UNABHÄNGIGES
DATENSCHUTZ
ZENTRUM SAARLAND

27. Tätigkeitsbericht

2017 / 2018

27. Tätigkeitsbericht

der Landesbeauftragten für Datenschutz und Informationsfreiheit

Berichtszeitraum: 2017/2018

Dem Landtag und der Landesregierung
vorgelegt am: 10. April 2019
(Landtagsdrucksache 16/780)

UNABHÄNGIGES
DATENSCHUTZ
ZENTRUM SAARLAND

Die Landesbeauftragte für Datenschutz
und Informationsfreiheit

Fritz-Dobisch-Straße 12 • 66111 Saarbrücken
Postfach 10 26 31 • 66026 Saarbrücken
Telefon 0681 94781-0
Fax 0681 94781-29
E-Mail poststelle@datenschutz.saarland.de
Internet www.datenschutz.saarland.de
www.informationsfreiheit.saarland.de

Im Interesse einer besseren Lesbarkeit wird im Text überwiegend darauf verzichtet, geschlechtsspezifische Formulierungen zu verwenden. Sämtliche Personenbezeichnungen richten sich in gleicher Weise an die Angehörigen aller Geschlechter.

Vorwort

Der vorliegende Tätigkeitsbericht bezieht sich auf die Jahre 2017 und 2018 – zwei Jahre, die mit Blick auf den Datenschutz durchaus als turbulent bezeichnet werden können. Der Geltungsbeginn der europäischen Datenschutz-Grundverordnung (DSGVO) im Mai 2018 hat – trotz zweijähriger Übergangsphase seit Inkrafttreten der Verordnung im Mai 2016 – auf der einen Seite zwar für erhebliche Verunsicherung bei den Datenverarbeitern geführt, er hat auf der anderen Seite aber auch das Thema Datenschutz mehr denn je in den Fokus einer breiten Öffentlichkeit gerückt.

Neben der medialen Aufmerksamkeit, die das neue europäische Datenschutzrecht erfahren hat, führten auch zahlreiche Meldungen über öffentlich gewordene Datenschutzverletzungen und Datenmissbräuche zu einer allgemeinen Sensibilisierung für diesbezügliche Fragestellungen und Zusammenhänge, die nicht zuletzt erhebliche Auswirkungen auf die Arbeit des Unabhängigen Datenschutzzentrums Saarland hatten.

Durch eine signifikante Steigerung der an unsere Behörde adressierten Anfragen lag gerade in der ersten Hälfte des Jahres 2018 der Schwerpunkt unserer Tätigkeit sowohl in der Beratung der datenverarbeitenden Stellen als auch in der Aufklärung der Bürgerinnen und Bürger. Die weitreichende Bandbreite an Einzelfragen, die sowohl Entscheider in international agierenden Unternehmen als auch Verantwortliche im örtlichen Verein oder der saarländischen Verwaltung bewegte, stellte und stellt in ihrem Umfang auch weiterhin eine gewaltige Belastungsprobe für unsere Dienststelle dar. Obwohl mit der DSGVO das Rad nicht neu erfunden wurde, ergeben sich nach wie vor unzählige Auslegungsfragen, aber auch zahlreiche neuen Aufgaben und Befugnisse für unsere Behörde, die neue Schwerpunktsetzungen erfordern. Dies gilt im Besonderen hinsichtlich der in der DSGVO vorgesehenen europaweiten und verpflichtenden Kooperationsmechanismen, die einer fragmentierten Rechtsauslegung durch eine Vielzahl aufsichtsbehördlicher Akteure vorbeugen sollen. Die hiermit verbundenen Aufgaben bedeuten gerade für kleine Aufsichtsbehörden, wie der hiesigen, eine neue Dimension und stellen eine besondere Herausforderung dar.

Die neuen Anforderungen des europäischen Datenschutzrechts werden auch in den nächsten Jahren für unsere Behörde einen Schwerpunkt bilden – zumal mit der ePrivacy-Verordnung ein weiteres europäisches datenschutzrechtliches Regelwerk seinen Schatten vorauswirft. Es ist Aufgabe der Aufsichtsbehörden, diese Entwicklungen zu begleiten und sowohl im Rahmen der Gesetzgebungsverfahren als auch in der Gesetzesanwendung die Grundrechte und Grundfreiheiten der betroffenen Personen zu wahren. Für unsere Dienststelle wird der bevorstehende weitere Aufgabenzuwachs nur mit einer entsprechenden Personalausstattung zu bewältigen sein.

Auch die zunehmende digitale Durchdringung unserer Lebenswirklichkeit wird in den kommenden Jahren eine Herausforderung für den Datenschutz darstellen. Bereits jetzt erkennen Algorithmen und Künstliche Intelligenz Gesichter, erstellen me-

dizinische Diagnosen und treffen Personalentscheidungen – den technischen Möglichkeiten sind kaum noch Grenzen gesetzt. Um die mit der Digitalisierung verbundenen Potentiale auch für das Saarland und seine Bürgerinnen und Bürger nutzbar zu machen, verfolgen Landesregierung und Landtag eine Digital-Strategie, mit dem Ziel in diesem Bereich eine Vorreiterrolle einzunehmen. Da aber eine Vielzahl digitaler Anwendungen auf der Verarbeitung großer Mengen personenbezogener Daten beruht, dürfen die Belange der jeweiligen Individuen nicht aus dem Auge verloren werden; vielmehr muss bereits bei der Entwicklung sowie der Umsetzung innovativer Technologien immer das Recht des Einzelnen auf Datenschutz gewahrt werden. Daher sehen wir es auch als unsere Aufgabe an, den im Saarland in Gang gekommenen Digitalisierungsprozess konstruktiv zu begleiten.

Aufgrund der intensiven Diskussionen um die Datenschutz-Grundverordnung in den vergangenen beiden Jahren ist die Informationsfreiheit in der öffentlichen Wahrnehmung leider etwas in den Hintergrund getreten. Dies bedeutet allerdings keineswegs, dass diese an Bedeutung verloren hat. Vielmehr ist der freie Zugang zu Informationen der Verwaltung eine wesentliche Grundlage für die Teilhabe der Bürger am gesellschaftlichen und politischen Leben.

Während das Recht der Bürger auf Zugang zu amtlichen Informationen durch zahlreiche Gerichtsentscheidungen im Berichtszeitraum gestärkt worden ist, ist auf der anderen Seite aber auch erkennbar, dass der Gesetzgeber hinsichtlich der Schaffung bzw. Ausdehnung informationsfreiheitlicher Regelungen zurückhaltender geworden ist. Auch im Saarland ist keine Tendenz erkennbar, das mittlerweile in die Jahre gekommene Informationsfreiheitsgesetz zu einem zeitgemäßen Transparenzgesetz fortzuentwickeln.

Der vorliegende Bericht wird der letzte im Zweijahresrhythmus veröffentlichte gemeinsame Bericht über unsere Tätigkeit im Bereich des Datenschutzes und der Informationsfreiheit sein. Ab dem Jahre 2019 werden wir entsprechend den Vorgaben der DSGVO für den Datenschutzbereich Jahresberichte erstellen, die sich in Umfang und Aufbau von dem gewohnten Konzept unterscheiden werden. Für den Bereich der Informationsfreiheit hingegen wurde im Saarländischen Informationsfreiheitsgesetz der bisherige zweijährliche Berichtszeitraum beibehalten, so dass die beiden Berichte künftig getrennt erstellt und veröffentlicht werden.

Ganz herzlich bedanken möchte ich mich an dieser Stelle bei allen Mitarbeiterinnen und Mitarbeitern, die sich sehr intensiv und mit großem Engagement in die neuen datenschutzrechtlichen Vorschriften und den damit verbundenen Aufgabenkatalog eingearbeitet haben und die trotz teilweise sehr enger personeller Besetzung der Dienststelle der Vielzahl anfallender Anliegen mit fundiertem Fachwissen und der gebotenen Praxistauglichkeit gerecht geworden sind.

Saarbrücken, im April 2019

Monika Grethel

Landesbeauftragte für Datenschutz
und Informationsfreiheit

Inhaltsverzeichnis

DATENSCHUTZ

1 Überblick

1.1 Entwicklungen im Datenschutzrecht

1.1.1 Anwendung der Datenschutz-Grundverordnung

Seit dem 25. Mai 2018 ist die Europäische Datenschutz-Grundverordnung (DSGVO)[1] in allen Mitgliedstaaten der Europäischen Union (EU) unmittelbar anwendbares Recht. Darüber hinaus ist sie seit dem 20. Juli 2018 auch in den restlichen Staaten des Europäischen Wirtschaftsraums – Island, Liechtenstein und Norwegen – wirksam. In Kraft getreten ist die DSGVO allerdings bereits im Mai 2016. Die Übergangsfrist von zwei Jahren zwischen Inkrafttreten und Geltungsbeginn sollte allen datenverarbeitenden Stellen die Möglichkeit geben, sich frühzeitig auf die neue Rechtslage einzustellen und die erforderlichen Umsetzungsmaßnahmen zu ergreifen. Allerdings ist die Datenschutzreform in der öffentlichen Wahrnehmung zunächst weitgehend unbeachtet geblieben. Breite Resonanz hat sie im Wesentlichen erst erfahren, nachdem insbesondere in den Medien die potentiell hohen Bußgelder bei Datenschutzverstößen von bis zu 20 Millionen Euro bzw. alternativ 4-Prozent des weltweiten Jahresumsatzes und die Gefahr einer Welle von wettbewerbsrechtlichen Abmahnungen bei Datenschutzverstößen thematisiert worden sind. Dies sorgte vor allem bei kleineren und mittleren Unternehmen sowie Vereinen leider für erhebliche Verunsicherung, jedoch mit der durchaus begrüßenswerten Konsequenz, dass diese sich mit den neuen datenschutzrechtlichen Vorgaben auseinanderzusetzen hatten.

Gerade kleinere Wirtschaftsakteure und insbesondere Vereine übten dahingehend Kritik, dass sie von den Anforderungen der DSGVO in gleicher Weise berührt sind wie datenhungrige Großkonzerne und Soziale Netzwerke.

Zugegebenermaßen bringen die Anforderungen des neuen Regelungsrahmens häufig gerade für kleine Unternehmen und Vereine mit überwiegend ehrenamtlich Tätigen erhebliche Schwierigkeiten mit sich, da sie im Regelfall nicht über die notwendigen personellen Ressourcen und das fachliche Know-how verfügen, um die Anforderungen der DSGVO in konkrete Maßnahmen und Handlungsschritte zu überführen. Ob es geboten ist, für solche Verarbeiter gewisse Entlastungen bei der Anwendung der datenschutzrechtlichen Vorgaben vorzunehmen, wird sicherlich in der bereits im Mai 2020 anstehenden ersten Evaluierung der DSGVO durch die EU-Kommission zu erörtern sein.

Nichtsdestotrotz sind Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten unabhängig von

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. Nr. L 119, S. 1, ber. ABl. Nr. L 314, S. 72 und ABl. 2018 Nr. L 127, S. 2).

der Größe der datenverarbeiten Stelle und dem Umfang der jeweiligen Datenverarbeitungsprozesse zu wahren. Vor dem Hintergrund dieses Schutzzwecks der DSGVO gelten spezifische datenschutzrechtliche Vorgaben gleichsam sowohl für den global agierenden Handelsriesen wie für den örtlichen Fußballverein; angesichts der zunehmenden Verwendung digitaler Technologien ist es zudem für das Vertrauen der Verbraucher bzw. Mitglieder bei der Verarbeitung ihrer personenbezogenen Daten von großer Bedeutung, dass Verantwortliche sorgsam mit ihren Daten umgehen.

Ein weiterer Grund für die Verunsicherung vieler Anwender der DSGVO war und ist der dem Vollharmonisierungsanspruch und der technikneutralen Ausgestaltung geschuldete hohe Abstraktionsgrad einzelner Regelungen der Verordnung, der eine Bandbreite an Deutungsmöglichkeiten bietet und dem Anwender die Umsetzung der Vorgaben erschwert. In Erscheinung getretene Unklarheiten hatten vielfach pauschale Kritik am Datenschutzrecht und Zweifel an der Wirksamkeit der Datenschutzreform nach sich gezogen. Ebenso wurden immer wieder Stimmen laut, die die bestehende föderale Struktur der Aufsichtsbehörden in Frage gestellt haben, da es bei verschiedenen Auslegungsfragen nicht immer einheitliche Auffassungen der Aufsichtsbehörden gibt. So nachvollziehbar das Bedürfnis nach einheitlichen verbindlichen Rechtsauffassungen der Aufsichtsbehörden auch ist, so wenig nachvollziehbar ist die hieraus resultierende Forderung nach einer einzigen nationalen Aufsichtsbehörde, da sich das Vorhandensein ortsnaher, kompetenter Ansprechpartner, die einen Einblick in die Verhältnisse vor Ort haben, bislang bewährt hat.

Schließlich sind divergierende Rechtsauffassungen auch keine spezifische Problematik des Datenschutzrechts, vielmehr ist es einer Rechtsanwendung immanent, dass verschiedene Behörden rechtliche Vorschriften unterschiedlich auslegen. Da gesetzliche Regelungen nicht immer völlig eindeutig sind, kann der Gesetzeswortlaut durchaus unterschiedliche Auslegungen zulassen, die – jeweils auch unter Berücksichtigung der Einzelfallgerechtigkeit – vertretbar sein können. Weitgehende Rechtssicherheit bei der Auslegung von Gesetzen besteht daher in der Regel erst dann, wenn (Ober-)Gerichte abschließende Entscheidungen zu auslegungsbedürftigen Regelungen getroffen haben. Auch bei der Klärung zahlreicher Fragen in Bezug auf die DSGVO wird letztlich erst der Europäische Gerichtshof für alle Beteiligten rechtssichere Antworten geben.

Die Europäische Datenschutzkonvention[2] ist nunmehr beinahe 40 Jahre alt, die europäische Datenschutzrichtlinie[3] knapp 25 Jahre und die Datenschutz-Grundverordnung gerade einmal 1 Jahr in der Anwendung. Man sollte der Praxis ausreichend Zeit geben, um eine einheitliche Rechtsauffassung ausbilden zu können.

Um den Anwendern im praktischen Vollzug der DSGVO Hilfestellungen zu leisten, arbeitet die Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) auf nationaler Ebene sehr intensiv daran, abge-

[2] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108).

[3] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. Nr. L 281, S. 31, ber. 2017 Nr. L 40, S. 78).

stimmte Hinweispapiere zu verschiedenen datenschutzrechtlichen Themen zu erstellen. Diese Papiere der Datenschutzkonferenz sind ebenso wie weitergehende Informationen sowohl über die Internetseite des Unabhängigen Datenschutzzentrums Saarland als auch über die neu erstellte Webseite der Datenschutzkonferenz (www.datenschutzkonferenz-online.de) abrufbar.

Zur Gewährleistung einer einheitlichen Aufsichtspraxis in ganz Europa enthält das neue Recht darüber hinaus detaillierte Vorgaben zur Kooperation aller europäischen Aufsichtsbehörden, was eine kohärente Anwendung der datenschutzrechtlichen Vorgaben nicht nur national, sondern europaweit sicherstellen soll. Eine zentrale Stellung nimmt hierbei der Europäische Datenschutzausschuss ein, der zwar nicht die letztverbindlichen gerichtlichen Entscheidungen ersetzen wird, der aber durchaus verbindliche Vorgaben für die Praxis der Aufsichtsbehörden machen kann.

Neben den tatsächlich bestehenden Unsicherheiten hinsichtlich einer rechtlich korrekten Auslegung zahlreicher Vorschriften der DSGVO haben häufig Fehleinschätzungen der datenverarbeitenden Stellen dazu geführt, dass insbesondere in den Medien die Wirksamkeit der DSGVO in Frage gestellt wurde. Bei sorgfältiger Subsumtion der rechtlichen Vorgaben wären allerdings zahlreiche dieser als „Datenschutzskandale“ bezeichneten Fehlinterpretationen datenschutzrechtlicher Vorschriften zu vermeiden gewesen.

Insgesamt fällt aus Sicht der Aufsichtsbehörden ein erstes Fazit nach mehr als sieben Monaten Geltung der DSGVO positiv aus. Deutlich erkennbar ist, dass die Sensibilisierung der Bürger für datenschutzrechtliche Fragen sehr stark zugenommen hat. Betroffene nehmen vermehrt ihre Rechte, insbesondere auf Auskunft und Löschung gegenüber den verantwortlichen Stellen wahr, und wenden sich mit Beschwerden wegen unrechtmäßiger Datenverarbeitung an unsere Behörde.

Aber auch Unternehmen und Vereine haben zu einem großen Teil ein Bewusstsein für Fragen des Datenschutzes entwickelt und ihre Verantwortung bei der Verarbeitung personenbezogener Daten erkannt. Um den datenverarbeitenden Stellen im Saarland Hilfestellungen bei der Anwendung der neuen Regelungen zu geben, wurde im Berichtszeitraum durch unsere Dienststelle die Beratung und Information und nicht die Sanktionierung von möglichen Verstößen in den Vordergrund der Tätigkeit gestellt. Denn nur wenn die neuen gesetzlichen Verpflichtungen bei den verantwortlichen Stellen hinreichend bekannt sind und diese Stellen auch ein Verständnis dafür entwickeln, weshalb die Einhaltung der Regelungen für einen Schutz der informationellen Selbstbestimmungsrechts der Betroffenen von Bedeutung ist, kann die DSGVO die gewünschten Ziele, nämlich den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten bei gleichzeitiger Gewährleistung des freien Verkehrs der Daten in der ganzen Union erreichen.

Obwohl in der Öffentlichkeit eine Überforderung der verantwortlichen Stellen bei der Umsetzung der DSGVO massiv beklagt wurde, wurde der Umstand, dass nicht nur die saarländische, sondern nahezu alle Aufsichtsbehörden Deutschlands jedenfalls bis Ende 2018 kaum nennenswerte Sanktionen verhängt haben, häufig als Mangel an der Wirksamkeit des neuen Rechts betrachtet.

Selbst wenn unsere Behörde künftig ihre Aufsichtsfunktion auch im Bereich der Sanktionierung von Datenschutzverstößen als wesentliche Aufgabe nicht vernachlässigen

darf und wird, stellt die Beratung der verantwortlichen Stellen auch weiterhin einen wichtigen Baustein unserer Tätigkeit dar.

Und dass die Regelungen der DSGVO einen wichtigen Impuls für einen hohen Datenschutzstandard nicht nur in Europa, sondern auch weltweit gegeben haben und nicht – wie häufig befürchtet – die Digitalisierungsfortschritte hemmen werden, zeigt die Tatsache, dass sie beispielsweise als Vorbild für neue Datenschutzgesetze, u. a. in Kalifornien, dienen.

1.1.2 Bundesrechtliche Anpassungen an die Datenschutz-Grundverordnung

Obwohl die Datenschutz-Grundverordnung (DSGVO) als eine europäische Verordnung unmittelbar geltendes Recht in allen Mitgliedstaaten der EU ist, ist sie dennoch in einigen Bereichen ausfüllungsbedürftig; insgesamt mehr als 70 sog. Spezifizierungsklauseln geben den nationalen Gesetzgebern die Möglichkeit oder verpflichten diese, durch eigene gesetzliche Regelungen das europäische Recht zu konkretisieren, zu ergänzen und zu modifizieren. Dabei müssen aber die nationalen Regelungen immer die Vorgaben und Grundsätze der DSGVO beachten. Widerspricht eine nationale Regelung im Rahmen der Anwendung auf einen konkreten Einzelfall dem europäischen Recht, gilt aufgrund des Anwendungsvorrangs des Unionsrechts die DSGVO unmittelbar und die nationale Regelung bleibt unangewendet.

Mit dem Datenschutzanpassungs- und Umsetzungsgesetz EU hat der Bundesgesetzgeber das Bundesdatenschutzgesetz (BDSG)[4], das unter anderem für Unternehmen und Vereine die maßgebende ergänzende Rechtsquelle neben der DSGVO darstellt, neu gefasst. Die Datenschutzaufsichtsbehörden des Bundes und der Länder haben im Gesetzgebungsverfahren zahlreiche Regelungen des Gesetzes kritisiert, jedoch wurden die Kritikpunkte größtenteils nicht berücksichtigt.

Wie umfangreich der gesetzgeberische Handlungsbedarf trotz der vollharmonisierenden europarechtlichen Regelungen auf nationaler Ebene noch ist, wird daran deutlich, dass sich zum Ende des Berichtszeitraum auf Bundesebene ein Zweites Datenschutzanpassungs- und Umsetzungsgesetz in der parlamentarischen Beratung befindet, mit dem weitere 154 bereichsspezifische Vorschriften an das europäische Recht angepasst werden sollen. Aber auch mit diesem Gesetzespaket findet der Anpassungsprozess noch kein Ende, da nach wie vor zahlreiche weitere Gesetze, wie bspw. das Telekommunikationsgesetz, anzupassen sind.

[4] Bundesdatenschutzgesetz vom 30.6.2017 (BGBl. I S. 2097).

1.1.3 Landesrechtliche Anpassungen an die Datenschutz-Grundverordnung

Im Saarland ist die Neufassung des für alle öffentlichen Stellen des Landes anwendbaren Saarländischen Datenschutzgesetzes (SDSG)[5] rechtzeitig vor Geltungsbeginn der DSGVO erfolgt. Unsere Dienststelle war durch das zuständige Ministerium für Inneres, Bauen und Sport bereits sehr frühzeitig in den Gesetzgebungsprozess eingebunden und konnte zahlreiche Anregungen geben, die auch zu einem großen Teil aufgegriffen und Eingang in das Gesetz gefunden haben. Zu begrüßen ist insbesondere, dass es gelungen ist, lediglich in moderatem Umfang Einschränkungen der Betroffenenrechte bei den Informationspflichten (§ 10 SDSG), den Auskunftsrechten (§ 11 SDSG) und den Benachrichtigungspflichten (§ 12 SDSG) im Gesetz zu regeln und dass die öffentlichen Stellen die Gründe zu dokumentieren haben, weshalb sie im Einzelfall von den entsprechenden Beschränkungen Gebrauch gemacht haben, was eine spätere Überprüfung durch uns als Aufsichtsbehörde ermöglicht und vereinfacht. Sinnvoll finden wir auch, dass bei der Einführung neuer Verfahren grundsätzlich am Erfordernis einer förmlichen Freigabe – allerdings ohne unsere Beteiligung – festgehalten wird, dass aber diese Freigabe zumindest dann nicht erforderlich ist, wenn es sich um Verfahren mit nur geringem Risiko für die hiervon Betroffenen handelt (siehe § 15 Abs. 2 SDSG). Die bisherige Rechtslage, die eine Beteiligung unserer Dienststelle selbst bei der Einführung von Telefonverzeichnissen, elektronischen Kalendern oder Zimmer- und Inventarverzeichnissen vorsah, soweit darin personenbezogene Daten verarbeitet wurden, war praxisfern, bürokratisch und bot auch aus Sicht der Rechte und Freiheiten der betroffenen Personen kaum einen Mehrwert. Leider nicht durchsetzen konnten wir uns mit der Forderung, die im Zusammenhang mit der Einführung einer Data-Warehouse-Lösung neu eingefügte Vorschrift des § 22 Abs. 4 SDSG und die danach zulässigen Auswertezwecke für Daten von Beschäftigten im öffentlichen Dienst zu beschränken [vgl. hierzu Kap. 8.1 (S. 70 ff.)].

Darüber hinaus sind auch im Saarland mittlerweile einige – aber auch noch nicht alle – Fachgesetze an die DSGVO angepasst worden, bei denen wir ebenfalls im Gesetzgebungsverfahren frühzeitig beteiligt wurden. Besonders hervorzuheben sind in diesem Zusammenhang die Anpassungen des Gesetzes zur Förderung der elektronischen Verwaltung im Saarland (E-Government-Gesetz Saarland)[6] und dessen § 3 Abs. 5, der die rechtlichen Voraussetzungen dafür schafft, dass Leistungen saarländischer Behörden in Zukunft über ein Verwaltungsportal angeboten und abgerufen werden können. Ebenfalls erwähnenswert ist unsere Zusammenarbeit mit dem Ministerium für Finanzen und Europa und dem CISPA – Helmholtz-Zentrum i.G. GmbH – beim Entwurf eines Gesetzes zur Abwehr von Gefahren für die Daten in der Informations- und Kommunikationsinfrastruktur des Landes (Informationssicherheitsgesetz Saarland). Dieses Gesetz fokussiert den Ausgleich zwischen dem Interesse der Landesverwaltung, die Funktionsfähigkeit ihrer IT-Infrastrukturen zu gewährleisten und

[5] Gesetz zur Anpassung des Saarländischen Datenschutzgesetzes an die Verordnung (EU) 2016/679 vom 16. Mai 2018 (Amtsbl. I S. 254).

[6] Vom 15.11.2017 (Amtsbl. I S. 1007), zuletzt geändert d. Gesetz v. 16.5.2018 (Amtsbl. I S. 254).

diese gleichzeitig vor Angriffs- und Kompromittierungsversuchen zu schützen, und den schutzwürdigen Interessen der Bürger und Beschäftigten, die über diese IT-Infrastruktur mit der öffentlichen Verwaltung kommunizieren.

Auch für den Bereich des Rundfunks und der Presse mussten die bestehenden Vorschriften geändert werden, um das grundrechtliche Spannungsverhältnis zwischen dem Datenschutz und der Meinungs- und Informationsfreiheit in Einklang zu bringen. Daher hat der saarländische Landtag zeitgleich mit dem SDSG den Einundzwanzigsten Rundfunkstaatsvertrag, der zahlreiche datenschutzrechtliche Regelungen für den öffentlich-rechtlichen Rundfunk enthält, umgesetzt und zudem das Saarländische Mediengesetz (SMG)[7] angepasst.

Zu diesem Gesetzentwurf konnten wir leider erst im parlamentarischen Verfahren eine Stellungnahme abgeben. Die von uns geäußerten Bedenken an der Europarechtskonformität verschiedener Vorschriften blieben allerdings weitgehend unberücksichtigt. Auch unsere Anmerkungen zu den erst im Wege eines Abänderungsantrages im parlamentarischen Beratungsverfahren neu hinzugekommenen datenschutzrechtlichen Vorschriften im SMG haben leider keine Berücksichtigung mehr gefunden. Gerade die darin enthaltenen Regelungen hinsichtlich der Ausgestaltung der Landesmedienanstalt als eine spezifische Aufsichtsbehörde sowie deren Zuständigkeiten, insbesondere in Bezug auf Anbieter sozialer Netzwerke, enthalten zahlreiche Ungereimtheiten und hätten einer eingehenderen parlamentarischen Erörterung bedurft.

Eine erwähnenswerte Regelung auf Landesebene ist schließlich noch die durch den saarländischen Landtag erlassene Datenschutzordnung, welche die durch die Nichtanwendbarkeit der DSGVO im parlamentarischen Bereich entstehende datenschutzrechtliche Lücke schließt [vgl. hierzu Kap. 5.1 (S. 49 ff.)].

Wenn auch der europäische Gesetzgeber die Grundsätze für den Datenschutz in ganz Europa mit Erlass der DSGVO einheitlich festgelegt hat, zeigt diese Darstellung gleichwohl deutlich, dass den nationalen Gesetzgebern dennoch Spielräume verbleiben, um eigene Akzente zu setzen. Diese Spielräume sollten allerdings dergestalt genutzt werden, dass Deutschland auch weiterhin in datenschutzrechtlicher Sicht eine Vorreiterrolle in Europa einnimmt. Konkret bedeutet dies, der Versuchung zu widerstehen, unter Ausnutzung oder Überdehnung aller Regelungsmöglichkeiten die datenschutzrechtlichen Vorgaben zu lockern und hierdurch die Rechte der Bürger einzuschränken.

Ob alle bisher erlassenen Anpassungsgesetze des Bundes und der Länder den europarechtlichen Vorgaben entsprechen, wird hoffentlich zeitnah durch die EU-Kommission überprüft werden, da sämtliche Mitgliedstaaten verpflichtet sind, der Kommission alle nationalen Regelungen zur Anpassung an die DSGVO mitzuteilen. Insgesamt lässt sich aber konstatieren, dass zumindest in Bezug auf das saarländische Landesrecht eine frühzeitige Beteiligung unserer Dienststelle in den bisherigen Gesetzgebungsverfahren dazu geführt hat, dass sowohl aus datenschutzrechtlicher als auch

[7] Gesetz Nr. 1490 - Saarländisches Mediengesetz vom 27.2.2002 (Amtsbl. 2002 S. 498), zuletzt geändert d. Gesetz v. 16.5.2018 (Amtsbl. I S. 268).

aus datenschutzpolitischer Sicht tragfähige Kompromisse Eingang in die Gesetze gefunden haben. Wir hoffen und sind zuversichtlich, dass die Landesregierung uns auch bei zukünftigen Gesetzgebungsvorhaben mit datenschutzrechtlichem Bezug frühzeitig einbinden wird.

1.1.4 JI-Richtlinie und deren Umsetzung in nationales Recht

Zusammen mit der DSGVO ist auf europäischer Ebene auch die Richtlinie (EU) 2016/680 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 (JI-Richtlinie)[8] auf den Weg gebracht worden. Diese Richtlinie, die erstmals unionsweit einen Mindeststandard für den Datenschutz bei Polizei- und Justizbehörden festlegt, ist zeitgleich mit der DSGVO im Mai 2016 in Kraft getreten und verpflichtet die Mitgliedstaaten der EU, ihre Vorgaben bis zum 6. Mai 2018 in nationales Recht umzusetzen. Auf Bundesebene wurden mit der Verabschiedung des ersten Datenschutzanpassungs- und Umsetzungsgesetzes im neuen BDSG bereits erste grundsätzliche Regelungen zur Umsetzung der Richtlinie für Bundesbehörden geschaffen.

Der saarländische Gesetzgeber hatte hingegen zunächst davon absehen wollen, zeitgleich mit der Verabschiedung des SDSG Regelungen zur Umsetzung der JI-Richtlinie zu treffen. Vielmehr war beabsichtigt, die Umsetzung jeweils in den fachspezifischen Gesetzen für die Polizei, den Strafvollzug und den Maßregelvollzug vorzunehmen. Da in dem Gesetzentwurf für das SDSG zunächst – anders als nach der bisherigen Rechtslage – keine Regelung über die datenschutzrechtliche Aufsicht und Kontrolle der Ermittlungstätigkeit der Staatsanwaltschaft enthalten und auch in den geplanten Gesetzen zur Umsetzung der JI-Richtlinie keine entsprechende Regelung vorgesehen war, hätte dies dazu geführt, dass die Tätigkeit der Staatsanwaltschaft gerade in den besonders grundrechtsensitiven Bereichen, wie verdeckten Ermittlungs- und Überwachungsmaßnahmen, keiner datenschutzrechtlichen Kontrolle mehr unterlegen hätte. Um diese Situation zu vermeiden, wurde auf unseren Hinweis hin noch im parlamentarischen Verfahren eine entsprechende Ergänzung in das SDSG aufgenommen.

Darüber hinaus wurden im Berichtszeitraum keine weiteren Gesetze zur Umsetzung der JI-Richtlinie erlassen. Ende des Jahres 2018 wurde uns allerdings im Rahmen des externen Anhörungsverfahrens ein Entwurf für ein Polizeidatenverarbeitungsgesetz zugeleitet. Dieser Entwurf enthält neben der Umsetzung der JI-Richtlinie in nationales Recht auch aufgrund der Rechtsprechung des Bundesverfassungsgerichts zum

[8] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. Nr. L 119, S. 89, ber. ABl. 2018 Nr. L 127, S. 9).

Bundeskriminalamtgesetz (BKAG)[9] vom 20. April 2016 notwendig gewordene Korrekturen bei heimlichen Überwachungsmaßnahmen.[10]

Bereits dieser erste Entwurf des Polizeidatenverarbeitungsgesetzes zeigt, dass auch im Saarland – wie bereits in anderen Bundesländern – auf den Einsatz von Staatstrojanern gesetzt werden soll. Entsprechende technische Mittel werden unbemerkt auf den Computern und Smartphones verdächtiger Personen installiert und sollen es den Ermittlungsbehörden erlauben, die elektronische Kommunikation der Betroffenen mitzuprotokollieren bevor diese übertragen wird; denn während der Übertragung ist eine Kenntnisnahme mit den klassischen Mitteln der Telekommunikationsüberwachung aufgrund der dann vorhandenen Verschlüsselung der übertragenen Daten oft nicht erfolgsversprechend. Eine solche Maßnahme stellt einen erheblichen Eingriff in das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme, dem sog. IT-Grundrecht, dar, der nur unter engen Voraussetzungen verhältnismäßig ist. Zu diesen Verhältnismäßigkeitsanforderungen gehört insbesondere auch, dass entsprechende Maßnahmen nicht – auch nicht mittelbar – zu einem Risiko für die Vertraulichkeit und Integrität der IT-Systeme von unbeteiligten Dritten werden. Gerade das kann aber der Fall sein, wenn der Staat entsprechende Sicherheitslücken, die er zur Einschleusung verwendet, hortet und nicht an die Soft- und Hardwarehersteller meldet.

Da die Einschleusung der Ermittlungssoftware (des Trojaners) mittels Ausnutzung von Sicherheitslücken in Soft- und Hardware geschieht, die den jeweiligen Herstellern – im Regelfall – noch unbekannt sind, werden die Behörden diese Lücken geheim halten wollen um sie auch zukünftig als „Hintertür" zum Aufbringen der Überwachungssoftware verwenden zu können, anstatt auf das Schließen der Lücken bei den Herstellern hinzuwirken. Damit bleiben entsprechende Sicherheitslücken „ungepatcht" und können in der Folge nicht nur von Ermittlungsbehörden unter Einhaltung rechtstaatlicher Grundsätze ausgenutzt werden, sondern auch von kriminellen Hackern oder Geheimdiensten anderer Staaten missbraucht werden, die auf die Systeme der Nutzer über diese Sicherheitslücken zugreifen. Hierdurch entsteht eine Gefährdung der IT-Systeme aller Bürger ebenso wie für die IT-Systeme von Unternehmen und der Verwaltung, da die Sicherheitslücke nicht lediglich in einem spezifischen Nutzersystem vorhanden, sondern in der dort verwendeten Soft- und / oder Hardware, die ebenso auch in Wirtschaft und Verwaltung Verwendung findet. Zu erinnern ist in diesem Zusammenhang an "WannaCry", den großen Cyberangriff im Mai 2017. Die zugrundeliegende Sicherheitslücke, die hier ausgenutzt wurde, war dem US-Geheimdienst NSA seit Langem bekannt.

Mit der oben beschrieben Vorgehensweise wird eine allgemeine, großflächige Absenkung der IT-Sicherheit in Kauf genommen und die IT-Systeme der Bürger, der Wirtschaft und des Staates werden einem erhöhten Risiko ausgesetzt. Aus dem IT-Grundrecht folgt aber gerade eine Schutzpflicht des Staates, die Vertraulichkeit und Integrität informationstechnischer Systeme zu gewährleisten, woraus sich eine Pflicht ergibt, auf eine Schließung solcher Schwachstellen hinzuwirken.

---

[9] Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten vom 1. Juni 2017 (BGBl. I S. 1354).

[10] Vgl. 26. Tätigkeitsbericht, 2015/2016, Kap. 3.1., S. 37 ff.

Was die bis dato noch nicht erfolgte bereichspezifische Umsetzung der JI-Richtlinie anbelangt, ist darauf hinzuweisen, dass für die polizeilichen Datenverarbeitungen bis zum Inkrafttreten der diesbezüglichen Neuregelungen und damit der Umsetzung der JI-Richtlinie, kein datenschutzrechtliches Vakuum herrscht, was die Verarbeitung personenbezogener Daten durch die Polizei angeht. Wegen der Formulierung des § 3 SDSG gelten für die Verarbeitung personenbezogener Daten durch die Polizei bis auf Weiteres die Vorschriften des SDSG und der DSGVO entsprechend, soweit nicht das derzeitige Saarländische Polizeigesetz speziellere Regelungen normiert. Denn die Tätigkeit der Polizei ist eine solche, die „nicht in den *(sachlichen)* Anwendungsbereich der Verordnung (EU) 2016/679" fällt, der wiederum in Art. 2 der DSGVO normiert ist. Dort ist die 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 ausdrücklich ausgenommen (Art. 2 Abs. 2 lit. d DSGVO).

1.1.5 ePrivacy-Verordnung

Die DSGVO regelt allgemein die Verarbeitung personenbezogener Daten durch öffentliche und nicht-öffentliche Stellen. Sie enthält indes keine speziellen Regelungen für den Umgang mit Daten und Informationen im Rahmen der elektronischen Kommunikation. Vielmehr war es die Absicht der EU-Kommission, zeitgleich mit der DSGVO eine Verordnung zu erlassen, die die rechtlichen Rahmenbedingungen beim Umgang mit sämtlichen Daten und Informationen, die aus der elektronischen Kommunikation herrühren, regelt und die eine Ergänzung und Präzisierung der DSGVO für diesen Bereich darstellt. Die Vorschriften dieser ePrivacy-Verordnung[11] sollen die bisher auf EU-Ebene gültige ePrivacy-Richtlinie aus dem Jahre 2002[12] und die diese abändernde sog. Cookie-Richtlinie aus dem Jahre 2009[13] ersetzen und an die Anforderungen des digitalen Zeitalters anpassen.

Ein erster Entwurf für diese Verordnung wurde erst am 10. Januar 2017 vorgelegt,[14] so dass angesichts des zu erwartenden Verhandlungsbedarfs die Einhaltung des ursprünglichen Zeitplans schon von vorneherein fraglich war. Die Beratungen im EU-

[11] Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation).

[12] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Dokumentation (ABl. Nr. L 201, S. 37).

[13] Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz vom 25.11.2009 (ABl. Nr. L 337, S. 11).

[14] Elektronisch abrufbar unter: http://ec.europa.eu/news-room/dae/document.cfm?doc_id=42678 (letzter Zugriff: 1.3.2019).

Parlament und im EU-Ministerrat verzögerten sich dann auch immer wieder und sind während der österreichischen Ratspräsidentschaft im zweiten Halbjahr 2018 nahezu zum Erliegen gekommen. Der Zeitpunkt des Beginns des sog. Trilog-Verfahrens zwischen EU-Kommission, EU-Parlament und EU-Ministerrat, das den Abschluss des Gesetzgebungsverfahrens darstellt, ist daher bis zum Ende des vorliegenden Berichtszeitraums nicht abzusehen. Aber auch nach einer Einigung in dem Trilog-Verfahren wird es noch eine Übergangszeit von mindestens einem Jahr, voraussichtlich aber eher zwei Jahren, bis zur endgültigen Wirksamkeit geben, so dass die ePrivacy-Verordnung wohl kaum vor 2021 anwendbar sein wird.

Der Verordnungsentwurf sieht vor, dass von seinem Anwendungsbereich neben den klassischen Telekommunikationsdiensten wie Telefon, E-Mail oder SMS, auch internetbasierte Kommunikationsdienste (sog. OTT-Dienste), wie WhatsApp, Facebook oder Skype, erfasst werden sollen.

Ein Grund für die Verzögerung ist, dass bislang keine Einigung über den Umgang mit Cookies und anderen Methoden zur Verfolgung des Onlineverhaltens der User (Tracking) erzielt werden konnte. Unternehmen der Werbeindustrie sowie andere Unternehmen, die ihr Geld mit den Daten der Nutzer verdienen, fordern, diese Daten auch ohne Einwilligung des Betroffenen auf der Grundlage einer Interessenabwägung zu Werbezwecken nutzen zu dürfen. Die Bundesregierung unterstützt die Belange der Werbeindustrie insoweit, als sie die kostenfreie Nutzung werbefinanzierter Onlinedienste von der Einwilligung des Nutzers in Cookies für Werbezwecke abhängig machen will.

Weiterer Beratungsbedarf ergibt sich auch wegen der erst später in den Entwurf aufgenommenen Regelung, wonach der Umgang mit sog. Metadaten einer Kommunikation (bspw. angerufene Nummern, besuchte Websites, der geografische Standort, Uhrzeit, Datum und Dauer eines von einer Person getätigten Anrufs) auch ohne Einwilligung der Nutzer für wirtschaftliche Zwecke des Anbieters zulässig sein soll. Da sich jedoch nicht nur aus den Inhaltsdaten einer Kommunikation, sondern auch aus den Metadaten tiefe Einblick in das Privatleben der an der elektronischen Kommunikation beteiligten Personen tätigen lassen, z. B. mit wem sie kommunizieren und wo ihre Interessen liegen, handelt es sich auch bei den Metadaten um schützenswerte personenbezogene Daten, deren Verarbeitung insbesondere für wirtschaftliche Zwecke nur mit einer ausdrücklichen Einwilligung zulässig sein darf.

Gerade in dem Bereich der elektronischen Kommunikation, die einen bedeutsamen Bestandteil des Lebens aller Bürger darstellt, sind klare Regelungen, die die Vertraulichkeit der Kommunikation der Betroffenen schützen, ein wesentliches Element zum Schutz der Privatsphäre und des Datenschutzrechts. Daher sollte sich auch der deutsche Gesetzgeber seiner Verantwortung bewusst sein und den weiteren Gesetzgebungsprozess in diesem Sinne unterstützen bzw. vorantreiben.

Jedenfalls muss der Gesetzgebungsprozess trotz der massiven Lobbyarbeit der Online-Werbewirtschaft, die ihre werbebasierten Geschäftsmodelle gefährdet sieht, im Sinne des Schutzes der Betroffenen wieder Fahrt aufnehmen.

1.2 Aus der Dienststelle

1.2.1 Gesetzliche Ausgestaltung der Aufsichtsbehörde

Mit der Neufassung des Saarländischen Datenschutzgesetzes (SDSG) sind auch die Regelungen für die Landesbeauftragte bzw. den Landesbeauftragten für den Datenschutz und die dazugehörige Behörde an die Datenschutz-Grundverordnung (DSGVO) angepasst worden. Zur Gewährleistung der europarechtlich geforderten völligen Unabhängigkeit der oder des Landesbeauftragten für Datenschutz wurde das Unabhängige Datenschutzzentrum Saarland zwar nicht wie zahlreiche andere Datenschutzaufsichtsbehörden zu einer obersten Landesbehörde. Allerdings ist durch die gesetzlichen Regelungen trotz der weiterhin bestehenden organisatorischen Angliederung an den Landtag des Saarlandes gewährleistet, dass die Aufgabenwahrnehmung ohne jegliche Einflussnahme und damit unabhängig erfolgen kann.

Wie bereits bisher werden die Haushaltsmittel für die Dienststelle der Landesbeauftragten in einem separaten Einzelplan im Kapitel des Landtags ausgewiesen, so dass insoweit auch die geforderte finanzielle Unabhängigkeit des Datenschutzzentrums gegeben ist. Dennoch wurde diese finanzielle Unabhängigkeit nicht vollständig durch den Gesetzgeber umgesetzt. Da das Datenschutzzentrum kein Mitglied der Landesregierung ist und daher bei den Beratungen zur Haushaltsaufstellung nicht beteiligt ist, muss durch entsprechende Regelungen sichergestellt werden, dass im Haushaltsaufstellungsverfahren kein Einfluss auf die Haushaltsanmeldung der Behörde genommen werden kann. Ob und in welchem Umfang der Haushaltsvoranschlag der Datenschutzaufsichtsbehörde in den endgültigen Haushalt übernommen wird, darf allein das Parlament nach übergeordneten politischen und fiskalischen Gesichtspunkten entscheiden. Dementsprechend haben wir angeregt, für die Landesbeauftragte für Datenschutz – wie dies auch für den Rechnungshof geregelt ist – die in §§ 27 Abs. 3, 28 Abs. 3 und 29 Abs. 3 Landeshaushaltsordnung (LHO)[15] genannten Rechte im Rahmen der Aufstellung des Entwurfs des Haushaltsplans für entsprechend anwendbar zu erklären. Diese Anregung wurde allerdings vom Gesetzgeber nicht aufgegriffen.

1.2.2 Personelle Ausstattung der Aufsichtsbehörde

Bereits in dem letzten Tätigkeitsbericht wurde näher ausgeführt, dass ein stetig wachsender Beratungs- und Informationsbedarf sowohl der datenverarbeitenden Stellen als auch der Bürgerinnen und Bürger sowie eine steigende Zahl verpflichtend durchzuführender Prüfungen durch die Aufsichtsbehörden zwangsläufig auch mit ei-

[15] Haushaltsordnung des Saarlandes in der Fassung der Bekanntmachung v. 5.11.1999 (Amtsbl. 2000 S. 194), zuletzt geändert d. Gesetz v. 12.12.2018 (Amtsbl. I S. 832).

nem steigenden Personalbedarf bei unserer Dienststelle einhergeht. Mit Geltungseintritt der Datenschutz-Grundverordnung sind umfangreiche neue Aufgaben für die Datenschutzaufsichtsbehörden hinzugekommen. Dies machte die ohnehin schon erforderliche personelle Verstärkung unserer Dienststelle umso dringender, zumal seit der Zusammenführung der Datenschutzaufsicht im öffentlichen und im nicht-öffentlichen Bereich bei der Landesbeauftragten für Datenschutz und Informationsfreiheit im Jahre 2012 die Dienststelle personell nicht mehr verstärkt wurde und mit insgesamt dreizehn Stellen auch im bundesweiten Vergleich im Hinblick auf die personelle Ausstattung das Schlusslicht bildete.

Zur Bewältigung der anstehenden Aufgaben wurden daher für das Haushaltsjahr 2018 insgesamt acht neue Stellen beantragt. Wenn auch der saarländische Landtag letztlich nur vier zusätzliche Stellen bewilligt hat, zeigt dies angesichts der nach wie vor angespannten Haushaltslage des Saarlandes dennoch, dass der Haushaltsgesetzgeber die Notwendigkeit einer Stärkung der Aufsichtsbehörde erkannt und entsprechend gehandelt hat.

Die Besetzung der neu zugewiesenen Stellen sowie die durch Personalwechsel erforderlich gewordenen Stellenneubesetzungen dauerten leider bis in das dritte Quartal des Jahres 2018, was für die Dienststelle rund um den Zeitpunkt des Wirksamwerdens der DSGVO im Mai 2018 eine kaum zu bewältigende Herausforderung darstellte; gerade im ersten Halbjahr 2018 war der Beratungsbedarf der verantwortlichen Stellen hinsichtlich Umsetzung der neuen datenschutzrechtlichen Vorschriften enorm groß und personell kaum zu bewältigen.

Da bereits frühzeitig erkennbar war, dass die für das Haushaltsjahr 2018 vorgesehenen 17 Planstellen nicht ausreichen werden, um insbesondere die mit der DSGVO verbundenen Herausforderungen zu bewältigen, hat der Landtag zum Ende des Berichtszeitraums für den Doppelhaushalt 2019/2020 zwei weitere Stellen bewilligt. Für diese Unterstützung möchte ich den Abgeordneten des saarländischen Landtags ausdrücklich danken.

Bis zu den nächsten Haushaltsberatungen wird sich noch deutlicher zeigen, welche Auswirkungen die neuen Regelungen auf die Tätigkeit der Aufsichtsbehörden haben werden und in welchem Umfang – gerade auch im Hinblick auf weitere zu erwartende aufsichtsbehördliche Aufgaben, wie sie bspw. die ePrivacy-Verordnung mit sich bringen wird – personell nachjustiert werden muss. Ungeachtet des aufgrund des neuen Rechtsrahmens erweiterten Aufgabenspektrums der Datenschutzaufsichtsbehörden, werden insbesondere die fortschreitende Digitalisierung nicht nur im Bereich der Wirtschaft, sondern auch in der öffentlichen Verwaltung weitere Herausforderungen für den Datenschutz mit sich bringen, die nur durch personell starke und fachlich kompetent besetzte Datenschutzbehörden bewältigt werden können. Im Saarland ergibt sich weiterhin die Besonderheit, dass durch den Forschungsschwerpunkt zum Thema IT-Sicherheit an der hiesigen Universität der Kooperationsbedarf seitens der bestehenden und neuen Institute mit der Datenschutzaufsicht zunehmen wird.

1.2.3 Veranstaltungen und Informationsmaterialien

Der Informationsbedarf der verantwortlichen Stellen hinsichtlich der DSGVO und ihrer Umsetzung war im Berichtszeitraum erwartungsgemäß außerordentlich hoch. Daher haben wir einen Schwerpunkt unserer Tätigkeit auf Beratung und Sensibilisierung der verantwortlichen Stellen gelegt, was sowohl bei den nicht-öffentlichen als auch bei den öffentlichen Stellen des Landes auf große Resonanz gestoßen ist.

Um den Unternehmen Hilfestellungen für die Anwendung der DSGVO in der Praxis zu geben, hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) sogenannte „Kurzpapiere" zu verschiedenen Schwerpunktthemen veröffentlicht. Diese Kurzpapiere dienten den Unternehmen als erste Orientierungen bei der Auslegung der neuen Vorschriften.

Unerwartet hoch war die Verunsicherung der Vereine hinsichtlich ihrer Pflichten bei der Umsetzung der neuen datenschutzrechtlichen Vorgaben. Der damit einhergehende Bedarf an Beratung und die vielfachen Anfragen von Vereinsvertretern an unsere Dienststelle haben uns dazu veranlasst, einen Informationsflyer zu erstellen, in dem die wesentlichen datenschutzrechtlichen Pflichten, die auch von Vereinen umzusetzen sind, dargestellt werden. Die große Nachfrage nach diesem Flyer hat deutlich gezeigt, dass den Vereinen bewusst geworden ist, dass die datenschutzrechtlichen Vorgaben auch für sie Anwendung finden und sie diese Pflichten auch sehr ernst nehmen. Im Rahmen unserer personellen Möglichkeiten haben wir neben den schriftlichen Informationen auch Veranstaltungen für Vereine angeboten, wobei aufgrund der Auslastung des Datenschutzzentrums gewährleistet sein musste, dass sich die jeweiligen Einladungen an einen möglichst großen Kreis interessierter Zuhörer richteten.

Für Unternehmen haben wir in Zusammenarbeit mit der Industrie- und Handelskammer des Saarlandes verschiedene Veranstaltungen angeboten, durch die zahlreiche Unternehmen und deren Datenschutzbeauftragte erreicht werden konnten. Weitere Veranstaltungen wurden beispielsweise gemeinsam mit der Arbeitskammer und den Handwerksinnungen durchgeführt.

Auch seitens der öffentlichen Verwaltung war das Interesse an den neuen datenschutzrechtlichen Vorgaben der DSGVO und der landesrechtlichen Anpassungen sehr groß. Daher hielten die Landesbeauftragte und mehrere Mitarbeiter zahlreiche Vorträge in den verschiedensten Bereichen der Landesverwaltung und allgemein für die behördlichen Datenschutzbeauftragten der Landesverwaltung. Besonders großen Zuspruch gab es auch für zwei Veranstaltungen für kommunale Mitarbeiter. Großes Interesse besteht auch nach wie vor an Veranstaltungen, die sich mit der Umsetzung datenschutzrechtlicher Regelungen im Bildungsbereich befassen.

Aber auch die Bürgerinnen und Bürger haben sich sehr dafür interessiert, was sich mit den neuen datenschutzrechtlichen Regelungen für sie ändert und welche Rechte ihnen als Betroffene nach der DSGVO zustehen. Dies zeigte sich ganz besonders am Tag der offenen Tür des Landtags des Saarlandes, bei dem die Dienststelle des Datenschutzzentrums die Möglichkeit hatte, ihre Tätigkeit an einem Informationsstand zu präsentieren.

Dass allgemein ein deutlich gestiegenes Interesse an Fragen des Datenschutzes und der Tätigkeit unserer Dienststelle besteht, belegt auch der enorme Anstieg an Anfragen nicht nur der regionalen, sondern auch der überregionalen Medien. Mittlerweile erreichen das Datenschutzzentrum nahezu täglich Auskunftsersuchen zu allgemeinen Themen oder zu spezifischen Einzelsachverhalten.

1.2.4 Zusammenarbeit mit dem Landtag

Die Zusammenarbeit unserer Dienststelle mit dem Landtag ist ein ganz wesentlicher Aspekt, unsere Arbeit gegenüber dem Gesetzgeber – außerhalb der gesetzlich vorgegebenen Verpflichtung zur Vorlage eines Tätigkeitsberichts – transparent zu machen und zugleich die Abgeordneten über wesentliche datenschutzrechtliche Entwicklungen zu informieren.

Mit Beginn der neuen Legislaturperiode im Frühjahr 2017 wurde für die parlamentarische Behandlung der Themen aus den Bereichen Datenschutz und Informationsfreiheit nicht wie in der vorangegangenen Legislaturperiode ein selbstständiger Ausschuss, sondern ein Unterausschuss des Ausschusses für Inneres und Sport mit einer gegenüber einem regulären Ausschuss reduzierten Mitgliederzahl eingesetzt. Insgesamt tagte dieser Unterausschuss im Berichtzeitraum 15-mal, wobei er davon siebenmal zu den Beratungen des Ausschusses für Inneres und Sport hinzugezogen wurde, in dem die saarländischen Gesetze zur Anpassung an die DSGVO behandelt wurden und zu denen unserer Dienststelle die Gelegenheit zur Stellungnahme eingeräumt worden ist. In den meisten anderen Sitzungen des Unterausschusses haben wir zu aktuellen datenschutzrechtlichen und informationstechnischen Fragestellungen Auskünfte erteilt und Stellungnahmen abgegeben.

Darüber hinaus wurde die Landesbeauftragte auch von anderen Ausschüssen um datenschutzrechtliche Würdigungen verschiedener Sachverhalte gebeten. Beispielhaft sei in diesem Zusammenhang die Stellungnahme der Landesbeauftragten zu datenschutzrechtlichen Fragen der Telemedizin genannt [vgl. hierzu Kap. 10.5 (S. 89)].

Insgesamt gab es stets eine vertrauensvolle Zusammenarbeit sowohl mit der Landtagsverwaltung als auch mit den verschiedenen im Landtag vertretenen Fraktionen, für welche an dieser Stelle ein Dank auszusprechen ist.

1.2.5 Zusammenarbeit mit anderen Stellen

Bereits in der Vergangenheit haben die Datenschutzaufsichtsbehörden des Bundes und der Länder immer intensiv zusammengearbeitet. Mit der DSGVO wird nicht nur diese Zusammenarbeit, sondern auch die Kooperation mit den Aufsichtsbehörden der europäischen Mitgliedstaaten intensiver werden, denn nur so kann die angestrebte einheitliche Anwendung der DSGVO in ganz Europa erreicht werden.

Auf EU-Ebene wurde der Europäische Datenschutzausschuss EDSA (European Data Protection Board – EDPB) als das wichtigste Gremium für die Zusammenarbeit der

EU-Mitgliedstaaten eingerichtet. Er ist eine Einrichtung der Europäischen Union mit eigener Rechtspersönlichkeit,[16] nimmt seine Aufgaben und Befugnisse unabhängig wahr und unterliegt hierbei keinen Weisungen.[17] Der EDSA hat seinen Sitz in Brüssel und setzt sich aus den Leitern der nationalen Datenschutzbehörden (bzw. deren Vertretern) und dem Europäischen Datenschutzbeauftragten (EDSB) zusammen. Ein für die Dauer von fünf Jahren gewählter Vorsitz vertritt den Ausschuss.

Deutschland ist durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) als gemeinsame Vertreterin der Aufsichtsbehörden des Bundes und der Länder im EDSA vertreten. Als Stellvertreter wählt der Bundesrat eine Leiterin oder einen Leiter der Aufsichtsbehörde eines Landes. Für die Ermittlung einer gesamtdeutschen Position im EDSA gibt es ein im Bundesdatenschutzgesetz (BDSG) vorgeschriebenes Verfahren.

Zur Hauptaufgabe des EDSA gehört, die einheitliche Anwendung der DSGVO sowie der EU-Datenschutz-Richtlinie im Bereich Justiz und Inneres (JI-Richtlinie) in allen EU-Mitgliedstaaten sicherzustellen.[18] Hierfür weisen ihm die DSGVO und die JI-Richtlinie ein umfangreiches Aufgabenspektrum[19] zu. Bei seinen Aufgaben wird der EDSA durch die sog. Subgroups unterstützt, die die unterschiedlichen Themengebiete fachspezifisch begleiten. Eine besondere Rolle fällt dem EDSA bei der Zusammenarbeit der einzelnen europäischen Aufsichtsbehörden im Kohärenzverfahren[20] zu, das die einheitliche Rechtsanwendung sowie die Aufsicht über die Einhaltung des Datenschutzes innerhalb der EU sicherstellen soll.

Auf nationaler Ebene ist das Unabhängige Datenschutzzentrum Saarland an 23 Arbeitskreisen, die mindestens einmal im Jahr tagen, beteiligt. Zudem finden jährlich zwei Datenschutzkonferenzen auf Bundesebene, dazugehörig zwei Vorkonferenzen und mindestens vier Sonderkonferenzen statt. Daneben beteiligt sich das Datenschutzzentrum an zahlreichen Workshops, Ad-Hoc-Arbeitsgruppen und Taskforces, so dass – wie auch bei anderen Datenschutzbehörden – immer mehr Mitarbeiter in die Zusammenarbeit auf bundesdeutscher bzw. europäischer Ebene mit dem Ziel einer einheitlichen Anwendung des Datenschutzrechts eingebunden sind.

Im Rahmen dieser Zusammenarbeit spielen die bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit angesiedelte Zentrale Anlaufstelle (ZASt) und das Internal Market Information System (IMI) eine wichtige Rolle.

Die Datenschutz-Grundverordnung ermöglicht es, dass ein Mitgliedstaat durchaus mehrere nationale Datenschutzaufsichtsbehörden haben kann. Die föderale Struktur der Bundesrepublik Deutschland ist mit der Datenschutzbeauftragten des Bundes und insgesamt 17 allgemeinen Datenschutzaufsichtsbehörden der Länder einzigartig in Europa. Um eine reibungslose Zusammenarbeit der Aufsichtsbehörden Deutschlands mit den europäischen Aufsichtsbehörden zu gewährleisten, hat der deutsche Gesetzgeber quasi als Bindeglied zwischen der europäischen und der nationalen

[16] Art. 68 DSGVO.

[17] Art. 69 DSGVO.

[18] Art. 70 Abs. 1 DSGVO.

[19] Art. 70 Abs. 1 lit. a-y DSGVO; Art. 51 Abs. 1 lit. a-j JIRL.

[20] Art. 63 DSGVO.

Ebene die ZASt als „single contact point“ etabliert, die diese Zusammenarbeit koordiniert und gewährleistet, dass die deutschen Aufsichtsbehörden auf europäischer Ebene mit einer einheitlichen und verhandlungsstarken Position auftreten. Zudem ermöglicht sie es den nationalen europäischen Aufsichtsbehörden, der Europäischen Kommission und dem EDSA ohne Kenntnisse innerstaatlicher Zuständigkeiten, effektiv mit den deutschen Aufsichtsbehörden zu kommunizieren.

Das IMI-System hingegen ist eine bereits 2012 von der EU-Kommission entwickelte webbasierte Kommunikationsplattform. Sie ermöglicht es Behörden aus allen EU-Mitgliedstaaten (sowie Norwegen, Island und Liechtenstein), auf allen jeweils zuständigen Ebenen (europäisch, national, regional und lokal) schnell und einfach elektronisch miteinander zu kommunizieren und notwendige Informationen auszutauschen. Hindernisse, wie sie sich z. B. durch Sprachbarrieren oder unterschiedliche Verwaltungsstrukturen ergeben, können leichter überwunden bzw. die Suche nach dem richtigen Ansprechpartner kann erleichtert werden.

Mit Geltung der DSGVO wurden nunmehr auch die europäischen Datenschutzaufsichtsbehörden in das IMI-System eingebunden, um eine möglichst reibungslose und schnelle Zusammenarbeit in grenzüberschreitenden Angelegenheiten zu ermöglichen.

2 Justiz und Recht

2.1 Veröffentlichung einer Schöffenliste

Der Geltungseintritt der Datenschutz-Grundverordnung (DSGVO) am 25. Mai 2018 hat auch im öffentlichen Bereich allerorten zu einer erhöhten Sensibilität in Fragen des Datenschutzes geführt. Positiv ist dabei zu vermerken, dass die behördlichen Stellen des Landes und seine Kommunen auch bereits Jahrzehnte lang praktizierte Verwaltungstätigkeiten in datenschutzrechtlicher Hinsicht auf den Prüfstand stellen und gegebenenfalls an die neuen gesetzlichen Vorgaben anpassen. In vielen derartigen Anpassungsprozessen wird das Unabhängige Datenschutzzentrum Saarland als Aufsichtsbehörde zu Rate gezogen. Nicht selten zeigt sich dabei, dass auf den ersten Blick vermeintlich kritische Verarbeitungsprozesse bei genauerer Betrachtung gleichwohl einer datenschutzrechtlichen Kontrolle standhalten.

Ein anschauliches Beispiel für letzteres ist die Veröffentlichung personenbezogener Daten in Form von Vorschlagslisten für die Wahl ehrenamtlicher Richter in Strafsachen (Schöffen).

Gemäß § 28 des Gerichtsverfassungsgesetzes (GVG)[21] werden für die Verhandlung und Entscheidung der zur Zuständigkeit der Amtsgerichte gehörenden Strafsachen, soweit nicht der Strafrichter entscheidet, Schöffengerichte gebildet. Das Schöffenamt ist ein Ehrenamt, welches von erwachsenen deutschen Staatsangehörigen im Alter von 25 bis 70 Jahren ausgeübt werden kann/darf (§§ 31, 33 GVG).

Hinsichtlich der Auswahl der Schöffinnen und Schöffen überträgt das Gerichtsverfassungsgesetz den Gemeinden die Aufgabe, durch Aufstellung von Vorschlagslisten die Schöffenwahl vorzubereiten (§ 36 Abs. 1 S. 1 GVG). Der diesbezügliche Inhalt der Vorschlagslisten wird in § 36 Abs. 2 S. 2 GVG geregelt und setzt sich zwingend aus dem Geburtsnamen, dem Familiennamen, dem Vornamen, dem Tag und Ort der Geburt, der Wohnanschrift und dem Beruf der vorgeschlagenen Personen zusammen. § 36 Abs. 3 GVG ordnet weiter an, dass die aus diesen Daten zusammengesetzte Vorschlagsliste in der Gemeinde eine Woche lang zu jedermanns Einsicht „*aufzulegen*" (§ 36 Abs. 3 GVG) und der Zeitpunkt der Auflegung vorher öffentlich bekannt zu machen ist.

Die Tragweite dieser gesetzlich angeordneten Datenverarbeitung mag zunächst vielleicht verwundern, werden hierbei doch auch sehr persönliche Informationen, wie das Geburtsdatum, die Wohnanschrift und der Beruf einer Person der Öffentlichkeit offengelegt. Aus hiesiger Sicht ist es demnach verständlich, dass von Seiten der Gemeinden diesbezügliche Bedenken an unsere Behörde herangetragen wurden. Zu berücksichtigen ist jedoch, dass auch der Datenschutz dem immanenten Spannungsverhältnis widerstreitender Rechtspositionen (Normenkollisionen) nicht vollständig

[21] In der Fassung der Bekanntmachung vom 9. Mai 1975 (BGBl. I S. 1077), zuletzt geändert d. Gesetz v. 30.10.2017 (BGBl. I S. 3618).

entzogen ist. Mit anderen kollidierenden Verfassungsgütern ist er vielmehr in einen angemessenen Ausgleich zu bringen, was im Einzelfall auch ein Beschneiden datenschutzrechtlicher Positionen gebietet, sofern eine entsprechende Rechtfertigung hierfür ersichtlich ist.

Eine derartige Rechtfertigung findet sich für die Veröffentlichung der in Bezug genommenen Vorschlagslisten in dem Umstand, dass mit der Bekleidung des Schöffenamtes Befugnisse der Rechtsprechung einhergehen (§ 30 Abs. 1 GVG) und somit ein gesteigertes öffentliches Interesse an der zur Wahl stehenden Personen besteht. Die diesbezügliche Transparenz soll hinreichende Gewähr dafür bieten, dass die jeweilige Person die Fähigkeit zur Bekleidung des Schöffenamtes besitzt. Insbesondere das jedermann zustehende, voraussetzungslose Einspruchsrecht[22] gegen die Vorschlagsliste für Schöffen gemäß § 37 GVG kann nur dann in effektiver Art und Weise ausgeübt werden, wenn die Person des zu berufenden Schöffen hinreichend bekannt ist.

2.2 Einführung der Online-Anhörung in der Zentralen Bußgeldbehörde

Im Oktober 2017 übersandte uns das Landesverwaltungsamt (LaVA) in seiner Funktion als Zentrale Bußgeldbehörde (ZBB) ein Konzept zur Einführung der Online-Anhörung in Bußgeldverfahren bei Verkehrsordnungswidrigkeiten mit der Bitte um Wahrnehmung unserer Beteiligungsrechte. Grund für die Information und Beteiligung des Datenschutzzentrums ist, dass es sich bei der geplanten Verfahrensänderung um eine informationstechnische Erweiterung des bisher bestehenden Systems handelt.

Das Landesverwaltungsamt setzte bisher zur Bearbeitung der Ordnungswidrigkeitsverfahren das Fachverfahren WinOWiG ein. Gem. § 55 des Gesetzes über Ordnungswidrigkeiten (OWiG)[23] ist dem Betroffenen in einem Verkehrsordnungswidrigkeitenverfahren die Möglichkeit zu geben, im Rahmen einer Anhörung zu dem vorgeworfenen Verstoß Stellung zu nehmen. Derzeit erfolgt diese Anhörung in Papierform. Im Fachverfahren WinOWiG besteht nach Angaben der ZBB die Möglichkeit der technischen Implementierung eines Moduls „Online-Anhörung", wodurch dem Betroffenen die Möglichkeit eröffnet werden soll, die Angaben im Rahmen eines Anhörungsverfahrens über ein Online-Portal unter Verzicht auf die Papierform direkt an die Behörde zu übermitteln. Konkret sollen die Betroffenen mittels persönlicher Zugangsdaten, die auf dem Anhörungsbogen angegeben sind, online auf einem abgesicherten Server die Beweisbilder zu ihrem Fall einsehen, den Anhörungsbogen ausfüllen und an die ZBB zurückschicken können. Die Daten sollen automatisch im Programm übernommen werden. Für die Online-Anhörung soll ein eigener Server beim IT-Dienstleistungszentrum des Landes eingerichtet werden.

---

22 *Goers*, in: Graf BeckOK GVG (2018), § 37 Rn. 1.

23 Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19.2.1987 (BGBl. I S. 602), zuletzt geändert d. Gesetz v. 17.12.2018 (BGBl. I S. 2571).

Aus unserer Sicht bestehen keine grundsätzlichen Bedenken gegen die Einführung der Online-Anhörung in Bußgeldverfahren bei Verkehrsordnungswidrigkeiten. Der Schwerpunkt unserer Bewertung lag daher auf der Gewährleistung/Umsetzung technischer und organisatorischer Maßnahmen.

Zur Gewährleistung der Vertraulichkeit und Integrität der über das Onlineformular erfassten Daten war beabsichtigt, ein von der Entwicklerfirma eigens entwickeltes, proprietäres Kryptoverfahren (in Form einer Blockverschlüsselung) einzusetzen. Zur Gewährleistung der Schutzziele der Vertraulichkeit und Integrität muss ein Verfahren zum Einsatz kommen, das dem Stand der Technik entspricht. Maßstab für den Stand der Technik sind unter anderem die entsprechenden technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die uns zur Verfügung gestellten Informationen ließen eine Bewertung der Belastbarkeit des kryptographischen Verfahrens indes nicht zu. Vielmehr drängte sich der Eindruck auf, dass die Sicherheit des Kryptoverfahrens hier entscheidend von der Geheimhaltung des Verschlüsselungsalgorithmus abhing („Security through obscurity"). Dies, wie auch das Fehlen einer (externen) Zertifizierung des Kryptoverfahrens führten dazu, dass wir auf eine Änderung der kryptographischen Absicherung des Verfahrens drängten. Denn weder entspricht es nach hiesiger Auffassung dem Stand der Technik, dass die Sicherheit eines Kryptoverfahrens allein durch die Entwickler bewertet wird, sondern vielmehr bedarf es einer Evaluierung durch externe Experten, um eine hinreichende Belastbarkeit nachweisen zu können. Noch entspricht es dem Stand der Technik, wenn Kryptoverfahren zum Einsatz kommen, deren Sicherheit auf der Geheimhaltung des Verfahrens beruhen. Aus datenschutzrechtlicher Sicht hinreichend starke Verschlüsselungsalgorithmen wie beispielsweise der Advanced Encryption Standard oder das RSA-Kryptosystem, erfordern gerade keine Geheimhaltung des Verfahrens, sondern nur des verwendeten Schlüssels („Kerckhoffs'sches Prinzip").

Unklar – mit Blick auf die Planungen des LaVA – ist noch, ob die Online-Anhörung nur für die Anhörung von Betroffenen genutzt werden soll oder auch für Zeugenvernehmungen. Da für Zeugenvernehmungen die Schriftform bzw. gemäß § 110c OWiG i. V. m. § 32a StPO die Vorgaben des elektronischen Rechtsverkehrs erforderlich sind, müssten die Erklärungen von Zeugen qualifiziert elektronisch signiert werden, was die von der Software-Firma zur Verfügung gestellte Lösung aber derzeit nicht sicherstellt.

Einwände hatten wir auch gegen die Verarbeitung/Protokollierung der IP-Adresse. Geplant war diese zu protokollieren, um später nachweisen zu können, dass das Formular von einer bestimmten Person ausgefüllt wurde. Die IP-Adresse als Anknüpfungsmerkmal für den Nachweis der Identität einer bestimmten Person hielten wir hingegen für ungeeignet. Sofern ein (rechtliches) Erfordernis zum Nachweis der Identität besteht, existiert mit der eID-Funktion des Personalausweises eine zuverlässige alternative Möglichkeit, die es dem Betroffenen erlaubt, sich – anders als über die Verwendung der IP-Adresse – sicher, eindeutig und vor allem transparent über das Onlineformular gegenüber der Bußgeldbehörde identifizieren zu können.

Die Einführung der Online-Anhörung ist bei Erstellung dieses Tätigkeitsberichtes noch nicht abgeschlossen. Wir werden das Verfahren weiter begleiten.

2.3 Nutzung von Daten aus dem Personalausweis- und Passregister zum Zweck der Fahreridentifizierung

Auch im vorliegenden Berichtszeitraum wandten sich Beschwerdeführer an unsere Dienststelle und zeigten sich besorgt über die Verwaltungspraxis der Erforschung und Ahndung von Verkehrsordnungswidrigkeiten mittels Lichtbildabgleichs über den Datenbestand des Personalausweis- und Passregisters. Hierbei veranlassen die zuständigen Behörden, oftmals auch zum Zwecke der Sanktionierung relativ geringfügiger Ordnungswidrigkeiten im Verwarngeldbereich, einen Datenabgleich, bei welchem sie sich die jeweiligen Informationen von den zuständigen Personalausweis- und Passbehörden übermitteln lassen. Erst auf diese Weise erscheint es ihnen vielfach möglich, anhand von Vergleichsbildern Nachforschungen im unmittelbaren Familienkreis des Fahrzeughalters anzustellen und so den in Bezug genommenen Fahrzeugführer zu identifizieren.

Ihre rechtlichen Grundlagen findet die vorgenannte Verwaltungspraxis in § 24 Abs. 2 Personalausweisgesetz (PAuswG)[24] und § 22 Abs. 2 Paßgesetz (PaßG)[25]. Hiernach dürfen Personalausweis- und Passbehörden anderen Behörden auf deren Ersuchen Daten aus den von ihnen geführten Registern übermitteln, wenn *„(…) die ersuchende Behörde ohne Kenntnis der Daten nicht in der Lage wäre, eine ihr obliegende Aufgabe zu erfüllen und die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können (…)"*.

Konkretisiert wird das diesbezügliche Verfahren durch den Erlass des damaligen Ministeriums für Inneres, Familie, Frauen und Sport vom 14. April 2005 zur Nutzung von Daten aus dem Personalausweis- und Passregister zum Zweck der Fahreridentifizierung (Az.: D4-B 1-1; Tgb.-Nr.: 15/05). Hiernach ist zwingende Voraussetzung eines Lichtbildabgleichs, dass vor der Datenübermittlung von der Passbehörde an die Bußgeldbehörde dem Betroffenen – in der Regel dem Halter des Kraftfahrzeugs (Kfz) – unter Vorlage des im Zuge der Verkehrsüberwachung angefertigten Lichtbildes Gelegenheit zur Stellungnahme zu geben ist.

Ausdrücklich Abstand genommen hat das Innenministerium hingegen von seiner vormalig restriktiven Erlasslage, wonach dem Ermittlungsersuchen eine *„(…) bedeutende Verkehrsordnungswidrigkeit (…)"* zugrunde liegen musste. Begründet wird dies zum einen mit Erwägungen einer effektiven Verfolgung und Sanktionierung von Verkehrsverstößen, zum anderen mit der Überlegung, dass die Alternative zu einem Lichtbildabgleich, nämlich das Treffen von Ermittlungsmaßnahmen vor Ort im familiären und nachbarlichen Umfeld, sich oftmals als besonders eingriffsintensiv darstellen könnten, der Lichtbildabgleich mithin das mildere Mittel sei.

---

[24] Gesetz über Personalausweise und den elektronischen Identitätsnachweis vom 18. Juni 2009 (BGBl. I S. 1346), zuletzt geändert d. Gesetz v. 18. Juli 2017 (BGBl. I S. 2745).

[25] Paßgesetz vom 19. April 1986 (BGBl. I S. 537), zuletzt geändert d. Gesetz v. 7. Juli 2017 (BGBl. I S. 2310).

