Die Landesbeauftragte für
Datenschutz und Informationsfreiheit

28. Tätigkeitsbericht Datenschutz

UNABHÄNGIGES DATENSCHUTZ ZENTRUM SAARLAND

2019

28. Tätigkeitsbericht

der Landesbeauftragten für Datenschutz und Informationsfreiheit

Berichtszeitraum: 2019

Dem Landtag und der Landesregierung
vorgelegt am 11. März 2020
(Landtagsdrucksache 16/1200)

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 28. Tätigkeitsbericht des Unabhängigen Datenschutzzentrums Saarland bezieht sich erstmals ausschließlich auf ein Kalenderjahr und ersetzt damit den gewohnten zweijährigen Turnus unserer Berichterstattung.

Die von der Datenschutz-Grundverordnung (DSGVO) vorgegebene Verkürzung des Berichtzeitraums ist zugleich Anlass für eine strukturelle Überarbeitung des Berichtkonzepts, um auch durch eine Straffung der Darstellung die Prägnanz zu erhöhen. So soll der Fokus weniger auf einer detaillierten Darstellung von Einzelfällen, als vielmehr auf Ausführungen zu grundsätzlichen Fragen des Datenschutzes liegen, insbesondere zu solchen Fragestellungen, welche besonders häufig an unsere Dienststelle herangetragen werden. Auch werden die Entschließungen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) dem Bericht nicht mehr als Anhänge beigefügt. Als begleitende und vertiefende Lektüre zu dem Tätigkeitsbericht veröffentlichen wir diese Entschließungen ebenso wie die weiteren Informationsmaterialien der DSK und unserer Dienststelle – wie gewohnt – auf unserer nunmehr neu gestalteten Webseite. Unsere Tätigkeit im Bereich der Informationsfreiheit werden wir weiterhin für jeweils zwei Kalenderjahre in einem eigenständigen Bericht darstellen.

Ein Rückblick auf den Berichtszeitraum zeigt, dass sich Unternehmen und Behörden mittlerweile mit der neuen Rechtslage auseinandergesetzt und ihre teilweise über Jahrzehnte gewachsenen Verarbeitungsstrukturen hieran angepasst haben. Diese erfreuliche Entwicklung darf jedoch nicht darüber hinwegtäu-

schen, dass weiterhin in vielen Bereichen noch Anpassungsbedarf besteht. Daher ist auch nicht verwunderlich, dass ein erheblicher Beratungsbedarf der verantwortlichen Stellen auszumachen und die Zahl entsprechender Anfragen an unsere Dienststelle nach wie vor sehr hoch ist. Auf der einen Seite finden diese Beratungen zu einem großen Teil im Rahmen von individuellen Erörterungen mit den Verantwortlichen statt, auf der anderen Seite aber auch durch die Zurverfügungstellung von Leitlinien, Orientierungshilfen und Anwendungshinweisen. Den Rechtsanwendern kann somit eine wertvolle Orientierung bei der Auslegung der teilweise sehr abstrakten Regelungen der DSGVO angeboten werden.

Die enge und effektive Zusammenarbeit innerhalb der DSK ist ein ganz wesentliches Instrument, um durch die Veröffentlichung abgestimmter Rechtsauffassungen den Anwendern der DSGVO von behördlicher Seite eine größtmögliche Rechtssicherheit zu geben und um das Ziel einer europaweit einheitlichen Rechtsanwendung im Bereich des Datenschutzes zu erreichen. Dieser Abstimmungsprozess stellt neben der Bearbeitung der deutlich gestiegenen Anzahl datenschutzrechtlicher Beschwerden und Anfragen inzwischen einen weiteren personal- und arbeitsintensiven Schwerpunkt unserer Tätigkeit dar.

Aber auch der europaweiten Zusammenarbeit der Aufsichtsbehörden in den zahlreichen Arbeitsgremien, die dem Europäischen Datenschutzausschuss zuarbeiten, kommt mittlerweile eine immer größere Bedeutung zu. Bedauerlicherweise ist unsere Dienststelle derzeit personell noch nicht in der Lage, sich in diesen europaweiten Abstimmungsprozess in dem gewünschten Umfang einzubringen. Dies wird sich jedoch künftig als eine dringende Notwendigkeit erweisen, ist es doch die europäische

Ebene, auf welcher die wesentlichen datenschutzrechtlichen Fragen auch und gerade in Bezug auf die global agierenden Internetunternehmen und IT-Dienstleister beantwortet werden. Im Rahmen dieser Entscheidungsprozesse, welche nicht zuletzt auch erhebliche Auswirkungen auf verantwortliche Stellen und betroffene Personen im Saarland haben werden, sehen wir es als erforderlich an, unser Bundesland mit starker Stimme vertreten zu können.

Im Berichtszeitraum zeigte sich erneut sehr deutlich, dass die mit der zunehmenden Digitalisierung verbundenen Möglichkeiten der Verarbeitung immer umfangreicherer Datenbestände mit steigenden Gefahren für das Recht auf informationelle Selbstbestimmung der Bürger verbunden sind. Ein deutliches Zeichen hierfür ist die kontinuierlich steigende Zahl der an unsere Dienststelle gerichteten Meldungen von Datenschutzverletzungen, etwa aufgrund von Cyberangriffen. Auch die wachsende Zahl von Beschwerden verdeutlicht, dass viele Bürger die immer weitgreifendere Datenerhebung nicht weiter hinnehmen wollen. Aufgrund der zunehmenden Komplexität der digitalen Verarbeitungsvorgänge ist die aufsichtsbehördliche Tätigkeit in diesem Bereich vielfach sehr arbeits- und zeitintensiv. Eine Aufstockung der personellen Ressourcen würde auch in diesem Bereich zu einer wesentlichen Förderung der aufsichtsbehördlichen Tätigkeit beitragen und in vielen Fällen zu einer deutlichen Verkürzung der Verfahrensdauer führen.

Diese einleitenden Worte über die Schwerpunkte unserer Aufgabenwahrnehmung im vergangenen Jahr vorausgeschickt, soll Ihnen der vorliegende Bericht nunmehr die vielfältigen Tätigkeitsbereiche unserer Behörde näherbringen. Selbstverständlich kann dieser nur einen Einblick in die tägliche Arbeit unserer

Dienststelle geben; gleichwohl haben wir darauf geachtet, dass er das breite Spektrum an datenschutzrechtlichen Fragestellungen, die von einer Datenschutzaufsichtsbehörde zu beantworten sind, widerspiegelt. An dieser Stelle danke ich ganz herzlich allen Mitarbeiterinnen und Mitarbeitern, die mit ihrem großen persönlichen Engagement sowohl bei der fachlichen Bearbeitung der Verfahren als auch bei der internen Organisation der Arbeitsabläufe als Team für das reibungslose Funktionieren unserer Dienststelle sorgen.

