzlich zulässig ist der Adresshandel daher (nur noch) dann, wenn der Betroffene zuvor ausdrücklich und informiert eingewilligt hat. Diese Adressen sind dann auch bei entsprechend umfassender Einwilligung anmietbar oder verkäuflich.

Vom Betroffenen selbst veröffentlichte Daten. Teilweise wird argumentiert, Art. 9 Abs. 2 Buchstabe e DS-GVO sei entsprechend auch beim Adresshandel heranzuziehen. Wenn also der Betroffene seine Daten – z. B. seine Adresse – bewusst öffentlich gemacht hat, dann könne man diese Daten auch für den Adresshandel abgreifen. Diese Argumentation ist abzulehnen. Zum einen betrifft Art. 9 Abs. 2 Buchstabe e DS-GVO den Umgang mit besonderen Kategorien von Daten. Zum anderen ist auch für die Anwendung dieser Norm ein einschlägiger Erlaubnistatbestand des Art. 6 DS-GVO erforderlich.

Außerdem liegt zwar regelmäßig eine bewusste, aber auch eine zweckgebundene Veröffentlichung vor: Wenn jemand seine Adresse samt Telefonnummer in ein Telefonbuch eintragen lässt, willigt er darin ein, von anderen kontaktiert werden zu können. Er beabsichtigt damit nicht, seine Daten für die unbegrenzte Datenerhebung von Adresshändlern freizugeben. Für die Angaben in einem gesetzlich erzwungenen Impressum ist dies schon lange allgemeine Meinung.

Die rechtlichen Grenzen für den Adresshandel wurden mit der DS-GVO (endlich!) wesentlich enger gezogen als bisher. Adresshandel wird künftig regelmäßig nur noch mit einer vorherigen, informierten Einwilligung zulässig sein. Der LfDI wird dies entsprechend umsetzen. Die weitere Entwicklung – etwa auch durch einschlägige Rechtsprechung – bleibt aber auch hier abzuwarten.

9.3 Die wertlose Bonitätsbewertung

Eine Wirtschaftsauskunftei speichert zu einem Einzelkaufmann neben dessen Erreichbarkeitsdaten auch dessen Kontonummer, dass dieser verheiratet und geschäftsfähig sei und seine Verbindlichkeiten regelmäßig begleiche. Die Auskunftei rechtfertigt diese Speicherungen damit, man benötige diese Angaben, um Anfragen zur Bonität des Unternehmens beantworten zu können.

Nach Artikel 6 Absatz 1 lit. f der EU-Datenschutzgrundverordnung (EU-DSGVO) sind Wirtschaftsauskunfteien grundsätzlich berechtigt, Angaben zu Personen und zu Unternehmen zu erheben, zu sammeln, zu speichern und ggf. an Dritte zu übermitteln, wenn dafür ein berechtigtes Interesse besteht, dem keine höherrangigen Interessen der Betroffenen entgegenste-

hen. Das betrifft entsprechend dem Erwägungsgrund 47 insbesondere gesicherten Angaben, die auf eine Gefahr für die Wirtschaft schließen lassen, also Zahlungsunwilligkeit, Zahlungsunfähigkeit und Insolvenz (sog. Bonitätsnegativmerkmale). Zu Unternehmen in weiterem Sinne können auch sonstige Angaben, nämlich solche, die nicht auf ein Risiko schließen lassen, aber gleichwohl geeignet sind, dessen Bonität zu bewerten, (sog. Positivmerkmale) erfasst und verarbeitet werde. Bei Einzelkaufleuten und Kleinstgesellschaften werden davon sogar Angaben zum Inhaber oder zum Geschäftsführer umfasst, da hier zwischen dem Unternehmen selbst und den „hinter" ihm stehenden Personen eine enge wirtschaftliche Bindung besteht. Ausgenommen davon sind jedoch Informationen aus der Privatsphäre dieser Personen.

In dem uns vorgelegten Fall waren die Speicherungen durch die Auskunftei rechtswidrig. Die Erreichbarkeit des Unternehmens und Selbstverständlichkeiten, etwa dass der Inhaber geschäftsfähig und generell zahlungsfähig ist, sind für sich genommen nicht für die Bonitätsbewertung erforderlich. Diese Angaben werden nicht benötigt, um Anfragen Dritter dergestalt zu bescheiden, dass nichts Negatives vorliegt. Dazu würde die Auskunft – wie bei den meisten Personen, die die Auskunftei gar nicht kennt – genügen, dass der Betroffene der Auskunftei nicht bekannt ist, es also keine aussagekräftigen – nachteiligen – Speicherungen gibt. Für die „positive" Einschätzung des Unternehmens sind derartige Angaben ebenfalls nicht erforderlich, da nach der Rechtsprechung stets ein „gutes Bonitätszeugnis" erteilt werden muss, wenn der Auskunftei keine oder nicht ausreichend aussagekräftige Erkenntnisse bekannt sind.

Vergleichbares gilt für die Information, dass der Geschäftsmann verheiratet ist. Diese Angabe gehört zu seiner Privatsphäre und geht potentielle Vertragspartner nichts an. Auch die Bankverbindung darf in diesem Zusammenhang nicht offenbart werden. Bezüglich dieser Angabe geht das „Geheimhaltungsinteresse" des Unternehmers vor.

Wir haben die Auskunftei nach Art. 58 Abs. 1 lit. d EU-DSGVO auf die Unzulässigkeit ihrer Praxis hingewiesen und behalten uns vor, im Wiederholungsfall Verbote nach Absatz 2 dieser Vorschrift anzuordnen bzw. ein Bußgeld festzusetzen.

9.4 Die Chronik und der Datenschutz

Die DS-GVO hat nicht nur bei Unternehmen, sondern auch im familiären und gesellschaftlichen Bereich für viel Verunsicherung geführt. Im Berichtszeitraum erreichten uns mehrere Anfragen zu dem Thema „Verfassen einer Chronik".

Ein Arzt bat uns um Rat, dessen Stammbaum mütterlicherseits bis ins 12. Jahrhundert zurückreicht und dessen Familie eine Familienchronik pflegt. Er war aufgrund der DS-GVO so verunsichert, dass er die Fortführung der Familienchronik und der Traditionstreffen seiner Familie in Gefahr sah. Da die Veröffentlichung der Chronik nur innerhalb der Familie des Arztes erfolgt und es sich bei der von ihm und seiner Familie getätigten Ahnenforschung und Fortführung der Familienchronik um die Ausübung rein familiärer Tätigkeiten handelte, konnten wir den Anfragenden beruhigen: Die beschriebene Datenverarbeitung fällt nicht unter den sachlichen Anwendungsbereich der DS-GVO (vgl. Art. 2 Abs. 2 lit. c) DS-GVO). Die Verordnung macht der Familienchronik und den Traditionstreffen keinen Strich durch die Rechnung.

Anders verhält es sich bei der Beratungsanfrage eines pensionierten Bürgers, der die Geschichte seines Heimatdorfes veröffentlichen möchte. Der Pensionär beabsichtigte eine Chronik zu verfassen, die jedes Wohngebäude des Dorfes auflistet, damit die Historie der Dorfgemeinschaft für die Leser nachvollziehbar wird. Ein um-

fassendes Projekt für den Chronisten, bei dem es aus datenschutzrechtlicher Sicht einiges zu beachten gibt. In diesem Fall ist eine Erhebung personenbezogener Daten und deren Veröffentlichung in der Regel nur mit Einwilligung der Betroffenen möglich. Ausgenommen hiervon sind Daten von Personen der Zeitgeschichte und Informationen aus öffentlich zugänglichen Quellen, wie beispielsweise öffentliche Register, Zeitungen oder Archiven. Nach dem Landesarchivgesetz (LArchG) hat jedermann das Recht, Archivgut in öffentlichen Archiven nach Ablauf der Schutzfristen zu nutzen (§ 6 Abs. 1 LArchG). Davon erfasst ist auch die Recherche zur Erstellung einer Dorfchronik. Eine Nutzung von Archivgut ist jedoch dann einzuschränken, wenn Grund zur Annahme besteht, dass schutzwürdige Belange betroffener Personen oder Dritter beeinträchtigt werden (§ 6 Abs. 6 Nr. 2 LArchG). Dieser Schutz erstreckt sich auch auf Nachkommen oder sonstige Verwandte – insoweit lässt sich auch von einem postmortalen Datenschutz sprechen. Die Regelungen aus dem Archivrecht können für die datenschutzrechtliche Beurteilung für das Verfassen einer Dorfchronik sinngemäß herangezogen werden, da vom Chronisten gemäß Art. 6 Abs. 1 lit. f) DS-GVO die schutzwürdigen Belange der Betroffenen angemessen zu berücksichtigen sind. Wir hoffen, dass sich der Chronist von den datenschutzrechtlichen Anforderungen nicht abhalten lassen wird, die Geschichte seines Heimatdorfes zu Papier zu bringen und zu veröffentlichen und wünschen ihm hierfür viel Erfolg.