Bereits im Berichtzeitraum 2005/2006 (vgl. 21. Tätigkeitsbericht, S. 27) äußerte der damalige Landesbeauftragte für Datenschutz und Informationsfreiheit seine Bedenken gegenüber dieser bis zum heutigen Tag unveränderten Erlasslage, da hiernach bereits dann eine Erhebung von Daten aus dem Personalausweis- und Passregister zulässig sei, wenn lediglich die Verfolgung und Ahndung geringfügiger Verstöße im Verwarngeldbereich im Raum stehe. Eine Abwägung zwischen dem Grundrecht auf informationelle Selbstbestimmung und dem Sanktionsinteresse des Staates gebiete indes Zurückhaltung in den Bereichen geringfügiger Gesetzesverstöße, gerade vor dem Hintergrund, dass die Existenz von Lichtbildern des Gesichts in den Personalausweis- und/oder Passregistern den Bürgerinnen und Bürgern nicht zur Disposition stünde, diese folglich hierdurch bereits einen – wenn auch verfassungskonformen – Eingriff in ihr Persönlichkeitsrecht erdulden müssten, was auf der Gegenseite als Korrelat eine Weiterverarbeitung dieser Daten nur unter besonderen Voraussetzungen gebiete.

An der Richtigkeit und Aktualität dieser Erwägungen hat sich bis zum heutige Tag nichts geändert. Im Gegenteil erscheint es unter Geltung der Datenschutz-Grundverordnung sowie der Datenschutz-Richtlinie im Bereich von Justiz und Inneres umso dringlicher, durch eine zurückhaltende Weiterverarbeitung von Registerdaten dem in beiden Rechtsregimen verankerten Verhältnismäßigkeitsgebot Rechnung zu tragen.

Dies bedeutet zunächst, dass im Rahmen des Ermittlungsverfahrens streng nach Erlasslage zu verfahren ist, d. h. der betroffenen Person vor einem Einsichtnahmeersuchen unter Vorlage des zur Dokumentation des Verkehrsverstoßes angefertigten Lichtbildes Gelegenheit zur Stellungnahme zu geben ist. In diesem Zusammenhang ist der Betroffene (§ 66 Abs. 1 Nr. 1 OWiG) ausdrücklich darauf hinzuweisen, dass im Falle einer Auskunftsverweigerung ein entsprechender Lichtbildabgleich vorgenommen werden kann. Erst wenn der Betroffene trotz dieser Information keine Angaben zu der Verkehrsordnungswidrigkeit machen kann oder will, kommt eine Weiterverarbeitung der Registerdaten in Form eines Lichtbildabgleichs nach § 24 Abs. 2 Nr. 2 u. 3 PAuswG und § 22 Abs. 2 Nr. 2 u. 3 PaßG in Betracht.

Des Weiteren beschränkt das sowohl dem deutschen Recht[26] als auch dem Unionsrecht[27] immanente Gebot der Verhältnismäßigkeit ein Übermittlungsersuchen in den Fällen, in welchen dem beabsichtigten Lichtbildabgleich eine nur geringfügige Verkehrsordnungswidrigkeit zugrunde liegt. Dieses allgemein anerkannte Rechtstaatsprinzip untersagt auch vom Grundsatz her zunächst gesetzlich zulässige Maßnahmen, sofern deren Nutzen zu den dadurch herbeigeführten Beeinträchtigungen außer Verhältnis steht.[28]

Letzteres ist aus hiesiger Sicht insbesondere in Fällen der Verwarnung mit Verwarngeld nach § 56 Abs. 1 OWiG der Fall. Die Verwarnung, ob mit oder ohne Verwarngeld, beschränkt sich auf Sachverhalte geringfügiger Verkehrsverstöße. Sie stellt keine Vergeltung gegenüber dem Verwarnten dar und enthält auch keinen ethischen

[26] *Grzeszieck*, in: Maunz/Dürig, GG (48. EL), Art. 20 Rn. 107.

[27] *Kingreen*, in: Calliess/Ruffert, EUV/AEUV (5. Aufl. 2016), Art. 36 Rn. 88.

[28] *Grzeszieck*, in: Maunz/Dürig, GG (48. EL), Art. 20 Rn. 117.

Schuldvorwurf.[29] Als Mittel zur Festigung der Verkehrsdisziplin kann die Verwarnung nach allgemein pädagogischer Erfahrung nur dann Wirksamkeit entfalten, wenn sie der Tat auf dem Fuße folgt.[30] Dies schließt es aus, eine Verwarnung erst nach u. U. länger andauernden Ermittlungen nach dem Fahrzeugführer zu erteilen.

Gleiches gilt für Geldbußen in Höhe eines Verwarngeldes. Auch in diesen Fällen erscheint es mehr als fraglich, ob die Verfolgung und Ahndung einer relativ geringfügigen Gesetzesübertretung Eingriffe in Grundrechte eines unbestimmten, größeren Personenkreises rechtfertigt. Von der Verwaltungspraxis, über die Einwohnermeldeämter alle für einen Lichtbildabgleich in Betracht kommenden Personen im Haushalt des/der Kfz-Halters/Kfz-Halterin zu ermitteln, ist daher zumindest in den Fällen Abstand zu nehmen, in welchen die Höhe der beabsichtigten Geldbuße einen Betrag von 55,- € (vgl. § 56 Abs. 1 S. 1 OWiG) nicht übersteigt.

2.4 Datenübermittlung durch eine Gemeinde an gerichtlich bestellten Gutachter

Im Berichtszeitraum erhielten wir eine Beschwerde über einen gerichtlich bestellten Sachverständigen, der sich bei der Erstellung eines Gutachtens im Rahmen eines Baurechtsstreites bei einer Gemeindeverwaltung Daten erschlichen haben soll, die in keinem Zusammenhang mit dem Inhalt des gerichtlichen Beweisbeschlusses gestanden haben sollen. Diese Daten habe er dann in unzulässiger Weise durch Verwendung in dem Gutachten auch der Gegenseite des Gerichtsverfahrens zur Kenntnis gebracht. In gleicher Sache übersandte uns das Landesverwaltungsamt als Kommunalaufsicht die Beschwerde derselben Petenten gegen die Gemeinde, die die streitgegenständlichen Daten herausgegeben hatte, zur Überprüfung möglicher datenschutzrechtlicher Verstöße.

Es handelte sich um ein laufendes Gerichtsverfahren, bei dem sich die Parteien um die Nutzung eines Grundstückes stritten. Zur Klärung der Frage, ob die Nutzung des streitgegenständlichen Grundstückes nur einem bestimmten Zweck dienen sollte, erließ das zuständige Amtsgericht einen Beweisbeschluss zur Einholung eines Sachverständigengutachtens. Der gerichtlich bestellte Gutachter holte bei verschiedenen Stellen zu diesem Sachverhalt Auskünfte ein, unter anderem auch bei der Gemeinde, in der das streitgegenständliche Grundstück liegt. Die Gemeinde gab dem Sachverständigen aufgrund des vorgelegten Beweisbeschlusses eine Chronologie der Genehmigungsanfragen zu den Nachbargrundstücken der Beschwerdeführer aus den Jahren 2006 bis 2017 heraus. Diese Chronologie machte der Sachverständige zum Gegenstand seines Gutachtens und zog daraus Schlussfolgerungen für die Nutzungsmöglichkeiten des streitgegenständlichen Grundstückes.

Der Sachverhalt war nach alter Rechtslage zu beurteilen. Zunächst war zu prüfen, ob in einem laufenden Gerichtsverfahren eine Kontrollbefugnis unsererseits besteht, da

[29] BVerfG, Beschl. v. 04.07.1967 – 2 BvL 10/62, NJW 1967, S. 1748 (1749).

[30] BVerfG, Beschl. v. 04.07.1967 – 2 BvL 10/62, NJW 1967, S. 1748 (1749).

§ 2 Abs. 1 S. 4 Saarländisches Datenschutzgesetz a. F. (SDSG a. F.)[31] bestimmt, dass für Gerichte die Regelungen des SDSG nur gelten, soweit sie Verwaltungsaufgaben wahrnehmen. Allerdings wurde hier kein Handeln des Gerichts beanstandet, sondern die Erhebung und Weitergabe der Daten durch den gerichtlich bestellten Sachverständigen und die Übermittlung der Daten durch die Gemeinde an diesen. § 2 Abs. 1 S. 4 SDSG darf nicht so weit auszulegen sein, dass bei laufenden Gerichtsverfahren überhaupt keine Datenschutzkontrolle außerhalb der Verwaltungstätigkeit der Gerichte stattfinden kann.

Nach der datenschutzrechtlichen Prüfung des Sachverhaltes teilten wir den Beschwerdeführern mit, dass nach unserer Auffassung die Übermittlung der Daten durch die Gemeinde an den gerichtlich bestellten Sachverständigen nach § 16 Abs. 1 S. 1 lit. c SDSG a. F. zulässig war, da der Sachverständige durch Vorlage des Beweisbeschlusses ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft gemacht hat und für die Gemeinde kein Grund zu der Annahme bestand, dass das Geheimhaltungsinteresse der Betroffenen überwiegen könnte. Es handelte sich um ein gerichtliches Verfahren. Eine Prüfung, welche tatsächlichen und rechtlichen Schlussfolgerungen sich aus den übermittelten Daten für das Gerichtsverfahren ziehen lassen konnten, oblag nicht der Gemeinde, sondern zunächst dem Gutachter und dann dem Gericht. Die Gemeinde durfte davon ausgehen, dass es den Parteien um die rechtliche Klärung ihrer Nachbarschaftsstreitigkeit ging. Daher war es für die Gemeinde nicht ersichtlich, dass möglicherweise ein Geheimhaltungsinteresse der Betroffenen bestand.

Ähnliches galt für die Erhebung personenbezogener Daten bei der Gemeinde sowie die Übermittlung dieser an das Gericht durch den gerichtlich bestellten Sachverständigen. Gem. § 28 Abs. 1 S. 1 Nr. 2 Bundesdatenschutzgesetz a. F. (BDSG a. F.)[32] war das Erheben und Übermitteln personenbezogener Daten zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Der Gutachter hatte hier im Rahmen des Beweisbeschlusses Daten bei der Gemeinde zu den streitgegenständlichen Grundstücken eingeholt und diese in seine gutachterliche Bewertung über Historie und Zustand der Gebäude und Nutzungen der streitgegenständlichen Grundstücke aufgenommen. Die schlussendliche Bewertung in tatsächlicher und rechtlicher Hinsicht oblag dem Gericht.

Wir wiesen die Beschwerdeführer darüber hinaus darauf hin, dass Einwände gegen das Gutachten im gerichtlichen Verfahren geltend zu machen sind. Im Hinblick auf bei der Gemeinde gespeicherte Daten wiesen wir außerdem auf Auskunftsrechte gem. § 20 SDSG a. F. und die Sperrmöglichkeit nach § 21 Abs. 3 S. 2 SDSG a. F. hin.

---

[31] Saarländisches Gesetz zum Schutz personenbezogener Daten vom 28.1.2008 (Amtsbl. S. 293, ber. S. 883), letztmalig geändert d. Gesetz v. 15.11.2017 (Amtsbl. I S. 1007).

[32] Bundesdatenschutzgesetz vom 20.12.1990 (BGBl. I S. 2954), letztmalig geändert d. Gesetz v. 30.10.2017 (BGBl. I S. 3618).

2.5 Novellierung des § 203 StGB

§ 203 Strafgesetzbuch (StGB)[33] stellt den Schutz von Geheimnissen vor unbefugter Offenbarung sicher, die Angehörigen bestimmter Berufsgruppen (zum Beispiel Ärzte, Rechtsanwälte, Steuerberater oder Wirtschaftsprüfer) im Rahmen ihrer beruflichen Tätigkeit anvertraut werden. Bisher bestand für Berufsgeheimnisträger, die externe Dienstleister wie z. B. Abrechnungsfirmen und IT-Anbieter in Anspruch nehmen wollten, das Risiko, sich strafbar zu machen, wenn diese externen Unternehmen Kenntnis von den geschützten Berufsgeheimnissen erhalten konnten. Daher sah auch der Bundesgesetzgeber die Notwendigkeit, in diesem Bereich Rechtssicherheit für die Berufsgeheimnisträger zu schaffen. Mit dem „Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen"[34] sollte daher im Berichtszeitraum eine entsprechende Änderung des § 203 StGB erfolgen.

Da die Vorschrift in einem engen Bezug zum Datenschutz steht, haben sich die Datenschutzaufsichtsbehörden während des Gesetzgebungsverfahrens mit der beabsichtigten Novellierung befasst und eine Entschließung der Datenschutzkonferenz (DSK) verabschiedet (siehe Kap. 17.2). Darin wurde bemängelt, dass der Gesetzentwurf in Teilen nicht mit der Datenschutz-Grundverordnung (DSGVO) vereinbar sei. So sei es *„(…) weder mit dem Schutzzweck von § 203 StGB vereinbar noch datenschutzrechtlich zulässig, dass Berufsgeheimnisträger, wie im neuen § 203 StGB vorgesehen, die Verantwortung für die Datenverarbeitung ohne Einwilligung der Betroffenen an externe Dienstleister übertragen."* Es sei wichtig, die geplanten straf- und berufsrechtlichen Regelungen mit den datenschutzrechtlichen Vorschriften zu synchronisieren.

Der Gesetzgeber ist auf die Vorschläge aus der Entschließung jedoch nicht eingegangen. In der seit 9. November 2017 gültigen Fassung lautet § 203 Abs. 3 StGB daher:

„Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken."

Es bleibt abzuwarten, inwiefern der Gesetzgeber durch die Rechtsprechung aufgefordert wird, diese gesetzliche Regelung mit der DSGVO in Einklang zu bringen.

---

[33] Strafgesetzbuch in der Fassung der Bekanntmachung vom 13.10.1998 (BGBl. I S. 3322), zuletzt geändert d. Gesetz v. 18.12.2018 (BGBl. I S. 2639).

[34] Vom 30. Oktober 2017 (BGBl. I S. 3618).

2.6 Informationspflicht bei der Verarbeitung personenbezogener Daten durch Berufsgeheimnisträger

Wiederholt erhielten wir im Berichtszeitraum Anfragen betroffener Personen, die sich über Art und Umfang der datenschutzrechtlichen Informationspflichten durch Berufsgeheimnisträger informieren wollten. Konkret ging es in den entsprechenden Eingaben darum, ob in zivilrechtlichen Streitigkeiten der gegnerische Rechtsanwalt über Art und Umfang der Verarbeitung personenbezogener Daten nach Art. 14 Datenschutz-Grundverordnung (DSGVO) informieren müsse.

Grundsätzlich sieht Art. 14 DSGVO eine Informationspflicht vor, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden, d. h. die Datenerhebung ohne deren Mitwirkung erfolgt ist. Von einer Erhebung personenbezogener Daten ist danach regelmäßig bereits dann auszugehen, wenn ein Unternehmen oder sonstiger Verantwortlicher einen Rechtsanwalt mit der Wahrnehmung seiner Interessen beauftragt, da hierzu eine Weitergabe von Informationen über die Person des (Prozess-)Gegners und über das zugrundeliegende Rechtsverhältnis erforderlich ist. Die mit dieser Weitergabe korrespondierende Entgegennahme und Verwendung entsprechender Informationen durch den Rechtsanwalt stellt grundsätzlich eine die Informationspflicht nach Art. 14 DSGVO auslösende Erhebung personenbezogener Daten dar.

Für Berufsgeheimnisträger, wie Rechtsanwälte, hat der Bundesgesetzgeber in § 29 Abs. 1 S. 1 Bundesdatenschutzgesetz (BDSG) jedoch eine Ausnahme von der Informationspflicht vorgesehen, soweit durch ihre Erfüllung Informationen offenbart würden, die ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. § 29 Abs. 1 S. 2 BDSG sieht ähnliche Einschränkungen der Informationspflicht auch für das Recht auf Auskunft nach Art. 15 DSGVO vor.

Für die Pflicht der Informationserteilung gegenüber dem Prozessgegner und die Pflicht zur Auskunftserteilung sind die Ausnahmevorschriften des § 29 Abs. 1 S. 1 und 2 BDSG regelmäßig zu bejahen. Denn dem anwaltlichen Berufsgeheimnis unterfällt regelmäßig bereits die Tatsache, dass der Berufsgeheimnisträger für einen bestimmten Mandanten tätig wird. Zumeist würden bereits Teilinformationen Rückschlüsse auf diese Tatsache zulassen. Gerade Rechtsanwälte haben demzufolge gegenüber Gegnern, Zeugen und sonstigen „Drittbetroffenen", deren Daten sie im Rahmen einer Mandatsführung zwangsläufig verarbeiten (etwa in einen Schriftsatz benennen) keine Informationspflicht nach Art. 14 DSGVO.

Hiervon unberührt bleiben selbstverständlich die Informationspflichten nach spezielleren Rechtsvorschriften, z. B. § 43d Bundesrechtsanwaltsordnung (BRAO)[35].

[35] Bundesrechtsanwaltsordnung vom 1.8.1959 (BGBl. I S. 565), zuletzt geändert d. Gesetz v. 30.10.2017 (BGBl. I S. 3618).

3 Polizei

3.1 Videoüberwachung Vorplatz Hauptbahnhof und Bereich Johanneskirche

Bereits seit Ende 2016 gibt es Pläne der saarländischen Polizei in den Bereichen des Vorplatzes des Saarbrücker Hauptbahnhofs sowie im näheren Umfeld der Johanneskirche in Saarbrücken eine stationäre Videoüberwachungsanlage zu installieren. Die Landesbeauftragte für Datenschutz wurde über das Vorhaben und Art und Weise der geplanten Umsetzung frühzeitig informiert. Diese Planungen werden nunmehr konkret und mit einer Inbetriebnahme kann im Jahr 2019 gerechnet werden.

Zur Vorbereitung der entsprechenden Ausschreibungsunterlagen hat uns die mit der Planung und Realisierung der stationären Videoüberwachungsmaßnahme betraute Arbeitsgruppe frühzeitig eingebunden, sodass wir die Möglichkeit hatten, zusammen mit dem Landespolizeipräsidium (LPP) vor allem technische Anforderungen zu definieren, die das Gesamtsystem bestehend aus Videoerfassungseinheiten, Signaltransportkomponenten sowie Datenspeicherungssystemen und Datenauswertesysteme erfüllen muss, um datenschutzrechtliche Grundsätze hinreichend zu berücksichtigen. Für die ersten Wochen des Jahres 2019 sollen die Testsysteme von drei Anbietern für jeweils eine Woche vor Ort im Echtbetrieb erprobt werden. Die Auswahl eines geeigneten Anbieters, dessen System die zuvor definierten Anforderungen erfüllt, obliegt nunmehr alleine dem Landespolizeipräsidium.

Die materiellen Voraussetzungen für die Durchführung einer stationären Videoüberwachungsmaßnahme durch die Polizei normiert § 27 Abs. 1 Nr. 1 Alt. 2 Saarländisches Polizeigesetz (SPolG)[36]. Danach ist die Überwachung solcher Örtlichkeiten zulässig, bei denen auf Grund von Tatsachen anzunehmen ist, dass dort Straftaten verabredet, vorbereitet oder verübt werden. Unter Nachweis und Einbeziehung der durch das LPP vorgetragenen Fallzahlen bestand im Ergebnis Konsens, dass die Voraussetzungen von § 27 Abs. 1 Nr. 1 Alt. 2 SPolG in Bezug auf die Örtlichkeiten Vorplatz Hauptbahnhof und Johanneskirche vorliegen.

Anders hingegen bewerteten wir das Vorliegen der Voraussetzungen des § 27 Abs. 1 Nr. 1 Alt. 1 SPolG, nämlich das Anfertigen von Bildaufzeichnungen zur Abwehr einer Gefahr für die öffentliche Sicherheit, das seitens des LPP als alternative Rechtfertigung für die Inbetriebnahme der geplanten Videoüberwachungsmaßnahme vorgebracht wurde. Die Voraussetzungen dieser Tatbestandsalternative, insbesondere das Vorliegen einer konkreten Gefahr für ein Schutzgut der öffentlichen Sicherheit, sind mit Blick auf die Rechtsprechung des Bundesverfassungsgerichts[37] nach hiesiger Auffassung nicht gegeben. Eine konkrete Gefahr liegt hiernach vor, wenn im Einzelfall

[36] Saarländisches Polizeigesetz vom 26.3.2001 (Amtsbl. S 1074), zuletzt geändert d. Gesetz v. 22.8.2018 (Amtsbl. I S. 674).

[37] Urteil vom 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07, Rn. 251 (zitiert nach juris).

eine Sachlage oder ein Verhalten bei ungehindertem Ablauf des objektiv zu erwartenden Geschehens mit hinreichender Wahrscheinlichkeit ein polizeilich geschütztes Rechtsgut schädigen wird. Die konkrete Gefahr wird danach durch drei Kriterien bestimmt: den Einzelfall, die zeitliche Nähe des Umschlagens einer Gefahr in einen Schaden und den Bezug auf individuelle Personen als Verursacher. Hinsichtlich der konkreten Gefahr müssen zumindest tatsächliche Anhaltspunkte vorliegen, sich also bestimmte Tatsachen feststellen lassen, die eine Gefahrenprognose tragen und damit zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die polizeiliche Maßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann. Diese Voraussetzungen rechtfertigen möglicherweise eine Videoüberwachung in einem konkreten Einzelfall, nicht jedoch die Installation einer stationären, dauerhaften Videoüberwachungsanlage.

Kritisch sehen wir die beabsichtigte, aber bis dato noch nicht entschiedene Ausleitung des Videosignals im Bereich des Vorplatzes Hauptbahnhof an die Bundespolizei. Für eine anlasslose, generelle Zurverfügungstellung des Videosignals fehlt es nach hiesiger Auffassung an einer Rechtsgrundlage, weshalb eine Zurverfügungstellung des Livebildes nur dann und nur solange in Betracht kommt, wie eine konkrete Gefahrsituation vorliegt.

Mit Geltungseintritt der Datenschutz-Grundverordnung (DSGVO) und gleichzeitigem Inkrafttreten des Saarländischen Datenschutzgesetzes (SDSG) in seiner neuen Fassung am 25. Mai 2018 änderte sich die Rechtslage insoweit, als eine Anhörung unserer Dienststelle unter Vorlage der maßgeblichen Errichtungsanordnung vor dem erstmaligen Einsatz eines Verfahrens und demnach der Freigabe durch die verantwortliche Stelle nicht mehr gesetzlich vorgeschrieben ist. Eine Genehmigung oder andere Form der Freigabe durch das Datenschutzzentrum ist in dem seit 25. Mai 2018 geltenden datenschutzrechtlichen Regelungsrahmen demnach nicht mehr vorgesehen und daher vor der finalen Inbetriebnahme des Systems nicht erforderlich. Nach Start des Echtbetriebs ist zu gegebener Zeit eine Auditierung des Gesamtsystems durch die hiesige Dienststelle geplant.

3.2 Mobiles Arbeiten der Vollzugspolizei

Bereits seit Ende des Jahres 2016 beschäftigte sich eine landesweite Arbeitsgruppe der saarländischen Polizei mit dem Projekt „VU-App – Mobile Verkehrsunfallerfassung bei der Polizei des Saarlandes“. Durch den Einsatz mobiler Endgeräte, wie Tablets oder Smartphones, sollten die Einsatzkräfte vor Ort bei der Aufnahme eines Verkehrsunfalls entlastet werden. Statt der bisherigen Aufnahme der Unfalldaten mithilfe handschriftlicher Notizen, Skizzen und in Form von Fotos können die Daten nunmehr unmittelbar vor Ort in einer eigens dafür entwickelten Applikation erfasst werden. Die bislang anschließend in der Polizeiinspektion vorzunehmende händische Eingabe der für den Verkehrsunfall relevanten Daten in das Vorgangsbearbeitungs-

system POLADIS (Polizeiliches Auskunfts-, Datenverarbeitungs- und Informationssystem) erübrigt sich, da die Daten automatisiert über eine Schnittstelle in POLADIS übertragen werden.

Das Projekt wurde im Zuge einer bestehenden IT-Kooperation der Polizeien Saarland und Rheinland-Pfalz als „Mobiles Arbeiten der Vollzugspolizei" weiterentwickelt. So können nunmehr nicht nur Verkehrsunfälle, sondern auch Strafanzeigen mit einer eigens durch die Polizei entwickelten App direkt in das mitgeführte mobile Endgerät eingegeben und bearbeitet werden. Alle wichtigen Daten zu einem Unfall und/oder einer Strafanzeige werden bereits vor Ort erfasst und automatisch in POLADIS übertragen. Durch die Schnittstelle zu POLADIS und mithin das Entfallen der nachträglichen manuellen Datenerfassung sollen Datenerfassungsfehler minimiert, die Datenqualität verbessert und letztendlich eine Zeitersparnis im Backoffice der Polizei erreicht werden.

Die beiden Applikationen Verkehrsunfall und Strafanzeige wurden uns im Rahmen der Pilotierung vorgestellt. Ein besonderes Augenmerk lag unsererseits darauf, wie eine sichere Anbindung der eingesetzten Tablets oder Smartphones an das Backend – hier den Informationsverbund der saarländischen Polizei – gewährleistet werden kann.

Als kritisch erachteten wir eine Funktionalität der App, die als Eingabeunterstützung für den Nutzer gedacht war. Die dem polizeilichen Nutzer zur Verfügung stehenden Eingabemasken sahen unterschiedliche Datenfelder vor, über die vom Beamten Eingaben zu Unfalltag, -zeit oder -art sowie persönliche Angaben zu den Unfallbeteiligten zu tätigen waren. Um das Ausfüllen dieser Datenfelder zu beschleunigen und Fehleingaben zu reduzieren, war vorgesehen, dass der Beamte die Felder entweder mittels Diktierfunktion im Wege der Nutzung von Spracherkennungsalgorithmen ausfüllen konnte oder alternativ durch das Abfotografieren von Personalausweis und/oder Führerschein in Kombination mit einer sich daran anschließenden Texterkennung die Möglichkeiten hatte, die Felder automatisiert mit den Angaben aus den entsprechenden Ausweisdokumenten zu befüllen.

Technisch war vorgesehen, die Funktion der Spracherkennung und Texterkennung über die Einbindung der von Microsoft angebotenen Microsoft Cognitive Services API (Application Programming Interface) zu realisieren, an die die noch unstrukturierten Rohdaten (Ton- und Bildaufnahme) übertragen werden sollten, um dort entsprechend aufbereitet und in strukturierter Form an die App zurückübertragen zu werden.

Neben formalen Einwänden, die insbesondere darin bestanden, dass Microsoft nicht dazu bereit war, einen der damaligen Rechtslage nach § 5 SDSG a. F. genügenden Auftragsdatenverarbeitungsvertrag abzuschließen, blieb auch unklar, wie Microsoft mit den übertragenen Rohdaten nach Durchführung der Sprach- und Textanalyse weiterverfährt. Entsprechende Zusicherungen, die sicherstellen sollten, dass die Rohdaten nach Durchführung des Analyseverfahrens nicht mehr durch Microsoft aufbewahrt und/oder für andere Zwecke verwendet werden, konnten uns nicht vorgelegt werden, weshalb wir – im Ergebnis erfolgreich – für eine Abschaltung dieser Funktionalitäten votierten.

Perspektivisch soll für den polizeilichen Alltag auch auf andere polizeiliche Informationssysteme mit den Mobilgeräten zugegriffen werden. So sollen die Polizistinnen und Polizisten im Einsatz vor Ort beispielsweise zur Überprüfung von Personalien Daten aus dem Einwohnermeldesystem abfragen können. In Planung sei ebenso die Integration des Zentralen-Verkehrs-Informations-Systems (ZEVIS), mit dem die Polizei auf das Kraftfahrzeugzentralregister zugreift, etwa um Kfz-Kennzeichen zu überprüfen. Wir werden diese Entwicklung weiter datenschutzkonform beratend begleiten.

3.3 Implementierung der „Digitalen Kriminalpolizeilichen personenbezogenen Sammlung“ in das Verfahren POLIS-Saarland

Zur Erfüllung ihrer Aufgaben auf dem Gebiet der Gefahrenabwehr und der Strafverfolgung werden von den Behörden des Polizeivollzugsdienstes „Kriminalpolizeiliche personenbezogene Sammlungen“ (KpS) geführt. Sie können als Kriminalakten oder Dateien geführt werden, soweit die maßgebenden rechtlichen Grundlagen eine Verarbeitung personenbezogener Daten zulassen. Da die Kriminalakten von der saarländischen Polizei künftig elektronisch geführt werden sollten, war es notwendig die „Digitalisierte Kriminalpolizeiliche personenbezogene Sammlung“ (DKpS) in das Verfahren POLIS-Saarland zu integrieren. Dies stellte eine umfangreiche Verfahrensänderung dar, weshalb das Ministerium für Inneres, Bauen und Sport uns nach § 7 Abs. 2 SDSG a. F. die überarbeitete Errichtungsanordnung (EAO) mit der Bitte um Wahrnehmung unserer Beteiligungsrechte übersandte.

Eine nähere datenschutzrechtliche Befassung galt der Art und Weise der Migration personenbezogener Daten aus den Altverfahren. Diese Datenmigration sollte durch eine erste automatisierte Befüllung der DKpS aus dem Verfahren „Digitale Kriminalakte“ stattfinden. Die digitalen Kriminalakten standen als Mikrofilme zur Verfügung und wurden in eine Tagged Image Format (TIF)-Datei gespeichert. Mit Blick auf die Erfahrungen bei der Datenmigration der Inpol-Falldatei Rauschgift[38] sowie auf die Rechtsprechung des VG Köln[39] zur Anwendung von Aussonderungsprüffristen, haben wir daher dem Ministerium für Inneres, Bauen und Sport in unserer abschließenden Stellungnahme mitgeteilt, dass wir es für erforderlich halten, sämtliche als TIF - Dateien migrierten Datenbestände, die älter als zehn Jahre sind, zu löschen.

Ein weiteres Augenmerk galt sowohl der Einhaltung der Lösch- und Aussonderungsprüffristen sowie der Gewährleistung eines reibungslosen Verfahrensablaufes hinsichtlich der Mitteilungen der Staatsanwaltschaften im Strafverfahren (MiStra) als auch der Mitteilungen der Ahndungsbehörden in Ordnungswidrigkeitsverfahren. Die

[38] Vgl. Entschließung der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder Kühlungsborn, den 10. November 2016: Gemeinsame Prüfung der Falldatei Rauschgift deckt gravierende Mängel auf; Konsequenzen für polizeiliche Datenverarbeitung notwendig.

[39] Urteil vom 23. April 2015 – 20 K 3184/14, Rn. 54, 55 (zitiert nach juris).

MiStra haben je nach Verfahrensausgang wesentlichen Einfluss auf die Dauer der Speicherung wie auch auf die Löschung in polizeilichen Systemen. In der Vergangenheit erreichten die MiStra die im Landespolizeipräsidium (LPP) eingerichtete zentrale Stelle für die Vergabe von Löschfristen oft verspätet, sei es, dass die Mitteilungen verspätet durch die verantwortliche Staatsanwaltschaft versandt wurden oder polizeiintern nicht oder wesentlich verspätet der zuständigen Stelle zugeordnet wurden. Auf Nachfrage wurde uns mitgeteilt, dass zwischenzeitlich seitens der Staatsanwaltschaft eine Auflistung abgeschlossener Verfahren aus deren elektronischem Informationssystem *web.sta* zur automatisierten Datenbereinigung in elektronischer Form generiert und der Polizei zur Verfügung gestellt werde, es derzeit aber noch keine Implementierung im polizeilichen Verfahren POLIS gebe, um die von der Staatsanwaltschaft zur Verfügung gestellten Informationen über Verfahrensausgänge automatisiert einzulesen. Wir haben daher zur Einhaltung der Löschfristen um eine möglichst zeitnahe Implementierung im Verfahren POLIS gebeten.

Ein weiterer Punkt war der Umgang mit der Speicherung personenbezogener Daten von Opfern, Zeugen und Hinweisgebern. Da es sich bei der „Digitalisierten Kriminalpolizeilichen personenbezogenen Sammlung" um ein Verfahren handelt, das aus Rheinland-Pfalz übernommen wird, ist es wegen der rheinland-pfälzischen Rechtslage dort dergestalt implementiert, dass Daten dieser Personen (Opfer, Zeugen, Hinweisgeber), auch wenn sie im Rahmen strafrechtlicher Ermittlungsverfahren bekannt geworden sind, unter bestimmten Voraussetzungen zur vorbeugenden Bekämpfung von Straftaten zweckändernd gespeichert und genutzt werden dürfen. Eine dem rheinland-pfälzischen Recht gleichlautende oder ähnliche Norm enthält das Saarländische Polizeigesetz (SPolG) nicht. Nach § 30 Abs. 2 SPolG kann die Vollzugspolizei personenbezogene Daten lediglich von solchen Personen zur vorbeugenden Bekämpfung von Straftaten verarbeiten, die die Polizei im Rahmen von Strafermittlungsverfahren gewonnen hat und die sich auf Personen beziehen, die verdächtig sind, eine mit Strafe bedrohte Tat begangen zu haben. Eine Speicherung personenbezogener Daten von Opfern, Zeugen oder Hinweisgebern in der DKpS kommt daher nach der saarländischen Rechtslage regelmäßig nicht in Betracht. Daher muss sichergestellt werden, dass entsprechende personenbezogene Daten nicht in der DKpS gespeichert werden.

Ein letzter Kritikpunkt war die beabsichtigte zweckändernde Speicherung von personenbezogenen Daten aus Ordnungswidrigkeitenverfahren zur vorbeugenden Bekämpfung von Straftaten, die wir für datenschutzrechtlich unzulässig erachteten. Die Polizei wollte auch bei Ordnungswidrigkeiten von erheblicher Bedeutung diese weiterhin aufbewahren, wenn wegen der Art, Ausführung oder Schwere der Tat oder der Persönlichkeit der oder des Betroffenen die Gefahr der Wiederholung besteht. § 30 Abs. 2 SPolG gestattet die entsprechende zweckändernde Nutzung personenbezogener Daten indes nur in Fällen einer Straftat, nicht jedoch bei Ordnungswidrigkeiten. Damit kommt eine zweckändernde Nutzung personenbezogener Daten aus Ordnungswidrigkeitsverfahren in der Regel nicht in Betracht, sondern höchstens dann, wenn die Ordnungswidrigkeit zusammen mit einer Straftat tateinheitlich begangen wurde. Es bedurfte daher aus unserer Sicht einer entsprechenden Klarstellung in der EAO. Dies ist nach hiesigem Kenntnisstand beim LPP in Bearbeitung.

4 Steuern und Kataster

4.1 Outsourcing von Druck, Adressierung und Kuvertierung behördlicher Schreiben

Noch immer besteht seitens verschiedener Kommunalverwaltungen der Wunsch, Druck, Adressierung und Kuvertierung behördlicher Schreiben unter dem Gesichtspunkt der Kostenersparnis an externe Dienstleister zu vergeben. Gerade im Bereich des Steuer- und Abgabenrechts wirft diese Praxis aber erhebliche datenschutzrechtliche Fragen auf.

Nach alter Rechtslage war die Vergabe von Druck, Kuvertierung und Versand von Abgabebescheiden durch externe Dienstleister nicht zulässig. Grund hierfür war, dass § 30 Abs. 4 Abgabenordnung (AO)[40] eine Offenbarungsbefugnis steuerlicher Daten nur unter bestimmten Voraussetzungen zuließ [vgl. 25. Tätigkeitsbericht, Kap. 8.3 (S. 63 f.)].

Nachdem § 30 AO im Mai 2018 erweitert wurde, ist nunmehr das Outsourcen von Druck, Adressierung und Kuvertierung von Bescheiden mit Inhalten, die dem Steuergeheimnis unterliegen, unter den Voraussetzungen des § 30 Abs. 9 AO prinzipiell möglich.

Danach kommt das Outsourcing von Druck, Adressierung und Kuvertierung von insbesondere Steuer- und Abgabenbescheiden nunmehr ausnahmsweise dann in Betracht, wenn die Verarbeitung ausschließlich durch Personen erfolgt, die zur Wahrung des Steuergeheimnisses verpflichtet sind. Dies sind nur solche Personen, die zu dem in § 30 Abs. 1 und 3 AO genannten Personenkreis gehören. Nicht zur Wahrung des Steuergeheimnisses verpflichtet sind alle anderen Personen, die nicht zu diesem Personenkreis gehören und für die sich diese Verpflichtung auch nicht aus einem anderen Gesetz ergibt. Eine Verpflichtung auf das Steuergeheimnis, die sich ausschließlich aus einer vertraglichen Vereinbarung zwischen Finanzbehörde und Dienstleister ergibt, erfüllt diese Voraussetzungen nicht, weshalb auch weiterhin eine Beauftragung privater Dienstleistungsunternehmen im Bereich der AO regelmäßig nicht in Betracht kommt.

Grundsätzlich denkbar wäre es nun aber, dass, beispielsweise im Rahmen einer interkommunalen Zusammenarbeit, Druck, Adressierung und Kuvertierung von Steuer- und Abgabenbescheiden durch eine andere Kommune vorgenommen wird.

Weiterhin relevant bleiben indes die inhaltlichen Vorgaben an eine entsprechende Outsourcing-Vereinbarung. Datenschutzrechtlich ist das Outsourcing von Druck, Adressierung und Kuvertierung als Auftragsverarbeitung zu qualifizieren und hat sich

[40] Abgabenordnung in der Fassung der Bekanntmachung vom 1.10.2002 (BGBl. I S. 3866, 2003 I S. 61), zuletzt geändert d. Gesetz v. 18.12.2018 (BGBl. I S. 2639).

an den Regelungen des Art. 28 Datenschutz-Grundverordnung (DSGVO) auszurichten. Von besonderer Bedeutung ist dabei, dass

- Subunternehmer nur nach Genehmigung durch den Auftraggeber beauftragt werden dürfen,
- das Weisungsrecht dokumentiert ist,
- und geeignete technische und organisatorische Maßnahmen die Sicherheit der Daten und die Auskunftsrechte der Betroffenen garantieren.

In jedem Fall ist zwischen Verantwortlichem und Auftragsverarbeiter ein Vertrag abzuschließen, in dem Gegenstand und Dauer der Verarbeitung, Art und Zwecke der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien von betroffenen Personen festgelegt sind. Obgleich die Vorlage eines Vertragsentwurfs zur Prüfung bei der Landesbeauftragten für Datenschutz nicht mehr erforderlich ist, stehen wir den Kommunen gerne beratend zur Seite.

4.2 Ortskirchensteuer

Eine saarländische Kommune wurde von der zuständigen Kirchengemeinde gebeten, die Ortskirchensteuer ab dem Jahr 2018 im Rahmen der Grundsteuererhebung einzuziehen.

§ 15 Abs. 1 des Saarländischen Kirchensteuergesetzes (KiStG)[41] sieht insoweit vor, dass auf Antrag einer in der Steuerordnung genannten kirchlichen Körperschaft die Kirchensteuer vom Grundbesitz durch die Gemeinden verwaltet wird. § 4 der Kirchensteuerordnung der katholischen Diözese Speyer regelt eine entsprechende Befugnis zur Erhebung einer Ortskirchensteuer nach Maßgabe der Grundsteuermessbeträge.

Die für die Einziehung der Ortskirchensteuer benötigten Informationen sollten durch die Kommune mittels eines Abgleichs der im Melderegister gespeicherten Daten zur Konfession und der beim kommunalen Steueramt vorhandenen Informationen zur Grundsteuer A und B gewonnen werden

Die Erhebung der Ortskirchensteuer wird als Auftragsangelegenheit gemäß § 6 Kommunalselbstverwaltungsgesetz (KSVG)[42] durchgeführt. Zwar dürfen nach § 37 Abs. 1 Bundesmeldegesetz (BMG)[43] im Melderegister gespeicherte Daten und damit Informationen über die Religionszugehörigkeit (§ 3 Abs. 1 Nr. 11 BMG) innerhalb der Verwaltungseinheit, der die Meldebehörde angehört, weitergegeben werden, was einen Abgleich durch das kommunale Steueramt grundsätzlich möglich macht.

---

41 Gesetz Nr. 926 über die Erhebung von Kirchensteuern im Saarland vom 25.11.1970 in der Fassung der Bekanntmachung vom 5.5.2015 (Amtsbl. I S. 284).

42 Kommunalselbstverwaltungsgesetz vom 15.1.1964 in der Fassung der Bekanntmachung vom 27.6.1997 (Amtsbl. S. 682), zuletzt geändert d. Gesetz v. 15.6.2016 (Amtsbl. I S. 840).

43 Bundesmeldegesetz vom 3.5.2013 (BGBl. I S. 1084), zuletzt geändert d. Gesetz v. 18.7.2017 (BGBl. I S. 2745).

Die Kommune beabsichtigte aber, mit der Durchführung dieses Abgleichs einen externen Dienstleister zu beauftragen. Dies hätte aber vorausgesetzt, dass dem Dienstleister nicht nur Meldedaten, sondern auch dem Steuergeheimnis nach § 30 Abgabenordnung (AO) unterliegende Daten offenbart werden. Eine Offenbarung steuerlich relevanter Sachverhalte ist indes nur in den in § 30 Abs. 4 AO genannten Fällen zulässig. Keine der dort genannten Alternativen war hier einschlägig, eine Offenbarungsbefugnis lag daher nicht vor. Auch sah die AO zum damaligen Zeitpunkt die Möglichkeit einer Verarbeitung von Steuerdaten im Auftrag noch nicht vor [vgl. hierzu 4.1 (S. 45)]. Die Beauftragung eines externen Dienstleisters war somit datenschutzrechtlich nicht zulässig, was wir der Kommune auch so mitgeteilt haben.

4.3 Durchführung eines Grenztermins

Ein Grenztermin dient der Vermessung und Abmarkung von Flurstückgrenzen. Im Grenztermin werden in aller Regel mehrere Flurstücke neu vermessen. Er wird von der zuständigen Katasterbehörde durchgeführt. In einer an uns gerichteten Beschwerde wurde sich darüber beklagt, dass *„in öffentlicher Runde Namen/Geburtsnamen in einer Gruppe von 20 Personen, auch vor Nicht-Anwohnern, laut und deutlich preisgegeben wurden".*

Zur Sachverhaltsaufklärung wurde die betroffene Katasterverwaltung um Stellungnahme gebeten. Das für die Fachaufsicht zuständige Ministerium für Umwelt und Verbraucherschutz erteilte hierzu Auskunft.

Zu dem Grenztermin waren ordnungsgemäß alle Betroffenen, d. h. die Flurstückseigentümer, eingeladen worden. Darüber hinaus waren aber auch unbeteiligte Personen zu dem Grenztermin erschienen. So befanden sich ein ehemaliger Flurstückseigentümer (die Veräußerung des Flurstücks war bei der Vorbereitung des Grenztermins noch nicht vom Amtsgericht an die Katasterverwaltung übermittelt worden) und „Gäste" (die Eltern eines Beteiligten) unter den Anwesenden. Diese Unbeteiligten wurden nach der Feststellung der Anwesenheit nicht gebeten, den Grenztermin zu verlassen, sondern deren Anwesenheit wurde durch den Verhandlungsleiter des Grenztermins geduldet. Hierdurch erhielten diese unbeteiligten Personen Kenntnis über eigentums- und grundstücksrelevante Sachverhalte Dritter, wogegen sich die Beschwerde richtete. Außerdem wendet sie sich dagegen, dass bei der Feststellung der Anwesenheit die Namen der Flurstückseigentümer für unbeteiligte Dritte wahrnehmbar laut verlesen werden.

Rechtsgrundlagen für die Durchführung eines Grenztermins sind die §§ 17 bis 19 des Saarländischen Vermessungs- und Katastergesetzes (SVermKatG)[44], die Sonderungs-

[44] Saarländisches Gesetz über die Landesvermessung und das Liegenschaftskataster vom 16.10.1997, zuletzt geändert d. Gesetz v. 22.8.2018 (Amtsbl. I S. 674).

und Abmarkungsverordnung (SonAbmV)[45] sowie die Verwaltungsvorschrift für die Durchführung von Liegenschaftsvermessungen im Saarland (VV-LiegVerm)[46].

Als Beteiligte am Grenztermin kommen nach § 17 Abs. 2 SVermKatG i. V. m. Ziff. 7.1 VV-LiegVerm allein die Eigentümer und Erbbauberechtigten der betroffenen Flurstücke in Betracht. Sie können sich durch schriftlich Bevollmächtigte vertreten lassen. Gemäß Ziff. 7.2 VV-LiegVerm hat sich der Verhandlungsleiter des Grenztermins in geeigneter Weise Gewissheit über die am Termin teilnehmenden Personen zu verschaffen. Vor dem Hintergrund, dass es sich vorliegend um einen größeren Teilnehmerkreis handelte, war es aus unserer Sicht praktikabel und zulässig die Anwesenheit der geladenen Personen durch Aufrufen der Namen festzustellen. Da diese Namen der Beteiligten später in der anzufertigenden Niederschrift über den Grenztermin (§ 19 Abs. 2 SVermKatG) aufzuführen sind, ist ein Verstoß gegen datenschutzrechtliche Bestimmungen durch das Aufrufen der Namen und die damit einhergehende Bekanntgabe gegenüber den anderen Anwesenden nicht zu erkennen.

Datenschutzrechtlich bedenklich war allerdings die Anwesenheit von Gästen, die nach Darstellung des Landesamtes für Vermessung, Geoinformation und Landentwicklung (LVGL) die Eltern eines Beteiligten und früheren Eigentümer des Grundstücks waren. Nach den o. g. Vorschriften gelten als Beteiligte nur die Eigentümer oder Erbbauberechtigten und im Vertretungsfalle deren schriftlich Bevollmächtigte. Andere Personen können am Grenztermin nur teilnehmen, wenn ihre Interessen durch die Grenzbestimmung und Abmarkung berührt werden (§ 3 SonAbmV). Das wurde im vorliegenden Fall aber nicht dokumentiert. Wir haben das Ministerium darauf hingewiesen, dass es für die Teilnahme dieser Personen am Grenztermin keine gesetzliche Grundlage gab und zukünftig darauf zu achten ist, dass nur Beteiligte im Sinne von § 17 Abs. 2 SVermKatG i. V. mit § 3 SonAbmV an Grenzterminen teilnehmen dürfen.

Das Ministerium für Umwelt und Verbraucherschutz hat die Katasterbehörde (LVGL) angewiesen in Zukunft darauf zu achten, dass nur Beteiligte im Sinne des SVermKatG am Grenztermin teilnehmen.

[45] Sonderungs- und Abmarkungsverordnung vom 5.6.2009 (Amtsbl. S. 914), zuletzt geändert d. Verordnung v. 30.3.2015 (Amtsbl. I S. 245).

[46] Ordnungsnummer 9/2067, elektronisch abrufbar unter http://www.vorschriften.saarland.de/ (letzter Zugriff: 1.3.2019).

5 Landtag

5.1 Datenschutz im parlamentarischen Bereich

Bereits kurz nach Geltungseintritt der Datenschutz-Grundverordnung (DSGVO) wurde unsere Behörde mit der Frage konfrontiert, inwieweit die neuen europarechtlichen Vorgaben die innerparlamentarischen personenbezogenen Datenverarbeitungsvorgänge ausgestalten und begrenzen. Der Fokus der Betrachtung lag dabei auf der parlamentarischen Aufgabenwahrnehmung des Landtages bzw. seiner Abgeordneten und Fraktionen.

Gemäß Art. 2 Abs. 2 lit. a findet die DSGVO keine Anwendung auf die Verarbeitung personenbezogener Daten, *„(…) im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt"*. Die diesbezügliche Aussage ist als bloße Klarstellung zu werten und nimmt Bezug auf den unionsrechtlichen Grundsatz der begrenzten Einzelermächtigung.[47] Gemäß Art. 5 Abs. 2 EUV[48] wird die EU hiernach nur innerhalb der Grenzen jener Zuständigkeiten tätig, welche die Mitgliedstaaten ihr in den Verträgen zur Verwirklichung der darin niedergelegten Ziele übertragen haben. Alle der Union nicht in den Verträgen übertragenen Zuständigkeiten verbleiben bei den Mitgliedstaaten.

Neben den in Erwägungsgrund 16 ausdrücklich genannten und vom Anwendungsbereich der DSGVO ausgeschlossenen Bereichen der nationalen Sicherheit und der Gemeinsamen Außen- und Sicherheitspolitik (GASP) ist auch die engere parlamentarische Arbeit und Organisation innerhalb der Mitgliedstaaten, insbesondere die nationalverfassungsrechtliche Ausgestaltung des Abgeordnetenmandats, vom Anwendungsbereich des europäischen Datenschutzregimes ausgenommen. Eine normative Stütze findet dies in Art. 4 Abs. 2 S. 1 EUV, wonach die Union die jeweilige nationale Identität der Mitgliedstaaten achtet, *„(…) die in ihren grundlegenden politischen und verfassungsmäßigen Strukturen einschließlich der regionalen und lokalen Selbstverwaltung zum Ausdruck kommt"*.[49]

Auch wenn sich die diesbezügliche Bereichsausnahme nicht auf sämtliche (Neben-) Bereiche der parlamentarischen Arbeit erstreckt, als Beispiele können etwa die Mittelbewirtschaftung und das Beschäftigen eigenen Personals durch die Abgeordneten genannt werden, sind jedenfalls die den parlamentarischen Entscheidungsfindungs-

[47] *Kühling/Raab*, in: Kühling/Buchner, DS-GVO/BDSG (2. Aufl. 2018), Art. 2 Rn. 21.

[48] Vertrag über die Europäische Union i. d. F. des Vertrages von Lissabon v. 13.12.2007 (Abl. Nr. C 306 S. 1 u. a.) zuletzt geändert d. Beitrittsakte v. 09.12.2011 (Abl. 2012 Nr. L 112 S. 21).

[49] *Mundil*, Deutscher Bundestag – Datenschutz für Abgeordnete, WD 3 – 3010 -056/18, S. 5.

prozess unmittelbar betreffenden Verarbeitungstätigkeiten, mithin die parlamentarischen Kerntätigkeiten, hiervon erfasst.[50] Selbige wird man als wesentliche, den Aufbau und das Eigenverständnis des Staates prägende Entscheidungen ansehen müssen, welche von unionsrechtlichen Vorgaben – auch solchen nur mittelbarer Natur – freigestellt sind.

Unter den parlamentarischen Kerntätigkeiten wird man dabei die in den nationalen Verfassungen unmittelbar geregelten Grundsätze der gesetzgebenden Gewalt sowie die diesbezüglich erlassenen förmlichen Gesetze und Geschäftsordnungen verstehen müssen, zumindest soweit diese das freie Abgeordnetenmandat und den innerparlamentarischen Entscheidungsfindungsprozess betreffen und näher ausgestalten [vgl. Art. 70 Abs. 1 Verfassung des Saarlandes (SVerf)]. Erfasst sind hiervon allen voran personenbezogene Datenverarbeitungen im Zusammenhang mit der Einbringung von Gesetzes- und Beschlussvorlagen (§ 64 LtG[51]), die Verarbeitungstätigkeiten der Landtagsausschüsse (Art. 77 SVerf, §§ 37 ff. LtG), die Verhandlungen des Landtages (Art. 72 SVerf) sowie dessen Beschlussfassungen (Art. 74 SVerf, §§ 65 ff. LtG).

Gemäß § 2 Abs. 2 Saarländisches Datenschutzgesetz (SDSG) unterliegen *„der Landtag, seine Mitglieder, die Fraktionen sowie ihre jeweiligen Verwaltungen und Beschäftigten"* darüber hinaus auch nicht den nationalen Bestimmungen des saarländischen Datenschutzgesetzes, *„(…) soweit sie bei der Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten".*

Letzteres bedeutet indes nicht, dass auf Ebene des Landtages ein datenschutzfreier Raum bestünde. Wie sich aus der Gesetzesbegründung zum SDSG ergibt (LT-Drucksache 16/279, zu § 2 Abs. 1, S. 30), ist der Landtag zum einen von der Anwendung des SDSG nur insoweit ausgenommen, als er keine Verwaltungsaufgaben wahrnimmt. Verwaltungsaufgaben sind diejenigen Aufgaben, welche darauf gerichtet sind, die finanziellen, organisatorischen und personellen Voraussetzungen für die Tätigkeiten der genannten Stellen zu schaffen oder zu unterhalten, also insbesondere die Personalbewirtschaftung. Zum anderen obliegt dem Landtag des Saarlandes nach § 2 Abs. 2 SDSG die Pflicht, sich auch für den Bereich der parlamentarischen Tätigkeit eine eigene Datenschutzordnung zu geben, was er mit Wirkung vom 25. Mai 2018 getan hat.

Der den Geltungsbereich dieser Datenschutzordnung regelnde § 1 bestimmt diesbezüglich, dass *„(…) für die Verarbeitung personenbezogener Daten bei der Wahrnehmung parlamentarischer Aufgaben durch den Landtag, seine Mitglieder, seine Gremien, die Fraktionen und deren Beschäftigte sowie durch die Landtagsverwaltung (…)"* die Vorschriften der Datenschutzordnung einschlägig sind. Auf die Verarbeitung personenbezogener Daten durch Abgeordnete ist die Datenschutzordnung nur insoweit anwendbar als die Daten *„(…) Gegenstand parlamentarischer Beratungen oder Initiativen sind oder waren (…)".*

Die diesbezügliche Datenschutzkontrolle obliegt gem. § 12 Abs. 1 Datenschutzordnung dem Präsidium des Landtages, welches auch als Beschwerdestelle fungiert

[50] Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 5. September 2018.

[51] Gesetz über den Landtag des Saarlandes v. 20.6.1973 (Amtsbl. S. 517), zuletzt geändert d. Gesetz v. 14.11.2018 (Amtsbl. I S. 817).

(§ 12 Abs. 2). Der Landesbeauftragten für Datenschutz und Informationsfreiheit kommt in diesem Zusammenhang eine ausschließlich beratende Funktion zu (§ 12 Abs. 5).

Für die Zuständigkeit der Landesbeauftragten für Datenschutz und Informationsfreiheit im Bereich des Saarländischen Landtages ergibt sich aus dem bisher Gesagten folgendes:

Die in der Verfassung des Saarlandes, dem Gesetz über den Landtag des Saarlandes sowie der Geschäftsordnung des Saarländischen Landtages geregelten Bereiche parlamentarischer Tätigkeiten unterliegen nicht der Zuständigkeit der Landesbeauftragten für Datenschutz und Informationsfreiheit. Auch eine Verarbeitung personenbezogener Daten im Rahmen der im 10. Abschnitt (§§ 56 ff.) der Geschäftsordnung des Landtages geregelten Anfragen und Aussprachen stellt einen Gegenstand parlamentarischer Beratung bzw. Initiative dar und unterliegt dem Geltungsbereich der Datenschutzordnung des Saarländischen Landtages (§ 1 Abs. 1 S. 2), unterfällt demnach der Aufsicht des Präsidiums des Landtages.

Die Datenschutzordnung des Landtages bestimmt in § 1 Abs. 2, dass bei der Wahrnehmung von Verwaltungsaufgaben für die Verarbeitung personenbezogener Daten das SDSG zur Anwendung kommt. § 2 Abs. 2 S. 2 Ziff. 1-4 benennt dabei 4 spezielle Fälle, bei denen es sich um Verwaltungsaufgaben handelt: 1) wirtschaftliche Angelegenheiten des Landtages, 2) die Personalverwaltung des Landtages, 3) die Ausübung des Hausrechts und der Polizeigewalt, 4) die Ausführung der Gesetze durch den Landtagspräsidenten. § 1 Abs. 3 der Datenschutzordnung des Landtages regelt darüber hinaus ausdrücklich, dass für die Verarbeitung personenbezogener Daten von Beschäftigten der Fraktionen und der Abgeordneten § 22 SDSG entsprechend anzuwenden ist. Letztere Bereiche unterfallen gemäß § 16 Abs. 1 SDSG der Aufsicht der Landesbeauftragten für Datenschutz und Informationsfreiheit.

Mit § 9 SDSG wurde zudem eine Vorschrift aufgenommen, die es der Landesregierung gestattet, die bei ihr vorhandenen Daten für die Beantwortung parlamentarischer Anfragen und zur Vorlage von Unterlagen und Berichten an den Landtag im Rahmen seiner parlamentarischen Kontrollaufgaben und in dem dafür erforderlichen Umfang zu verarbeiten. Zu diesen parlamentarischen Kontrollaufgaben gehört neben der Regierungskontrolle im engeren Sinne in Form von Anfragen und der Arbeit von Untersuchungsausschüssen insbesondere auch die Bearbeitung von Petitionen.

6 Kommunales

6.1 Anwendbarkeit der DSGVO und des SDSG im Bereich der kommunalen Volksvertretungen

Mit der Frage einer Anwendbarkeit der Datenschutz-Grundverordnung (DSGVO) und des Saarländisches Datenschutzgesetzes (SDSG) im parlamentarischen Bereich des Landtages des Saarlandes ist unweigerlich die Frage einer Anwendbarkeit selbiger Rechtsordnungen im Bereich der Kommunalparlamente (Gemeinde-, Stadtrat/Kreistag) verbunden.

Eine direkte Anwendung der Bereichsausnahme des § 2 Abs. 1 S. 4, Abs. 2 SDSG auf Kreistage bzw. Stadt- und Gemeinderäte scheidet bereits aufgrund des eindeutigen Wortlauts der Vorschrift aus. Letztere adressiert sich ausschließlich an den Landtag bzw. dessen Mitglieder als oberste Volksvertretung auf Ebene des Landes.

Auch eine analoge Anwendung kommt nach hiesiger Einschätzung nicht in Betracht. Eine solche setzt nach allgemeiner Methodenlehre eine planwidrige Regelungslücke des Gesetzes sowie eine Vergleichbarkeit der in Bezug genommenen Sachverhalte voraus. Insofern kann bereits das Vorliegen einer planwidrigen Gesetzeslücke angezweifelt werden. Planwidrig ist eine solche nur dann, wenn die in Rede stehende Regelungssituation vom Gesetzgeber nicht gesehen wurde oder wegen späterer Veränderungen der Umstände nicht gesehen werden konnte.[52] Von letzterem ist nicht auszugehen. Aus der Gesetzesbegründung zu § 2 SDSG geht deutlich hervor, dass der Landtag – wie nach bisheriger Rechtslage – gerade aufgrund seiner Stellung als Verfassungs- und Legislativorgan von einer direkten Anwendung der unions- und landesrechtlichen Datenschutzbestimmungen ausgenommen werden soll.[53] Den kommunalen Volksvertretungen kommt – ungeachtet ihrer landläufigen Bezeichnung als Kommunalparlamente – keine vergleichbare Position im Staatsaufbau zu. Gemäß §§ 29 Abs. 1, 155 Kommunalselbstverwaltungsgesetz (KSVG) sind die Stadt- und Gemeinderäte sowie die Kreistage Verwaltungsorgane und keine Parlamente im eigentlichen Sinne.[54] Auch die parlamentarischen Rechte und Grundsätze, insbesondere der Immunität, Indemnität und Diskontinuität, gelten auf Ebene der kommunalen Volksvertretungen nicht.[55] Die gesetzlich geregelte Bereichsausnahme für den parlamentarischen Bereich findet folglich auch mangels Vergleichbarkeit keine Anwendung auf die kommunalen Parlamente. Dementsprechend sind die Regelungen

---

52 *Meissner/Steinbeiß-Winkelmann*, in : Schoch/Schneider/Bier, VwGO (27. EL. 2014), Rn. 54.

53 Bezug genommen wird auf den am 21. März 2018 in den Landtag des Saarlandes eingebrachten Entwurf des Gesetzes zur Anpassung des Saarländischen Datenschutzgesetzes an die Verordnung (EU) 2016/679, (Drs. 16/279).

54 *Wohlfarth*, in: Gröpl/Guckelberger/Wohlfarth, Landesrecht Saarland (3. Aufl. 2017), § 3 Rn. 56.

55 *Wohlfarth*, Kommunalrecht für das Saarland (3. Aufl. 2003), S. 123.

der DSGVO und des SDSG für die Datenverarbeitungen der Kommunalparlamente anwendbar.

Eine Frage, die im Zusammenhang mit der Datenverarbeitung durch kommunale Parlamente an uns herangetragen wurde, war, ob dem datenschutzrechtlichen Regime der DSGVO eine das einzelne Mitglied einer kommunalen Volkvertretung treffende Pflicht zur Bestellung eines behördlichen Datenschutzbeauftragten zu entnehmen ist. Gem. Art. 37 Abs. 1 lit. a DSGVO benennt der Verantwortliche zwingend einen Datenschutzbeauftragten, wenn die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird. Das einzelne Rats-/Kreistagsmitglied stellt weder eine Behörde noch eine sonstige öffentliche Stelle dar. Der Begriff der öffentlichen Stelle definiert sich anhand des nationalen Rechts.[56] Maßgeblich ist, dass sich die Erfüllung öffentlicher Aufgaben auf Grundlage eines öffentlich-rechtlichen Sonderrechts vollzieht, welches in seinen Regelungswirkungen über die im Verhältnis zwischen Privatpersonen geltenden Bestimmungen hinausgeht.[57] Auf ein solches Sonderrecht können sich die Mitglieder der kommunalen Volksvertretungen nicht berufen.

Zwar wird in Bezug auf Abgeordnete des Deutschen Bundestages z. T. eine andere Rechtsauffassung vertreten, welche sich u. a. darauf stützt, dass aus der Einordnung der Fraktion als öffentliche Stelle folge, dass zugleich auch die fraktionsbildenden Mandatsträger als solche zu klassifizieren seien.[58] Auch aus § 2 Abs. 2 SDSG, welcher die Mitglieder des Landtages – mithin die Abgeordneten – in Wahrnehmung parlamentarischer Aufgaben vom Anwendungsbereich des SDSG ausnimmt, kann der Schluss gezogen werden, dass das Landesrecht – zumindest aus datenschutzrechtlicher Sicht – die Abgeordneten des Landtages als öffentliche Stellen i. S. d. § 1 Abs. 1 SDSG begreift, da die Bereichsausnahme in § 2 Abs. 2 SDSG ansonsten überflüssig wäre. Auf die Mitglieder der kommunalen Volksvertretungen trifft dies indes nicht zu. Als Mitglieder eines kommunalen Organs sind sie Bestandteil der Gemeindeverwaltung, wenngleich auch in den §§ 30, 157 KSVG mit besonderen Statusrechten ausgestattet. Verantwortlicher für die Datenverarbeitung i. S. d. Art. 4 Nr. 7 DSGVO ist die Gemeinde (Stadt)/der Landkreis als Organträger bzw. der (Ober-)Bürgermeister, Landrat als von Gesetzes wegen berufenes Vertretungsorgan,[59] nicht hingegen das einzelne Ratsmitglied.

---

[56] Art. 29-Datenschutzgruppe, Guidelines on Data Protection Officers, Working Paper 243 v. 5.4.2017, Ziff. 2.1.1; *Heberlein*, in: Ehmann/Selmayr, DS-GVO (1. Aufl. 2017), Art. 37, Rn. 19.

[57] *Heberlein*, in: Ehmann/Selmayr, DS-GVO (1. Aufl. 2017), Art. 37, Rn. 19; EUGH, Urt. v. 19.12.2013 – C-279/12 (ECLI: EU:C:2013:853).

[58] *Mundil*, Deutscher Bundestag – Datenschutz für Abgeordnete, WD 3 – 3010 -056/18, S. 5.

[59] Vgl. die diesbezüglichen Ausführungen der Artikel-29-Datenschutzgruppe zur Zuordnung der Verantwortlichkeit in Organisationseinheiten (Stellungnahme 1/2010, WP 169, S. 19).

6.2 Zulässigkeit flächendeckender Hundebestandsaufnahmen

Bereits in unserem 18. Tätigkeitsbericht 1999/2000 hatten wir ausgeführt, dass wir eine Hundebestandsaufnahme unter Einschaltung externer Dienstleister für datenschutzrechtlich nicht zulässig halten. Dennoch erreichen uns immer wieder Anfragen von Kommunen, die beabsichtigen, mit Hilfe externer Dienstleister eine flächendeckende Hundebestandsaufnahme durchzuführen.

Eine solche Hundebestandsaufnahme gestaltet sich regelmäßig dergestalt, dass die jeweiligen Kommunen Adressverzeichnisse aller Haushalte im Gemeindegebiet erstellen und den Mitarbeitern eines externen Dienstleisters übergeben, die dann systematisch alle diese Haushalte aufsuchen. Sie machen sich vor Ort je nach Situation durch Klingeln, Klopfen, Rufen o. ä. bemerkbar und bitten die Haushaltsbewohner um Auskunft dazu, ob in dem Haushalt ein Hund gehalten wird und ggfs. seit wann der Hund gehalten wird und welcher Rasse das Tier angehört. Dabei sollen die Mitarbeiter auf die Freiwilligkeit der Befragung hinweisen. Die entsprechenden Auskünfte ebenso wie zwangsläufig gemachte Wahrnehmungen – Herumlaufen eines Hundes, Zwingerhunde, Hundegebell o. ä. – die auf das Vorhandensein eines Hundes schließen lassen, werden dokumentiert und den Gemeinden übergeben. Diese gleichen die so erhaltenen Informationen mit den bereits beim kommunalen Steueramt vorhandenen Informationen ab. Abweichungen werden von der Gemeinde durch weitere Nachforschungen beim Steuerpflichtigen geklärt. Entsprechend der Ergebnisse dieser Recherche erfolgt ggfs. die Veranlagung oder Nachveranlagung.

In aller Regel erfolgt die Vergütung des beauftragten Unternehmens auf Basis eines Erfolgshonorars, welches für jeden ermittelten, nicht angemeldeten Hund eine gestaffelte „Prämienzahlung" beinhaltet. Dies stellt sich insofern als Problem dar, als sich die betreffenden Mitarbeiter, welche die Vor-Ort-Befragung durchführen, sodann einem gewissen Erfolgsdruck ausgesetzt fühlen. Dass diese u. U. weitergehende, d. h. über eine bloße Befragung hinausgehende, Aufklärungsarbeit betreiben, liegt nicht im Bereich des Unwahrscheinlichen. Zu denken ist hierbei insbesondere an eine ausforschende Beobachtung der Grundstücke bzw. der jeweiligen Grundstücksinhaber, was einen ganz erheblichen Eingriff in deren allgemeines Persönlichkeitsrecht darstellen würde.

Die Durchführung von Hundebestandsaufnahmen durch beauftragte Dienstleister ist mit Blick auf datenschutzrechtliche und steuerrechtliche Vorgaben in mehrfacher Hinsicht zu beanstanden.

Zum einen ist der Hundehalter (oder auch Familienangehörige) nicht verpflichtet, anlasslos Auskünfte gegenüber dem kommunalen Steueramt oder den von diesem beauftragten Dritten zu erteilen. Der insoweit allein maßgebliche § 93 Abgabenordnung (AO) bestimmt, dass Voraussetzung für ein entsprechendes Auskunftsersuchen ist, dass die Heranziehung eines Auskunftspflichtigen im Einzelfall aufgrund hinreichender konkreter Umstände geboten ist. Unzulässig sind nach der Rechtsprechung

des Bundesfinanzhofs jedoch Auskunftsersuchen „*ins Blaue hinein*“[60]. Es bedarf daher konkreter Anhaltspunkte dafür, dass ein bestimmter Steuerpflichtiger seinen steuerlichen Pflichten nicht nachkommt.

Mit Blick auf die Befragung von Haushaltsangehörigen oder Dritten (z. B. Nachbarn), die selbst nicht Hundehalter sind, ist zudem zu berücksichtigen, dass nach § 93 Abs. 1 AO zwar auch andere Personen als die am Steuerverfahren Beteiligten bzw. der Steuerschuldner/Steuerpflichtiger der Finanzbehörde die zur Feststellung eines für die Besteuerung erheblichen Sachverhalts erforderlichen Auskünfte zu erteilen haben. Allerdings sollen sie nach dem in § 93 Abs. 1 S. 3 AO geregelten Subsidiaritätsgrundsatz erst dann zur Auskunft angehalten werden, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziel führt oder keinen Erfolg verspricht (Vorrang der Direkterhebung).

Die Finanzbehörde – bzw. im Rahmen der Kommunalabgaben die erhebende Gemeinde – darf eine Auskunft von Personen, die nicht am Besteuerungsverfahren beteiligt sind, daher nur verlangen, wenn ein hinreichender Anlass für Ermittlungen besteht und wenn das Auskunftsersuchen zur Sachverhaltsaufklärung geeignet und notwendig, die Pflichterfüllung für den Betroffenen möglich und seine Inanspruchnahme erforderlich, verhältnismäßig und zumutbar ist.

Einige Kommunen haben sich vor dem Hintergrund der strengen Vorgaben des § 93 AO damit beholfen, dass sie in ihren kommunalen Hundesteuersatzungen eine (anlasslose) Pflicht von Grundstückseigentümern oder deren Vertretern zur Erteilung von Auskünften über die auf dem betreffenden Grundstück gehaltenen Hunde und deren Halter bzw. Eigentümer normiert haben. Eine solche Regelung in der Hundesteuersatzung ist indes rechtlich unwirksam, da es der Gemeinde insoweit an einer satzungsrechtlichen Regelungskompetenz fehlt. Der Umfang der Regelungsbefugnisse ist in § 2 Kommunalabgabengesetz (KAG)[61] normiert. Nach dessen Abs. 1 S. 2 besteht eine Regelungskompetenz lediglich im Hinblick auf den Kreis der Abgabenpflichtigen, den die Abgabe begründenden Tatbestand, den Maßstab und den Satz der Abgabe sowie den Zeitpunkt der Entstehung der Abgabenpflicht und deren Fälligkeit. Die Kommunen sind danach nicht befugt, eigene, neue und im Vergleich zu § 93 AO in Bezug auf den Adressatenkreis weitere Auskunftspflichten, mithin Verfahrensregelungen, in einer kommunalen Satzung zu treffen. Dementsprechend besteht keine Befugnis zur Normierung von Auskunftspflichten für Personen (hier: Grundstückeigentümer), die gerade nicht nach der Hundesteuersatzung steuerpflichtig und damit letztlich unbeteiligt sind. Der kommunale Satzungsgeber kann keine über § 93 Abs. 1 AO hinausgehenden Kompetenzen verleihen, eine Auskunft von Unbeteiligten zu fordern. Die Verfahrensvorschriften der AO, auf die in § 12 Abs. 1 Nr. 3 lit. a KAG verwiesen wird, also auch § 93 AO, gelten unmittelbar für alle Kommunalabgaben; von ihnen kann durch Satzung nicht abgewichen werden.

Abgesehen davon, dass es schon an einer Satzungsbefugnis der Kommunen für eine Auskunftsverpflichtung der Grundstückseigentümer fehlt, kommt als weiteres Prob-

---

[60] Urteil vom 23.10.1990 – VIII R 1/86, Rn. 17 (zitiert nach juris).

[61] Gesetz Nr. 1074 vom 26.4.1978 in der Fassung der Bekanntmachung vom 29.5.1998 (Amtsbl. S. 691), zuletzt geändert d. Gesetz v. 22.8.2018 (Amtsbl. I S. 674).

lem hinzu, dass auch keine Befugnis der Kommunen besteht, Dritte mit der Ermittlung steuerlich relevanter Sachverhalte zu beauftragen oder dies in einer Satzung zu regeln.

Die Regelungsbefugnis in § 2 KAG erlaubt es nur, *„(…) dass die **Festsetzung** und die **Erhebung** von Abgaben von einer damit beauftragten Stelle außerhalb der Verwaltung vorgenommen werden"* darf. Eine Einschaltung von Dritten im steuerrechtlichen **Ermittlung**sverfahren, also bei der Bestimmung der rechtlichen und tatsächlichen Verhältnisse des Steuerpflichtigen, die für die Besteuerung bedeutsam sind, ist somit schon begrifflich ausgeschlossen und von § 2 KAG nicht gedeckt. Eine Einschaltung privater Dienstleister scheidet damit in jedem Fall aus.

Von einigen Kommunen wurde die Frage gestellt, wie demgegenüber eine „freiwillige" Hundebestandsaufnahme zu bewerten sei, die nicht von privaten Dienstleistern, sondern von Mitarbeitern des kommunalen Steueramtes durchgeführt werde.

Als Rechtsgrundlage einer freiwilligen Befragung kommt allein das Rechtsinstitut der Einwilligung gemäß Art. 6 Abs. 1 lit. a Datenschutz-Grundverordnung (DSGVO) in Betracht. Hauptwesensmerkmal der Einwilligung ist ihre Freiwilligkeit. Freiwillig bedeutet, dass der Entschluss in die Datenverarbeitung ohne Druck oder Zwang erfolgen muss. Dies verbietet jedoch nicht nur eine zielgerichtete, unmittelbare Einwirkung auf den Willensbildungsprozess der betroffenen Person. Auch unbeabsichtigte, mittelbare Zwangslagen führen u. U. zu einer Unwirksamkeit der Einwilligung. Für die kommunalen Behörden gilt es in diesem Zusammenhang zu berücksichtigen, dass sie als Träger hoheitlicher Gewalt den Bürgerinnen und Bürgern vielfach in einem Über-/Unterordnungsverhältnis gegenübertreten. In Erwägungsgrund 43 greift die DSGVO diese Konstellation eigens auf. Hiernach soll in Fällen eines *„klare[n] Ungleichgewicht[es]"* zwischen dem Verantwortlichen und der betroffenen Person, insbesondere in Fällen, in denen der Verantwortliche eine Behörde ist, die Einwilligung *„keine gültige Rechtsgrundlage liefern".*

Eine solche mittelbare Zwangslage erblicken wir in vorliegender Konstellation. Einer Befragung, welche darauf abzielt, das Vorliegen von Steuertatbeständen zu ermitteln und im Zuge welcher die betroffene Person hierfür auf ihrem oder einem anderen Privatgrundstück aufgesucht wird, wohnt zwangsläufig der Charakter einer obrigkeitlichen Maßnahme inne, bei welcher sich die betroffene Person, selbst unter hinreichender Aufklärung über die Freiwilligkeit, zu einer Auskunft genötigt sehen kann. Letzteres resultiert insbesondere aus der Überlegung, dass im Falle einer Auskunftsverweigerung bei der befragten Person die Sorge entstehen kann, die Auskunftsverweigerung könne zu ihren Lasten gewertet werden und u. U. weitere behördliche Ermittlungen nach sich ziehen.