Saarbrücken, im März 2020

Monika Grethel

Landesbeauftragte für Datenschutz
und Informationsfreiheit

Inhaltsverzeichnis

Abbildungsverzeichnis

1.

Zahlen und Fakten

1 Zahlen und Fakten

Die Datenschutz-Grundverordnung (DSGVO) verpflichtet die Datenschutzaufsichtsbehörden zur jährlichen Erstellung eines Berichts über die Schwerpunkte ihrer Tätigkeit (Art. 59). Diese Tätigkeitsberichte stellen eine wesentliche Informationsquelle für die Öffentlichkeit und die Parlamente über aktuelle Entwicklungen im Datenschutzrecht dar. Um einen ersten und allgemeinen Überblick über die Anzahl der Sachverhalte zu geben, mit denen sich die deutschen Aufsichtsbehörden im Berichtszeitraum befasst haben und um die Transparenz und Vergleichbarkeit der Tätigkeit der Aufsichtsbehörden zu erhöhen, hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) gemeinsame Kriterien zur statistischen Darstellung von Tätigkeitsschwerpunkten aufgestellt. Entsprechend dieser Vereinbarung werden im Folgenden die wesentlichen Kategorien von Verfahren, mit denen sich das Unabhängige Datenschutzzentrum Saarland im Berichtszeitraum zu befassen hatte, aufgeführt, wobei landesspezifische Aufgaben und Tätigkeiten nicht erfasst werden.

1.1 Beschwerden

Hier wird eine Übersicht über die Anzahl von Beschwerden, die im Berichtszeitraum eingegangen sind, gegeben. Als Beschwerden werden solche Vorgänge erfasst, die schriftlich eingehen und bei denen eine natürliche Person eine persönliche Betroffenheit darlegt. Die zahlreichen an die Dienststelle gerichteten Anregungen, einem als datenschutzwidrig angenommenen Sachverhalt aufsichtsbehördlich nachzugehen, fließen mithin nicht in die Statistik ein. Diese werden ebenso wie (fern-)münd-

liche Beschwerden nur dann statistisch erfasst, wenn sie verschriftlicht werden und zu weitergehenden Maßnahmen Veranlassung geben.

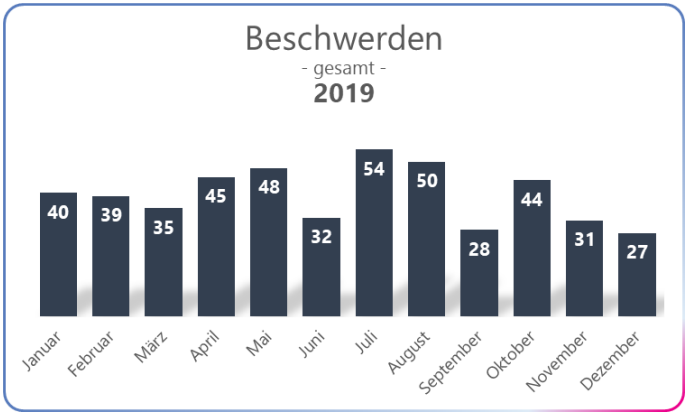

Abb. 1: Beschwerden (gesamt) 2019

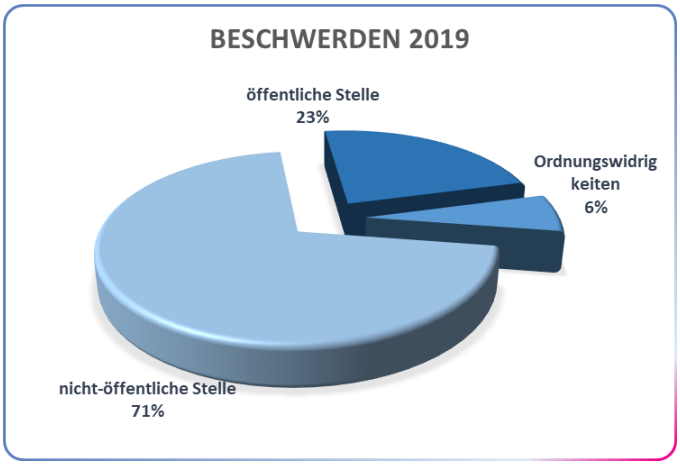

Abb. 2: Beschwerden (Aufteilung) 2019

1.2 Beratungen

Hier wird eine Übersicht über die Anzahl von schriftlichen Beratungen gegeben. Dies umfasst Beratungen von Verantwortlichen, betroffenen Personen und der Landesregierung. Ausschließlich (fern-)mündliche Beratungen werden statistisch nicht erfasst, obwohl diese einen sehr hohen Anteil der an unsere Dienststelle gerichteten Anfragen darstellen und einen hohen zeitlichen Aufwand erfordern.

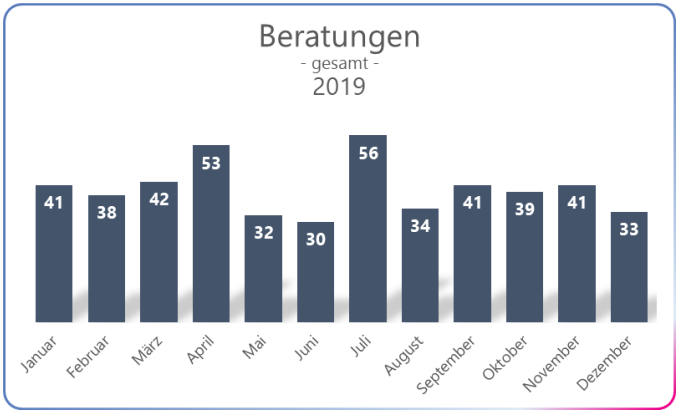

Abb. 3: Beratungen (gesamt) 2019

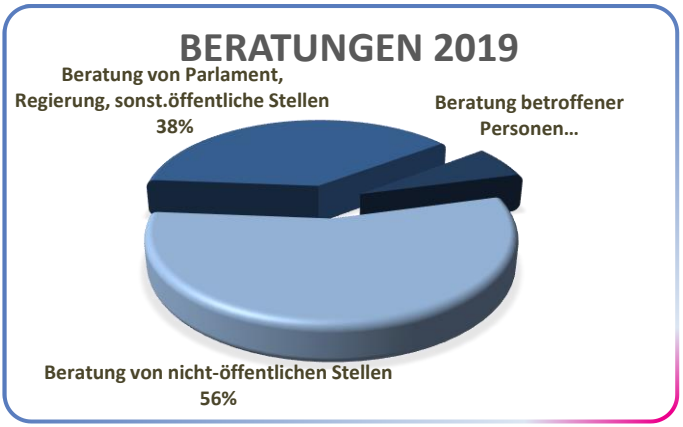

Abb. 4: Beratungen (Aufteilung) 2019

1.3 Meldungen von Datenschutzverletzungen

Hier wird eine Übersicht über die Anzahl schriftlich eingegangener Meldungen von Verantwortlichen über Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DSGVO gegeben.