9.5 Der private Falschparker-Ermittler

Vielerorts bedienen sich Einkaufscenter, Supermärkte u.ä. privater Dienstleister, um die Benutzung der ihren Kunden zur Verfügung gestellten Privatparkplätze zu kontrollieren. Bei festgestellten Parkverstößen machen die privaten „Falsch-Parker-Ermittler" gegenüber den Fahrern und Haltern „Vertragsstrafen" geltend, welche in der Regel ein Vielfaches über den üblichen Parkgebühren liegen. Zur Durchsetzung dieser Vertragsstrafen werden diverse personenbezogene Daten erhoben und verarbeitet (Kennzeichen, Typ und Farbe des Fahrzeugs, Uhrzeit, Fotos vom Fahrzeug, Halterabfrage), so dass sich neben der originär zivilrechtlichen Frage nach der Anspruchsbegründung insbesondere auch datenschutzrechtliche Fragen stellen, mit denen sich viele Beschwerdeführer an mich wenden.

Hinsichtlich der Datenerhebung ist grundsätzlich folgendes festzustellen:

Bei der Einfahrt auf dem Parkplatz wird mit Hinweisschildern auf die Nutzungsbedingungen (Allgemeine Einstellbedingungen), die verpflichtende Benutzung von Parkscheiben, die Höchstparkdauer sowie das bei Verstoß gegen die Bedingungen fällige erhöhte Nutzungsentgelt (Vertragsstrafe) hingewiesen. Mit Abstellen des Fahrzeuges auf einem so beschilderten Kundenparkplatz kommt zwischen den jeweiligen Fahrern und den privaten Überwachungsunternehmen ein Nutzungsvertrag unter Geltung der Nutzungsbedingungen zu Stande. Bei der „Vertragsstrafe" handelt es sich somit um ein vertraglich vereinbartes Nutzungsentgelt. Da gem. Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO die Verarbeitung personenbezogener Daten rechtmäßig ist, wenn die Verarbeitung für die Erfüllung eines Vertrags erforderlich ist, ist hiernach die zur Durchsetzung des Nutzungsentgeltes erforderliche Datenerhebung als zulässig anzusehen.

Darüber hinaus ist die Datenerhebung hinsichtlich der Halterdaten – insbesondere die Halterabfrage beim Kraftfahrt-Bundesamt – nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO zulässig. Danach ist eine Verarbeitung personenbezogener Daten rechtmäßig, wenn diese „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich (ist), sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener

Daten erfordern, überwiegen (…).“ Derjenige, der sein Fahrzeug unbefugt auf ein Privatgrundstück abstellt, begeht verbotene Eigenmacht im Sinne von § 858 Abs. 1 BGB (BGH, Urteil vom 18.12.2015, Az. V ZR 160/14, Rz. 13). Der Fahrzeughalter ist insoweit Zustandsstörer, ihm ist als Halter die Störung zuzurechnen, die dadurch entsteht, dass das Fahrzeug von der Person, welcher er das Fahrzeug freiwillig zur Benutzung im Straßenverkehr überlassen hat, unberechtigt abgestellt wird (BGH, aaO., Rz. 22). Die zur Durchsetzung der sich hieraus ergebenden Ansprüche erforderliche Datenerhebung ist hinsichtlich der Halterdaten somit nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO zulässig.

Darüber hinaus ist die Halterabfrage beim Kraftfahr-Bundesamt auch nach § 39 Abs. 1 StVG zulässig, da „die Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt“ werden.

Zusammenfassend ist somit festzustellen, dass die beschriebene Datenerhebung durch private Überwachungsunternehmen als solches grundsätzlich nicht zu beanstanden ist.

Im Übrigen haben die Unternehmen sowohl bei der Datenerhebung als auch der -verarbeitung datenschutzrechtliche Bestimmungen zu beachten, deren Einhaltung von mir kontrolliert wird: So ist die Datenerhebung allein auf die zur Anspruchsdurchsetzung erforderlichen Daten zu beschränken; die Daten dürfen allein zu legitimen Zwecken wie z. B. im Rahmen des Forderungsmanagements weitergegeben werden; die Rechte der Betroffenen wie Auskunfts- und Löschanspruch sind seitens der verantwortlichen Unternehmen zu wahren, wobei die zulässig erhobenen Daten grundsätzlich auf Grund der steuer- und handelsrechtlichen Aufbewahrungsfristen nach Art. 17 Abs. 3 lit. b DS-GVO i.V.m. § 257 HGB, § 147 AO bis zu 10 Jahre aufzubewahren sind.

Ob das seitens der privaten Überwachungsunternehmen geltend gemachte erhöhte Nutzungsentgelt im Einzelfall tatsächlich besteht, ist eine zivilrechtliche Frage, welche der LfDI nicht klären kann. In jedem Fall sollte bei begründeten Einwendungen dem Anspruch qualifiziert, d. h. unter Nennung der Einwendungen, widersprochen werden, da ansonsten das Überwachungsunternehmen grds. berechtigt wäre, den Vorgang einer Wirtschaftsauskunftei zu melden. Im Übrigen überwache ich die Einhaltung der datenschutzrechtlichen Bestimmungen bei den verantwortlichen Unternehmen, wobei die zur Durchsetzung der zivilrechtlichen Ansprüche erforderliche Datenerhebung prinzipiell nicht zu beanstanden ist.

9.6 Datenschutz in Vereinen bei Organisation und Durchführung sportlicher Wettkämpfe

Was müssen Vereine bei der der Datenverarbeitung beachten, wenn sie sportliche Wettkämpfe organisieren und durchführen?

Vereine und deren Verbände veranstalten regelmäßig öffentliche Turniere, in denen Sportler eines Vereins oder mehrerer Vereine gegeneinander antreten und ihre Kräfte messen. Das Spektrum reicht vom vereinsinternen Wettkampf bis zur internationalen Meisterschaft.

Vor, während und nach diesen Ereignissen findet Datenverarbeitung statt. Wettkämpfe müssen organisatorisch vorbereitet und ordnungsgemäß durchgeführt werden. Die Vereine und Verbände selbst, aber auch die Presse und andere Akteure berichten öffentlich über sie.

Profisportler und Amateure, Kinder, Jugendliche und Erwachsene, behinderte und nichtbehinderte Menschen nehmen an solchen Veranstaltungen teil.

„Der Datenschutz" soll dies nicht verhindern oder erschweren. Dieses Grundrecht soll vielmehr alle Beteiligten davor schützen, dass ihnen durch unrechtmäßige Datenverarbeitung Nachteile entstehen.

Müssen alle Teilnehmer Einwilligungen unterschreiben, damit ein Wettkampf durchgeführt werden kann?

Nein. Die für die Organisation und Durchführung des Turniers erforderlichen Daten dürfen ohne Einwilligung verarbeitet werden, da der Turnierteilnahme regelmäßig eine vertragliche Verbindung zugrundeliegt, Art. 6 Abs. 1 lit. b DS-GVO. Lediglich, wenn personenbezogene Daten verarbeitet werden sollen, die für die Vertragserfüllung nicht erforderlich, sondern lediglich nützlich sind, wäre eine Einwilligung nötig. Es bietet sich an, auf die Verarbeitung nicht erforderlicher Daten zu verzichten, um den damit verbundenen Aufwand, aber auch das Risiko eines gem. Art. 7 Abs. 3 DS-GVO jederzeit möglichen Widerrufs der Einwilligung, zu vermeiden.

Müssen alle Teilnehmer über die Datenverarbeitung informiert werden?

Ja. Mit der Ausschreibung der Veranstaltung ist der Aufruf an Sportler und/oder Vereine verbunden, sich bzw. andere Teilnehmer unter Nennung von Namen, Alter, Sportart usw. anzumelden. Das ist eine Erhebung personenbezogener Daten entweder bei dem betroffenen Sportler selbst oder bei dessen Verein. Entsprechend ist gem. Art. 13 oder Art. 14 DS-GVO hierüber zu informieren.