Verstärkt wird die diesbezügliche Zwangslage durch den Umstand, dass die Befragung vor Ort und im Regelfall ohne vorherige Ankündigung oder Terminvereinbarung erfolgt. Es erscheint uns nicht fernliegend, dass es in diesem Zusammenhang zu einer – wenn auch ungewollten – Überrumpelungssituation kommt, in welcher sich die betroffene Person, selbst nach hinreichender rechtlicher Aufklärung über die Freiwilligkeit, zu einer Auskunft gedrängt fühlt, welche sie unter anderen Umständen vielleicht nicht getätigt hätte.

Zusammenfassend stehen wir folglich der flächendeckenden Hundebestandsaufnahme, auch unter Berücksichtigung einer Ausgestaltung in Form einer freiwilligen Befragung, nach wie vor ablehnend gegenüber.

6.3 Fotografien im Rahmen der kommunalen Öffentlichkeitsarbeit

Einen weiteren Schwerpunkt der vergangenen Monate bildete die Datenverarbeitung im Rahmen der kommunalen Öffentlichkeitsarbeit. Gerade in diesem Bereich herrscht vielerorts noch eine gewisse Unsicherheit, was vor allem dem Umstand geschuldet sein dürfte, dass der nationale Gesetzgeber bislang nur wenige Vorschriften erlassen hat, welche die Öffentlichkeitsarbeit staatlicher Stellen bereichsspezifisch und normenklar regeln.

Die rechtlichen Grundlagen für die Öffentlichkeitsarbeit der Kommunen fußen in großen Teilen auf den allgemeinen Grundsätzen der institutionellen Garantie der kommunalen Selbstverwaltung (Art. 28 Abs. 2 GG[62], Art. 117 Abs. 3 SVerf[63]) sowie – insbesondere was die verfassungsrechtlichen Grenzen anbelangt – auf der Rechtsprechung des Bundesverfassungsgerichts[64]. Wie in anderen Angelegenheiten der örtlichen Gemeinschaft können die Kommunen ihre Öffentlichkeitsaufgaben hiernach ohne spezialgesetzliche Grundlage ausgestalten, haben hierbei jedoch die datenschutzrechtlichen Vorgaben zu beachten.

6.3.1 Veröffentlichung von Fotografien kommunaler Veranstaltungen

Werden im Rahmen kommunaler Veranstaltungen, von Festivitäten oder zu sonstigen öffentlichen Anlässen Fotografien mit Personenbezug angefertigt, so ist hierbei besonderen datenschutzrechtlichen Erfordernissen Rechnung zu tragen. Kaum ein Thema wurde in den vergangenen Monaten dabei derart kontrovers diskutiert wie die Fortgeltung[65] des Kunsturhebergesetzes (KUG)[66] unter dem Rechtsregime der Datenschutz-Grundverordnung (DSGVO). Die diesbezügliche Diskussion – welche an dieser Stelle nicht weiter vertieft werden soll – dreht sich im Kern um die Frage, ob

---

62 Grundgesetz für die Bundesrepublik Deutschland v. 23.5.1949 (BGBl. S. 1), zuletzt geändert d. Gesetz v. 13.7.2017 (BGBl. I S. 2347).

63 Verfassung des Saarlandes v. 15.12.1947 (Amtsbl. S. 1077), zuletzt geändert d. Gesetz v. 13.7.2016 (Amtsbl. I S. 178).

64 Urteil v. 2.3.1977 – 2 BvE 1/76, BVerfGE 44, S. 125 ff.

65 Der Begriff „Fortgeltung“ ist hierbei im untechnischen Sinne zu verstehen. Aufgrund des sog. Anwendungsvorranges des Unionsrechts vor dem nationalen Recht müsste man rechtsdogmatisch eigentlich von „Anwendbarkeit“ sprechen.

66 Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie v. 9.1.1907, zuletzt geändert d. Gesetz v. 16.2.2001 (BGBl. I S. 266).

die DSGVO eine Öffnungsklausel enthält, welche es dem nationalen Gesetzgeber gestattet, im Bereich der Veröffentlichung von Personenbildnissen ein Regelungssystem zu erlassen, welches das Recht auf Schutz personenbezogener Daten (Recht am eigenen Bild) und sonstige widerstreitende Verfassungsgüter, insbesondere das Recht auf freie Meinungsäußerung und Informationsfreiheit aber auch die Verarbeitung für journalistische, wissenschaftliche, künstlerische und literarische Zwecke miteinander in einen angemessenen Ausgleich bringt (sog. Prinzip der praktischen Konkordanz).

Bis zur Geltungswirkung der DSGVO stellte das KUG dem Rechtsanwender hierfür ein relativ austariertes und bewährtes Regelungssystem zur Verfügung. In seinem § 22 legt dieses Gesetz als Grundsatz fest, dass Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden dürfen. § 23 Abs. 1 Nr. 1 - 4 erlaubt als Ausnahmeregelung sodann weitreichende Durchbrechungen dieses Grundsatzes, etwa dann, wenn die abgebildeten Personen *„(…) nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen".*

Die Unsicherheit in einigen kommunalen Verwaltungen war verständlicherweise groß, als dieses Regel-Ausnahme-System in der Fachliteratur zunehmend zur Disposition gestellt wurde.[67] Fast schon befremdlich muteten manche Reaktionen – wohlgemerkt nicht von Seiten der saarländischen Kommunen – hierauf an; als extremes Beispiel sei an dieser Stelle das Schwärzen der Gesichter von Kindern in Erinnerungsfotoalben einer kirchlichen Kindertageseinrichtung genannt.

Die Empfehlungen, welche unsere Behörde den saarländischen Kommunen vor diesem Hintergrund mit auf den Weg gab, können – ungeachtet der teilweise komplizierten dogmatischen Diskussion innerhalb der Fachliteratur – als pragmatisch und leicht handhabbar beschrieben werden. Denn ungeachtet der Frage, ob das KUG unter den Regelungen der DSGVO weiterhin Anwendung findet und in Art. 85 DSGVO eine entsprechende Öffnungsklausel oder ein Regelungsauftrag erblickt werden kann, können die Abwägungskriterien, welche dem KUG zugrunde liegen, als weiterhin maßstabsprägend angesehen werden.

Diese Abwägungskriterien verlangen dem Verantwortlichen in datenschutzrechtlicher Hinsicht indes ein gewisses Maß an diesbezüglicher Planung und Ausgestaltung seiner Öffentlichkeitsarbeit ab. Die Beantwortung der Frage, ob für das Ablichten einer Person[68] und einer späteren Veröffentlichung der Fotografien deren Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO erforderlich ist und in welcher Form und in welchem Umfang die Person über die Datenverarbeitung zu informieren ist, hängt nämlich maßgeblich von der jeweiligen Situation ab und erfordert unter Umständen ständige Anpassungen.

---

[67] Eingehend hierzu *Benedikt/ Kranig*, DS-GVO und KUG – ein gespanntes Verhältnis, ZD 1/2019, S. 4 ff.

[68] Die Regelungen des KUG beziehen sich ausschließlich auf das „Verbreiten" und „öffentliche Zurschaustellen", stellen ungeachtet ihrer Anwendbarkeit hingegen keine Rechtsgrundlage für die Vorfrage des Fotografierens dar.

6.3.2 Hinreichende Informationen

Werden im Rahmen kommunaler Veranstaltungen und Festivitäten Fotografien mit Personenbezug angefertigt und veröffentlicht, so ist hierauf zunächst in hinreichender Form hinzuweisen (Art. 13 DSGVO). Dies kann etwa durch Aushänge geschehen, welche an prominenter Stelle der Örtlichkeit angebracht werden oder in Form von Hinweisen auf den Einladungsschreiben. Wichtig ist in diesem Zusammenhang, dass aus diesen Hinweisen nicht nur die Intention zu fotografieren hervorgeht, sondern sich die Information auch und gerade auf die Veröffentlichungsabsicht und die Form der Veröffentlichung bezieht. Letzteres hat in hinreichend konkreter Form zu geschehen, d. h. auch das Veröffentlichungsmedium ist genau zu bezeichnen. Beabsichtigt die Kommune etwa eine Veröffentlichung im Rahmen eines sozialen Netzwerkes oder auf ihrer Internetpräsenz, so genügt keineswegs lediglich der Hinweis auf eine *„Veröffentlichung im Rahmen einer Internetpräsenz"* oder *„(...) im Rahmen eines sozialen Netzwerks".* Die jeweilige Plattform und die Internetseite ist vielmehr beim Namen zu nennen (Facebook etc.). Nur hierdurch wird es der betroffenen Person ermöglicht, die potentielle Verbreitung und Gefährdung ihrer personenbezogenen Daten abzuschätzen.

6.3.3 Einwilligung in die Fotografie

Für die Beantwortung der Frage, wann eine Einwilligung der betroffenen Person in die Fotografie und deren Veröffentlichung – mit entsprechender Information nach Art. 13 DSGVO – vonnöten ist, kann nach hiesiger Auffassung weitgehend auf die Regelungen und Grundsätze des KUG zurückgegriffen werden. Eine Veröffentlichung von Fotografien ohne Einwilligung ist insbesondere dann möglich, wenn die dargestellten Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen. Von letzterem kann selbstverständlich umso weniger ausgegangen werden, je mehr die Person in den Fokus der Aufnahme gerät, das Bild folglich den Charakter eines Porträts erhält. Die Übergänge sind hierbei zweifellos fließend und die Grenzen oftmals schwer zu bestimmen. Ein Indiz für eine einwilligungsbedürftige Fotografie kann jedoch das Wahrnehmen des Fotografen durch die betreffende Person bei deren Anfertigung, etwa in Form eines bewussten Blickkontaktes mit der bzw. Lächelns in die Kamera sein. In diesen Fällen ist die Distanz zwischen dem Fotografen und der abgelichteten Person in aller Regel derart gering, dass letztere nicht mehr als bloßes Beiwerk einer Örtlichkeit oder Landschaft abgelichtet wird und folglich darüber informiert werden muss, zu welchem Zweck die Aufnahme erfolgt und in welcher Form und Anzahl eine Veröffentlichung beabsichtigt ist. Am sinnvollsten dürfte sich dies durch ein kurzes Gespräch des Fotografen mit den betroffenen Personen realisieren lassen, durch welches diesen sodann auch Gelegenheit gegeben wird, sich aus dem Fokus der Kamera zu entfernen.

Besondere Aufmerksamkeit ist gefordert, wenn Kinder oder Jugendliche den Gegenstand der Fotografie bilden. Art. 8 DSGVO knüpft die Einwilligungsfähigkeit von Minderjährigen an die Vollendung des 16. Lebensjahres. Direkte Anwendung findet diese

Vorschrift zwar nur auf Einwilligungen eines Kindes in Bezug auf Dienste der Informationsgesellschaft. Der Norm kann jedoch eine allgemeine Aussage dahingehend entnommen werden, dass für eine Verarbeitung von Daten jüngerer Minderjähriger im Regelfall die Einwilligung der vertretungsberechtigen Personen (i. d. R. der Eltern) erforderlich ist.[69] Insbesondere im Bereich von Kindertageseinrichtungen, Spielplätzen und Sportfesten dürfte die vorherige Einwilligung der Eltern in die anzufertigenden Fotografien und deren Veröffentlichung damit unerlässlich sein.

Abschließend wurden die Kommunen auch dahingehend sensibilisiert, dass bei der Auswahl der zu veröffentlichenden Fotografien darauf geachtet werden sollte, dass die abgelichtete Person nicht in einer unvorteilhaften oder ihr vielleicht sogar peinlichen Situation dargestellt ist. Dies stellt letztlich eine Selbstverständlichkeit dar, erfordert jedoch eine nicht unerhebliche Mehrarbeit auf Seiten des Fotografen und der mit der Veröffentlichung betrauten Personen, welche die Fotografien vor einer Veröffentlichung im wahrsten Sinne des Wortes noch einmal genauer „unter die Lupe" nehmen müssen.

6.4 Nutzung von Meldedaten für Gratulationen/Jubiläen/Veranstaltungen

Obzwar der Geltungseintritt der Datenschutz-Grundverordnung (DSGVO) die saarländischen Kommunen in den allerwenigsten Fällen zu einer Abkehr von freiwilligen Selbstverwaltungsaufgaben zwang, so erschien es unserer Behörde in einigen Fällen gleichwohl notwendig, die Kommunen darauf hinzuweisen, dass gewisse jahrzehntelang ausgeübte Verwaltungstätigkeiten an die neuen gesetzlichen Vorgaben anzupassen sind.

Ein gutes Beispiel hierfür, mit welchem sich das Unabhängige Datenschutzzentrum Saarland intensiv auseinanderzusetzen hatte, ist die datenschutzrechtliche Zulässigkeit der Übermittlung, Weitergabe und Nutzung von Meldedaten zu nicht melderechtlichen Zwecken, etwa für Gratulationen zu Alters- und Ehejubiläen, Geburten und sonstigen besonderen Anlässen oder für Einladungen zu kommunalen Veranstaltungen.

Den rechtlichen Rahmen für die Übermittlung von Einwohnermeldedaten durch die Meldebehörde an andere öffentliche Stellen bildet das Bundesmeldegesetz (BMG)[70]. Gemäß § 37 Abs. 1 S. 1 BMG dürfen innerhalb der Verwaltungseinheit, welcher die Meldebehörde angehört, unter den in § 34 Abs. 1 BMG genannten Voraussetzungen sämtliche der in § 3 Abs. 1 BMG aufgeführten Daten und Hinweise, insbesondere Familien- und Vorname, Geburtsdatum und -ort sowie die derzeitige Anschrift, weitergegeben werden.

---

[69] Vgl. *Klement*, in: Simitis/Hornung/Spiecker, Datenschutzrecht (1. Aufl. 2019), Art. 8 Rn. 12, welcher das vollendete 13. Lebensjahr als „(…) *absolute Untergrenze* (…)" erachtet.

[70] Bundesmeldegesetz vom 3.5.2013 (BGBl. I S. 1084), zuletzt geändert d. Gesetz v. 18.7.2017 (BGBl. I S. 2745).

Meldebehörden im Sinne des Bundesmeldegesetzes sind gemäß § 1 BMG i. V. m. § 1 des saarländischen Gesetzes zur Ausführung des Bundesmeldegesetzes[71] die Gemeinden. Der Begriff der Gemeinde dient dabei als Oberbegriff für die Städte und Gemeinden im technischen Sinne, mithin für die kleinste örtliche Verwaltungseinheit mit Rechtsfähigkeit in unserem Staatsgebilde. Zusammen mit den übrigen Ämtern und Abteilungen bildet die Meldebehörde die Verwaltungseinheit Gemeinde. Ein Datentransfer von der Meldebehörde (Meldeamt) an die übrigen Stellen innerhalb der Gemeindeverwaltung stellt im rechtlichen Sinne demnach keine „Datenübermittlung", mithin einen Datentransfer an andere (externe) öffentliche Stellen dar (vgl. §§ 33 - 36 BMG), sondern ist als bloß innerbehördliche „Datenweitergabe" i. S. d. § 37 Abs. 1 S. 1 BMG anzusehen.[72]

Obgleich kommunale Vertretungsorgane und sonstige Funktionsträger Teil der Kommunalverwaltung sind, erwächst ihnen hieraus nicht automatisch die Berechtigung zur Verarbeitung personenbezogener Daten, welche einer anderen Verwaltungseinheit innerhalb des Verwaltungsträgers zu einem bestimmten Zweck rechtlich zugeordnet sind. Es herrscht insoweit der datenschutzrechtliche Grundsatz der informationellen Gewaltenteilung, welcher im Groben besagt, dass auch innerbehördliche Datenverarbeitungen einer strikten Trennung unterliegen.

Voraussetzung der Rechtmäßigkeit einer solchen Datenweitergabe ist gemäß § 34 Abs. 1 S. 1 BMG, dass diese zur Erfüllung einer in der Zuständigkeit der Meldebehörde (Meldeamt) oder in der Zuständigkeit der empfangenden Stelle (andere fachliche Organisationseinheit innerhalb der Gemeindebehörde) liegenden öffentlichen Aufgabe erforderlich ist. Der Daten empfangenden Stelle müssen mithin von Gesetzes wegen Aufgaben übertragen sein, zu deren Erfüllung sich die Weitergabe der Meldedaten erforderlich zeigt.

Erfolgt eine Weitergabe personenbezogener Daten, wie etwa des Geburtsdatums eines neugeborenen Kindes oder eines Jubilars, von der Meldebehörde an eine andere Stelle innerhalb derselben Verwaltungseinheit, so ist es sowohl für die Rechtmäßigkeit dieser Weitergabe als auch für die anschließende Verarbeitung der übermittelten Daten in Form einer Gratulation oder sonstigen Geste entscheidend, dass eine diesbezügliche Aufgabenzuweisung an die empfangende Stelle besteht, die als Anknüpfungspunkt für die datenschutzrechtliche Rechtfertigung dient. Eine solche bereichsspezifische Aufgabenzuweisung findet sich für die Kommunen weder im Kommunalselbstverwaltungsgesetz (KSVG) noch ist sie dem übrigen Fachrecht zu entnehmen.

6.4.1 Amtliche Glückwünsche als freiwillige Selbstverwaltungsaufgabe

Wie bereits ausgeführt, enthält weder das Kommunalselbstverwaltungsgesetz (KSVG) noch das übrige Fachrecht eine ausdrückliche, bereichsspezifische Aufgabenzuweisung zur Überbringung amtlicher Glückwünsche. Insbesondere kann § 50 Abs.

[71] Art. 1 des Gesetzes Nr. 1869 vom 13.10.2015 (Amtsbl. I S. 712).

[72] *Süßmuth*, Bundesmeldegesetz (2. Aufl., 4. Lfg. Sept. 2015), § 37 Rn. 1, 3.

2 BMG (Melderegisterauskunft in besonderen Fällen), welcher die Registerauskunft u. a. für besondere Alters- und Ehejubiläen regelt, keine solche Aufgabenzuweisung entnommen werden.

Diese Vorschrift kodifiziert lediglich eine besondere Form der Gruppenauskunft nach § 46 Abs. 1 BMG. Mandatsträger wie Gemeinderatsmitglieder oder Bürgermeister dürfen hiernach hinsichtlich Alters- oder Ehejubiläen Auskunft über Familienname, Vorname, Doktorgrad, Anschrift sowie Datum und Art des Jubiläums erhalten. Hierdurch besteht zwar die tatsächliche Möglichkeit zur Gratulation. Die Frage, ob jedoch auch in rechtlicher Hinsicht gratulieren werden darf, wird durch § 50 Abs. 2 BMG nicht beantwortet.

Auch die speziellen Regelungen der Meldedaten-Übermittlungsverordnung (MeldDÜV)[73] enthalten zwecks der Vornahme von Ehrungen bei gewissen Altersjubiläen lediglich eine Übermittlungsermächtigung an die Staatskanzlei (vgl. § 18 MeldDÜV). Die damit korrespondierende Verarbeitungsbefugnis auf Seiten der Staatskanzlei kann sich beispielsweise aus den Vorschriften des Gesetzes über Titel, Orden und Ehrenzeichen ergeben.

In Ermangelung spezieller Vorschriften für Kommunen erscheint es aus hiesiger Sicht rechtlich vertretbar, die anlassbezogene Gratulation durch den Bürgermeister oder einen anderen Gemeindevertreter in bestimmten Konstellationen als kommunale Selbstverwaltungsaufgabe anzusehen und dieser Selbstverwaltungsaufgabe unter Rückgriff auf Art. 6 Abs. 1 lit. e, Abs. 3 lit. b DSGVO, § 4 Abs. 1 SDSG eine Verarbeitungsbefugnis über die diesbezüglich erforderlichen personenbezogenen Daten zu entnehmen.

Gemäß Art. 28 Abs. 2 GG und Art. 117 Abs. 2 u. 3 SVerf haben die Städte und Gemeinden das Recht, alle Angelegenheiten der örtlichen Gemeinschaft im Rahmen der Gesetze in eigener Verantwortung zu regeln. Hierunter fallen diejenigen Bedürfnisse und Interessen, welche in der örtlichen Gemeinschaft wurzeln oder auf diese einen spezifischen Bezug haben.[74] Erfasst sind Angelegenheiten, welche nicht schon durch Gesetz anderen Trägern der öffentlichen Verwaltung zugewiesen sind, sofern die räumlichen Schranken des Gemeindegebiets nicht überschritten werden.[75] Für die Einordnung einer bestimmten Aufgabe als örtliche Angelegenheit kommt es in funktionaler Hinsicht darauf an, ob ein Bezug zur Gemeindebevölkerung oder zum Gemeindegebiet besteht.[76]

In Ermangelung anderweitiger gesetzlicher Regelungen kann das Beglückwünschen von Einwohnern der Gemeinde zu besonderen Anlässen als freiwillige Selbstverwaltungsaufgabe angesehen werden. Insbesondere in Gemeinden, in welchen eine derartige Tradition bereits seit längerer Zeit gepflegt wird, dürfte ein diesbezügliches

---

[73] Verordnung über die Zulassung der regelmäßigen Übermittlung von Daten aus dem Melderegister an Behörden oder andere öffentliche Stellen vom 30.10.2015 (Amtsbl. S. 752), zuletzt geändert d. Gesetz v. 18.4.2018 (Amtsbl. S. 332).

[74] BVerfG, Beschluss vom 23.11.1988 – 2 BvR 1619/83, 2 BvR 1628/83, BVerfGE 79, S. 127 (151).

[75] BVerfG, a.a.O. S. 146 ff.

[76] *Grupp*, in: Wendt/Rixecker, Verfassung des Saarlandes, Art. 117, Rn. 7.

Verwaltungshandeln über eine bloße Geste hinausgehen und bereits den Charakter einer ständigen Übung erfahren haben.

Aus hiesiger Sicht stellt es sich sodann jedoch als Erfordernis dar, dass die diesbezügliche Aufgabenwahrnehmung, insbesondere hinsichtlich ihrer Grenzen, durch Satzung gemäß § 12 Abs. 1 S. 1, § 147 Abs. 1 S. 1 KSVG rechtsverbindlich geregelt wird. Einer solchen Regelung stehen dabei keine unionsrechtlichen Vorgaben entgegen. Gemäß Art. 6 Abs. 1 lit. e i. V. m. Abs. 3 lit. b DSGVO wird die Rechtsgrundlage für eine Datenverarbeitung durch das mitgliedstaatliche Recht festgelegt, welchem der Verantwortliche unterliegt (vgl. Erwägungsgrund 45). Letzteres Recht beschränkt sich nicht auf förmliche Parlamentsgesetze. Eine unionsrechtskonforme Datenverarbeitungsgrundlage kann vielmehr auch durch eine untergesetzliche Normsetzung erfolgen, insbesondere durch Rechtsverordnungen und kommunale Satzungen.[77] Erforderlich ist jedoch, dass diese untergesetzlichen Normen mit höherrangigem nationalem Recht in Einklang stehen sowie dass der Zweck und Umfang der Datenverarbeitung in normenklarer, d. h. für die betroffene Person nachvollziehbarer Art und Weise, hervorgeht.[78]

In letzterem Zusammenhang ist dem Wertungsgehalt des BMG Rechnung zu tragen, welches in Bezug auf Auskunftsersuchen anlässlich von Jubiläen in § 50 Abs. 2 S. 2 das Recht auf informationelle Selbstbestimmung und das Öffentlichkeitsinteresse in einen Ausgleich zueinander bringt. Eine diesbezügliche Satzung hat sich demnach auf solche Alters- und Ehejubiläen zu beschränken, welche aufgrund ihrer Jahreszahl als außergewöhnlich anzusehen sind und an denen deshalb ein gesteigertes öffentliches Interesse besteht. Das BMG zieht in § 50 Abs. 2 S. 2 für Altersjubiläen eine Untergrenze von 70 Jahren und lässt eine Registerauskunft hiernach im Fünf-Jahres-Rhythmus zu. Eine jährliche Auskunft kann erst ab dem 100. Lebensjahr erteilt werden. Als auskunftswürdiges Ehejubiläum wird das 50. und jedes folgende Ehejubiläum erachtet. Eine kommunale Satzung sollte diese Gesetzeswertung aufgreifen und sich an den diesbezüglichen Vorgaben orientieren.

Letzteres bedeutet indes nicht, dass die Jahresgrenzen des § 50 Abs. 2 S. 2 BMG zwingend zu übernehmen wären. Aus § 50 Abs. 2 BMG, welcher – wie bereits erwähnt – eine bestimmte Form der Gruppenauskunft in Form der Übermittlung, nicht jedoch die weitere Verarbeitung der hieraus erlangten Daten durch die empfangende Stelle regelt, kann jedoch der Schluss gezogen werden, dass dem jeweiligen Ereignis eine nach allgemeiner gesellschaftlicher Anschauung herausragende Bedeutung beizumessen ist. Dies kann, je nach örtlicher Auffassung, auch die Vollendung des 65. oder 50. Lebensjahres sein. Entscheidend ist auch, wie sich die diesbezügliche Verwaltungspraxis bislang darstellte. Gerade in Städten und Gemeinden, in welchen eine öffentliche Gratulation in der Vergangenheit regelmäßig vorgenommen wurde, gar eine kommunale „Tradition" darstellt, erscheint es auch aus datenschutzrechtlicher Sicht nicht zielführend, mit dieser Tradition aufgrund einer zu restriktiven datenschutzrechtlichen Sichtweise zu brechen.

Maßgeblich ist demnach, dass die Gratulationen sich auf wichtige Lebensereignisse beschränken. Welche dies letztlich sind, kann und muss die Kommune aufgrund ihrer

---

77 *Buchner/Petri*, in: Kühling/Buchner, DS-GVO/BDSG (2. Aufl. 2018), Art. 6, Rn. 84.

78 *Buchner/Petri*, a.a.O.

universellen Aufgabengarantie aus Art. 28 Abs. 2 S. 1 GG i. V. m. Art. 117 Abs. 3 SVerf. durch Satzung und unter Berücksichtigung des Persönlichkeitsrechts des ins Auge gefassten Adressatenkreises eigenverantwortlich regeln.

In allen vorgenannten Fallkonstellationen einer Gratulation ist den betroffenen Personen ein satzungsrechtliches Widerspruchsrecht in die Verarbeitung ihrer personenbezogenen Daten einzuräumen. Zwar enthält Art. 21 Abs. 1 DSGVO bereits ein gesetzlich normiertes Recht auf Widerspruch gegen eine Verarbeitung nach Art. 6 Abs. 1 S. 1 lit. e DSGVO. Eine gesetzlich vorgeschriebene Datenverarbeitung kann die betroffene Person hiernach jedoch nur dann unterbinden, wenn sich dies aus Gründen einer besonderen persönlichen Situation rechtfertigt. Im Falle einer satzungsrechtlich gestatteten Gratulation einer Privatperson durch die öffentliche Hand fällt unseres Erachtens eine Abwägung des Für und Wider der Datenverarbeitung indes stets zu Gunsten des zu Beglückwünschenden aus. Letzteres rechtfertigt die Kodifikation eines voraussetzungslosen Widerspruchrechts innerhalb der jeweiligen Satzung.

6.4.2 Gratulationen anlässlich der Geburt eines Kindes

Die Geburt eines Kindes stellt ein Ereignis dar, welches dem engen persönlichen Lebensbereich der Eltern zuzuordnen ist und aus Aspekten der informationellen Selbstbestimmung einen höheren Persönlichkeitsschutz erfordert, als dies bei Geburtstagen und sonstigen Jubiläen der Fall ist. Es kann dem Wunsch der Eltern entsprechen – und hierin ist sodann zugleich deren berechtigtes Interesse zu erblicken –, dass mit Ausnahme der gesetzlich vorgeschriebenen Fälle von Seiten der öffentlichen Verwaltung aus Anlass der Geburt nicht an sie herangetreten wird. Bereits bei der Geburt des ersten Kindes ist diesem Umstand Rechnung zu tragen, sprich es ist sicherzustellen, dass die Eltern auch tatsächlich in die Lage versetzt werden, ihr Widerspruchsrecht zeitnah mit der Geburt wahrnehmen zu können. Verwaltungsorganisatorisch ließe sich dies etwa durch eine entsprechende Mitteilung der Meldebehörde im Zeitpunkt der Registrierung des Kindes verwirklichen, aufgrund welcher die Eltern sodann ihr Widerspruchsrecht ausüben können.

6.4.3 Veröffentlichung von Glückwünschen in Druckmedien und auf Internetpräsenzen

Zu berücksichtigen ist abschließend, dass sich aus den vorgenannten Erwägungen keinerlei rechtliche Befugnisse zur Veröffentlichung personenbezogener Daten von Jubilaren bzw. neugeborenen Kindern und deren Eltern herleiten lässt. Obzwar die kommunale Selbstverwaltungsgarantie die Befugnis umfasst, sich sämtlicher örtlicher Angelegenheiten in Eigenverantwortung anzunehmen und diese Angelegenheiten durch Satzung zu regeln, findet diese institutionelle Garantie ihre Grenzen in der verfassungsmäßigen Ordnung, insbesondere in den Grundrechten. Das Allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG in seiner Ausprägung

als Recht auf informationelle Selbstbestimmung verbürgt dem Einzelnen die Befugnis grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.[79]

Eine kommunale Tradition, welche sich eine Veröffentlichung von besonderen Lebensereignissen der Einwohner zum Gegenstand nimmt, hat sich in den Grenzen des diesbezüglichen Persönlichkeitsrechts zu bewegen. Es ist insofern ein Interessenausgleich zwischen dem öffentlichen Interesse an Information und dem privaten Interesse an Diskretion herzustellen. Es erscheint geboten, von einer Veröffentlichung in Printmedien und auf Internetseiten abzusehen bzw. eine solche Veröffentlichung nur mit ausdrücklicher und informierter Einwilligung der betroffenen Person vorzunehmen. Denn obgleich Lebensereignisse wie Jubeltage und die hierauf bezogenen öffentlichen Kundgebungen in den allermeisten Fällen die betreffende Person ausschließlich in ihren positiven Facetten hervorheben dürften, so bedarf es dennoch keiner weiteren Erläuterung, dass in diesem Zusammenhang auch der Wunsch bestehen kann, nicht öffentlich genannt zu werden. Diesem berechtigten Interesse an der Geheimhaltung der persönlichen Lebensumstände gilt es Rechnung zu tragen. Von der Praxis einer ungefragten Veröffentlichung in Gemeindeblättern oder auf kommunalen Internetpräsenzen ist demnach grundsätzlich Abstand zu nehmen. Wird eine solche Verarbeitung auf eine Einwilligung der betroffenen Person gestützt, so sollte darauf geachtet werden, dass die Einwilligung über Art der Veröffentlichung (Amtsblatt, konkrete Benennung der Internetseite) und Umfang (welche Informationen sollen veröffentlicht werden?) informiert.

6.4.4 Einladungen zu kommunalen Veranstaltungen

Kritisch, und in der Regel aus datenschutzrechtlicher Sicht als unzulässig zu werten, sind Einladungen zu deren Personalisierung auf Daten des Melderegisters zugegriffen wird und in deren Zusammenhang die diesbezügliche Datenverarbeitung nicht explizit durch eine Rechtsgrundlage gedeckt ist.

Als praxisrelevant und problematisch hat sich dabei die Veranstaltung sog. „Seniorennachmittage" herausgestellt, zu deren Zweck Einwohner einer bestimmten Altersgruppe individuell angeschrieben und eingeladen werden. Werden die diesbezüglichen Alters- und Adressdaten durch die einladende Stelle, z. B. den Bürgermeister oder den Ortsvorsteher, unter Rückgriff auf Meldedaten erlangt, so fehlt es nach hiesiger Auffassung für eine solche Datenweitergabe an einer entsprechenden Rechtsgrundlage.

Wie bereits dargestellt ist die rechtliche Voraussetzung einer solchen innerbehördlichen Datenweitergabe gem. § 34 Abs. 1 S. 1 BMG, dass die Weitergabe zur Erfüllung der in der Zuständigkeit der Meldebehörde (Meldeamt) oder in der Zuständigkeit der empfangenden Stelle (andere fachliche Organisationseinheiten innerhalb der Gemeindebehörde) liegenden öffentlichen Aufgaben erforderlich ist. Erfolgt eine Weitergabe personenbezogener Daten, vorliegend von Personen eines gewissen Le-

[79] BVerfG, Urteil vom 15.12.1983 – 1 BvR 209, u. a./83, Beck RS 1983, 197403.

bensalters, von der Meldebehörde an eine andere Stelle innerhalb der Verwaltungseinheit, so ist es sowohl für die Rechtmäßigkeit dieser Weitergabe als auch für die anschließende Verarbeitung der übermittelten Daten in Form einer Einladung entscheidend, dass eine diesbezügliche Aufgabenzuweisung vorliegt.

Eine solche bereichsspezifische Aufgabenzuweisung findet sich weder im Kommunalselbstverwaltungsgesetz (KSVG) noch im übrigen Fachrecht. Ungeachtet dessen erscheint eine solche Datenverarbeitung in aller Regel nicht erforderlich, da auf die betreffenden Veranstaltungen nicht durch persönliche Ansprache, sondern auch auf andere Weise (Gemeindeblatt, Aushang, Internetpräsenz, Flyer etc.) aufmerksam gemacht werden kann.

6.5 Kfz-Kennzeichenerfassung bei einem Wertstoffzentrum

Ein Bürger einer saarländischen Kommune übermittelte uns einen Zeitungsbericht in dem berichtet wurde, dass der Leiter des örtlichen Wertstoffzentrums die Kennzeichen von Kraftfahrzeugen notiert. Wegen § 3 Abs. 2 Saarländisches Datenschutzgesetz (SDSG) fällt auch die nichtautomatisierte Verarbeitung durch öffentliche Stellen in den Anwendungsbereich des Datenschutzrechts.

„Wenn bei ihm jemand mit seinem Bauholz wieder kehrt macht, weil ihm die paar Euro zu viel sind, notiert er sich schon mal das Autokennzeichen. Um es anschließend ans Ordnungsamt weiter zu leiten. Mancher überlegt es sich dann doch noch mal…".
(Saarbrücker Zeitung vom 17.8.2018)

Unsere Anfrage beim zuständigen Bürgermeister der Kommune ergab, dass er keinerlei Kenntnis von der Praxis der Kennzeichenerfassung hatte und der Mitarbeiter aus eigenem Antrieb handelte. Eine Übermittlung an das Ordnungsamt habe zu keinem Zeitpunkt stattgefunden.

Die Belegschaft des Wertstoffzentrums wurde darauf hingewiesen, dass die Erfassung der Kfz-Kennzeichen unzulässig ist und zukünftig zu unterbleiben hat. Die Liste mit den bereits erfassten Kennzeichen wurde vernichtet.

6.6 Umsetzung der DSGVO bei den Feuerwehren

Die Datenschutz-Grundverordnung (DSGVO) hat auch innerhalb der Feuerwehren für Unsicherheiten im rechtskonformen Umgang mit personenbezogenen Daten gesorgt. Kaum verwunderlich also, dass man sich mit der Bitte um eine Informationsveranstaltung an unsere Dienststelle gewandt hat und wir diesem Wunsch nachgekommen sind. Sowohl beim Landesfeuerwehrausschuss als auch beim Landesfeuerwehrverband wurden Informationsveranstaltungen zur DSGVO angeboten.

Grundsätzlich muss bei der Verarbeitung personenbezogener Daten im Feuerwehrbereich unterschieden werden zwischen der Datenverarbeitung in Ausübung hoheitlicher Aufgaben der Hilfsorganisation Feuerwehr und der Datenverarbeitung im Rahmen von Feuerwehrverbänden und Fördervereinen der Feuerwehr.

6.6.1 Hilfsorganisation Feuerwehr

Bei dem Brandschutz und der Technischen Hilfeleistung handelt es sich um hoheitliche Aufgaben der Kommunen, für die in den meisten Fällen die Freiwilligen Feuerwehren zuständig sind.

Soweit eine Datenverarbeitung zur Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, eröffnet Art. 6 Abs. 1 lit. e i. V. m. Abs. 3 lit. b DSGVO dem nationalen Gesetzgeber u. a. die Möglichkeit, eigene Vorschriften zu erlassen.

Der Saarländische Gesetzgeber hat von dieser Befugnis Gebrauch gemacht und in § 52 des Saarländischen Brand- und Katastrophenschutzgesetzes (SBKG)[80] eine eigene Regelung getroffen, die die Datenverarbeitung in diesem Zusammenhang legitimiert.

Da es sich bei den Feuerwehren um kommunale Einrichtungen handelt, ist in der Regel der Datenschutzbeauftragte der Kommune auch als Datenschutzbeauftragter in den Freiwilligen Feuerwehren zuständig.

6.6.2 Fördervereine/Feuerwehrverbände

Landes- und Kreisfeuerwehrverband sowie Fördervereine der Freiwilligen Feuerwehren nehmen keine hoheitlichen Aufgaben wahr. Das heißt konkret, dass sie insoweit als nicht-öffentliche Stellen anzusehen sind und für die personenbezogene Datenverarbeitung in diesen Bereichen die Vorgaben aus der DSGVO maßgebend sind. Was genau Vereine und Verbände bezugnehmend auf die Vorgaben der DSGVO zu beachten haben, wurde von unserer Dienststelle in der Broschüre „Datenschutz im Verein“ beschrieben, die in unserem Internetangebot unter dem Pfad „Themen – Vereine“ zu finden ist. Auch die Fördervereine und die Feuerwehrverbände sind gut beraten, sich diesen Ratgeber genau anzuschauen und die Vorgaben der DSGVO in ihrer Zuständigkeit umzusetzen.

[80] Gesetz über den Brandschutz, die Technische Hilfe und den Katastrophenschutz im Saarland vom 29.11.2006, zuletzt geändert d. Gesetz v. 17.6.2015 (Amtsbl. S. 454).

7 Pass-, Melde- und Ausländerwesen

7.1 Prüfung der Nutzung des saarländischen Meldeportals zur Abfrage von personenbezogenen Daten

Seitens des Landespolizeipräsidiums wurde dem Unabhängigen Datenschutzzentrum Saarland ein dienstrechtlicher Vorgang zur Kenntnis gebracht, aus dem ersichtlich war, dass im Rahmen von polizeilichen Abfragen aus dem Melderegister anzugebende Aktenzeichen bzw. Abfragegründe wiederholt nicht hinreichend konkret gefasst waren, mit der Folge, dass eine datenschutzrechtliche Überprüfung der Zulässigkeit der Abfragen nicht möglich war.

Zur Prüfung, ob es sich hier um Einzelfälle handelte oder die diesbezüglichen Vorgaben in größerem Umfang verletzt worden waren, wurde das Landespolizeipräsidium gebeten, eine Stichprobe der nach § 40 Abs. 1, 2 und 3 Bundesmeldegesetz (BMG) zu führenden Protokollierung zur Verfügung zu stellen.

§ 40 BMG

(1) Die Meldebehörde hat bei einem automatisierten Abruf von Daten einer einzelnen Person Folgendes zu protokollieren:

1. *die abrufberechtigte Stelle,*
2. *die abgerufenen Daten,*
3. *den Zeitpunkt des Abrufs,*
4. *soweit vorhanden, das Aktenzeichen der abrufenden Behörde und*
5. *die Kennung der abrufenden Person.*

(2) Werden Daten über eine Vielzahl nicht näher bezeichneter Personen nach § 34 Abs. 2 abgerufen, sind zusätzlich der Anlass, die Abrufkriterien und die Anzahl der Treffer zu protokollieren.

(3) Ist die abrufende Stelle eine der in § 34 Abs. 4 S. 1 genannten Behörden, hat sie die Protokollierung vorzunehmen.

(4) Die Protokolldaten sind mindestens zwölf Monate aufzubewahren und zu sichern. Sie sind spätestens zum Ende des Kalenderjahres zu löschen, das auf die Speicherung folgt. Die Protokolldaten dürfen nur für Zwecke der Datenschutzkontrolle, hieraus folgender Strafverfahren, der Sicherstellung des Betriebs der Register und der Auskunftserteilung an die betroffene Person verarbeitet und genutzt werden.

Anhand der daraufhin durch den behördlichen Datenschutzbeauftragten des Landespolizeipräsidiums zur Verfügung gestellten Protokolldaten wurde die weitere Prüfung ermöglicht, in deren Rahmen sich rausstellte, dass die Eingabefelder für Aktenzeichen und Anlass der Abfrage oft nicht mit der nötigen Ernsthaftigkeit ausgefüllt wurden. Im Ergebnis herrschte Einigkeit darüber, hinsichtlich der genauen Bezeichnung des Aktenzeichens bzw. des Abfrageanlasses – insbesondere durch ein

Aufgreifen der Thematik im Rahmen von Fortbildungsveranstaltungen sowie Erstellung eines entsprechenden Informationsschreibens seitens des Datenschutzbeauftragten des Landespolizeipräsidiums – eine Sensibilisierung der polizeilichen Anwender herbeizuführen.

Aus Anlass der oben geschilderten Eingabe erfolgte eine allgemeine Prüfung hinsichtlich des Abfrageverhaltens der öffentlichen Stellen des Saarlandes.

Mit dem von der eGo-Service-Saar GmbH (fachlich) betriebenen Meldeportal Saar besteht innerhalb des Saarlandes eine zentrale Möglichkeit zur Durchführung von Melderegisterabfragen mittels eines automatisierten Abrufverfahrens. Das Meldeportal gliedert sich in einen öffentlich zugänglichen, jedoch kostenpflichtigen Bereich, der insbesondere Bürgern und Unternehmen offensteht und einen nicht-öffentlichen Bereich, der aus dem Landesdatennetz allein den saarländischen Behörden zur Nutzung zur Verfügung steht. Im Rahmen des Datenabrufs ist in der Eingabemaske ein Feld zur Begründung der Anfrage, insbesondere durch Angabe eines Aktenzeichens, zu befüllen.

Gegenstand der durch das Unabhängige Datenschutzzentrum Saarland vorgenommenen Prüfung war schwerpunktmäßig die Frage, ob und wie die Bediensteten der saarländischen Behörden ihrer Pflicht zur Begründung der einzelnen Abfragen über das Meldeportal nachkommen und inwiefern hierdurch datenschutzrechtliche Grundprinzipien wie Transparenz und Nachvollziehbarkeit zum Schutz der Betroffenen bei der Verarbeitung personenbezogener Daten gewahrt werden.

Grundlage der Prüfung war die Auswertung der Protokolldaten der Monate März und April 2017. Die Protokolldaten enthielten Angaben über den Zeitpunkt der jeweiligen Abfrage, über die abfragende Person und deren Behörde sowie zu den Abfrageparametern, d. h. nach wem bzw. unter Angabe welcher Kriterien nach einzelnen Personen im Meldedatenbestand gesucht wurde und schließlich, welche Gründe bzw. welchen Anlass der Nutzer für seine Abfrage angegeben hatte.

Von dem uns zur Verfügung gestellten Protokolldatenauszug wurden insgesamt 170.234 Einzelabfragen geprüft.

Die rechtlichen Rahmenbedingungen für Melderegisterübermittlungen zwischen öffentlichen Stellen sind in den §§ 33 bis 43 BMG festgelegt. Werden Meldedaten im automatisierten Abrufverfahren an eine Behörde übermittelt, ist dies zu protokollieren. Zuständig für die Protokollierung ist nach § 40 Abs. 1 BMG die Meldebehörde, deren Meldedaten abgefragt werden bzw. die gem. § 3 Abs. 2 S. 5 Saarländisches Gesetz zur Ausführung des Bundesmeldegesetzes (AGBMeldG)[81] eingerichtete Vermittlungsstelle. Eine Ausnahme gilt nach § 40 Abs. 3 BMG für die in § 34 Abs. 4 S. 1 BMG genannten Polizei-, Sicherheits-, Justiz- und Finanzbehörden. Diese haben die Protokollierung selbst vorzunehmen.

Beim Abruf von Daten einzelner Personen („Einzelauskunft") sind nach § 40 Abs. 1 BMG die abrufberechtigte Stelle, die abgerufenen Daten, der Zeitpunkt des Abrufs, soweit vorhanden das Aktenzeichen der abrufenden Behörde sowie die Kennung der

[81] Art. 1 des Gesetzes Nr. 1869 vom 13.10.2015 (Amtsbl. I S. 712), zuletzt geändert d. Gesetz v. 22.8.2018 (Amtsbl. S. 674).

abrufenden Person zu protokollieren. Bei sog. Listenauskünften, bei denen die Abfrage nicht unter Angabe des Namens einer bestimmten Person erfolgt, sondern allgemeinere Kriterien verwendet werden, die potentiell auf mehr als nur eine Person zutreffen, sind nach § 40 Abs. 2 BMG zusätzlich zu den oben genannten Merkmalen die Abrufkriterien, der Anlass der Abfrage und die Anzahl der Treffer zu protokollieren.

Die Pflicht zur Protokollierung dient dem Schutz datenschutzrechtlicher Grundprinzipien. Die Angabe des Aktenzeichens bzw. des Anlasses der Abfrage dient dabei insbesondere der Dokumentierung des Zwecks der Abfrage. Dies soll gem. § 40 Abs. 4 S. 3 BMG u. a. für die betroffene Person die Nachvollziehbarkeit der Verarbeitung ihrer personenbezogenen Daten gewährleisten und darüber hinaus die interne Kontrolle durch die behördlichen Datenschutzbeauftragten sowie die externe Kontrolle durch die Landesbeauftragte für Datenschutz ermöglichen.

Hinsichtlich der Dokumentation der Abfragegründe fiel auf, dass in der Eingabemaske des Meldeportals nicht zwischen Einzel- und Listenabfrage unterschieden wurde, sondern für Abfragegrund und -anlass lediglich ein einziges(!) Eingabefeld vorhanden war.

Entscheidendes Kriterium bei der Prüfung der ordnungsgemäßen Befüllung des Eingabefeldes war, ob mit dem vom Nutzer eingegebenen Inhalt – wie im Meldeportal selbst verlangt – eine Zuordnung zu einem konkreten Vorgang möglich war.

Unter Zugrundelegung des vorgenannten Kriteriums wurde festgestellt, dass in dem Auswertungszeitraum insgesamt 121.911 Abfragen kritisch zu bewerten waren, was im Verhältnis zu allen untersuchten Abfragen einer Quote von 71,6 % entspricht. Auch ergaben sich bei lediglich acht der 92 überprüften Stellen nach Sichtung der Protokollierungen keine Gründe zur Beanstandung.

Bei einem hohen Prozentsatz der zu beanstandenden Abfragen erfolgte die Eingabe einer offenbar willkürlichen Ziffern- oder Buchstabenfolge (bspw. „xyz“) oder unspezifischer Angaben (bspw. „Asyl“).

Aufgrund des Umstandes, dass eine überwiegende Zahl der Melderegisterabfragen durch öffentliche Stellen des Saarlandes als problematisch einzustufen sind, ist es aus unserer Sicht erforderlich, dass die behördlichen Datenschutzbeauftragten bei den Behörden des Landes und der Kommunen durch geeignete Stichprobenverfahren die Dokumentationspraxis der eigenen Mitarbeiter stärker in den Blick nehmen.

Die darüber hinaus von uns angeregte verpflichtende Eingabe von Abfragegrund (Aktenzeichen) **und** Abfrageanlass wurde zwischenzeitlich seitens der eGo-Service-Saar GmbH umgesetzt. Des Weiteren wird zukünftig zur Vermeidung der Eingabe willkürlicher Buchstaben- bzw. Ziffernfolgen die Möglichkeit geschaffen werden, eine Liste behördenspezifischer Anfrageanlässe zu erstellen, aus der seitens des Anfragenden der jeweilige Anfrageanlass ausgewählt werden kann.

7.2 Änderung der Saarländischen Meldedaten-Übermittlungsverordnung

Die Saarländische Meldedaten-Übermittlungsverordnung (MeldDÜV) regelt die Rechtsgrundlagen für die regelmäßige Datenübermittlung der Meldebehörden an bestimmte saarländische Behörden und sonstige öffentliche Stellen sowie für das automatisierte Abrufverfahren durch diese Stellen.

Im Rahmen einer Beteiligung unserer Dienststelle an einer beabsichtigten Änderung der MeldDÜV durch das Ministerium für Inneres, Bauen und Sport erfolgten unsererseits kritische Anmerkungen zu der geplanten Neufassung des § 54 MeldDÜV.

Die bisherige Übergangsvorschrift des § 54 MeldDÜV erlaubte den Meldebehörden für den Zeitraum bis zur technischen Umsetzung des elektronischen Rückmeldeverfahrens den Abruf von Daten aus den Melderegistern anderer Meldebehörden.

Nach dem uns vorgelegten Entwurf einer Neufassung der Vorschrift sollte die Abrufmöglichkeit trotz zwischenzeitlich erfolgter Umsetzung des elektronischen Rückmeldeverfahrens, dessen Fehlen ursprünglich Anlass für die Schaffung des § 54 MeldDÜV war, für die Meldebehörden „zur Erfüllung ihrer Aufgaben" weiterhin möglich sein. Im Rahmen der Verordnungsbegründung wurde hinsichtlich der den Meldebehörden obliegenden Aufgaben insbesondere auf die Fortschreibungspflicht gem. § 6 Bundesmeldegesetz (BMG) verwiesen.

Demgegenüber war aufgrund der Umsetzung des elektronischen Rückmeldeverfahrens nach unserer Auffassung kein Raum für eine weiterhin bestehende Befugnis der Meldebörden, über die allgemeine Behördenauskunft hinausgehende Daten bei anderen Meldebehörden abzurufen. Aufgrund des Regelungsinhalts des § 55 BMG, der ausdrücklich auf die Erfüllung von Aufgaben der *Länder* abstellt, ist insbesondere zweifelhaft, ob eine dahingehende Gesetzgebungskompetenz des Landes besteht oder diese nicht gem. Art. 73 Abs. 1 Nr. 3 GG i. V. m. §§ 2, 6 BMG ausschließlich beim Bundesgesetzgeber liegt.

Daneben wurde unsererseits angemerkt, dass die Formulierung „zur Erfüllung ihrer Aufgaben" zu weit gefasst sei und dass sich die beabsichtigte Neufassung im Abschnitt „Rückmelde-, Übergangs- und Schlussvorschriften" aufgrund der Gesetzessystematik an falscher Stelle befinde.

Unsere Anregungen wurden weitestgehend aufgegriffen. Im finalisierten Entwurf wurde durch das Ministerium für Inneres, Bauen und Sport der Passus „zur Erfüllung ihrer Aufgaben" um die Formulierung „insbesondere für die Berichtigung, Ergänzung und Fortschreibung des Melderegisters im Sinne des § 6 BMG" ergänzt. Des Weiteren wurde mitgeteilt, dass eine Verschiebung der Vorschrift vom vierten in den dritten Abschnitt der Verordnung erfolgen würde. Den weitergehenden kritischen Anmerkungen – insbesondere hinsichtlich der Frage der Gesetzgebungskompetenz – wurde leider keine Rechnung getragen.

7.3 Umgang mit Personalausweiskopien durch die Meldebehörden

Im Rahmen der elektronischen Aktenführung wurde in einer saarländischen Gemeinde die Vorgehensweise praktiziert, anlässlich des Zuzugs einer Person den Personalausweis der vorsprechenden Person zum Zwecke des Nachweises ihrer Identität einzuscannen und das eingescannte Dokument als zusätzlichen Nachweis der Richtigkeit des Melderegisters zu speichern. Diese Praxis wurde seitens unserer Dienststelle überprüft mit dem Ergebnis, dass eine Rechtsgrundlage für die Ablichtung und Speicherung von Personalausweisen im Melderegister nicht ersichtlich ist und insbesondere § 3 Abs. 1 S. 1 Bundesmeldegesetz (BMG) nicht als Rechtsgrundlage in Betracht kommt.

§ 3 BMG erlaubt zur Erfüllung der Aufgaben der Meldebehörden nach § 2 Abs. 1 und 3 BMG die Speicherung von Daten sowie die zum Nachweis von deren Richtigkeit erforderlichen Hinweise im Melderegister. Durch die Aufnahme von Hinweisen soll insbesondere gewährleistet werden, dass bei Unstimmigkeiten über die Richtigkeit von Daten die Möglichkeit besteht, Nachforschungen anzustellen, um die Richtigkeit zu belegen.

Nach diesseitiger Einschätzung fehlt es vorliegend jedoch bereits an der Geeignetheit der Aufbewahrung einer Personalausweiskopie als Nachweis für die Richtigkeit des Melderegisters. Insofern ist auszuführen, dass die Identität der vorsprechenden Person *per se* keinen Hinweis auf die Richtigkeit der gespeicherten Daten geben kann.

Hinsichtlich einer der Eintragung in das Melderegister *vorangehenden* Identitätsprüfung der vorsprechenden Person fehlt es demgegenüber an der Erforderlichkeit des Einscannens und Speicherns. Der Umstand, dass § 3 Abs. 1 Ziff. 17 BMG die aus dem Ausweis zu speichernden Daten explizit auf Ausstellungsbehörde, Ausstellungsdatum, letzten Tag der Gültigkeitsdauer und Seriennummer sowie ggf. Sperrkennwort und Sperrsumme begrenzt, impliziert bereits, dass weitergehende Inhalte – auch in der Form von Hinweisen – nicht gespeichert werden sollen. Darüber hinaus läuft die Speicherung des Ausweisdokuments in Gänze, einschließlich des Lichtbildes, dem Grundsatz der Datensparsamkeit gem. Art. 5 Abs. 1 lit. c der Datenschutz-Grundverordnung (DSGVO) zuwider, insbesondere weil dem Erfordernis einer Identitätsprüfung schon durch bloße Vorlage des Ausweisdokuments und Fertigung eines entsprechenden Vermerks Rechnung getragen werden könnte.

Im Übrigen ist die Verarbeitung personenbezogener Daten durch die Ablichtung von Personalausweisen gem. § 20 Abs. 2 S. 3 Personalausweisgesetz (PAuswG) – außer in den gesetzlich vorgegebenen Fällen – nur mit Einwilligung des Ausweisinhabers möglich.

Die Gemeinde wurde gebeten, das Verfahren nach unseren Vorgaben datenschutzkonform anzupassen und darüber hinaus wurde sie auf die bei der Datenspeicherung einzuhaltenden Löschfristen hingewiesen.

7.4 Fragenkatalog zur Verfassungstreue im Rahmen der Einbürgerung

Das Ministerium für Inneres, Bauen und Sport bat in seiner Funktion als Einbürgerungsbehörde um datenschutzrechtliche Einschätzung eines mit dem Einbürgerungsantrag vom Antragsteller auszufüllenden Fragebogens zur Verfassungstreue.

Der Fragenkatalog zielt darauf ab, etwaige Anhaltspunkte für Ausschlussgründe gem. § 11 Staatsangehörigkeitsgesetz (StAG)[82] zu eruieren.

§ 11 Staatsangehörigkeitsgesetz

„Die Einbürgerung ist ausgeschlossen, wenn

1. tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass der Ausländer Bestrebungen verfolgt oder unterstützt oder verfolgt oder unterstützt hat, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziele haben oder die durch die Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden, es sei denn, der Ausländer macht glaubhaft, dass er sich von der früheren Verfolgung oder Unterstützung derartiger Bestrebungen abgewandt hat, oder

2. nach § 54 Abs. 1 Nr. 2 oder 4 des Aufenthaltsgesetzes ein besonders schwerwiegendes Ausweisungsinteresse vorliegt.

Satz 1 Nr. 2 gilt entsprechend für Ausländer im Sinne des § 1 Abs. 2 des Aufenthaltsgesetzes und auch für Staatsangehörige der Schweiz und deren Familienangehörige, die eine Aufenthaltserlaubnis auf Grund des Abkommens vom 21. Juni 1999 zwischen der Europäischen Gemeinschaft und ihren Mitgliedstaaten einerseits und der Schweizerischen Eidgenossenschaft andererseits über die Freizügigkeit besitzen."

Abgefragt werden anhand des Fragenkatalogs insbesondere die Teilnahme an politisch, religiös oder ideologisch motivierten Gewalthandlungen, Mitgliedschaften bei oder Kontakte zu bestimmten Organisationen, Modalitäten der Einreise in die Bundesrepublik Deutschland sowie des Aufenthalts in Deutschland, Auslandsaufenthalte etc.

Insofern war die Vereinbarkeit der Erhebung der mit dem Fragenkatalog im Einzelnen abgefragten Daten mit datenschutzrechtlichen Vorgaben zu prüfen, wobei insbesondere zweifelhaft ist, ob den Antragsteller insofern eine Mitwirkungspflicht trifft, insbesondere vor dem Hintergrund, das die Beweislast für das Vorliegen von Ausschlussgründen gem. § 11 StAG bei der Behörde liegt.[83] Lehnt man, wie hier vertreten, bei der Prüfung von Ausschlusstatbeständen nach § 11

[82] Staatsangehörigkeitsgesetz vom 22.7.1913 (RGBl. I S. 583), zuletzt geändert d. Gesetz v. 11.10.2016 (BGBl. I S. 2218).

[83] VG des Saarlandes, Urteil vom 28. Februar 2012 – 2 K 895/10, Rn. 57 (zitiert nach juris).

StAG eine Mitwirkungspflicht des Einbürgerungsbewerbers mit der Begründung ab, dass die Einbürgerungsbehörde für das Vorliegen von Ausschlusstatbeständen darlegungs- und beweispflichtig ist, so hat dies Auswirkungen darauf, ob und in welchem Umfang die Einbürgerungsbehörde anlasslos Ermittlungen bzw. Nachforschungen zur Feststellung von Ausschlussgründen tätigen darf und kann. Dies hat zur Konsequenz, dass mit dem Fragenkatalog – anlasslos, also ohne dass im Einzelfall in der Person des Bewerbers Anhaltspunkte für einen der in § 11 StAG genannten Ausschlusstatbestände vorliegen - keine personenbezogenen Information vom Antragsteller erhoben werden dürfen, die darauf abzielen, eine Prüfung des § 11 StAG zu ermöglichen. Auf unsere Rechtsauffassung haben wir das Ministerium hingewiesen.

Das aufgrund der Anforderungen der Datenschutz-Grundverordnung (DSGVO) im Zusammenhang mit dem Fragenkatalog zur Verfassungstreue überarbeitete Informationsblatt nach Art. 13, 14 DSGVO über die Verarbeitung personenbezogener Daten im Einbürgerungsverfahren wurde auf Bitten des Ministeriums ebenfalls seitens unserer Dienststelle auf Konformität mit den datenschutzrechtlichen Vorgaben überprüft. Hinweise unsererseits hinsichtlich des Entfalls von Informationen über zu einem späteren Zeitpunkt mit gesondertem Einverständnis einzuholende Auskünfte über Sozialdaten, der Formulierung betreffend die Einholung personenbezogener Auskünfte bei Behörden in Drittländern sowie der Angabe der Kontaktdaten des behördlichen Datenschutzbeauftragten wurden im Folgenden seitens des Ministeriums eingearbeitet.

Des Weiteren wurde unsererseits angemerkt, dass die beabsichtigte unbefristete Aufbewahrung der Unterlagen des Einbürgerungsverfahrens aufgrund des in Art. 17 Abs. 1 lit. a DSGVO normierten Rechts auf Löschung von Daten bei Wegfall ihrer Notwendigkeit datenschutzrechtlichen Bedenken unterfällt.

8 Beschäftigtendatenschutz

8.1 Data-Warehouse für Zwecke des Personalmanagements

Im Rahmen der Beteiligung nach § 26 Abs. 2 S. 2 Saarländisches Datenschutzgesetz a. F. (SDSG a. F.) (heute: § 19 Abs. 2 S. 2 SDSG) wurden wir durch die Landesregierung über die Pläne informiert, für Zwecke des Personalmanagements eine sog. Data-Warehouse-Lösung, also ein zentrales Datenbanksystem, das aus verschiedenen Datenquellen Analysen erstellt, zu entwickeln. Mit der Konzeptionierung und Entwicklung einer solchen Softwarelösung hatte die Personalentwicklungs- und Koordinationsstelle das Ministerium für Finanzen und Europa beauftragt.

Das ursprüngliche Konzept sah vor, dass Grundlage der Data-Warehouse-Lösung die unterschiedlichen IT-Systeme sein sollten, die in den einzelnen Ressorts für die unterschiedlichen Zwecke der Personalverwaltung geführt werden. Die entsprechenden Datenbanken, beziehungsweise die darin enthaltenen personenbezogenen Daten, sollten zu Auswertungszwecken in einer weiteren, parallel einzurichtenden Datenbank zusammengeführt werden. Diese Zusammenführung sollte ursprünglich nicht nur ressortintern, sondern ressortübergreifend erfolgen und an zentraler Stelle betrieben werden. Weder war abschließend spezifiziert, welche Datenbanken zusammengeführt werden sollten, noch war der Umfang der Datenkategorien definiert, die zusammengeführt werden sollten.

Ziel der Zusammenführung sollte sein, die Datenbestände in einem einheitlichen Abrufverfahren den beteiligten Stellen/Personen mittels standardisierter Auswertungen und ressortspezifischer Ad-hoc-Auswertungen für Analysezwecke zugänglich zu machen. Die Data-Warehouse-Lösung sollte es den einzelnen Ressorts ermöglichen, aus verteilten und unterschiedlich strukturierten Datenbeständen durch zentrale Zusammenführung eine globale und integrierte Sicht auf die Quelldaten zu schaffen, um damit übergreifende Auswertungen zu tätigen. Prinzipiell wäre hierbei auch eine Nutzung des Systems für umfassende Data-Mining-Analysen zur Erkennung von bestimmten Regelmäßigkeiten und verborgenen Zusammenhängen denkbar.

Technisch sollte dies durch das Bereithalten einer zentralen, einheitlichen und konsistenten Datenbasis realisiert werden. Diese Datenbasis im Analysesystem sollte von den Quelldaten unabhängig sein und die Möglichkeit einer zentralen Archivierung der Daten mit Historisierung bieten. Hierzu war beabsichtigt, die Daten aus den unterschiedlichen Quellsystemen einmal monatlich auszulesen, um sie nach einer Transformation in ein einheitliches Datenformat im Analysesystem dauerhaft vorzuhalten. Eine Anonymisierung oder Pseudonymisierung sollte nicht stattfinden.

Die mit der Einführung einer Data-Warehouse-Lösung geschaffenen Verknüpfungs- und Auswertemöglichkeiten begegneten aus hiesiger Sicht ganz grundsätzlichen datenschutzrechtlichen Bedenken. Das Recht auf informationelle Selbstbestimmung

gewährleistet als Ausprägung des allgemeinen Persönlichkeitsrechts die Befugnis des Einzelnen, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Der Schutzbereich ist bereits dann berührt, wenn personenbezogene Daten in einer Art und Weise genutzt werden, die der Betroffene nicht überschauen oder beherrschen kann. Denkbar wäre es beispielsweise, dass personenbezogene Daten aus Zeiterfassungssystemen mit Beihilfedaten zusammengeführt werden, um hierdurch personenbezogene Auswertungen im Hinblick auf die Gründe von krankheitsbedingten Abwesenheiten bzw. Fehlzeiten zu analysieren oder daraufhin auszuwerten, wie viele Krankheitstage pro Mitarbeiter vorliegen.

Um derartigen Gefährdungen durch die Nutzung automatisierter Datenverarbeitungssysteme wirksam zu begegnen, bedarf es in Abhängigkeit zum Eingriffsgewicht der Sicherstellung einer ausreichenden Transparenz gegenüber den betroffenen Personen, einer aufsichtlichen Kontrolle, der Möglichkeit effektiven Rechtsschutzes sowie entsprechender organisatorischer und verfahrensrechtlicher Sicherungen, die die Einhaltung der Grundsätze des Art. 5 Abs. 1 Datenschutz-Grundverordnung (DSGVO) sicherstellen und dabei neben dem Prinzip der Datenminimierung und dem Prinzip der Speicherbegrenzung insbesondere ausreichenden Schutz gegen Zweckentfremdung gewähren.

Nach Art. 5 Abs. 1 lit. c DSGVO müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Dieser Grundsatz der Datenminimierung verbietet eine Speicherung personenbezogener Daten, welche für die im Zeitpunkt der Erhebung/Speicherung festgelegten Zwecke nicht erforderlich sind, auch wenn dies mit dem Ziel erfolgt, diese zusätzlichen Daten für mögliche zukünftige Auswertung vorzuhalten. Damit soll seitens des Verordnungsgebers gerade der Entstehung von Datenpools vorgebeugt werden. Das ursprünglich vorgelegte Konzept enthielt jedoch keine derartigen Beschränkungen. Der Grundsatz der Zweckbindung nach Art. 5 Abs. 1 lit. b DSGVO besagt, dass personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke verarbeitet werden dürfen. Aus dieser Zweckfestlegung muss – im vorliegenden Fall für den betroffenen Beschäftigten – der Verwendungszusammenhang eindeutig erkennbar sein; dies dient der Information der betroffenen Person, die wissen muss, warum und wofür seine personenbezogenen Daten benötigt bzw. gewünscht werden. Eine vage oder globale Umschreibung der Zwecke genügt diesen Anforderungen nicht. Nur wenn Sinn und Zweck der jeweiligen Vorgänge präzise vorab festgelegt sind, kann der Beschäftigte wirklich beurteilen und prognostizieren was mit seinen Daten passiert.

Für Datenverarbeitungsverfahren, die wie hier der Erstellung statistischer Auswertungen dienen sollen, sind jedoch Einschränkungen des Zweckbindungsgebotes zulässig, sodass prinzipiell auch die Speicherung personenbezogener Daten auf Vorrat für noch nicht hinreichend konkretisierte Zwecke zulässig sein kann; allerdings darf hierfür nicht jede personenbezogene Information verwendet werden, sondern es muss genau geprüft werden, ob das Ziel nicht auch durch eine frühzeitige Anonymisierung der Daten erreicht werden kann. Zudem bedarf es besonderer Vorkehrungen für die Durchführung und Organisation der Verarbeitung. Dies hat zur Konsequenz, dass die eine Identifizierung der betroffenen Personen ermöglichenden Daten zum frühestmöglichen Zeitpunkt gelöscht werden müssen (Prinzip der Speicherbegrenzung, Art.

5 Abs. 1 lit. e DSGVO) und bis dahin von den übrigen Auswertemerkmalen getrennt und unter besonderem Verschluss aufbewahrt werden müssen.

Um trotz unserer grundsätzlichen Bedenken die Einführung einer Data-Warehouse-Lösung für Zwecke des Personalmanagements realisieren zu können, hat der Landesgesetzgeber mit der Neufassung des Saarländischen Datenschutzgesetzes (SDSG) in § 22 Abs. 4 eine Regelung eingeführt, die ein solches Verfahren legitimieren soll. Die Vorschrift geht auf einen von uns vorgelegten Formulierungsvorschlag zurück, mit dem präzise gesetzliche Vorgaben geschaffen werden, aus denen sich der Umfang der Quellsysteme bzw. der Datenkategorien, die Dauer der Datenspeicherung und die zulässigen Auswertezwecke ergeben.

§ 22 SDSG - Verarbeitung von Beschäftigtendaten

„(4) Die nach Abs. 1 gespeicherten personenbezogenen Daten von Beschäftigten dürfen durch den Verantwortlichen zur Ermöglichung von Auswertungen zu den in Abs. 1 genannten Zwecken zusammengeführt und für die Dauer der Speicherung in den Quellsystemen vorgehalten werden."

Die neue gesetzliche Regelung erlaubt die zentrale Zusammenführung von personenbezogenen Daten, die bei der verantwortlichen Stelle zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses bereits vorhanden sind. Der Begriff „*zusammenführen*" stellt dabei klar, dass das Vorhalten im Data-Warehouse nur als technischer Zwischenschritt zu verstehen ist, mit der Folge, dass personenbezogene Daten, die zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses nicht mehr erforderlich sind und daher in den Quellsystemen zu löschen sind, auch im Data-Warehouse nicht mehr vorgehalten werden dürfen. Durch den Verweis auf bereits gespeicherte Daten wird ausgeschlossen, dass für das Data-Warehouse weitere personenbezogene Daten erhoben werden dürfen. Durch die Verwendung des Begriffs „*Ermöglichung*" wird klargestellt, dass noch nicht eine abschließende, konkret benannte Liste von Auswertungen vorliegen muss. Vielmehr soll das System die Erstellung auch noch nicht konkret zu benennender Auswertungen ermöglichen und damit flexibel bleiben, dies jedoch nur solange wie diese Auswertungen der Erreichung der in § 22 Abs. 1 SDSG genannten Zwecke dienen, was durch technische und organisatorische Maßnahmen sicherzustellen ist. Die Verwendung von besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO ist – wie sich auch aus der Gesetzesbegründung ergibt – ebenso ausgeschlossen, wie die Verwendung von personenbezogener Daten von Bewerbern.

Leider konnten wir uns im Gesetzgebungsverfahren nicht mit unserer Forderung durchsetzen, die im Rahmen eines solchen Systems zulässigen Auswertungen auf Zwecke der Personalplanung und des Personaleinsatzes zu beschränken. Es bestand aber Einigkeit dahingehend, dass die Risiken, die von einem solchen Data-Warehouse-System für die Rechte und Freiheiten der Beschäftigten ausgehen, durch angemessene technische und organisatorische Maßnahmen kompensiert werden müssen. Insofern begrüßen wir, dass in der Gesetzesbegründung ausdrücklich aufgenommen worden ist, dass zu diesen technischen und organisatorischen Maßnahmen insbesondere auch die Einrichtung eines behördeninternen Freigabeverfahrens

zählt, das immer dann zu durchlaufen ist, bevor in dem Data-Warehouse-System neue Auswertemöglichkeiten geschaffen werden. Nach hiesiger Auffassung sollten in einem solchen behördeninternen Freigabeverfahren die Personalvertretungen eingebunden werden, um die Interessen der Beschäftigten ausreichend zu berücksichtigen.

8.2 Nutzung von Facebook-Daten für ein Disziplinarverfahren

Im November 2018 wandte sich ein Mitarbeiter aus dem Bereich Personalangelegenheiten des Landespolizeipräsidiums (LPP) an unsere Dienststelle. Er trug vor, dass er ein disziplinarrechtliches Ermittlungsverfahren in Bezug auf das Dienstverhältnis und eine Nebenbeschäftigung eines saarländischen Polizeibeamten zu führen habe. Nun sei ihm zur Kenntnis gelangt, dass dieser Polizeibeamte bei Facebook ein Konto mit einem privaten Profil eingerichtet habe und sich aus der Kommunikation mit Freunden in Facebook im geschlossenen Nutzerkreis mögliche Hinweise auf eine Nebenbeschäftigung ergäben. Ein Facebook-Freund des betreffenden Beamten sei ebenfalls Polizeibeamter und könne ihm die Daten zur Verfügung stellen. Ferner führte der Ermittlungsbeamte aus, dass seiner Auffassung nach im Falle eines Disziplinarverfahrens § 22 Abs. 3 Saarländisches Datenschutzgesetz (SDSG) Anwendung finden könne.

Nach § 22 Abs. 3 SDSG dürfen zur Aufdeckung von Straftaten oder einer erheblichen Dienstpflichtverletzung personenbezogene Daten von Beschäftigten nach Abs. 1 oder 2 nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Dienst- oder Arbeitsverhältnis eine Straftat oder eine erhebliche Dienstpflichtverletzung 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 der Verarbeitung im Hinblick auf den Anlass nicht unverhältnismäßig sind. § 22 SDSG findet Anwendung auf Beschäftigtendaten, also solche personenbezogene Daten, die im Zusammenhang mit einer Beschäftigung vor, während oder auch nach einem Beschäftigungsverhältnis erhoben werden. Nur diese Daten könnten im konkreten Fall, sofern eine erhebliche Dienstpflichtverletzung vorliegt, gemäß § 22 Abs. 3 SDSG auch zu bestimmten anderen Zwecken verarbeitet werden. Bei den vom Betroffenen in Facebook nicht allgemein zugänglich eingestellten privaten Profil- und Kommunikationsdaten handelt es sich aber zweifelsfrei nicht um Beschäftigungsdaten des Dienstherrn, so dass auch bei einer erheblichen Dienstpflichtverletzung eine Nutzung dieser Daten nicht auf § 22 Abs. 3 SDSG gestützt werden darf.

Darüber hinaus stellt sich die Frage, inwieweit eine Datenübermittlung durch den Facebook-Freund und Polizeibeamten, der in diesem Kontext als Privatperson und nicht als Polizeibeamter handeln würde, an den gemeinsamen Dienstherrn, hier die Personalstelle, zulässig wäre. Hierfür war zunächst zu klären, in welchen gesetzlichen

Anwendungsbereich die Datenübermittlung einer Privatperson an eine öffentliche Stelle fällt.

Nach Art. 2 Abs. 1 Datenschutz-Grundverordnung (DSGVO) gilt diese Verordnung 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. Ausgenommen ist gemäß Art. 2 Abs. 2 lit. c DSGVO i. V. m. Erwägungsgrund 18 die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten jedoch ohne Bezug zu einer beruflichen Tätigkeit. Die Weitergabe personenbezogener Daten, die Äußerungen betreffen, die eine andere Person in einem sozialen Netzwerk gegenüber einem eingeschränkten Nutzerkreis gemacht hat, an öffentliche Stellen zur Verfolgung und Ahndung dieser Äußerungen im Wege eines Disziplinarverfahrens stellt keine persönliche oder familiäre Tätigkeiten mehr da, da der persönlich bzw. familiäre Wirkkreis verlassen wird.

Wird die Anwendbarkeit der DSGVO im konkreten Fall bejaht, so ist in der Folge zu prüfen, ob die Datenverarbeitung, hier die Datenübermittlung durch eine Privatperson an eine öffentliche Stelle, auch nach Art. 6 DSGVO rechtmäßig erfolgen kann. Die Verarbeitung ist gemäß Art. 6 Abs. 1 lit. f i. V. m. Erwägungsgrund 47 nur 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. Nach Erwägungsgrund 47 ist das Bestehen eines berechtigten Interesses in jedem Fall besonders sorgfältig zu ermitteln, wobei auch zu prüfen ist, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. 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. Selbst wenn berechtigte Interessen des Dritten, hier des Dienstherrn, bejaht werden, wird die Zulässigkeit der Datenverarbeitung im konkreten Fall nach unserer Auffassung scheitern, da die betroffene Person nicht bereits zum Zeitpunkt der Erhebung absehen konnte, dass seine Äußerungen zu einer Nebentätigkeit im geschlossenen Nutzerkreis von Facebook für den späteren konkreten Zweck eines Verwaltungsermittlungsverfahrens genutzt werden würden.