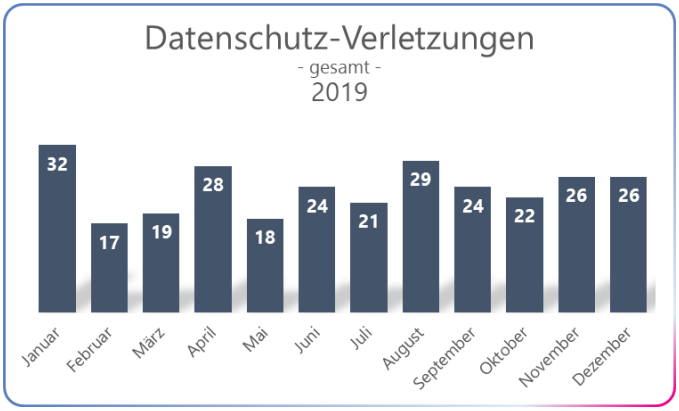

Abb. 5: Datenschutzverletzungen 2019

1.4 Abhilfemaßnahmen

Um drohende datenschutzrechtliche Verstöße zu verhindern oder festgestellte Verstöße zu sanktionieren, werden den Aufsichtsbehörden in Art. 58 Abs. 2 DSGVO verschiedene Abhilfemaßnahmen zur Verfügung gestellt, die sie – je nach Schwere der Verstöße – nach pflichtgemäßem Ermessen anwenden. Hier wird die Anzahl folgender Abhilfemaßnahmen aufgelistet, die im Berichtszeitraum getroffen wurden:

- Warnungen nach Art. 58 Abs. 2 lit. a,
- Verwarnungen nach Art. 58 Abs. 2 lit. b,
- Anweisungen und Anordnungen nach Art. 58 Abs. 2 lit. c – g und j,
- Geldbußen nach Art. 58 Abs. 2 lit. i sowie
- Widerruf von Zertifizierungen nach Art. 58 Abs. 2 lit. h.

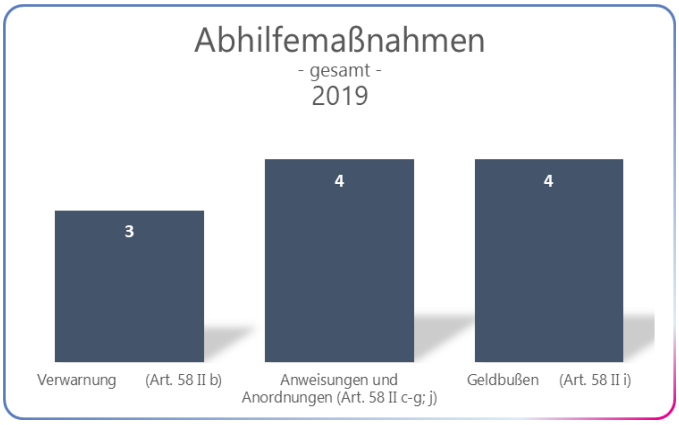

Abb. 6: Abhilfemaßnahmen (gesamt) 2019

1.5 Europäische Verfahren

Einen zunehmenden Stellenwert bei der Aufgabenwahrnehmung des Unabhängigen Datenschutzzentrums Saarland (UDZ) kommt der Zusammenarbeit mit anderen europäischen Datenschutzaufsichtsbehörden zu.

Wie bereits im letzten Tätigkeitsbericht beschrieben, enthält die Datenschutz-Grundverordnung (DSGVO) in ihrem Kapitel VII. für alle europäischen Datenschutzaufsichtsbehörden verbindliche Verfahrensvorgaben, die eine engere Zusammenarbeit und damit eine einheitliche Anwendung der DSGVO innerhalb der gesamten EU gewährleisten sollen. Obwohl der dadurch gestiegene Koordinierungsaufwand auch beim UDZ in zunehmendem Maße erhebliche personelle und zeitliche Ressourcen beansprucht, ist dieser Mehraufwand wiederum durch den für alle Seiten gewinnbringenden europäischen Austausch gerechtfertigt.

Ein Teilaspekt dieser Verfahren besteht darin, dass nationale Datenschutzaufsichtsbehörden die Möglichkeit erhalten, auf Verfahren in anderen EU-Mitgliedstaaten Einfluss zu nehmen, sofern diese auch für die eigenen Bürger von Bedeutung sind. So kann jede Aufsichtsbehörde sicherstellen, dass die Rechte der Bürger im eigenen (Bundes-)Land gewahrt bleiben, selbst dann, wenn datenverarbeitende Stellen im innereuropäischen Ausland niedergelassen sind. Voraussetzung hierfür ist, dass die verantwortliche Stelle personenbezogene Daten „grenzüberschreitend" (Art. 4 Nr. 23 DSGVO) verarbeitet. Dies ist etwa dann der Fall, wenn Daten Betroffener durch Niederlassungen in mehreren EU-Mitgliedstaaten verarbeitet werden oder etwa

wenn Personen in mehreren EU-Mitgliedstaaten von einer Verarbeitung erheblich betroffen sind.

	Bundesrepublik Deutschland	Saarland
Verfahren mit Betroffenheit Art. 56	570	154
Verfahren mit Federführung Art. 56	63	2
Verfahren gem. Kapitel VII DSGVO	1109	476

Abb. 7: Europäische Verfahren (gesamt) 2019

Zu diesem Zweck hatte auch das UDZ im Jahr 2019 in 906 Fällen zu beurteilen, inwieweit es als „betroffene Aufsichtsbehörde" im Sinne des Art. 4 Nr. 22 DSGVO an diesen grenzüberschreitenden Verfahren zu beteiligen war, weil beispielweise eine Niederlassung der verarbeitenden Stelle im Saarland existiert oder weil auch saarländische Bürger von einer konkreten Verarbeitung erheblich betroffen sein könnten.