Die Information kann mit einer Online-Ausschreibung verbunden (verlinkt) oder auf Wunsch zugesandt werden. Auch ein Aushang vor Ort während des Turniers mag für künftige Datenverarbeitungen sinnvoll sein.

Darf über das Ereignis berichtet werden?

Ja. Hier besteht ein berechtigtes Interesse der Vereine, Art. 6 Abs. 1 lit. f DS-GVO. Wer sich auf ein berechtigtes Interesse beruft, muss dieses bei der Information benennen und mit entgegenstehenden Interessen abwägen. Nur wenn und soweit die Interessen, Grundrechte, Grundfreiheiten der Betroffenen nicht überwiegen, darf vom Verein berichtet werden. Das wird regelmäßig der Fall sein. Presse und Rundfunk sind hinsichtlich einer Berichterstattung über den Wettkampf besonders privilegiert.

Das Ereignis kann Erfolge und Misserfolge, Verletzungen und Regelverstöße samt Sanktionen umfassen. Bei der Berichterstattung ist das öffentliche Informationsinteresse gegen berechtigte Vertraulichkeitserwartungen abzuwägen.

Die Schutzbedürftigkeit besonders von Kindern, aber auch von anderen besonderen Personengruppen ist zu beachten. Eine Veröffentlichung im Internet unter voller Namensnennung birgt Risiken für die Betroffenen. Ein so dokumentiertes (Fehl-) Verhalten kann ihnen künftig nachhängen. Es gibt außerdem Menschen, die bedroht werden und deren Vereinszugehörigkeit (und: erwartbarer künftiger Aufenthaltsort) daher nicht im Internet recherchierbar sein sollte. Das sind nur einige der Gründe, warum die Information vorab wichtig ist: Es kann besondere Umstände geben, die gegen eine Veröffentlichung sprechen, die dem Veranstalter aber nicht bekannt sind. Es sind mehrere Varianten denkbar, wie das berechtigte Interesse des Vereins, das Wettkampfgeschehen zu dokumentieren, mit den berechtigten Interessen insbesondere von Kindern in Einklang gebracht werden kann:

- Denkbar ist zunächst eine Pseudonymisierung. Es könnte gerade im Internet darauf verzichtet werden, immer den (vollen) Namen zu nennen. Stattdessen könnte die Startnummer oder z. B. eine Kombination aus dem Vornamen und dem ersten Buchstaben des Nachnamens ausreichend sein.
- Soweit doch der volle Name veröffentlicht werden muss, könnte sich die

Internet-Veröffentlichung darauf beschränken, die Daten in einem nicht ohne weiteres durchsuch- und maschinenlesbaren Format anzuzeigen. Also z. B. das (ohne Texterkennung) eingescannte Bild von der Ergebnisliste, nicht aber die durchsuchbare Datei selbst. Damit wäre gewährleistet, dass derjenige, der nach Ergebnissen bestimmter Wettkämpfe sucht, diese findet und „manuell lesen" kann. Wer aber nach Namen von Teilnehmern im Internet sucht oder automatisiert ausliest, findet die Ergebnisse nicht.

- Je geringer die Bedeutung des Ereignisses ist, desto schneller sollten die Informationen wieder aus dem Netz genommen werden.
- Negativ zu bewertende Ereignisse (Disqualifizierung, Aufgabe, Regelverstöße u. ä.) sollten gerade im Amateurbereich, bei Kindern u. ä. anonym genannt und begründet werden (z. B. „ein Teilnehmer musste wegen Verlassens der Strecke disqualifiziert werden"). Auch muss der Verstoß nicht immer detailreich geschildert werden. Eine Beleidigung etwa wörtlich zu zitieren geht sowohl zulasten des „Täters" als auch des „Opfers".

Je nach Informationsinteresse der Öffentlichkeit und Schutzwürdigkeit der Teilnehmer können die vorgeschlagenen Maßnahmen in unterschiedlicher Kombination angewandt werden.

Die Veranstalter benötigen keine Einwilligung der Teilnehmer, soweit die Datenverarbeitung für Organisation und Abwicklung des Wettkampfs erforderlich ist. Sie müssen die Teilnehmer aber über die beabsichtigte Datenverarbeitung umfassend informieren. Bei der Berichterstattung ist auf schutzwürdige Personengruppen und besondere Interessenlagen Rücksicht zu nehmen. Das gilt besonders bei Internetveröffentlichungen.

Näheres zu Informationspflichten ist in der Orientierungshilfe „Datenschutz im Verein nach der Datenschutzgrundverordnung (DS-GVO)", beschrieben.

- Siehe https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf.
- Ein Muster findet sich im Praxisratgeber „Datenschutz im Verein nach der DS-GVO", https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Praxisratgeber-für-Vereine.pdf.

Aus der Dienststelle

11.1 Personelles & Ressorts

Im Jahr 2018 stand meine Dienststelle nicht nur vor der Herausforderung, die Umstellung der öffentlichen und nicht-öffentlichen Stellen auf die Datenschutz-Grundverordnung zu begleiten — was alle Beschäftigten an sich schon an die Grenzen der Leistungsfähigkeit brachte. Daneben waren auch erhebliche personelle und organisatorische Veränderungen zu stemmen. Die mit dem letzten Doppelhaushalt 2018/2019 meiner Dienststelle zugewiesenen neuen Stellen waren zu besetzen und räumlich unterzubringen. Erfreulicherweise fanden die Stellenausschreibungen reges Interesse. Die vielen Bewerbungen qualifizierter Juristinnen und Juristen sowie von Angehörigen technischer Berufe machen deutlich, dass das Thema Datenschutz auch in der Wahrnehmung vieler Berufssuchender massiv an Bedeutung zugenommen hat, wobei sich etliche der Bewerberinnen und Bewerber bereits im Rahmen ihres Studium mit Datenschutzthemen befasst hatten und/oder im Rahmen erster beruflicher Tätigkeiten bei Anwälten oder Unternehmen erste Erfahrungen mit datenschutzrechtlichen Fragen sammeln konnten. Insgesamt eine erfreuliche Erkenntnis, die Mut macht.

Die Eingliederung der neuen Kolleginnen und Kollegen brachte nicht nur die Herausforderung mit sich, alle sach- und interessengerecht in die innere Organisation einzugliedern, was zu einer nahezu monatlichen Änderung des Geschäftsverteilungsplans führte. Die rasche Aufeinanderfolge neuer Kolleginnen und Kollegen führte auch dazu, dass man mitunter kaum dabei hinterher kam, sich Namen und Gesichter zu merken. Aber auch dies wurde letztlich gemeistert, so dass ich aktuell sagen kann: mission accomplished! Alle Stellen sind besetzt, alle neuen Kolleginnen und Kollegen sind in der Dienststelle angekommen.

Was allerdings noch nicht zu aller Zufriedenheit gelöst ist, ist die Raumsituation. Das schnelle und deutliche Anwachsen des Personalkörpers stellt meine Dienststelle vor das fast unlösbare Problem einer angemessenen Unterbringung aller Kolleginnen und Kollegen. Nachdem wir uns schon aus Platzgründen von Sozial- und Besprechungsräumen sowie unserer Bücherei verabschiedet hatten, mussten wir weiter „verdichten", das heißt Doppel- und zum Teil Dreifachbelegungen der Diensträume in Kauf nehmen. Mit bewundernswertem Verständnis haben das die Kolleginnen und Kollegen akzeptiert. Ein Dauerzustand darf dies jedoch nicht bleiben. Schon früh habe ich mich an den Landesbetrieb Vermögen und Bau gewandt und auf unsere Situation hingewiesen. Erfreulicherweise stieß ich dort auf großes Verständnis. Für die Unterstützung bei der Suche nach neuen Räumlichkeiten, die sich im Innenstadtbereich Stuttgarts keinesfalls einfach gestaltet, bin ich dem Landesbetrieb sehr dankbar. Aktuell zeichnet sich ab, dass wir in absehbarer Zeit ein neues Domizil beziehen können, das unseren Bedürfnissen haargenau entspricht.