Im Ergebnis wäre daher eine Datenübermittlung des Facebook-Freundes an den gemeinsamen Dienstherrn als unzulässig zu bewerten. Darüber hinaus könnte der Betroffene nach Art. 82 DSGVO gegebenenfalls einen Schadensersatzanspruch gegen den verantwortlichen Datenübermittler geltend machen.

8.3 Zuverlässigkeitsprüfung nach Luftsicherheitsgesetz

Zum Schutz vor Angriffen auf die Sicherheit des zivilen Luftverkehrs hat die Luftsicherheitsbehörde, im Saarland angesiedelt beim Ministerium für Wirtschaft, Arbeit, Energie und Verkehr, gemäß § 7 Luftsicherheitsgesetz (LuftSiG)[84] die Zuverlässigkeit von Beschäftigten zu überprüfen, die beispielsweise Zugang zu Sicherheitsbereichen im Flughafen haben. Dazu gehören unter anderem auch Reinigungsfirmen, Instandhaltungsbetriebe, aber auch Fracht- und Postunternehmen.

Die Überprüfung erfolgt gemäß § 7 Abs. 2 LuftSiG auf Antrag des Betroffenen.

Ein Beschäftigter eines solchen Unternehmens hat sich mit einer Beschwerde an uns gewandt und mitgeteilt, dass sein Arbeitgeber neben den erforderlichen Daten auch eine Kopie seines Personalausweises zur Vorlage bei der Luftsicherheitsbehörde benötige. Der Beschwerdeführer bemängelte sowohl die Tatsache, dass sein Arbeitgeber die prüfungsrelevanten Daten gebündelt für die Luftsicherheitsbehörde sammele als auch die verpflichtende Anforderung zur Vorlage einer Kopie seines Personalausweises.

Der Antwort des Arbeitgebers auf unsere Bitte um diesbezügliche Stellungnahme konnten wir entnehmen, dass die gebündelte Sammlung der Unterlagen für die Luftsicherheitsbehörde als Service des Unternehmens an seine Beschäftigten zu verstehen sei und es natürlich jedem Beschäftigten frei stehe, die erforderlichen Unterlagen selbst bei der Luftsicherheitsbehörde einzureichen. Es müsse jedoch auch gegenüber dem Arbeitgeber der Nachweis geführt werden, dass die Zuverlässigkeitsprüfung durch die Luftsicherheitsbehörde erfolgreich bestanden wurde.

Zur Vorlage einer Kopie des Personalausweises führte der Arbeitgeber aus, dass er sich diesbezüglich auf das Formblatt zur Zuverlässigkeitsüberprüfung der Luftsicherheitsbehörde bezogen habe, in dem ausdrücklich eine Kopie des Personalausweises angefordert wird. Als Nachweis wurde uns das entsprechende Formular vorgelegt.

Auf unsere Nachfrage, gestützt auf welche Rechtsgrundlage eine Kopie des Personalausweises angefordert werde, teilte die Luftsicherheitsbehörde mit, dass das Formular bundesweit unter den Luftsicherheitsbehörden abgestimmt sei.

Gem. § 7 Abs. 3 Nr. 1 LuftSiG darf die Luftsicherheitsbehörde die Identität des Betroffenen zur Überprüfung der Zuverlässigkeit überprüfen. Das LuftSiG enthält aber keine Regelung, wonach Kopien von Ausweisen erstellt werden dürfen oder müssen [gesetzlich geregelte Fälle gibt es z. B. in § 8 Abs. 2 S. 2 Geldwäschegesetz (GWG)[85],

[84] Vom 11.1.2005 (BGBl. I S. 78), zuletzt geändert d. Gesetz v. 23.2.2017 (BGBl. I S. 298).

[85] Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten vom 23.6.2017 (BGBl. I S. 1822), zuletzt geändert d. Gesetz v. 10.7.2018 (BGBl. I S. 1102).

§ 95 Abs. 4 S. 3 Telekommunikationsgesetz (TKG)[86], § 64 Abs. 1 Nr. 2 Fahrerlaubnisverordnung (FeV)[87]]. Bei dieser Sachlage sind die spezialgesetzlichen Regelungen des Personalausweisgesetzes (PAuswG)[88] zu beachten.

§ 14 PAuswG besagt Folgendes:

"Die Erhebung und Verwendung personenbezogener Daten aus dem Ausweis oder mithilfe des Ausweises darf ausschließlich erfolgen durch

1. zur Identitätsfeststellung berechtigte Behörden nach Maßgabe der §§ 15 bis 17

2. öffentliche Stellen und nichtöffentliche Stellen nach Maßgabe der §§ 18 bis 20."

Die §§ 15 bis 17 PAuswG sehen jedoch keine Fälle vor, in denen Kopien von Ausweisen erstellt werden dürfen oder müssen. Selbst wenn man als Auffangtatbestand § 14 Ziff. 2 heranziehen würde, wäre § 20 Abs. 2 PAuswG zu beachten:

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

Hieraus ergibt sich, dass Ausweiskopien nur mit der ausdrücklichen Zustimmung des Ausweisinhabers gefertigt und als Identitätsnachweis verwendet werden dürfen. Die Kopien dürfen damit von öffentlichen Stellen nicht als Identitätsnachweis verlangt werden, sondern der Ausweisinhaber ist darauf hinzuweisen, dass er den Identitätsnachweis mit einer Ausweiskopie führen kann, aber nicht muss. Darüber hinaus ist zu beachten, dass dann auch Ausweisdaten, die nicht zur Identifizierung benötigt werden, auf der Kopie vom Ausweisinhaber geschwärzt werden können und sollen (wie z. B. die Augenfarbe).

Unsere rechtliche Bewertung ergab daher, dass die Forderung zur Vorlage einer Ausweiskopie, ohne auf die Freiwilligkeit dieser Vorlage und auf die Möglichkeit der Schwärzung der Daten, die nicht zur Identifizierung benötigt werden, hinzuweisen, datenschutzrechtlich bedenklich ist. Aus unserer Sicht musste die Luftsicherheitsbehörde Alternativen zum Identitätsnachweis per Ausweiskopie anbieten und darauf hinweisen, dass bei freiwilliger Vorlage einer Kopie des Personalausweises diese unverzüglich vernichtet und nicht in der Akte vorgehalten wird. Das Verfassen eines Vermerkes "Personalausweiskopie hat vorgelegen" wäre ausreichend.

Die Luftsicherheitsbehörde hat daraufhin ihr Formular entsprechend unserer Vorgaben datenschutzgerecht gestaltet. Aufgrund dieses Vorfalls wurden Überlegungen

---

[86] Telekommunikationsgesetz vom 22.6.2004 (BGBl. I S. 1190), zuletzt geändert d. Gesetz v. 29.11.2018 (BGBl. I S. 2230).

[87] Verordnung über die Zulassung von Personen zum Straßenverkehr vom 13.12.2010 (BGBl. I S. 1980), zuletzt geändert d. Verordnung v. 3.5.2018 (BGBl. I S. 566).

[88] Gesetz über Personalausweise und den elektronischen Identitätsnachweis vom 18.6.2009 (BGBl. I S. 1346), zuletzt geändert d. Gesetz v. 18.7.2017 (BGBl. I S. 2745).

getätigt, das Luftsicherheitsgesetz eventuell so zu novellieren, dass die Vorlagepflicht des Personalausweises gesetzlich geregelt werden soll.

8.4 GPS-Ortung von Beschäftigten

Im Berichtszeitraum haben sich mehrfach Beschäftigte an uns gewandt, die sich über die Installation von GPS-Geräten in ihren Dienstfahrzeugen und die damit einhergehende Überwachung durch ihren Arbeitgeber beschwert haben.

Durch die Auswertung von GPS-Daten kann festgestellt werden, zu welchem Zeitpunkt sich die Empfangsgeräte, die in den von den Beschäftigten genutzten Fahrzeugen installiert sind, an welchen Orten befunden haben. Das System ermöglicht damit, den genauen Aufenthalt von Beschäftigten, soweit sie sich in unmittelbarer Nähe ihrer Einsatzfahrzeuge befinden, in zeitlicher und örtlicher Hinsicht permanent während der Arbeitszeiten abzubilden und zu verfolgen. Auch wenn sich diese Angaben unmittelbar nur auf das Empfängerteil beziehen, entsteht durch die beim Arbeitgeber mögliche Gerätezuordnung zu den ein entsprechendes Fahrzeug führenden Beschäftigten ein Personenbezug. Die Standortdaten der GPS-Empfangsgeräte stellen daher personenbezogene Daten im Sinne von Art. 4 Nr. 1 Datenschutz-Grundverordnung (DSGVO) dar.

Ein solcher Einsatz von Ortungstechnik setzt nach Art. 5 Abs.1 lit. a i. V. m. Art. 6 Abs.1 DSGVO voraus, dass die Verarbeitung personenbezogener Daten durch eine Rechtsvorschrift erlaubt wird oder dass die Betroffenen in diese Verarbeitung eingewilligt haben.

Im Arbeitsverhältnis lässt sich die grundsätzlich durch Art. 88 DSGVO i. V. m. § 26 Bundesdatenschutzgesetz (BDSG) geregelte Verarbeitung von Beschäftigtendaten nur in engen Grenzen auf Einwilligungen der Beschäftigten stützen, denn aufgrund des Abhängigkeitsverhältnisses zum Arbeitgeber liegt die für eine Einwilligung vorausgesetzte Freiwilligkeit der Entscheidung (vgl. § 26 Abs. 2 BDSG) in aller Regel nicht vor. Dies gilt gerade auch für die ausschließlich im Interesse des Arbeitgebers stattfindende und für die Beschäftigten mit einem ständigen Überwachungsdruck verbundene Verarbeitung von Standortdaten. Eine Legitimierung dieser Datenverarbeitung durch die Einwilligung der Beschäftigten scheidet somit in der Regel aus.

Gemäß § 26 Abs. 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses u. a. auch dann verarbeitet werden, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. Bei der Beurteilung der Erforderlichkeit von Überwachungsmaßnahmen am Arbeitsplatz muss grundsätzlich eine Interessenabwägung zwischen den Interessen des Arbeitgebers an einem reibungslosen Betriebsablauf und dem Interesse der Arbeitnehmer am Schutz ihrer Persönlichkeitsrechte am Arbeitsplatz vorgenommen werden. Hierbei ist zu beachten, dass eine ständige Überwachung der Mitarbeiter während der gesamten Arbeitszeit und der damit einhergehende permanente Überwachungsdruck in schwerwiegender Weise in das allgemeine Persönlichkeitsrecht der Arbeitnehmer eingreifen.

Ein GPS-Einsatz zur Mitarbeiterdisposition kann zwar als ein legitimes Interesse des Arbeitgebers i. S. d. Vorschrift angesehen werden, um Zeit zu sparen oder Aufträge effizienter abwickeln zu können. Für die Wahrnehmung dieses Zwecks ist es jedoch vollkommen ausreichend, wenn der Arbeitgeber die Standortdaten seiner Beschäftigten ausschließlich in Echtzeit verarbeitet. Hier genügt die Kenntnis des aktuellen Fahrzeugstandortes und der aus den Veränderungen erkennbaren Bewegungsrichtung. Eine dauerhafte GPS-Überwachung ist hingegen in diesem Fall nicht erforderlich und greift in unzulässiger Weise in die Rechte der Arbeitnehmer ein. Lediglich in besonderen Ausnahmefällen, wie beispielsweise bei Geldtransportern oder Rettungsfahrzeugen, kann eine andere Betrachtung geboten sein.

Da die Telematik-Systeme meist auch zur Kontrolle der Arbeitszeiten und des Fahrverhaltens genutzt werden können, ist das GPS-System auch zur Leistungs- und Verhaltenskontrolle der Beschäftigten geeignet. Eine Nutzung der zu Dispositionszwecken erhobenen Daten zur Kontrolle der Mitarbeiter stellt jedoch eine Zweckänderung dar und ist grundsätzlich unzulässig.

Vor dem Einsatz derartiger Überwachungsmaßnahmen sollte zur Wahrung des Mitbestimmungsrechts die Personalvertretung beteiligt werden.

8.5 Bewerbung über den Dienstweg

In manchen saarländischen Behörden wird immer noch das sogenannte „Bewerbungsverfahren über den Dienstweg" praktiziert. Dabei muss ein Beamter, der sich auf eine behördeninterne oder -externe Stellenausschreibung bewirbt, den „Dienstweg" einhalten. Das heißt, alle unmittelbaren Vorgesetzten des Beamten müssen die Bewerbung zur Kenntnis nehmen, bis sie bei der zuständigen Personalabteilung eingereicht werden kann. Dies hat zur Folge, dass einige Beamten befürchten, durch Bewerbungen bei ihren Vorgesetzten einen schlechten Eindruck zu hinterlassen und ihnen ihr Anliegen zukünftig nachteilig ausgelegt werden kann. Genau mit diesem Anliegen hat sich ein Beschwerdeführer an unsere Dienststelle gewandt und die Praxis der Bewerbungsvorlage über den Dienstweg datenschutzrechtlich hinterfragt.

Schon im Jahre 1995 war die geschilderte Praxis der Bewerbung auf dem Dienstweg Gegenstand datenschutzrechtlicher Überlegungen auf Bundesebene. Das Bundesministerium des Inneren teilte in einer Antwort an die Datenschutzaufsichtsbehörden die vorgetragenen Bedenken und stellte fest: „Eine Bewerbung eines Beamten auf eine behördeninterne oder externe Stellenausschreibung stellt von ihrem Sinn und Zweck her keinen Antrag im Sinne der Dienstpetition dar. Vielmehr haben die Bewerbung und das der Bewerbung zugrundeliegende Ausschreibungs- und Auslese-verfahren eine eigenständige Bedeutung, die die Einhaltung des Dienstweges nicht voraussetzt."

Weiterhin führte das Bundesministerium für Inneres in seiner damaligen Antwort aus: „Die Pflicht des Beamten, seine Vorgesetzten rechtzeitig über einen von ihm angestrebten Wechsel zu unterrichten, wird dem Informationsbedürfnis des Dienstherrn voll gerecht, so dass auch aus diesem Grunde eine Vorlage der Bewerbung auf dem Dienstweg nicht erforderlich ist".

Auch in unserem Tätigkeitsbericht für die Jahre 2011/2012 (siehe Kap. 16.1.2 S. 87 f.) wurde dieses Verfahren thematisiert. Alle saarländischen Ministerien wurden durch unsere Dienststelle mit Schreiben vom 3. September 2012 darauf hingewiesen, dass das Bewerbungsverfahren über den Dienstweg aus datenschutzrechtlicher Sicht unzulässig ist.

Nachdem auf die betreffenden Schreiben Bezug genommen wurde, hat die Behörde, die das Bewerbungsverfahren über den Dienstweg praktizierte, davon Abstand genommen.

8.6 Weiterleitung von E-Mails bei Abwesenheit der Beschäftigten

Ein Beschäftigter einer saarländischen Kommune hat sich Anfang 2017 mit einer Eingabe an uns gewandt und sich darüber beschwert, dass die Kommune während seiner Abwesenheit ohne sein Wissen und ohne seine vorherige Zustimmung eine automatisierte Weiterleitung der E-Mails seines dienstlichen E-Mail-Accounts zum Account eines anderen Beschäftigten der Kommune veranlasst hatte. Da nicht auszuschließen war, dass auch E-Mails mit privatem Charakter von außen an den dienstlichen Account des Beschäftigten gesendet werden können, sah der Betroffene die automatisierte Weiterleitung als unrechtmäßig und somit als unzulässige Datenübermittlung an Unbefugte an. Darüber hinaus vermutete der Betroffene, dass man Einsicht in sein E-Mail-Konto genommen habe, um zu sehen, welche für die Weiterführung der dienstlichen Geschäfte erforderlichen Mails dort eingegangen seien.

Die Kommune erklärte hierauf in ihrer Stellungnahme, dass die private Nutzung des Accounts verboten sei und man wichtige dienstliche Informationen im Account des Beschäftigten vermutete. Zur Sicherstellung eines ordnungsgemäßen Dienstbetriebes sei nach Absprache mit dem behördlichen Datenschutzbeauftragten der Kommune das Mailkonto des Betroffenen in Gegenwart eines Mitgliedes des Personalrates und einer weiteren neutralen Person geöffnet und nach dienstlichen Informationen durchsucht worden. Mails mit rein privatem Charakter seien nicht vorgefunden worden. Da die Abwesenheit des Betroffenen immer noch andauere, habe man eine automatisierte Weiterleitung auf das Konto eines anderen Beschäftigten der Kommune eingerichtet.

Ausgehend von der rein dienstlich zulässigen Nutzung eines E-Mail-Kontos, darf der Arbeitgeber ein- und ausgehende E-Mails grundsätzlich zur Kenntnis nehmen.

Soweit vorliegend die Einsichtnahme als Ultima Ratio aufgrund dringend benötigter dienstlicher Informationen erforderlich war, wurde durch die Vorgehensweise der Gemeinde der Schutz der Persönlichkeitsrechte des Betroffenen dadurch hinreichend gewahrt, dass die Einsichtnahme unter Hinzuziehung eines Vertreters des Personalrates und einer weiteren neutralen Person erfolgt ist und solche E-Mails, die einen privaten Charakter erkennen ließen, nicht geöffnet wurden.

Die Einrichtung einer automatisierten Weiterleitung an einen anderen Beschäftigten stellte hingegen nicht das mildeste Mittel zur Regelung des E-Mail-Verkehrs für die

Zeit der Abwesenheit dar. Der Einrichtung eines Abwesenheitsassistenten ist in einem solchen Fall der Vorzug zu geben. Besondere Umstände, die eine Weiterleitung erforderlich erscheinen lassen, konnten uns darüber hinaus auch nicht dargelegt werden. Die betroffene Kommune hat ihr Vorgehen bei Abwesenheit von Beschäftigten unseren Vorgaben entsprechend datenschutzkonform angepasst.

Arbeitgeber und Dienstherrn sollten für den Fall der unerwarteten Abwesenheit seiner Beschäftigten durch Unfall, Krankheit oder sogar Tod klare Regelungen treffen, wie mit dem E-Mail-Account der Beschäftigten verfahren wird. Eine Anleitung hierzu kann der Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz entnommen werden. Die Orientierungshilfe ist in unserem Internetangebot hinterlegt.

8.7 Mitarbeiterfotos im Internet

Eine ehemalige Mitarbeiterin einer Arztpraxis wandte sich mit einer Beschwerde an uns, da ihr früherer Arbeitgeber auf seiner Praxishomepage noch immer ein Foto ihrer Person veröffentlichte und sie weiterhin als Mitarbeiterin der Praxis aufführte. Mehrere Versuche der Beschwerdeführerin, den Praxisinhaber dazu zu bewegen, das Foto auf seiner Praxishomepage zu löschen, blieben ergebnislos. Letztendlich sah sich die Mitarbeiterin aufgrund der Untätigkeit des ehemaligen Arbeitgebers dazu gezwungen, sich an die Aufsichtsbehörde zu wenden.

Derzeit besteht noch eine gewisse Rechtsunsicherheit, welche Rechtsnormen für die Veröffentlichung von Mitarbeiterfotos im Internet einschlägig sind. Neben den Vorgaben der Datenschutz-Grundverordnung (DSGVO) könnten in diesem Fall auch diejenigen des Kunsturhebergesetzes sowie die des § 26 Bundesdatenschutzgesetz (BDSG) zu beachten sein. Allen genannten Vorschriften ist jedoch gemein, dass eine Veröffentlichung entweder einer Einwilligung des Betroffenen oder eines überwiegenden Interesses des Arbeitgebers nach einer Abwägung zwischen seinen Interessen an einer Veröffentlichung der Mitarbeiterfotos und den gegenläufigen Interessen des Beschäftigten bedarf.

Soweit eine Veröffentlichung von Fotos auf eine Einwilligung des Mitarbeiters gestützt werden soll, ist zu beachten, dass eine Einwilligung im Beschäftigungsverhältnis an hohe gesetzliche Hürden geknüpft ist. Während die Einwilligung im Sinne der DSGVO grundsätzlich formfrei erteilt werden kann, sieht § 26 Abs. 2 S. 3 BDSG für Einwilligungen im Rahmen eines Beschäftigungsverhältnisses grundsätzlich die Schriftform vor. Darüber hinaus muss die Einwilligung bestimmt, informiert und freiwillig abgegeben werden. Für die Beurteilung der Freiwilligkeit sieht § 26 Abs. 2 BDSG vor, dass die in einem Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person berücksichtigt werden muss. Gemäß § 26 Abs. 2 S. 2 BDSG kann die Freiwilligkeit insbesondere dann vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und Beschäftigte ein gleichgelagertes Interesse verfolgen. Ausweislich der Gesetzesbegründung zu dieser Passage ist dies ausdrücklich der Fall für die Aufnahme von Fotos für das

betriebsinterne Intranet, weil hierbei ein betriebliches Zusammenwirken im Vordergrund stehe.

Da im vorliegenden Fall die Einwilligung der Beschäftigten zur Veröffentlichung ihres Fotos als Mitarbeiterin der Arztpraxis widerrufen wurde, kein Beschäftigungsverhältnis mehr bestand und keine Interessen des Praxisinhabers für eine weitere Veröffentlichung der Fotos geltend gemacht werden konnte, musste das Bild aufgrund fehlender Rechtsgrundlage zur Datenverarbeitung von der Praxishomepage entfernt werden. Dies wurde nach einem unsererseits erfolgten Anschreiben der Praxis auch umgehend veranlasst.

9 Datenschutzbeauftragte

9.1 Pflicht zur Benennung eines Datenschutzbeauftragten

Kaum eine Regelung der Datenschutz-Grundverordnung (DSGVO) hat rund um den Termin des Geltungseintritts im Mai 2018 für so große Unsicherheit gesorgt, wie die Benennungspflicht eines Datenschutzbeauftragten gemäß Art. 37 DSGVO in Verbindung mit § 38 Bundesdatenschutzgesetz n. F. (BDSG n. F.). Dabei sind diese Regelungen in weiten Teilen aus dem BDSG a. F. übernommen worden und schon seit Jahren geltendes Recht für Akteure wie Unternehmen und solche Vereine, die mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten betrauen. Auch die Regelung, dass die fehlende Bestellung eines Datenschutzbeauftragten bußgeldbewehrt ist, stellt keine Neuerung im deutschen Datenschutzrecht dar. Neu hingegen ist die Verpflichtung der verantwortlichen Stelle, der Aufsichtsbehörde die Kontaktdaten des Datenschutzbeauftragten mitzuteilen (Art. 37 Abs. 7 DSGVO). Aufgrund dieser Mitteilungspflicht hat unsere Dienststelle bis Ende 2018 ca. 2.200 Meldungen erhalten. Für die Meldungen wurde von unserer Dienststelle ein elektronisches Meldeportal zur Verfügung gestellt, das man über unseren Internetauftritt erreichen kann.

Um den Verantwortlichen mehr Rechtssicherheit bei der Anwendung der Regelungen zu geben, wurde von der Datenschutzkonferenz (DSK) das Kurzpapier Nr. 12 erstellt, das Ausführungen zur Bestellpflicht eines Datenschutzbeauftragten beinhaltet. Das Kurzpapier ist unserem Internetangebot zu entnehmen.

Trotzdem kommt es bei der Auslegung der Normen immer wieder zu Unsicherheiten, weil der Gesetzgeber unbestimmte Rechtsbegriffe verwendet hat, die der Auslegung bedürfen.

9.1.1 „Umfangreich“ im Sinne des Artikel 37 DSGVO

Art. 37 Abs.1 DSGVO besagt:

„(1) Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn

a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln,

*b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine **umfangreiche** regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder*

*c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der **umfangreichen** Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 besteht."*

Sowohl unter lit. b als auch lit. c der Norm wird der Begriff „umfangreich" verwendet. Wann genau eine umfangreiche Datenverarbeitung vorliegt, wird jedoch im Gesetzestext nicht genauer ausgeführt. Allerdings kann dem Erwägungsgrund 91 der DSGVO entnommen werden, welche Verarbeitungsvorgänge darunter subsumiert werden können. Dies können u. a. solche Verarbeitungen sein, die eine große Menge personenbezogener Daten oder eine große Zahl von Personen betreffen und die wahrscheinlich – beispielsweise aufgrund ihrer Sensibilität – ein hohes Risiko mit sich bringen sowie Verarbeitungsvorgänge, bei denen in großem Umfang neue Technologien eingesetzt werden oder solche, denen ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen immanent ist.

Bezüglich einer Datenverarbeitung durch Ärzte, Apotheker und sonstige Angehörige eines Gesundheitsberufes hat sich die DSK, vorbehaltlich einer anderslautenden Regelung durch den Europäischen Datenschutzausschuss (EDSA), im Beschluss vom 26. April 2018 derart geäußert, dass dann von einer umfangreichen Datenverarbeitung auszugehen ist, wenn mindestens zehn Beschäftigte mit der personenbezogenen Datenverarbeitung betraut sind [vgl. hierzu Kap. 9.2 (S. 90)]. Dieser Beschluss ist unserem Internetangebot zu entnehmen.

9.1.2 „Ständig" im Sinne des § 38 Abs.1 BDSG

Ergänzend zu Art. 37 DSGVO ist gemäß § 38 Abs.1 BDSG ein Datenschutzbeauftragter zu benennen, soweit in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Diese Regelung wurde auch aus den Vorschriften des BDSG a. F. übernommen. Ungeachtet dessen wird der Rechtsbegriff „ständig" auch jetzt unterschiedlich ausgelegt.

Im Saarland vertritt das Unabhängige Datenschutzzentrum die Auffassung, dass man sich auf die Kommentierung und Rechtsauslegung vor Wirksamwerden der DSGVO zum Rechtsbegriff „ständig" berufen kann. Demnach ist eine Person ständig mit der Datenverarbeitung beschäftigt, die auf unbestimmte Zeit mit der Verarbeitung personenbezogener Daten betraut ist. Dabei spielen weder die Arbeitszeit noch der Zeitpunkt der Aufgabenübertragung eine Rolle. Sowohl der gerade erst eingestellte Arbeitnehmer bzw. derjenige, der gerade erst mit der Datenverarbeitung beauftragt ist, als auch der Teilzeitbeschäftigte sind mit zu berücksichtigen, sofern nur das Beschäftigtsein mit der Datenverarbeitung auf unbestimmte Zeit gerichtet ist.[89]

[89] Vgl. *Linnenkohl*, Der betriebliche Beauftragte für den Datenschutz, NJW 1979, S. 1190 ff.; *Gola/ Schomerus*, in: Gola/Klug/Körffer, BDSG, 12. Aufl. (2015), § 4f Rn. 11.

9.1.3 Kann eine juristische Person zum Datenschutzbeauftragten benannt werden?

Zur Frage, ob eine juristische Person zum Datenschutzbeauftragten benannt werden darf oder nicht, existiert bislang noch keine gesicherte Rechtsansicht. Die DSGVO spricht in ihrer englischen Fassung im Zusammenhang mit dem Datenschutzbeauftragten wie folgt:

- Art. 38 Abs. 2 „(…) to maintain his or her expert knowledge"
- Art. 38 Abs. 3 S. 2 „(…) he or she shall not be dismissed"
- Art. 38 Abs. 5 u. Art. 39 Abs. 2 „his or her tasks"

Letzteres kann u. a. als Indiz dafür gewertet werden, dass das Rechtsregime der DSGVO für die Person des Datenschutzbeauftragten von einer natürlichen Person ausgeht und eine juristische Person nicht selbst als externer Datenschutzbeauftragter benannt werden kann.

Bis zu einer abschließenden Aussage des EDSA zu dieser Thematik können wir deshalb lediglich die Benennung einer natürlichen Person empfehlen.

9.1.4 Bestrebungen zur Aufweichung der Benennungspflicht

Gegen Ende des Berichtszeitraums haben die Ausschüsse für Innere Angelegenheiten und Wirtschaft des Bundesrates die Empfehlung ausgesprochen, die Verpflichtung für Unternehmen, ab zehn Mitarbeitern einen Datenschutzbeauftragten benennen zu müssen, entweder gänzlich abzuschaffen oder zumindest aufzuweichen. Konkret wurden folgende Änderungsvorschläge unterbreitet:

- Die komplette Streichung der besonderen Benennungspflicht nach BDSG in Deutschland.
- Die Beschränkung der Benennungspflicht auf Unternehmen, die Daten „zu gewerblichen Zwecken" verarbeiten.
- Die Anhebung der Grenze für die Benennungspflicht von zehn auf fünfzig Mitarbeiter.

Die Empfehlungen für den Bundesrat basieren möglicherweise auf der irrtümlichen Annahme, dass die Zehn-Personen-Grenze des § 38 BDSG Auswirkungen darauf hätte, ob überhaupt Maßnahmen zur DSGVO-Umsetzung durchgeführt werden müssten (z. B. Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten oder Erfüllung von Informationspflichten). Eine Streichung oder Anhebung der Grenze würde jedoch lediglich dazu führen, dass kein Datenschutzbeauftragter mehr benannt werden muss; die genannten Pflichten der DSGVO jedoch trotzdem, dann ohne Unterstützung durch den Datenschutzbeauftragten, erfüllt werden müssen.

Die Rolle des Datenschutzbeauftragten ist ein seit Jahrzehnten bewährtes datenschutzrechtliches Instrument in Deutschland. Der Datenschutzbeauftragte ist angesichts komplexer datenschutzrechtlicher Vorgaben und drohender Bußgelder als kompetenter Ansprechpartner und Berater wichtiger denn je. Es geht nicht um Bürokratie, sondern um Sicherheit für Unternehmen, Unternehmer, Kunden und Verbraucher. Mit einem kompetenten und geschulten Datenschutzbeauftragten kann ein Unternehmen, das datenschutzrechtlich gut aufgestellt ist, dies auch als Wettbewerbsvorteil nutzen. Ein Imageschaden durch Datenverluste kann schwerwiegende wirtschaftliche Auswirkungen mit sich bringen. Der Vertrauensverlust von Kunden ist fast nicht mehr zu revidieren.

Dies hat auch die Mehrheit der politisch Verantwortlichen so gesehen und den Plänen zur Aufweichung der Benennungspflicht zumindest vorerst eine Absage erteilt.

9.2 Datenschutzbeauftragter in der Arztpraxis

Im Hinblick auf die ab 25. Mai 2018 anzuwendende Datenschutz-Grundverordnung (DSGVO) haben sich im Berichtszeitraum zahlreiche saarländische Arztpraxen an das Unabhängige Datenschutzzentrum Saarland gewandt und um Beratung gebeten. Dabei trat besonders häufig die Fragestellung auf, unter welchen Voraussetzungen eine Arztpraxis einen Datenschutzbeauftragten (DSB) benennen muss.

Die Verpflichtung zur Benennung eines Datenschutzbeauftragten kann sich für den Verantwortlichen sowohl aus der DSGVO selbst als auch aus dem Bundesdatenschutzgesetz n. F. (BDSG n. F.) ergeben.

Art. 37 Abs. 1 lit. c DSGVO sieht eine Bestellpflicht unter anderem dann vor, wenn *„die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 besteht".* Zu den Daten gem. Art. 9 DSGVO zählen u. a. Gesundheitsdaten, die in einer Arztpraxis verarbeitet werden. Fraglich für die Arztpraxen war, wann die Datenverarbeitung als „umfangreich" anzusehen ist.

Bei der Auslegung dieses Begriffs kann Erwägungsgrund 91 zur DSGVO herangezogen werden, in dem es heißt: *„Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt."*

Sich daran orientierend hat die Datenschutzkonferenz (DSK) als Hilfestellung einen Beschluss gefasst, in dem die Pflicht zur Bestellung eines DSB für Arztpraxen und sonstige Gesundheitsberufe behandelt wird (siehe hierzu Anlage 17.12). Darin wird festgehalten, dass sowohl bei Einzelpraxen als auch bei Gemeinschaftspraxen in der Regel nicht von einer umfangreichen Datenverarbeitung im Sinne von Art. 37 Abs. 1 lit. c DSGVO auszugehen ist.

Allerdings kann sich dennoch eine Bestellpflicht ergeben, vor allem dann, wenn in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind. Diese ergibt sich dann aus § 38 Abs. 1 BDSG. Dabei ist zu beachten, dass nach Auffassung der DSK der Arzt bei der Personenzahl mit zu berücksichtigen ist.

Vorbehaltlich einer anderen Auslegung durch den Europäischen Datenschutzausschuss (EDSA) hat das Datenschutzzentrum Anfragen von Ärzten entsprechend den Ausführungen im DSK-Beschluss beantwortet.

9.3 Datenschutzbeauftragter in beliehenen Handwerksbetrieben

Eine der ersten Anforderungen, welche die Datenschutz-Grundverordnung (DSGVO) mit Geltungseintritt an die für die Datenverarbeitung verantwortlichen Stellen stellte, war die Benennung eines Datenschutzbeauftragten. Während die Benennungspflicht nichtöffentlicher Stellen gemäß Art. 37 Abs. 1 lit. b u. lit. c DSGVO, § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG) vor allem mit der Sensibilität und/oder dem Umfang der Datenverarbeitung steht und fällt, sind Behörden oder sonstige öffentliche Stellen gemäß Art. 37 Abs. 1 lit. a DSGVO in jedem Fall zur Benennung einer mit dem Datenschutz beauftragten Person verpflichtet, unabhängig davon, wie intensiv sich deren Verarbeitungstätigkeit tatsächlich gestaltet.

Eine Besonderheit nehmen hierbei diejenigen Berufsgruppen ein, welche zwar privatrechtlich organisiert sind und am freien Markt handwerklich-gewerbliche Dienstleistungen anbieten, die als Beliehene im Rahmen ihrer Berufsausübung jedoch zugleich auch staatliche hoheitliche Aufgaben wahrnehmen. Zu nennen sind hier das Schornsteinfegerwesen sowie diverse von Kfz-Werkstätten im Rahmen von Kfz-Betriebstauglichkeitsuntersuchungen angebotene Leistungen.

Die hieraus folgende berufliche „Doppelstellung" wirft aus datenschutzrechtlicher Sicht unweigerlich die Frage auf, ob sie eine Pflicht zur Benennung eines Datenschutzbeauftragten nach sich zieht und falls ja, wie weit diese Pflicht reicht.

Die Pflicht zur Benennung eines Datenschutzbeauftragten ist rechtlich durch zwei Gesetzeswerke normiert. Im Kern findet sich ihre Regelung auf europarechtlicher Ebene in Art. 37 DSGVO, aus dessen Abs. 1 lit. a die vorweg bereits beschriebene Ernennungspflicht für Behörden und öffentliche Stellen zu entnehmen ist. Für die nicht öffentlichen Verantwortlichen findet sich die Pflicht in Art. 37 Abs. 1 lit. b und c DSGVO. Im Gegensatz zu der obligatorischen Benennungspflicht für öffentliche Stellen knüpfen letztgenannte Regelungen indes an besondere Verarbeitungssituationen an, gelten demnach nicht uneingeschränkt für jeden Verantwortlichen. Erfasst werden von ihnen nur solche Datenverarbeitungen, welche es aufgrund ihrer besonderen Merkmale erforderlich machen, dass eine erfahrene und weisungsfreie Person über sie wacht. Sowohl Art. 37 Abs. 1 lit. b als auch lit. c DSGVO verfolgen dabei einen

risikobasierten Ansatz, welcher darauf abstellt, wie sensibel und kritisch sich die Verarbeitungstätigkeit darstellt und welche Gefahren sich aus ihr für die betroffenen Personen ergeben können.[90]

Die Vorschrift des § 38 BDSG flankiert die Benennungspflicht für nicht-öffentliche Stellen sodann auf nationaler Ebene und erweitert sie zugleich. Ergänzend zu Art. 37 Abs. 1 lit. b und c DSGVO benennt der Verantwortliche hiernach einen Datenschutzbeauftragten soweit in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt werden oder – unabhängig von der Beschäftigtenanzahl – wenn Verarbeitungen vorgenommen werden, welche einer Datenschutzfolgenabschätzung nach Art. 35 DSGVO unterliegen.

Hinsichtlich der eingangs genannten Berufsgruppen vertritt das Unabhängige Datenschutzzentrum Saarland nachfolgende Rechtsansicht.

Auch nach der Novellierung des Schornsteinfeger-Handwerksgesetzes (SchfHwG) im Jahre 2008[91] ist das Schornsteinfegerwesen in der Bundesrepublik Deutschland nicht vollständig liberalisiert. Zwar ist das sog. Kehrmonopol des Staates in großen Teilen gelockert worden, so dass es den Grundstückseigentümern nunmehr offen steht, einige Wartungsaufgaben an ihren Heizungsanlagen einem Schornsteinfeger ihrer Wahl zu übertragen. Bestimmte Tätigkeiten sind jedoch nach wie vor den bevollmächtigten Bezirksschornsteinfegern vorbehalten (Bsp. Feuerstättenschau), welche hierbei als Beliehene hoheitliche Tätigkeiten wahrnehmen (§ 8 i. V. m. §§ 14 ff. SchfHwG).

Im Rahmen dieser Tätigkeit sind bevollmächtigte Bezirksschornsteinfeger Verantwortliche i. S. d. Art. 4 Nr. 7 DSGVO, § 2 Abs. 1 S. 3 SDSG und unterliegen der Pflicht, einen behördlichen Datenschutzbeauftragten nach Art. 37 Abs. 1 lit. a DSGVO zu benennen.

Vorgenanntes gilt in gleichem Maße für privatunternehmerisch tätige Autowerkstätten, welche als gemäß Nr. 1.1 Anlage VIII c Straßenverkehrs-Zulassungs-Ordnung (StVZO)[92] anerkannte „AU-Werkstätten" neben den „üblichen" Werkleistungen spezielle Abgasuntersuchungen anbieten. Hierbei handelt es sich um solche Abgasuntersuchungen, welche gemäß Nr. 3.1.1.1 Anlage VIII StVZO einen eigenständigen Bestandteil der andernfalls durch einen anerkannten Prüfingenieur (z. B. TÜV, Dekra, KÜS, GTÜ) durchgeführten Hauptuntersuchung (HU) bilden. Soweit derartige Leistungen erbracht werden, handeln die Kfz-Werkstätten im Rahmen hoheitlicher Aufgaben und sind öffentliche Stellen i. S. d. § 2 Abs. 4 S. 2 BDSG, § 2 Abs. 1 S. 3 SDSG, was eine Bestellungspflicht nach Art. 37 Abs.1 lit. a DSGVO nach sich zieht.

Obgleich von Gesetzes wegen in beiden vorgenannten Konstellationen demnach kein Weg an der Benennung einer sich speziell mit dem Datenschutz befassenden Person vorbeiführt, wird von hiesiger Seite nicht verkannt, dass gerade die Durchführung von Abgasuntersuchungen als Teiluntersuchung zur Hauptuntersuchung

---

[90] *Drewes*, in: Simitis/Hornung/Spiecker, Datenschutzrecht (2018), Art. 37 Rn. 12.

[91] Gesetz über das Berufsrecht und die Versorgung im Schornsteinfegerhandwerk v. 26.11.2008 (BGBl. I S. 2242), zuletzt geändert d. Gesetz v. 17.7.2017 (BGBl. I S. 2495).

[92] Straßenverkehrs-Zulassungs-Ordnung vom 26.4.2012 (BGBl. I S. 679), zuletzt geändert d. Verordnung v. 20.10.2017 (BGBl. I S. 3723).

nur einen Bruchteil der übrigen Werkstattarbeiten ausmachen dürfte und gerade kleinere Betriebe von der Pflicht zur Bestellung eines eigenen Datenschutzbeauftragten oftmals strukturell wie finanziell überfordert sein dürften. Gleiches gilt für die meisten Schornsteinfegerbetriebe, denen hierzu oftmals nicht die personellen Ressourcen zur Verfügung stehen dürften.

In der Bestellung gemeinsamer Datenschutzbeauftragter nach Art. 37 Abs. 3 DSGVO, etwa durch die jeweiligen Berufsinnungen, sehen wir einen praktikablen Weg, den gesetzlichen Verpflichtungen nachzukommen. Hierbei ist jedoch der Größe und Organisationsstruktur der jeweiligen Stellen Beachtung zu schenken und gegebenenfalls sind mehrere Personen mit dem Datenschutz zu betrauen.

10 Gesundheit und Soziales

10.1 Datenschutz in der Arztpraxis

Im zeitlichen Zusammenhang mit dem Wirksamwerden der Datenschutz-Grundverordnung (DSGVO) erreichten das Unabhängige Datenschutzzentrum Saarland zahlreiche Anfragen von Ärzten und Patienten. Gerade im Gesundheitsbereich, wo regelmäßig besonders sensible Daten verarbeitet werden, war eine große Verunsicherung im Hinblick auf die Anwendung der DSGVO wahrzunehmen.

So kam die Befürchtung auf, man dürfe Patienten im Wartezimmer nicht mehr mit ihrem Namen aufrufen. Nach Auffassung des Datenschutzzentrums geht eine derartige Auslegung der DSGVO im Regelfall zu weit. Das Ansprechen der Patienten mit Namen verstößt aus unserer Sicht weder gegen datenschutzrechtliche Vorgaben noch gegen die ärztliche Schweigepflicht; diese gelebte Praxis gehört zum normalen Umgang zwischen Arzt und Patient. Dennoch sollte auch hier mit der nötigen Sensibilität verfahren werden und ggf. in einzelnen Fällen, wie beispielsweise in besonders sensiblen medizinischen Fachbereichen oder bei besonderen räumlichen Gegebenheiten, auf einen namentlichen Aufruf verzichtet werden. Auch sind entgegenstehende Wünsche der Patienten zu berücksichtigen.

Datenschutzrechtlich ohne Zweifel unzulässig ist es hingegen, im Empfangs- oder Wartebereich von Arztpraxen Diagnosen im Beisein anderer Patienten zu erörtern.

Mehrfach wurde die Frage aufgeworfen, in welcher Form eine Arztpraxis ihren Informationspflichten nach Art. 13 DSGVO nachkommen muss.

Art. 13 DSGVO sieht vor, dass jeder Verantwortliche der betroffenen Person zum Zeitpunkt der Datenerhebung spezifische Informationen zur Verfügung stellen muss. Dazu gehören unter anderem Name und Kontaktdaten der verantwortlichen Stelle, Kontaktdaten des Datenschutzbeauftragten (soweit vorhanden) und die Zwecke der Verarbeitung.

Zur Erfüllung dieser Pflichten kommen das Aushändigen eines Informationsblattes, ein Aushang in den Räumlichkeiten der Praxis oder ggf. ein Hinweis auf die Datenschutzerklärung auf der Internetseite der Praxis in Frage.

Zum Teil wurden Patienten aufgefordert, die Kenntnisnahme der bereitgestellten Informationen mit ihrer Unterschrift zu bestätigen. Aus anderen Bundesländern wurden Fälle bekannt, in denen bei Verweigerung der Unterschrift gar die Behandlung verwehrt wurde. Daraufhin sah sich die Datenschutzkonferenz veranlasst, diesbezüglich eine Klarstellung vorzunehmen. So heißt es im Beschluss vom 5. September 2018:

„Die Informationspflicht nach Art. 13 DSGVO bezweckt lediglich, dass der Patientin bzw. dem Patienten die Gelegenheit gegeben wird, die entsprechenden Informationen einfach und ohne Umwege zu erhalten. Sie oder er muss diese jedoch nicht zur Kenntnis nehmen, wenn sie oder er dies nicht möchte. Um seinen Nachweispflichten gegenüber der Aufsichtsbehörde nachzukommen, kann der Verantwortliche das

Aushändigen der Information vermerken oder einen konkreten Verfahrensablauf betreffend die Umsetzung der Informationspflicht dokumentieren, aus dem hervorgeht, wie die Patientin oder der Patient die Informationen im Regelfall erhält."

Unsere Dienststelle berät Arztpraxen dahingehend, dass das Aushändigen eines Informationsblattes beim erstmaligen Besuch der Praxis in Verbindung mit einem entsprechenden Vermerk in der Akte ausreichend ist.

10.2 Auskunftsanspruch gegenüber einem Krankenhaus

In einer Anfrage an unsere Dienststelle bat ein Bürger um unsere Einschätzung dazu, in welcher Form und in welchem Umfang ein Patient seinen Anspruch auf Auskunft über seine personenbezogenen Daten und Einsicht in seine Behandlungsunterlagen gegenüber einem Krankenhaus geltend machen kann. Im Laufe der Sachverhaltsaufklärung stellte sich heraus, dass es um ein konkretes Auskunftsersuchen gegenüber einer saarländischen Klinik ging. Der Beschwerdeführer beklagte sich zum einen darüber, dass seinem Auskunftsbegehren (noch) nicht vollständig nachgekommen worden sei. Zum anderen wurden ihm für die bereitgestellten Unterlagen Kosten in Rechnung gestellt, obwohl sich seiner Auffassung nach aus den gesetzlichen Vorgaben ein Anspruch auf Kostenfreiheit ergebe.

Hier hat sich zunächst die Frage nach der einschlägigen Rechtsgrundlage für das Auskunftsersuchen gestellt. Der Beschwerdeführer hatte zu Beginn auf § 34 Abs. 1 Bundesdatenschutzgesetz a. F. (BDSG a. F.) verwiesen. Diese Vorschrift war hier jedoch nicht anzuwenden. Stattdessen kamen § 13 Saarländisches Krankenhausgesetz (SKHG)[93] und § 630g Bürgerliches Gesetzbuch (BGB)[94] als Anspruchsgrundlagen in Betracht. Beide Vorschriften sind spezialgesetzliche Regelungen und gehen der Anwendung des Bundes- und Landesdatenschutzgesetzes vor. § 630g BGB normiert die vertragliche Verpflichtung zur Gewährung des Einsichtsrechts für Behandlungsverträge und besteht für Patienten zusätzlich neben dem datenschutzrechtlichen Anspruch aus § 13 SKHG.

§ 13 Abs. 7 SKHG sieht vor, dass Patienten kostenfreie Auskunft über die gespeicherten personenbezogenen Daten und Einsicht in die Behandlungsdokumentation verlangen können. Daraus ergibt sich, dass Auskunftsersuchen, die sich auf Grundlage dieser Vorschrift an saarländische Krankenhäuser richten, im Hinblick auf alle medizinischen Daten kostenfrei zu beantworten sind. Dies gilt auch für die Auskunft über Daten, die von der Krankenhausverwaltung verarbeitet worden sind. Das Krankenhaus kann sich diesbezüglich nicht auf § 630g BGB berufen und nach dieser Vorschrift Gebühren für das Erteilen der Auskunft erheben.

Im vorliegenden Fall war von einem Auskunftsersuchen nach § 13 Abs. 7 SKHG auszugehen. Dem stimmte auch die betroffene Klinik auf Nachfrage zu und teilte mit,

---

[93] Saarländisches Krankenhausgesetz vom 6.11.2015 (Amtsbl. I S. 857), zuletzt geändert d. Gesetz v. 22.8.2018 (Amtsbl. I S. 674).

[94] In der Fassung der Bekanntmachung vom 2.1.2002 (BGBl. I S. 42, ber. S. 2909 u. 2003 I S. 738), zuletzt geändert d. Gesetz v. 31.1.2019 (BGBl. I S. 54).

dass die zunächst festgesetzte Gebühr für die Erteilung der Auskunft wieder zurückgenommen worden sei. Auch seien die zunächst noch fehlenden Auskünfte zwischenzeitlich erteilt worden.

Nachdem somit der konkrete Auskunftsanspruch des Beschwerdeführers vollständig und kostenfrei erfüllt war, forderte er vom Krankenhaus eine allgemeine Aussage dazu, wie Begehren nach Auskunft und Einsicht dort zukünftig umgesetzt würden. Die Klinik teilte daraufhin mit, dass man sich vorbehalte, je nach Einzelfall unter Berücksichtigung der einschlägigen rechtlichen Grundlagen eine Entscheidung zu treffen. Dies war aus Sicht des Unabhängigen Datenschutzzentrums Saarland nicht zu beanstanden.

10.3 Krankengeldfallmanagement bei gesetzlichen Krankenkassen

Im Berichtszeitraum erhielt unsere Dienststelle eine Eingabe, in der sich ein Versicherter über das Vorgehen seiner gesetzlichen Krankenkasse im Zusammenhang mit der Zahlung von Krankengeld beschwerte. Er war der Auffassung, dass insbesondere die Aufgabentrennung zwischen Krankenkasse und Medizinischem Dienst der Krankenversicherungen (MDK) im Hinblick auf die Datenerhebung nicht hinreichend beachtet werde und die Kasse von den Versicherten Unterlagen anfordere, die nur für den MDK bestimmt seien. In der Vergangenheit waren bereits ähnliche Eingaben zu verzeichnen, in denen sich Versicherte auch darüber beschwerten, dass die Krankenkasse sie wiederholt telefonisch kontaktiert habe und sie sich durch häufige Nachfragen zu ihrem Gesundheitszustand unter Druck gesetzt fühlten.

Wir nahmen daher die aktuelle Beschwerde zum Anlass, das Krankengeldfallmanagement der betreffenden Krankenkasse näher zu untersuchen. In einem Vor-Ort-Termin ließen wir uns die internen Abläufe erläutern. Stichprobenhaft nahmen wir Einsicht in Fallakten und führten ein Gespräch mit einer Sachbearbeiterin der zuständigen Abteilung.

In den Akten waren zum Teil Unterlagen vorhanden, die nach unserer Auffassung für die Aufgabenerfüllung der Krankenkasse nicht zwingend erforderlich sind. Die Krankenkasse führte dazu aus, dass Versicherte häufig auch unaufgefordert Dokumente übersenden würden. Es wurde vereinbart, dass diese mit entsprechender Kennzeichnung aufbewahrt werden dürfen, soweit sie für den aktuellen Leistungsfall relevant sind. In diesem Zusammenhang wurde auch die im Fünften Buch Sozialgesetzbuch (SGB V)[95] verankerte Aufgabentrennung zwischen der Krankenkasse und dem MDK erörtert. Demnach darf die Krankenkasse grundsätzlich nur die Daten erheben, die für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind (§ 284 SGB V). Eine darüber hinaus gehende Datenerhebung kann zulässig sein, wenn ein Versicherter seinen Anspruch auf individuelle Beratung und Hilfestellung nach § 44 Abs. 4 SGB V

[95] Vom 20.12.1988 (BGBl. I S. 2477), zuletzt geändert d. Gesetz v. 11.12.2018 (BGBl. I S. 2394).

wahrnehmen möchte. In diesem Fall ist allerdings zunächst eine schriftliche Einwilligung des Versicherten einzuholen.

Für die telefonische Kontaktaufnahme existieren bei der Krankenkasse interne Arbeitshilfen, die sehr umfangreiche Fragenkataloge enthalten. In diesem Zusammenhang wurde klargestellt, dass beim telefonischen Erstkontakt die Fragen an den Versicherten auf das zu begrenzen sind, was für die originäre Aufgabenerfüllung erforderlich ist. Weitergehende Fragen dürfen erst gestellt werden, wenn eine Einwilligung zum Verfahren nach § 44 Abs. 4 SGB V vorliegt.

Daneben wurden mit der Krankenkasse Verbesserungsvorschläge für die verwendeten Vordrucke (Einwilligung, Schweigepflichtentbindungserklärung) erläutert. Wichtig ist hierbei der Hinweis, dass die Einwilligung stets freiwillig erfolgt und jederzeit für die Zukunft widerrufen werden kann.

So konnte in Kooperation mit der Kasse erreicht werden, dass im Krankengeldfallmanagement die datenschutzrechtlichen Bestimmungen besser umgesetzt werden.

10.4 Kopieren des Personalausweises in einer Bereitschaftsdienstpraxis

Ein immer wiederkehrendes Thema für das Unabhängige Datenschutzzentrum Saarland ist die datenschutzrechtliche Zulässigkeit des Anfertigens von Ausweiskopien.

Im Berichtszeitraum wandte sich ein Bürger an unsere Dienststelle, der beim Aufsuchen einer Bereitschaftsdienstpraxis aufgefordert wurde, eine Kopie seines Personalausweises anfertigen zu lassen. Die Mitarbeiterin der Praxis habe ihm auf Nachfrage mitgeteilt, dass die Kassenärztliche Vereinigung eine Ausweiskopie fordere.

Ein grundsätzliches Verbot, Ausweisdokumente zu kopieren, besteht seit mehreren Jahren nicht mehr. Ein solches Verbot findet sich weder im Personalausweisgesetz noch in der Personalausweisverordnung. Beim Anfertigen der Kopie handelt es sich aber um eine Datenerhebung, die einer rechtlichen Grundlage bedarf.

Für die Bereitschaftsdienstpraxis, bei der es sich um einen Patientenservice der Kassenärztlichen Vereinigung Saarland (Körperschaft des öffentlichen Rechts) und der niedergelassenen Ärzte handelt, war zum Zeitpunkt der Eingabe – mangels einer fachspezifischen Regelung – § 12 Abs. 1 Saarländisches Datenschutzgesetz a. F. (SDSG a. F.) einschlägig. Danach galt, dass das Erheben personenbezogener Daten nur zulässig ist, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist.

Von einer Erforderlichkeit für das Kopieren des Ausweises durch die Praxis war im vorliegenden Fall jedoch nicht auszugehen. Ein Vermerk in der Patientenakte über die Vorlage des Personalausweises hätte zur Identifizierung ohne weiteres genügt. Diese Auffassung teilte auch die um Stellungnahme gebetene Kassenärztliche Vereinigung, die davon ausging, dass es sich hier um einen Einzelfall gehandelt hatte. Dennoch wurde zugesagt, die Praxen noch einmal für die Thematik zu sensibilisieren.

Weitere Beschwerden oder Eingaben diesbezüglich waren seither nicht mehr zu verzeichnen.

10.5 Telemedizin im Rettungswesen: Datenübertragung von der Notfallstelle zum Krankenhaus

Telemedizin ist ein Sammelbegriff für verschiedenartige Versorgungskonzepte im Gesundheitswesen, bei denen medizinische Leistungen der Gesundheitsversorgung in den Bereichen Diagnostik, Therapie und Rehabilitation sowie bei der ärztlichen Konsultation über räumliche (oder auch zeitliche) Distanz hinweg erbracht werden. Hierfür werden Informations- und Kommunikationstechnologien eingesetzt. Ziel der Telemedizin ist unter anderem die Verbesserung von Qualität und Zugänglichkeit der medizinischen Versorgung und die Schaffung effizienter und benutzerfreundlicher elektronischer Gesundheitsdienste.

Im September 2018 hatte sich der Landtag des Saarlandes in einer Anhörung mit dem aktuellen Stand der Telemedizin im Saarland beschäftigt. Da bei der Anwendung solcher Technologien sehr sensible und daher besonders schutzwürdige Daten von Patienten übermittelt werden, spielt der Datenschutz in diesem Bereich eine wichtige Rolle, so dass auch die Landesbeauftragte für Datenschutz und Informationsfreiheit zur Anhörung eingeladen war. In ihrer Stellungnahme wies sie auf die speziellen gesetzlichen Vorgaben für den Umgang mit Gesundheitsdaten hin.

Als Beispiel für ein saarländisches Projekt aus dem Bereich Telemedizin, das im Berichtszeitraum durch das Unabhängige Datenschutzzentrum Saarland begleitet wurde, führte die Landesbeauftragte die Datenübertragung zwischen Rettungswagen und aufnehmendem Krankenhaus an, die eine bessere Erstversorgung eingelieferter Patienten bezweckt.

Im Rahmen der federführend vom saarländischen Ministerium für Soziales, Gesundheit, Frauen und Familie durchgeführten Studie „Myokardinfarktregister Saarland“ wurde als zentrale Maßnahme die EKG-Übermittlung durch den Zweckverband für Rettungsdienst und Feuerwehralarmierung Saar (ZRF) bereits von der Notfallstelle an die saarländischen Herzkatheter-Kliniken beschlossen. In der Optimierung dieser Schnittstelle zwischen Rettungsdienst und Klinik wurde eine wichtige Möglichkeit zur Verbesserung der Versorgung von Herzinfarktpatienten gesehen. So kann durch eine detaillierte Vorinformation leichter die richtige Zielklinik festgelegt werden, und diese kann sich frühzeitig und effektiver auf den Patienten vorbereiten. Zudem kann der vor Ort behandelnde Notarzt durch die Klinik unterstützt und beraten werden.

Bereits im Vorfeld hatte der ZRF alle Rettungswagen und Notarzt-Einsatzfahrzeuge im Saarland mit Defibrillator-Monitor-Einheiten („corpuls3“) ausgestattet, die das Notfallteam in der Diagnostik vor Ort unterstützen. Nach Ergänzung um entsprechende Hard- und Software besteht mit diesen Einheiten die Möglichkeit der Datenübertragung an einen zentralen Server.

Der Ablauf des Verfahrens sieht so aus, dass nach Aufzeichnung eines EKGs am Notfallort das Rettungsteam aus einem „Telefonbuch" des corpuls3 verschiedene Zieladressen (Namen der Krankenhäuser) auswählen kann, an die das EKG versendet werden soll. Die Datenübertragung erfolgt dann über den Server der Integrierten Leitstelle des ZRF zur jeweiligen Klinik. Das EKG wird in Form eines PDF-Dokuments als E-Mail-Anhang an eine durch das Krankenhaus vorgegebene E-Mail-Adresse übermittelt, begleitet von einem Telefonanruf in der Klinik, durch den der Patient angekündigt und auf die E-Mail hingewiesen wird.

Für diese Datenübertragung mittels Telemetrie hat der Gesetzgeber im Zuge der Novellierung des Saarländischen Rettungsdienstgesetzes (SRettG)[96] mit § 21 Abs. 5 eine ausdrückliche Ermächtigungsgrundlage geschaffen: *„Positions- und Telemetriedaten von Rettungsdienstfahrzeugen dürfen zur Integrierten Leitstelle des Saarlandes übermittelt und dort zur Unterstützung der Dispositionsentscheidung, zur Einsatzüberwachung und zur Dokumentation verwendet werden."* Das neue SRettG ist im August 2018 in Kraft getreten.

Es bestand Einigkeit darüber, dass die datenschutzrechtliche Verantwortung mit Übermittlung des EKG vom ZRF an die Klinik übergeht. Ab diesem Zeitpunkt finden die Regelungen zum Schutz von Patientendaten nach dem Saarländischen Krankenhausgesetz (SKHG) Anwendung.

Nachdem die rechtlichen und auch technischen Voraussetzungen erfüllt waren, bestanden von Seiten unserer Dienststelle keine Bedenken gegen die Einführung des Verfahrens, so dass der Echtbetrieb in 2018 aufgenommen wurde.

10.6 Versand von Arztrechnungen mittels E-Post

In der Vergangenheit hatte sich unsere Dienststelle bereits mehrfach zu den datenschutzrechtlichen Aspekten des Outsourcings von Druck, Adressierung und Kuvertierung behördlicher Schreiben geäußert (siehe auch Kap. 4.1). Im aktuellen Berichtszeitraum gingen in diesem Zusammenhang Eingaben bzw. Anfragen beim Unabhängigen Datenschutzzentrum Saarland ein, die die Nutzung von E-Post-Verfahren durch private Stellen im Gesundheitsbereich zum Thema hatten.

Konkret ging es dabei um die Frage, unter welchen Voraussetzungen das von der Deutschen Post AG angebotene E-Post-System für den Versand von Arztrechnungen genutzt werden kann. Bei diesem Verfahren prüft die Deutsche Post AG zunächst, ob der Empfänger am E-Post-System teilnimmt. Ist dies der Fall, erfolgt die Zustellung auf elektronischem Weg an das E-Mail-Postfach des Empfängers. Andernfalls übernimmt die Deutsche Post E-POST Solutions GmbH Ausdruck, Adressierung und Kuvertierung des E-Post-Briefes und stellt ihn auf klassischem Weg postalisch zu.

Durch die Eingabe eines Patienten wurden wir darauf aufmerksam gemacht, dass eine im Saarland ansässige Abrechnungsstelle für Ärzte das E-Post-Verfahren zum

[96] Vom 13.1.2004 (Amtsbl. S. 170), zuletzt geändert d. Gesetz v. 22.8.2018 (Amtsbl. I S. 674).

Versand von Arztrechnungen nutzt. Hierbei hat sich neben der Frage nach der datenschutzrechtlichen Zulässigkeit auch die Frage nach der Vereinbarkeit mit den Vorgaben zur ärztlichen Schweigepflicht (Berufsgeheimnis nach § 203 StGB) gestellt.

Zunächst wurde festgestellt, dass zwischen der betreffenden Abrechnungsstelle und der Deutschen Post AG eine Vereinbarung zur Auftragsdatenverarbeitung gem. § 11 Bundesdatenschutzgesetz a. F. (BDSG a. F.) über die Nutzung des E-Postbriefes mit elektronischer Zustellung vorlag. Für die Nutzung des E-Postbriefes mit klassischer Zustellung bestand ein Untervertrag der Deutschen Post AG mit der Deutsche Post E-POST Solutions GmbH.

Unabhängig von dem Erfordernis einer wirksamen Auftragsdatenverarbeitung war für die Zulässigkeit dieser Form der Zustellung eine Entbindung von der ärztlichen Schweigepflicht durch den betroffenen Patienten notwendig. Zwar wurde uns bestätigt, dass die Ärzte, die die Dienstleistung der Abrechnungsstelle in Anspruch nehmen, hierfür eine Einwilligung des Patienten einholen. Diese bezog sich jedoch nur auf die Weitergabe der Daten an die Abrechnungsstelle für Zwecke der Abrechnung. Den Patienten war nicht bewusst, dass zusätzlich eine Einbindung der Deutschen Post AG bzw. der Deutsche Post E-POST Solutions GmbH erfolgt.

Wir haben der Abrechnungsfirma mitgeteilt, dass wir die Nutzung des E-Post-Verfahrens unter diesen Voraussetzungen als unzulässig ansehen, weil durch die Datenweitergabe ohne ausdrückliche Einwilligung des Patienten gegen die ärztliche Schweigepflicht verstoßen wird. Diese hat daraufhin die verwendeten Einverständniserklärungen um einen Passus erweitert, in dem es ausdrücklich um die Einwilligung zum E-Post-Verfahren geht. Der Patient konnte nunmehr frei entscheiden, ob er mit der Einbindung der Deutschen Post AG bzw. Deutsche Post E-POST Solutions GmbH einverstanden ist. Danach bestanden keine grundsätzlichen datenschutzrechtlichen Bedenken mehr gegen den Einsatz des Verfahrens.

Im Rahmen weiterer Eingaben bzw. Anfragen zur Nutzung von E-Post haben wir ebenfalls darauf hingewiesen, dass bei Einwilligung bzw. Abgabe der Einverständniserklärung für den Patienten transparent sein muss, dass neben der Abrechnungsstelle auch die Deutsche Post AG bzw. die Deutsche Post E-POST Solutions GmbH eingebunden werden soll. Zudem kann eine Einwilligung nur auf freiwilliger Basis erfolgen, d. h. der Patient muss auf die Möglichkeit hingewiesen werden, dass die Abrechnungsfirma seine Rechnungen selbst erstellt und versendet, wenn er keine Einverständniserklärung abgibt.

10.7 Vernichtung von Dokumenten

Im Rahmen einer anonymen Eingabe wurde dem Unabhängigen Datenschutzzentrum Saarland vorgetragen, dass ein im Saarland ansässiger privater Pflegedienst sensible Unterlagen mit Informationen über Mitarbeiter und betreute Patienten über die „Blaue Tonne“ entsorge, so dass ein unberechtigter Zugriff durch Dritte auf die Dokumente nicht auszuschließen sei.

Zu den Grundsätzen der Verarbeitung personenbezogener Daten gehört es, geeignete technische und organisatorische Maßnahmen zum Schutz vor unbefugtem Zugriff zu treffen. Dies spielt gerade bei der Vernichtung bzw. Entsorgung von Unterlagen eine wichtige Rolle.

Vorgaben zur datenschutzgerechten Entsorgung finden sich in der Norm ISO/IEC 27001. Diese spezifiziert die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung des Kontexts einer Organisation. Hierin sind Regelungen zu Geräten und Betriebsmitteln im Hinblick auf eine sichere Entsorgung enthalten.

Der betroffene Pflegedienst konnte auf Nachfrage unserer Dienststelle belegen, dass mit der Aktenvernichtung ein hierauf spezialisierter, TÜV-zertifizierter Dienstleister beauftragt ist und somit Bedenken hinsichtlich unsachgemäßer Entsorgung ausräumen

10.8 Veröffentlichung von Daten und Fotos der Bewohner eines Seniorenheims

Im Berichtszeitraum erhielt das Unabhängige Datenschutzzentrum Saarland die Anfrage einer Senioreneinrichtung, ob es erlaubt sei, Namen, Geburtsdaten und Fotos von Bewohnern in der Einrichtung auszuhängen, z. B. für einen „Geburtstagsbaum".

Es ist davon auszugehen, dass dem Pflegepersonal die Daten der Bewohner in der Regel bereits bekannt sind, zumindest in dem Umfang, wie es für die Aufgabenerfüllung der Pflegekräfte erforderlich ist. Bei einem Aushang werden die Daten allerdings auch anderen Bewohnern offenbart sowie Personen, die beispielsweise Angehörige besuchen und die keinen Bezug zu den übrigen Patienten in der Einrichtung haben.

Beim Aushang von Fotos mit Namen und Geburtsdaten handelt es sich somit aus datenschutzrechtlicher Sicht um eine Datenübermittlung an Dritte, für die entweder eine rechtliche Grundlage vorliegen muss oder eine Einwilligung einzuholen ist. Eine Rechtsgrundlage existiert nicht, so dass nur der Weg über eine Einwilligung bleibt.

Das Seniorenheim wurde daher darüber informiert, dass ein Aushang nur mit Einverständnis der Betroffenen oder ggf. deren gesetzlicher Vertreter zulässig ist.

10.9 Verletzung des Briefgeheimnisses durch ein Jobcenter

Eine Bürgerin wandte sich im Berichtszeitraum an unsere Dienststelle und beschwerte sich darüber, dass ein saarländisches Jobcenter – ihrer Auffassung nach zum wiederholten Mal – gegen das Briefgeheimnis verstoßen habe. Sie habe von dort ein unverschlossenes Kuvert erhalten.

Beim händischen Versand von Poststücken lassen sich Fehler durch menschliche Unachtsamkeit nie ganz ausschließen. Die verantwortliche Stelle hat aber durch geeignete technische und organisatorische Maßnahmen dafür Sorge zu tragen, dass solche Fehler soweit wie möglich vermieden werden.

Wir haben die Beschwerde zum Anlass genommen, das Thema Briefversand bei einem Vor-Ort-Termin im betroffenen Jobcenter zusammen mit anderen datenschutzrechtlichen Problematiken anzusprechen. Eine letztendliche Aufklärung im konkreten Fall der Beschwerdeführerin, wie das Kuvert offen zur Beschwerdeführerin gelangen konnte, war nicht möglich. Die Verantwortlichen haben jedoch zugesichert, die Mitarbeiter nochmals auf die erforderliche Sorgfalt beim Postversand hinzuweisen. Als zusätzliche Maßnahme sollen wenn nötig Klebestreifen eingesetzt werden, um ein ungewolltes Öffnen von Briefumschlägen während der Postzustellung zu verhindern.

Es war davon auszugehen, dass es sich bei dem geöffneten Kuvert um einen Einzelfall handelte; für das Vorliegen eines generellen organisatorischen Problems im Jobcenter gab es keine Anhaltspunkte.

11 Schule und Bildung

11.1 Schulworkshops an Grundschulen und weiterführenden Schulen

Bereits seit dem Schuljahr 2013/2014 bietet das Unabhängige Datenschutzzentrum Saarland mit großem Erfolg an weiterführenden Schulen kostenlose Schülerworkshops zum Umgang mit persönlichen Daten im Internet an. Mittlerweile wurden im Saarland allein an weiterführenden Schulen über 10.000 Schülerinnen und Schüler in den Workshops im Zusammenhang mit der Nutzung von Social Media-Angeboten wie WhatsApp, Snapchat, Instagram, Facebook oder Twitter zu mehr Selbstverantwortung und digitaler Rücksichtnahme angeleitet.

Im Januar 2017 haben wir unser Angebot für Schulworkshops im Saarland um Workshops für Schüler der vierten Klassenstufe an saarländischen Grundschulen ergänzt.

Immer früher nutzen Kinder und Jugendliche die Möglichkeiten digitaler Medien, sei es per PC, Tablet oder Smartphone. Die digitale Medienkompetenz stellt nach dem Lesen, Schreiben und Rechnen die vierte Kulturtechnik dar, die zunehmend an Bedeutung gewinnt. Vor diesem Hintergrund wurde von Eltern und Lehrern angeregt, bereits in der vierten Klassenstufe der Grundschulen eine Informationsveranstaltung für Schülerinnen und Schüler zum richtigen Umgang mit digitalen Medien anzubieten.

Ziel der Workshops ist es, die Fähigkeiten von Kindern und Jugendlichen zu fördern, verantwortungsvoll mit ihren eigenen Daten und respektvoll mit den Daten anderer umzugehen. Dabei geht es nicht darum, sie von Social Media-Angeboten fernzuhalten, sondern sie für Gefahren und Risiken der digitalen Welt zu sensibilisieren.

Die seit Januar 2017 angebotenen Workshops für Grundschulen begegnen einem überwältigenden Interesse. Bis Ende 2018 konnten bereits 228 Workshops an Grundschulen gehalten werden. Insgesamt konnten so innerhalb von zwei Jahren ca. 4.800 Schülerinnen und Schüler an saarländischen Grundschulen zum datenschutzgerechten Umgang im Internet sensibilisiert werden.

Der Unterricht wird von externen Referenten durchgeführt, die vom Datenschutzzentrum geschult wurden. Er ist für Grundschüler auf die Dauer von zwei Unterrichtsstunden angelegt und wird den Schülerinnen und Schülern der Klassenstufe vier angeboten. An weiterführenden Schulen umfasst der Workshop vier Unterrichtsstunden und ist an die Klassenstufe sechs gerichtet. Das Angebot ist für alle Schulen kostenlos. Beantragen kann man die Workshops per Faxformular, das in unserem Internetangebot hinterlegt ist.

11.2 Digitalisierung in Schulen

Im Hinblick auf die Anforderungen im späteren Arbeitsleben und die fortschreitende Digitalisierung der Arbeitswelt müssen die Schulen diese Entwicklung zukünftig noch offensiver angehen und die Chancen und Möglichkeiten der Digitalisierung für Schüler erlebnisnah und praxisorientiert vermitteln können. Schüler sollten beispielsweise nicht nur unterscheiden können, woran man Fake-News erkennen kann, sie sollten auch wissen, welche Rechte und Pflichten sie im Umgang mit Medien und im Internet zu beachten haben.

Doch nicht nur die Vermittlung von Medienkompetenz im Unterricht oder Robotik als mögliches Wahlfach müssen hierbei Beachtung finden; man muss auch den rechtlichen Rahmen an die sich stets verändernde Digitalisierung anpassen.

Egal ob bei der Einführung von schulinternem WLAN, eines elektronischen Klassenbuches, Bring your own device (Byod)-Projekten, der schuleigenen Homepage oder beim Gebrauch interaktiver Aufgabenstellungen sind rechtliche Rahmenbedingungen unvermeidbar, um die Schule, die Schulträger, die Lehrkräfte und letztendlich auch die Schüler vor rechtlichen Konsequenzen zu schützen.

Dabei spielt auch der Datenschutz eine gewichtige Rolle. Durch die enge und gute Zusammenarbeit der Mitglieder der AG Medienkompetenz (ein Zusammenschluss mehrerer Akteure, die auf dem Gebiet der Medienkompetenz im Saarland tätig sind und seit 2008 regelmäßig ihre Arbeit aufeinander abstimmen), gab es im Berichtszeitraum zahlreiche Informationsveranstaltungen, gerade auch durch unsere Dienststelle, zu datenschutzrechtlich relevanten Themen im Bildungsbereich.

Auffällig bei den anschließenden Fragerunden aus der Praxis ist, dass die Rechtslage nicht mehr mit der rasanten technischen Entwicklung standhalten kann. Umso wichtiger ist es, die Lehrkräfte über rechtliche Gegebenheiten bei der Einführung neuer Technologien zu beraten und Gesetze zeitnah an die neuen Gegebenheiten anzupassen. Hier steht das Datenschutzzentrum dem Ministerium für Bildung und Kultur weiterhin mit Rat und Tat zur Seite und hofft auf eine weiterhin gute Kooperation.

Der Datenschutz will und kann hier nicht als „Verhinderer" moderner Technologien im Bildungssektor auftreten, sondern verfolgt die Strategie, neue Technologien datenschutzkonform zu begleiten, um mögliche, drohende Konsequenzen von vorneherein bestmöglich ausschließen zu können. Um dieses Ziel jedoch umsetzen zu können, müssen auch die Anbieter der Technologien die Datenschutzgrundsätze „privacy by design" und „privacy by default" akzeptieren und bei der Gestaltung ihrer Produkte auf die Einhaltung der Datenschutz-Grundverordnung (DSGVO) und sonstiger datenschutzrechtlicher Vorgaben achten, damit das informationelle Selbstbestimmungsrecht von Lehrkräften, Schülern und Eltern auch beim Einsatz neuer Technologien gewahrt bleibt.

11.3 Dritter Saarländischer Medienkompetenztag

Am 29. September 2017 fand in Kirkel zum dritten Mal der Saarländische Medienkompetenztag statt, der von der AG Medienkompetenz, einem Zusammenschluss mehrerer Organisationen, die Medienkompetenz vermitteln und zu deren Gründungsmitglieder auch das Unabhängige Datenschutzzentrum Saarland zählt, organisiert wurde.