In 154 Fällen wurde diese Betroffenheit für das UDZ bejaht. Im Rahmen dieser Verfahren war das UDZ zweimal „federführend" (Art. 56 Abs. 1 DSGVO) zuständig, so dass in diesen Verfahren die entsprechenden Verfahrenshandlungen gegenüber verantwortlichen Stellen direkt durch das UDZ vorzunehmen waren. Hierbei erfolgt eine Abstimmung mit anderen von der Verarbeitung betroffenen Datenschutzaufsichtsbehörden innerhalb der EU. Sind diese etwa nicht mit dem Vorgehen und den durch die federführende Aufsichtsbehörde geplanten Maßnahmen einverstanden, weil sie den Sachverhalt abweichend beurteilen, haben sie die Möglichkeit, gegen den Entscheidungsentwurf der federführenden Aufsichtsbehörde Einspruch einzulegen. Bezogen auf hiesige Dienststelle wurde dabei eines der Verfahren

ohne Einwände anderer europäischer Aufsichtsbehörden abgeschlossen. Ein weiteres Verfahren befindet sich noch in Bearbeitung.

Darüber hinaus wurden mehrere freiwillige Amtshilfeersuchen europäischer Aufsichtsbehörden an das UDZ gerichtet, im Rahmen derer ein allgemeiner Austausch über diverse datenschutzrechtliche Fragestellungen erfolgte.

1.6 Förmliche Begleitung von Rechtsetzungsvorhaben

Hier werden die von dem Parlament und der Regierung angeforderten und durchgeführten Stellungnahmen zu Gesetzgebungsvorhaben genannt. Ein solches Vorhaben wird durch unsere Dienststelle einmal statistisch erfasst, selbst wenn die Stellungnahmen gegenüber unterschiedlichen Stellen in verschiedenen Verfahrensstadien erfolgen. Gerade bei Gesetzgebungsverfahren erfolgt unsere Beteiligung oft bereits im Rahmen der ressortinternen Entwurfserstellung, sodann bei der externen Anhörung und schließlich im Zusammenhang mit der parlamentarischen Anhörung im Landtag. Ebenfalls statistisch erfasst wird die Teilnahme an öffentlichen Ausschüssen und Stellungnahmen gegenüber Gerichten.

Im Berichtzeitraum wurde das UDZ hiernach in 11 Rechtsetzungsvorhaben verfahrensbegleitend tätig.

II.

Aus der Dienststelle

2 Aus der Dienststelle

2.1 Personal und Organisation

2.1.1 Personelle Ausstattung

Der Landtag hat unserer Dienststelle für das Haushaltsjahr 2018 vier Stellen und für den Doppelhaushalt 2019/2020 zwei weitere Stellen zur Bewältigung des mit dem erheblichen Aufgabenzuwachs der Aufsichtsbehörden durch die Datenschutz-Grundverordnung (DSGVO) verbundenen Arbeitsaufwands bewilligt. Diese Stellen konnten bis zum Ende des Berichtszeitraums besetzt werden. Aufgrund verschiedener Umstände, wie Elternzeit und Teilzeitbeschäftigung, liegt die Zahl der Vollzeitäquivalente allerdings noch unter der Zahl der im Haushaltsplan ausgewiesenen Planstellen.

Die ersten Erfahrungen mit den zahlreichen zusätzlichen Aufgaben und Befugnissen einer Datenschutzaufsichtsbehörde nach Wirksamwerden der DSGVO sowie die rechtlich und technisch immer komplexer werdenden Verfahren zeigen allerdings deutlich, dass eine weitere Personalaufstockung weiterhin notwendig sein wird.

2.1.2 Relaunch des Internetauftritts des Datenschutzzentrums

Was heute als modern und interessant gilt, kann morgen schon veraltet wirken. Neben spezifischen Kriterien müssen für den Internetauftritt einer Organisation – insbesondere einer öffentlichen Verwaltung – auch Vorgaben rechtlicher und sicherheitstechnischer Art durch sog. technisch-organisatorische Maßnahmen umgesetzt werden.

Vor diesem Hintergrund hat sich das Unabhängige Datenschutzzentrum dazu entschieden, seinen bereits acht Jahre alten Webauftritt einem Relaunch zu unterziehen.

Es wird nunmehr ein aktuelles Content-Managementsystem eingesetzt, mit dessen Hilfe sämtliche Inhalte redaktionell bearbeitet und anschließend publiziert werden können.

In erster Linie präsentiert sich der Webauftritt des Datenschutzzentrums in einem neuen zeitgemäßen Design. Ziel war hier die Struktur der Seiten zu verbessern und zu optimieren, diese für den Besucher ansprechender zu gestalten und so die Benutzerfreundlichkeit zu erhöhen.

Ein weiterer Grund für den Relaunch war, den Webauftritt designspezifisch so zu gestalten, dass die publizierten Inhalte auch für mobile Endgeräte wie Smartphones und Tablets optimiert dargestellt werden und damit ein durchgängiges Responsive-Webdesign umzusetzen.

Gleichzeitig wurde dabei auch Wert darauf gelegt, dass möglichst viele Inhalte barrierefrei zugänglich sind.

Zusätzlich sollten verschiedene Funktionalitäten, wie Kontakt- und Beschwerdeformulare und weitere Formulare für die Meldung von Datenschutzverletzungen und die Benennung von Datenschutzbeauftragten, der Downloadbereich und die Suchfunktionen verbessert werden.

Die aktualisierte Website des Datenschutzzentrums ist unter der Adresse **https://www.datenschutz.saarland.de** erreichbar.

2.1.3 ISMS-Zertifizierung des UDZ

Mit der steigenden Komplexität der Systeme, dem hohen Grad der Vernetzung und der Abhängigkeit unserer Gesellschaft von der IT gehen auch Sicherheitsrisiken einher.