Im Rahmen einer Besprechung der Abteilungsleiterinnen und –leiter 1 der Ministerien im Frühjahr 2018 in den Räumen meiner Dienststelle, in der es um die Neuerungen der Datenschutz-Grundverordnung für die Behörden des Landes ging, wurde der Gedanke geboren, den Datenschutzbeauftragten der Ministerien und der Regierungspräsidien eine Plattform zu bieten, auf der sie sich fachlich austauschen können. Behördliche Datenschutzbeauftragte sind nicht selten Einzelkämpferinnen/Einzelkämpfer innerhalb

ihrer Organisation. Da die praktischen Fragen und Probleme in der Umsetzung und Anwendung datenschutzrechtlicher Vorschriften häufig allgemeiner Natur sind, ist das Bedürfnis, sich mit anderen abzustimmen, auch um letztlich zu einer landeseinheitlichen Linie zu finden, verständlich. Ich habe diese Idee von Anfang an begrüßt und unterstützt und mich bereit erklärt, die Organisation zu übernehmen. In der Folge fanden bereits zwei Treffen statt. Diese waren geprägt von lebhaften Diskussionen mit dem Ziel, pragmatische Lösungen zu finden, was zumeist auch gelungen ist. Für mich und meine Mitarbeiterinnen und Mitarbeiter besteht der Wert dieser Runden darin, einen unmittelbaren Einblick in die tägliche Praxis der Behörden zu bekommen und unsere „Botschaften" ohne große Umwege in die Praxis zu transportieren. Die Resonanz der Teilnehmerinnen und Teilnehmer auf diese Treffen war überaus positiv. Die Vielzahl der Tagesordnungspunkte, die vorgeschlagen wurden, zeigt, dass der Bedarf an einem solchen Arbeitsgremium besteht. Da in der letzten Dezembersitzung 2018 nur ein Teil des Programms erledigt werden konnte, wurde zeitnah im Frühjahr 2019 ein weiteres Treffen vereinbart.

Ich halte dies eine für eine großartige Sache. Was allerdings diese Freude etwas trübt ist der Umstand, dass mir von einzelnen Teilnehmern die Botschaft übermittelt wurde, dass die hausinterne Unterstützung der/des Datenschutzbeauftragten durch die Behördenleitung mitunter im Argen liegt oder sie sogar ganz fehlt. Hier sind die Ministerien und die Regierungspräsidien zum Teil deutlich unterschiedlich aufgestellt.

Ich halte eine ungenügende Unterstützung der internen Datenschutzbeauftragten für fatal: Damit werden nicht nur formal Pflichten nach der DS-GVO verletzt, zugleich begibt man sich der Möglichkeit, im Interesse der Bürgerinnen und Bürger eine rechtskonforme Verarbeitung personenbezogener Daten sicherzustellen. Insbesondere die Ministerien sollten hier mit gutem Beispiel für den nachgeordneten Bereich und die Kommunen vorangehen. Ich behalte mir vor, auf die betroffenen Behörden mit dem Ziel einer besseren Unterstützung der behördlichen Datenschutzbeauftragten zuzugehen.

Mit dem Inkrafttreten des an die Datenschutz-Grundverordnung angepassten Landesdatenschutzgesetzes (LDSG) am 21. Juni 2018 änderte sich auch die Stellung meines Amtes und meiner Dienststelle im Aufbau der Landesverwaltung. Nach § 20 Absatz 1 Satz 1 LDSG sowie § 7 des Landesverwaltungsgesetzes ist der Landesbeauftragte für den Datenschutz nun eine oberste Landesbehörde und steht damit auf gleicher Stufe wie die Ministerien und der Rechnungshof. Dies bedeutete gleichzeitig ein Abschied vom Landtag, dem meine Dienststelle bis dahin zugeordnet war. Den Mitarbeiterinnen und Mitarbeitern der Landtagsverwaltung sowie der Landtagsverwaltung insgesamt danke ich sehr herzlich für die großartige Unterstützung insbesondere in der Personalverwaltung und in Haushaltsangelegenheiten, die sie mir und meinem Vorgänger über die Jahre haben zuteilwerden lassen. Jetzt, da wir unsere Angelegenheiten eigenständig erledigen müssen, zeigt sich noch deutlicher als bisher, welche enormen Anstrengungen damit verbunden sind. Letztlich ist das der Preis, der gezahlt werden muss, um der europäischen Vorgabe einer völligen Unabhängigkeit der Datenschutzaufsichtsbehörde gerecht zu werden. Gleichzeitig kommt in der Aufwertung meiner Dienststelle aber auch deren deutlich gestiegene Bedeutung und Verantwortung zum Ausdruck. Neben der Landtagsverwaltung gilt daher erneut dem gesamten Parlament mein herzlicher Dank für die Ausstattung und Unterstützung.

11.2 Wahl zur Beauftragten für Chancengleichheit

Am 22.11.2018 wurden innerhalb meiner Dienststelle die Ergebnisse der erstmaligen Wahl zur Beauftragten für Chancengleichheit (BfC) veröffentlicht. Bei einer Wahlbeteiligung von 84,4 % der wahlberechtigten Frauen wurden die neue BfC und deren Stellvertreterin gewählt.

Die BfC nimmt für meine Dienststelle seit dem genannten Datum die durch das Gesetz zur Verwirklichung der Chancengleichheit von Frauen und Männern Betroffenen im öffentlichen Dienst in Baden-Württemberg und zur Änderung des Landeshochschulgesetzes (Chancengleichheitsgesetz) vom 23. Februar 2016 wahr. Zum Stand 01.01.2017 hatten die Dienststelle des LfDI 41 aktive Mitarbeiter*innen, davon 24 weibliche (58,5 %) und 17 männliche (41,5 %). Als unabhängige oberste Landesbehörde umfasste die Dienststelle zum 31.12.2018 59 aktive Mitarbeiter*innen. Davon sind 34 weiblich (57,6 %) und 25 männlich (42,4 %). Die detaillierte Bestandsaufnahme wird der von der Dienststelle nun zu erstellende Chancengleichheitsplan enthalten. Eine der zentralen Aufgaben der BfC wird es sein, im Rahmen der frühzeitigen Beteiligung intensiv an der Erstellung dieses Chancengleichheitsplanes gemäß § 5 Abs. 4 Chancengleichheitsgesetzes mitzuwirken.

Daneben wird die BfC in vielfältigen Verfahren und Bereichen, wie beispielsweise bei der Durchführung von Stellenausschreibungen, im Hinblick auf Einstellung sowie Beförderung und bei der Planung und Gestaltung von Fort- und Weiterbildungsmaßnahmen (weitere Zuständigkeiten sind im Chancengleichheitsgesetz geregelt), im Rahmen der Beteiligung mitwirken. Insoweit kommt der BfC gemäß § 21 Chancengleichheitsgesetz auch ein Beanstandungsrecht im Hinblick auf mit dem Chancengleichheitsgesetz unvereinbaren Maßnahmen der Dienststelle zu.

Die BfC steht für die Mitarbeiter*innen der Dienststelle in Belangen der Chancengleichheit zudem als persönliche Ansprechpartnerin zur Verfügung und wird auf die Durchsetzung dieser Belange hinwirken. Auch Fortbildungsmaßnahmen zur Erzielung einer gelebten Chancengleichheit in der Dienststelle werden für das Jahr 2019 bereits in Zusammenarbeit mit der Dienststelle geplant.