Unter dem Motto „Souverän in der digitalen Welt" sprach Prof. Dr. Herbert Scheithauer in seiner Keynote über Zusammenhänge zwischen Medien- und sozialer Kompetenz und erörterte Möglichkeiten, die der Sozialraum „Schule" und der Unterricht bieten, um Heranwachsenden einen souveränen und kritischen Umgang mit Medien zu vermitteln. Im Anschluss boten parallel stattfindende Impulsvorträge und Workshops Einblicke rund um das Themenfeld „Digitale Medien im pädagogischen Einsatz". So konnten die Teilnehmer zwischen den Themen „Prävention von Cybermobbing und Förderung von Medienkompetenz an Schulen", „Medienkomp@ss für Grundschulen im Saarland", „Schule gegen Cybermobbing" und dem von unserer Dienststelle mitgestalteten Vortrag zu „Datenschutz und Urheberrechte in der schulischen Praxis" wählen. Gerade in dem von uns mitgestalteten Vortrag wurde klar, welche Unsicherheit insbesondere bei den Lehrkräften im Umgang mit personenbezogenen Daten im schulischen Umfeld herrscht. Dementsprechend hoch war die Nachfrage, an diesem Workshop teilnehmen zu können. Nachmittags wurden Praxisveranstaltungen zu Coding, Calliope, IDeRBlog und einem Social Media Spiel angeboten, die dem Fachpublikum Möglichkeiten aufzeigen sollten, die angeführten Themen praxisnah im Unterricht einzusetzen.

Über 100 pädagogische Fachkräfte, Erzieher, Sozialpädagogen und Lehrkräfte informierten sich in Vorträgen und diskutierten während der Impulsvorträge und Praxisworkshops. Die Veranstaltung war aufgrund der örtlichen Gegebenheiten wie bereits in den Vorgängerveranstaltungen ausgebucht. Leider konnten deswegen nicht alle Interessenten berücksichtigt werden. Die Teilnehmer des 3. Saarländischen Medienkompetenztages haben der Veranstaltung durchweg eine positive Resonanz bescheinigt und haben Ihr Interesse bekundet, auch an der nächsten Veranstaltung dieser Art, die turnusgemäß im Herbst 2019 stattfinden wird, teilnehmen zu wollen.

12 Telemedien

Besonderer Beratungsbedarf bestand im Berichtszeitraum vor allem auch im Bereich des Datenschutzes in den Telemedien. Viele Bürger waren durch Berichte in Presse, Rundfunk und Internet zu potentiell drohenden Abmahnungen verständlicher Weise verunsichert und baten um Hilfestellung durch unsere Dienststelle. Insbesondere Betreiber privater Webseiten, aber auch Vereine sowie kleine und mittlere Unternehmen wurden durch uns unterstützt.

Positiv hervorzuheben ist zunächst, dass auch im Bereich der Telemedien durch die Datenschutz-Grundverordnung (DSGVO) das Bewusstsein bei Verantwortlichen und Betroffenen zu datenschutzrechtlich relevanten Aspekten auf Webseiten gestiegen ist. Begrüßenswert ist dabei, dass bei einem großen Teil der Webseitenbetreiber die Erkenntnis gereift ist, dass sie für den Schutz der personenbezogenen Daten ihrer Besucher verantwortlich sind. Wo vorher zumindest fahrlässig Plug-Ins, Trackingmethoden und Drittanbieterinhalte eingebunden wurden, ohne sich weitere Gedanken über Implikationen für Betroffene zu machen, ist die Bereitschaft gestiegen, Internetangebote datenschutzfreundlicher zu gestalten. Nicht verschwiegen werden soll aber auch der teils hohe Aufwand für die Webseitenbetreiber, der mit zunehmender Komplexität des jeweiligen Internetangebotes ansteigt.

Ein Teil der Verantwortung der Webseitenbetreiber besteht daher vor allem darin, kritisch zu überprüfen, welche der auf der Webseite eingesetzten Dienste wirklich erforderlich sind. Denn oftmals lässt sich der Aufwand, der beispielsweise mit Auskunftsersuchen der Betroffenen oder mit der Pflicht zur Erstellung einer transparenten Datenschutzerklärung einhergeht, maßgeblich eindämmen, wenn Sinn und Nutzen der verwendeten Dienste grundsätzlich hinterfragt wird. Auch bei Webseiten liegt es demnach nicht nur im Interesse der Betroffenen, sondern auch im unmittelbaren Eigeninteresse des jeweils verantwortlichen Webseitenbetreibers den Rechtsgedanken der Datenminimierung aus Art. 5 Abs. 1 lit. c DSGVO entsprechend zu berücksichtigen.

Unbefriedigend hingegen scheint die Situation im Hinblick auf die noch im Entwurfsstadium befindliche ePrivacy-Verordnung, die ursprünglich zeitgleich mit der DSGVO in Kraft treten sollte. Denn gerade mit der ePrivacy-Verordnung sollen Aspekte des Datenschutzes in Telemedien gesondert und damit vorrangig vor der DSGVO geregelt werden. Dies betrifft beispielsweise den Einsatz von Cookies, aber auch die Auswertung des Verhaltens der Webseitenbesucher zu Marketingzwecken oder dem Einsatz von Over-The-Top-Diensten (solche Dienste setzen auf einem Internetzugangsdienst auf).

12.1 IP-Adressen

Geprägt wurde das Datenschutzrecht in den Telemedien durch die Rechtsprechung des Europäischen Gerichtshofes (EuGH) im Jahr 2016, der in seiner Entscheidung im

Fall Breyer[97] klargestellt hat, dass IP-Adressen jedenfalls dann als personenbezogene Daten anzusehen sind – und damit auch dem Anwendungsbereich des Datenschutzrechts unterliegen – wenn der Betreiber der Webseite über rechtliche Mittel verfügt, mit deren Hilfe er Betroffene identifizieren kann. Ein ähnlich weites Verständnis der Personenbeziehbarkeit fand ebenso Niederschlag in Erwägungsgrund 30 zur DSGVO, wonach IP-Adressen als Online-Kennungen im Sinne des Art. 4 Nr. 1 2. Halbsatz DSGVO, und damit auch als personenbezogene Daten anzusehen sind. Ebendiese Einordnung gewährleistet ein hohes Schutzniveau für Betroffene und ist auf sonstige in den Telemedien gebräuchliche Identifikatoren übertragbar, soweit diese personenbeziehbar im obigen Sinne sind. Dies hat unter anderem auch Auswirkungen auf den Inhalt der Datenschutzerklärung auf Webseiten. In dieser müssen folglich auch detaillierte Informationen dazu vorgehalten werden, zu welchen Zwecken, für welche Dauer und auf welcher Rechtsgrundlage etwa eine längerfristige Speicherung von IP-Adressen in Logfiles erfolgt.

12.2 Datenschutzerklärung

Die meisten Anfragen zum Datenschutz auf Webseiten erhielt unsere Dienststelle zur konkreten Ausgestaltung von Datenschutzerklärungen. Viele Betreiber von Webseiten griffen bei der Erstellung der Datenschutzerklärungen auf im Internet zugängliche Muster zurück. In der aufsichtsbehördlichen Praxis fiel in diesem Zusammenhang jedoch auf, dass die Muster in sehr vielen Fällen via „Copy & Paste“ übernommen wurden, ohne dass deren konkreter Inhalt dahingehend überprüft wurde, ob er auch mit den Eigenheiten der jeweiligen Webseite übereinstimmt. Denn letztlich bildet die Datenschutzerklärung – abgesehen von einigen allgemeinen Informationen die in jeder Erklärung vorhanden sein müssen – spiegelbildlich die konkreten Verarbeitungsvorgänge auf der Webseite ab. Je individueller also das eigene Internetangebot ist, desto spezifischer muss auch die dazugehörige Datenschutzerklärung abgefasst werden. Muster sollten von Webseitenbetreibern daher nur verwendet werden, wenn damit eine kritische Überprüfung und Anpassung einhergeht.

Für den Inhalt der Datenschutzerklärung sind die Vorgaben des Art. 13 Datenschutz-Grundverordnung (DSGVO) maßgeblich. Aus diesem ergeben sich die Informationen, die zwingend in die Datenschutzerklärung aufzunehmen sind: Namen und Kontaktdaten des für die Webseite Verantwortlichen, sofern ein Datenschutzbeauftragter vorhanden ist auch dessen Kontaktdaten, ein Hinweis auf die Rechte der Betroffenen nach der DSGVO sowie ein Hinweis auf das Bestehen eines Beschwerderechts der Betroffenen bei einer Aufsichtsbehörde.

Zum letztgenannten Punkt ist es zweckdienlich – sei es auch nach dem Wortlaut des Art. 13 Abs. 2 lit. d DSGVO nicht verpflichtend – die Kontaktdaten der zuständigen Aufsichtsbehörde konkret zu nennen, da dies den Betroffenen die Wahrnehmung ihrer Rechte erleichtert. Dabei sollte aber eine Formulierung gewählt werden die verdeutlicht, dass es den Betroffenen dabei unbenommen bleibt, sich auch an andere

[97] EuGH, Urteil vom 19.10.2016 – C-582/14, Rn. 49 (zitiert nach juris).

Aufsichtsbehörden zu wenden. Denn diese Möglichkeit sieht Art. 77 Abs. 1 DSGVO ausdrücklich vor.

Darüber hinaus sind weitere Informationen gesondert für jeden Verarbeitungsvorgang auf der Webseite anzugeben. Je nach Funktionalität der Webseite müssen diese Punkte also mehrmals Berücksichtigung finden. Gesonderte Verarbeitungsvorgänge wären beispielsweise der Aufruf der Webseite selbst, bereitgestellte (Kontakt-)Formulare, ein Newsletterdienst, Analytics, Tracking oder jeder eingebundene Drittanbieterinhalt, der personenbezogene Daten der Webseitenbesucher verarbeitet oder an Dritte übermittelt. In jedem dieser Fälle sind sodann Angaben darüber zu machen, welche personenbezogenen Daten der Webseitenbesucher im Rahmen des jeweiligen Vorganges verarbeitet, eine Erläuterung, zu welchem Zweck und auf welcher Rechtsgrundlage die Verarbeitung erfolgt sowie die Dauer der Speicherung der Daten oder eine Angabe der Kriterien, nach denen die Speicherdauer festgelegt wird. Es kann nicht oft genug betont werden, dass allgemeine Angaben zu den obigen Punkten, die sich nicht konkret auf einzelne Verarbeitungsvorgänge beziehen, untauglich sind, um den Informationspflichten aus Art. 13 DSGVO gerecht zu werden.

Ein Hinweis darauf, dass der Betroffene eine gegebene Einwilligung mit Wirkung für die Zukunft widerrufen kann ist nur dann erforderlich, wenn auch tatsächlich Einwilligungen von den Webseitenbesuchern eingeholt wurden. Anderenfalls wäre ein Hinweis auf ein etwaiges Widerrufsrecht für Betroffene irreführend. Sinnvollerweise sollte der Hinweis an der Stelle in der Datenschutzerklärung erfolgen, an der der Verarbeitungsvorgang beschrieben wird, für den eine Einwilligung eingeholt wurde. Sofern eine Verarbeitung auf Art. 6 Abs. 1 lit. f DSGVO gestützt wird, ist außerdem eine Erläuterung erforderlich, welche berechtigten Interessen der Webseitenbetreiber damit verfolgt und dass dem Betroffenen hierbei ein Widerspruchsrecht nach Art. 21 DSGVO zusteht. Abschließend muss auf etwaige Empfänger der Daten, aber auch auf eine (beabsichtigte) Übermittlung personenbezogener Daten an ein Drittland hingewiesen werden, nebst Angabe, inwiefern diese Drittlandübermittlung zulässig erfolgen kann.

Letztendlich soll auch nochmals Art. 12 Abs. 1 S. 1 DSGVO hervorgehoben werden. Nach diesem muss die Datenschutzerklärung *„in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache"* abgefasst sein. Bei Form und Stil der Datenschutzerklärung verbleiben dem Verantwortlichen damit zwar Spielräume, er sieht sich aber auch der Gratwanderung ausgesetzt, dass er den Webseitenbesuchern einerseits im Bedarfsfall technische Vorgänge beschreiben muss, dies andererseits aber so tun muss, dass es für die Betroffenen verständlich bleibt. Denkbar wäre daher auch, dass in einem ersten Schritt die wesentlichen, zwingend zu erteilenden Informationen möglichst kurz und präzise in der Datenschutzerklärung aufgeführt werden. Auf einer zweiten Ebene könnten dann durch Verlinkungen oder aufklappbare Elemente weitergehende Informationen vorgehalten werden, die den Betroffenen nicht geläufige Begriffe erläutern oder sonstige Informationen zur Verfügung stellen, die ein Verständnis der Datenschutzerklärung erleichtern.

Nicht der Verständlichkeit dienen jedenfalls allgemeine Wiederholungen des Gesetzestextes. Diese erfüllen regelmäßig keinen Zweck, führen aber in den meisten Fällen

dazu, dass die Datenschutzerklärung unnötig lang wird und erschwert damit den Betroffenen die Wahrnehmung der wirklich für sie relevanten Informationen.

12.3 Facebook-Fanpages

Mit Urteil vom 5. Juni 2018 – C-210/16 hat der Europäische Gerichtshof (EuGH) entschieden, dass Betreiber einer Facebook-Fanpage gemeinsam mit dem Netzwerk für die Verarbeitung der personenbezogenen Daten der Seitenbesucher verantwortlich sind. Normale Benutzerprofile waren damit nicht Gegenstand der Entscheidung. Die gemeinsame Verantwortlichkeit von Facebook und den Fanpagebetreibern hat dabei jedoch eine Reihe von rechtlichen Implikationen zur Folge, die den Betrieb einer Fanpage zum aktuellen Zeitpunkt nicht datenschutzkonform möglich erscheinen lassen.

Zur Einordnung der sich aus dem Urteil ergebenden Folgerungen wurde durch die Datenschutzkonferenz (DSK) eine Taskforce Fanpage etabliert, an der auch das Unabhängige Datenschutzzentrum Saarland beteiligt ist. In diesem Rahmen hat die DSK im Juni 2018 eine Entschließung[98] veröffentlicht sowie im September 2018 einen Beschluss[99] gefasst.

Fanpagebetreibern wird es insbesondere ohne weitergehende Informationen über die durch Facebook vorgenommenen Verarbeitungsvorgänge nicht möglich sein, ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 Datenschutz-Grundverordnung (DSGVO) nachzukommen. Denn diese umfasst auch die Pflicht darlegen zu können, inwiefern der konkrete Verarbeitungsvorgang *„auf rechtmäßige Weise“* erfolgt (Art. 5 Abs. 2 i. V. m. Abs. 1 lit. a DSGVO). Als (Mit-)Verantwortliche bedürfen nämlich auch die Fanpagebetreiber einer Rechtsgrundlage für die Verarbeitungen im Rahmen ihrer Fanpage. Nach bisherigen Erkenntnissen werden aber den Fanpagebetreibern keine genaueren und hinreichend transparenten Informationen zu den Verarbeitungstätigkeiten auf der sozialen Plattform durch das Unternehmen Facebook zur Verfügung gestellt. Damit setzt Facebook die Fanpagebetreiber einer datenschutzwidrigen Situation aus, derer sie sich aktuell nur durch eine Verzicht auf eine Fanpage erwehren könnten. Mit der Bewertung dieser Situation werden sich daher zu Beginn des Jahres 2019 sowohl die Taskforce als auch die DSK beschäftigen. Entsprechende Beschlüsse werden wir sodann auf unserer Internetseite veröffentlichen.

12.4 (Kontakt-)Formulare

Die Ausgestaltung etwaiger (Kontakt-)Formulare auf der Webseite richtet sich nach dem jeweiligen Verwendungszweck, den das Formular erfüllen soll. In den meisten Fällen wird es in diesem Zusammenhang nicht nötig sein, gesonderte Einwilligungen

[98] https://www.datenschutzkonferenz-online.de/media/en/20180605_en_fb_fanpages.pdf (letzter Zugriff: 5.3.2019).

[99] https://www.datenschutzkonferenz-online.de/media/dskb/20180905_dskb_facebook_fanpages.pdf (letzter Zugriff: 5.3.2019).

der Webseitenbesucher einzuholen. Als Rechtsgrundlage für die Verwendung der so erhobenen Daten kommt nämlich vor allem bei allgemeinen Kontaktformularen das berechtigte Interesse des Webseitenbetreibers im Sinne des Art. 6 Abs. 1 lit. f Datenschutz-Grundverordnung (DSGVO) in Betracht.

Denkbar ist es aber auch, die Verwendung eines Kontaktformulars auf Art. 6 Abs. 1 lit. b DSGVO zu stützen, wenn dieses beispielsweise dazu genutzt werden soll, potentiellen Kunden die Kontaktaufnahme bezüglich vorvertraglicher Maßnahmen zu ermöglichen.

Auch eine gesondert erteilte Einwilligung kann im Rahmen eines Formulars bei den Webseitenbesuchern eingeholt werden. In der Regel zwingend ist dies dort, wo über das Formular auch besondere Kategorien personenbezogener Daten erhoben und verarbeitet werden sollen (vgl. Art. 9 DSGVO). Dabei müssen jedoch die Anforderungen der DSGVO an eine wirksame Einwilligung im Sinne des Art. 4 Nr. 11 in Verbindung mit Art. 7 DSGVO beachtet werden, da der Webseitenbetreiber ansonsten Gefahr läuft, die Daten mangels wirksamer Einwilligung rechtswidrig zu erheben. Bevor er seine Eingaben absendet, müssten dem Betroffenen daher alle nach dem Art. 4 Nr. 11, 7 DSGVO notwendigen Informationen erteilt werden. Hierzu gehört u. a. auch, dass die betroffene Person einen Hinweis auf das Widerrufsrecht erhält.

12.5 Verschlüsselung auf Webseiten

Schon in den letzten beiden Tätigkeitsberichten wurde thematisiert, dass es bereits nach der bisherigen Rechtslage notwendig war, dass Telemedien gegen Verletzungen des Schutzes personenbezogener Daten technisch gesichert werden. Der Betreiber der Webseite gewährleistet dies insbesondere, indem er eine Transportverschlüsselung einsetzt, um beispielsweise beim Einsatz von (Kontakt-)Formularen auf der Webseite die Übermittlung der dort eingegebenen Daten gegen den unbefugten Zugriff durch Dritte zu schützen.

Auch die Datenschutz-Grundverordnung (DSGVO) weist nun in Art. 32 Abs. 1 lit. a ausdrücklich darauf hin, dass insbesondere die Verschlüsselung eine geeignete technische Maßnahme zum Schutz personenbezogener Daten sein kann. Bei der Beurteilung, welche Maßnahmen durch den Verantwortlichen zu ergreifen sind, sind dabei der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Vor allem eine Transportverschlüsselung von Webseiten gehört somit zu den Basismaßnahmen, die von Webseitenbetreibern notwendigerweise umzusetzen sind.

13 Wirtschaft und Vereine

13.1 Vorbereitende Beratung der Wirtschaft im Hinblick auf die DSGVO

Schon vor Beginn des Berichtszeitraums gingen beim Unabhängigen Datenschutzzentrum Saarland die ersten Beratungsanfragen saarländischer Unternehmen zur Umsetzung der Datenschutz-Grundverordnung (DSGVO) ein. Im Laufe des Jahres 2017 nahmen diese Anfragen in erheblichem Umfang zu und fanden ab dem Mai 2018 mit Wirksamwerden der DSGVO ihren Höhepunkt. Daher hatte das Datenschutzzentrum im Jahr 2018 einen Schwerpunkt seiner Tätigkeit auf Beratung und Information der in der Wirtschaft Verantwortlichen gelegt.

Diese Flut an Beratungsanfragen im Zeitraum von Mai bis September 2018 war nicht nur angesichts der angespannten Personalsituation, sondern auch im Hinblick auf die thematische Bandbreite der Ersuchen kaum zu bewältigen. Nichtsdestotrotz stand bereits in der ersten Jahreshälfte 2018 eine beträchtliche Anzahl an konzertierten Informationsmaterialien zur Verfügung, die Basis für die aufsichtsbehördliche Beratung waren. Diese sog. Kurzpapiere[100], die von der Datenschutzkonferenz (DSK) veröffentlicht wurden, geben für verschiedene Datenschutzthemen aufsichtsbehördliche Positionen wieder und werden bis dato fortgeschrieben und ergänzt.

Vor allem die Kurzpapiere Nr. 1 „*Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO*", Nr. 8 „*Maßnahmenplan „DS-GVO" für Unternehmen*" und Nr. 10 „*Informationspflichten*" fanden von Beginn an erhebliche Resonanz. Dabei sollte nicht unerwähnt bleiben, dass die beiden letzten Kurzpapiere durch unsere Dienststelle federführend erarbeitet wurden.

Insoweit ein erheblicher Beratungsbedarf der saarländischen Wirtschaft bereits seit Inkrafttreten der DSGVO im Mai 2016 von den Berufs- und Interessenverbänden sowie von den Wirtschaftskammern an das Datenschutzzentrum herangetragen wurde, wurde eine Reihe von Veranstaltungen zum neuen europäischen Datenschutzrecht vorgesehen, um nicht nur dem Informationsbedarf der Wirtschaft gerecht zu werden, sondern gleichzeitig auch ein Forum für Fragestellungen zu geben.

In den Räumen der Industrie- und Handelskammer Saarland (IHK) fand im Februar 2018 die Veranstaltung „*Das neue Datenschutzrecht kommt: Das müssen Sie wissen!*" statt, für die aufgrund der großen Nachfrage Folgetermine im April 2018 angeboten wurden. Viele Fragen wurden aber auch im Nachgang in telefonischer Beratung oder durch Termine in unserer Dienststelle und ggf. auch vor Ort erörtert.

[100] Elektronisch abrufbar auf der Internetpräsenz des Unabhängigen Datenschutzzentrums Saarland (https://datenschutz.saarland.de/datenschutz/anwendungshinweise-dsgvo/kurzpapiere/).

Die in Zusammenarbeit mit der IHK im April 2018 durchgeführten Veranstaltungen „*Die neue EU-Datenschutz-Grundverordnung - Neuerungen und Herausforderungen für KMU*" und „*Werbung und Datenschutz*" war ebenfalls stark frequentiert.

Im Rahmen von zwei Veranstaltungen setzte die Arbeitskammer des Saarlandes in Kooperation mit dem Datenschutzzentrum einen Schwerpunkt auf den Mitarbeiterdatenschutz mit dem Vortragsthema „*Die neue EU-Datenschutz-Grundverordnung und der Beschäftigtendatenschutz*".

Daneben fand im Jahr 2018 eine Vielzahl weiterer Termine statt, die sich mitunter an spezifische Interessenten, wie Inhaber von Handwerksbetrieben und Vereinsvorstände, richteten.

Da sich gerade auch Vertreter von Vereinen in besonderem Maße ratsuchend an das Datenschutzzentrum gewandt hatten,[101] wurden die Handreichungen „*Datenschutz im Verein*" und „*Veröffentlichung von Fotoaufnahmen im Verein*" erstellt,[102] in denen die häufigsten Fragen zum jeweiligen Thema aufgegriffen und beantwortet werden.

13.2 Auskunfteien, Versicherungs- und Kreditwirtschaft

Wie in den anderen Bereichen auch, war der Berichtszeitraum von der Umsetzung der Datenschutz-Grundverordnung (DSGVO) geprägt. Bereits im Jahr 2017 begannen in den Bereichen der Auskunfteien, Versicherungsunternehmen und der Kreditwirtschaft die Gespräche mit den jeweiligen Verbänden (u. a. dem Gesamtverband der deutschen Versicherungswirtschaft, dem Bundesverband deutscher Banken, dem Giro- und Sparkassenverband, dem Bundesverband der Deutschen Volksbanken und Raiffeisenbanken, Verband „Die Wirtschaftsauskunfteien"). Bei den Gesprächen, die im Rahmen von Sitzungen der Arbeitsgemeinschaften des Düsseldorfer Kreises und später im Rahmen von Sitzungen der Arbeitskreise der Datenschutzkonferenz stattfanden und an denen das Unabhängige Datenschutzzentrum Saarland beteiligt war, ging es um die konkrete Umsetzung der DSGVO und die Klärung offener Rechtsfragen in diesem Zusammenhang. In diesen bilateralen Gesprächen zwischen dem Wirtschaftsverbänden und den Aufsichtsbehörden konnten zudem konkrete Sachverhalte erörtert und rechtlich geklärt werden. Dabei hat sich unserer Ansicht nach deutlich gezeigt, dass die Wirtschaftsverbände sich an der Thematik des Datenschutzes nicht nur interessiert gezeigt haben, sondern einer datenschutzfreundlichen Ausgestaltung offen gegenüber standen, auch wenn es an der einen oder anderen Stelle deutliche Reibungspunkt mit den Aufsichtsbehörden gab. Schlussendlich konnte in vielen Punkten eine Einigung und damit Rechtssicherheit für die in den Verbänden organisierten Unternehmen auf der einen Seite erzielt werden und auch ein hohes Maß an Datenschutz für die betroffenen Personen (v.a. Kunden und Verbraucher) auf der anderen Seite erreicht werden.

[101] Siehe dazu Kap. 13.5. (S. 124 ff.)

[102] Elektronisch abrufbar auf der Internetpräsenz des Unabhängigen Datenschutzzentrums Saarland (https://datenschutz.saarland.de/themen/vereine/datenschutz-im-verein/).

Parallel hierzu fanden außerdem Gespräche über die Genehmigung von zwei Code of Conducts statt (im Bereich der Auskunfteien und der Versicherungswirtschaft). Bei einem Code of Conduct handelt es sich um einen Kodex, der mit den Aufsichtsbehörden, den Verbraucherschützern und einem Wirtschaftsverband entwickelt wird und eine freiwillige Selbstverpflichtung der Mitgliedsunternehmen für den Umgang mit personenbezogenen Daten enthält. Der Kodex enthält vor allem definierte Verhaltensregeln und konkretisiert damit die allgemeinen Regeln des Datenschutzrechts. Ein Code of Conduct schafft damit nicht nur Rechtssicherheit für die Mitgliedsunternehmen, sondern stellt auch einen Mehrwert für die von der Datenverarbeitung betroffenen Personen dar. Es wäre daher aus unserer Sicht wünschenswert, wenn weitere Verbände solche Verhaltensregeln zusammen mit den Aufsichtsbehörden auf den Weg bringen würden.

Daneben war das Datenschutzzentrum auch konkreter Ansprechpartner für die im Saarland ansässigen Unternehmen dieser Branchen. In zahlreichen Einzelberatungen wurden die saarländischen Unternehmen unterstützt, soweit dies aufgrund der extrem hohen Auslastung des Datenschutzzentrums möglich war. Auch hier war das Ziel zum einen die saarländische Wirtschaft bei der Umsetzung des Datenschutzrechts zu unterstützen und zum anderen für die betroffenen Personen eine datenschutzfreundliche Ausgestaltung zu erreichen. Dieses Ziel wurde auch vielfach erreicht.

Trotzdem sollte an dieser Stelle nicht unerwähnt bleiben, dass es im alltäglichen Umgang mit den Datenschutzregeln, sowohl nach der alten als auch nach der neuen Rechtslage einige Eingaben von betroffenen Personen gab. Diese Eingaben betrafen in der Mehrzahl die Geltendmachung von Auskunftsansprüchen und in der Folge auch von der Ausübung des Rechts auf Löschung. In der Regel konnte den betroffenen Personen sehr schnell durch Intervention unserer Dienststelle geholfen werden. Nur in wenigen Ausnahmefälle kam es zu strittigen Auseinandersetzungen zwischen dem verantwortlichen Unternehmen und dem Unabhängigem Datenschutzzentrum Saarland bzw. musste unsere Behörde von aufsichtsrechtlichen Befugnissen Gebrauch machen, um die rechtmäßigen Ansprüche der Betroffenen durchzusetzen.

Daneben wandten sich auch viele betroffene Personen an unsere Dienststelle mit der Bitte um Beratung. In den meisten Fällen konnten den Bürgern geholfen werden. In den Fällen, in denen dies nicht der Fall war, handelte es sich ausschließlich um Beratungsersuchen, die nicht in die Zuständigkeit unserer Dienststelle fallen. Die Betroffenen wurden sodann von uns an die zuständigen Stellen verwiesen bzw. direkt der Kontakt zu der zuständigen Stelle vermittelt.

13.2.1 Auskunfteien – Einzelfälle

Auskunfteien sind Wirtschaftsunternehmen, die u. a. Informationen über die Kreditwürdigkeit bzw. über das Zahlungsverhalten von Privatpersonen und Unternehmen auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO verarbeiten. Zu diesen Informationen gehören auch sachliche Negativmerkmale, wie beispielsweise zu Unrecht nicht beglichene Forderungen, Informationen zu Einträgen im Schuldnerverzeichnis und aus Insolvenzverfahren. Diese Informationen dürfen Dritten auf Anfrage zur Verfügung

gestellt werden, wenn diese ein berechtigtes Interesse an einer solchen Information geltend machen. Dies ist regelmäßig dann der Fall, wenn ein potentieller Vertragspartner mit dem Betroffenen eine geschäftliche Beziehung eingehen will, welche für ihn mit einem finanziellen Risiko behaftet ist. Dies trifft insbesondere für Dauerschuldverhältnisse (z. B. Kreditverträge, Mietverträge oder ggf. auch Mobilfunkverträge) zu.

Eine unzulässige Datenverarbeitung durch eine Auskunftei kann für den Betroffenen weitreichende Folgen haben; wird beispielsweise fälschlicherweise eine vermeintlich nicht beglichene Forderung eingemeldet, dann führt dies zu einer Verschlechterung des sogenannten Bonitätscores des Betroffenen. Dieser Score gibt als Zahlenwert an, wie hoch die Wahrscheinlichkeit eines Kreditausfalls ist. Ein schlechter Scorewert kann dann dazu führen, dass die betroffene Person nicht mehr als kreditwürdig eingestuft wird. Der Abschluss von Finanzierungs- oder Leasinggeschäften ist in diesen Fällen nahezu unmöglich.

Personenverwechselung – Was tun?

Auch im Berichtszeitraum meldeten sich wiederholt Beschwerdeführer bei unserer Dienststelle, die Schreiben von verschiedenen Inkassounternehmen in Forderungsangelegenheiten erhielten, die den Betroffenen völlig unbekannt waren. Aufgrund der Schilderungen war zu vermuten, dass es sich in diesen Fällen um eine aufgrund von Namensgleichheit bedingte Verwechslung von tatsächlichem Schuldner und Empfänger des Inkassoschreibens handelte.

Solche Verwechselungen können etwa auf dem nachfolgend geschilderten Sachverhalt beruhen: Zum Zwecke des Forderungseinzugs übermitteln Gläubiger Schuldnerdaten an Inkassounternehmen. Für den Fall, dass Schreiben des Inkassounternehmens nicht zugestellt werden können, beispielsweise wegen Umzugs des Schuldners oder wegen bewusster Falschangabe, kann dann eine Abfrage über den Schuldner bei einer Auskunftei erfolgen, um die aktuelle Wohnanschrift zu ermitteln. Hierbei wird in der Regel Name, Anschrift und Geburtsdatum mit dem hinterlegten Datensatz abgeglichen. Wenn die Anschrift des Schuldners gerade nicht bekannt ist, kann dies bei identischem Namen und Geburtsdatum zu einer fehlerhaften Beauskunftung seitens der Auskunftei führen.

Den Betroffenen wurde in solchen Fällen geraten, die Schreiben der Inkassofirmen auf keinen Fall unbeantwortet zu lassen. Die unberechtigten Forderungen sollten in jedem Fall gegenüber dem Inkassounternehmen schriftlich bestritten werden.

Darüber hinaus sollten Betroffene gegenüber der Inkassofirma und der Auskunftei einen Anspruch auf Auskunft gemäß Art. 15 DSGVO geltend machen. Dieser Auskunftsanspruch gewährt Betroffenen u. a. eine Auflistung aller über ihre Person verarbeiteten Daten und über deren Herkunft. Betroffene erhalten hierdurch Kenntnis von der Stelle, die den falschen Datensatz übermittelt hat und können dort dann einen Anspruch auf Berichtigung gem. Art. 16 DSGVO geltend machen. Außerdem sollte sich der Betroffene, um künftige Personenverwechslungen zu vermeiden, mit der betreffenden Auskunftei in Verbindung setzen und darauf hinwirken, dass dem Datensatz ein Hinweis hinzugefügt wird, dass es bei ihm zu Personenverwechslungen gekommen ist.

Auch sollten Betroffene regelmäßig Auskunftsersuchen an die gängigen Auskunfteien richten, um dann prüfen zu können, ob ihrem Datensatz bereits falsche Informationen hinzugefügt wurden. In diesen Fällen können Betroffene ebenso einen Anspruch auf Berichtigung unrichtiger Daten geltend machen.

Datenschutz bei Inkassounternehmen

Im Berichtszeitraum meldete sich ein Beschwerdeführer bei hiesiger Dienststelle und bat um aufsichtsbehördliches Tätigwerden gegen ein im Saarland ansässiges Inkassounternehmen, von dem er ein Forderungsschreiben erhalten hatte, in dem nicht nur die Hauptforderung, Mahn- und Zinskosten geltend gemacht wurden, sondern auch die Kosten über eine Bonitätsauskunft. Der Beschwerdeführer wollte daraufhin wissen, welche Daten das Unternehmen über seine Person verarbeitet und stellte daher ein Auskunftsersuchen nach § 34 Bundesdatenschutzgesetz a. F. (BDSG a. F.) in der bis 25. Mai 2018 gültigen Fassung. Das Unternehmen teilte ihm darauf u. a. mit, dass seine Daten nicht an Dritte weitergeleitet wurden.

Bei Bonitätsabfragen werden allerdings die identifizierenden Angaben einer Person an eine Auskunftei übermittelt mit dem Ziel zu erfahren, ob über diese Person negative Eintragungen aufgrund von unzuverlässigem Zahlungsverhalten bekannt sind. Insofern war anzunehmen, dass das Inkassounternehmen, entgegen seiner Auskunft, Daten des Betroffenen an eine oder mehrere Auskunfteien übermittelt hatte. Der Beschwerdeführer sah sich aufgrund dieses Umstands und nachdem auf seine Anfrage nach dem Verfahrensverzeichnis nach § 4e in Verbindung mit § 4g Abs. 2 BDSG a. F. nicht reagiert wurde, nicht weiter in der Lage, seine Betroffenenrechte auf direktem Weg geltend zu machen und bat die Aufsichtsbehörde um Unterstützung.

Aufgrund des geschilderten Sachverhalts wurde das besagte Unternehmen von hiesiger Dienststelle zur Stellungnahme aufgefordert. Insbesondere sollte das Unternehmen darstellen, wie das Verfahren im Falle eines geltend gemachten Auskunftsersuchens nach § 34 BDSG a. F. organisatorisch ausgestaltet ist und aus welchem Grund das Auskunftsersuchen des Petenten nicht in der gesetzlich vorgesehenen Weise beantwortet wurde. Des Weiteren wurde das Verfahrensverzeichnis erfragt und um Stellungnahme gebeten, weshalb dem Beschwerdeführer dieses nicht zur Verfügung gestellt wurde. Abschließend sollte Klarheit darüber geschaffen werden, ob und bejahendenfalls auf welcher Rechtsgrundlage über den Beschwerdeführer eine Bonitätsauskunft eingeholt wurde.

Von Seiten des Unternehmens wurde ausgeführt, dass die nicht zufriedenstellende Beantwortung des Auskunftsersuchens auf mehrere Faktoren zurückzuführen gewesen sei.

Neben der Verhinderung des zuständigen Sachbearbeiters und des erhöhten Arbeitsaufkommens sei die Beantwortung des Auskunftsersuchens auch nicht – wie unternehmensintern vorgesehen – mit der Geschäftsleitung abgestimmt worden. Dies sei auch der Grund dafür gewesen, dass dem Beschwerdeführer das Verfahrensverzeichnis nicht in der gesetzlich vorgesehenen Weise zur Verfügung gestellt wurde. Es wurde außerdem eingeräumt, dass über den Betroffenen eine Bonitätsabfrage eingeholt wurde und damit eine Datenübermittlung an Dritte – entgegen der eigenen Mitteilung – stattgefunden hatte. Rechtsgrundlage hierfür sei § 28 Abs. 1 Nr. 2

BDSG a. F., da die Bonitätsauskunft dazu diene, die Erfolgsaussichten einer Beitreibung der betreffenden Inkassoforderung einzuschätzen.

Dem Inkassounternehmen wurde seitens der Aufsichtsbehörde mitgeteilt, dass die angeführten Umstände im Unternehmen nicht dazu führen dürften, dass die Betroffenenrechte nicht in einer angemessenen Frist gewährleistet werden können. Im Hinblick auf das Auskunftsersuchen wurde daher ein Muster entworfen, in dem alle zu beauskunftenden Informationen und auch weitere Angaben wie Herkunft, Empfänger der Daten sowie der Zweck der Speicherung enthalten waren. Auch wurde eine neue interne Dienstanweisung abgestimmt, die den Mitarbeitern des Unternehmens zur Verfügung gestellt wurde. Darin wurde u. a. die Frist für die Bearbeitung derartiger Auskunftsersuchen auf maximal drei Wochen festgelegt. Zudem wurden konkrete Mitarbeiter für die Bearbeitung entsprechender Ersuchen festgelegt.

Nicht zu beanstanden war im konkreten Fall die Einholung der Bonitätsauskunft, da das gesetzlich erforderte berechtigte Interesse hierfür gegeben war. Gemäß § 28 Abs. 1 S. 1 Nr. 2 BDSG a. F. ist die Übermittlung personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung offensichtlich überwiegt. Die Erfolgsaussichten einer Beitreibung der betreffenden Inkassoforderung im Wege der Bonitätsauskunft einschätzen zu können, ist als berechtigtes Interesse im Sinne der Vorschrift einzustufen.[103]

Nachdem auch das Verfahrensverzeichnis in einigen Punkten ergänzt wurde, konnten dem Petenten alle Informationen zur Verfügung gestellt werden. Allerdings hat dieser Fall wieder einmal gezeigt, dass sich viele Inkassounternehmen ihrer datenschutzrechtlichen Verantwortung nicht bewusst sind und erst im Rahmen eines aufsichtsbehördlichen Verfahrens auf die damit verbundenen Anforderungen aufmerksam werden.

13.2.2 Kreditwirtschaft – Kopieren, Scannen und Speichern von Personalausweisen

Bereits im Berichtszeitraum des 26. Tätigkeitsberichts hatte sich die Aufsichtsbehörde mit der Frage auseinandergesetzt, unter welchen Voraussetzungen und in welchem Umfang im Einzelfall das Einscannen oder die Anfertigung einer Kopie des Personalausweises datenschutzrechtlich zulässig ist. Diese Frage stellte sich insbesondere häufig im Verhältnis von Bankinstitut und Kunde.

[103] Die beschriebene Datenverarbeitung wäre auch unter dem Regelungsregime der DSGVO zulässig gewesen. Die DSGVO kennt im Gegensatz zum BDSG a. F. keinen eigenen Regelungstatbestand für die Verarbeitung personenbezogener Daten durch Auskunfteien, weshalb auf Art. 6 Abs. 1 lit. f DSGVO zurückzugreifen ist. Auch nach dieser Vorschrift hätte das Interesse des Inkassounternehmens an der Einschätzung einer erfolgreichen Forderungsbeitreibung das Interesse des betroffenen Schuldners überwogen.

In diesem Zusammenhang war zu berücksichtigen, dass ein Personalausweis grundsätzlich gemäß dem damals geltenden Personalausweisgesetz (PersAuswG)[104] und den dortigen Bestimmungen des § 14 in Verbindung mit § 20 weder zum automatisierten Abruf noch zur automatisierten Speicherung personenbezogener Daten verwendet werden durfte. Jedoch fanden sich bereits nach damals geltender Rechtslage in § 3 Abs. 1 Nr. 1 i. V. m. § 4 Abs. 1 Geldwäschegesetz a. F. (GwG a. F.)[105] in Verbindung mit § 154 Abgabenordnung (AO) Regelungen, wonach u. a. Bankinstitute in bestimmten Fällen zur Identifikations- und Legitimationsprüfung verpflichtet waren. Dabei grenzte § 4 Abs. 3 Nr. 1 GwG a. F. die zur Feststellung der Identität des Vertragspartners zu erhebenden Angaben auf den Namen, den Geburtsort, das Geburtsdatum, die Staatsangehörigkeit und die Anschrift ein. Diese nach § 4 Abs. 4 Nr. 1 GwG a. F. einem amtlichen Ausweis zu entnehmenden Angaben waren nach § 8 Abs. 1 GwG a. F. aufzuzeichnen und um die Ausweisnummer und die ausstellende Behörde zu ergänzen. Die Anfertigung einer Kopie des gültigen Ausweises galt dabei nach § 8 Abs. 1 S. 3 GwG a. F. als Aufzeichnung der darin enthaltenen Angaben.

Der Personalausweis enthält aber auch Angaben, die über die nach GwG a. F. bzw. AO erforderlichen Angaben hinausgehen (bspw. Augenfarbe oder Körpergröße oder auch die Zugangsnummer), so dass das Einscannen und die Kopie des Personalausweises mit sämtlichen darin enthaltenen Angaben von der Aufsichtsbehörde nicht als zulässig erachtet wurde und nur bei entsprechender Schwärzung der nicht erforderlichen Angaben von einer rechtmäßigen Datenverarbeitung auszugehen war.

Diese unter Zugrundelegung der alten Rechtslage richtige Schlussfolgerung ist jedoch unter Geltung des neuen Geldwäschegesetzes[106] nunmehr anderweitig geregelt. Die novellierte Fassung des § 8 Abs. 2 S. 2 GwG bestimmt nämlich ausdrücklich, dass die in diesem Zusammenhang Verpflichteten, also u. a. Bankinstitute und Versicherungsunternehmen, zur Erfüllung ihrer nunmehr aus § 10 GwG resultierenden allgemeinen Sorgfaltspflichten und in § 11 konkretisierten Identifizierungspflicht das Recht und sogar die Pflicht haben, vollständige Kopien u. a. eines im Rahmen der Identitätsüberprüfung vorgelegten Personalausweises gemäß § 12 Abs. 1 S. 1 Nr. 1 GwG anzufertigen oder diesen vollständig optisch digitalisiert zu erfassen.

Die Aufsichtsbehörde wies also im Rahmen entsprechender Anfragen und Beschwerden auf diese neue Rechtslage hin und geht seither davon aus, dass das Einscannen und Kopieren von Personalausweisen eines Bankkunden durch die Bank zur Erfüllung einer rechtlichen Verpflichtung gemäß Art. 6 Abs. 1 lit. c DSGVO unter den Voraussetzungen der entsprechenden Bestimmungen im Geldwäschegesetz erforderlich und rechtmäßig ist.

---

[104] In der Gültigkeit vom 29.7.2017 bis 14.5.2018 (BGBl. I 2009 S. 1346, BGBl. I 2017 S. 2745).

[105] In der Gültigkeit vom 26.6.2017 bis 24.5.2018 (BGBl. I 2017 S. 1822).

[106] Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten – Geldwäschegesetz vom 23.6.2017 (BGBl. I S. 1822), zuletzt geändert d. Gesetz v. 10.7.2018 (BGBl. I S. 1102).

13.2.3 Versicherungswirtschaft – Anforderungen an ein rechtskonformes Löschkonzept in der Versicherungswirtschaft

Aus den in der DSGVO niedergelegten Grundsätzen der Speicherbegrenzung und der Zweckbindung der Datenverarbeitung sowie dem in Art. 17 DSGVO normierten Recht betroffener Personen auf Löschung, folgt die Pflicht von datenverarbeitenden Stellen sicherzustellen, dass personenbezogene Daten nur so lange gespeichert werden, wie dies für die Zweckerreichung erforderlich ist. Weiterhin hat der Verantwortliche nach Maßgabe des Art. 24 DSGVO angemessene technische und organisatorische Maßnahmen zur Einhaltung der Vorgaben der DSGVO umzusetzen. Vor diesem Hintergrund sind von Verantwortlichen notwendigerweise standardisierte Regeln zur Löschung personenbezogener Daten vorzusehen und zu implementieren. Abhängig vom Umfang der von dem Verantwortlichen betriebenen Datenverarbeitung kann die Etablierung eines feingranularen Löschkonzepts notwendig sein.

Gerade im Bereich der Versicherungswirtschaft werden große Datenbestände verarbeitet, die zudem oftmals – wie bspw. im Falle der Krankenversicherungen – besonders sensible und schutzwürdige Daten enthalten. Dies erfordert insgesamt ein strukturiertes und systematisches Vorgehen beim Umgang mit personenbezogenen Daten.

Im Berichtszeitraum wandte sich ein Beschwerdeführer an die Aufsichtsbehörde mit dem Begehren, einer privaten Krankenversicherung die Löschung bestimmter personenbezogener Daten aufzugeben. Er beklagte, sein Versicherungsvertrag bestehe nunmehr seit über 5 Jahren nicht mehr und es gebe keine Grundlage für die weitere Speicherung von Daten, welche seinen Gesundheitszustand betreffen. Die Versicherung hingegen berief sich auf handels-, steuer- und vertragsrechtliche Aufbewahrungspflichten und gab an, grundsätzlich sämtliche mit dem Vertrag verbundenen personenbezogene Daten zunächst 10 und anschließend 20 weitere Jahre mit eingeschränktem Zugriff vorzuhalten.

Hier gilt es zu berücksichtigen, dass insbesondere private Krankenversicherungen zu einer differenzierten Auseinandersetzung angehalten sind, ob bzw. in welchem Umfang und wie lange eine fortdauernde Speicherung personenbezogener Daten des Versicherten zur Erfüllung etwaiger Leistungsansprüche auch nach Kündigung des Vertrages erforderlich sind und welche der vorhandenen Unterlagen unter handels- oder steuerrechtliche Aufbewahrungspflichten fallen und aus diesem Grund für die in diesen Vorschriften im Einzelnen vorgesehene Zeiträume vorzuhalten sind. Im Rahmen der dem Verantwortlichen nach Art. 5 Abs. 1 in Verbindung mit Abs. 2 DSGVO obliegenden Rechenschaftspflicht ist konkret darzulegen, welche personenbezogenen Daten auf welcher rechtlichen Grundlage verarbeitet werden. Hierzu ist es erforderlich, dass nach Art und Zweck der Daten differenziert wird. Erst diese Differenzierung ermöglicht es, ein den Vorgaben der DSGVO entsprechendes Löschkonzept mit spezifischen Löschfristen umzusetzen, das somit auch den Interessen der Betroffenen im erforderlichen Maße Rechnung trägt.

Die Versicherung wurde deshalb seitens der Aufsichtsbehörde darauf hingewiesen, dass die nicht nach Art und Zweck der Daten differenzierende generelle Vorhaltung sämtlicher mit einem Versicherungsvertrag verbundenen personenbezogenen Daten für einen Zeitraum von insgesamt 30 Jahren sowie der pauschale Verweis auf handels-, steuer- und vertragsrechtliche Aufbewahrungspflichten den Anforderungen der DSGVO insoweit nicht genügt und aufgefordert, ein den datenschutzrechtlichen Vorgaben entsprechendes Löschkonzept vorzulegen. Das Verfahren war zum Zeitpunkt der Berichtsfassung noch nicht abgeschlossen.

13.3 Wohnungswirtschaft – häufige Fragestellungen

Einer der Themenbereiche, der von einer großen Anzahl an Beschwerden geprägt ist, ist die Wohnungswirtschaft. Akteure, wie beispielweise private oder institutionelle Vermieter, Wohnungseigentümergemeinschaften, Hausverwaltungen und Makler verarbeiten personenbezogene Daten von Mietinteressenten, Mietern und Wohnungseigentümern mitunter in einem sehr weitreichenden Umfang, so dass Konflikte vorprogrammiert sind, welche häufig als Beschwerden an das Datenschutzzentrum herangetragen werden.

Aufgrund der Komplexität der datenschutzrechtlichen Fragestellungen in diesem Wirtschaftsbereich und der Tatsache, dass die überwiegende Anzahl der datenverarbeitenden Stellen Privatpersonen oder kleine Unternehmen sind, ergeben sich in der Beratungs- und Prüfpraxis immer wieder erhebliche Probleme bei der Einhaltung und Umsetzung datenschutzrechtlicher Vorgaben.

Häufig treten Fragestellungen und Beschwerden im Zusammenhang mit dem Fragerecht des Vermieters auf. Gerade Vermieter und insbesondere Wohnungsgesellschaften verarbeiten eine Vielzahl personenbezogener Daten. Dies reicht von der Abfrage des Namens, der Kontaktdaten, des Geburtsdatums, der Anzahl der einziehenden Personen und der Bankverbindung bis hin zur Vorlage von Gehaltsnachweisen. Bei der Menge an erhobenen Daten scheint vielen nicht bewusst zu sein, dass nur solche Daten abgefragt werden dürfen, die für das Zustandekommen des Mietvertrages überhaupt erforderlich sind. Aufgrund der angespannten Wohnungsmarktsituation gerade in Großstädten können es sich Mieter aber nicht erlauben, die Beantwortung einzelner Fragen mit Hinweis auf den Datenschutz zu verweigern, da sie so zwangsläufig Gefahr laufen, aus dem potentiellen Bewerberkreis ausgeschlossen zu werden.

Bereits der 26. Tätigkeitsbericht enthält dazu im Kapitel 19 unter Verweis auf die diesbezügliche Orientierungshilfe „Einholung von Selbstauskünften bei Mietinteressenten“ detaillierte Ausführungen. Aufgrund des Wirksamwerdens der Datenschutz-Grundverordnung (DSGVO) zum 25. Mai 2018 wurde die Orientierungshilfe hinsichtlich der neuen Rechtlage überarbeitet und kann auf der Webseite des Datenschutzzentrums abgerufen werden.

Im Hinblick auf die in der Beratungs- und Prüfpraxis sichtbar geworden Problem- und Fragestellungen ist auch eine zeitnahe Veröffentlichung einer FAQ-Liste für den

Bereich Wohnungswirtschaft auf der Webseite des Datenschutzzentrums beabsichtigt.

Datenschutz bei Wohnungsinteressenten

In einem an das Datenschutzzentrum herangetragenen Sachverhalt wurde dem Beschwerdeführer eine Wohnungsbesichtigung verweigert, da er im Vorfeld keine Angaben zu seinem Einkommen machen wollte. Dem Vermieter wurde daraufhin mitgeteilt, dass zur Vereinbarung eines Besichtigungstermins die Abfrage des Namens, der Anschrift und der Kontaktdaten zulässig ist, von einer Erhebung weiterer Daten ist jedoch abzusehen bis der Betroffene im Anschluss an eine Wohnungsbesichtigung ernsthaftes Interesse an der Anmietung der Wohnung bekundet.

Auch wäre es zulässig, wenn sich der Vermieter im Rahmen des Besichtigungstermins den Personalausweis zur Identitätsfeststellung vorlegen lässt und dies handschriftlich vermerkt, wohingegen ein Abfotografieren des Personalausweises unzulässig ist, da hierdurch weit mehr Daten als für die Identitätsfeststellung erforderlich erhoben werden.

Konkrete Nachweise im Hinblick auf die Zahlungsfähigkeit des Mieters, wie beispielsweise Gehaltsnachweise, dürfen erst dann gefordert werden, wenn der Mietinteressent konkrete Mietabsichten geäußert hat und der Vermieter beabsichtigt, diesem die Wohnung zu vermieten, der Vertragsabschluss also unmittelbar bevorsteht. In diesem Zusammenhang wäre auch die Einholung einer Bonitätsauskunft über den Mietinteressenten zulässig, da der Vermieter ein berechtigtes Interesse daran hat, seine Wohnung nur an zahlungskräftige und –willige Mieter zu vermieten. Einer Einwilligung bedarf es hierfür nicht.

Weitergabe von Kontaktdaten an Handwerksbetriebe

Eine Fallkonstellation, die immer wieder für Unverständnis bei Mietern und Wohnungseigentümern sorgt, ist die Weitergabe von Kontaktdaten (Telefonnummer oder E-Mail) durch den Vermieter oder die Hausverwaltung an beauftragte Handwerksbetriebe im Falle anstehender Reparaturarbeiten.

Zwar ließe sich argumentieren, dass ein Mieter oder Wohnungseigentümer, der einen in seiner Wohnung liegenden Schaden beim Vermieter oder der Hausverwaltung meldet, selbst ein zwingendes Interesse daran hat, dass dieser Schaden möglichst zeitnah durch ein Fachunternehmen behoben wird, allerdings setzt dies nicht zwangsläufig die Weitergabe der Telefonnummer oder E-Mail-Adresse an den Handwerker voraus.

Grundsätzlich wäre es auch möglich, dass die Terminvereinbarung über den Vermieter oder die Hausverwaltung abgewickelt wird. Aus diesem Grund halten wir die Weitergabe der Telefonnummer an ein Handwerksunternehmen – mit der Ausnahme von Notfällen – nur dann zulässig, wenn der betroffene Mieter oder Eigentümer darin eingewilligt hat. Da die Einwilligung an keine Formvorgaben gebunden ist, wäre es beispielsweise möglich, den Mieter oder Eigentümer im Rahmen der telefonischen Schadensmeldung nach seiner Einwilligung zu fragen und dies zu dokumentieren.

Zusammenarbeit mit Ableseunternehmen

Im Rahmen der Erstellung der Nebenkostenabrechnung beauftragen Wohnungsgesellschaften und Vermieter zum Ablesen der Verbrauchszähler an Heizkörpern externe Ablesefirmen. Aufgabe dieser Unternehmen ist es, den erfassten Verbrauch an den in den Wohnräumen befindlichen Heizkörpern abzulesen und diese Werte an die Vermieter bzw. die Wohnungsgesellschaften zur Erstellung der Nebenkostenabrechnung zu übermitteln.

Hierzu wurde die Frage an hiesige Dienststelle herangetragen, auf welcher rechtlichen Grundlage die Datenübermittlung von Ableseunternehmen an Vermieter gestützt werden könne. Bei den in diesem Zusammenhang übermittelten Daten handelt es sich um personenbezogene Daten der Mieter, da diese eine Aussage über das Verbrauchsverhalten der einzelnen Parteien ermöglichen.

Allerdings wird das Ableseunternehmen hier lediglich als „verlängerter Arm" des Vermieters tätig. Über Zwecke und Mittel der Datenverarbeitung entscheidet einzig und allein der Vermieter, dem Ableseunternehmen kommt kein eigener Entscheidungsspielraum zu. Zwischen Vermieter und Ableseunternehmen ist vor diesem Hintergrund eine Vereinbarung über eine Auftragsverarbeitung im Sinne des Art. 28 DSGVO abzuschließen.

Verwalter einer Wohnungseigentümergemeinschaft sind keine Auftragsverarbeiter

Wiederholt wurde beim Datenschutzzentrum angefragt, ob zwischen Verwalter und einer Wohnungseigentümergemeinschaft ein Auftragsverarbeitungsverhältnis im Sinne des Art. 28 DSGVO vorliegt und dementsprechend eine Vereinbarung abzuschließen ist.

Der Verwalter im Sinne des Wohnungseigentumsgesetzes (WEG)[107] verarbeitet gestützt auf den Verwaltervertrag und auf Grundlage der Aufgabenzuweisung des WEG personenbezogene Daten in eigener Verantwortlichkeit, so dass keine für eine Auftragsverarbeitung sprechende Weisungsbefugnis seitens der Eigentümer angenommen werden kann.

Zudem ist das spezifische Verhältnis zwischen Wohnungseigentümer und Verwalter hierbei zu beachten. Der Verwalter ist selbst Organ der Wohnungseigentümergemeinschaft und handelt in deren Namen (Bundesgerichtshof, Beschluss vom 2.6.2005 – V ZB 32/05). Vor dem Hintergrund dieser Organeigenschaft des Verwalters ist vielmehr von einer (Gesamt-)Verantwortlichkeit der Wohnungseigentümergemeinschaft im datenschutzrechtlichen Sinne auszugehen, die den Verwalter ausdrücklich umfasst.

[107] Gesetz über das Wohnungseigentum und das Dauerwohnrecht vom 15.3.1951 (BGBl. I S. 175, ber. S. 209), zuletzt geändert d. Gesetz v. 5.12.2014 (BGBl. I S. 1962).

Funkbasierte Verbrauchserfassung an Heizkörpern

In zunehmenden Maße wenden sich Mieter mit der Frage an das Datenschutzzentrum, ob die Anbringung von fernauslesbaren Verbrauchserfassungsgeräten durch den Vermieter datenschutzrechtlich zulässig ist.

Bei Nachfrage, welche Informationen den beschwerdeführenden Mietern seitens des Vermieters im Rahmen des geplanten Einsatzes der Geräte zur Verfügung gestellt worden sind, wird zumeist mitgeteilt, dass lediglich auf die höchstrichterlich entschiedene Duldungspflicht verwiesen werde (Bundesgerichtshof (BGH), Urteil vom 28.9.2011 – VIII ZR 326/10). Diese Entscheidung des BGH ist im Ergebnis im Hinblick auf Vorgaben der Verordnung über die Heizkosten (HeizkostenVO)[108] – hier insbesondere § 4 Abs. 2 HeizkostenVO – zwar nachvollziehbar, jedoch befasst sich der BGH ausdrücklich nicht mit Fragen zur datenschutzrechtlichen Zulässigkeit der Erfassungsgeräte.

Auch die einer Mietpartei zuordenbaren Heizkosten sind grundsätzlich personenbezogene oder -beziehbare Daten im Sinne des Art. 4 Nr. 1 DSGVO, so dass für deren Verarbeitung der datenschutzrechtliche Regelungsrahmen maßgeblich ist und es grundsätzlich einer datenschutzrechtlichen Legitimationsgrundlage im Sinne des Art. 6 Abs. 1 DSGVO bedarf. Da der Gebäudeeigentümer nach § 4 Abs. 1 HeizkostenVO verpflichtet ist, den anteiligen Verbrauch der Nutzer an Wärme und Warmwasser zu erfassen, kann diese gesetzlich vorgeschriebene Verarbeitung der personenbezogenen bzw. -beziehbaren Verbrauchsdaten grundsätzlich auf Art. 6 Abs. 1 lit. c DSGVO gestützt werden.

Soweit die HeizkostenVO allein dem Gebäudeeigentümer die Auswahl der Art der Gebrauchserfassung überlässt, kann grundsätzlich auch eine funkbasierte Verbrauchserfassung an Heizkörpern zum Einsatz kommen.[109]

Da die heizkostenrechtlichen Regelungen – neben technischer Vorgaben in § 5 HeizkostenVO – über die Pflicht zur Erfassung des Verbrauchs hinaus jedoch keine spezifischen Vorgaben zur Verarbeitung der Verbrauchsdaten macht, ist für die Verarbeitung im Weiteren der Normenbestand der DSGVO maßgebend.

Um der Rechenschaftspflicht nach Art. 5 Abs. 2 und Art. 24 Abs. 1 DSGVO zu genügen, sind durch den datenschutzrechtlich verantwortlichen Gebäudeeigentümer vor Inbetriebnahme einer funkbasierten Verbrauchserfassung an Heizkörpern spezifische Vorkehrungen zu treffen.

Neben formalen Pflichten – wie beispielsweise die Aufnahme in das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO, Vorkehrungen zur Wahrung der Betroffenenrechte nach Art. 15 ff. DSGVO, der Abschluss einer Vereinbarung über Auftragsverarbeitung nach Art. 28 DSGVO mit dem beauftragten Ableseservice u. a. – sind von der Art der Verarbeitung abhängige technische und organisatorische Maßnahmen im Sinne der Art. 25 DSGVO und solche zur Datensicherheit im Sinne des Art. 32 DSGVO zu treffen.

---

[108] Verordnung über die verbrauchsabhängige Abrechnung der Heiz- und Warmwasserkosten in der Fassung der Bekanntmachung vom 5.10.2009 (BGBl. I S. 3250).

[109] § 4 Abs. 2 S. 2 HeizkostenVO sieht lediglich ein Mitspracherecht der Nutzer (Mieter) vor, sofern das Erfassungssystem vom Gebäudeeigentümer gemietet oder geleast wird.

Im Zusammenhang mit einer automatisierten Verbrauchserfassung ist vor allem zu gewährleisten, dass keine ständige Auslesung des nutzerspezifischen Verbrauchs stattfindet und damit die Gefahr einer Profilbildung im Raum steht. Zweckspezifisch ist für die Abrechnungszwecke eine einmal jährlich oder – im Fall des Nutzerwechsels – anlassbezogen stattfindende Auslesung der Verbrauchswerte ausreichend und durch organisatorische Festlegungen vorzusehen.

Ferner sind dem Gebot der Datenminimierung entsprechend auch keine über den zum Stichtag gegebenen Verbrauchswert und die jeweilige Nutzerkennung hinausgehenden Daten, die beispielsweise auf Lebensumstände der Nutzer schließen lassen, zu verarbeiten.

Gerade im Hinblick auf den Einsatz funkbasierter Geräte ist zudem durch geeignete technische Maßnahmen auszuschließen, dass Dritte unbefugt die Verbrauchswerte abrufen können.

Neben der heizkostenrechtlichen Mitbestimmung nach § 4 Abs. 2 S. 2 HeizkostenVO und der mietrechtlichen Ankündigungspflicht aus § 555a Abs. 2 Bürgerliches Gesetzbuch (BGB) ist der Einsatz einer funkbasierten Verbrauchserfassung gegenüber den betroffenen Mietern gerade auch datenschutzrechtlich transparent darzustellen.

Art. 13 DSGVO gibt diesbezüglich vor, welche Informationen im Einzelnen gegenüber den betroffenen Personen zu geben sind. Ungeachtet dessen, dass die Vorschrift eine Informationserteilung erst zum Zeitpunkt der konkreten Datenerhebung vorsieht, empfiehlt es sich, den Kreis der betroffenen Mieter zum frühestmöglichen Zeitpunkt über die geplante Umstellung der Erfassung, die in diesem Zusammenhang verarbeiteten Daten und die Ableseintervalle zu informieren.

Gerade für Vermieter, die Teil einer Wohnungseigentümergemeinschaft sind, gilt unter Bezugnahme auf die Entscheidung des Landgerichts Dortmund vom 28. Oktober 2014 – 9 S 1/14 zu beachten, dass hinsichtlich des Einsatzes von Geräten zur funkbasierten Verbrauchserfassung ein hinsichtlich der Verarbeitungszwecke konkretisierender Gemeinschaftsbeschluss erforderlich ist.

13.4 Digitalwirtschaft – GPS-gestütztes Ortungssystem zur Überwachung von Personen

Durch Berichterstattung in Presse und Rundfunk wurde das Unabhängige Datenschutzzentrum Saarland noch im Geltungszeitraum des alten Bundesdatenschutzgesetzes a. F. (BDSG a. F.) auf einen Anbieter von Ortungssystemen aufmerksam, der sich mit seinen Produkten insbesondere an private Endkunden richtete. Bei den Produkten handelte es sich um GPS-gestützte Ortungssysteme, die in drei Varianten angeboten wurden: Einerseits wurde ein Gerät angeboten, das in Fahrzeugen aller Art angebracht werden kann, daneben ein kleines mobiles Ortungsgerät und schließlich eine App mit Zugriff auf die Ortungsfunktion des jeweiligen Betriebssystems des Smartphones.

Problematisch an der Konzeption der Produkte war insbesondere deren Einsatzzweck; so warb der Anbieter ausdrücklich damit, dass mit seinen Lösungen Kinder

oder andere aufsichts- und hilfsbedürftige Personen überwacht werden können. Dem Kunden war es daher möglich, im Rahmen einer Echtzeitverfolgung den aktuellen Standort des Überwachten abzurufen und darüber hinaus ein zeitlich unbegrenztes Bewegungsprofil des Überwachten über eine Webplattform des Anbieters erstellen zu lassen. Dabei waren keine regelmäßigen Löschroutinen implementiert, vielmehr erfolgte eine Löschung der Daten erst mit Kündigung des Vertrages. Auch war der Zugriff der Mitarbeiter des Unternehmens auf die Positionsdaten der Überwachten nicht ausreichend eingeschränkt.

Festzustellen war zunächst, dass es sich bei den zum Zwecke der Ortung von Personen verwendeten Daten um personenbeziehbare Daten handelte, für die auch bereits nach alter Rechtslage das Datenschutzrecht Anwendung fand.

Selbige Einordnung muss nunmehr auch im Lichte der Datenschutz-Grundverordnung (DSGVO) gelten. Für die Überwachung der betroffenen Personen war dabei regelmäßig die Legitimationsgrundlage fraglich, da kein Hinweis bzw. Nachweis über die Einholung einer Einwilligung vorgelegen hat. An dieser Stelle sollte erwähnt werden, dass eine Rechtfertigung auf Grundlage berechtigter Interessen nicht infrage kam, denn die dauerhafte Überwachung einer betroffenen Person greift in schwerwiegendem Maße in dessen Rechte ein, insbesondere dann, wenn er sich der Überwachung womöglich nicht einmal bewusst ist. Eine derart umfassende Überwachung einer Person ist damit üblicherweise nur mit Einwilligung des Betroffenen als zulässig zu erachten.

Im Hinblick auf das geäußerte Votum des Datenschutzzentrums wurde sodann vom Anbieter die langfristige Protokollierung der Positionsdaten deaktiviert. Die Speicherdauer der Positionsdaten wurde auf maximal 5 Minuten begrenzt. Auch wurde sichergestellt, dass eine Überwachung Dritter nur stattfindet, wenn diese eine ausdrückliche und informierte Einwilligung in die Verarbeitung ihrer personenbezogenen Daten geben.

Für die Einwilligung von Kindern ist dabei eine Orientierung an den normativen Vorgaben des Art. 8 DSGVO naheliegend[110], mit der Folge, dass für Kinder, die das 16. Lebensjahr nicht vollendet haben, der Träger der elterlichen Verantwortung anstelle des betroffenen Kindes einwilligen kann, wenngleich eine solche Überwachung von Kindern mit Blick auf deren Persönlichkeitsrechte grundsätzlich abzulehnen ist.

13.5 Datenschutz im Verein

13.5.1 Beratung der Vereine

Das Wirksamwerden der Datenschutz-Grundverordnung (DSGVO) betraf nicht nur Unternehmen und den öffentlichen Sektor, sondern auch Vereine, die vielfach ausschließlich ehrenamtlich organisiert sind. Auch hier war die Verunsicherung hinsichtlich der neuen datenschutzrechtlichen Regelungen sehr groß. Ein weiterer Grund für

[110] *Karg*, in: BeckOK DatenschutzR (26. Ed. 1.11.2018) Art. 8 DSGVO, Rn. 42.

diese Verunsicherung war zudem, dass das Thema Datenschutz lange Zeit nicht im Fokus der Aufmerksamkeit der Verantwortlichen in den Vereinen lag und dadurch bereits ein gewisser Nachholbedarf hinsichtlich des Datenschutzes nach der alten Rechtslage bestand. Dies führte sodann zu einem erheblichen Anpassungsbedarf. Soweit jedoch die Vereine bereits die vor der DSGVO geltenden datenschutzrechtlichen Vorgaben beachtet hatten, waren für diese datenverarbeitenden Stellen vergleichsweise geringe Anpassungsmaßnahmen vorzunehmen und nur einige wenige, aber dennoch bedeutende Neuerungen (wie zum Beispiel die Informationspflichten) einzuführen.

Um die Vereine bei der Umsetzung der DSGVO zu unterstützen, hat das Unabhängige Datenschutzzentrum Saarland bereits zu Beginn des Jahres 2018 die Broschüre „Datenschutz im Verein" veröffentlicht,[111] in welcher die wesentlichen Punkte genannt werden, die bis zur Anwendung der DSGVO zwingend umgesetzt sein mussten.

Die wichtigsten Punkte werden nachstehend aufgeführt und kurz erläutert.

a) Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten

Nach Art. 30 DSGVO sind auch Vereine verpflichtet, ihre Datenverarbeitungsvorgänge in einem sog. Verzeichnis von Verarbeitungstätigkeiten zu dokumentieren. Dies betrifft beispielsweise Angaben darüber, welche Datenkategorien zu welchem Zweck verarbeitet werden, welcher Personenkreis Zugriff auf dieses Daten hat, an welche Empfänger die Daten weitergegeben und wie lange die Daten gespeichert werden. Verarbeitungstätigkeiten im Verein sind beispielsweise die Mitglieder- und Beitragsverwaltung, der Wettkampfbetrieb, die Organisation von Veranstaltungen, die Öffentlichkeitsarbeit, die Vornahme von Ehrungen, der Newsletterversand und vieles mehr. Das Verzeichnis ist schriftlich oder elektronisch zu führen und muss der Aufsichtsbehörde auf Verlangen vorgelegt werden. Ein Muster ist auf der Webseite der Aufsichtsbehörde abrufbar.[112]

b) Erstellung einer Datenschutzerklärung (Anpassung der Aufnahmeanträge)

Die DSGVO sieht vor, dass der von der Verarbeitung Betroffene im Zeitpunkt der Datenerhebung über die Datenverarbeitung umfassend zu informieren ist. (Art. 12 ff. DSGVO). Dies hat zur Folge, dass ein Verein in seinem Aufnahmeantrag eine Datenschutzerklärung aufnehmen muss, um so sicherzustellen, dass ein potentielles neues Mitglied den konkreten Umfang der Datenverarbeitung einschätzen kann. Die Informationspflichten ergeben sich hierbei aus Art. 13 DSGVO, wobei die in Abs. 1 genannten Angaben annähernd deckungsgleich zu den Angaben im Verzeichnis von Verarbeitungstätigkeiten sind. Im Einzelnen sind dies Angaben zum Verein als Verantwortlichem, ggf. zum Datenschutzbeauftragten, über die Zwecke und die Rechtsgrund-

[111] Elektronisch abrufbar auf der Internetpräsenz des Unabhängigen Datenschutzzentrums Saarland (https://datenschutz.saarland.de/themen/vereine/datenschutz-im-verein/).

[112] https://datenschutz.saarland.de/datenschutz/anwendungshinweise-dsgvo/verzeichnis-von-verarbeitungstaetigkeiten/.

lage der Datenverarbeitung, über das berechtigte Interesse an der Datenverarbeitung (wenn Art. 6 Abs. 1 S. 1 lit. f DSGVO Rechtsgrundlage der Verarbeitung ist), über die Empfänger der Datenverarbeitung sowie zur Übermittlung in ein Drittland. Darüber hinaus ist nach Art. 13 Abs. 2 DSGVO über die Betroffenenrechte zu informieren, wie beispielsweise die Rechte auf Auskunft, Berichtigung und Löschung. Ebenfalls muss auf das Beschwerderecht bei einer Datenschutzaufsichtsbehörde sowie auf die jederzeitige Widerrufsmöglichkeit einer Einwilligung ohne Angaben von Gründen hingewiesen werden. Sofern der Aufnahmeantrag in Papierform ausgehändigt wird, sollte die Datenschutzerklärung diesem vollständig als fester Bestandteil beigefügt werden.

c) *Der Datenschutzbeauftragte*

Es ist zu prüfen, ob ein Datenschutzbeauftragter bestellt werden muss. Dies ist u. a. dann der Fall, wenn mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten betraut sind. Letzteres bestimmt sich danach, ob die Datenverarbeitung nicht nur gelegentlich erfolgt, sondern sich aus den Aufgaben des Funktionsträgers zwangsläufig ergibt. Der Kassierer beispielsweise verarbeitet regelmäßig personenbezogene Daten, da er kontrolliert, ob die Mitglieder ihre Beiträge geleistet haben. Auch der Schriftführer, der zur Mitgliederversammlung einlädt oder die Niederschriften anfertigt, wird bei der Zählung zu berücksichtigen sein. Ebenso können auch der Jugendwart, einzelne Abteilungs-, Trainings- oder Übungsleiter in diesem Zusammenhang relevant sein, wenn sie beispielsweise regelmäßig per E-Mail mit Vereinsmitgliedern kommunizieren. Etwas anderes gilt jedoch, wenn der Jugendwart oder der Übungsleiter nur gelegentlich und unregelmäßig E-Mails versendet.

Selbst dann, wenn eine Pflicht zur Bestellung eines Datenschutzbeauftragten zu verneinen ist, kann es durchaus sinnvoll sein, einen zentralen Ansprechpartner für datenschutzrechtliche Fragen im Verein zu bestimmen, der für die Umsetzung der Anforderungen der DSGVO und des BDSG verantwortlich ist.

Ein Verein ist wie jede andere datenverarbeitende Stelle bei seiner Tätigkeit an die Vorgaben der DSGVO und des BDSG gebunden. Allerdings ergeben sich gerade im vereinsspezifischen Kontext einige besondere Datenverarbeitungsvorgänge, die einer kurzen Erläuterung bedürfen.

13.5.2 Veröffentlichung von Bildaufnahmen

Im Rahmen der Beratungstätigkeit wurde häufig die Frage gestellt, ob und ggf. unter welchen Voraussetzungen weiterhin Fotos von Veranstaltungen, Mitgliedern oder dem Vereinsleben veröffentlicht werden dürfen. Hiesigerseits wird die Auffassung vertreten, dass eine Veröffentlichung von Bildaufnahmen grundsätzlich auch ohne Einwilligung der abgebildeten Personen nach Art. 6 Abs. 1 S. 1 lit. f DSGVO zulässig

erfolgen kann, wobei immer die konkreten Umstände des Einzelfalls zu berücksichtigen (unproblematisch ist beispielsweise das Mannschaftsfoto von Erwachsenen; problematisch kann hingegen das Mannschaftsfoto von Minderjährigen sein, da abhängig von deren Alter die Einwilligung der Erziehungsberechtigten erforderlich sein kann). Bei der datenschutzrechtlichen Bewertung wird auch das Medium (Vereinswebseite oder gedruckte Vereinszeitschrift) und die Dauer der Veröffentlichung zu berücksichtigen sein, da online abrufbare Informationen einer potentiell unbegrenzten Anzahl an Personen zugänglich sind.