Seit 2016 steigen die Cyberangriffe insbesondere auf öffentliche Einrichtung bzw. deren IT-Infrastrukturen stetig an.[1] Ferner ermittelte die Allianz für Cybersicherheit aus Umfragen der Jahre 2017 und 2018, dass rund 60% der berichteten Angriffe auf Malware-Infektionen zurückzuführen sind.[2]

Eine im Berichtszeitraum besonders relevante Malware ist Emotet. Das schon seit 2010 bekannte Schadprogramm ist seit Anfang 2019 wieder vermehrt mit Hilfe von schädlichen Office-Dokumenten (Word, Excel und E-Mails) verteilt worden – mit immer ausgefeilteren Mechanismen. Die Evolution von Emotet zeigt sich insbesondere an neuen Fähigkeiten wie dem Outlook-Harvesting (der Analyse des Mailverlaufs infizierter Computer), dem Nachladen von beliebigen anderen Schadprogrammen im Kontext kooperierender und arbeitsteiliger hochprofessioneller Computerkriminalität sowie der Verwendung von Techniken, die bisher nur bei Advanced Persistent Threats (APTs) eingesetzt wurden. Neben Malware gibt es weitere Angriffsvektoren, die die Funktionsfähigkeit (Verfügbarkeit), die Integrität und die Vertraulichkeit insbesondere von IT-Systemen öffentlicher Institutionen, fokussieren. Hierzu gehören DDoS-Angriffe (Ziel ist

[1] Vgl. Bundesamt für Sicherheit in der Informationstechnologie, Lage der IT-Sicherheit in Deutschland 2019, elektronisch abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=7

[2] Vgl. Bericht der Allianz für Cybersicherheit 2019, elektronisch abrufbar unter: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html

hierbei die Einschränkung der Erreichbarkeit einer Behörde) und Botnetze (Ziele sind hier das Abfischen personenbezogener Daten und die missbräuchliche Verwendung von IT-Infrastrukturen einer Behörde für kriminelle Handlungen), um nur zwei wesentliche technische Angriffsmöglichkeiten zu nennen.

Um Cyber-Sicherheit erfolgreich gewährleisten zu können, ist die Abwehr von Angriffen der wesentliche Aspekt. Sensibilisierung und Eigenverantwortung im Umgang bei der Digitalisierung sind neben technischen Lösungen notwendige Antworten auf den zunehmenden Missbrauch digitaler Identitäten und Angriffe von außen. Wirksamer Schutz ist aber nur möglich, wenn die allgemeine wie auch die konkrete Gefährdungslage zumindest im Überblick bekannt sind. Eine regelmäßige und gezielte Neubewertung der bestehenden Risiken ist aufgrund der dynamischen Entwicklung der Cyber-Sicherheitslage unabdingbar, um geeignete präventive und reaktive Maßnahmen auszuwählen.

Um diese wachsenden Anforderungen und die rechtlichen Vorgaben zu erfüllen, Angriffe auf Informationen und Systeme von außen wie auch von innen abwehren zu können und dabei insbesondere die Kosten überschaubar zu halten, ist es daher sinnvoll, ein entsprechendes Informationssicherheitsmanagementsystem (ISMS) zu etablieren und nachhaltig zu betreiben.

Unter dem Begriff ISMS ist ein umfassendes, ganzheitliches und standardisiertes Managementsystem zu verstehen. Dieses umfasst definierte Regeln und Prozesse, die der Definition, Steuerung, Kontrolle, Wahrung und fortlaufenden Optimierung der Informationssicherheit in einer Organisation dienen.

Im Kern verlangt Art. 32 Datenschutz-Grundverordnung (DSGVO) die Etablierung eines Datenschutzmanagementsystems, das auf einem ISMS aufbaut.

Der IT-Planungsrat, das zentrale Gremium für die föderale Zusammenarbeit in der Informationstechnik, hat in seiner 16. Sitzung[3] den Leitfaden "Informationssicherheitsmanagementsystem in 12 Schritten (ISIS12)" als pragmatisches und leicht skalierbares Vorgehensmodell zur Etablierung eine Sicherheitsmanagementsystems empfohlen. ISIS12 wurde insbesondere für die Anforderungen der kommunalen Verwaltungsbereiche und für Unternehmen aus dem Klein- und Mittelstand entwickelt und versucht durch eine schrittweise Umsetzung, den Spagat zwischen der Notwendigkeit einerseits und dem organisatorisch Leistbaren andererseits zu schaffen.

Der gesamte Prozess von der Sensibilisierung der Mitarbeiter, Einschätzung der Gefährdungslage bis hin zur Abwehr von Angriffen kann durch ein ISMS wie ISIS12 gesteuert und überwacht werden.

Vor diesem Hintergrund hat sich das UDZ entschieden, ein Managementsystem zu implementieren. Die in Art. 32 Abs. 1 lit. d DSGVO geforderte regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung wurde durch ein entsprechendes Audit geprüft und anschließend durch die Deutsche Gesellschaft zur Zertifizierung von Managementsystemen (DQS GmbH) zum 9. Oktober 2019 erfolgreich zertifiziert. Die Nachhaltigkeit der Umsetzung wird

[3] Elektronisch abrufbar unter: https://www.it-planungsrat.de/SharedDocs/Sitzungen/DE/2015/Sitzung_16.html?pos=5

einerseits durch den im Datenschutzzentrum etablierten kontinuierlichen Verbesserungsprozess und andererseits durch ein jährlich stattfindendes Überwachungsaudit sichergestellt.

2.2 Öffentlichkeitsarbeit und Schulungen

2.2.1 Öffentlichkeitsarbeit

Auch im Berichtsjahr war der Bedarf an Informationen zur Datenschutz-Grundverordnung (DSGVO) sehr hoch. Dementsprechend haben wir, wie bereits im Vorjahr, eine ganze Reihe von Veranstaltungen entweder selbst durchgeführt oder an zahlreichen Veranstaltungen als Referenten teilgenommen. Insgesamt konnten wir dadurch in über 50 Veranstaltungen Interessierte für datenschutzrechtliche Fragen sensibilisieren und fortbilden. Während bei den Veranstaltungen des Vorjahres noch im Vordergrund stand, interessierten Stellen einen ersten Überblick über die neuen Datenschutzregeln zu verschaffen, haben wir nunmehr den Fokus eher auf die sich zwischenzeitlich herauskristallisierten Problembereiche und Auslegungsfragen gerichtet. Dabei waren neben rein datenschutzrechtlichen Themen häufig Fragen um den technischen Schutz von Daten Gegenstand der Diskussionen.