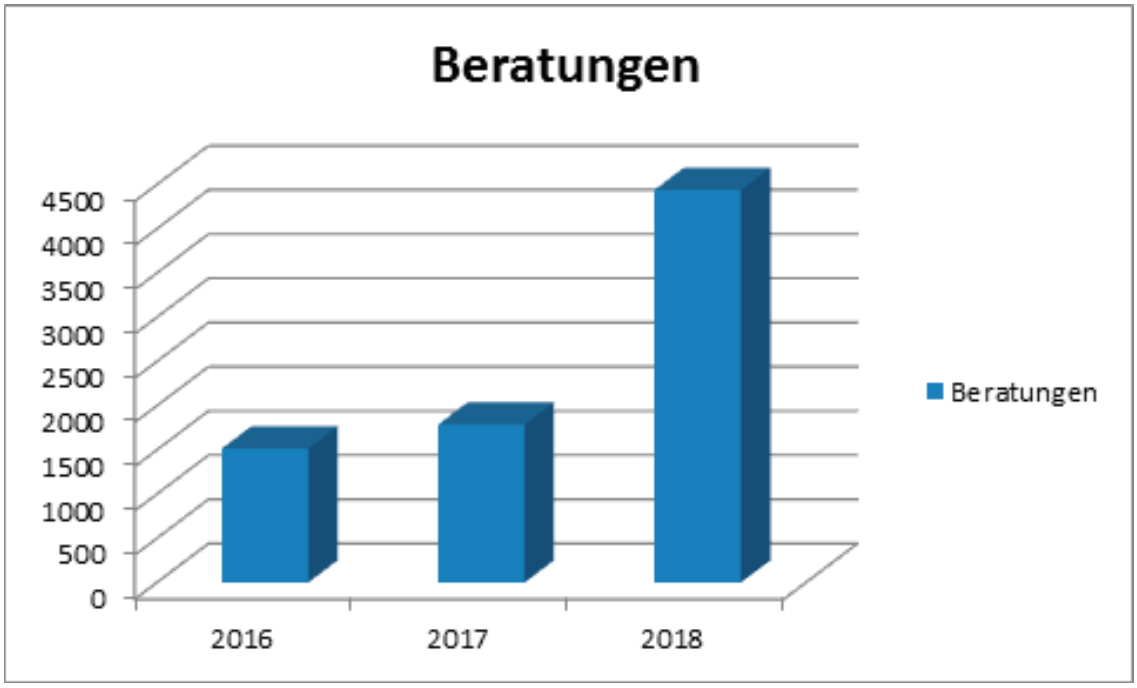
11.3 Dienststellenstatistik

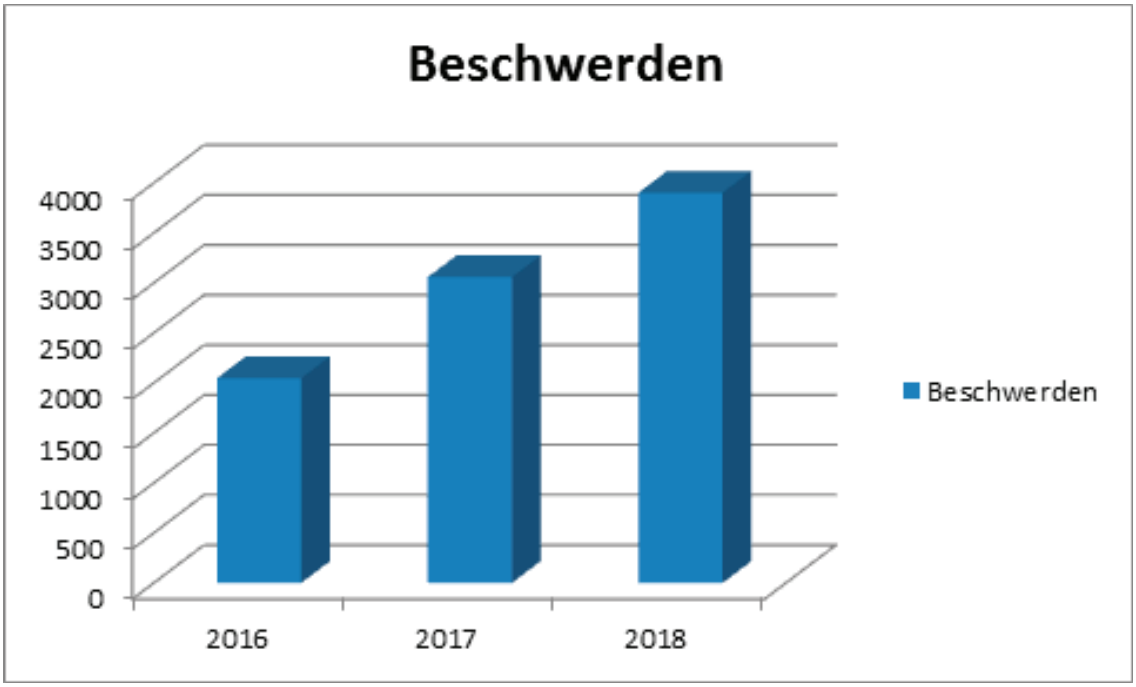
In den Berichtszeitraum 2018 fiel das Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO) am 25. Mai 2018. Die Auswirkungen der neuen Rechtsordnung auf den Geschäftsbetrieb meiner Dienststelle waren erheblich. In den reinen Statistikzahlen kommt dies nur unvollständig zum Ausdruck. Gleichwohl zeigt sich auch daran, dass die Datenschutzaufsicht mehr denn je gefordert ist, den Ansprüchen betroffener Bürgerinnen und Bürger ebenso gerecht zu werden wie derjenigen von Wirtschaft, Verbänden, Behörden und nicht zuletzt der Politik.

Bezeichnung	**2016**	**2017**	**2018**
Beschwerden			
- öffentlicher Bereich	840	1186	1188
- nicht-öffentlicher Bereich	1208	1872	2714
Kontrollen			
- öffentlicher Bereich	12	23	5
- nicht-öffentlicher Bereich	4	32	8
Beratungen			
- öffentlicher Bereich	878	991	1492
- nicht-öffentlicher Bereich	637	795	2948

Vergleicht man die Zahlen der in den letzten beiden Jahren jeweils eingegangenen Beschwerden, ergibt sich eine Steigerung insgesamt um ca. 30 Prozent. Während die Beschwerden über Behörden annähern konstant blieben, nahmen sie im privaten Bereich im Vergleich zum Vorjahr um ca. 50 Prozent deutlich zu. Insbesondere in diesem Bereich scheint die intensive Öffentlichkeitsarbeit meiner Dienststelle ebenso wie die mediale Berichterstattung rund um das Thema Datenschutz-Grundverordnung Früchte getragen und das Datenschutzbewusstsein der Bürgerinnen und Bürger geschärft zu haben. Zur Steigerung der Eingabezahlen beigetragen hat dabei sicher auch die Anfang 2018 angebotene Möglichkeit der Online-Beschwerde, die rege genutzt wird.

Massiv zugenommen hat die Zahl der Beratungen. Hier ergibt sich im Vergleich zu 2017 im Behördenbereich eine Steigerungsrate von 50 Prozent, im privaten Bereich sogar um 270 Prozent. In diesen Zahlen kommt deutlich die Unsicherheit im Umgang mit der neuen Rechtsordnung zum Ausdruck. Vor allem kleine und mittlere Unternehmen und Vereine sowie im öffentlichen Bereich die Gemeinden waren dabei Hauptadressaten unserer Beratungstätigkeit.


Beratungen
4500
4000
3500
3000
2500
2000
1500
1000
500
0
2016
2017
2018
Beratungen


Beschwerden
4000
3500
3000
2500
2000
1500
1000
500
0
2016
2017
2018
Beschwerden

Ähnliche Steigerungsraten waren bei den Meldungen von Datenpannen zu verzeichnen. Diese haben sich im Jahr 2018 mit 774 Meldungen mehr als verzehnfacht. Zu erklären ist dies einerseits dadurch, dass die Meldepflicht jetzt erstmals auch für Behörden gilt. Zum anderen hat die Drohung mit empfindlichen Geldbußen sicher auch dazu beigetragen, dass die bisher im privaten Bereich schon bestehende Pflicht nun ernster genommen wird.

Im Vergleich zum letzten Berichtszeitraum deutlich zurückgegangen ist dagegen die Zahl der anlassunabhängigen Kontrollen. Dies ist vor allem darauf zurückzuführen, dass die personellen Kapazitäten meiner Dienststelle nahezu vollständig durch die Abarbeitung der Beschwerden und die Beratungstätigkeit aufgebraucht wurden. Ziel für 2019 ist es, hier wieder verstärkt aktiv zu werden. Inwieweit sich dieses Ziel verwirklichen lässt, hängt jedoch nicht unwesentlich auch von der weiteren Entwicklung in anderen Bereichen der meine Dienststelle treffenden umfangreichen Aufgaben nach der Datenschutz-Grundverordnung ab.

11.4 Datenschutz en vogue - Datenschutz als KULTuraufgabe

In meinem ersten Amtsjahr habe ich – unabhängig von unserer Aufgabenerfüllung als Aufsichtsbehörde auf traditionelle Art und Weise – Daten zum Kulturgut erhoben und damit Datenschutz zur KULTuraufgabe erklärt. Im Rahmen einer ständigen Veranstaltungsreihe wird das Thema Datenschutz aus ungewöhnlichen Blickwinkeln beleuchtet und mit Kooperationspartnern in unterschiedlichen kulturellen Bereichen etabliert.