Weiterhin sind in jedem Fall die Informationspflichten nach Art. 12 ff. DSGVO zu erfüllen. Wird beispielsweise beabsichtigt, Spielszenen eines Fußballspieles zu veröffentlichen, müsste durch eine entsprechende Beschilderung an den Zugängen zum Sportplatz darauf hingewiesen werden. Auch zu diesem Aspekt hat unsere Dienststelle eine Handlungsempfehlung veröffentlicht, welche ebenfalls auf unserer Internetseite abrufbar ist.[113]

13.5.3 Betrieb von Webseiten

Um eine Vereinswebseite datenschutzrechtlich zulässig betreiben zu können, sind mehrere Punkte zu berücksichtigen:

- Sofern ein Verein auf seiner Webseite ein Kontaktformular anbietet, über das sich interessierte Personen bei dem Verein selbst oder bei einem Newsletter anmelden können, ist durch geeignete technische Maßnahmen zu gewährleisten, dass die Datenübermittlung sicher erfolgt. Eine dem Stand der Technik entsprechende Maßnahme ist hierbei die sog. SSL- bzw. TLS-Verschlüsselung, welche für Laien an dem in der Linkzeile aufgeführten „https" zu erkennen ist. Vereine, deren Webseite nicht über ein ausreichendes Sicherheitszertifikat verfügt, sollten sich mit ihrem Webhoster in Verbindung setzen und die Sicherheitslücke schnellstmöglich beheben.
- Selbst dann, wenn kein Kontaktformular oder keine Möglichkeit zur Newsletter-Anmeldung vorhanden ist, findet in den meisten Fällen eine Datenverarbeitung statt, die den meisten Webseitenbetreibern oftmals nicht bewusst ist. Bei einem Seitenabruf werden u. a. die IP-Adresse, der Zeitpunkt des Abrufs verarbeitet oder Tracking- und Analyticsverfahren verwendet. Auch hierbei handelt es sich um personenbezogene Daten. Der Webseitenbetreiber muss daher dafür Sorge tragen, dass er eine Datenschutzerklärung bereithält, die von jeder Unterseite seiner Webseite über einen Link abgerufen werden kann und auch die tatsächlich erfolgenden Verarbeitungen personenbezogener Daten umfasst.

[113] Elektronisch abrufbar unter: https://datenschutz.saarland.de/themen/vereine/datenschutz-im-verein/.

- Im Hinblick auf die Veröffentlichung von Fotos auf der Webseite ist das zuvor Gesagte zu berücksichtigen. Sofern Zweifel an der Rechtmäßigkeit der Veröffentlichung von Bildaufnahmen auf der Webseite bestehen, sollten sich Vereine über eine Einwilligung der Betroffenen rechtlich absichern.
- Das Einbinden von Social Plugins (d. h. die Einbindung von sozialen Plattformen) sollte nur dann erfolgen, wenn über ein sog. Double-Opt-In-Verfahren sichergestellt ist, dass der betroffene Webseitenbesucher in informierter Weise in die dahinterstehende Datenverarbeitung eingewilligt hat. Im Hinblick auf den Betrieb einer Facebook-Fanpage hat der Europäische Gerichtshof (EuGH) festgestellt, dass Facebook und Fanpage-Betreiber als gemeinsame Verantwortliche im Sinne des Art. 26 DSGVO anzusehen sind und daher eine schriftliche Vereinbarung zwischen beiden Parteien zu schließen ist, in der u. a. zu regeln ist, wer für die Erfüllung der Betroffenenrechte zuständig ist. [114] Die Datenschutzkonferenz hat sich zu diesem Thema in einer Entschließung und einem gemeinsamen Beschluss positioniert.[115]

13.5.4 Veröffentlichung von Jubiläen und Ehrungen in der Vereinszeitschrift

Die Aufsichtsbehörde wurde seitens einiger Vereine um eine rechtliche Einschätzung gebeten, ob es zulässig sei, Vereinsjubilare sowie Ehrungen in den Vereinszeitschriften zu veröffentlichen. Den Vereinen geht es hierbei oftmals um die Pflege eines guten mitgliedschaftlichen Miteinanders und der Wertschätzung der betroffenen Mitglieder. Nach hiesiger Auffassung kann die besagte Datenverarbeitung grundsätzlich nach Art. 6 Abs. 1 S. 1 lit. f DSGVO zulässig erfolgen. Unstrittig ist, dass der Verein ein berechtigtes Interesse daran hat, dass Verhältnis zu seinen Mitgliedern möglichst positiv zu gestalten. Hierzu kann u. a. gehören, besondere Leistungen einzelner Mitglieder zu honorieren oder auch zu Jubiläen zu gratulieren und hierüber vereinsöffentlich zu informieren. Voraussetzung hierfür ist aber einerseits, dass ein Verein im Rahmen seiner Informationspflichten die Mitglieder über dieses Vorgehen frühzeitig in Kenntnis setzt. Dies hat auch den praktischen Effekt, dass sich solche Mitglieder, die einer Veröffentlichung ihrer Daten weniger aufgeschlossen sind, ihre Bedenken beim Verein anmelden und damit einer Veröffentlichung zuvor kommen können. Ebenfalls ist dann darauf zu achten, dass die geplante Veröffentlichung als solche im Verzeichnis von Verarbeitungstätigkeiten dargestellt wird, da im Sinne des Zweckbindungsgrundsatzes personenbezogene Daten nur zu konkret festgelegten Zwecken verarbeitet werden dürfen.

---

[114] EuGH, Urteil vom 5.6.2018 – C-210/16, Rn. 39 ff. (zitiert nach juris); siehe auch Kap. 12, (Telemedien).

[115] Elektronisch abrufbar unter: https://datenschutz.saarland.de/datenschutz/datenschutzkonferenz/.

14 Direktmarketing

14.1 Werbeanrufe im B2C-Bereich – Generierung von vermeintlichen Einwilligungen im Rahmen von Gewinnspielen

Im Berichtszeitraum wurde das Unabhängige Datenschutzzentrum Saarland hinsichtlich unverlangter telefonischer Werbeanrufe durch ein saarländisches Versicherungsunternehmen eingeschaltet. Nach Aufforderung zur Stellungnahme machte das Unternehmen geltend, der Beschwerdeführer habe sich auf einer Website zur Teilnahme an einem Gewinnspiel angemeldet und in diesem Rahmen auch eine Einwilligung in die Verwendung seiner Telefonnummer für Zwecke des Direktmarketings erteilt. Als Beleg wurde eine Online-Registrierung vorgelegt, in welcher der Name, die Adresse und die Telefonnummer des Beschwerdeführers sowie das Eintragungsdatum mit einer IP-Adresse ersichtlich waren und eine Einwilligung in postalische und telefonische Werbung vermerkt war. Zusätzlich wurde auf ein (unausgefülltes) Formular der Website verwiesen, das eine Einwilligung durch Aktivieren einer Checkbox vorsah.

Hierauf hingewiesen, wies der Beschwerdeführer eine Gewinnspielteilnahme und die Erteilung einer Einwilligung in die Werbeansprache glaubhaft von sich. Auf den darauffolgenden Hinweis der Aufsichtsbehörde, dass der Beschwerdeführer nach eigener Aussage an besagtem Gewinnspiel nicht teilgenommen hat und dass die ohne weitere Authentifizierung erfolgende Eintragung von Daten in einem Webformular und Aktivierung einer Checkbox (sog. Single-Opt-In) auch ohne Weiteres missbräuchlich verwendet werden könne, legte das Versicherungsunternehmen eine erweiterte Online-Registrierung vor, in der zusätzlich eine E-Mail-Adresse und mit Zeitstempel und IP-Adresse versehene Angaben zur Aktivierung eines Bestätigungslinks aufgeführt waren. Das Unternehmen machte geltend, dass eine E-Mail an die eingetragene Adresse mit der Bitte um Bestätigung der Teilnahme gesendet worden sei, woraufhin eine solche Bestätigung des Beschwerdeführers durch Anklicken des in der Mail angegebenen Links erfolgt sei (sog. Double-Opt-In). Der Beschwerdeführer wandte dahingegen ein, die in der Online-Registrierung angegebene E-Mail-Adresse nicht zu kennen.

Im Rahmen der datenschutzrechtlichen Bewertung ist zunächst zu prüfen, ob eine Einwilligung gemäß Art. 6 Abs. 1 lit. a Datenschutz-Grundverordnung (DSGVO) für die in Frage stehende Verarbeitung für Zwecke des Direktmarketings von der betroffenen Person wirksam erklärt wurde.

Unabhängig davon, dass das Vorbringen der Beschwerdegegnerin durch die Vorlage zweier unterschiedlicher Online-Registrierungen aus Sicht der Aufsichtsbehörde bereits zweifelhaft ist, kann ein elektronisch durchgeführtes Double-Opt-In-Verfahren – selbst wenn man dieses vorliegend unterstellt – nach der Rechtsprechung des Bun-

desgerichtshofs (Urteil vom 10.2.2011– I ZR 164/09) ein tatsächlich fehlendes Einverständnis eines Verbrauchers in Werbeanrufen nicht ersetzen. Der BGH geht davon aus, dass der elektronisch – also bspw. per E-Mail – bestätigte Eingang eines Online-Formulars über die Teilnahme an einem Gewinnspiel mit Angabe einer Telefonnummer nicht als Nachweis des Anschlussinhabers für ein Einverständnis in Werbeanrufe ausreicht. In einem solchen Fall trägt der Werbende – jedenfalls soweit es sich um Telefonwerbung handelt – die Darlegungs- und Beweislast dafür, dass der Telefonanschluss der E-Mail-Adresse, unter der die Bestätigung abgesandt wurde, zuzuordnen ist. Nur für den Fall der E-Mail-Werbung könne durch ein sog. „Double-Opt-In-Verfahren" von einer hinreichenden Dokumentation einer Einwilligung ausgegangen werden, nicht aber für die vom Beschwerdegegner vorgenommene telefonische Werbung.

Diese vor dem Hintergrund eines wettbewerbsrechtlichen Sachverhalts getroffenen höchstrichterlichen Erwägungen lassen sich insoweit auch auf die rein datenschutzrechtliche Frage übertragen, inwiefern bei den über das Gewinnspiel generierten Einwilligungen von wirksamen Erklärungen der betroffenen Person im Sinne des Art. 4 Nr. 11 in Verbindung mit Art. 7 Abs. 1 DSGVO ausgegangen werden kann.

Aufgrund der bereits dargestellten Konzeption der Generierung von Einwilligungen im Rahmen des Gewinnspiels kann seitens des Webseitenbetreibers und der Versicherungsunternehmens nicht gewährleistet und von dem Verantwortlichen nicht zweifelsfrei nachgewiesen werden, dass tatsächlich die von der konkreten telefonischen Werbeansprache betroffene Person eine dahingehende Einwilligung in die Verwendung ihrer Telefonnummer für Zwecke des Direktmarketings erteilt hat. Das Verfahren begünstigt vielmehr, dass über das Webformular bspw. durch Dritte beliebig Telefonnummern betroffener Personen, unter anderem auch rechtsmissbräuchlich, eingetragen werden können.

Vor diesem Hintergrund kann nach Ansicht der Aufsichtsbehörde vorliegend nicht von einer wirksam erteilen Einwilligung der betroffenen Person im Sinne der DSGVO ausgegangen werden. Dies gilt im Übrigen gleichermaßen für weitere betroffene Personen, deren personenbezogene Daten über die Gewinnspiel-Website im Rahmen des beschriebenen Verfahrens generiert und von dem Beschwerdegegner für die telefonische Werbeansprachen verwendet werden. Folglich wurde seitens der Aufsichtsbehörde eine entsprechende Anordnung nach Art. 58 Abs. 2 lit. f DSGVO getroffen, mit dem Ziel, die Verwendung der über das Gewinnspiel generierten Kontaktdaten betroffener Personen für die telefonische Werbeansprache zu untersagen.

14.2 Werbeanrufe im B2C-Bereich – Werbeanrufe aufgrund zuvor eingeholter Informationen bei Bestandskunden im Rahmen der „Freundschaftswerbung“

Bereits unter Geltung der alten Rechtslage war problematisch, inwieweit bei Dritten oder Bestandskunden personenbezogene Daten über potenzielle Interessenten bzw. Neukunden erfragt und zu Werbezwecken verwendet werden dürfen. Nach Auffassung der Aufsichtsbehörden war Werbung anhand von bei Dritten erlangten Adressdaten nach dem Bundesdatenschutzgesetz a. F. (BDSG a. F.) unter Berücksichtigung des Direkterhebungsgrundsatzes und des Listenprivilegs in § 28 Abs. 3 S. 2 Nr. 1 BDSG a. F., welcher die Nutzung von Adressdaten zur Werbung nur dann erlaubte, wenn die Datenerhebung beim Betroffenen selbst oder aus allgemein zugänglichen Verzeichnissen erfolgte, unzulässig.

Nachdem sich der Direkterhebungsgrundsatz ebenso wenig wie das Listenprivileg in der Datenschutz-Grundverordnung (DSGVO) wiederfindet, stellte sich aufgrund einer Beschwerde einer von einer solchen Werbung betroffenen Person nunmehr die Frage, wie die sog. „Freundschaftswerbung“ nach der neuen Rechtslage zu beurteilen ist. In dem konkreten Fall wurden jedoch keine Postadressdaten, sondern Telefonnummern von potenziellen Neukunden bei Bestandskunden erfragt, um diese sodann zur telefonischen Kontaktaufnahme zu Werbezwecken zu nutzen.

Ausgangspunkt der Beurteilung sind die in der DSGVO normierten Grundsätze des Art. 5 DSGVO, wonach eine Verarbeitung personenbezogener Daten insbesondere rechtmäßig erfolgen muss, d. h. einer Rechtsgrundlage gemäß Art. 6 DSGVO bedarf.

Als Rechtsgrundlage kam vorliegend Art. 6 Abs. 1 lit. f DSGVO in Betracht, wonach eine Verarbeitung rechtmäßig ist, 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 überwiegen. Dabei war zu berücksichtigen, dass telefonische Werbeansprachen regelmäßig als belästigend und störend empfunden werden. Mithin ist im Rahmen der datenschutzrechtlichen Interessenabwägung auch die entsprechende wettbewerbsrechtliche Wertung zu beachten,[116] wonach die Werbung mit einem Telefonanruf gegenüber einem Verbraucher ohne dessen vorherige ausdrückliche Einwilligung gemäß § 7 Abs. 2 Nr. 2 Gesetz gegen den unlauteren Wettbewerb (UWG)[117] als unzumutbare Belästigung zu qualifizieren ist.

Im Rahmen der Gesamtabwägung kam die Aufsichtsbehörde schließlich zu dem Ergebnis, dass bei der Erhebung und Nutzung von bei Bestandskunden erfragten Telefonnummern zu Werbezwecken schutzwürdige Interessen betroffener Personen

[116] Vgl. hierzu eingehend die Ausführungen in Kap. 14.3 zur Frage der Zulässigkeit von Cold Calls im B2B- Bereich.

[117] Gesetz gegen den unlauteren Wettbewerb in der Fassung der Bekanntmachung vom 3.3.2010 (BGBl. I S. 254), zuletzt geändert d. Gesetz v. 17.2.2016 (BGBl. I S. 233).

überwiegen und diese Art der Werbeansprache damit auch nach neuer Rechtslage datenschutzrechtlich unzulässig ist. Dem Beschwerdegegner wurde die Rechtslage erläutert und Gelegenheit gegeben, seine Praxis der Neukundengewinnung an die datenschutzrechtlichen Erfordernisse anzupassen.

14.3 Werbeanrufe im B2B-Bereich – Rechtsprechung des Verwaltungsgerichts des Saarlandes zu Cold Calls

Bereits im 26. Tätigkeitsbericht wurde in Kapitel 18.2 (S. 159 ff.) über die aufsichtsbehördliche Bewertung von unverlangten Werbeanrufen durch ein saarländisches Unternehmen im B2B-Bereich berichtet.

Diese telefonischen Werbebotschaften waren u. a. an Zahnarztpraxen adressiert und erfolgten mit der Zielsetzung, den Adressaten eine Abnahmemöglichkeit für im Zusammenhang mit der zahnärztlichen Tätigkeit anfallenden Edelmetallabfälle anzubieten.

Das werbende Unternehmen stand bis zum Zeitpunkt des Werbeanrufs in keinem geschäftlichen Kontakt mit dem Adressaten des Anrufs und hatte die für die Werbeansprache genutzten Telefonnummern nach eigener Darlegung aus öffentlich zugänglichen Rufnummernverzeichnissen erhoben.

Nach aufsichtsbehördlicher Bewertung unter Zugrundelegung der bis zum 24. Mai 2018 geltenden Rechtslage konnte die verfahrensgegenständliche telefonische Werbeansprache jedoch nicht datenschutzrechtlich zulässig erfolgen.

Da keine Einwilligung der Betroffenen in die telefonische Werbeansprache vorgelegen hatte, war die datenschutzrechtliche Zulässigkeit nach § 28 Abs. 3 Bundesdatenschutzgesetz a. F. (BDSG a. F.) in Rückgriff auf wettbewerbsrechtliche Erwägungen zu prüfen.

Das Ergebnis der Bewertung war die datenschutzrechtliche Unzulässigkeit der praktizierten Marketingmaßnahme, so dass mit Bescheid vom 10. Januar 2017 deren Untersagung und die Löschung der rechtsgrundlos gespeicherten Daten angeordnet wurde. Gegen diese Anordnung klagte das werbende Unternehmen und wandte sich gegen die Auffassung der Aufsichtsbehörde.

Die Entscheidung des Verwaltungsgerichts

Mit Urteil vom 9. März 2018 – 1 K 257/17 hat das Verwaltungsgericht des Saarlandes die Klage abgewiesen und damit die aufsichtsbehördliche Rechtsauffassung bestätigt.

Im Einzelnen führt das VG in seiner Entscheidung aus, dass der Anwendungsbereich des BDSG a. F. eröffnet ist, da es sich bei den für Werbezwecke erhobenen und genutzten Daten der Praxisinhaber (Name, Vorname, Anschrift und Telefonnummer) um personenbezogene Daten im Sinne des § 3 Abs. 7 BDSG a. F. handelt, die ohne Einwilligung des Betroffenen für Werbezwecke nur nach Maßgabe des § 28 Abs. 3 S. 3 in Verbindung mit § 28 Abs. 3 S. 2 Nr. 1 BDSG a. F. verarbeitet werden dürfen, wenn

dem keine schutzwürdigen Interessen des Betroffenen im Sinne des § 28 Abs. 3 S. 6 BDSG a. F. entgegenstehen.

Die Schutzwürdigkeit der Interessen Betroffener wiegt dann schwer, wenn die konkrete Werbeansprache nach dem Gesetz gegen den unlauteren Wettbewerb (UWG) als unzumutbare Belästigung zu bewerten ist. Nach § 7 Abs. 2 Nr. Alt. 2 UWG ist eine telefonische Werbeansprache gegenüber einem sonstigen Marktteilnehmer dann unzumutbar, wenn nicht zumindest eine mutmaßliche Einwilligung des Betroffenen anzunehmen ist.

Unter Berücksichtigung der in diesem Zusammenhang maßgeblichen Rechtsprechung des Bundesgerichtshofs, kann nach Ansicht des Gerichts nicht von einer mutmaßlichen Einwilligung der betroffenen Zahnärzte ausgegangen werden, so dass die Werbeanrufe eine unzumutbare Belästigung in wettbewerbsrechtlicher Hinsicht darstellen. Somit sind die Werbeanrufe auch wegen entgegenstehender schutzwürdiger Interessen als datenschutzrechtlich unzulässig zu bewerten.

Weiterhin führt eine Auslegung der maßgebenden Regelungen „de lege ferenda", das heißt im Hinblick auf die Regelungen der zum damaligen Zeitpunkt zwar bereits in Kraft getretenen, aber noch nicht geltenden Datenschutz-Grundverordnung (DSGVO), zu keinem anderen Ergebnis. Nach Ansicht des Gerichts zeichnet sich zum Zeitpunkt der Entscheidung keine andere Bewertung des zu entscheidenden Sachverhalts nach der DSGVO ab, vor allem vor dem Hintergrund, dass die noch im Entwurfsstadium befindliche ePrivacy-Verordnung als lex specialis zur DSGVO spezifischere Regeln zum Telefonmarketing mit sich bringen wird.

Antrag auf Zulassung der Berufung

Mit Antrag auf Zulassung der Berufung wurde die Entscheidung des Gerichts seitens des Bevollmächtigten des werbenden Unternehmens aufgrund ernstlicher Zweifel an der Richtigkeit des Urteils und der grundsätzlichen Bedeutung der Rechtssache angegriffen.

Im Wesentlichen wurde dazu vorgetragen, dass die datenschutzrechtliche Zulässigkeit der Werbeanrufe ab 25. Mai 2018 ausschließlich nach Art. 6 Abs. 1 lit. f DSGVO zu bewerten ist und – im Hinblick auf den Vollharmonisierungsanspruch der DSGVO – wettbewerbsrechtliche Regelungen nach deutschem Recht keine oder allenfalls eine untergeordnete Rolle bei der Bewertung spielen.

Die Werbeanrufe seien überdies nach Art. 6 Abs. 1 lit. f DSGVO datenschutzrechtlich nicht zu beanstanden, da in Erwägungsgrund 47 *Direktwerbung* ausdrücklich als berechtigtes Interesse benannt wird und keine schutzwürdigen Interessen Betroffener ersichtlich seien, soweit die für die werbliche Kontaktaufnahme verwendeten Daten aus öffentlichen Quellen erhoben würden und die Zahnärzte lediglich im Rahmen ihrer beruflichen Tätigkeit angesprochen werden.

Aufsichtsbehördliche Erwiderung

Den Ausführungen im Zulassungsantrag war aus aufsichtsbehördlicher Perspektive vor allem im Hinblick auf die Rolle wettbewerbsrechtlicher Regelungen bei der datenschutzrechtlichen Bewertung entgegenzutreten.

§ 7 UWG stellt eine Vorschrift des deutschen Lauterkeitsrechts dar und ist die mitgliedstaatliche Umsetzung einer europarechtlichen Norm der Datenschutzrichtlinie für elektronische Kommunikation (Art. 13 Richtlinie 2002/58/EG; kurz: ePrivacy-Richtlinie). Diese Norm räumt dem mitgliedstaatlichen Gesetzgeber Gestaltungsspielräume ein, von denen der deutsche Gesetzgeber durch die Regelung des wettbewerbsrechtlichen Einwilligungsvorbehalts bei telefonischen Werbeansprachen auch Gebrauch gemacht hat.

UWG und die ePrivacy-Richtlinie bleiben nach wie vor neben der DSGVO wirksam. Die Richtlinie wird erst durch die geplante ePrivacy-Verordnung, die die DSGVO als lex specialis für den Bereich der elektronischen Kommunikation präzisieren und ergänzen soll, abgelöst werden. Dass der Verordnungsgeber eine Parallelwirkung von ePrivacy-Richtlinie – somit auch von Sonderwegen im nationalen Recht – und DSGVO mit den diesbezüglichen rechtlichen Unwägbarkeiten in der Übergangszeit in Kauf nimmt, wird überdies in Art. 95 DSGVO und dem damit korrespondierenden Erwägungsgrund 173 deutlich.

In Art. 16 Abs. 4 und 5 der aktuellen Entwurfsfassung der ePrivacy-Verordnung spiegelt sich zudem wider, dass der europäische Verordnungsgeber weiterhin mitgliedstaatliche Gestaltungsspielräume für das telefonische Direktmarketing gegenüber natürlichen und juristischen Personen durch Öffnungsklauseln für den nationalen Gesetzgeber ermöglicht. Dafür, dass der deutsche Gesetzgeber die Absicht verfolgt, die Legitimationsgrundlagen für die Zulässigkeit von Werbeanrufen nach Wirksamwerden der ePrivacy-Verordnung gänzlich neu zu regeln,[118] ergeben sich keine Anhaltspunkte. Vielmehr verfolgt die Bundesregierung in den aktuellen Verhandlungen zur ePrivacy-Verordnung das „Ziel, den Schutz vor unerwünschter Kommunikation so zu erhalten, wie er in der derzeit geltenden Regelung des Art. 13 der Richtlinie 2002/58/EG enthalten ist".[119] Es wird also davon auszugehen sein, dass der Regelungsgehalt des § 7 Abs. 2 Nr. 2 UWG auch in Zukunft wenigstens erhalten bleiben wird, wenn nicht sogar eine Verschärfung im Hinblick auf Direktwerbung gegenüber juristischen Personen forciert wird.[120]

Da im Übrigen auch eine rein mitgliedstaatliche Rechtslage die vernünftigen Erwartungen der betroffenen Person im Zusammenhang mit Maßnahmen der Datenverarbeitung prägt, wird auch insoweit das Argument des Vollharmonisierungsanspruchs der DSGVO faktisch konterkariert. Betroffene werden in Kenntnis des wettbewerbsrechtlichen Einwilligungsvorbehalts für Marketingmaßnahmen und in Ermangelung eines vorherigen geschäftlichen Kontaktes mit dem werbenden Unternehmen davon ausgehen, dass ohne eine erteilte Einwilligung oder Vorliegen einer zumindest mutmaßlichen Einwilligung im B2B-Bereich eine telefonische Werbeansprache unterbleibt.

---

[118] Beispielsweise wäre eine generelle Zulässigkeit von Werbeanrufen denkbar, bis die betroffene Person ihren Widerspruch erklärt (Opt-Out-Lösung), oder die Schaffung eines zentralen Registers, in das sich Betroffene eintragen lassen müssen um keine Werbeanrufe mehr zu erhalten.

[119] BT-Drs 19/6709, S. 4.

[120] *Köhler*, Die Regelung der „unerbetenen Kommunikation" in der ePrivacy-Verordnung und ihre Folgen für das UWG, WRP 2017, S. 1291 (1294).

Somit sind auch für die datenschutzrechtliche Bewertung nach Art. 6 Abs. 1 lit. f DSGVO Vorgaben nach dem UWG von entscheidender Bedeutung.

Über den Antrag auf Zulassung der Berufung war seitens des OVG zum Zeitpunkt der Berichtsfassung noch nicht entschieden.

Fazit

Art. 6 Abs. 1 lit. f DSGVO stellt im Zusammenspiel mit dem korrespondierenden Satz 7 des Erwägungsgrundes 47 gerade keinen Freibrief für kanalübergreifende Maßnahmen des Direktmarketings aus. Die oftmals in der Prüf- und Beratungspraxis anzutreffende Ansicht, dass mit der ausdrücklichen Erwähnung der Zwecke des Direktmarketing im besagten Erwägungsgrund eine besondere Privilegierung von Datenverarbeitungen für Werbezwecke einhergeht, ist nicht überzeugend. Vielmehr benennt der Verordnungsgeber – mangels eines spezifischen Normenbestands für den Bereich Direktmarketing im verfügenden Teil der DSGVO – dieses Verarbeitungsinteresse lediglich beispielhaft als legitim.

Vor dem Hintergrund des Vollharmonisierungsanspruchs und des technikneutralen Ansatzes der DSGVO ist Art. 6 Abs. 1 lit. f DSGVO von einem hohen Abstraktionsgrad geprägt und erfordert notwendigerweise eine komplexe Betrachtung des Verarbeitungskontexts und der Interessenlage.

Die teilweise in der Literatur[121] und auch regelmäßig in der Beratungspraxis vorzufindende Ansicht, dass nach Wirksamwerden der DSGVO wettbewerbsrechtliche Rahmenbedingungen aus § 7 UWG bei der nach Art. 6 Abs. 1 lit. f DSGVO vorzunehmenden Interessenabwägung angesichts des Vollharmonisierungsanspruchs nahezu unberücksichtigt bleiben müssten, ist aus aufsichtsbehördlicher Perspektive kritisch zu sehen.

Da die nach wie vor wirksame ePrivacy-Richtlinie und die in der zukünftigen ePrivacy-Verordnung vorgesehenen Öffnungsklauseln den Mitgliedstaaten für den Bereich des Direktmarketings Gestaltungsspielräume eröffnen, ist weiterhin eine Berücksichtigung wettbewerbsrechtlicher Maßgaben bei der datenschutzrechtlichen Bewertung unumgänglich.

Somit muss auch nach der geltenden Rechtslage bei der Bewertung der datenschutzrechtlichen Zulässigkeit der Datenverarbeitung für Zwecke des telefonischen Direktmarketings gegenüber einer natürlichen Person – ggf. auch im Zusammenhang mit deren beruflicher Tätigkeit oder wirtschaftlichen Betätigung – der wettbewerbsrechtliche Einwilligungsvorbehalt nach § 7 Abs. 2 Nr. 2 UWG Beachtung finden.

[121] Bspw. *Schulz*, in: Gola DS-GVO (2. Aufl. 2018), Art. 6 Rn. 73.

15 Videoüberwachung im nicht-öffentlichen Bereich

15.1 Neuer Regelungsrahmen für den Kameraeinsatz

Wie bereits in den vergangenen Jahren nahmen Videoüberwachungsmaßnahmen wieder einen erheblichen Teil des an das Datenschutzzentrum gerichteten Beschwerdevolumens ein. Nach wie vor ist die Bandbreite der Beschwerden nahezu unverändert und betrifft kameragestützte Überwachungsmaßnahmen an Privathäusern, die Überwachung von Mitarbeitern, Kameras in Verkaufsräumen und der Gastronomie sowie Einsätze von mobilen Kameras wie Dashcams oder bei Drohnen.

Mittlerweile thematisieren jedoch die mit Abstand meisten Beschwerden den Einsatz von Kameras im nachbarschaftlichen Umfeld. Im Berichtszeitraum wurden diesbezüglich über 120 Beschwerden an die Dienststelle adressiert.

Im Rahmen der Prüf- und Beratungspraxis ist auch im Berichtszeitraum festzustellen, dass datenschutzrechtliche Vorgaben im Zusammenhang mit dem Betrieb von Videokameras für eine erhebliche Anzahl an Verantwortlichen keine oder allenfalls eine untergeordnete Rolle spielen.

Ein möglicher Erklärungsansatz hierfür kann ggf. die Komplexität der datenschutzrechtlichen Bewertung, die ein Kameraeinsatz erfordert, sein.

Mit Wirksamwerden der Datenschutz-Grundverordnung (DSGVO) gilt auch für die Zulässigkeit von Videoüberwachungsmaßnahmen ein anderer rechtlicher Beurteilungsspielraum.

Da die Einwilligung der betroffenen Personen im Sinne des Art. 6 Abs. 1 lit. a DSGVO für kameragestützte Datenverarbeitungen, von wenigen Ausnahmen abgesehen,[122] keine geeignete Legitimationsgrundlage darstellt und Videoüberwachungsmaßnahmen lediglich bereichsspezifisch gesetzlich angeordnet und somit auf Grundlage des Art. 6 Abs. 1 lit. c DSGVO betrieben werden,[123] stellt Art. 6 Abs. 1 lit. f DSGVO seit dem 25. Mai 2018 nunmehr die datenschutzrechtliche Richtschnur für Verantwortliche, die personenbezogene Daten unter Zuhilfenahme von stationären oder mobilen Kameras verarbeiten, dar.

Wie auch nach der bisherigen Rechtslage ist bei der Prüfung einer Überwachungsmaßnahme nach Art. 6 Abs. 1 lit. f DSGVO auf ein berechtigtes Interesse des Verantwortlichen, wie beispielsweise Einbruchs- oder Vandalismusprävention, abzustellen.

---

[122] Beispielsweise kann der Einsatz von Drohnen über Privatgrundstücken nur mit der Einwilligung der Verfügungsberechtigten (z. B. der Eigentümer) legitimiert werden.

[123] Die Videoüberwachung in Kassenbereichen von Banken und innerhalb von Spielhallen ist durch Unfallverhütungsvorschriften gesetzlich vorgeschrieben.

Neu ist jedoch, dass auch berechtigte Interessen Dritter für den Kamerabetreiber von Belang sein können. Typischerweise wird so beispielsweise der Betreiber eines Einkaufszentrums, der Ladenflächen an Dritte vermietet, auch im Hinblick auf die Interessen der Mieter eine Videoüberwachung zur Vermeidung von Diebsstählen oder zur Täterermittlung einsetzen können.

Weiterhin muss die Videoüberwachung zur Wahrung eines berechtigten Interesses erforderlich sein und es dürfen schutzwürdige Interessen der betroffenen Personen nicht überwiegen.

Nicht erforderlich ist beispielsweise eine Videoüberwachung des öffentlichen Verkehrsraums vor einem Gebäude, wenn der Zweck des Kameraeinsatzes der Schutz der Hausfassade vor Vandalismusschäden ist. Hier reicht die Beschränkung der Überwachung auf einen spezifischen Toleranzbereich vor der Fassade.

Für das schutzwürdige Interesse ist auch im Hinblick auf Erwägungsgrund 47 der DSGVO die Erwartungshaltung der betroffenen Personen mit zu berücksichtigten. Insoweit sind bestimmte Bereiche regelmäßig nach wie vor für Kameras ein Tabu (wie beispielsweise gastronomisch genutzte Bereiche, Ruhe-/Wartezonen, Umkleiden, Toiletten u. a.).

Neben Art. 6 Abs. 1 lit. f DSGVO ist § 4 Bundesdatenschutzgesetz n. F. (BDSG n. F.) als mitgliedstaatliches Recht zu beachten, der die Vorgängerregelung des § 6b BDSG a. F. in der bis 25. Mai 2018 geltenden Fassung nahezu wortgleich fortleben lässt.[124]

Soweit Beschäftigte von einer Videoüberwachungsmaßnahme betroffen sind, sind ferner die Vorgaben des § 26 BDSG maßgeblich. Da gerade im Bereich der Videoüberwachung von Beschäftigten immer wieder Einwilligungserklärungen der Betroffenen eingeholt und vorgelegt werden, ist im Hinblick auf die normativen Vorgaben des § 26 Abs. 2 BDSG zu beachten, dass die Freiwilligkeit dieser Einwilligung der Mitarbeiter in ihre eigene Überwachung regelmäßig in Zweifel zu ziehen ist.

Videoüberwachungsmaßnahmen stellen regelmäßig Verfahren der automatisierten Datenverarbeitung dar, so dass der verantwortliche Betreiber der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO unterliegt.

Unter anderem ist der Kameraeinsatz somit zum Gegenstand des Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 DSGVO zu machen und des Weiteren sind Vorkehrungen zur Wahrung der Betroffenenrechte nach Art. 15 ff. DSGVO zu treffen. Wenn zudem beispielsweise ein Sicherheitsunternehmen mit der Durchführung der Videoüberwachung betraut ist, ist eine Vereinbarung über eine Auftragsverarbeitung im Sinne des Art. 28 DSGVO abzuschließen.

Darüber hinaus sind technische und organisatorische Maßnahmen im Sinne des Art. 25 und des Art. 32 DSGVO zu ergreifen. Neben der zeitlichen Beschränkung des Einsatzes von Kameras, sind seitens des Verantwortlichen alle Möglichkeiten auszuschöpfen, die eine datenschutzfreundliche Ausgestaltung der Überwachungsmaßnahme gewährleisten. Abgesehen werden sollte beispielsweise regelmäßig von

[124] Ob der deutsche Gesetzgeber überhaupt befugt war, eine eigene Vorschrift zur Videoüberwachung durch nicht-öffentliche Stellen ins BDSG aufzunehmen, ist zurzeit Gegenstand eines Diskurses.

schwenkbaren Kameras oder solchen mit Zoomfunktion. Auch sollten Audioaufnahmen und eine ungesicherte drahtlose Übertragung von Bilddaten grundsätzlich technisch ausgeschlossen sein. Ferner sind neben dem selbstverständlichen Schutz vor unberechtigten Zugriffen auf die Überwachungsinfrastruktur bzw. auf die mit ihrer Hilfe gespeicherten personenbezogenen Daten und der Regelung von Zugriffsrechten, voreingestellte Passwörter zu ändern und die Komponenten regelmäßig mit Sicherheitsupdates zu versorgen.

Um dem Transparenzgebot der DSGVO gerecht zu werden, sind betroffene Personen im Sinne des Art. 13 DSGVO über die Videoüberwachung zu informieren. Da die Vorschrift einen erheblichen Informationsumfang verpflichtend vorgibt, kann dabei grundsätzlich auch gestuft informiert werden; durch Anbringung von Hinweisbeschilderung an exponierten Stellen sind den von der Videoüberwachung betroffenen Personen die Basisinformationen nach Art. 13 Abs. 1 DSGVO zur Verfügung zu stellen und die Möglichkeit des Erhalts weiterer Informationen, beispielsweise durch ein weiteres Hinweisschild an zentraler Stelle mit allen Informationen nach Art. 13 Abs. 1 und 2 DSGVO oder durch Verweis auf eine Webseite mit entsprechender Datenschutzerklärung mittels QR-Code, aufzuzeigen.[125]

Um den Anwendern von Videoüberwachungsmaßnahmen eine Hilfestellung zur Bewertung von Videoüberwachungsmaßnahmen zu geben, hat die Datenschutzkonferenz (DSK) das Kurzpapier Nr. 15 veröffentlicht, welches auf der Webseite des Datenschutzzentrums abgerufen werden kann.[126] Daneben werden durch die DSK zeitnah weitere Veröffentlichungen zum Thema Videoüberwachung erfolgen.

15.2 Datenschutzrechtliche Bewertung von Kameras in einer Apotheke

Der Fall von in einer Apotheke installierten Videoüberwachungskameras beschäftigte das Unabhängige Datenschutzzentrum Saarland erstmals im Jahr 2014 und fand seinen Abschluss im Berichtszeitraum mit einer Entscheidung des Oberverwaltungsgerichts des Saarlandes vom 14. Dezember 2017 – 2 A 662/17. Hinsichtlich der aufsichtsbehördlichen Bewertung der Videoüberwachungsmaßnahme kann auf den 25. Tätigkeitsbericht (Kap. 19.8 S. 124 ff.) und hinsichtlich einer detaillierten Darstellung der erstinstanzlichen Entscheidung des Verwaltungsgerichts des Saarlandes auf die Ausführungen im 26. Tätigkeitsbericht (Kap. 15.4 S. 129 ff.) Bezug genommen werden.

Zusammengefasst folgte das VG in seiner Entscheidung vom 29. Januar 2016 – 1 K 1122/14 dabei im Hinblick auf die im Verkaufsraum (Offizin) stattfindende Video-

[125] Entwürfe für derartige Hinweisschilder können auf der Webseite des Datenschutzzentrums unter https://datenschutz.saarland.de/themen/videoueberwachung/ abgerufen werden.

[126] https://datenschutz.saarland.de/fileadmin/datenschutz/ds-gvo/kurzpapiere/dsk_kpnr_15.pdf.

überwachung der Auffassung des Datenschutzzentrums. Danach war die Überwachungsmaßnahme in diesem Bereich weder zur Wahrnehmung des Hausrechts erforderlich (§ 6b Abs. 1 Nr. 2 Bundesdatenschutzgesetz a. F. (BDSG a. F.) noch wurde klägerseitig ein berechtigtes Interesse (§ 6b Abs. 1 Nr. 3 BDSG a. F.) ausreichend dargelegt.

Die im nur für Mitarbeiter zugänglichen Teil der Apotheke installierte Kamera zur Überwachung des Betäubungsmittelschranks erachtete das Gericht jedoch mit Verweis auf die nachträglich vorgelegten Einwilligungen der Beschäftigten als zulässig und hob den Bescheid der Aufsichtsbehörde dahingehend auf.

Da nach unserer Auffassung sowohl die Umstände, die gegen eine Wirksamkeit der von den Beschäftigten erklärten Einwilligung sprechen, als auch die formalen Anforderungen des § 4a Abs. 1 S. 2 BDSG a. F. in der verwaltungsgerichtlichen Entscheidung nicht in ausreichendem Maße Beachtung fanden, wurde von unserer Behörde im März 2016 ein Antrag auf Zulassung der Berufung beim OVG gestellt. Auch der Apothekenbetreiber stellte einen solchen Antrag im Hinblick auf die erstinstanzlich verneinte Zulässigkeit der Videoüberwachung im Verkaufsraum.

Nachdem beide Berufungsanträge durch das OVG mit Beschluss vom 7. August 2017 zugelassen wurden, hob das OVG schließlich mit Urteil vom 14. Dezember 2017 die Entscheidung der Vorinstanz in dem vom Apothekenbetreiber beantragten Umfang auf und wies die Berufung des Datenschutzzentrums zurück.

Das Berufungsgericht sieht in der streitgegenständlichen Videoüberwachung sowohl in der Offizin, als auch in dem nur den Mitarbeitern zugänglichen Teil der Apotheke keinen datenschutzrechtlichen Verstoß.

Wesentliche Elemente der Entscheidung des OVG

Nach der Bewertung des OVG ist die Überwachung in der Offizin sowohl zur Wahrnehmung des Hausrechts als auch zur Wahrnehmung berechtigter Interessen des Apothekers erforderlich. Das Gericht bejaht – entgegen der erstinstanzlichen Auffassung – für den Verkaufsraum eine konkrete Gefährdungslage, mit Verweis auf die angeführten, jedoch unbelegt gebliebenen Inventurdifferenzen. Auch spreche nach Ansicht des Gerichts die im Rahmen einer Ortsbesichtigung festgestellte Ausgestaltung und hohe Kundenfrequentierung des Selbstbedienungsbereichs (Verkaufsregale, die leicht „abgeräumt" werden können), für eine Gefährdungslage im Hinblick auf Diebstähle durch Kunden. Zudem gehe, so die Auffassung des Gerichts, mit der verfahrensgegenständlichen Videoüberwachung kein erheblicher Eingriff in das informationelle Selbstbestimmungsrecht der Kunden einher, so dass die Abwägung mit dem Überwachungsinteresse des Apothekeninhabers kein Überwiegen schutzwürdiger Interessen Betroffener zum Ergebnis haben könne.

Auch die Videoüberwachung des nur für Mitarbeiter zugänglichen Bereichs vor dem unverschlossenen Betäubungsmittelschrank sieht das Berufungsgericht aufgrund der Erforderlichkeit zur Durchführung des Beschäftigungsverhältnisses und der wirksam erteilten Einwilligungen der Beschäftigten als zulässig an.

Das OVG macht sich in diesem Zusammenhang die Argumentation des Apothekenbetreibers zu Eigen und hält einen Anfangsverdacht wegen Diebstahls durch einen

oder mehrere Beschäftigte für gerechtfertigt. Im Hinblick auf das Überwachungsinteresse des Arbeitgebers sei der Eingriff in das Recht auf informationelle Selbstbestimmung der Beschäftigten aufgrund der nur kurzzeitigen Aufenthaltsdauer im überwachten Bereich zudem als vergleichsweise gering anzusehen, so dass im Ergebnis keine schutzwürdigen Interessen der Überwachung entgegenstehen.

Anders als die Aufsichtsbehörde zieht das OVG die Freiwilligkeit der Einwilligung nicht in Zweifel und ist der Auffassung, dass Beschäftigte bei Verweigerung oder Widerruf der Einwilligung nicht befürchten müssen, Nachteile im Beschäftigungsverhältnis zu erfahren oder gar als tatverdächtig stigmatisiert zu werden. Das Gericht begründet seine Einschätzung damit, dass Arbeitnehmer nicht zur Erteilung der Einwilligung verpflichtet seien und eine aufgrund einer Verweigerung erfolgende Benachteiligung eine arbeitgeberseitige Pflichtverletzung darstellen würde.

Ferner stößt auch die inhaltliche Ausgestaltung der Einwilligungserklärung beim Gericht auf keine Bedenken. Ungeachtet dessen, dass nach aufsichtsbehördlicher Auffassung der vom Arbeitgeber vorgegebene Erklärungstext dem Arbeitnehmer in keiner Weise eine informierte Einwilligung ermöglicht, war nach Ansicht des Berufungsgerichts von einer hinreichend bestimmten Einwilligung und einer ausreichenden Information der Beschäftigten auszugehen, die den Anforderungen des § 4a Abs. 1 S. 2 und 3 BDSG a. F. genügt.

Kritische Würdigung der Entscheidung des OVG

Das Urteil ist unserer Auffassung nach nicht nur im Hinblick auf Arbeitnehmerinteressen als kritikwürdig zu bezeichnen, sondern gerade auch in datenschutzrechtlicher Hinsicht, soweit wesentliche Grundsätze und Gebote des Datenschutzrechts keine ausreichende Berücksichtigung gefunden haben.

Trotz der für datenverarbeitende Stellen gegebenen Verpflichtung eindeutige Zwecke festzulegen, wurde weder im aufsichtsbehördlichen Verwaltungsverfahren noch im gerichtlichen Verfahren von dem Apothekenbetreiber eine solche schriftliche Dokumentation über die Zwecke der Überwachungsmaßnahme zur Verfügung gestellt. Ein Verfahrensverzeichnis im Sinne des § 4e BDSG a. F., in dem notwendigerweise konkrete Überwachungszwecke zu fixieren gewesen wären, wurde von dem Apothekenbetreiber ausdrücklich nicht erstellt und noch in der mündlichen Verhandlung als „Förmelei" bezeichnet.

Damit ging einher, dass im Berufungsverfahren je nach Verfahrensstand verschiedenste Überwachungszwecke aufgezählt und unterschiedliche Personengruppen für Entwendungen verantwortlich gemacht wurden.

Während initial Inventurdifferenzen, für welche der Apotheker ausdrücklich nicht die Mitarbeiter, sondern Drogenabhängige verantwortlich gemacht hat, als Anlass für die Überwachung genannt wurden, wurden zu einem späteren Zeitpunkt Diebstähle im Verkaufsraum durch Kunden, danach vorrangig Entwendungen durch Mitarbeiter und schließlich der Schutz der Mitarbeiter vor Überfällen angeführt.

Das Berufungsgericht ging somit im Weiteren von einer Gefährdungslage aus, ohne dass von dem Apothekenbetreiber eine detaillierte und aussagekräftige Schadensdokumentation vorgelegt wurde, die hinreichend belegt, welche Art von Vermögens-

schäden zu welchem Zeitpunkt an welchem Ort eingetreten sind, oder nachvollziehbare Anhaltspunkte für einen gegen Personen oder Personengruppen gerichteten Tatverdacht vorgetragen worden wären.

Weiterhin war die Überwachungsanlage offenkundig auch nicht geeignet, überhaupt Tathandlungen zu dokumentieren. Obwohl die streitgegenständlichen Kameras zum Zeitpunkt der behaupteten Inventurdifferenzen und des angeführten Betäubungsmittelverlustes im Einsatz waren, konnte mithilfe der Videokameras kein konkreter Tatverdacht begründet oder ein Tatzeitpunkt eingegrenzt werden. Den sich vor diesem Hintergrund aufdrängenden Zweifeln an der Geeignetheit der Überwachungsmaßnahme zur Dokumentation von Diebstählen oder zur Täteridentifizierung konnte sich das Gericht jedoch nicht anschließen.

Gleiches gilt für die mögliche und nach der Betäubungsmittelverordnung auch rechtlich gebotene Beschränkung des Zugriffs auf den Betäubungsmittelschrank auf wenige ausgewählte Mitarbeiter zur Vermeidung ungerechtfertigter Entnahmen, insoweit das Gericht darin keine Alternative zur eingriffsintensiveren Videoüberwachung erkennen konnte.

Auch die gerichtliche Bewertung der nachträglich im Verfahren vorgelegten Einwilligungserklärungen der Mitarbeiter als wirksame Legitimationsgrundlage für die Videoüberwachung konnte vor dem Hintergrund nicht überzeugen, als die Auswirkungen des strukturellen Ungleichgewichts im konkreten Verhältnis zwischen Arbeitnehmer und Arbeitgeber auf die Wirksamkeit der abgegebenen Einwilligung nicht ausreichend berücksichtigt wurden.

Den Ausführungen beider Instanzen zur Zulässigkeit von Einwilligungserklärungen im Beschäftigungsverhältnis kann dahingehend zugestimmt werden, dass diese nicht per se als datenschutzrechtliche Legitimationsgrundlage ausgeschlossen sind. Weder dem Gesetz selbst noch dem strukturellen Machtungleichgewicht zwischen Arbeitnehmer und Arbeitgeber an sich kann ein genereller Ausschluss der Möglichkeit der wirksamen Einwilligung im Beschäftigungsverhältnis entnommen werden. Nichts anderes ergibt sich unter Berücksichtigung der Rechtsprechung des Bundesarbeitsgerichts (Urteile vom 11. Dezember 2014 – 8 AZR 1010/13 und 19. Dezember 2015 – 8 AZR 1011/13). Jedoch ist bei Abgabe von Einwilligungserklärungen im Arbeitsverhältnis grundsätzlich eine konkrete Betrachtung geboten, ob die Umstände des Einzelfalls gegen eine Freiwilligkeit bei der Abgabe der Einwilligungserklärung sprechen und diese als Legitimationsgrundlage ausscheiden lassen.

Im zu entscheidenden Fall standen die Beschäftigten vor der Wahl, entweder die Einwilligung in die eigene Überwachung zu erklären oder sich durch die Verweigerung der Einwilligung als Tatverdächtige zu stigmatisieren. Eine in Anbetracht berechtigter Bedenken gegen die Videoüberwachung des Arbeitgebers verweigerte Einwilligung eines Mitarbeiters oder deren Widerruf hätte angesichts der zuletzt im Verfahren geäußerten Verdachtsmomente des Arbeitsgebers somit dazu führen können, dass der Arbeitnehmer erhebliche Nachteile im Arbeitsverhältnis befürchten muss.

Sobald zudem ein einziger betroffener Arbeitnehmer seine Einwilligung verweigert oder widerruft, kann die Einwilligung nicht länger als datenschutzrechtliche Legiti-

mationsgrundlage für die Überwachungsmaßnahme in ihrer Gesamtheit herangezogen werden.[127] Dementsprechend kann auch bezüglich der Folgen der Weigerung oder des Widerrufs der Einwilligung nicht davon ausgegangen werden, dass für die betroffenen Beschäftigten faktisch eine freie Wahlmöglichkeit besteht.

Auch entsprachen die im verwaltungsgerichtlichen Verfahren nachgereichten Einwilligungserklärungen inhaltlich nicht den datenschutzrechtlichen Vorgaben. Weder wurde der intendierte Zweck (die Überwachung der Mitarbeiter im Hinblick auf Entwendungen) noch die konkrete Ausgestaltung der Überwachungsmaßnahme (Löschfristen, zugriffsberechtigte Personen, Umstände der Auswertung etc.) oder ein Hinweis auf die Folgen der Verweigerung der Einwilligung und die damit verbundene Fortsetzung der Überwachung auf Grundlage einer anderen rechtlichen Grundlage in der textlich knappen Erklärung benannt oder gar erläutert.

Davon, dass die Beschäftigten in voller Kenntnis der Sachlage eine freie Entscheidung hätten treffen können, kann somit nicht die Rede sein.

Fazit

Aus aufsichtsbehördlicher Sicht ist die Entscheidung des OVG des Saarlandes nicht überzeugend, insoweit grundsätzliche datenschutzrechtliche Gebote bei der Entscheidungsfindung erkennbar keine oder eine untergeordnete Rolle gespielt haben und Einwilligungserklärungen von Beschäftigten als valide und geeignete datenschutzrechtliche Legitimationsgrundlage für deren Überwachung bewertet werden.

Trotz des erfolgten Hinweises im Berufungsverfahren fand zudem bei der Entscheidungsfindung durch das Gericht die ab 25. Mai 2018 geltende Rechtslage keinen Eingang. Zur Frage nach der Wirksamkeit von Einwilligungserklärungen im Beschäftigungsverhältnis macht § 26 Abs. 2 BDSG normative Vorgaben, die ausdrücklich gegen die Freiwilligkeit der Einwilligungserklärungen im entschiedenen Sachverhalt sprechen.

Vor diesem Hintergrund ist nicht überraschend, dass ein erstes Verwaltungsgericht der Praxis der Einholung von Einwilligungserklärungen von Beschäftigten nach der neuen Rechtslage einen Riegel vorgeschoben hat (Verwaltungsgericht Stuttgart, Urteil vom 12. Juli 2018 – 11 K 6401/16). Das Verwaltungsgericht bewertet einen in diesem Zusammenhang vergleichbaren Sachverhalt der kameragestützten Mitarbeiterüberwachung vollkommen gegensätzlich und verneint die Wirksamkeit der Einwilligungserklärungen von Mitarbeitern und die datenschutzrechtliche Zulässigkeit einer anlasslosen Videoüberwachung von Beschäftigten.

15.3 Wildkameras

Im 26. Tätigkeitsbericht wurde unter Kapitel 15.9. dargestellt, dass das Unabhängige Datenschutzzentrum Saarland unter Zugrundelegung der damaligen Rechtslage von einer Meldepflicht im Falle des Betriebs von Wildbeobachtungskameras ausging und

[127] *Ziehbarth*, Anmerkung zu OVG Saarlouis – 2 A 662/17, MMR 2018 S. 259 (263).

vor diesem Hintergrund drei Jäger vor dem Verwaltungsgericht des Saarlandes auf Feststellung klagten, dass insbesondere im Bereich von Kirrungen eine entsprechende Meldepflicht nicht bestehe.

Nachdem das Verwaltungsgericht die Auffassung der Aufsichtsbehörde, dass sich eine Meldepflicht der Kamerabetreiber aus § 4d Abs. 1 Bundesdatenschutzgesetz a. F. (BDSG a. F.) ergibt, bestätigt und die Klage abgewiesen hatte, beantragten die Kläger die Zulassung der Berufung, welche durch das Oberverwaltungsgericht des Saarlandes (OVG) wegen der Bedeutung der Rechtssache zugelassen wurde.

Im Berichtszeitraum schließlich wies das OVG mit Urteilen vom 14. September 2017 (2 A 216/16; 2 A 197/16; 2 A 213/16) die Berufungen zurück und bestätigte die Entscheidungen des VG.

Hierfür war unter anderem entscheidend, dass es sich bei der Beobachtung von Kirrungen mittels entsprechender Tierbeobachtungskameras nach Ansicht des Gerichts um keine ausschließlich private Tätigkeit handelt. Denn nur dann wäre die Anwendbarkeit des BDSG a. F. nach der Haushaltsausnahme des § 1 Abs. 2 Nr. 3 2. Halbsatz BDSG a. F. ausgeschlossen gewesen. Obergerichtlich wurde die Auffassung bestätigt, dass es sich bei den erfassten Kirrungen um öffentlich zugängliche Räume im Sinne des § 6b BDSG a. F. handelt, da diese einerseits faktisch uneingeschränkt betretbar sind und sich aus ihrer Gestaltung auch nicht klar ergebe, dass es sich um eine nicht zu betretende Fläche handelt. Weiterhin folge die Notwendigkeit einer präventiven datenschutzrechtlichen Überprüfung bereits daraus, dass nicht ausgeschlossen werden kann, dass von den Wildkameras der an die Kirrung angrenzende Waldbereich erfasst wird. Das OVG wies in seinen Urteilen unter Bezugnahme auf die Kritik der Kläger an dem durch die Meldepflicht veranlassten Verwaltungsaufwand schließlich darauf hin, dass die Meldepflicht nach § 4 d BDSG a. F. mit Geltung der Datenschutz-Grundverordnung (DSGVO) zum 25. Mai 2018 entfallen und durch eine Dokumentationspflicht ersetzt werden wird.

Die Revision wurde durch das OVG nicht zugelassen, wogegen die Kläger Beschwerde beim Bundesverwaltungsgericht (BVerwG) erhoben. Dieser Beschwerde wurde nicht abgeholfen. Mit Beschluss vom 25. April 2018 führte das BVerwG hierzu aus, dass – wie vom OVG zutreffend dargestellt – es sich bei der Meldepflicht nach § 4d BDSG a. F. um auslaufendes Recht handele. Wegen des ersatzlosen Wegfalls der gesetzlichen Grundlage könnten sich deshalb die entscheidungserheblichen Rechtsfragen über das Bestehen einer Meldepflicht im Revisionsverfahren nicht mehr stellen.

Ungeachtet der Tatsache, dass die Meldepflicht für die Tierbeobachtungskameras nunmehr entfallen ist, müssen Betreiber solcher Anlagen auch zukünftig die datenschutzrechtlichen Anforderungen bei der Durchführung einer Videoüberwachung einhalten.

16 Technisch-organisatorischer Datenschutz

16.1 Meldungen nach Art. 33 DSGVO

Nach Art. 33 Datenschutz-Grundverordnung (DSGVO) sind Verantwortliche dazu verpflichtet, innerhalb von 72 Stunden Verletzungen des Schutzes personenbezogener Daten an die jeweils zuständige Aufsichtsbehörde zu melden. Beim Unabhängigen Datenschutzzentrum Saarland gingen seit Geltung der DSGVO bis Ende 2018 insgesamt 74 Meldungen ein.[128] Neben abhandengekommenen Datenträgern oder fehlversandten Unterlagen wurden insbesondere auch Fälle von Ransomware (Erpressungstrojaner) gemeldet. Die Meldepflicht aus Art. 33 DSGVO gibt den Aufsichtsbehörden einen Einblick in datenschutzrelevante Vorfälle bei Verantwortlichen. Die eingehenden Meldungen ermöglichen es den Aufsichtsbehörden zu überprüfen, ob die Datenpanne auf ein grundsätzliches Problem beim Verantwortlichen bei der Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen (TOMs) zum Schutz der Daten von Betroffenen zurückzuführen ist. Ist dies der Fall, kann die Aufsichtsbehörde im Interesse der Betroffenen geeignete Maßnahmen bei den Verantwortlichen veranlassen, die zukünftige Verletzungen zu vermeiden helfen.

Auslösendes Ereignis für die Meldepflicht ist die Verletzung des Schutzes personenbezogener Daten. Als solche gilt die

„Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden" (Art. 4 Nr. 12 DSGVO).

Klassischerweise handelt es sich bei den meisten Datenpannen um solche, bei denen Unbefugte Zugriff auf personenbezogene Daten Dritter erhalten, jedoch kann auch ein reiner Verlust personenbezogener Daten ein Risiko für Betroffene und damit einen meldepflichtigen Vorgang darstellen. So wurde das Datenschutzzentrum über Berichterstattung in Presse und Rundfunk darauf aufmerksam, dass ein saarländisches Unternehmen Opfer eines Erpressungsversuchs unter Einsatz von Ransomware wurde. Die Unternehmensdaten wurden durch die Software verschlüsselt und sollten erst nach Zahlung eines Lösegelds wieder entschlüsselt werden. Im vorliegenden Fall konnte ein Risiko für Betroffene ausdrücklich nicht ausgeschlossen werden, da unter anderem beispielsweise keine Gehälter mehr an die Beschäftigten ausgezahlt werden

[128] Im Vergleich dazu sind im Jahr 2017 nach § 42a Bundesdatenschutzgesetz a. F. lediglich 3 Fälle von Datenpannen gemeldet worden.

konnten. Allein ein Verlust der Zugriffsmöglichkeit auf personenbezogene Daten war daher in diesem Fall meldepflichtig.[129]

Bei den eingegangenen Meldungen wurde deutlich, dass es bei der Umsetzung erforderlicher TOMs nach wie vor große Unterschiede gibt. Zwar wurden in vielen Fällen etwaige Risiken für Betroffene durch entsprechende Maßnahmen wie Verschlüsselung und Backups der Daten minimiert. In einigen Fällen wurde die Aufsichtsbehörde jedoch auf Missstände bei den Verantwortlichen aufmerksam, auf deren Beseitigung sodann hingewirkt wurde. Als erstaunlich ist zudem zu bezeichnen, dass sogar bei IT-Dienstleistern grundlegende Maßnahmen wie die Verschlüsselung von Datenträgern, ganz besonders bei mobilen Endgeräten, noch nicht zum Standardrepertoire gehören.

Auch bei Beachtung sämtlicher Anforderungen des Datenschutzrechts und Umsetzung aller gebotenen TOMs können Verletzungen des Schutzes personenbezogener Daten nie in Gänze ausgeschlossen werden. Daher hat eine Meldung nach Art. 33 DSGVO nicht zwangsläufig weitergehende Maßnahmen der Aufsichtsbehörde zur Folge, sofern diese davon überzeugt ist, dass der Verantwortliche trotz der Datenpanne alle erforderlichen Maßnahmen ergriffen hatte, um diese zu vermeiden.

Datenpannen können dem Datenschutzzentrum via Online-Formular gemeldet werden.[130]

16.2 Auftragsverarbeitung

Im Berichtszeitraum wurde das Unabhängige Datenschutzzentrum Saarland vielfach um rechtliche Einschätzung hinsichtlich der Fragestellung gebeten, unter welchen Voraussetzungen und in welchen Fällen von einer Auftragsverarbeitung auszugehen ist und damit die Anforderungen des Art. 28 Datenschutz-Grundverordnung (DSGVO) zu berücksichtigen sind. Dabei konnte in vielen Fällen auf die in dem von der Datenschutzkonferenz zur Auftragsverarbeitung veröffentlichten Kurzpapier Nr. 13 aufgestellten Grundsätze zurückgegriffen und verwiesen werden.[131]

Der Begriff des „Auftragsverarbeiters" ist in Art. 4 Nr. 8 und der Begriff des „Verantwortlichen" in Abgrenzung hierzu in Art. 4 Nr. 7 DSGVO definiert. Danach ist unter Auftragsverarbeiter jede Stelle zu verstehen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet und Verantwortlicher ist die Stelle, die allein oder gemeinsam mit anderen über die Mittel und Zwecke der Verarbeitung personenbezogener Daten entscheidet. Ausgangspunkt für die Beurteilung der Frage, ob eine Auftragsverarbeitung vorliegt, ist danach stets, wer im konkreten Fall über die Zwecke und Mittel der Datenverarbeitung entscheidet, wobei es maßgeblich auf die

---

[129] Weitere Informationen zur Thematik finden sich im Working Paper 250rev.01 des Europäischen Datenschutzausschusses (EDSA): https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de (letzter Zugriff: 5.3.2019).

[130] Elektronisch abrufbar unter: https://datenschutz.saarland.de/online-services/datenpanne-melden-fuer-verantwortliche/.

[131] Elektronisch abrufbar unter https://datenschutz.saarland.de/datenschutz/anwendungshinweise-dsgvo/kurzpapiere/.

Entscheidung über die Verarbeitungszwecke ankommt. Die Entscheidung über die technischen und organisatorischen Fragen der Verarbeitung kann insofern auch auf den Auftragsverarbeiter delegiert werden.

Dabei wird im Kurzpapier darauf hingewiesen, dass bei der Inanspruchnahme externer Fachleistungen bei einem eigenständig Verantwortlichen keine Auftragsverarbeitung vorliegt. Davon kann in der Regel bei der Beauftragung bspw. von Steuerberatern, Rechtsanwälten, Wirtschaftsprüfern, eines Inkassobüros mit Forderungsübertragung, von Post- und Kurierdiensten zum Transport von Briefen oder eines Bankinstituts zum Geldtransfer ausgegangen werden.

Abgrenzungsschwierigkeiten ergeben sich in diesem Zusammenhang beispielsweise für den Fall der ausgelagerten Lohn- und Gehaltsabrechnung durch einen Steuerberater. Hier wurde mehrfach die Frage an die Aufsichtsbehörde herangetragen, ob die von einem Steuerberater vorgenommene externe Lohn- und Gehaltsabrechnung als Auftragsverarbeitung oder als eigenverantwortliche Datenverarbeitung einzuordnen ist.

Hierzu gibt es, auch unter den Aufsichtsbehörden, unterschiedliche Auffassungen, die von einer grundsätzlichen Eigenverantwortlichkeit der Tätigkeit des Steuerberaters als freier Beruf bis hin zu einem grundsätzlichen Vorliegen einer Auftragsverarbeitung im Falle einer reinen Lohn- und Gehaltsbuchhaltung durch einen Steuerberater reichen.

Dabei liegt den gegenläufigen Positionen eine unterschiedliche Sicht auf die im Zusammenhang mit der Lohn- und Gehaltsbuchhaltung verbundenen Tätigkeiten zu Grunde.

Soweit man allein die laufende Lohn- und Gehaltsbuchhaltung betrachtet, ist zu berücksichtigen, dass diese nach einem Urteil des Bundesverfassungsgerichts vom 27. Januar 1982 (1 BvR 807/80) nicht dem Buchführungsprivileg der steuerberatenden Berufe unterliegen dürfen und daraufhin vom Verbot der unbefugten Hilfeleistung in Steuersachen ausgenommen wurden. Folglich wird diese seither auch von gewerblichen Lohnbüros angeboten und durchgeführt. Dabei sind für die Frage der Auftragsverarbeitung insbesondere die der Entscheidung zu Grunde liegenden Erwägungen von Bedeutung. Das Bundesverfassungsgericht begründet seine Entscheidung damit, dass *„(…) die laufende Lohnbuchhaltung regelmäßig keine schwierigen rechtlichen Würdigungen verlangt, sondern sich als eine nicht durch besondere rechtliche Erwägungen geprägte schematisierte Subsumtion von Lohnzahlungsvorgängen unter die amtlichen Lohnsteuertabellen und das betriebliche Lohnkonto darstellt."* [132]

Unter Zugrundelegung dieser Ausführungen erscheint es zunächst naheliegend, die reine Lohn- und Gehaltsbuchhaltung als Auftragsverarbeitung zu qualifizieren. Da diese keine besonderen rechtlichen Bewertungen erforderlich macht und es sich vielmehr um einen schematisierten Verarbeitungsvorgang handelt, ist auch kein dem Dienstleister verbleibender Entscheidungsspielraum im Hinblick auf den Zweck oder die Mittel der Datenverarbeitung ersichtlich.

[132] BVerfG, Beschluss vom 27.1.1982 – 1 BvR 807/80, Rn. 67 (zitiert nach juris).

Andererseits dürfte ein Steuerberater in der Praxis kaum allein mit der laufenden Lohn- und Gehaltsbuchhaltung betraut sein, ohne in diesem Zusammenhang auch über den schematisierten Verarbeitungsvorgang hinaus entweder umfassend oder auch speziell im Rahmen der auszuführenden Lohn- und Gehaltsbuchhaltung beratend tätig zu sein. Den Steuerberater treffen mithin berufliche Pflichten wie bspw. zur eigenverantwortlichen und gewissenhaften Berufsausübung, so dass er stets zu einer gewissen Überprüfung bspw. der mitgeteilten Lohndaten und einer entsprechenden steuer- und sozialversicherungsrechtlichen Würdigung angehalten ist.

Es bedarf deshalb stets einer differenzierten und eingehenden Betrachtung der Umstände und des Kontexts, in dem die jeweilige Verarbeitung steht, um diese als eigenverantwortlich oder als Auftragsverarbeitung einordnen zu können. Betreffend der Lohn- und Gehaltsabrechnung gibt es in diesem Zusammenhang noch einen gewissen Klärungsbedarf. Die Aufsichtsbehörden befinden sich hierzu aktuell im Austausch mit dem Ziel, zu einer möglichst einheitlichen und den tatsächlichen wie rechtlichen Gegebenheiten Rechnung tragenden Bewertung zu kommen.

Während in dem vorgenannten Fall der Lohn- und Gehaltsbuchhaltung Abgrenzungsschwierigkeiten vor dem Hintergrund der Frage entstehen, wer über die Zwecke und Mittel der Verarbeitung entscheidet, ist für andere Dienstleistungsbereiche vielmehr problematisch, unter welchen Voraussetzungen und in welchen Fällen von einer Verarbeitung personenbezogener Daten auszugehen ist und deshalb ein Vertrag über eine Auftragsverarbeitung zu schließen ist.

So ist bspw. für den Bereich der IT-Wartung oder Fernwartung nach den Ausführungen im Kurzpapier Nr. 13[133] dann von einer Auftragsverarbeitung auszugehen, wenn die Notwendigkeit oder Möglichkeit des Zugriffs auf personenbezogene Daten gegeben ist. Für die Annahme einer Auftragsverarbeitung ist daher nicht vorausgesetzt, dass eine zielgerichtete Verarbeitung personenbezogener Daten stattfindet oder die Verarbeitung personenbezogener Daten Hauptgegenstand der Dienstleistung bzw. des Vertrages ist.

Dementgegen führt die rein technische Wartung einer IT-Infrastruktur (wie bspw. Arbeiten an der Stromzufuhr, Kühlung oder Heizung) durch einen Dienstleister nicht zu einer Qualifikation als Auftragsverarbeitung.

Zu beachten gilt es weiterhin, dass die gesetzlichen Geheimhaltungs- und beruflichen Verschwiegenheitspflichten auch im Rahmen der Auftragsverarbeitung gelten, d. h. dass Daten, die vor diesem Hintergrund vertraulich zu behandeln sind, dem Auftragsverarbeiter grundsätzlich nicht offenbart werden dürfen. Etwas anderes gilt aber beispielsweise durch das „Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen" für die in § 203 Abs. 1 oder 2 Strafgesetzbuch (StGB)[134] genannten Berufsgeheimnisträger (Rechtsanwälte, Steuerberater, Ärzte etc.), wenn sie externe Dienstleister in Anspruch nehmen und diese an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken. In solchen Fällen ist eine Offenbarung unter den Voraussetzungen des § 203 Abs. 3 und 4 StGB erlaubt, wobei der Auftragsverarbeiter dann gemäß § 203 Abs.

[133] Elektronisch abrufbar unter https://datenschutz.saarland.de/fileadmin/datenschutz/ds-gvo/kurzpapiere/dsk_kpnr_13.pdf.

[134] Siehe auch Kap. 2.6 S. 39 f.

4 StGB ebenfalls einer strafrechtlich sanktionierten Verschwiegenheitspflicht unterliegt.

16.3 Datenschutz-Folgenabschätzung

Auch im Bereich der Datenschutz-Folgenabschätzung (DSFA) wandten sich Verantwortliche an das Unabhängige Datenschutzzentrum Saarland mit der Bitte um Hilfestellung bei der Beurteilung, ob für spezifische Verarbeitungsvorgänge notwendigerweise eine DSFA durchzuführen ist. Mit der DSFA hält die Datenschutz-Grundverordnung (DSGVO) in Art. 35 ein Werkzeug bereit, mit dem Verantwortliche bereits im Vorfeld einer Datenverarbeitung systematisch Risiken für Betroffene erkennen, beurteilen und eindämmen können.

Der zunächst abstrakte Begriff der DSFA steht inhaltlich für einen – jedenfalls in seiner grundlegenden Systematik und Logik – einfachen Vorgang:

In einem ersten Schritt (Vorprüfung) beurteilt der Verantwortliche, ob es der Durchführung einer DSFA bedarf. Dies ist der Fall, wenn die konkrete Verarbeitungstätigkeit *„voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge"* hat (Schwellwertanalyse). Stellt sich im Rahmen dieser Einschätzung heraus, dass kein hohes Risiko durch eine Verarbeitung besteht, trifft den Verantwortlichen keine Pflicht eine DSFA durchzuführen. Notwendigerweise sind in jedem Fall jedoch die Kerninhalte der diesbezüglichen Erwägungen zu dokumentieren.

Um es den Verantwortlichen zu erleichtern die Schwellwertanalyse durchzuführen, hat die Datenschutzkonferenz (DSK) eine Liste im Sinne des Art. 35 Abs. 4 DSGVO – umgangssprachlich auch als „Blacklist" oder auch „Muss-Liste" bezeichnet – für den nicht-öffentlichen Bereich veröffentlicht. Diese Liste enthält verschiedene Verarbeitungstätigkeiten, für die aus Sicht der Aufsichtsbehörden immer eine DSFA durchzuführen ist. Sie wurde maßgeblich von der Unterarbeitsgruppe DSFA (UAG DSFA) der DSK erarbeitet, an der auch das Unabhängige Datenschutzzentrum Saarland beteiligt ist. Basis für die in die Liste aufgenommenen Verarbeitungstätigkeiten ist das Working Paper 248rev.01,[135] das ursprünglich bereits von der Art. 29-Gruppe ausgearbeitet und vom Europäischen Datenschutzausschuss (EDSA) in seiner ersten Sitzung übernommen wurde.

Da die Liste auch Verarbeitungstätigkeiten enthält, die potentiell einen grenzüberschreitenden Bezug aufweisen können[136], war für sämtliche Listen der europäischen Aufsichtsbehörden das Kohärenzverfahren beim EDSA zu durchlaufen. Im Rahmen dieser Verfahren ergingen sodann die ersten Stellungnahmen des EDSA seit Geltung der DSGVO.[137] Dabei ergab die Überprüfung der deutschen Liste durch den EDSA, dass diese in ihrem Kern – abgesehen von einigen wenigen geforderten Korrekturen

[135] https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de (letzter Zugriff: 5.3.2019).

[136] Vgl. Art. 35 Abs. 6 DSGVO.

[137] https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_de (letzter Zugriff: 5.3.2019).

– in der von der DSK beschlossenen Form bestehen bleiben konnte. Die vom EDSA geforderten Änderungen wurden anschließend von der UAG DSFA umgesetzt und von der DSK angenommen.

Die Liste ist in der jeweils aktuellen Fassung einerseits auf der Webseite des Datenschutzzentrums[138], aber auch auf dem Internetangebot der DSK[139] abrufbar.

Findet sich die von einem Verantwortlichen geplante Verarbeitungstätigkeit nicht in der Liste der deutschen Aufsichtsbehörden, bedeutet dies jedoch nicht zwangsläufig, dass keine DSFA durchzuführen ist. Vielmehr muss der Verantwortliche dann eigenständig eine Schwellwertanalyse vornehmen und überprüfen, ob von der Verarbeitung für Betroffene voraussichtlich ein hohes Risiko ausgeht.

Bei der Bewertung des Risikos ist einerseits die Schwere der potentiellen Schäden, andererseits die Eintrittswahrscheinlichkeit des Schadens zu berücksichtigen. Besteht also nur eine begrenzte Wahrscheinlichkeit für ein bestimmtes Schadensszenario, kann es dennoch erforderlich sein, eine DSFA durchzuführen, wenn die drohenden Schäden besonders schwerwiegend wären. Umgekehrt können auch drohende Schäden von mittlerem Ausmaß eine DSFA erforderlich machen, wenn deren Eintritt besonders wahrscheinlich ist. Weitergehende Informationen enthalten einerseits das Kurzpapier Nr. 5 der DSK[140] sowie das Working Paper 248rev0.1[141] des EDSA, in welchem insbesondere weitere Kriterien aufgeführt sind, die bei der Beurteilung des Risikos herangezogen werden können. Dabei steigt das voraussichtliche Risiko einer Verarbeitung, je mehr der folgenden Kriterien erfüllt sind:

- Vertrauliche oder höchst persönliche Daten
- Daten zu schutzbedürftigen Betroffenen
- Datenverarbeitung in großem Umfang
- Systematische Überwachung
- Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
- Bewerten oder Einstufen (Scoring)
- Abgleichen oder Zusammenführen von Datensätzen
- Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
- Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert

---

138 https://datenschutz.saarland.de/themen/datenschutz-folgenabschaetzung/ (letzter Zugriff: 5.3.2019).