Auf große Resonanz stieß unsere erste Veranstaltung bei der Vertretung des Saarlandes bei der Europäischen Union in Brüssel. Gemeinsam mit dem letztjährigen Vorsitzenden der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), dem rheinland-pfälzischen Landesbeauftragten für Datenschutz und Informationsfreiheit, einem Vertreter der Generaldirektion Justiz und Verbraucherschutz der Europäischen Kommission sowie dem Datenschutzbeauftragten im Mi-

nisterium der Deutschsprachigen Gemeinschaft in Belgien haben wir über erste Erfahrungen in der grenzüberschreitenden Zusammenarbeit der europäischen Aufsichtsbehörden diskutiert.

Das insgesamt gestiegene Interesse an Fragen des Datenschutzes zeigte sich auch an der Zahl der an das Unabhängige Datenschutzzentrum gerichteten Medienanfragen. Die intensive Beobachtung der allgemeinen Entwicklungen im Datenschutzrecht hat noch einmal zu einer Verdoppelung der bereits im Vorjahr deutlich gestiegenen Zahl an Anfragen geführt. Dabei standen neben Anfragen zur Sanktionspraxis unserer Behörde und zu dem Stand der Umsetzung der DSGVO in Unternehmen und Behörden auch immer wieder datenschutzrechtliche Bewertungen tagesaktueller Themen im Fokus der Anfragen.

Das ungebrochene Interesse der Öffentlichkeit an datenschutzrechtlichen Fragestellungen belegt, dass Datenschutz kein Randthema ist, sondern alle Bereiche der Gesellschaft in ihrem Alltag beschäftigt. Daher wird der aktiven Öffentlichkeitsarbeit in unserer Dienststelle perspektivisch ein noch höheres Gewicht beigemessen werden müssen.

2.2.2 Arbeitsgemeinschaft der obersten Landesbehörden

Unter der Koordination des Saarländischen Ministeriums für Inneres, Bauen und Sport wurde im Februar des Jahres 2019 eine ressortübergreifende Arbeitsgemeinschaft zur DSGVO ins Leben gerufen, an welcher neben den übrigen Landesministerien und der Staatskanzlei des Saarlandes auch unsere Behörde in beratender Funktion beteiligt war.

Ziel der mittlerweile ausgelaufenen Arbeitsgemeinschaft war die einheitliche Auslegung und Anwendung der DSGVO auf Ebene der obersten Landesbehörden. Die zu diesem Zweck gegründeten drei Unterarbeitsgruppen setzten sich in mehreren Terminen schwerpunktbezogen mit den *Grundsatzfragen zum Datenschutz*, dem *Datenschutz in Personalangelegenheiten* sowie dem *Datenschutz im Rahmen der Öffentlichkeitsarbeit* auseinander. Hierbei konnten zahlreiche datenschutzrechtliche Fragestellungen zwischen den Fachbereichen der teilnehmenden Ministerien sowie der Staatskanzlei und den jeweiligen Referaten des UDZ erörtert werden. Die gefundenen Lösungen fanden Eingang in Formulare und Merkblätter (etwa im Bereich der Informationspflichten nach Art. 13 u. 14 DSGVO) und bilden die Grundlage für konkrete situationsbezogene Handlungsvorgaben (z. B. für Fotoaufnahmen im Rahmen öffentlicher Veranstaltungen).

2.2.3 Schulung der Videobeobachter der Polizei

Im März 2017 startete das Landespolizeipräsidium Saarland (LPP) das Projekt Videoüberwachung an kriminalitätsgefährdeten Orten in der Landeshauptstadt Saarbrücken[4].

Um die Bevölkerung an den sogenannten Kriminalitätsschwerpunkten bereits vor dem Eintritt einer tatsächlichen Gefahr effektiv schützen zu können, soll eine Videoüberwachungsmaßnahme in Form eines sog. Monitorings durchgeführt werden. Dies bedeutet, dass eine möglichst ständige Beobachtung der Geschehnisse an den festgelegten Überwachungsbereichen stattfindet. Um in Gefahrensituationen schnell reagieren zu kön-

[4] Vgl. 27. Tätigkeitsbericht, 2017/2018, Kap. 3.1, S. 40 f.

nen, ist Teil des Projektes auch die Einrichtung einer Videobeobachtungszentrale in der Führungs- und Lagezentrale beim LPP. Die Beobachtung dort soll von eigens hierfür geschulten Beobachtern durchgeführt werden.

Hierzu wurde unter der Federführung der Fachhochschule für Verwaltung des Saarlandes (FHSV) ein Ausbildungskonzept für die zukünftig als Videobeobachter eingesetzten Mitarbeiter erarbeitet. Um die mit einer Videoüberwachung in Zusammenhang stehenden datenschutzrechtlichen Aspekte zu vermitteln, wurde unsere Dienststelle gebeten, eine Mitarbeiterin für diesen Schulungszweck zu entsenden.

Wir sind dieser Bitte gerne nachgekommen und haben im Rahmen von zwei Schulungsblöcken eine jeweils vierstündige Unterrichtsveranstaltung durchgeführt.

Im ersten Teil wurde zunächst ein Überblick über das anwendbare Datenschutzrecht unter Berücksichtigung der speziellen Regelungen für den Polizeibereich gegeben. Sodann wurden Grundbegriffe des Datenschutzrechts erläutert. Darüber hinaus haben wir uns beispielsweise mit Auskunftsrechten betroffener Personen beschäftigt. Es wurde auch besprochen, wann der Umgang mit personenbezogenen Daten die Schwelle zur Ordnungswidrigkeit oder Straftat überschreitet und welche rechtlichen Konsequenzen dies nach sich ziehen kann.

Im zweiten Teil wurden die künftigen Videobeobachter anhand verschiedener Fallbeispiele im Umgang mit personenbezogenen Daten im Rahmen ihrer Tätigkeit in der Videobeobachtungszentrale sensibilisiert.

2.2.4 Schulung an der Verwaltungsschule

Im Bereich der Beschäftigtenausbildung an der Saarländischen Verwaltungsschule haben Mitarbeiter unserer Behörde die Vorbereitung und Durchführung der Unterrichtseinheiten im Bereich Datenschutzrecht übernommen. Ergänzend dazu erfolgte im Berichtszeitraum erstmals auch die Beschäftigtenausbildung der Mitarbeiter von Jobcentern hinsichtlich der speziellen Regelungen des Sozialdatenschutzes.