Um das Thema Datenschutz innerhalb der Gesellschaft fest zu verankern und vor allem um dem Datenschutz zugrundeliegende Schutzzwecke sichtbar und greifbar zu machen ist es unumgänglich, Neues zu wagen und ungewöhnliche Wege zu beschreiten. Die Zeiten einer Behörde im Elfenbeinturm sind deshalb vorbei – wir müssen für die Bürgerin, den Bürger und die Gesellschaft insgesamt sichtbarer und unser Thema greifbar werden. So stellen wir uns gemeinsam den Fragen und Herausforderungen dieser Zeit. Es gibt so viele Möglichkeiten, sich diesem großen Thema „Datenschutz" zu nähern – mit erhobenem Zeigefinger, mit Sanktions- und Schreckensszenarien, mit Stammtischparolen, mit Ärger, mit Langeweile, mit Angst, mit Vorträgen, mit Gesetzbüchern, mit vielen unverständlichen Worten, mit Akten, mit…

aber auch mit Sprühkreide, mit Kinofilmen, mit einer tracking-App und Geschäften, die sich kurzfristig im Sinne der FREIHEIT umbenennen, mit Kindern, die staunend beobachten, dass Datenschutz einen Regenbogen auf die Straße bringt,…

Wie immer gilt: Es kommt darauf an, was man daraus macht! - und meine Behörde und ich versuchen, ganz viel daraus zu machen!

11.4.1 Der Film Pre-Crime

Im April dieses Jahres haben wir den Kinofilm Pre-Crime an der Hochschule für Polizei Baden-Württemberg in Villingen-Schwenningen präsentiert und im Anschluss daran eine Podiumsdiskussion mit dem Regisseur des Films Matthias Heeder und einer Vertreterin des Landeskriminalamtes angeboten.

Kurz zum Film:

Einer perfekten Welt ohne Verbrechen scheint nichts mehr im Wege zustehen. Zukünftig werden potentielle Verbrecher BEVOR sie eine Straftat begehen werden, auf Basis von algorithmischen Berechnungen unter Beobachtung gestellt. Die Realität scheint diese Dystopie bereits eingeholt zu haben. Predictive Policing und Algorithmen-gestützte Polizeiarbeit, die auch in Racial Profiling münden kann, wird in vielen Großstädten bereits getestet.

Welchen Preis hat die Utopie absoluter Sicherheit? Und welche Konsequenzen hat es, wenn sich der Computer irrt?

Einen polizeikritischen Film in einer Polizeihochburg zu zeigen war eine spannende Kombination – insbesondere, da sich das Publikum nicht nur aus Studenten, sondern natürlich auch aus Vertretern der Hochschule, des Landeskriminalamtes und auch aus interessierten Bürgern zusammengesetzt hat. Dreistellige Besucherzahlen – trotz eines

zeitgleich stattfindenden Champions League Spiels - und ein überregionales Presseecho machen deutlich, dass nicht nur wir das Thema Datenschutz spannend finden…
Hier ein Auszug.

11.4.2 Datenschutz bringt Farbe in die Stadt…..

Im Juni 2018 habe ich den Konzeptkünstler Florian Mehnert und sein Kunstprojekt FREIHEIT 2.0 nach Stuttgart geholt. Bei FREIHEIT 2.0 handelt es sich um eine Kunstinstallation im öffentlichen Raum. FREIHEIT 2.0 stellt die Frage: „Was hat Big Data mit Freiheit zu tun?" Welchen Wert und welche Bedeutung hat Freiheit in einer Zeit zunehmender digitaler Präsenz und Transparenz? Ist Freiheit überhaupt noch zeitgemäß? Ist Freiheit nicht die Voraussetzung jeder Privatsphäre?

Die Kunstinstallation FREIHEIT 2.0 besteht aus vier Elementen und jeder kann daran teilhaben und sich aktiv einbringen.

Element 1: Self-Tracking-App
Die App nutzt die GPS-Funktion des Smartphones, um alle 30 Sekunden die geographische Position des Nutzers zu bestimmen. Die Erhebung und Verarbeitung der Daten erfolgte anonymisiert und verschlüsselt. Mit Hilfe dieser App wird deutlich, wie aus individuellen Verhaltensweisen und Bewegungsprofilen Daten generiert werden können.

Diese Bewegungsprofile der Tracking App waren für die Dauer des Projektes als interaktive Projektionen im Stadtpalais Stuttgart zu sehen. Unabhängig davon ist die App weiterhin aktiv. Sie können die Fortschreibung der Bewegungsprofile unter:
http://www.freiheit.florianmehnert.de/app/location/go/
abrufen.

Die App ist noch immer kostenlos verfügbar. Sie haben also immer noch die Gelegenheit sich an der Aktion FREIHEIT 2.0 aktiv zu beteiligen und einzubringen.

Element 2: Umfirmierung von Geschäften

Es handelt sich hierbei um die zeitweilige Umbenennung von 26 Geschäften und der Kirche St. Maria im Stuttgarter Gerberviertel deren Namen und Bezeichnungen jeweils individuell um den Begriff „Freiheit" erweitert wurde. Eine Rechtsanwaltskanzlei, die sich u. a. auf Strafrecht spezialisiert hatte, wurde umfirmiert zu „Rechtsanwälte der Freiheit", ein Espressoladen wurde zum „Espressoladen der Freiheit",...Die Bandbreite der Geschäfte, die sich beteiligt haben war enorm: u. a. eine Apotheke, eine Zahnarztpraxis, ein Barbier, eine Maßschneiderei,…

Diese Umbenennungen der gewohnten Geschäfte lassen die Kunden und Betrachter aufmerksam werden und veranlassen Nachfragen, die hervorragend geeignet sind in eine thematische Diskussion einzusteigen.

Element 3: Leitsystem

Ein auf der Straßen der Stadt Stuttgart aufgebrachtes temporäres Leitsystem verbindet die umfirmierten Geschäfte des Gerberviertels mit dem Stadtpalais, in dem die BIG DATA Kolloquien und die Ausstellung der Bewegungsprofile stattfinden.

Das mehrfarbige Leitsystem symbolisiert die eigentlich nicht sichtbaren digitalen Datenspuren, die wir stetig hinterlassen auf den Straßen und Wegen der Stadt wider.

Element 4: BIG DATA Kolloquien

Diese Kolloquien haben sich über knapp vier Wochen hinweg die Möglichkeit geboten, mit Referenten aus den Bereichen Wirtschaft, Philosophie, Soziologie, Recht und Psychologie über die ganze Vielfalt der Digitalisierung zu diskutieren.

Darüber hinaus ist besonders hervorzuheben, dass wir ein Konzert in der Kirche „St. Maria als" und zwei Veranstaltungen für Kinder und Jugendliche mit insgesamt knapp 150 Kindern und Jugendlichen präsentieren konnten.
Parallel zu den Veranstaltungen vor Ort wurden die meisten Kolloquien im livestream übertragen und sind unter:
http://www.freiheit.florianmehnert.de/stream.html
abrufbar.

Sie können unter:

- unser gesamtes Programm:
  http://www.freiheit.florianmehnert.de/programm.html
- den Kino-Trailer mit dem das Kino der Freiheit im Gerberviertel unsere Aktion um- und beworben hat
  http://www.freiheit.florianmehnert.de/trailer.html
- das SWR Radio Interview, Freiheit 2.0: Was hat Big Data mit Freiheit zu tun", 04.06.2018
  https://www.swr.de/swr2/kultur-info/was-hat-big-data-mit-freiheit-zu-tun-florian-mehnert-in-stuttgart/-/id=9597116/did=21809476/nid=9597116/bygn2d/index.html
- die SWR Sendung: Kunscht
  https://www.swr.de/kunscht/freiheit-/-/id=12539036/did=21579454/nid=12539036/n7z86n/index.html
- weitere Infos zu FREIHEIT 2.0 in Stuttgart
  http://www.freiheit.florianmehnert.de

abrufen.

Als Freiheitsschützer war es für mich selbstverständlich, die Kunstaktion im wahrsten Sinne des Wortes tatkräftig zu unterstützen und selbst Hand anzulegen. Zum Auftakt der Kunstaktion haben meine Mitarbeiter und ich uns aktiv an der Anbringung des Leitliniensystems beteiligt, insgesamt waren rund 50 km Kreidestreifen auf die Straßen und Wege der Landeshauptstadt aufzubringen.

Bei dieser Aktivität wurden wir auch von der Presse begleitet:
https://www.stuttgarter-zeitung.de/inhalt.kunstaktion-in-stuttgart-bunte-streifen-fuer-besseren-datenschutz.e8913afd-3ee5-417c-ab0d-3e1cf3d3eccf.html

Für mich ist Kunst ist ein wunderbares Medium, um Fragen zu stellen, Antworten zu suchen und auch zu finden!