139 https://www.datenschutzkonferenz-online.de/anwendungshinweise.html (letzter Zugriff: 5.3.2019).

140 https://datenschutz.saarland.de/fileadmin/datenschutz/ds-gvo/kurzpapiere/dsk_kpnr_5.pdf (letzter Zugriff: 5.3.2019).

141 https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de (letzter Zugriff: 5.3.2019).

Falls zwei der obigen Kriterien im Rahmen der konkreten Verarbeitungstätigkeit relevant sind, wird in der Regel ein hohes Risiko für Betroffene bestehen und eine DSFA durchzuführen sein. Auch diese Faustregel gilt jedoch nur als erster Anhaltspunkt und macht eine konkrete Einzelfallbetrachtung nicht entbehrlich.

Sollten bei der Bewertung Zweifel verbleiben, kommt eine Konsultation der Aufsichtsbehörde in Betracht. Dabei ist es erforderlich, dass mit der Anfrage eine detaillierte Beschreibung der Verarbeitungstätigkeit bezogen auf Zweck, Mittel sowie geplante technische und organisatorische Maßnahmen zur Verfügung gestellt wird. Darüber hinaus sind die bisherigen Erwägungen zum voraussichtlichen Risiko durch den Verantwortlichen darzulegen. Nur auf Grundlage dieser Informationen kann eine aufsichtsbehördliche Einschätzung im Rahmen der Konsultation erfolgen.

Ist die Verarbeitung in der Liste der DSK aufgeführt oder hat eine eigene Schwellwertanalyse ein voraussichtlich hohes Risiko ergeben, ist sodann eine DSFA nach Maßgabe der Anforderungen des Art. 35 Abs. 7 DSGVO durchzuführen.

16.4 Technische und organisatorische Maßnahmen in Arztpraxen

Die Digitalisierung schreitet auch in Arztpraxen stetig voran. Dies bringt einerseits viele Vorteile mit sich, andererseits aber auch neue Herausforderungen, da der IT-Betrieb grundsätzlich nicht das Kerngeschäft einer Arztpraxis darstellt.

Seit dem 25. Mai 2018 gilt mit der Datenschutz-Grundverordnung (DSGVO) ein neues und gegenüber dem nationalen Recht vorrangiges Datenschutzrecht. Gerade in Arztpraxen, in denen besonders sensible Daten verarbeitet werden, muss ein Bewusstsein für den Datenschutz und die Informationssicherheit entwickelt werden. Das ist wichtig, da mit der DSGVO ein deutlich erhöhter Sanktionsrahmen geschaffen wurde und Verstöße gegen den Datenschutz schärfer geahndet werden können.

16.4.1 Aspekte bzgl. Datenschutz in der Arztpraxis

Folgende Hauptaspekte sind bzgl. des Datenschutzes in einer Arztpraxis zu bedenken: Erstens das Verhältnis zum Patienten, zweitens das Verhältnis zu externen Dienstleistern und Dritten und drittens die interne Datenschutzorganisation bzw. das Datenschutzmanagement.

Im Hinblick auf das *Verhältnis zum Patienten* sind für den Arzt folgende Punkte zu beachten:

- Definition eines Prozesses zur Einholung von Einwilligungserklärungen für besondere Datenverarbeitungsvorgänge
- Berücksichtigung von Informationspflichten
- Einrichtung eines praxisinternen Prozesses zur Wahrung des Auskunftsrechts des Patienten

- Festlegung eines Verfahrens, um das Recht des Patienten auf Löschung zu wahren

Die Berücksichtigung des Verhältnisses zu externen Dienstleistern und/oder Dritten erfordert es, dass, soweit Verträge mit externen Dienstleistern, z. B. mit privaten Verrechnungsstellen oder zur Ausführung von Wartungsaufgaben an der IT-Infrastruktur, bestehen oder abgeschlossen werden sollen, diese Verträge auf ihre Vereinbarkeit mit den neuen datenschutzrechtlichen Vorschriften sowie mit den strafrechtlichen Bestimmungen zur ärztlichen Schweigepflicht[142] überprüft werden. Handelt es sich hierbei um eine Auftragsverarbeitung sollten entsprechende Vereinbarungen getroffen werden, deren Anforderungen sich aus Art. 28 Abs. 3 DSGVO ableiten. Zusätzlich zu den datenschutzrechtlichen Vorgaben, sollten in Verträgen mit externen Dienstleistern auch Klauseln aufgenommen werden, die diese zur Geheimhaltung verpflichten.

Im Hinblick auf den dritten Aspekt benötigen Ärzte für ihre Praxis ein *Datenschutzmanagement*, um sicherzustellen und dokumentiert nachweisen zu können, dass sie den Datenschutz entsprechend der DSGVO wahren.

Folgende Punkte sind hierbei zu beachten bzw. umzusetzen:

- **Überprüfung aller internen Verarbeitungsvorgänge in der Arztpraxis**

Alle in der Praxis durchgeführten elektronischen Verarbeitungsvorgänge sowie die Verarbeitung von Patientendaten in Karteien sind auf die datenschutzrechtliche Konformität hin zu überprüfen. Hierzu sind insbesondere geeignete technisch-organisatorische Maßnahmen zu ergreifen. In bestimmten Fällen muss auch eine sog. Datenschutzfolgenabschätzung durchgeführt werden (Art. 35 DSGVO), um mögliche Risiken bei der Verarbeitung von personenbezogenen Daten abzuschätzen und Maßnahmen zum Schutz der Daten zu ergreifen.

- **Erstellung eines Verzeichnisses für Verarbeitungsvorgänge in der Praxis**

In der Arztpraxis muss eine Bestandsaufnahme durchgeführt werden, mit welcher ermittelt werden kann, welche Daten auf welcher Rechtsgrundlage verarbeitet werden. Alle Arztpraxen müssen ein Verzeichnis der Verarbeitungstätigkeiten führen (Art. 30 DSGVO), wobei für jede Gruppe von Datenverarbeitungsvorgängen ein entsprechendes Formular auszufüllen ist.

- **Benennung eines Datenschutzbeauftragten**

Einige Arztpraxen müssen einen Datenschutzbeauftragten benennen (Art. 37 DSGVO), der entweder in der Praxis beschäftigt ist oder als externer Dienstleister beauftragt wird. Das ist in jedem Fall anzunehmen, wenn in der Praxis mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (§ 38 Abs. 1 BDSG). Hierfür ist durch den Praxisinhaber eine Person zu benennen, die für diese Aufgabe fachlich qualifiziert ist. Der Datenschutzbeauftragte ist ferner der zuständigen Aufsichtsbehörde zu melden und seine Kontaktdaten sind zu veröffentlichen. Er kontrolliert intern nicht nur die Einhaltung des Datenschutzes und der Datensicherheit, sondern er fungiert auch als kompetenter

[142] Vgl. oben, Kap. 2.5.

Ansprechpartner für alle im Zusammenhang mit dem Datenschutz aufkommenden Fragen.

Weitere Details hierzu befinden sich im Tätigkeitsbericht unter Kap. 9.2.

- **Erarbeitung einer internen Datenschutzrichtlinie**

Die Erstellung einer Datenschutzrichtlinie fundamentiert das Bewusstsein für den Datenschutz und die Datenschutzrisiken. In dieser sollten Regelungen bzgl. Verhaltensweisen bei Erfassung von Patientendaten, klare Verantwortlichkeiten oder Zugriffsrechte bzw. -beschränkungen für Mitarbeiter festgelegt werden. Darüber hinaus sollte in einer solchen Richtlinie festgelegt werden, wie und wo der Nachweis über die einschlägige Rechtsgrundlage für die Verarbeitung dokumentiert wird.

- **Überprüfung und Anpassung vorhandener Verträge und Formulare**

Sind Verträge mit Dritten oder Formulare in der Arztpraxis vorhanden, müssen sowohl diese Formulare als auch verwendete Verträge mit Dritten überprüft und an das neue Datenschutzrecht angepasst werden. Beispielsweise müssen Einwilligungserklärungen einen Hinweis bzgl. der Widerrufbarkeit enthalten. Im Rahmen der Einholung einer Einwilligung in der Datenverarbeitung, ist im Vorhinein über deren Widerrufbarkeit zu informieren.

- **Sicherheit der Datenverarbeitung**

Durch geeignete technisch-organisatorische Maßnahmen (z. B. Einsatz von Virenschutz und Malware, Verschlüsselung, usw.) ist die Sicherheit der Datenverarbeitung in der Arztpraxis, insbesondere vor Angreifern von innen als auch von außen, zu gewährleisten.

16.4.2 Gefahren

Die Standardisierung durch einheitliche IT-Systeme setzt sich immer mehr durch. Jedoch stellen Arztpraxen häufig lediglich den Nutzen von speziellen Praxis-IT-Systemen, die sie oft in Eigenregie betreiben, in den Vordergrund ihrer Betrachtung, fokussieren aber „noch nicht" die Absicherung der Systeme und die darin befindlichen personenbezogenen Daten.

Die Bedrohung der Datensicherheit in Arztpraxen steigt durch die zunehmende Vernetzung stetig an. Als eine Gefahrenquelle ist Malware zu nennen, bspw. Verschlüsselungstrojaner, die sich durch E-Mails getarnt, rasant verbreiten und sich auf die Verfügbarkeit und Integrität der personenbezogenen Daten negativ auswirken können.

16.4.3 Schutzmaßnahmen

Vorbeugung ist bekanntlich die beste Medizin! Dies gilt auch für den Datenschutz in einer Arztpraxis.

Um die saarländischen Arztpraxen insbesondere für das Thema „Malware – Verschlüsselungstrojaner“ zu sensibilisieren, wurde ein Fragebogen, der die wesentlichen Themenbereiche zum Schutz gegen Malware umreißt, entwickelt und auf der Website des Unabhängigen Datenschutzzentrum Saarland publiziert. Mit Hilfe des Fragebogens kann jede Arztpraxis durch Beantwortung der Fragen überprüfen, ob sie für den Fall eines Datenverschlüsselungsangriffs die notwendigen Schritte zum Schutz der Patientendaten ergriffen hat.

16.5 Datensicherheit und Informationssicherheit mit einem Managementsystem

Um die Anforderungen des Datenschutzes nachhaltig, effizient und risikobasiert in einer Organisation zu implementieren, ist es gerade auch mit Blick auf die komplexen rechtlichen, technischen und organisatorischen Anforderungen, die sich aus der Datenschutz-Grundverordnung (DSGVO) ergeben, sinnvoll, ein Datenschutzmanagementsystem (DSMS) zu etablieren und verbindlich zu betreiben.

Unter einem Managementsystem generell ist eine Systematisierung von Aufgaben, Pflichten, Verfahren und Regeln innerhalb einer Organisation zu verstehen.

Verbreitet sind sog. Informationssicherheitsmanagementsysteme (ISMS), welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

In ähnlicher Weise stellt ein DSMS die Wirksamkeit der datenschutzrelevanten technischen und organisatorischen Maßnahmen wie auch die Einhaltung der rechtlichen Vorgaben in den Prozessen und Systemen der Organisation sicher. In Anlehnung an bestehende Managementsysteme (z. B. DIN EN ISO 9001 Qualitätsmanagement oder DIN ISO/IEC 27001 Informationssicherheitsmanagement) sichert ein iterativer Verbesserungsprozess eine regelmäßige Überprüfung der Einhaltung und eine nachhaltige und effiziente Umsetzung der Datenschutzanforderungen.

Mit Blick auf die Anforderungen der Datensicherheit aus Art. 32 DSGVO lassen sich bei der Nutzung eines Informationssicherheitsmanagementsystems oftmals Synergieeffekte zur Gewährleistung auch der datenschutzrechtlichen Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit generieren. ISIS12 (Informations-Sicherheits-management System in 12 Schritten) stellt ein Modell zur Einführung eines Informationssicherheitsmanagementsystems dar, mit dem auch die technischen und organisatorischen Anforderungen aus Art. 32 DSGVO systematisiert werden können. ISIS12 kann damit ein Baustein auf dem Weg zur Einführung eines Datenschutzmanagementsystems darstellen.

16.5.1 Zweck und Einsatzort

Die Einführung eines Managementsystems, ob für Informations- oder Datensicherheit, stellt sowohl Verwaltungen als auch Unternehmen oft vor große Hürden.

Schwierigkeiten bei der praktischen Einführung und Umsetzung eines Managementsystems zur Gewährleistung von Vertraulichkeit, Verfügbarkeit und Integrität bestehen erfahrungsgemäß vor allem in personellen Engpässen und mangelndem Fachwissen.

Das Vorgehensmodell von ISIS12 fußt auf dem Grundgedanken, die Lücke zwischen Notwendigkeit und organisatorisch Leistbaren zu schließen und dabei dem Anwender sowohl einen technisch-organisatorischen als auch rechtlichen Rahmen vorzugeben.

ISIS12 richtet sich insbesondere an die für die Verarbeitung personenbezogener Daten verantwortlichen Stellen aus dem kommunalen Verwaltungsbereich sowie aus dem Klein- und Mittelstand. Mit Hilfe von ISIS12 können sowohl die Anforderungen an die Informationssicherheit als auch an die Datensicherheit definiert, gesteuert, kontrolliert, aufrechterhalten und fortlaufend verbessert werden.

Der IT-Planungsrat, als föderales Gremium zur IT-Koordination von Bund und Ländern, hat in seiner 16. Sitzung[143] den Leitfaden "Informations-Sicherheits-Management-System in 12 Schritten (ISIS12)"[144] als ein pragmatisches und skalierbares Vorgehensmodell zum Aufbau und Etablierung eines Sicherheitsmanagementsystems bezeichnet. Auch die Landesregierung unterstützt die Einführung von Informationssicherheitsmanagementsystemen auf der Grundlage von ISIS12.

16.5.2 Aufbau und Struktur von ISIS12

Der ISIS12-Prozess ist in 12 Schritte gegliedert, die in drei Grobphasen eingeteilt sind:

- Initialisierungsphase,
- Festlegung der Aufbau- und Ablauforganisation und
- Entwicklung und Umsetzung

Die zwölf Schritte werden sequentiell durchlaufen und verfolgen dabei einen Top-Down-Ansatz. Die Leitungsebene trägt die Verantwortung für die Informationssicherheit und den Datenschutz, initiiert den dafür notwendigen Sicherheitsprozess und stellt die dafür erforderlichen personellen Ressourcen (Informationssicherheits- und Datenschutzbeauftragter) zur Verfügung, ohne die die weiteren Schritte nicht erfolgreich umzusetzen sind.

In den ersten beiden Phasen werden die Vorarbeiten, wie die Erstellung der Leitlinie für Informationssicherheit, der Leitlinie für Datenschutz und die Festlegung der Aufbau- und Ablaufstruktur durchgeführt, bevor mit den operativen Arbeiten, d. h. der Konzeption und Implementierung der integrierten Sicherheitskonzeption begonnen wird.

---

[143] Elektronisch abrufbar unter: https://www.it-planungsrat.de/SharedDocs/Sitzungen/DE/2015/Sitzung_16.html?pos=5 (letzter Zugriff: 5.3.2019).

[144] https://isis12.it-sicherheitscluster.de/ (letzter Zugriff: 5.3.2019).

Ein Managementsystem ist ein wiederkehrender Prozess. Die nachstehende Abbildung veranschaulicht das ISIS12-Vorgehensmodell und den sich wiederholenden Prozess. Zusätzlich befinden sich in den einzelnen Schritten auch Elemente (hier grau markiert) zur Gewährleistung der Vorgaben technisch/organisatorischer Art, wie sie sich insbesondere aus Kapitel 4 der seit dem 25. Mai 2018 geltenden DSGVO ergeben.

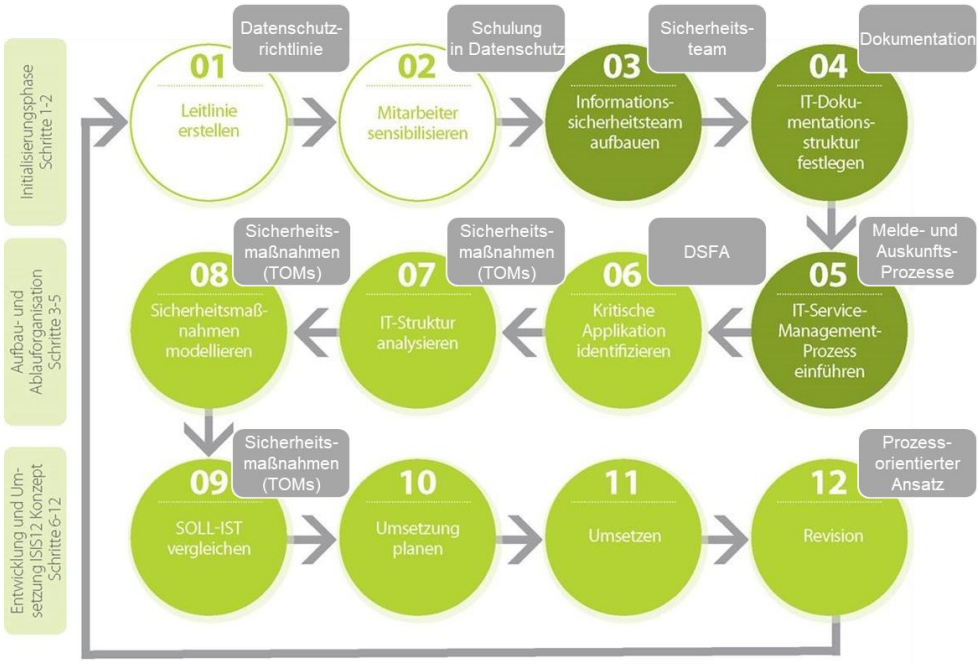


Abbildung 1: ISIS12 – Vorgehensmodell

Quelle: Bayerischer IT-Sicherheitscluster e.V. [https://www.it-sicherheitscluster.de/ueber-uns-2/]

16.5.3 Berücksichtigung der Anforderungen der DSGVO

In den einzelnen Schritten des ISIS12-Vorgehensmodells wird der Anwender bei der Einhaltung der sich aus dem vierten Abschnitt der DSGVO ergebenden Vorgaben unterstützt. Dies reicht von der Meldung des Datenschutzbeauftragten an die Aufsichtsbehörde, der Erstellung einer Datenschutzleitlinie, über Schulung der Mitarbeiter und Erstellung der notwendigen Dokumentation bis hin zu Melde- und Auskunftsprozessen, einer **Risikoanalyse** und **Datenschutz-Folgenabschätzung (DSFA)** auf Basis des erstellten Verzeichnisses der Verarbeitungstätigkeiten und schlussendlich der Unterstützung von TOMs.

16.5.4 Schutzbedarfsfeststellung / Risikoanalyse

Unverzichtbare Voraussetzung für die Umsetzung der sich aus Art. 32 DSGVO ergebenden Pflichten ist die Dokumentation der in einer Organisation vorhanden Verarbeitungstätigkeiten und Verfahren. Hierfür ist das Erstellen eines **Verzeichnisses aller Verarbeitungstätigkeiten** gemäß Art. 30 DSGVO selbst dann hilfreich, wenn hierzu formal-rechtlich keine Verpflichtung besteht. Mit Hilfe des Verzeichnisses nach Art. 30 DSGVO wird nämlich eine Strukturierung oder Gruppierung von Verarbeitungstätigkeiten anhand von Prozessen, Geschäftsvorfällen oder Verarbeitungstätigkeiten ermöglicht und so eine methodische Herangehensweise bei der Ermittlung der angemessenen Sicherheitsmaßnahmen nach Art. 32 DSGVO gefördert.

Art. 32 Abs. 1 DSGVO verlangt vom Verantwortlichen und vom Auftragsverarbeiter, dass zum Schutz personenbezogener Daten angemessene Sicherheitsmaßnahmen ergriffen werden müssen:

Die DSGVO benennt in Art. 32 Abs. 1 die folgenden Kriterien, die zu berücksichtigen sind, um mit Blick auf die Sicherheit der Verarbeitung ein angemessenes Schutzniveau umzusetzen und entsprechende Sicherheitsmaßnahmen ermitteln zu können:

- Stand der Technik,
- die Implementierungskosten,
- Art, Umfang, Umstände und Zwecke der Verarbeitung
- und die Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen.

Die getroffenen technisch-organisatorischen Maßnahmen müssen also dem Schutzbedarf der zu verarbeitenden personenbezogenen Daten entsprechen. Werden in einer Organisation entsprechend sensible Daten verarbeitet, müssen besondere Schutzmaßnahmen ergriffen werden, da die Verarbeitung solcher Daten mit einem höheren Risiko für den Betroffenen belegt ist. Die **Bestimmung des Risikos** führt zur Bestimmung der Schutzklasse und diese bestimmt die **Angemessenheit** der Maßnahmen.

Zunächst geht es also, wie im klassischen Risikomanagement, darum, Risiken zu identifizieren (Art, Ursachen und Auswirkungen) und Risiken zu analysieren (Eintrittswahrscheinlichkeiten und Auswirkungen). Jedoch ist das Zielobjekt nicht wie sonst üblich die Organisation, sondern die **Rechte und Freiheiten der betroffenen Personen**.

Hier tritt der Vorteil einer integrierten Betrachtung von Datensicherheit und Informationssicherheit zu Tage, wie dies der Ansatz des ISIS12-Modells ist. Während im Datenschutz und der Informationssicherheit zur Beurteilung der Sicherheit von personenbezogenen Daten und der Sicherheit von Informationen die identischen Prinzipien angewandt werden, erfolgt die Bewertung der Risiken aus unterschiedlichen Perspektiven.

Wegen dieses unterschiedlichen Blickwinkels können die Ergebnisse aus einer Risikobewertung der Informationssicherheit für die Erfüllung der sich aus Art. 32 DSGVO

ergebenden Pflichten nicht einfach übernommen werden. Die Ergebnisse der Datensicherheits- und der Informationssicherheits-Risikobewertung können zwar zufällig identisch, müssen es aber nicht zwangsläufig sein. Mit der Vorgehensweise nach ISIS12 wird eine einheitliche Betrachtung gewährleistet.

16.5.5 Zertifizierung

Der Aufbau, die Etablierung und der nachhaltige Betrieb des ISIS12-Managementsystems können durch ein unabhängiges Institut zertifiziert werden. Hier werden im Rahmen eines Audits durch einen sachverständigen Dritten mittels eines zweigeteilten Prozesses einerseits die Dokumentenlage und andererseits die zielorientierte Umsetzung der technisch-organisatorischen Maßnahmen überprüft. Fällt die Prüfung positiv aus, erhält die Organisation ein Zertifikat, welches die Einhaltung von Schutzmaßnahmen und damit ein dem Stand der Technik entsprechendes Informationssicherheitsniveau bescheinigt.

16.5.6 Fazit

Das ISIS12-Vorgehensmodell bietet der einsetzenden Organisation ein einfaches, schnell einzuführendes und zu betreibendes Verfahren zur Absicherung der Informations- und Datensicherheit. Auf dieser Basis können dann die technischen und organisatorischen Anforderungen des vierten Kapitels der DSGVO entlang der zwölf zu durchlaufenden Schritte mitberücksichtigt werden. Insbesondere die Ableitung des Verfahrensverzeichnisses aus der Liste der kritischen Anwendungen, darauf aufbauende Risikobetrachtung und die sich anschließende DSFA unterstützen die verantwortlichen Stellen dabei, an alle wesentlichen Punkte zur Erfüllung datenschutzrechtlicher Vorgaben zu denken.

Mehrwerte dieses Vorgehensmodells bilden der dem System immanente Maßnahmenkatalog, der sich auf die Inhalte der IT-Grundschutz-Kataloge und der ISO/IEC 27001 stützt und somit technische und organisatorische Maßnahmen zur Gewährleistung der Informationssicherheit enthält. Hiermit werden oftmals gleichzeitig auch Anforderungen zur Gewährleistung der Datensicherheit unter Berücksichtigung der Vorgaben von Art. 32 DSGVO erfüllt. Zudem wird die Möglichkeit einer Zertifizierung durch ein unabhängiges Institut geboten.

16.6 Akkreditierung von Zertifizierungsstellen durch Fachbegutachter der Aufsichtsbehörden

Im Rahmen der Einführung der Datenschutz-Grundverordnung (DSGVO) rückt die Zertifizierung als Teilprozess einer Konformitätsbewertung immer stärker in den Vordergrund. Art. 42 Abs. 1 DSGVO fordert die Einführung von datenschutzspezifischen

Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen. Mit diesen kann dann vom Verantwortlichen oder Auftragsverarbeiter der Nachweis erbracht werden, dass die DSGVO bei Verarbeitungsvorgängen eingehalten wird.

Art. 43 Abs. 1 S. 2 DSGVO enthält hinsichtlich der Akkreditierung der Zertifizierungsstellen Vorgaben für die Mitgliedstaaten. In Deutschland sind diese Vorgaben in § 39 Bundesdatenschutzgesetz (BDSG) dahingehend spezifiziert worden, dass die Befugnis, als Zertifizierungsstelle tätig zu werden, durch die für die datenschutzrechtliche Aufsicht über die Zertifizierungsstelle zuständige Aufsichtsbehörde des Bundes oder der Länder auf der Grundlage einer Akkreditierung durch die Deutsche Akkreditierungsstelle (DAkkS) erteilt wird. Die DAkkS ist die nationale Akkreditierungsstelle der Bundesrepublik Deutschland mit Sitz in Berlin, Braunschweig und Frankfurt a.M. Sie ist eine privatwirtschaftliche, aber nicht gewinnorientierte Organisation, die als Beliehene hoheitliche Aufgaben wahrnimmt. Bei Tätigkeiten der hoheitlichen Akkreditierung unterliegt die DAkkS dem deutschen Verwaltungsverfahrensgesetz (VwVfG) und weiteren verwaltungsrechtlichen Vorgaben. Zertifizierungsstellen dürfen nur dann akkreditiert werden, wenn die in Art. 43 Abs. 2 DSGVO aufgeführten Kriterien erfüllt sind. So müssen sie bspw. nachweisen, dass sie unabhängig sind, über das erforderliche Fachwissen verfügen und ihre Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

Zur Durchführung eines Akkreditierungsverfahrens ist es notwendig, dass entsprechende Zertifizierungsprogramme von Zertifizierungsstellen entwickelt werden, mit denen Produkte, Prozesse oder Dienstleistungen im Sinne der DSGVO auf Konformität analysiert und bewertet werden. Diese Zertifizierungsprogramme sind vorab von der Zertifizierungsstelle oder dem Programmeigner der Akkreditierungsstelle vorzulegen. Dort wird das jeweilige Programm gemäß DIN EN ISO/IEC 17011 auf Eignung geprüft und im positiven Fall akkreditiert.

16.6.1 Akkreditierungs- und Zertifizierungsprozess

Bei einer Akkreditierung handelt es sich um einen komplexen Prozess. Zuerst müssen die formellen Vorgaben der DIN EN ISO/IEC 17065 aufgrund von Art. 43 Abs. 3 DSGVO ergänzt und konkretisiert werden. Insbesondere sind hier die spezifischen datenschutzrechtlichen Vorgaben aus Art. 42 und Art. 43 DSGVO zu berücksichtigen. Daran schließt sich eine materielle Prüfung an.

Hierzu bedient sich die DAkkS der Fachexpertise der deutschen Datenschutzaufsichtsbehörden. Vor diesem Hintergrund wurden in der hiesigen Aufsichtsbehörde zwei Mitarbeiter im Umgang mit den einschlägigen Normen (z. B. ISO/IEC 17065, ISO 27001) von der DAkkS geschult und zu sog. "DAkkS-Auditoren" berufen.

Erst nach einer erfolgreichen Akkreditierung können Zertifizierungsstellen Produkte, Prozesse oder Dienstleistungen im Rahmen eines Audits auf Einhaltung der Vorgaben der Verordnung hin überprüfen und im positiven Fall zertifizieren, sprich mit einem entsprechenden Prüfsiegel bzw. Datenschutzsiegel, auszeichnen.

17 Datenschutzkonferenz

17.1 Entschließung: Novellierung des Personalausweisgesetzes – Änderungen müssen bürger- und datenschutzfreundlich realisiert werden!

24. Januar 2017

Die Bundesregierung plant grundlegende Änderungen des Personalausweisrechts. Nach dem vom Bundeskabinett beschlossenen Gesetzentwurf (BR-Drs. 787/16) werden das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger übergangen und Datenschutz sichernde Standards unterlaufen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert daher insbesondere folgende datenschutzrechtliche Anforderungen zu berücksichtigen:

- Die obligatorische Aktivierung der eID-Funktion ist dann hinnehmbar, wenn dauerhaft sichergestellt ist, dass daraus keine verpflichtende Nutzung der eID-Funktion des Personalausweises resultiert. Die Entscheidung über die Nutzung der eID-Funktion muss allein bei den Bürgerinnen und Bürgern liegen. Deren Selbstbestimmungsrecht muss gewahrt bleiben.
- An der bisherigen Verpflichtung der Ausweisbehörden, Bürgerinnen und Bürger über die eID-Funktion des Personalausweises schriftlich zu unterrichten, sollte festgehalten werden. Nur durch eine bundesweit einheitliche Vorgabe zu einer solchen Information wird sichergestellt, dass alle Bürgerinnen und Bürger in hinreichend verständlicher Form aufgeklärt werden.
- Vor einer Datenübermittlung aus dem Personalausweis müssen die Bürgerinnen und Bürger Kenntnis über den Zweck der Übermittlung erhalten; zur Wahrnehmung des Rechts auf informationelle Selbstbestimmung müssen die Betroffenen stets – wie bislang – nachvollziehen können, in welchem konkreten Kontext ihre Identitätsdaten übermittelt werden. Zudem sollte die bisherige Möglichkeit, die Übermittlung einzelner Datenkategorien auszuschließen, beibehalten werden.
- Die Einführung von organisationsbezogenen Berechtigungszertifikaten bei Diensteanbietern wird abgelehnt. Um sicherzustellen, dass Diensteanbieter nur die für den jeweiligen Geschäftsprozess erforderlichen Angaben übermittelt bekommen, sollte an der aktuellen Rechtslage festgehalten werden, nach der der antragstellende Diensteanbieter die Erforderlichkeit der aus der eID-Funktion des Personalausweises zu übermittelnden Angaben nachweisen muss und an den jeweils festgelegten Zweck gebunden ist.

- Berechtigungszertifikate dürfen nur an Diensteanbieter erteilt werden, die Datenschutz und Datensicherheit gewährleisten. Daher sollten antragstellende Diensteanbieter nach wie vor durch eine Selbstverpflichtung die Erfüllung dieser Anforderungen schriftlich bestätigen und nachweisen müssen.
- Die maßgeblichen Regelungen für die mit der Anlegung und Nutzung von Servicekonten einhergehende Erhebung und Verarbeitung von Identitätsdaten aus dem Personalausweis sowie die sicherheitstechnischen Rahmenbedingungen sollten im Personalausweisgesetz getroffen werden.
- Die Voraussetzungen für die Erstellung und Weitergabe von Personalausweisablichtungen sollten gesetzlich konkreter normiert werden. Insbesondere das Prinzip der Erforderlichkeit ist durch eine verpflichtende Prüfung der Notwendigkeit der Anfertigung einer Ablichtung sowie durch eine Positivliste von Erlaubnisgründen zu stärken. Die Einwilligung der Betroffenen als alleinige Voraussetzung birgt die Gefahr, dass in der Praxis Ablichtungen angefertigt werden, obwohl sie nicht erforderlich sind. Zudem dürfte fraglich sein, ob betroffene Personen in eine solche Maßnahme stets informiert und freiwillig einwilligen können.
- Die zum 1. Mai 2021 vorgesehene Einführung eines nahezu voraussetzungslosen Abrufs des Lichtbildes im automatisierten Verfahren durch die Polizeibehörden des Bundes und der Länder sowie die Verfassungsschutzbehörden und Nachrichtendienste wird abgelehnt. Bisher dürfen zur Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten insbesondere die Polizei- und Ordnungsbehörden Lichtbilder automatisiert abrufen, wenn die Personalausweisbehörde nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährdet. Diese gesetzlichen Einschränkungen für das Abrufverfahren sollen nun entfallen. Zudem sollen alle Nachrichtendienste künftig voraussetzungslos Lichtbilddaten abrufen können. Die bisherige Rechtslage ist völlig ausreichend.

17.2 Entschließung: Einsatz externer Dienstleister durch Berufsgeheimnisträger rechtssicher und datenschutzkonform gestalten!

15. März 2017

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Bundesgesetzgeber auf, mit dem derzeit vorliegenden Gesetzentwurf der Bundesregierung „zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“ (BR-Drs. 163/17) den Einsatz externer Dienstleister durch Berufsgeheimnisträger rechtsicher und datenschutzkonform zu gestalten.

Die Schweigepflicht ist Grundlage des für die Berufsausübung notwendigen Vertrauensverhältnisses. Aber auch Berufsgeheimnisträger können heute nicht mehr wirtschaftlich agieren, ohne die moderne Informations- und Kommunikationstechnik zu nutzen. Kaum ein Anwalt oder Arzt verfügt über das notwendige Spezialwissen, um diese Technik selbst zu warten und vor ständig neuen Bedrohungen abzusichern. Der vorliegende Gesetzentwurf will deshalb eine Praxis legalisieren, die aus Gründen der Praktikabilität längst etabliert ist. Der strafrechtliche Schutz von Privatgeheimnissen soll die Beauftragung externer Dienstleister durch Berufsgeheimnisträger nicht länger erschweren. Im Gegenzug sollen diese Auftragnehmer künftig einer strafrechtlich sanktionierten Verschwiegenheitspflicht unterliegen. Dennoch versäumt es der Gesetzentwurf, insbesondere mit der vorgeschlagenen Formulierung zu § 203 StGB, klare Verhältnisse zu schaffen. Bisher sorgte unter Ärzten - und mitunter sogar Anwälten - der Umstand für Verwirrung, dass das, was datenschutzrechtlich legitim war, noch längst nicht strafrechtlich erlaubt sein musste. Was nach dem Gesetzentwurf nunmehr strafrechtlich erlaubt sein soll, könnte wiederum nach der neuen Europäischen Datenschutz-Grundverordnung mit empfindlichen Bußgeldern in Millionenhöhe sanktioniert werden. Denn es ist weder mit dem Schutzzweck von § 203 StGB vereinbar, noch datenschutzrechtlich zulässig, dass Berufsgeheimnisträger, wie im neuen § 203 StGB vorgesehen, die Verantwortung für die Datenverarbeitung ohne Einwilligung der Betroffenen an externe Dienstleister übertragen. Nicht absehbar ist zudem, ob die Zeugnisverweigerungsrechte und das Beschlagnahmeverbot in einem weiteren Gesetzgebungsverfahren entsprechend weitgehend auf alle denkbaren Dienstleister ausgeweitet werden, die an der Berufsausübung durch Berufsgeheimnisträger mitwirken.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder dringt daher darauf, den Gesetzentwurf nachzubessern und die geplanten straf- und berufsrechtlichen Regelungen mit den datenschutzrechtlichen Vorschriften zu synchronisieren. Es muss Berufsgeheimnisträgern möglich sein, externe Dienstleister zu Rate zu ziehen. Im Sinne der ungestörten Berufsausübung der Berufsgeheimnisträger und des Rechts auf informationelle Selbstbestimmung der Betroffenen sollten die Pflichten, die den Berufsgeheimnisträger dabei aus unterschiedlichen Rechtsgebieten treffen, aber soweit als möglich gleichlaufend ausgestaltet werden.

17.3 Entschließung: Neues Bundeskriminalamtgesetz – Informationspool beschneidet Grundrechte

16. März 2017

Der „Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes“ (BT-Drs. 18/11326 und 18/11163; BR-Drs. 109/17) ändert das polizeiliche Datenschutzrecht grundlegend und betrifft Polizeibehörden in Bund und Ländern gleichermaßen. Er beschränkt sich nicht darauf, die Vorgaben des Bundesverfassungsgerichts aus dem Urteil vom 20. April 2016 zum Bundeskriminalamtgesetz und aus der neuen EU-Richtlinie zum Datenschutz im Bereich Justiz und Inneres umzusetzen. Tat-

sächlich nimmt er sogar wichtige Datenschutzregeln und Verfahrenssicherungen zurück, die der Gesetzgeber nach dem Volkszählungsurteil des Bundesverfassungsgerichts geschaffen hatte. Der Entwurf ändert den bisherigen Informationsverbund für alle Polizeibehörden grundlegend. Dieser ist nicht mehr nach Dateien untergliedert und führt zu unverhältnismäßig weitreichenden Speicherungen. In dieser Form ist dies weder durch das Urteil des Bundesverfassungsgerichts zum BKAG noch durch die EU-Richtlinie zum Datenschutz im Bereich Justiz und Inneres veranlasst. Das Urteil des Bundesverfassungsgerichts fordert, den Zweck der jeweiligen Ermittlungsmaßnahmen bei allen weiteren Schritten zu berücksichtigen, bei denen die ermittelten Daten verwendet werden. Nicht im Einklang damit steht es, Verfahrenssicherungen und datenschutzrechtliche Rahmenbedingungen aufzugeben.

Abzulehnen ist insbesondere der vorgesehene Verzicht auf Errichtungsanordnungen. Diese sind bislang Ausgangspunkt sowohl für datenschutzrechtliche Kontrollen als auch die Selbstkontrolle der Polizeibehörden. In ihnen wird festgelegt, zu welchen Zwecken personenbezogene Daten gespeichert sind. Dies ist eine wesentliche verfassungsrechtliche Vorgabe. Die neuen Regeln führen zu umfassenden themenübergreifenden Verknüpfungen und Abgleichen aller gespeicherten Personen. Sie verkürzen die Kontrollmöglichkeiten der Datenschutzaufsichtsbehörden von Bund und Ländern.

Ebenso sind die künftig durch die geplante „Mitziehautomatik" erheblich längeren Speicherfristen abzulehnen. Die geplante Neuregelung hat zur Folge, dass alte Speicherungen – auch zu Personen, die lediglich im Verdacht standen, eine Straftat begangen zu haben und die nicht verurteilt wurden – bei jedem neuen Speicheranlass ungeprüft weiter fortgeschrieben werden. Dafür soll es schon genügen, wenn die betroffene Person als Zeuge oder Kontaktperson erneut in Erscheinung tritt. Auch dies verstößt gegen das durch die ständige Rechtsprechung des Bundesverfassungsgerichtes bekräftigte Übermaßverbot.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder fordert daher, den Gesetzentwurf in der parlamentarischen Beratung datenschutzkonform zu überarbeiten!

17.4 Gesetzesentwurf zur Aufzeichnung von Fahrdaten ist völlig unzureichend!

16. März 2017

Die Bundesregierung hat im Januar 2017 einen Entwurf zur Novellierung des Straßenverkehrsgesetzes (BT-Drs. 18/11300) vorgelegt, um die Nutzung automatisierter Fahrfunktionen auf Deutschlands Straßen zu erlauben. Dabei sollen Fahrdaten aufgezeichnet werden, anhand derer bewertet werden kann, zu welchem Zeitpunkt das Auto jeweils durch den Fahrer oder durch eine „automatisierte Fahrfunktion" gesteuert wurde und wann ein Fahrer die Aufforderung zur Übernahme der Steuerung erhalten hat. Ebenfalls aufgezeichnet werden sollen Daten zu technischen Störungen

automatisierter Fahrfunktionen. Mit den Daten soll sich nach einem Unfall klären lassen, ob die Technik und damit der Hersteller oder der Fahrer für einen Unfall verantwortlich war. Welche Daten dies sind und wie das Speichermedium ausgestaltet werden soll, regelt der Gesetzentwurf nicht.

Auf Verlangen der nach Landesrecht für Verkehrskontrollen zuständigen Behörden müssen die Fahrdaten diesen Behörden übermittelt werden. Die Fahrdaten sind auch Dritten zu übermitteln, wenn diese glaubhaft machen können, dass sie die Fahrdaten zur Geltendmachung, Abwehr oder Befriedigung von Rechtsansprüchen aus Unfällen benötigen. Unklar ist, wer die Daten übermitteln muss. Es bleibt ebenfalls unbestimmt, ob ggf. auch die Behörden Fahrdaten übermitteln dürfen.

Im Gesetzesentwurf sind außerdem weder die Zwecke noch die zu übermittelnden Daten hinreichend konkretisiert. Weiterhin geht nicht hervor, wie die Integrität, Vertraulichkeit und Verfügbarkeit bei der Aufzeichnung und Übermittlung der Fahrdaten sichergestellt werden soll.

Sollte der Entwurf in der vorgelegten Form in Kraft treten, besteht in Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion die Gefahr elektronischer Fahrtenschreiber, die personenbezogene Profile bilden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Gesetzgeber zu einer dem datenschutzrechtlichen Bestimmtheitsgebot genügenden Novellierung des Straßenverkehrsgesetzes und zur Stärkung der Datenschutzrechte der Fahrer auf.

Sofern man eine Datenverarbeitung überhaupt für erforderlich hält, ist folgendes zu regeln:

- die abschließende Aufzählung derjenigen Daten, die aufgezeichnet und gespeichert werden dürfen,
- die Bestimmung des für die Verarbeitung Verantwortlichen,
- die Ergänzung einer Übermittlungs-/Zugriffsregelung für den Fahrer/Halter,
- die Konkretisierung der Daten, die den nach Landesrecht zuständigen Behörden zu übermitteln sind,
- die datenschutzgerechte Ausgestaltung des Speichermediums, insbesondere die Festlegung einer angemessenen Speicherdauer anhand der Erforderlichkeit und des Zwecks der Beweisführung für die Haftung,
- eindeutige Festlegungen für die Trennung der Daten von den in den Fahrzeugdatenspeichern der Fahrzeuge gespeicherten Daten,
- die Konkretisierung der Zwecke für die Übermittlung der gespeicherten Daten,
- die Nennung des Adressaten für das Übermittlungsverlangen,
- die abschließende Nennung berechtigter Übermittlungsempfänger und ihrer jeweiligen Verarbeitungsbefugnisse mit im Übrigen strikter Zweckbindung und
- die Konkretisierung des Löschzeitpunkts der übermittelten Daten.

17.5 Einsatz von Videokameras zur biometrischen Gesichtserkennung birgt erhebliche Risiken

29./30. März 2017

In Pilotprojekten wird derzeit der Einsatz von Videoüberwachungssystemen erprobt, die erweiterte Möglichkeiten der Verhaltensauswertung und der Identifizierung von Beobachteten bieten. Neben der Mustererkennung steht besonders die biometrische Gesichtserkennung im Fokus dieser Projekte. Dies verschärft die ohnehin schon vorhandene Problematik derartiger neuer Überwachungsverfahren, mit denen „abweichendes Verhalten" erkannt werden soll.[145]

Der Einsatz von Videokameras mit biometrischer Gesichtserkennung kann die Freiheit, sich in der Öffentlichkeit anonym zu bewegen, gänzlich zerstören. Es ist kaum möglich, sich solcher Überwachung zu entziehen oder diese gar zu kontrollieren.

Anders als bei konventioneller Videoüberwachung könnten Passanten mit dieser Technik nicht nur beobachtet und anhand bestimmter Muster herausgefiltert werden, sondern während der Überwachung anhand von Referenzbildern (Templates) automatisiert identifiziert werden. Damit wird eine dauerhafte Kontrolle darüber möglich, wo sich konkrete Personen wann aufhalten oder bewegen und mit wem sie hierbei Kontakt haben. Ermöglicht wird so die Erstellung von umfassenden Bewegungsprofilen und die Verknüpfung mit anderen über die jeweilige Person verfügbaren Daten.

Neben den genannten massiven gesellschaftspolitischen Problemen bestehen auch erhebliche rechtliche und technische Bedenken gegen den Einsatz solcher Überwachungs-techniken. Biometrische Identifizierung arbeitet mit Wahrscheinlichkeitsaussagen; bei dem Abgleich zwischen ermitteltem biometrischen Merkmal und gespeichertem Template sind falsche Identifizierungen keine Seltenheit. Beim Einsatz dieser Technik durch Strafverfolgungsbehörden kann eine falsche Zuordnung dazu führen, dass Bürgerinnen und Bürger unverschuldet zum Gegenstand von Ermittlungen und konkreten polizeilichen Maßnahmen werden. Dieselbe Gefahr besteht, falls sie sich zufällig im öffentlichen Raum in der Nähe von gesuchten Straftätern oder Störern aufhalten.

Es gibt keine Rechtsgrundlage für die Behörden von Bund und Ländern für den Einsatz dieser Technik zur Gefahrenabwehr und Strafverfolgung. Die bestehenden Normen zum Einsatz von Videoüberwachungstechnik erlauben nur den Einsatz technischer Mittel für reine Bildaufnahmen oder -aufzeichnungen, nicht hingegen für darüber hinausgehende Datenverarbeitungsvorgänge. Aufgrund des deutlich intensiveren Grundrechtseingriffs, der durch Videotechnik mit erweiterter Auswertung einher-

[145] Vgl. Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum – nicht ohne Datenschutz".

geht, können die bestehenden gesetzlichen Regelungen nicht analog als Rechtsgrundlage herangezogen werden, da sie für einen solchen Einsatz verfassungsrechtlich zu unbestimmt sind.

Nach der Rechtsprechung des Bundesverfassungsgerichts sind Maßnahmen mit großer Streubreite ein erheblicher Grundrechtseingriff. So verlangt das Bundesverfassungsgericht bereits für das automatisierte Erfassen von KFZ-Kennzeichen zwecks Abgleichs mit dem Fahndungsbestand eine normenklare und verhältnismäßige Rechtsgrundlage, die einen anlasslosen und flächendeckenden Einsatz ausschließt. Da bereits die allgemeine Regelung zur Videoüberwachung nicht zur Erfassung von KFZ-Kennzeichen ermächtigt, muss dies erst recht für die viel stärker in die Grundrechte Betroffener eingreifende Videoüberwachung zwecks Abgleichs biometrischer Gesichtsmerkmale einzelner Personen gelten. Ein Einsatz der Videoüberwachung mit Gesichtserkennung darf daher auf derzeitiger Grundlage auch im Rahmen eines Pilotbetriebs nicht erfolgen.

Der europäische Gesetzgeber hat die enormen Risiken dieser Technik für die Privatsphäre erkannt und die Verarbeitung biometrischer Daten zur Identifizierung sowohl in der ab Mai 2018 wirksamen Datenschutz-Grundverordnung als auch in der bis Mai 2018 umzusetzenden Datenschutz-Richtlinie im Bereich Justiz und Inneres nur unter entsprechend engen Voraussetzungen für zulässig erachtet. Wird über den Einsatz dieser Technik nachgedacht, muss der Wesensgehalt des Rechts auf informationelle Selbstbestimmung gewahrt bleiben und es müssen angemessene und spezifische Regelungen zum Schutz der Grundrechte und -freiheiten der Betroffenen vorgesehen werden. Hierzu gehören u. a. eine normenklare Regelung für die Verwendung von Templates, z. B. von Personen im Fahndungsbestand, für den Anlass zum Abgleich des Templates mit den aufgenommenen Gesichtern sowie zum Verfahren zur Zulassung von technischen Systemen für den Einsatz.

Etwaige gesetzliche Regelungen müssten die vorgenannten verfassungs- und europarechtlichen Bedingungen beinhalten und den mit dieser Technik verbundenen erheblichen Risiken für die Freiheitsrechte der Bürgerinnen und Bürger angemessen Rechnung tragen!

17.6 Entschließung: Göttinger Erklärung vom Wert des Datenschutzes in der digitalen Gesellschaft

29./30. März 2017

Datenschutz ist zurzeit in aller Munde: Mit der Europäischen Datenschutzreform werden ab Mai 2018 in der ganzen Europäischen Union neue einheitliche Regeln gelten. Gegenwärtig sind die Gesetzgeber in Bund und Ländern mit Hochdruck dabei, das nationale Recht an die Europäischen Vorgaben anzupassen. Zugleich schreitet die Digitalisierung der Gesellschaft mit großen Schritten voran, etwa mit dem Internet der Dinge, der Wirtschaft 4.0 und künstlicher Intelligenz, und fordert die Wahrung des Datenschutzes und die Gewährleistung der Persönlichkeitsrechte heraus. Auch

der Staat erweitert fortwährend seine Befugnisse zur Verarbeitung personenbezogener Daten, sei es zur Bekämpfung des Terrorismus und zur Gewährleistung der öffentlichen Sicherheit, sei es bei der Digitalisierung staatlicher Dienstleistungen.

Dabei gerät aber leichtfertig eines aus dem Blick: Datenschutz ist ein Grundrecht, wie die Meinungsfreiheit oder die Eigentumsgarantie. Es bindet alle Staatsgewalten unmittelbar, schützt die Menschenwürde und die freie Entfaltung der Persönlichkeit und kann auch Aspekte der Teilhabe und Chancengleichheit betreffen. Alle gesetzlichen Regelungen, sowie die Geschäftsmodelle und Anwendungen auch im Bereich der Wirtschaft, haben dies zu berücksichtigen. Immer häufiger stellen aber Verantwortliche in Politik und Wirtschaft dieses grundrechtlich geschützte Recht auf informationelle Selbstbestimmung implizit oder sogar explizit in Frage. Datenschutz wird als Hindernis diskreditiert.

Dies betrachtet die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder mit großer Sorge. Es befremdet sehr, wenn Mitglieder der Bundesregierung und andere Stimmen in der Politik in letzter Zeit immer wieder betonen, es dürfe kein Zuviel an Datenschutz geben und das Prinzip der Datensparsamkeit könne nicht die Richtschnur für die Entwicklung neuer Produkte sein. Stattdessen wird für eine vermeintliche Datensouveränität geworben, deren Zielrichtung aber im Unklaren bleibt.

Die Konferenz betont, dass Informationen über Personen keine Ware sind wie jede andere und nicht allein auf ihren wirtschaftlichen Wert reduziert werden dürfen. Gerade in Zeiten von Big Data, Algorithmen und Profilbildung bieten die digitalen Informationen ein nahezu vollständiges Abbild der Persönlichkeit des Menschen. Mehr denn je muss daher die Menschenwürde auch im digitalen Zeitalter der zentrale Maßstab staatlichen und wirtschaftlichen Handelns sein. Zu einer menschenwürdigen und freien Entfaltung der Persönlichkeit gehört die freie Selbstbestimmung über das eigene Ich.

„Datensouveränität" verstanden als eigentumsähnliche Verwertungshoheit kann daher nur zusätzlich zum Recht auf informationelle Selbstbestimmung greifen, dieses jedoch keinesfalls ersetzen.

Die Konferenz fordert daher alle Entscheidungsträger in Politik und Wirtschaft auf, den hohen Wert des Rechts auf informationelle Selbstbestimmung für eine freiheitliche Gesellschaft zu achten und sich nachdrücklich vertrauensbildend für die Persönlichkeitsrechte einzusetzen. Datenschutz stellt kein Hindernis für die Digitalisierung dar, sondern ist wesentliche Voraussetzung für deren Gelingen.

Die Entwicklung datenschutzkonformer IT-Produkte und -Verfahren muss nachhaltig gefördert werden, um den Datenschutz zu einem Qualitätsmerkmal der europäischen Digitalwirtschaft zu machen.

17.7 Grundsatzpositionen und Forderungen für die neue Legislaturperiode

Die fortschreitende Digitalisierung eröffnet wirtschaftliche und gesellschaftspolitische Chancen. Mit ihr einhergehen jedoch erhebliche Risiken für die Persönlichkeitsrechte der Menschen. Ein an diese Entwicklungen angepasster und damit starker Datenschutz ist das Gebot der Stunde.

Die Datenschutzkonferenz formuliert zu Beginn der Legislatur elf handlungsorientierte Grundforderungen, deren Ziel es ist, das Datenschutzrecht weiter zu entwickeln und seine Durchsetzung und Akzeptanz zu fördern. Ein wirksamer Datenschutz ist Grundrechtsschutz und darf nicht als Hindernis betrachtet werden. Er muss vielmehr als integraler und förderlicher Bestandteil politischer, wirtschaftlicher und gesellschaftlicher Fortentwicklung verstanden und gelebt werden.

Digitale Souveränität – Datensouveränität

Die DSK fordert, das Verbotsprinzip nach der DSGVO nicht durch den Anspruch auf „Datensouveränität" aufzuweichen.

„Datensouveränität" ist ein Schlagwort in der politischen Auseinandersetzung um die zeitgemäße Positionierung des Datenschutzes, das in unterschiedlichen Zusammenhängen gebraucht wird. Aus der Alltagssprache entnommen, wird der aus dem Staatsrecht stammende Begriff „Souveränität" mit selbstbestimmtem Handeln assoziiert, der einen Anspruch auf (absolute) Herrschaft über die eigenen persönlichen Daten beinhaltet. Dies allerdings kommt nach gegenwärtigem Rechtsverständnis allenfalls im Kernbereich privater Lebensgestaltung in Betracht. Zudem trifft er datenschutzrechtliche Anforderungen ebenso wenig wie das mit dem neuen Begriff angestrebte Ziel, Daten zu einer rein wirtschaftlichen Größe zu machen und damit Einschränkungen des Datenschutzes zu verschleiern. Die DSK spricht sich daher dafür aus, auch künftig das aus der Menschenwürde abgeleitete Recht auf informationelle Selbstbestimmung in den Mittelpunkt zu stellen und bei dem funktionalen Begriff des datenschutzrechtlichen Verbotsprinzips zu bleiben.

Grundsatz der Datenminimierung

Die DSK fordert, der Datenminimierung die ihr gemäß DSGVO gebührende Überholspur auf dem Weg der Digitalisierung frei zu räumen.

Datenminimierung heißt, dass personenbezogene Daten auf das für die Zwecke der Verarbeitung erforderliche Maß beschränkt sein müssen. Dies ist notwendig, um die mit der Datenverarbeitung einhergehenden Risiken für die betroffenen Personen einzudämmen. Der Grundsatz der Datenminimierung lässt sich aus dem Verfassungsrecht der EU und Deutschlands ableiten und wurde zu einem der Hauptprinzipien der DSGVO erhoben (Art. 5 Abs. 1 lit. c DSGVO). Damit ist Datenminimierung Rahmenbedingung jeder Datenverarbeitung in Europa und steht nicht zur Disposition des deutschen Gesetzgebers.

Hierdurch werden Innovationen nicht verhindert: Clevere Datenminimierungslösungen können das Bedürfnis zur Auswertung von Informationen und die Notwendigkeit des Datenschutzes vereinen, z. B. indem auf den Personenbezug von Daten verzichtet wird. Technologische Projekte, die Datenminimierung innovativ und intelligent umsetzen und damit erst rechtskonforme Geschäftsmodelle im Zusammenhang mit Big Data-Anwendungen und „smarten" Lösungen ermöglichen, sollten gefördert werden.

Rahmenbedingungen für datenschutzfreundliche und sichere Systemgestaltung

Die DSK fordert, datenschutzfreundliche und sichere Systemgestaltung stärker öffentlich zu fördern.

Nach der DSGVO sollen nicht nur die erforderlichen technisch-organisatorischen Maßnahmen für Datensicherheit getroffen werden, sondern Datenschutz soll von Anfang an und über den gesamten Lebenszyklus hinweg in Produkte, Dienste und Anwendungen eingebaut sein.

Daher sollten Initiativen und Projekte verstärkt gefördert werden, die Datenschutz „by Design" und „by Default" gewährleisten und die Qualität der Datensicherheit verbessern. Die DSK fordert die Bundesregierung auf, sich für technologische Innovationen mit eingebautem Datenschutz einzusetzen und diese auch im Austausch mit Vertretern aus Wirtschaft, Forschung und Entwicklung voranzubringen. Auch sollten alle von der Bundesregierung geförderten Vorhaben mit Personenbezug zukünftig belegen, wie sie die Datenschutzanforderungen erfüllen, damit die Resultate rechtskonform sind. Datenschutzfreundliche und sichere Systemgestaltung ist im Sinne der Vorbildfunktion des öffentlichen Sektors in den öffentlichen Stellen des Bundes sowie in bestehenden oder aufzubauenden IT-Infrastrukturen nachzuweisen. Im Bereich der nationalen, europäischen und internationalen Standardisierung soll die Bundesregierung darauf hinwirken, dass Datenschutzanforderungen eine entsprechende Berücksichtigung finden. Dies betrifft auch einheitliche Vorgaben und Schnittstellen für den Selbstdatenschutz und ein angemessenes Niveau bei Zertifizierungen.

Klare gesetzliche Regelungen für automatisierte Entscheidungen durch Algorithmen

Die DSK fordert, für den Einsatz von Algorithmen im Hinblick auf Transparenz, Kontrolle und Begrenzung klare gesetzliche Regelungen zu schaffen.

Die digitale Informationsgesellschaft ist von Verfahren geprägt, die in unterschiedlichster Art und Weise automatisierte Entscheidungen treffen. Hinter ihnen verbergen sich Algorithmen, bei denen oft nicht ersichtlich ist, welche Daten als Grundlage für Entscheidungen herangezogen werden bzw. wie diese der Entscheidungsfindung dienen. Die Komplexität von Algorithmen macht es häufig unmöglich, ihre Funktionsweise analytisch zu bewerten. Sie entscheiden bspw. über Fahrzeugreaktionen, ob ein Kredit gewährt oder welcher Versicherungstarif angeboten wird und das meist ohne Berücksichtigung der individuellen Situation betroffener Personen. Es besteht

die Gefahr von Diskriminierungen und Stigmatisierungen, eingeschränkten Auswahlmöglichkeiten bis hin zu Fehlentscheidungen. Menschen dürfen algorithmischen Entscheidungen nicht bedingungslos ausgeliefert werden. Es bedarf daher Regelungen zu Einsatzvoraussetzungen, Entwicklung, Prüfung und Verwendung von Algorithmen, deren Einsatzzweck in automatisierten Entscheidungen liegt.

Die DSK fordert, die Einschränkung von Aufsichtsbefugnissen und Betroffenenrechten zurückzunehmen sowie die Regelungen zur Videoüberwachung europarechtskonform auszugestalten.

Den Untersuchungsbefugnissen der Aufsichtsbehörden sind Datenverarbeitungen entzogen, die dem Steuergeheimnis, der ärztlichen Schweigepflicht oder anderen Geheimhaltungspflichten unterliegen. Diese Beschneidung der Befugnisse gegenüber Berufsgeheimnisträgern geht weit über die Öffnungsklausel des Art. 90 DSGVO hinaus. Es sollte die bisherige Regelung des § 38 Abs. 3, 4 i. V. m. § 24 Abs. 2 und Abs. 6 BDSG-alt beibehalten werden. Die Aufsicht durch unabhängige Datenschutzbehörden dient den Interessen der betroffenen Personen. Geheimhaltungspflichten sind durch § 29 Abs. 3 S. 2 BDSG hinreichend geschützt.

Übermäßige Einschnitte in die Betroffenenrechte widersprechen dem Schutzcharakter der DSGVO. Beschränkungen dürfen nicht den Wesensgehalt der Grundrechte und Grundfreiheiten tangieren, müssen in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahmen darstellen sowie die in Art. 23 Abs. 1 DSGVO aufgezählten Ziele sicherstellen.

Die Vorschrift zur Videoüberwachung ist, soweit sie nicht-öffentliche Stellen betrifft, zu streichen. Sie lässt sich nicht auf den herangezogenen Art. 6 Abs. 1 S. 1 lit. e i. V. m. Art. 6 Abs. 3 S. 1 DSGVO stützen. Zudem erlaubt die ohnehin unmittelbar geltende DSGVO einen angemessenen Ausgleich zwischen den berechtigten Interessen der Verantwortlichen an einer Videoüberwachung und dem Schutz der Persönlichkeitsrechte der Betroffenen.

Innere Sicherheit unter Wahrung des Datenschutzes

Die DSK fordert, bei der Bekämpfung von Terrorismus und Kriminalität das Vertrauen unbescholtener Menschen in die Vertraulichkeit ihrer Kommunikation und die Unberührtheit ihrer Privatheit zu wahren.

Datenschutz steht nicht im Widerspruch zu Sicherheit. Datenschutz schafft Sicherheit, denn das Grundrecht auf Schutz personenbezogener Daten verlangt klare gesetzliche Regelungen, die transparent für den Einzelnen die Leitplanken für die Ausübung seiner Rechte und deren Grenzen festlegen. Datenschutz bringt Rechtsklarheit und Rechtsklarheit trägt zur Steigerung des Gefühls der Sicherheit bei. Nur Sicherheit in Freiheit ist wirkliche Sicherheit für alle.

Auch das Verhalten im öffentlichen Raum muss grundsätzlich von Beobachtung, Aufzeichnung biometrischer Erfassung und automatisierter Auswertung frei bleiben. Eine massenhafte, verdachtsunabhängige Erhebung und Speicherung von Daten widerspricht den Grund-rechten. Die Vorratsdatenspeicherung ist daher in all ihren Ausprägungen auf den Prüfstand zu stellen. Befugnisse zu Überwachungsmaßnahmen müssen einem gestuften System folgen, wonach sich die Rechtfertigung für einen Grundrechtseingriff an der Eingriffsintensität bemisst.

Betroffene sind über sicherheitsbehördliche Maßnahmen zu informieren. Sollte dies nicht möglich sein, ist umso mehr eine unabhängige Kontrolle zu gewährleisten: Eine effektive Datenschutzkontrolle muss Sanktions- und Anordnungsbefugnisse und auch die Kontrolle der Nachrichtendienste umfassen. Auch grenzüberschreitende Datenübermittlungen dürfen davon nicht ausgeschlossen sein. Diese Prinzipien sind bei einer Änderung oder Neufassung von Sicherheitsgesetzen auch aus Anlass der Anpassung an Vorgaben der EU zu beachten.

Arbeiten 4.0 – ein Beschäftigtendatenschutzgesetz für die neue Arbeitswelt

Die DSK fordert, den Beschäftigtendatenschutz durch ein eigenständiges Gesetz zu regeln

§ 26 BDSG-neu übernimmt weitgehend die bisher geltenden Regelungen des BDSG-alt. Diese sind jedoch unzureichend. Die Arbeitswelt 4.0 erweitert z. B. die Möglichkeiten der offenen und verdeckten technischen Überwachung erheblich. Ein angemessener Ausgleich zwischen In-formationsinteressen des Arbeitgebers und Schutz der Rechte und Freiheiten des Arbeitnehmers ist nur durch eine differenzierte, umfassende gesetzliche Regelung zu erreichen.

Big Data im Gesundheitswesen

Die DSK fordert, für die Auswertung von Gesundheitsdaten strikte gesetzliche Vorgaben zu machen.

Gesundheitsdaten unterliegen dem strengeren Regelungsregime für besondere Kategorien personenbezogener Daten. Zunehmend werden sehr große Mengen von Gesundheitsdaten aus den unterschiedlichsten Lebensbereichen zusammengeführt und mit sog. Big Data-An-wendungen systematisch ausgewertet.

Verknüpfungen zwischen verschiedenen Datenbeständen, die Gesundheitsdaten enthalten, dürfen nur auf der Grundlage spezieller rechtlicher Regelungen zugelassen werden. Die Re-Identifizierung und unerlaubte Zusammenführung von Daten, das Anlegen von Datenprofilen zu einer Person sowie der Handel mit Gesundheitsdaten sind zu verbieten und unter Strafe zu stellen. Es muss zudem gesetzlich festgelegt werden, dass mit anonymisierten bzw. hinreichend pseudonymisierten Daten gearbeitet wird, in welchen Zusammenhängen ausnahmsweise auf die Einwilligung als Legitimation für eine Verarbeitung von Gesundheitsdaten in Big Data-Anwendungen zurückgegriffen werden darf und unter welchen Voraussetzungen eine wirksame Einwilligung gegeben werden kann. Zudem sind Transparenzvorgaben z. B. hin-sichtlich der Analysemethoden, der Verarbeitungszwecke und der genutzten Datenbestände bei geplanten Big Data-Projekten zu machen. Es sollte gesetzlich vorgesehen werden, dass für jedes Big Data-Projekt im Gesundheitswesen das Votum der zuständigen Datenschutzaufsichtsbehörde eingeholt wird.

E-Health

Die DSK fordert, bei der Digitalisierung des Gesundheitswesens („E-Health") das Recht auf Schutz personenbezogener Daten der Patienten und Versicherten gesetzlich wirksam zu sichern.

Auch künftig muss das Vertrauensverhältnis zwischen Patienten und ihren Behandlern effektiv geschützt werden. Vor einer Nutzung neuer technischer Anwendungen ist deshalb ein den Anforderungen der DSGVO genügender Datenschutz- und Datensicherheitsstandard sicherzustellen. Bei einer Integration mobiler oder anderer neuer Technologien in die Regelversorgung sowie in das E-Health-System ist deren datenschutz- und datensicherheitsgerechte Ausgestaltung zu garantieren. Ebenso ist Transparenz für die Nutzer herzustellen. Zu verhindern ist, dass Gesundheitsdaten zur Bemessung von Versicherungstarifen laufend erhoben und vertragsbegleitend genutzt werden. Im Bereich der Krankenversicherung drohen mit der Erhebung von Gesundheitsdaten mittels sog. Wearables und Fitness-Apps Diskriminierungen von Versicherten durch das Angebot gesundheitsbezogener Tarife. Bei der Bemessung von Versicherungstarifen dürfen nicht die Patienten und Versicherten benachteiligt werden, die einer umfassenden Erfassung und Übertragung von Gesundheitsdaten nicht zustimmen.

Mit Datenschutz E-Government gestalten

Die DSK fordert, für die verwaltungsebenenübergreifende Umsetzung von E-Government Verwaltungsdienstleistungen sicher und datenschutzgerecht anzubieten.

Das Onlinezugangsgesetz schafft zwar durch einen Portalverbund zwischen allen Verwaltungsangeboten des Bundes, der Länder und der Kommunen sowie ein Nutzerkonto für jedermann die rechtlichen Voraussetzungen. Die DSK weist aber darauf hin, dass E-Government Akzeptanz in der Verwaltung wie bei den Bürgern bedingt.

Die DSK fordert deshalb Bund und Länder auf, mit Datenschutz E-Government konsequent vertrauenswürdig zu gestalten, im Sinne eines Datenschutzes „by Design" und „by Default". Die Ende-zu-Ende-Verschlüsselung der Kommunikation, Konzepte mit Datenschutzgarantien (z. B. datenschutzkonforme Bezahlsysteme und deutsche oder europäische „Trusted-Cloud"-Lösungen) und ein umfassendes Datenschutz- und Informationssicherheitsmanagement bilden dafür wesentliche Grundlagen. Rechtskonform müssen auch neue Entwicklungen wie „Data Driven Government" – Verwaltungsentscheidungen auf Basis von Daten und Analysen – umgesetzt werden: mit Techniken zur Anonymisierung und Aggregation statt zentralisierter Anhäufung und Auswertung personenbezogener Daten.

Stärkung des internationalen Datenschutzes

Die DSK fordert die Bundesregierung auf, sich bei Entscheidungen der Europäischen Kommission über die Zulässigkeit von Datentransfers in Drittstaaten für ein hohes Datenschutzniveau einzusetzen. Zudem sind Versuche abzuwehren, den Datenschutz durch internationale Handelsverträge einzuschränken.

Das Bestreben der Europäischen Kommission, Drittstaatentransfer auf der Basis von Angemessenheitsbeschlüssen zu vereinfachen, darf nicht zu einer Erosion des Grundrechts auf informationelle Selbstbestimmung führen.

Die Bundesregierung sollte sich daher dafür einsetzen, dass die vom EuGH (C-362/14) aufgestellten Grundsätze Maßstab für Angemessenheitsentscheidungen bleiben. Künftige Handelsverträge dürfen den Datenschutz nicht aushöhlen, indem datenschutzrechtliche Regelungen als Handelshemmnis angesehen oder zum Gegenstand etwaiger Investor-Staat-Streitverfahren werden. Auch datenschutzrechtliche Standards im Europarat, in der OECD und den Vereinten Nationen müssen ein vergleichbar hohes Datenschutzniveau aufweisen.

17.8 Entschließung: Keine anlasslose Vorratsspeicherung von Reisedaten

8./9. November 2017

Der Gerichtshof der Europäischen Union (EuGH) hat in seinem Gutachten vom 26. Juli 2017 (Gutachten 1/15) zum Fluggastdaten-Abkommen der EU mit Kanada die langfristige Speicherung von Fluggastdaten (Passenger Name Records -PNR-Daten) sämtlicher Passagiere für nicht mit der Europäischen Grundrechtecharta vereinbar erklärt und seine Position zu anlasslosen Speicherungen personenbezogener Daten bekräftigt. Er erteilt damit einer anlasslosen Vorratsdatenspeicherung von personenbezogenen Daten erneut eine klare Absage. Die Aussagen des EuGH sind nicht nur auf alle geltenden PNR-Instrumente übertragbar und stellen Anforderungen an die Anpassung des Fluggastdatengesetzes, sie betreffen auch die auf europäischer Ebene angestrebte Einrichtung eines Entry-Exit-Systems (EES) sowie eines EU-weiten Reiseinformations- und -genehmigungssystems (ETIAS), die ebenfalls weitreichende anlasslose Speicherungen beabsichtigen.

Zwar hält der EuGH es grundsätzlich für zulässig, Fluggastdaten automatisiert zu übermitteln und auszuwerten, um Personen zu ermitteln, die eine potentielle Gefahr für die öffentliche Sicherheit darstellen und bei ihrer Einreise einer gewissenhaften Kontrolle unterzogen werden sollen. Das gilt jedoch nicht für sensible Daten, die Rückschlüsse etwa auf die rassische und ethnische Herkunft, religiöse Überzeugungen oder das Sexualleben ermöglichen. Der Übermittlungszweck rechtfertigt auch nicht automatisch die weitere Verwendung und Speicherung der Daten. Die übermittelten Daten haben vielmehr ihren Zweck erfüllt, wenn sich während des Aufenthaltes keine konkreten Anhaltspunkte für geplante terroristische oder andere schwere Straftaten ergeben haben. In diesem Fall sieht der EuGH keine Rechtfertigung für eine weitere Speicherung der Daten.

Das Fluggastdatengesetz, mit dem die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von PNR-Daten zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität umgesetzt wurde, geht insbesondere durch die Einbeziehung der innereuropäischen Flüge, die im Widerspruch zu dem Grundsatz des freien Personenverkehrs im Schengen-Raum steht, noch über den verpflichtenden Teil der Richtlinie hinaus.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) sieht in den vom EuGH ausgesprochenen Feststellungen zur Rechtslage einen unverzichtbaren Maßstab für die Verordnungsvorschläge zur Einrichtung eines neuen Entry-Exit-Systems (EES) sowie eines EU-weiten Reiseinformations- und -genehmigungssystems (ETIAS).

Mit dem EES sollen alle Ein- und Ausreisen sowie Einreiseverweigerungen von Drittstaatlern in die EU zentral erfasst und für mehrere Jahre gespeichert werden (einschließlich biometrischer Identifizierungsmerkmale). Im ETIAS sollen zum Zwecke der Erleichterung der Grenzkontrollen vorab Daten von einreisewilligen visabefreiten Drittstaatlern erhoben und ebenfalls für mehrere Jahre zentral gespeichert werden. In beiden Datenbanken sollen also Daten, die im Rahmen der Einreise und Grenzkontrolle erhoben werden, ebenso wie nach dem PNR-Abkommen, ohne konkreten Anlass zentral für einen langen Zeitraum vorgehalten werden. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hält dies nicht für vertretbar.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert die je-weils zuständigen Gesetzgeber auf, zeitnah und konsequent sämtliche PNR-Instrumente der EU im Sinne der EuGH-Rechtsprechung nachzubessern, insbesondere das deutsche Fluggastdatengesetz.

Sie fordert die Bundesregierung zudem auf, sich auf europäischer Ebene für eine den Anforderungen der EU-Grundrechtecharta und der Rechtsprechung des EuGH entsprechende Ausgestaltung der angestrebten Systeme EES und ETIAS einzusetzen.

17.9 Entschließung: Umsetzung der DSGVO im Medienrecht

8./9. November 2017

Das Inkrafttreten der Datenschutzgrundverordnung (DSGVO) und deren Geltungsbeginn im Mai 2018 verlangt eine Anpassung der medienrechtlichen Datenschutzbestimmungen an die neuen Vorgaben. Dabei muss dem hohen Stellenwert der Meinungs- und Informationsfreiheit sowie der Presse-, Rundfunk- und Medienfreiheit gemäß Art. 5 Grundgesetz (GG) und Art. 11 EU-Grundrechtecharta (GRCh)[146] für die freiheitliche demokratische Grundordnung ebenso Rechnung getragen werden wie dem Recht auf Informationelle Selbstbestimmung gemäß Art. 1 i. V. m. Art. 2 GG und dem Recht auf Schutz personenbezogener Daten gemäß Art. 8 GRCh. Kollisionen der Schutzbereiche der Grundrechte sind im Sinne einer praktischen Konkordanz aufzulösen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder weist daher auf die Anpassungsklausel des Art. 85 DSGVO hin. Danach können die Mitgliedstaaten Ausnahmen und Abweichungen von bestimmten Vorgaben der

[146] Charta der Grundrechte der Europäischen Union vom 12.12.2007 in der Fassung vom 7.6.2016 (ABl. Nr. C 202 S. 389).

DSGVO normieren, wenn „dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen". Das sich daraus ergebende Regel-Ausnahme-Verhältnis bedeutet, dass die Vorgaben der DSGVO grundsätzlich auch auf sämtliche Verarbeitungen personenbezogener Daten zu grundrechtlich besonders geschützten journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken angewendet werden sollen.