2.3 Zusammenarbeit mit anderen Aufsichtsbehörden

Um eine einheitliche Anwendung des Datenschutzrechts und damit einen einheitlichen Schutz der betroffenen Personen in ganz Europa zu erreichen, nimmt die Abstimmung unter den Datenschutzaufsichtsbehörden eine immer größere Rolle in der täglichen Arbeit ein. Neben einer zunehmenden Zahl von Sitzungen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) und der verschiedenen Arbeitsgremien der DSK erfolgen aufgrund kurzfristig zu beantwortender Fragen häufig auch telefonische Abstimmungen. Ein Ergebnis dieser intensiven Beratungen ist die große Zahl an Entschließungen, Beschlüssen, Orientierungshilfen und Anwendungshinweisen, die zu verschiedensten datenschutzpolitischen und datenschutzrechtlichen Themen verabschiedet und auf unserer Internetseite (www.datenschutz.saarland.de) sowie auf der offiziellen Internetseite der Datenschutzkonferenz (www.datenschutzkonferenz-online.de) zur Verfügung gestellt werden.

An der zu dem thematischen Schwerpunkt „Künstliche Intelligenz" der letztjährigen DSK eingerichteten Task Force beteiligte

sich auch unsere Dienststelle aktiv und konnte passend zu diesem Schwerpunktthema den Arbeitskreis Technik zu einer Sitzung nach Saarbrücken in das Deutsche Forschungszentrum für Künstliche Intelligenz (DFKI) einladen. Die Vorträge verschiedener Wissenschaftler und die anschließenden intensiven Diskussionen lieferten interessante Einblicke in die Tätigkeit des DFKI und brachten zudem hilfreiche Ansätze für die weitere Behandlung dieses Themenbereichs innerhalb der DSK.

Erstmals hat sich unsere Dienststelle im vergangenen Jahr an der datenschutzrechtlichen Bewertung von internen Datenschutzrichtlinien, sog. Binding Corporate Rules (BCR), großer europäischer Konzerne beteiligt. Durch solche BCR können Konzerne die Umsetzung eines angemessenen Datenschutzniveaus bei der konzerninternen Verarbeitung personenbezogener Daten in Drittstaaten nachweisen.

Wenn wir auch bislang noch nicht an den Arbeitsgremien des Europäischen Datenschutzausschusses, dem wichtigsten Gremium für die Zusammenarbeit aller europäischen Aufsichtsbehörden, aktiv teilnehmen können, nehmen dennoch die inhaltliche Begleitung der auf europäischer Ebene erörterten Themen sowie die Abstimmung bei grenzüberschreitenden Verfahren einen breiten Raum im Rahmen unser Tätigkeit ein.

2.4 Zusammenarbeit mit dem Landtag

Auch in dem vergangenen Berichtszeitraum haben wir in den Sitzungen des Unterausschusses für Datenschutz und Informationsfreiheit des Landtages zu verschiedenen aktuellen und grundsätzlichen Themen aus dem Bereich des Datenschutzes Stellung genommen und zugleich einen Überblick über die Arbeit unserer Dienststelle geben können.

Neben Stellungnahmen zu verschiedenen Gesetzgebungsvorhaben konnten wir zudem im Ausschuss für Inneres und Sport eine datenschutzrechtliche Bewertung zu den personengebundenen Hinweisen in polizeilichen Informationssystemen abgeben sowie in der Enquêtekommission „Digitalisierung im Saarland – Bestandsaufnahme, Chancen und Maßnahmen" im Rahmen einer Anhörung zu den datenschutzrechtlichen Anforderungen an eine erfolgreiche Etablierung von E-Government-Prozessen Stellung nehmen.

III.

Ausgewählte Beratungen

3 Ausgewählte Beratungen

3.1 Justizvollzugsdatenschutzgesetz

Das Europäische Parlament und der Rat der Europäischen Union haben am 27. April 2016 zwei Regelungswerke zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten erlassen:

Einerseits die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung [DSGVO]) und andererseits 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 sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates [JIRL]). Anders als die DSGVO bedarf die JIRL in den Mitgliedstaaten einer Umsetzung in nationales Recht.

Mit dem saarländischen Justizvollzugsdatenschutzgesetz (JVollzDSG) ist der Landesgesetzgeber seiner sich aus Art. 63 der Richtlinie ergebenden Umsetzungsverpflichtung für die Bereiche des Straf-, Jugendstraf- und Untersuchungshaftvollzugs sowie für den Bereich der Unterbringung in der Sicherungsverwahrung und den Bereich des Jugendarrests nachgekommen.

Durch das zuständige Ministerium für Justiz wurden wir bereits sehr frühzeitig zu den Referentenentwürfen angehört und

konnten so an vielen Stellen im Gesetzentwurf auf eine datenschutzfreundliche Umsetzung der europäischen Vorgaben hinwirken. Im parlamentarischen Verfahren konzentrierte sich unsere datenschutzrechtliche Bewertung des Gesetzentwurfs nur noch auf einzelne ausgesuchte Regelungsbereiche.

So hätten wir uns gewünscht, dass der Gesetzgeber die Konsolidierung der datenschutzrechtlichen Vorschriften im Justizvollzug zum Anlass nimmt, das Datenschutzrecht in diesem Bereich insgesamt zu modernisieren.

So entspricht es nicht mehr einem modernen datenschutzrechtlichen Ansatz, für jeden einzelnen Verarbeitungsschritt (Erhebung, Speicherung, Übermittlung) jeweils eine eigene Rechtfertigungsgrundlage zu normieren. Vielmehr bedarf es nach den Vorstellungen des europäischen Gesetzgebers dann einer gesetzlichen Rechtfertigung, wenn personenbezogene Daten verarbeitet (Art. 3 Nr. 2 JIRL) werden. Der hier maßgebliche Begriff der Verarbeitung ist umfassend und nicht „kleinteilig"; man betrachtet nicht mehr isoliert jeden Verarbeitungsschritt, sondern nimmt unter der Voraussetzung einer eindeutigen und legitimen Zweckfestlegung eine Gesamtbewertung des Verarbeitungsvorgangs vor. Denn für das Grundrecht auf Datenschutz wie es in Art. 8 der Charta der Grundrechte der Europäischen Union normiert ist, ist vor allem der konkrete Verarbeitungszweck/-kontext entscheidend, da dieser die Verarbeitung begrenzt, die Zugriffsmöglichkeiten beschränkt, die Transparenz für die betroffene Person sicherstellt und die Verwendungsdauer der Daten bestimmt.

Ein weiterer Kritikpunkt war, dass der Gesetzentwurf aus unserer Sicht nicht immer präzise zwischen dem Grundsatz der Zweckbindung (Art. 4 Abs. 1 lit. b JIRL) und den diesen Grundsatz

durchbrechenden Vorschriften auf der einen Seite und dem Prinzip der Rechtmäßigkeit der Verarbeitung (Art. 4 Abs. 1 lit a JIRL) auf der anderen Seite differenziert. Dies kann in der Folge zu erheblichen Auslegungsproblemen führen.