11.4.3 Datenschutz sensibilisiert Kinder und Jugendliche

Unabhängig von unserem Engagement im Bereich: Datenschutz als KULTuraufgabe habe ich mir auch die Sensibilisierung von Kindern und Jugendlichen zur besonderen Aufgabe gemacht.

Unter dem Motto „Datenschutz – was geht mich das an?" hat sich ein Kurs der Dualen Hochschule Baden-Württemberg in Kooperation mit meiner Behörde mit dem Thema befasst. Unter Anleitung Ihrer Professoren wurden von den Studierenden mehrere sog. Demonstratoren entwickelt, um die Verarbeitung personenbezogener Daten verbundenen Gefährdungen sicht- und erfahrbar machen. Das Spektrum reichte dabei von heimlichen Datenauswertungen auf Smartphones, um Nutzerinnen auf Schritt und Tritt zu verfolgen und ihr Verhalten auszuforschen, über die für Endnutzer verständliche Visualisierung der Netzwerkübertragungen des Betriebssystems und Anwendungen, bis hin zur Videoüberwachung im öffentlichen Raum und ihren Gefährdungspotentialen. Im Rahmen eines durch den Förderverein der Dualen Hochschule Baden-Württemberg ausgelobten Preises wurde die App „bFREE" prämiert. Diese App implementiert vorder-

gründig einen kostenlosen Virenscanner mit attraktiven Features. Im Hintergrund aber ermöglicht sie einem Angreifer, jederzeit heimlich Kamera und Mikrofon zu aktivieren und sich die Aufnahmen übermitteln zu lassen, ebenso wie beliebige Dateien auf dem Gerät auszulesen oder den Standort des Smartphones abzufragen. Ihre App enthält aber auch wertvolle Hinweise, wie man sich vor böswilligen Apps schützen kann.

Eine Fortsetzung der Kooperation zwischen der Dualen Hochschule Baden-Württemberg und meiner Behörde ist bereits mit dem Wintersemester 2018 terminiert.

11.4.4 Datenschutz geht zur Schule

Nachdem eine Sensibilisierung für das Thema Datenschutz nicht früh genug erfolgen kann, unterstütze ich die Initiative „Datenschutz geht zur Schule" des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e. V. und baue diese in Baden-Württemberg aktiv aus.

Die Initiative „Datenschutz geht zur Schule" sensibilisiert Schülerinnen und Schüler zu einem bewussten Umgang mit dem Internet und den sozialen Medien. In diesem Zusammenhang haben meine Mitarbeiter und ich zum Safer Internet Day am 5. Februar 2019 diverse Aktionstage in verschiedenen Städten und Schulen Baden-Württembergs geplant.

11.4.5 Die Herbstkonferenz des Datenschutzes

Quelle: BvD e.V./Ulrich Schneider

Nicht zuletzt konnte ich Ende Oktober 2018 als Schirmherr ein weiteres Mal die Datenschutz-Herbstkonferenz in Stuttgart präsentieren. Veranstalter dieser Fachtagung ist der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.. Die Schirmherrschaft habe ich mir in diesem Jahr mit meinem Kollegen Thomas Kranig, Präsident des Bayerischen Landesamtes für Datenschutzaufsicht, geteilt. Die ersten beiden Tage standen unter dem Motto „Wirtschaft trifft Aufsicht". Der dritte Tag der Veranstaltung bot eine Premiere: Unter dem Motto „Aufsichtsbehörde berät Behörden" haben wir Fachvorträge und Diskussionen speziell auf den Kreis von Behördenvertretern zugeschnitten. Die Resonanz auf unsere Veranstaltung war nicht nur in Baden-Württemberg immens – bei knapp 300 Teilnehmern waren wir bereits im Vorfeld der Veranstaltung gezwungen einen Anmeldestopp verfügen.

Die Herbstkonferenz bietet Fachvorträge, Diskussionen, Expertengespräche, Handlungsleitfäden, Beispiele aus der Praxis für alle, die mit dem Thema Datenschutz befasst sind. Die Formate „Wirtschaft trifft Aufsicht" und auch „Aufsichtsbehörde berät Behörden" sind bundesweit einmalig und bieten die Möglichkeit Themen, Fragen und Probleme direkt mit den Fachleuten und Vertretern der Aufsichtsbehörden erörtern zu können. Die Resonanz der Teilnehmer macht deutlich, dass wir auf dem richtigen Weg sind! Wir werden also auch im Herbst 2019 die Datenschutz-Herbstkonferenz fortführen.

Quelle: BvD e.V./Ulrich Schneider

Und welches Motto habe ich für 2019?

Weiter geht's!

11.5 Presse- und Öffentlichkeitsarbeit

Der Datenschutz ist ein bedeutendes, aber ein nicht immer leicht verständliches Thema. Deshalb ist es mir ein wichtiges Anliegen die Presse- und Öffentlichkeitsarbeit weiter auszubauen. Um möglichst viele der relevanten Zielgruppen zu erreichen, nutzt meine Dienststelle eine breite Palette an Maßnahmen in ihrer Öffentlichkeitsarbeit.

Für das insgesamt sehr umfangreiche Aufgabenspektrum steht meiner Dienststelle eine Stelle zur Verfügung.

Pressearbeit
Nicht nur für die regionalen, auch für die nationalen Medien ist meine Dienststelle Ansprechpartner bei allen Themen rund um den Datenschutz. Das Themenspektrum, mit dem wir dabei konfrontiert werden, reicht von Fotoaufnahmen während Sportveranstaltungen über Ordnungswidrigkeitenverfahren bis hin zu meinem Bericht zum G20-Gipfel in Hamburg.

Zudem fanden am 26. Januar 2018 und am 30. August 2018 Pressekonferenzen statt. Die thematischen Aufhänger waren jeweils die Vorstellung des 33. Datenschutz-Tätigkeitsberichts sowie die Studie zur Vergütungstransparenz von Top-Managementmitgliedern öffentlicher Unternehmen mit Herrn Prof. Dr. Ulf Papenfuß von der Zeppelin Universität.

Die Tabelle auf der nächsten Seite stellt eine Übersicht der Pressemitteilungen mit entsprechenden Links für das Jahr 2018 dar.

Datum	Name
02.01.	Save the Date – 7. Speyerer Forum zur digitalen Lebenswelt
08.01.	Twitter-Kanal des LfDI ein voller Erfolg
26.01.	LfDI Dr. Stefan Brink stellt den 33. Tätigkeitsbericht zum Datenschutz vor
06.02.	Türkische Datenschutz-Delegation zu Besuch beim LfDI
07.02.	Kommunen öffnen sich mit Open Data
21.02.	Gemeinsam die Informationsfreiheit stärken!
27.02.	„Informationszugang ist ein Stück Freiheit!" – LfDI stellt ersten Tätigkeitsbericht für die Informationsfreiheit in Baden-Württemberg vor
28.02.	Twitter-Account des LfDI knackt die 1.000er-Follower-Marke!
02.03.	Schützenhilfe für Vereine: LfDI stellt eine Orientierungshilfe für Vereine unter der Datenschutz-Grundverordnung zur Verfügung
15.03.	LfDI gibt Tipps zur Umsetzung der Datenschutzgrundverordnung in Sachen Beschäftigtendatenschutz Der Ratgeber kann hier abgerufen werden.
27.03.	Datenschutz in Pflegeeinrichtungen
28.03.	DS-GVO-Schulungen für Kommunen
03.04.	„Sie sind vorsorglich festgenommen" – Fortsetzung des Formates „Datenschutz als Kulturaufgabe"
19.04.	Veranstaltungsreihe „Datenschutz als Kulturaufgabe" und der Dokumentarfilm „PRE-CRIME" finden sehr gute Resonanz
08.05.	Neuer Look für die Homepage des Landesbeauftragten
25.05.	LfDI bringt Farbe in die Straßen der Landeshauptstadt!
25.05.	Neues Datenschutzrecht – Vorsicht ja Panik nein
13.06.	Herausforderungen der Datenschutzgrundverordnung mit Bravour gemeistert
19.07.	Erste-Hilfe-FAQ für Arztpraxen zur Umsetzung der DS-GVO
30.08.	Studie zur Offenlegung von Managementvergütungen
05.09.	Fotografieren im Fokus der DS-GVO
10.09.	Europa ist größer als die EU – Twinning-Projekt der EU in Albanien
17.09.	Dialog mit den Aufsichtsbehörden – Veranstaltung
19.09.	G 20-Bericht des LfDI Baden-Württemberg
22.11.	LfDI Baden-Württemberg verhängt sein erstes Bußgeld in Deutschland nach der DS-GVO
05.12.	Erstes Webinar zur DS-GVO in Schulen erfolgreich

Internetauftritt
Der Internetauftritt ist einer der wichtigsten Bausteine in der Kommunikation meiner Dienststelle. Im Berichtsjahr ist meine Webseite mit überarbeitetem Design und innovativer Technik neu gestartet. Die Konzeption sowie die technische Umsetzung wurden von einem hauseigenen Mitarbeiter übernommen. Nach dem Facelift ist die neue Website auf dem neuesten Stand der Technik und zudem optimal eingestellt für die Darstellung auf mobilen Endgeräten. Die bewährte Menüstruktur wurde beibehalten bzw. ausgebaut.