Bei der Umsetzung von Art. 85 DSGVO gilt es insbesondere folgende Anforderungen zu beachten:

- Ausnahmen oder Abweichungen von der Anwendung der DSGVO auf die Verarbeitung personenbezogener Daten im journalistischen Bereich müssen notwendig sein, um freie Meinungsäußerung und Informationsfreiheit gemäß Art. 11 GRCh sicherzustellen.
- Einen regelhaften Vorrang der Presse-, Rundfunk- und Medienfreiheit sieht die DSGVO nicht vor. Sie verlangt vielmehr, einen angemessenen Ausgleich zwischen den Grundrechten herzustellen, wenn diese in Widerstreit geraten (vgl. 153. Erwägungsgrund der DSGVO).
- Die Grundsätze des Datenschutzes (Art. 5 DSGVO) müssen hinreichend Beachtung finden. Jedenfalls steht es nicht im Einklang mit dem Recht auf Schutz personenbezogener Daten, wenn die Grundsätze des Datenschutzes im Journalismus in weitem Umfang ausgeschlossen werden. Eine Regelung kann keinesfalls als notwendig i. S. d. DSGVO angesehen werden, wenn sie zum Zwecke der Abwägung mit der Meinungs- und Informationsfreiheit die Transparenzrechte und Interventionsmöglichkeiten für betroffene Personen sowie Verfahrensgarantien über eine unabhängige Aufsicht missachtet.
- Über den eingeräumten Gestaltungsspielraum geht es hinaus, wenn die Verarbeitung personenbezogener Daten durch Hilfsunternehmen zu undifferenziert vom Geltungsbereich der DSGVO ausgenommen wird, ohne dass diese Aktivitäten unmittelbar der journalistischen Tätigkeit dienen. Die Reichweite der journalistischen Tätigkeit bedarf zudem einer Konkretisierung.
- Die künftige Aufsicht über den Datenschutz beim Rundfunk ist unabhängig auszugestalten. Sie bedarf wirksamer Abhilfebefugnisse bei Datenschutzverstößen.
- Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert daher für die Anpassung von Rundfunk-Staatsverträgen, Presse- und Medien-gesetzen:
- Die gesetzlichen Anpassungen i. S. d. Art. 85 DSGVO müssen konkret und spezifisch – bezogen auf die jeweiligen Normen und Vorgaben der DSGVO – Ausnahmen und Abweichungen regeln und diese begründen.
- Bei der Ausübung der jeweiligen Regelungskompetenz ist das europäische Datenschutzrecht zwingend zu beachten. Eine faktische Beibehaltung der bisherigen nationalen Rechtslage würde dem nicht gerecht.

17.10 Entschließung: Facebook Datenskandal – Neues Europäisches Datenschutzrecht bei Sozialen Netzwerken durchsetzen!

25./26. April 2018

Im März 2018 wurde in der Öffentlichkeit bekannt, dass über eine von November 2013 bis Mai 2015 mit Facebook verbundene App nach Angaben des Unternehmens Daten von 87 Millionen Nutzern weltweit, davon 2,7 Millionen Europäern und etwa 310.000 Deutschen erhoben und an das Analyseunternehmen Cambridge Analytica weitergeben wurden. Dort wurden sie offenbar auch zur Profilbildung für politische Zwecke verwendet.

Aus diesem Anlass hat der national zuständige Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ein Bußgeldverfahren gegen Facebook eingeleitet. Er steht dabei in engem Austausch mit seinen europäischen Kollegen, insbesondere mit dem Information Commissioner's Office in Großbritannien sowie der Artikel-29-Gruppe. Der Datenskandal um Facebook und Cambridge Analytica wirft ein Schlaglicht auf den Umgang mit Millionen Nutzerdaten. Zudem dokumentieren die Vorgänge um Cambridge Analytica, dass Facebook über Jahre hinweg den Entwicklern von Apps den massenhaften Zugriff auf Daten von mit den Verwendern der Apps befreundeten Facebook-Nutzenden ermöglicht hat. Das geschah ohne eine Einwilligung der Betroffenen. Tatsächlich ist der aktuell diskutierte Fall einer einzelnen App nur die Spitze des Eisbergs. So geht die Zahl der Apps, die das Facebook-Login-System nutzen, in die Zehntausende. Die Zahl der davon rechtswidrig betroffenen Personen dürfte die Dimension des Cambridge-Analytica-Falls in dramatischer Weise sprengen und dem Grunde nach alle Facebook-Nutzenden betreffen. Das Vorkommnis zeigt zudem die Risiken für Profilbildung bei der Nutzung sozialer Medien und anschließendes Mikrotargeting, das offenbar zur Manipulation von demokratischen Willensbildungsprozessen eingesetzt wurde.

Die Datenschutzkonferenz fordert aus diesen offenbar massenhaften Verletzungen von Datenschutzrechten Betroffener folgende Konsequenzen zu ziehen:

- Soziale Netzwerke müssen ihre Geschäftsmodelle auf die neuen europäischen Datenschutzregelungen ausrichten und ihrer gesellschaftlichen Verantwortung nachkommen. Dazu gehört auch, angemessene Vorkehrungen gegen Datenmissbrauch zu treffen.
- Facebook muss den wahren Umfang der Öffnung der Plattform für App-Anbieter in den Jahren bis 2015 offenlegen und belastbare Zahlen der eingestellten Apps sowie der von dem Facebook-Login-System betroffenen Personen nennen. Ferner gilt es Betroffene über die Rechtsverletzungen zu informieren.
- In Zukunft muss Facebook sicherstellen, dass die Vorgaben der Datenschutz-Grundverordnung (DS-GVO) rechtskonform umgesetzt werden: Die Vorstellung von Facebook zur Einführung der automatischen Gesichtserkennung in Europa lässt erhebliche Zweifel aufkommen, ob das Zustimmungsverfahren

mit den gesetzlichen Vorgaben insbesondere zur Einwilligung vereinbar ist. Wenn Facebook die Nutzenden dazu drängt und es ihnen wesentlich leichter macht, der biometrischen Datenverarbeitung zuzustimmen, als sich ihr zu entziehen, führt dies zu einer unzulässigen Beeinflussung des Nutzers.

- Die Reaktionen auf datenschutzwidriges Verhalten sind dabei nicht allein auf den Vollzug des Datenschutzrechts beschränkt, sondern betreffen auch das Wettbewerbs- und Kartellrecht. Die Forderung nach einer Entflechtung des Facebook-Konzerns wird in dem Maße zunehmen, wie sich dieser durch die systematische Umgehung des Datenschutzes wettbewerbswidrige Vorteile auf dem Markt digitaler Dienstleistungen zu verschaffen versucht. Es bedarf europäischer Initiativen, um monopolartige Strukturen im Bereich der sozialen Netzwerke zu begrenzen und Transparenz von Algorithmen herzustellen.

Weil Datenverarbeitungsprozesse zunehmend komplexer und für Betroffene intransparenter werden, kommt der Datenschutzaufsicht eine elementare Rolle zu. Ihre fachliche Expertise ist gefragt, sie muss organisatorisch und personell in der Lage sein, beratend und gestaltend tätig zu sein. Ein starkes Datenschutzrecht und effektive Aufsichtsbehörden vermindern gemeinsam die Risiken für die Bürgerinnen und Bürger in der digitalen Gesellschaft. Sollten Facebook und andere soziale Netzwerke nicht bereit sein, den europäischen Rechtsvorschriften zum Schutz der Nutzenden nachzukommen, muss dies konsequent durch Ausschöpfung aller vorhandenen aufsichtsbehördlichen Instrumente auf nationaler und europäischer Ebene geahndet werden.

17.11 Entschließung: Zuverlässigkeitsüberprüfungen bei öffentlichen und privaten Veranstaltungen nur im erforderlichen Maß und nach einem rechtsstaatlichen und transparenten Verfahren

25./26. April 2018

Zunehmend werden im Rahmen von öffentlichen und privaten Veranstaltungen Personen, die in unterschiedlichen Funktionen auf einem Veranstaltungsgelände tätig werden wollen oder sonst Zutritt zu Sicherheitszonen begehren (bspw. Anwohner), durch Sicherheitsbehörden auf ihre Zuverlässigkeit überprüft. Auch bei privaten Veranstaltungen fordern die Polizeien die Veranstalter bisweilen dazu auf, dafür zu sorgen, dass alle im Rahmen der Veranstaltung Tätigen einer solchen Prüfung unterzogen werden. In den meisten Fällen ist alleinige Grundlage für diese Maßnahmen immer noch die Einwilligung der Betroffenen.

Bereits vor mehr als zehn Jahren haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 25./26. Oktober 2007 darauf hingewiesen, dass allein die Einwilligung der Betroffenen in eine Zuverlässigkeitsüberprüfung keine legitimierende Grundlage für solche tiefen Eingriffe in das Recht auf informationelle Selbstbestimmung darstellen kann. Die wiederholten Forderungen nach

Schaffung gesetzlicher Grundlagen haben seitdem die Gesetzgeber nur weniger Bundesländer aufgegriffen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) fordert die Gesetzgeber und die Verantwortlichen deshalb erneut nachdrücklich auf, für ein rechtsstaatliches und transparentes Verfahren solcher Zuverlässigkeitsüberprüfungen zu sorgen, das auf das absolut erforderliche Maß beschränkt bleibt, sowohl was den Umfang der Überprüfung als auch den betroffenen Personenkreis betrifft. Dabei sind insbesondere folgende Rahmenbedingungen zu beachten:

Zuverlässigkeitsüberprüfungen nur aufgrund einer spezifischen Rechtsgrundlage

Die Gesetzgeber werden aufgefordert, bereichsspezifische Rechtsgrundlagen zu schaffen, die den Grundsatz der Verhältnismäßigkeit beachten und aus denen sich die Voraussetzungen und der Umfang der Überprüfungen klar und für die Bürger erkennbar ergeben.

Zuverlässigkeitsüberprüfungen nur im erforderlichen Maß

Anwendung, Umfang, Kreis der betroffenen Personen und die Datenverarbeitung sind auf das Erforderliche zu beschränken. Generell dürfen Zuverlässigkeitsüberprüfungen nur bei solchen Veranstaltungen eingesetzt werden, die aufgrund ihrer spezifischen Ausprägung infolge einer belastbaren Gefahrenprognose als besonders gefährdet bewertet werden.

Korrespondierend müssen die personenbezogenen Daten, die in den zum Abgleich herangezogenen Dateien und Informationssystemen gespeichert sind, nicht nur eine ausreichende Qualität haben, es dürfen auch nur hinreichend gewichtige Delikte in die Überprüfung einbezogen werden. Zudem müssen die Kriterien, die zur Annahme von Sicherheitsbedenken führen, einen konkreten Bezug zu den abzuwehrenden Gefahren haben.

Zuverlässigkeitsüberprüfungen nur in einem transparenten Verfahren

Die Rechte und Freiheiten der betroffenen Personen müssen durch ein transparentes Verfahren gewährleistet werden. Dazu müssen insbesondere Anhörungsrechte der betroffenen Personen rechtlich verankert werden. Im praktischen Verfahren kann im Einzelfall auch die Einrichtung einer Clearingstelle sinnvoll sein. Zudem sollten zumindest die Datenschutzbeauftragten der Verantwortlichen frühzeitig vorab beteiligt werden, damit eine datenschutzrechtliche Beratung für eine datensparsame Ausgestaltung und Beschränkung des konkreten Verfahrens stattfinden kann.

17.12 Beschluss: Datenschutzbeauftragten-Bestellpflicht nach Artikel 37 Abs. 1 lit. c Datenschutz-Grundverordnung bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs

25./26. April 2018

1. Betreibt ein einzelner Arzt, Apotheker oder sonstiger Angehöriger eines Gesundheitsberufs eine Praxis, Apotheke oder ein Gesundheitsberufsunternehmen und sind dort einschließlich seiner Person in der Regel mindestens 10 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt, besteht eine gesetzliche Verpflichtung zur Benennung eines Datenschutzbeauftragten (DSB).

2. Bei Ärzten, Apothekern oder sonstigen Angehörigen eines Gesundheitsberufs, die zu mehreren in einer Berufsausübungsgemeinschaft (Praxisgemeinschaft) bzw. Gemeinschaftspraxis zusammengeschlossen sind oder die ihrerseits weitere Ärzte, Apotheker bzw. sonstige Angehörige eines Gesundheitsberufs beschäftigt haben, ist in der Regel nicht von einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten im Sinne von Art. 37 Abs. 1 lit. c DS-GVO auszugehen – in diesen Fällen ist unter Berücksichtigung von Punkt 3 dann kein DSB zu benennen, wenn weniger als 10 Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind.

3. Bei Ärzten, Apothekern oder sonstigen Angehörigen eines Gesundheitsberufs, die zu mehreren in einer Berufsausübungsgemeinschaft (Praxisgemeinschaft) bzw. Gemeinschaftspraxis zusammengeschlossen sind oder die ihrerseits weitere Ärzte, Apotheker bzw. sonstige Angehörige eines Gesundheitsberufs beschäftigt haben, bei denen ein hohes Risiko für die Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten zu erwarten ist, ist eine Datenschutzfolgenabschätzung vorgeschrieben und damit zwingend ein Datenschutzbeauftragter zu benennen. Dies kann neben einer umfangreichen Verarbeitung (z. B. große Praxisgemeinschaften), die ohnehin nach Art. 37 Abs. 1 lit. c DS-GVO zu einer Benennungspflicht führt, beispielsweise beim Einsatz von neuen Technologien, die ein hohes Risiko mit sich bringen, der Fall sein. Der Datenschutzbeauftragte ist damit auch dann zu benennen, wenn weniger als 10 Personen ständig mit der Verarbeitung personenbezogener Daten zu tun haben.

4. Der Begriff „Gesundheitsberuf" ist im Sinne der Aufzählung nach § 203 Abs. 1 StGB auszulegen und umfasst die in § 203 Abs. 1 Nr. 1, 2, 4 und 5 StGB aufgezählten Berufsbilder.

17.13 Entschließung: Die Zeit der Verantwortungslosigkeit ist vorbei: EuGH bestätigt gemeinsame Verantwortung von Facebook und Fanpage-Betreibern

6. Juni 2018

Die unabhängigen Datenschutzbehörden des Bundes und der Länder begrüßen das Urteil des Europäischen Gerichtshofs (EuGH) vom 5. Juni 2018, das ihre langjährige Rechtsauffassung bestätigt.

Das Urteil des EuGH zur gemeinsamen Verantwortung von Facebook und den Betreibern einer Fanpage hat unmittelbare Auswirkungen auf die Seitenbetreiber. Diese können nicht mehr allein auf die datenschutzrechtliche Verantwortung von Facebook verweisen, sondern sind selbst mitverantwortlich für die Einhaltung des Datenschutzes gegenüber den Nutzenden ihrer Fanpage.

Dabei müssen sie die Verpflichtungen aus den aktuell geltenden Regelungen der Datenschutz-Grundverordnung (DS-GVO) beachten. Zwar nimmt das Urteil Bezug auf die frühere Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr, doch die vom EuGH festgestellte Mitverantwortung der Seitenbetreiber erstreckt sich auf das jeweils geltende Recht, insbesondere auf die in der DS-GVO festgeschriebenen Rechte der Betroffenen und Pflichten der Verarbeiter.

Im Einzelnen ist Folgendes zu beachten:

- Wer eine Fanpage besucht, muss transparent und in verständlicher Form darüber informiert werden, welche Daten zu welchen Zwecken durch Facebook und die Fanpage-Betreiber verarbeitet werden. Dies gilt sowohl für Personen, die bei Facebook registriert sind, als auch für nicht registrierte Besucherinnen und Besucher des Netzwerks.
- Betreiber von Fanpages sollten sich selbst versichern, dass Facebook ihnen die Informationen zur Verfügung stellt, die zur Erfüllung der genannten Informationspflichten benötigt werden.
- Soweit Facebook Besucherinnen und Besucher einer Fanpage durch Erhebung personenbezogener Daten trackt, sei es durch den Einsatz von Cookies oder vergleichbarer Techniken oder durch die Speicherung der IP-Adresse, ist grundsätzlich eine Einwilligung der Nutzenden erforderlich, die die Anforderung der DS-GVO erfüllt.
- Für die Bereiche der gemeinsamen Verantwortung von Facebook und Fanpage-Betreibern ist in einer Vereinbarung festzulegen, wer von ihnen welche Verpflichtung der DS-GVO erfüllt. Diese Vereinbarung muss in wesentlichen Punkten den Betroffenen zur Verfügung gestellt werden, damit diese ihre Betroffenenrechte wahrnehmen können.

Für die Durchsetzung der Datenschutzvorgaben bei einer Fanpage ist die Aufsichtsbehörde zuständig, die für das jeweilige Unternehmen oder die Behörde zuständig

ist, die die Fanpage betreibt. Die Durchsetzung der Datenschutzvorgaben im Verantwortungsbereich von Facebook selbst obliegt primär der irischen Datenschutzaufsicht im Rahmen der europäischen Zusammenarbeit.

Die deutschen Aufsichtsbehörden weisen darauf hin, dass nach dem Urteil des EuGH dringender Handlungsbedarf für die Betreiber von Fanpages besteht. Dabei ist nicht zu verkennen, dass die Fanpage-Betreiber ihre datenschutzrechtlichen Verantwortung nur erfüllen können, wenn Facebook selbst an der Lösung mitwirkt und ein datenschutzkonformes Produkt anbietet, das die Rechte der Betroffenen wahrt und einen ordnungsgemäßen Betrieb in Europa ermöglicht.

17.14 Beschluss der DSK zu Facebook-Fanpages

5. September 2018

Mit Urteil vom 5. Juni 2018 hat der Gerichtshof der Europäischen Union (EuGH), Aktenzeichen C-210/16, entschieden, dass eine gemeinsame Verantwortlichkeit von Facebook-Fanpage-Betreiberinnen und Betreibern und Facebook besteht. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in ihrer Entschließung vom 6. Juni 2018 deutlich gemacht, welche Konsequenzen sich aus dem Urteil für die gemeinsam Verantwortlichen – insbesondere für die Betreiberinnen und Betreiber einer Fanpage – ergeben.

Bei einer gemeinsamen Verantwortlichkeit fordert die Datenschutz-Grundverordnung (DSGVO) unter anderem eine Vereinbarung zwischen den Beteiligten, die klarstellt, wie die Pflichten aus der DSGVO erfüllt werden.

Seit dem Urteil des EuGH sind drei Monate vergangen. Zwar hat Facebook einige Änderungen in seinem Angebot – zum Beispiel bezüglich der Cookies – vorgenommen, doch weiterhin werden auch bei Personen, die keine Facebook-Nutzerinnen und Nutzer sind, Cookies mit Identifikatoren gesetzt, jedenfalls wenn sie über die bloße Startseite einer Fanpage hinaus dort einen Inhalt aufrufen.

Auch werden nach wie vor die Fanpage-Besuche von Betroffenen nach bestimmten, teilweise voreingestellten Kriterien im Rahmen einer sogenannten Insights-Funktion von Facebook ausgewertet und den Betreiberinnen und Betreibern zur Verfügung gestellt.

Der EuGH hat unter anderem hervorgehoben, dass „die bei Facebook unterhaltenen Fanpages auch von Personen besucht werden können, die keine Facebook-Nutzer sind und somit nicht über ein Benutzerkonto bei diesem sozialen Netzwerk verfügen. In diesem Fall erscheint die Verantwortlichkeit des Betreibers der Fanpage hinsichtlich der Verarbeitung der personenbezogenen Daten dieser Personen noch höher, da das bloße Aufrufen der Fanpage durch Besucher automatisch die Verarbeitung ihrer personenbezogenen Daten auslöst."

Offizielle Verlautbarungen vonseiten Facebooks, ob und welche Schritte unternommen werden, um einen rechtskonformen Betrieb von Facebook-Fanpages zu ermöglichen, sind bisher ausgeblieben. Eine von Facebook noch im Juni 2018 angekündigte

Vereinbarung nach Art. 26 DSGVO (Gemeinsam für die Verarbeitung Verantwortliche) wurde bislang nicht zur Verfügung gestellt. Die deutschen Datenschutzaufsichtsbehörden wirken daher auf europäischer Ebene auf ein abgestimmtes Vorgehen gegenüber Facebook hin.

Auch Fanpage-Betreiberinnen und Betreiber müssen sich ihrer datenschutzrechtlichen Verantwortung stellen. Ohne Vereinbarung nach Art. 26 DSGVO ist der Betrieb einer Fanpage, wie sie derzeit von Facebook angeboten wird, rechtswidrig.

Daher fordert die DSK, dass nun die Anforderungen des Datenschutzrechts beim Betrieb von Fanpages erfüllt werden. Dazu gehört insbesondere, dass die gemein-sam Verantwortlichen Klarheit über die derzeitige Sachlage schaffen und die erforderlichen Informationen den betroffenen Personen (= Besucherinnen und Besucher der Fanpage) bereitstellen.

Eine gemeinsame Verantwortlichkeit bedeutet allerdings auch, dass Fanpage-Betreiberinnen und Betreiber (unabhängig davon, ob es sich um öffentliche oder nichtöffentliche Verantwortliche handelt) die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und dies nachweisen können. Zu-dem können Betroffene ihre Rechte aus der DSGVO bei und gegenüber jedem Verantwortlichen geltend machen (Art. 26 Abs. 3 DSGVO).

Insbesondere die im Anhang aufgeführten Fragen müssen deshalb sowohl von Facebook als auch und von Fanpage-Betreiberinnen und Betreibern beantwortet werden können.

Anhang: Fragenkatalog

1. In welcher Art und Weise wird zwischen Ihnen und anderen gemeinsam Verantwortlichen festgelegt, wer von Ihnen welche Verpflichtung gemäß der DSGVO erfüllt? (Art. 26 Abs. 1 DSGVO)
2. Auf Grundlage welcher Vereinbarung haben Sie untereinander festgelegt, wer welchen Informationspflichten nach Art. 13 und 14 DSGVO nachkommt?
3. Auf welche Weise werden die wesentlichen Aspekte dieser Vereinbarung den betroffenen Personen zur Verfügung gestellt?
4. Wie stellen Sie sicher, dass die Betroffenenrechte (Art. 12 ff. DSGVO) erfüllt werden können, insbesondere die Rechte auf Löschung nach Art. 17 DSGVO, auf Einschränkung der Verarbeitung nach Art. 18 DSGVO, auf Widerspruch nach Art. 21 DSGVO und auf Auskunft nach Art. 15 DSGVO?
5. Zu welchen Zwecken und auf welcher Rechtsgrundlage verarbeiten Sie die personenbezogenen Daten der Besucherinnen und Besucher von Fanpages? Welche personenbezogenen Daten werden gespeichert? Inwieweit werden aufgrund der Besuche von Facebook-Fanpages Profile erstellt oder angereichert? Werden auch personenbezogene Daten von Nicht-Facebook-Mitgliedern zur Erstellung von Profilen verwendet? Welche Löschfristen sind vorgesehen?
6. Zu welchen Zwecken und auf welcher Rechtsgrundlage werden beim Erst-aufruf einer Fanpage auch bei Nicht-Mitgliedern Einträge im sogenannten Local Storage erzeugt?

7. Zu welchen Zwecken und auf welcher Rechtsgrundlage werden nach Aufruf einer Unterseite innerhalb des Fanpage-Angebots ein Session-Cookie und drei Cookies mit Lebenszeiten zwischen vier Monaten und zwei Jahren gespeichert?
8. Welche Maßnahmen haben Sie ergriffen, um Ihren Verpflichtungen aus Art. 26 DSGVO als gemeinsam für die Verarbeitung Verantwortlicher gerecht zu werden und eine entsprechende Vereinbarung abzuschließen?

17.15 Beschluss: Anwendung der DSGVO im Bereich von Parlamenten, Fraktionen, Abgeordneten und politischen Parteien

5. September 2018

Die Konferenz nimmt das Ergebnis der Beratungen des Arbeitskreises Grundsatzfragen des Datenschutzes zur Kenntnis und empfiehlt für die weitere Rechtspraxis, die im Folgenden aufgeführten Positionierungen bei der Tätigkeit als Aufsichtsbehörde zu Grunde zu legen:

1. Soweit Datenverarbeitungen von Parlamenten (auch deren Organe einschließlich der Abgeordneten) den parlamentarischen Kerntätigkeiten zuzuordnen sind, findet die DSGVO keine Anwendung.
2. Parlamente (auch deren Organe einschließlich der Abgeordneten) unterliegen bei der Ausübung originär parlamentarischer Kerntätigkeiten nur dann datenschutzrechtlichen Vorgaben und der Aufsicht der Aufsichtsbehörde, wenn sich dies aus einer klaren gesetzlichen Regelung ergibt.
3. Die Einordnung von Tätigkeiten der Parlamente (auch deren Organe einschließlich der Abgeordneten) als verwaltende und fiskalische in Abgrenzung zur parlamentarischen Kerntätigkeit bedarf jeweils einer Bewertung im Einzelfall.
4. Soweit keine gesetzlichen Grundlagen für die parlamentarische Kerntätigkeit bestehen, wäre eine Datenschutzordnung des Parlaments zu empfehlen, die sich an der DSGVO orientieren sollte. Eine Beratung durch die Aufsichtsbehörde sollte in jedem Fall unbenommen bleiben.
5. Parteien als nicht-öffentliche Stellen sind grundsätzlich Normadressaten der DSGVO und unterliegen damit der Aufsicht der Aufsichtsbehörden. Eine mögliche Berücksichtigung ihres besonderen Status im Rahmen der Gesetzesanwendung bleibt unberührt.

17.16 Beschluss: Ablehnung der Behandlung durch Ärztinnen und Ärzte bei Weigerung der Patientin oder des Patienten, die Kenntnisnahme der Informationen nach Art. 13 DSGVO durch Unterschrift zu bestätigen

5. September 2018

Die Datenschutzaufsichtsbehörden des Bundes und der Länder sprechen sich dagegen aus, dass Ärztinnen und Ärzte oder andere Angehörige von Gesundheitsberufen die Behandlung ablehnen oder die Verweigerung der Behandlung androhen, wenn die Patientin oder der Patient die Informationen nach Art. 13 DSGVO nicht mit ihrer oder seiner Unterschrift versieht. Eine solche Praxis ist nicht mit der DSGVO vereinbar.

Die Informationspflicht nach Art. 13 DSGVO bezweckt lediglich, dass der Patientin bzw. dem Patienten die Gelegenheit gegeben wird, die entsprechenden Informationen einfach und ohne Umwege zu erhalten. Sie oder er muss diese jedoch nicht zur Kenntnis nehmen, wenn sie oder er dies nicht möchte.

Um seinen Nachweispflichten gegenüber der Aufsichtsbehörde nachzukommen, kann der Verantwortliche das Aushändigen der Information vermerken oder einen konkreten Verfahrensablauf betreffend die Umsetzung der Informationspflicht dokumentieren, aus dem hervorgeht, wie die Patientin oder der Patient die Informationen im Regelfall erhält.

17.17 Entschließung: Der Vorschlag der EU-Kommission für eine E-Evidence-Verordnung führt zum Verlust von Betroffenenrechten und verschärft die Problematik der sog. Vorratsdatenspeicherung

7./8. November 2018

Mit ihrem Vorschlag für eine E-Evidence-Verordnung (Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (COM (2018) 225 final)) möchte die EU-Kommission eine Alternative zum förmlichen Rechtshilfeverfahren schaffen und den Ermittlungsbehörden einen schnelleren Zugang zu Kommunikationsdaten ermöglichen. Die Strafverfolgungsbehörden der EU-Mitgliedstaaten sollen die Befugnis erhalten, Anbieter von Telekommunikations- und Internetdienstleistungen in anderen Mitgliedstaaten der EU und auch in Staaten außerhalb der EU (Drittstaaten) unmittelbar zur Herausgabe von Bestands-, Zugangs-, Transaktions- und Inhaltsdaten zu verpflichten.

Die DSK weist hierzu auf die kritische Stellungnahme des Europäischen Datenschutzausschusses hin (https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-commission-proposals-european-production-and_de). Diese stellt bereits das Vorliegen einer Rechtsgrundlage in Frage. Mit Besorgnis sieht die DSK vor allem auch die vorgeschlagene Abkehr vom Grundsatz der doppelten bzw. beiderseitigen Strafbarkeit.

Erstmals im Bereich der internationalen Zusammenarbeit in Strafsachen soll die Herausgabe von Daten nicht mehr davon abhängig sein, ob die verfolgte Tat dort, wo die Daten ersucht werden, überhaupt strafbar ist. Im Ergebnis könnten Unternehmen mit Sitz in Deutschland also zur Herausgabe von Daten an Ermittlungsbehörden in anderen EU-Mitgliedstaaten verpflichtet werden, obwohl die verfolgte Tat in Deutschland überhaupt keine Straftat ist. Das könnte zum Beispiel ein in Deutschland erlaubter Schwangerschaftsabbruch sein oder eine politische Meinungsäußerung, wenn diese im ersuchenden Staat strafbewehrt ist.

Zu befürchten ist hierbei auch, dass Drittstaaten die Regelung der EU als Blaupause für eigene Regelungen heranziehen werden. Provider in EU-Mitgliedstaaten würden sich dann vermehrt Herausgabeanordnungen von Drittstaaten ausgesetzt sehen, mit denen möglicherweise Straftaten aus einer völlig anderen Rechtstradition verfolgt werden.

Kritisch sieht die DSK auch, dass im Regelfall jegliche Information und Beteiligung der Justizbehörden des Staates, in dem der Provider seinen Sitz hat, unterbleibt und damit ein wichtiges verfahrensrechtliches Korrektiv fehlt. Ob die Rechtmäßigkeit eines Ersuchens überprüft wird, hängt im vorgeschlagenen Verfahren ausschließlich vom Verhalten der Provider ab. Nur wenn sich das Unternehmen weigert, Daten zu übermitteln, muss der ersuchende Staat bei den Behörden vor Ort um Vollstreckungshilfe bitten. Nur dann können diese noch in das Verfahren eingreifen. Werden Daten herausgegeben, erlangen die zuständigen Justizbehörden hiervon jedoch keine Kenntnis. Der Vorschlag sieht keine Informationspflicht gegenüber den Behörden am Sitz des Unternehmens vor. Provider verfolgen aber in der Regel wirtschaftliche Interessen und unterliegen in ihren Entscheidungen anderen Verpflichtungen als die Justizbehörden Hierdurch werden Betroffene deutlich schlechter gestellt.

Provider als Adressaten eines Ersuchens sehen sich künftig nicht mehr den Justizbehörden des eigenen Staates gegenüber, sondern müssen sich mit den Behörden des anordnenden Staates auseinandersetzen. Den Betroffenen wiederum steht, wenn überhaupt, nur ein Rechtsbehelf im ersuchenden Mitgliedsstaat zu, dessen Rechtsordnung ihnen in der Regel aber fremd ist.

Ein besonderes Verfahren ist vorgesehen, wenn sich Provider mit Sitz in Drittstaaten darauf berufen, dass die angeordnete Übermittlung gegen das dortige Recht verstößt. Für diesen Fall sieht der Vorschlag eine gerichtliche Überprüfung im anordnenden Staat vor. Wenn das Gericht zu der Auffassung gelangt, dass tatsächlich ein Rechtskonflikt vorliegt, muss es die zuständigen Behörden im Zielstaat der Anordnung beteiligen. Das Ergebnis der Konsultation ist für das Gericht verbindlich. Diese Regelung ist ausdrücklich zu begrüßen. Denn auch hier wird eine Blaupause geschaffen für die Frage, welche Rechte europäische Unternehmen in der umgekehrten Si-

tuation haben sollten, wenn sie aus Drittstaaten auf der Grundlage von deren Gesetzen (wie z. B. US-Cloud-Act) zu einer Übermittlung verpflichtet werden und welche Verbindlichkeit eine Konsultation der zuständigen Behörden in Europa für Gerichte in Drittstaaten haben sollte.

Besonders kritisch ist jedoch, dass in Deutschland Telekommunikationsdienstleister verpflichtet sind, u. a. sämtliche Verkehrsdaten für zehn Wochen zu speichern. Aus diesen Daten lassen sich genaue Schlüsse auf das Privatleben der Betroffenen, insbesondere deren Kontakt- und Interessenprofil ziehen. Die Problematik dieser sog. Vorratsdatenspeicherung verschärft sich deutlich, wenn ausländische Strafverfolgungsbehörden einen direkten Zugriff auf derartige Informationen erhalten.

Die DSK appelliert daher an alle im Gesetzgebungsverfahren Beteiligten, den Vorschlag für eine E-Evidence-Verordnung zu stoppen!

INFORMATIONSFREIHEIT

18 Transparenz in der öffentlichen Verwaltung – das Saarländische Informationsfreiheitsgesetz

18.1 Grundsätzliches zum Informationsfreiheitsrecht

Mit der Einführung des Saarländischen Informationsfreiheitsgesetzes (SIFG) im Jahr 2006 ist der Saarländische Gesetzgeber dem Vorbild des Bundes zur Schaffung eines gesetzlichen Anspruchs auf Zugang zu Behördeninformationen gefolgt und hat damit die Abkehr von dem althergebrachten Grundsatz der Amtsverschwiegenheit eingeleitet. So sieht dann auch § 1 SIFG einen grundsätzlich voraussetzungslosen Anspruch auf Zugang zu amtlichen Informationen gegenüber den Behörden des Landes, der Gemeinden und Gemeindeverbände vor. Neben den Ministerien, Landesbehörden, Kommunen und Landkreisen sind sämtliche Stellen der öffentlichen Verwaltung erfasst, soweit sie nicht im Bereich der Gesetzgebung (Landtag) oder im Bereich der Rechtsprechung (Gerichte) tätig werden. Ebenfalls ausgenommen sind Prüfungs- und Bildungseinrichtungen sowie der Verfassungsschutz, soweit diese nicht im Rahmen der allgemeinen Verwaltung tätig werden. Dem grundsätzlich voraussetzungslosen Informationsanspruch können außerdem bestimmte Interessen entgegenstehen. So sind über einen Verweis auf das Informationsfreiheitsgesetz des Bundes (IFG) öffentliche Interessen, der behördliche Entscheidungsprozess, private sowie wirtschaftliche Belange geschützt. Beispielsweise darf Zugang zu Betriebs- und Geschäftsgeheimnissen nur gewährt werden, wenn der Geheimnisträger eingewilligt hat.

Von einem flächendeckenden Verständnis eines transparenten staatlichen Verwaltungshandelns kann jedoch selbst nach über zwölf Jahren seit Inkrafttreten des Gesetzes nicht die Rede sein. Neben Fällen der kompletten Unkenntnis der informationsfreiheitlichen Regelungen wurden geltend gemachte Informationsansprüche von Seiten einiger Verwaltungsbehörden teilweise mit kaum nachvollziehbaren Gründen abgewiesen. So wurde häufig fehlerhaft argumentiert, dass das jeweilige Verwaltungshandeln nicht vom Anwendungsbereich des Gesetzes erfasst sei oder es wurde pauschal darauf verwiesen, dass dem Informationsbegehren datenschutzrechtliche Gründe entgegenstehen. Eine nähere Befassung im Sinne einer nachvollziehbaren Begründung der Ablehnung erfolgte in diesen Fällen zumeist nicht, obwohl dies nach dem SIFG geboten ist.

Eine sein Informationsbegehren ablehnende Entscheidung kann der Antragsteller mit Widerspruch und Klage angreifen. Um dem damit einhergehenden Prozess- und Kostenrisiko für den Antragsteller zu begegnen, sieht das SIFG für den Fall der Ablehnung eines Informationsbegehrens eine Möglichkeit für den Antragsteller vor, sich an die Landesbeauftrage für Informationsfreiheit zu wenden.

Der Informationsfreiheitsbeauftragten kommt in diesen Fällen eine vermittelnde Rolle zu. Sie prüft das Anliegen des Antragstellers und setzt sich, sofern Anhaltspunkte für Fehler bei der Sachbearbeitung erkennbar sind, mit der konkret betroffenen Behörde in Verbindung. Ziel dieses Konsultationsverfahrens ist es, auf die Einhaltung des Gesetzes hinzuwirken, wobei der Informationsfreiheitsbeauftragten selbst keine Anordnungs- bzw. Klagebefugnisse zustehen, sondern lediglich eine Beanstandung bei der für die auskunftsverpflichtete Stelle zuständigen Aufsichtsbehörde möglich ist. Sollte sich also eine Behörde selbst nach Mitteilung eines anderslautenden Votums der Informationsfreiheitsbeauftragten dem Auskunftsbegehren verwehren, muss die antragstellende Person entscheiden, ob sie Widerspruch oder Klage einreichen will.

Im Folgenden wird nur exemplarisch über einige wenige Fälle berichtet. Die tatsächliche Anzahl der Sachverhalte, in denen die Landesbeauftragte für Informationsfreiheit angerufen wurde oder Auskunft gegeben hat, sind weitaus größer.

18.2 Transparenz bei kommunalen Gesellschaften

Das Informationsinteresse des Bürgers tritt vermehrt dann in Erscheinung, wenn eine finanzielle Betroffenheit gegeben ist. Dies zeigt sich insbesondere in den Bereichen, in denen Gebühren oder Entgelte zu leisten sind. Das können beispielsweise Kanalbenutzungs-, Abwasser- oder allgemeine Verwaltungsgebühren sein. In einigen dieser Bereiche werden staatliche Leistungen nicht mehr durch die Behörden in ihrer Eigenschaft als Gebietskörperschaft des öffentlichen Rechts, sondern durch Privatrechtssubjekte erbracht, derer sich die öffentliche Hand zur Aufgabenerfüllung bedient. Zum Teil werden dabei Unternehmen in die Aufgabenerfüllung einbezogen, an denen die öffentliche Hand überhaupt keine Beteiligung besitzt.

In diesem Zusammenhang drängt sich die Frage auf, ob sich der Staat durch eine sog. *Flucht ins Privatrecht* den Transparenzpflichten nach dem Saarländischen Informationsfreiheitsgesetz (SIFG) vollständig entziehen kann, indem er beispielsweise die Wasserversorgung durch eine städtische Gesellschaft besorgen lässt. So erreichte hiesige Dienststelle im Berichtszeitraum die Eingabe eines Petenten, dessen an die Stadtwerke adressiertes Auskunftsersuchen mit der Begründung abgelehnt worden war, dass es sich bei den Stadtwerken nicht um eine Behörde, sondern um eine GmbH, also um eine juristische Person des Privatrechts, handele. Somit lägen dort keine amtlichen Informationen im informationsfreiheitsrechtlichen Sinne dort vor.

Der Informationszugangsanspruch erstreckt sich in der Tat in erster Linie auf Behörden. Allerdings sieht § 1 S. 1 SIFG in Verbindung mit § 1 Abs. 1 S. 3 Informationsfreiheitsgesetz des Bundes (IFG) vor, dass

„(…) einer Behörde im Sinne dieser Vorschrift (…) eine natürliche Person oder juristische Person des Privatrechts gleich(steht), soweit eine Behörde sich dieser Person zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben bedient."

Die Aufgaben der Stadtwerke sind vielfältig und können von der Versorgung mit Strom, Wasser, Fernwärme und Erdgas bis hin zum Betrieb des öffentlichen Personennahverkehrs reichen. Bei diesen elementaren Versorgungsangeboten spricht

man von Aufgaben der kommunalen Daseinsvorsorge; die Erbringung dieser Aufgaben stellt mithin grundsätzlich eine öffentlich-rechtliche Aufgabe dar. So ist beispielsweise die öffentliche Wasserversorgung nach § 50 Abs. 1 Wasserhaushaltsgesetz eine solche Aufgabe der Daseinsvorsorge. An dieser Eigenschaft ändert sich auch dann nichts, wenn eine Kommune die Wasserversorgung durch ihre privatrechtlich organisierten Stadtwerke erledigen lässt. Insofern schlägt der grundsätzliche Informationsanspruch auch auf die Stadtwerke durch.

Entscheidend ist, dass der Antrag nicht an die Stadtwerke direkt gerichtet wird, sondern an die jeweilige Kommune, welche die ihr obliegende Aufgabe durch die Stadtwerke erledigen lässt (§ 7 Abs. 1 S. 2 IFG). Diese entscheidet, ob dem Antrag auf Informationszugang stattgegeben wird oder ob ihm ein Ablehnungstatbestand nach dem IFG entgegenstehen könnte. Die in diesem Zusammenhang vielfach bemühten wirtschaftlichen Interessen nach § 6 S. 2 IFG sind jedoch gerade bei kommunalen Unternehmen, sofern sie sich im Hinblick auf die von ihnen angebotene Dienstleistung in keinerlei Marktkonkurrenz befinden, sondern – wie bei der Wasserversorgung – eine Monopolstellung innehaben, regelmäßig nicht geeignet, den Informationszugang zu verwehren.

18.3 Informationszugang und Gerichtsverfahren

In einem konkreten Fall begehrte ein Bürger Akteneinsicht in Unterlagen für ein Bauvorhaben, über welches bereits in der örtlichen Presse kritisch berichtet wurde. Die Behörde lehnte den Antrag auf Informationsfreiheit ab, da laut ihrer Einschätzung ein Gerichtsverfahren mit dem betreffenden Bürger unmittelbar bevorstünde und daher die Unterlagen nach § 3 Nr. 1 lit. g Informationsfreiheitsgesetz des Bundes (IFG) geschützt seien.

Diese Einschätzung konnte nicht geteilt werden, da ein Anspruch auf Informationszugang nach dem eindeutigen Wortlaut der zitierten Norm nur dann nicht besteht, wenn die Möglichkeit nachteiliger Auswirkungen auf ein *laufendes* Gerichtsverfahren besteht. Mithin ist der Informationszugang auch nicht schon deshalb ausgeschlossen, weil der Antrag Informationen betrifft, die einen Bezug zu einem laufenden Gerichtsverfahren haben. Vielmehr fordert das Gesetz, dass die Bekanntgabe der Information nachteilige Auswirkungen auf die *Durchführung* eines laufenden Gerichtsverfahrens haben kann. Bezugspunkt der nachteiligen Auswirkungen und Schutzgut dieser Vorschrift ist daher der Ablauf und nicht das Ergebnis des gerichtlichen Verfahrens. Vor diesem Hintergrund ist der individuelle Prozesserfolg der öffentlichen Hand gerade nicht erfasst. Vorliegend war indessen nicht ersichtlich, weshalb nachteilige Auswirkungen gerade auf die Durchführung des Gerichtsverfahrens zu befürchten sind, so dass die Voraussetzungen des § 3 Nr. 1 lit. g IFG nicht erfüllt waren und – da auch keine anderen Ausschlusstatbestände gegeben waren – dem Anspruch auf Informationszugang nachzukommen war.

18.4 Verhältnis des Auskunftsrechts nach § 37 KSVG zum Informationszugangsanspruch nach SIFG und IFG

Bereits im Jahr 2015 begehrte ein Antragsteller, der auch Mitglied in der Regionalverbandsversammlung war, gegenüber dem Regionalverband Saarbrücken die schriftliche Übersendung oder Akteneinsicht in Rechenschaftsberichte der Fraktionen der Regionalversammlung sowie die entsprechenden Prüfberichte des Regionalverbandsdirektors. Dies wurde seitens des Regionalverbandes abgelehnt. Hiergegen legte der Antragsteller Widerspruch beim Regionalverband ein und ersuchte zugleich die Landesbeauftragte für Informationsfreiheit um Vermittlung in seiner Angelegenheit. Er machte geltend, er sei als Bürger informationszugangsberechtigt und stützte sich auf § 1 Saarländisches Informationsfreiheitsgesetz (SIFG). Der Regionalverband hingegen lehnte den Informationszugang im Wesentlichen mit der Begründung ab, dass der Antragsteller Mitglied der Regionalverbandsversammlung sei und deshalb im Hinblick auf den Informationszugang die spezielleren Vorschriften des § 37 Kommunalselbstverwaltungsgesetz (KSVG) gelten würden, die gemäß § 1 Abs. 3 SIFG dem Informationsfreiheitsgesetz vorgehen würden. Der Regionalverband sah seine Rechtsauffassung durch einen Beschluss des Oberverwaltungsgerichts des Saarlandes im Rahmen eines vom Antragsteller initiierten einstweiligen Verfügungsverfahrens[147] bestätigt, in dem das Gericht noch einen Informationszugang verneinte, dies jedoch vor dem Hintergrund, dass der Antragsteller in dem seinerzeitigen Verfahren sein Auskunftsrecht dezidiert aus seiner Stellung als Mitglied der Regionalversammlung herleitete und ein Antrag nach dem Informationsfreiheitsgesetz des Bundes (IFG) nicht vorlag.

Hiesigerseits konnte den Ausführungen des Regionalverbandes nicht zugestimmt werden, da sich die Vorschrift des § 37 KSVG aus unserer Sicht nicht als eine Regelung im Sinne des § 1 Abs. 3 IFG darstellt, welche die Bestimmungen des IFG verdrängt bzw. ausschließt. In diesem Sinne äußerte sich bereits die damalige Landesbeauftragte für Datenschutz und Informationsfreiheit in einem im Februar 2013 in der Saarländischen Kommunalzeitschrift veröffentlichten Artikel[148], in dem das Verhältnis des § 37 KSVG zum Anspruch auf Informationszugang nach § 1 Abs. 1 IFG näher beleuchtet wurde. Danach weisen die beiden zitierten Vorschriften eben gerade keinen identischen sachlichen Regelungsgehalt auf, so dass auch keine Sperrwirkung von der Vorschrift des § 37 KSVG ausgehen kann. Hierauf wurde der Regionalverband hingewiesen. Ungeachtet dessen hielt der Regionalverband an seiner dargestellten Rechtsauffassung fest und lehnte den Antrag auf Informationszugang auch im Rahmen des Widerspruchsverfahrens mit der entsprechenden Begründung ab.

[147] OVG des Saarlandes, Beschluss vom 27.11.2015 – 2 B 218/15.

[148] *Judith Thieser,* Das Informations- und Akteneinsichtsrecht der Gemeinderatsmitglieder als „Jedermann" nach dem Saarländischen Informationsfreiheitsgesetz (SIFG)", SKZ 2013, 41.

Die hiergegen erhobene Klage des Antragstellers hatte in erster und zweiter Instanz Erfolg.[149] Die Gerichte argumentierten ebenfalls, dass den Normen des § 37 KSVG und § 1 Abs. 1 IFG kein identischer sachlicher Regelungsgegenstand zugrunde liegt. Das Oberverwaltungsgericht führt in seinem Urteil aus, dass § 37 KSVG auf eine Stärkung der Informationsrechte des Körperschaftsorgans (der Regionalversammlung) und seiner Mitglieder zielt, während das SIFG und IFG mit der Statuierung eines voraussetzungslosen Informationsrechts des einzelnen Bürgers einen gänzlich anderen Zweck verfolgen, nämlich den der Förderung allgemeiner Transparenz. Es betont weiterhin, dass selbst wenn man in den Vorschriften einen identischen sachlichen Regelungsgehalt sehen wolle, § 37 KSVG jedenfalls nicht als abschließende Regelung gegenüber dem IFG zu verstehen sei.

Soweit der Regionalverband sich auf einen früheren Beschluss des Oberverwaltungsgerichts[150] im Rahmen eines vom Antragsteller seinerzeit angestrengten einstweiligen Verfügungsverfahrens berufe, stellte das Berufungsgericht nunmehr klar, dass dieser Entscheidung eine andere Ausgangssituation zu Grunde lag, weil der Antragsteller seinen Anspruch auf Akteneinsicht in jenem Verfahren dezidiert aus seiner Stellung als Mitglied der Regionalversammlung hergeleitet hatte, so dass ein Zugangsanspruch damals bereits an dem Fehlen des notwendigen Antrags einer natürlichen Person scheiterte. Soweit der damaligen Entscheidung im Übrigen zusätzlich zu entnehmen sei, dass auf Grund von § 37 KSVG im kommunalen Bereich Informationszugangsrechte gemäß §§ 1 S. 1 SIFG, 1 Abs. 3 IFG generell ausgeschlossen seien, so hielt der Senat an dieser Auffassung nicht fest.

Mithin sieht das Oberverwaltungsgericht in den Rechenschafts- und Prüfberichten amtliche Informationen, verneinte das Vorliegen von Ausschlusstatbeständen und bestätigte folglich die Entscheidung des Verwaltungsgerichts, mit welcher der Regionalverband verpflichtet wurde, dem Antragsteller Zugang zu den streitgegenständlichen Berichten zu gewähren.

18.5 Informantenschutz

Im Berichtszeitraum wurde seitens einer Gemeinde bei hiesiger Behörde angefragt, ob die Einsichtnahme eines Beteiligten in Akten eines gewerberechtlichen Verwaltungsverfahrens derart beschränkt werden könne, dass bestimmte personenbezogene Daten eines Hinweisgebers geschwärzt werden.

Hiesigerseits wurde der betreffenden Gemeinde mitgeteilt, dass sich das Akteneinsichtsrecht von Beteiligten im Verwaltungsverfahren nach § 29 Saarländisches Verwaltungsverfahrensgesetz (SVwVfG) richtet und danach Einsicht in die das Verfahren betreffenden Akten grundsätzlich zu gestatten ist, soweit deren Kenntnis zur Geltendmachung oder Verteidigung der rechtlichen Interessen erforderlich ist. Allerdings ist die Behörde gemäß § 29 Abs. 2 SVwVfG zur Gestattung der Akteneinsicht nicht verpflichtet, soweit die Vorgänge nach einem Gesetz oder ihrem Wesen nach,

[149] Verwaltungsgericht des Saarlandes, Gerichtsbescheid vom 28. April 2017 – 3 K 159/16 – und OVG, Urteil vom 11. Juni 2018 – 2 A 452/17.

[150] OVG des Saarlandes, Beschluss vom 27.11.2015 – 2 B 218/15 .

namentlich wegen der berechtigten Interessen der Beteiligten oder dritter Personen, geheim gehalten werden müssen.

Daraus lässt sich für bestimmte Konstellationen ein Informantenschutz herleiten, der sich anhand einer Abwägung zwischen dem Interesse an der vertraulichen Behandlung von Angaben zur Person des Informanten und dem Auskunftsinteresse des Betroffenen ermittelt. Die höchstrichterliche Rechtsprechung gewährt dem Interesse an der Geheimhaltung des Informanten bzw. Hinweisgebers dabei regelmäßig Vorrang gegenüber dem Informationsinteresse des Akteneinsichtsbegehrenden.[151] Dabei kann sich das Geheimhaltungsinteresse auch auf das öffentliche Interesse an der Funktionsfähigkeit der Behörde stützen. Danach dürfen Behörden zum Schutz des Informanten dessen Identität geheim halten, wenn sie bei der Erfüllung ihrer öffentlichen Aufgaben (auch) auf die Angaben Dritter angewiesen sind.

Gleiches muss unter Zugrundelegung der informationsfreiheitlichen Regelungen gelten. Hiernach kann gemäß dem nach § 1 Abs. 1 S. 1 Saarländisches Informationsfreiheitsgesetz (SIFG) anwendbaren § 3 Nr. 7 Informationsfreiheitsgesetz des Bundes (IFG) ein Informationsanspruch im Hinblick auf eine vertraulich erhobene oder übermittelte Information ausgeschlossen sein, soweit das Interesse des Dritten an einer vertraulichen Behandlung im Zeitpunkt des Antrages auf Informationszugang noch fortbesteht. Unabhängig von der umstrittenen Frage, ob diese Vorschrift nur dem Schutz von Informanten oder auch dem Schutz der Behörde bzw. der behördlichen Aufgabenerfüllung dient, kommt man jedenfalls auch im Rahmen eines Verfahrens nach dem IFG zu vergleichbaren Ergebnissen.

Soweit man nach Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) parallel zu den zitierten Vorschriften eine Informationspflicht der Behörde nach Art. 14 Abs. 2 lit. f DSGVO oder ein Auskunftsrecht nach Art. 15 Abs. 1 lit. g DSGVO für die Preisgabe der Identität eines Hinweisgebers in Betracht zieht, dürfte auch hiernach vor dem Hintergrund des in der EU-Grundrechtecharta in Art. 8 normierten Rechts auf Schutz personenbezogener Daten eine einschränkende Auslegung des Informations- und Auskunftsanspruchs der betroffenen Person entsprechend den oben genannten und in der Rechtsprechung entwickelten Maßstäbe vorzunehmen sein.

Mithin kommt im Rahmen des Auskunftsanspruchs der Ausnahmetatbestand des Art. 15 Abs. 4 DSGVO in Betracht, welcher dahingehend auszulegen ist, dass durch die Datenkopie, aber auch durch die Auskunftserteilung, die Rechte und Freiheiten anderer Personen nicht beeinträchtigt werden dürfen. Auch hinsichtlich der Informationspflicht sind in Art. 14 Abs. 5 Ausnahmetatbestände normiert, wobei zum Schutz eines Hinweisgebers insbesondere Art. 14 Abs. 5 lit. b DSGVO in Betracht kommt, wenn die Offenlegung der Identität die Verwirklichung der Verarbeitungsziele voraussichtlich unmöglich macht oder ernsthaft beeinträchtigt. Überdies können nach Art. 14 Abs. 5 lit. c DSGVO Vorschriften der Mitgliedstaaten unter den dort genannten Voraussetzungen, insbesondere unter Berücksichtigung der widerstreitenden Interessen, eine Ausnahme von der Informationspflicht begründen. Daneben sieht Art. 23 DSGVO die Möglichkeit der Beschränkung sowohl von Betroffenenrechten als

[151] Vgl. BVerwG, Beschluss vom 22.07.2010 – 20 F 11/10, NVwZ 2010, S. 1493 (1494); Beschluss vom 03.08.2011 – 20 F 23.10, Rn. 8, juris.

auch von Informationspflichten durch Rechtsvorschriften der Mitgliedstaaten unter den dort genannten Voraussetzungen vor.

Im Saarland sind in diesem Zusammenhang die Vorschriften des § 10 Abs. 1 Nr. 3 und § 11 Abs. 2 Nr. 3 Saarländisches Datenschutzgesetz (SDSG) von Bedeutung, wonach von der Mitteilung solcher Informationen abzusehen ist, die zum Schutz Dritter geheim gehalten werden müssen. Insoweit eröffnen diese Vorschriften einen Spielraum zur Abwägung zwischen den Interessen von etwaigen Informanten und Auskunftsersuchenden.

Über den konkreten Fall des gewerblichen Verwaltungsverfahrens hinaus, ist damit grundsätzlich eine Schwärzung personenbezogener Daten von Hinweisgebern im Rahmen der Akteneinsicht auch unter Zugrundelegung der neuen Rechtslage als Mittel der Gewährleistung des Schutzes von Informanten erlaubt.

18.6 Ausblick: Konferenz der Informationsfreiheitsbeauftragten 2019 im Saarland

Das Saarland wird im Jahr 2019 den Vorsitz der Konferenz der Informationsfreiheitsbeauftragten (IFK) übernehmen. Die IFK setzt sich aus den Informationsfreiheitsbeauftragten des Bundes und der Länder, die über ein Informationsfreiheitsgesetz oder ein vergleichbares Gesetz verfügen, zusammen. Neben dem Saarland sind dies Baden-Württemberg, Berlin, Brandenburg, Bremen, Hamburg, Mecklenburg-Vorpommern, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen-Anhalt, Schleswig-Holstein, Thüringen und seit 2018 auch Hessen. Ziel der IFK ist es, das Recht auf Informationszugang zu fördern, für seine Fortentwicklung einzutreten und sich in Form von medienwirksamen Entschließungen, Positionspapieren und Stellungnahmen auf gemeinsame Standpunkte in Fragen der Informationsfreiheit zu verständigen. Interessierte Bürgerinnen und Bürger haben je nach verfügbarer Raumkapazität die Möglichkeit, nach Voranmeldung den Sitzungen beizuwohnen.

19 Entschließungen der Konferenz der Informationsfreiheitsbeauftragten des Bundes und der Länder

19.1 Entschließung: Open Data: Gesetzentwurf der Bundesregierung greift zu kurz!

24. April 2017

Die Informationsfreiheitsbeauftragten der Länder fordern den Deutschen Bundestag auf, statt des von der Bundesregierung vorgelegten Entwurfs eines Open-Data-Gesetzes (Erstes Gesetz zur Änderung des E-Government-Gesetzes) das Informationsfreiheitsgesetz des Bundes zu einem umfassenden Transparenzgesetz zu entwickeln. Bereits im Dezember letzten Jahres hat die Konferenz der Informationsfreiheitsbeauftragten in Deutschland ihre Bedenken angesichts des geplanten Open-Data-Gesetzes in einer Entschließung zum Ausdruck gebracht. Das mittlerweile fortgeschrittene Gesetzgebungsverfahren bietet Anlass, noch einmal ausdrücklich auf folgende Bedenken hinzuweisen:

Der Deutsche Bundestag hat sich am 31. März 2017 in erster Lesung mit dem Entwurf der Bundesregierung für ein Erstes Gesetz zur Änderung des E-Government-Gesetzes (BT-Drucksache 18/11614) befasst. Bund und Länder hatten am 14. Oktober 2016 vereinbart, Open Data zu stärken. Dabei verpflichteten sich die Länder, Open-Data-Gesetze nach dem Beispiel der Bundesregelung zu erlassen. Die Ergebnisse im aktuellen Gesetzgebungsverfahren auf Bundesebene werden daher erhebliche Auswirkungen auf die Landesgesetzgebung haben.

Neben Rohdaten auch Dokumente aktiv veröffentlichen

Der Entwurf richtet sich ausschließlich auf die Bereitstellung von Rohdaten. Informationen, die aus sich heraus verständlich sind, zum Beispiel Verträge, Gutachten, Stellungnahmen und ähnliche Dokumente, sind davon nicht umfasst. Für das von der Bundesregierung angestrebte Ziel der Stärkung zivilgesellschaftlicher Teilhabe ist dies aber ein entscheidender Gehalt des Gesetzes.

Transparenzregelungen gehören in Transparenzgesetze

Die Informationsfreiheitsbeauftragten der Länder sind der Ansicht, dass das Informationsfreiheitsgesetz des Bundes der richtige Standort für eine Open-Data-Regelung wäre. Die Aufnahme von Open-Data-Regelungen in das E-Government-Gesetz des Bundes fördert zwar den Open-Data-Gedanken. Dabei darf jedoch nicht übersehen werden, dass die Behörden des Bundes nach wie vor verpflichtet bleiben, amtliche

Informationen nach Maßgabe des Informationsfreiheitsgesetzes des Bundes zur Verfügung zu stellen. Eine zusätzliche Einzel-regelung für offene Daten passt nicht in das bislang informationstechnisch orientierte E-Government-Gesetz. Statt die Regelung dort einzufügen, sollten die vorgesehenen Regelungen im Informationsfreiheitsgesetz verankert werden. Dieses würde so zu einem modernen Transparenzgesetz, das erforderlichenfalls als weiteres Vorbild für die Landesgesetzgebung dienen könnte. Jede weitere Zersplitterung der ohnehin bereits unübersichtlichen Regelungen zum Informationszugang sollte vermieden werden.

Keine zusätzlichen Ausnahmen

Der Gesetzentwurf verweist zwar auf die Ausnahmetatbestände des Informationsfreiheitsgesetzes, enthält aber noch weitere Ausnahmen. Beispielsweise sollen nur Daten veröffentlicht werden, die außerhalb der Behörde liegende Verhältnisse betreffen. Das mit dem Gesetzentwurf verfolgte Ziel nach „mehr Teilhabe interessierter Bürgerinnen und Bürger und eine intensivere Zusammenarbeit der Behörde mit diesen“ dürfte damit nicht erreicht werden. Es erscheint insgesamt inkonsequent, Open Data durch Ausnahmen zu beschränken, die über die Regelung des Informationsfreiheitsgesetzes hinausgehen. Hiervon ist abzusehen. Die Weiterentwicklung der Informationsfreiheit kann nur im Abbau von Ausnahmen bestehen, nicht in deren Ausweitung.

Individueller Anspruch auf Veröffentlichung

Der Regierungsentwurf gewährt keinen individuellen Anspruch auf die Veröffentlichung von Daten. Ein solcher Anspruch, der von jedermann einklagbar wäre, ist als effektives Korrektiv zu einer reinen Selbstverpflichtung der öffentlichen Stellen jedoch unverzichtbar.

Für die Länder, die amtliche Informationen auf der Grundlage von Informationsfreiheitsgesetzen bereits in Informationsregistern zur Verfügung stellen, wie auch für die anderen Länder kann das geplante Open-Data-Gesetz in dieser Form keine Vorbildfunktion entfalten. Die Weiterentwicklung des Informationsfreiheitsgesetzes des Bundes zu einem Transparenzgesetz mit den dazugehörigen Open-Data-Regelungen könnte dagegen eine entsprechende Signalwirkung für die Länder haben.

Die Informationsfreiheitsbeauftragten der Länder fordern den Bundestag eindringlich auf, den eingeschlagenen Sonderweg zu überdenken.

19.2 Entschließung: Mit Transparenz gegen „Fake-News“

13. Juni 2017

Internet und soziale Medien eröffnen zunehmend auch Möglichkeiten für die gezielte Verbreitung von Falschmeldungen zur Beeinflussung der politischen Meinungs- und Willensbildung. Eine informierte und kritische Gesellschaft benötigt jedoch vielfältige, freie und qualitativ aussagekräftige Informationen für eine umfassende gesellschaftliche und politische Teilhabe. Da die öffentlichen Stellen der Länder und des Bundes über solche Informationen verfügen, kommt ihnen insoweit eine

Schlüsselrolle zu. Deshalb ist es von zentraler Bedeutung, dass staatliche Institutionen transparent agieren, um das Vertrauen in die Demokratie und in deren Akteure zu stärken. Für den Prozess der politischen Meinungs- und Willensbildung sind verlässliche und solide Informationen eine unverzichtbare Voraussetzung.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland appelliert an alle öffentlichen Stellen in Deutschland, sich ihrer Verantwortung für die Informationsfreiheit bewusst zu sein und durch größtmögliche Transparenz – sowohl auf Antrag als auch proaktiv – die Bürgerinnen und Bürger in ihrer politischen Willensbildung zu unterstützen. Sie wirbt dafür, dass sich öffentliche Stellen in Deutschland noch stärker öffnen, auf die Informationswünsche der Bürgerinnen und Bürger eingehen, mit behördlichen Dokumenten valide und qualitätsvolle Informationen aus vertrauenswürdiger Quelle bereitstellen und die Kontrolle durch die Bürgerinnen und Bürger ermöglichen.

Damit kann auch bewusst gestreuten Fehlinformationen, mit denen die Manipulation des Meinungsbildes und die Schwächung demokratischer Institutionen verfolgt wird, aktiv und aufgeklärt im öffentlichen Diskurs entgegengetreten werden.

19.3 Grundsatzpositionen der Landesbeauftragten für die Informationsfreiheit

6. Oktober 2017

Informationen sind die Basis einer Demokratie. Sie sind Grund- und Treibstoff des Prozesses der öffentlichen Meinungsbildung. Transparenz schafft Vertrauen zwischen Politik, Verwaltung und Bevölkerung. Das Recht auf Zugang zu Informationen stellt ein zentrales Element zur Regelung des Informationsflusses von staatlichen Stellen zu Bürgerinnen und Bürgern in Deutschland dar. Die Informationsfreiheitsbeauftragten der Länder wenden sich mit den folgenden Forderungen zunächst an die Bundespolitik mit dem Ziel, dass sie im Rahmen ihrer Kompetenzen diesen Grundaussagen zur Geltung verhilft. Auch gegenüber der Landespolitik sollen diese Forderungen als grundsätzliche Anregungen zur Weiterentwicklung und zum Ausbau der informatorischen Rechtsstellung des Einzelnen auch gegenüber der Landespolitik dienen.

I. Informationsfreiheit in die Verfassungen!

Der Anspruch auf freien Zugang zu amtlichen Informationen soll in das Grundgesetz und in die Landesverfassungen aufgenommen werden

In dem Beschluss vom 20. Juni 2017 (1 BvR 1978/13) stellt das Bundesverfassungsgericht fest, dass sich der Verfassungsrang der Informationszugangsfreiheit aus Art. 5 Abs. 1 S. 1 Grundgesetz herleitet, jedenfalls soweit der Gesetzgeber eine einfachgesetzliche Regelung getroffen hat. Wer die Informationsfreiheit ernst nimmt, kann sie nicht in das Belieben des Gesetzgebers stellen. Deshalb ist die explizite Normierung im Grundgesetz erforderlich. Damit wäre für die Länder, die immer noch kein Recht auf voraussetzungslosen Zugang haben, die Pflicht verbunden, ein solches

Recht einfachgesetzlich zu verankern. Auch im Jahr 2017 verfügt ein Viertel der Länder immer noch nicht über ein Informationsfreiheitsgesetz.

II. Ein Gesetz für den Informationszugang! Hin zu Transparenzgesetzen!

Zusammenfassung der verschiedenen Informationsfreiheitsgesetze in einem Gesetz und Weiterentwicklung zu Transparenzgesetzen mit umfassenden Veröffentlichungspflichten Bestehende Informationszugangsansprüche in unterschiedlichen Informationsfreiheits- bzw. Transparenz- und Fachgesetzen sollten verstärkt zusammengefasst werden. Die Ansprüche auf Einsicht in Verwaltungsakten und auf Zugang zu sonstigen Informationen öffentlicher Stellen sind derzeit auf eine Vielzahl von Einzelvorschriften verteilt: Sie finden sich in den Informationsfreiheitsgesetzen, in den Umweltinformationsgesetzen, im Verbraucherinformationsgesetz und in diversen weiteren Gesetzen. Dabei werden vergleichbare Sachverhalte unterschiedlich geregelt, etwa die Voraussetzungen für den Informationszugang, die Fristen zur Beantwortung von Anfragen, die Gebühren, welche für den Informationszugang zu entrichten sind, und die Rechte auf Anrufung der Informationsfreiheitsbeauftragten. Diese Zersplitterung erschwert die Wahrnehmung der Informationsrechte und trägt zu Unsicherheiten bei der Rechtsanwendung durch die Behörden bei.

Zukünftig sollten die Vorschriften so gestaltet werden, dass ein Höchstmaß an Transparenz und Bürgerfreundlichkeit erreicht wird. Neben diesen anzustrebenden Erleichterungen für die Bürgerinnen und Bürger bei der Durchsetzung ihrer Informationszugangsansprüche ist die Weiterentwicklung der jeweiligen Informationsfreiheitsgesetze zu Transparenzgesetzen ein wichtiges Anliegen. Solche Gesetze verbinden den individuellen, antragsgebundenen Informationszugangsanspruch mit der Verpflichtung öffentlicher Stellen, bestimmte Informationen von sich aus und antragsunabhängig auf Informationsplattformen im Internet zu veröffentlichen. Derartige gesetzliche Veröffentlichungspflichten erhöhen die Verwaltungstransparenz, die Nachvollziehbarkeit, Akzeptanz und Kontrolle behördlicher Entscheidungsprozesse. Die Verwaltung soll zukünftig ihre Daten automatisch zur Verfügung stellen. Ausnahmen für die Nichtzurverfügungstellung müssen begründet werden. Das wirtschaftliche Potential von offenen Verwaltungsdaten wird bisher nicht ausreichend genutzt.

III. Nachrichtendienste ins IFG!

Erweiterung des Anwendungsbereichs der Informationsfreiheitsgesetze durch Abschaffung der Bereichsausnahme für die Nachrichtendienste Die Informationsfreiheitsbeauftragten der Länder halten die in § 3 Nr. 8 IFG normierte Bereichsausnahme für die Nachrichtendienste für nicht erforderlich. Es läuft dem Transparenzgedanken zuwider, dass ein kompletter Verwaltungsbereich vom Informationsfreiheitsgesetz ausgenommen wird. Die Regelung führt dazu, dass die Nachrichtendienste im Fall eines Antrages nicht begründen müssen, warum eine Information nicht herauszugeben ist. Das bedeutet zudem, dass auch nicht-geheimhaltungsbedürftige Informationen zurückbehalten werden können. Die Informationsfreiheitsbeauftragten stellen mit ihrer Forderung nicht den Geheimnisschutz an sich in Frage. Sie sind vielmehr der Ansicht, dass es ausreicht, wenn sich die Nachrichtendienste hinsichtlich der Herausgabe bzw. Nichtherausgabe von Informationen auf die Ausschlusstatbestände des Informationsfreiheitsgesetzes berufen können. Somit wären die Nachrichten-

dienste dazu verpflichtet, ihre Entscheidungen zu begründen. Vergleiche mit Bundesländern wie beispielsweise Schleswig-Holstein, Rheinland-Pfalz und Mecklenburg-Vorpommern zeigen, dass die Verfassungsschutzbehörden auch ohne Bereichsausnahme nicht auf Geheimnisschutz verzichten müssen.

IV. Abschaffung unnötiger Ausnahmen!

Beschränkungen der Ausnahmeregelungen auf das verfassungsrechtlich zwingend gebotene Maß auf der Grundlage der Evaluierung des IFG Bund Bei der Regelung ihrer Informationsfreiheitsgesetze haben sich zahlreiche Länder in der Vergangenheit am Informationsfreiheitsgesetz des Bundes orientiert, das für sie eine Vorbildfunktion hatte. Nach dessen Evaluierung im Jahr 2012 ergibt sich für den Bund und damit inzident auch für diejenigen Bundesländer, die mit ihrem Landesrecht dem Bund gefolgt waren, erheblicher Reformbedarf. So ist etwa eine Reduzierung und Harmonisierung der Ausschlussgründe, die einem Informationszugang entgegenstehen können, angezeigt. Zu viele, teilweise redundante und sich überschneidende Ausschlussgründe konterkarieren Open Data, Open Government und damit Bürgerbeteiligung und Demokratie. Eine allgemeine Güterabwägung zwischen Informations- und Geheimhaltungsinteresse (public interest test) ist daher als Korrektiv erforderlich.

V. Mehr Transparenz in der Drittmittelforschung!

Sicherstellung von Transparenz der Kooperationen zwischen privaten und wissenschaftlichen Einrichtungen Unternehmensfinanzierte Forschung gewinnt zunehmende Bedeutung für die Hochschulen in der Bundesrepublik Deutschland. Deutschlandweit ist eine große Anzahl von Lehrstühlen direkt oder indirekt von Unternehmen finanziert. Oft sind Ziele und Umfang der Förderung für Außenstehende nicht erkennbar. Für eine Einordnung der Forschungsergebnisse und deren Bewertung ist die Kenntnis dieser Hintergründe jedoch bedeutsam. Die Freiheit von Forschung und Wissenschaft lebt von einer offenen Diskussion; die Geheimhaltung von Zusammenhängen kann diese Freiheiten einengen. Einer verborgenen Einflussnahme auf Forschungsgegenstände, Forschungsergebnisse und auf deren Veröffentlichung kann durch eine konsequente Politik der Offenheit begegnet werden. Deshalb sollten Kooperationsverträge zwischen Wissenschaft und Unternehmen grundsätzlich offengelegt werden. Die Pflicht zur Veröffentlichung der Verträge darf nur zurücktreten, soweit und solange die Bekanntgabe geschützte Interessen beeinträchtigt. Die regelmäßige Offenlegung der Finanzierung von Forschungsprojekten ist nach Auffassung der Informationsfreiheitsbeauftragten ein geeignetes Instrument, um die Freiheit der Forschung zu schützen, indem einseitige Abhängigkeiten oder auch nur deren Anschein vermieden werden. Eine bloße Selbstverpflichtung der Universitäten und Forschungseinrichtungen ist hierfür nicht ausreichend. Die Informationsfreiheitsbeauftragten der Länder fordern konsequente gesetzliche Regelungen zugunsten der Transparenz von drittmittelgeförderter Forschung in Bund und Ländern.

19.4 Entschließung: Soziale Teilhabe braucht konsequente Veröffentlichung von Verwaltungsvorschriften!

16. Oktober 2018

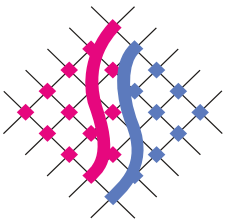
Eine offene und transparente Verwaltungskultur ist eine Voraussetzung dafür, dass sich Bürgerinnen und Bürger und Staat auf Augenhöhe begegnen. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert die Sozialleistungsträger auf, Verwaltungsvorschriften antragsunabhängig, zeitnah und benutzerfreundlich zu veröffentlichen, soweit sie dazu nicht bereits gesetzlich verpflichtet sind.[152]

Soziale Teilhabe aller Menschen in unserer Gesellschaft folgt aus dem im Grundgesetz verankerten Sozialstaatsprinzip. Ausdruck dieses Prinzips ist ein soziales Sicherungssystem, das durch Sozialleistungen auf Grundlage der Sozialgesetzbücher einen Grundstandard an sozialer Sicherheit gewährleisten soll. Nur informierte Bürgerinnen und Bürger können sie betreffende Entscheidungen von Sozialleistungsträgern verstehen, Ansprüche geltend machen, aber auch Pflichten wahrnehmen.

Alle Sozialleistungsträger bedienen sich Verwaltungsvorschriften, um innerhalb ihrer Behörde eine einheitliche Bearbeitungs- bzw. Entscheidungspraxis sicherzustellen. Verwaltungsvorschriften sind interne Weisungen, die regeln, wie Gesetze auszulegen und anzuwenden sind. Zwar binden Verwaltungsvorschriften unmittelbar nur die Verwaltung selbst; die auf ihrer Grundlage getroffenen Entscheidungen wirken aber nach außen. Verwaltungsvorschriften sind daher bekannt zu geben, damit *„der Betroffene (…) sich des Inhalts der durch sie für ihn begründeten Rechte und Pflichten vergewissern"*[153] kann. So agieren in diesem Bereich etwa die Bundesagentur für Arbeit sowie die Deutsche Rentenversicherung, die aktuelle Weisungen veröffentlichen. Viele andere Sozialleistungsträger geben die Informationen hingegen allenfalls auf Antrag heraus.

[152] Gesetzliche Verpflichtungen bestehen derzeit in: Hamburg, Bremen, Rheinland-Pfalz, Schleswig-Holstein (ab 1.1.2020).

[153] Urteil des Bundesverwaltungsgerichts vom 25.11.2004, Az. 5 CN 1.03.



UNABHÄNGIGES
DATENSCHUTZ
ZENTRUM SAARLAND

Die Landesbeauftragte für Datenschutz
und Informationsfreiheit

Fritz-Dobisch-Straße 12
66111 Saarbrücken
Telefon 0681 94781-0
Telefax 0681 94781-29
E-Mail poststelle@datenschutz.saarland.de
Internet www.datenschutz.saarland.de
www.informationsfreiheit.saarland.de