Entscheidend für den Relaunch war neben den technischen Neuerungen vor allem ein Zugewinn bei der Anwenderfreundlichkeit. Die Seite bietet nun ein frisches und übersichtliches Layout, Interessierte erhalten alle Informationen schnell, gezielt und mit nur wenigen Klicks.

Formulare
Ein zentrales Thema des Relaunchs war zudem, die Möglichkeiten der Online-Kontaktaufnahme zu erweitern. So ist es nun neben der Online-Beschwerde möglich, die Daten des Datenschutzbeauftragten eines Unternehmens sowie Datenpannen online an meine Dienststelle zu melden.

Online-Beschwerde
Mit dem Online-Beschwerde-Formular können Bürgerinnen und Bürger einfach Datenschutzverstöße verantwortlicher baden-württembergischer Stellen bei uns melden.

Beschwerdeführer, die das Online-Formular nicht verwenden möchten, können sich selbstverständlich weiterhin vertrauensvoll per Brief, (verschlüsselter) E-Mail, Telefon oder auch persönlich an meine Dienststelle wenden.

Datenpanne melden
Mit unserem Online-Formular zur Meldung von Datenpannen bieten wir baden-württembergischen Verantwortlichen die einfache Möglichkeit an, die Meldung einer Verletzung des Schutzes personenbezogener Daten nach Art. 33 DS-GVO, umgangssprachlich „Datenpanne" genannt, online vorzunehmen.

Datenschutzbeauftragten melden
Ab Geltung der EU-Datenschutz-Grundverordnung (25. Mai 2018) sind Verantwortliche und Auftragsverarbeiter dazu verpflichtet sein, die Kontaktdaten ihrer oder ihres Datenschutzbeauftragten der zuständigen Aufsichtsbehörde mitzuteilen. Für Stellen mit Sitz in Baden-Württemberg ist meine Dienststelle die zuständige Aufsichtsbehörde.

Mit unserem Online-Formular können Sie uns die Kontaktdaten Ihres Datenschutzbeauftragten nach Art. 37 Absatz 7 der DS-GVO mitteilen.

Im Berichtsjahr wurden meiner Dienststelle per Online-Formular 22.541 Kontaktdaten von Datenschutzbeauftragten gemeldet.

FAQs

Damit Sie sich schnell und unkompliziert einen Überblick über unsere Themen verschaffen können, haben wir in einer extra Rubrik auf unserer Webseite oft gestellte Fragen mit den dazugehörigen Antworten zusammengefasst.
Im Berichtsjahr eingestellte Dokumente (FAQs):

- Datenschutz in der Arztpraxis
- Fotografieren und Datenschutz – Wir sind im Bild!
- Informationsfreiheit
- Kommunen
- Datenschutz in der Pflege
- Vereine
- Veröffentlichung von Fotos speziell für Vereine

Dieser Abschnitt wird regelmäßig um weitere FAQs ergänzt. Es lohnt sich daher, hier immer wieder vorbeizuschauen.

Newsletter
Weiterhin freue ich mich, dass im Berichtsjahr die ersten beiden Newsletter meiner Dienststelle veröffentlicht wurden. Künftig möchte ich die Bürgerinnen und Bürger auch über dieses Medium in regelmäßigen Abständen mit den neuesten Informationen zu aktuellen Themen versorgen.

Der Newsletter kann hier abonniert werden:
https://www.baden-wuerttemberg.datenschutz.de/newsletter-anmeldung/

Publikationen
Im Berichtzeitraum konnten wieder zahlreiche Broschüren und Flyer publiziert werden. Auf meinem Internetauftritt findet man unter der Rubrik DS-GVO zahlreiche verschiedene Materialien mit Erläuterungen, Definitionen und Hinweisen zu den einzelnen Vorschriften und deren Umsetzung.

Neben den Kurzpapieren der Datenschutzkonferenz empfehle ich die Lektüre der folgenden Ratgeber und Schulungsfolien meiner Dienststelle:

- Handreichung Beschäftigten-Datenschutz
- Praxisratgeber Die/der Beauftragte für den Datenschutz
- Schulungsfolien DS-GVO für Kommunen
- Schulungsfolien „Einstieg ins Datenschutzrecht für behördliche Datenschutzbeauftragte"
- Orientierungshilfe „Datenschutz im Verein nach der DS-GVO"
- Praxisratgeber für Vereine

Twitter

Seit dem 24. November 2017 nutze ich Twitter um zu aktuellen Themen aus der Welt des Datenschutzes und der Informationsfreiheit zu berichten. Damit präsentiert sich meine Dienststelle als transparente, moderne und kritikfähige Behörde.

Meinem Twitter-Account folgen bereits knapp 3.000 Follower. 2018 wurden 1.000 Tweets abgesetzt und insgesamt wurden die Tweets ca. 4.500.000 Mal angesehen.

Die Twitternutzung ist dabei eingebettet in ein ganzes Maßnahmenpaket, mit dem wir unserer Richtlinie zur Nutzung Sozialer Medien gerecht werden.

Der LfDI nutzt Twitter künftig als zusätzlichen Informationsweg. Alle Informationen rund um die Themen Datenschutz und Informationsfreiheit – und alle Tweets – finden sich auch auf meiner Internetseite unter www.baden-wuerttemberg.datenschutz.de. Auch wer Twitter künftig nicht nutzen möchte – und dafür gibt es sicherlich gute Gründe – verpasst also nichts. Alle bekannten Möglichkeiten, mit meiner Dienststelle Kontakt aufzunehmen, bleiben selbstverständlich auch erhalten.

Ein wichtiger Nebeneffekt unserer Nutzung von Twitter: Alle Behörden, die ebenfalls soziale Netzwerke nutzen wollen, können das von uns entwickelte Nutzungskonzept, die Datenschutz-Folgenabschätzung und auch die Netiquette als Blaupause verwenden.

Internationale Kooperationen des LfDI

Besuch des türkischen Datenschutzbeauftragten
Der türkische Datenschutzbeauftragte, Präsident Prof. Dr. Faruk Bilir, hat auf seiner Deutschlandreise als erste Anlaufstelle meiner Dienststelle einen Besuch abgestattet. Der vierköpfigen Delegation ging es bei ihrem Besuch um einen ersten Erfahrungsaustausch mit einer deutschen Datenschutzbehörde.

Am Ende des Treffens betonten beide Teilnehmer, dass ihnen der Informationsaustausch auch in Zukunft am Herzen liege.

Twinning-Projekt der EU in Albanien
Albanien befindet sich auf dem Weg in die Europäische Union. Ende Juni 2014 wurde dem Land offiziell der Status eines EU-Beitrittskandidaten zuerkannt, die Eröffnung der Beitrittsverhandlungen wurde im Juni dieses Jahres beschlossen.

Von den Albanern werden nun umfangreiche Reformen erwartet – unter anderem beim Kampf gegen die organisierte Kriminalität und gegen die weit verbreitete Korruption. Hierbei unterstützt meine Dienststelle das Anti-Korruptions-Projekt der EU als Twinning-Experte und begleitet das Land auf seinem Weg zu europäischen Standards.

Feedback zu unserer Presse- und Öffentlichkeitsarbeit ist ausdrücklich erwünscht! Mein Team wird unter der E-Mailadresse pressestelle@lfdi.bwl.de die Kommentare aufgreifen, zu den Vorschlägen und Anregungen Stellung nehmen und Fragen beantworten. Auch auf unserem zusätzlichen Kommunikationskanal Twitter freue ich mich über Reaktionen unter dem Hashtag #LfDI-Homepage. Wir wollen unser digitales Angebot mit der Unterstützung der Nutzer nicht nur gut, sondern besser machen.

Stichwortverzeichnis

T

V

W

Z