Für problematisch erachteten wir zudem die in § 4 Abs. 1 JVollzDSG vorgesehene Möglichkeit der Einwilligung als allgemeinen Erlaubnistatbestand. Die Regelung der Einwilligung als weitgehende Möglichkeit zur Legitimierung der Verarbeitung personenbezogener Daten in § 4 Abs. 1 JVollzDSG begegnet Bedenken im Hinblick auf ihre Vereinbarkeit mit der JIRL. Vorzugswürdig wäre es, die Einwilligung nicht als gleichrangige Legitimationsgrundlage zu regeln, sondern nur für spezifische Situationen.

Eine weitere normative Ausdifferenzierung und Konkretisierung sahen wir auch im Hinblick auf die Vorschriften zum Umgang mit besonderen Kategorien personenbezogener Daten für geboten. Hierbei handelt es sich um Informationen, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse und weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie genetische und biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder zur sexuellen Orientierung. Diese können gemeinhin als besonders sensibel angesehen werden. Bezüglich dieser Daten verlangt die JIRL nach unserem Dafürhalten eine Konkretisierung der einzelnen Situationen, in denen solche Kategorien von Daten verarbeitet werden dürfen. Kritisch sehen wir daher die in § 6 Abs. 2 JVollzDSG normierte Generalklausel zur Erhebung besonderer Kategorien personenbezogener Daten. Erwägungsgrund 37 verlangt, dass aufgrund der Risiken, die von der

Verarbeitung besonderer Kategorien personenbezogener Daten ausgehen, diese nur dann verarbeitet werden sollen, wenn hinreichende Garantien existieren und dies – hierauf kommt es an – „in durch Rechtsvorschriften geregelten Fällen erlaubt" ist. Mit dieser Konkretisierungspflicht ist eine Generalklausel nach dem Muster des § 6 Abs. 2 JVollzDSG aus unserer Sicht nicht vereinbar.

Das Gesetz wurde vom Landtag des Saarlandes in seiner Sitzung am 4. Dezember 2019 beschlossen.

3.2 Enquêtekommission „Digitalisierung im Saarland"

Bereits im Jahr 2018 hatte der Landtag des Saarlandes eine Enquêtekommission „Digitalisierung im Saarland" eingesetzt, welche die Auswirkungen der Digitalisierung auf das Saarland, die Chancen und Risiken infolge der technischen Entwicklungen sowie geeignete Fördermaßnahmen ermitteln soll.

Im Rahmen der Beratungen hatte die Enquêtekommission beschlossen, auch das Thema E-Government näher zu beleuchten. Hierzu wurde die Landesbeauftragte für Datenschutz eingeladen, zu bestimmten Leitfragen zum Thema E-Government Stellung zu nehmen.

Im Rahmen dieser Anhörung haben wir ausführlich dargelegt, weshalb ein starker Datenschutz ein zentrales Element für die erfolgreiche Etablierung von E-Government-Prozessen darstellt,

da hierdurch die Akzeptanz entsprechender Verfahren gefördert wird.[5]

3.3 Co-Prüfung in BCR-Verfahren

Bei grenzüberschreitenden Datenübermittlungen gelten zusätzlich zu den allgemeinen, bei allen Datenverarbeitungsprozessen einzuhaltenden datenschutzrechtlichen Vorgaben (sog. „erste Stufe"), besondere Zulässigkeitsregelungen (sog. „zweite Stufe"). Die in den Vorschriften der Art. 44 ff. Datenschutz-Grundverordnung (DSGVO) niedergelegten Rechtsgrundlagen sollen gewährleisten, dass internationale Verarbeitungsprozesse das in der Europäischen Union geltende Datenschutzniveau nicht untergraben (Art. 44 S. 2 DSGVO).

Hierzu muss beim Datenempfänger im Drittland aufgrund der dort geltenden innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen ein angemessenes Datenschutzniveau existieren, das „(…) *tatsächlich ein Schutzniveau der Freiheiten und Grundrechte gewährleistet* [wird], *das dem in der Union aufgrund der Richtlinie 95/46 im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist*"[6].

In der Praxis relevant sind insbesondere Durchführungsbeschlüsse der EU-Kommission, mit der sie das Datenschutzniveau in bestimmten Sektoren, Regionen oder ganzen Drittstaaten für mit dem Unionsrecht angemessen erklärt (Angemessenheitsbeschlüsse, Art. 45 DSGVO) und ebenfalls von der Kommission verabschiedete Vertragsklauselwerke, die zwischen einzelnen

[5] Elektronisch abrufbar unter: https://www.datenschutz.saarland.de/datenschutz/stellungnahmen

[6] EuGH, Urteil vom 6. Oktober 2015 - C-362/14, Rn. 73., juris.

Vertragspartnern internationale Datenübermittlungen absichern können (sog. Standardvertragsklauseln, Art. 46 Abs. 2 lit. c DSGVO).

Für international agierende Konzerne besteht zudem die Möglichkeit, zumindest konzerninterne Datenflüsse, also grenzüberschreitende Datenübermittlungen zwischen konzernangehörigen Unternehmen, mittels verbindlicher interner Datenschutzvorschriften (sog. Binding Corporate Rules; BCR) zu legitimieren (Art. 47 DSGVO). Im Kern handelt es sich dabei um von dem jeweiligen Konzern entwickelte Datenschutzrichtlinien die von in der EU ansässigen Konzernunternehmen für die Übermittlung personenbezogener Daten an außerhalb der EU gelegene Konzernunternehmen eingehalten werden. Diese Regeln müssen alle Datenschutzgrundsätze und für die Betroffenen durchsetzbare Rechte enthalten, um angemessene Schutzmaßnahmen für die Datenübertragung zu gewährleisten. Sie müssen gegenüber allen an der Datenverarbeitung beteiligten Konzernunternehmen und deren Mitarbeitern rechtlich verbindlich und durchsetzbar sein.

Möchten Konzerne ihre internen Datenflüsse auf der Grundlage von BCRs durchführen, müssen sie diese internen Regeln zuvor der zuständigen, federführenden Datenschutzaufsichtsbehörde zur Genehmigung vorlegen. Die Behörde genehmigt die BCRs gemäß dem in Artikel 63 der DSGVO festgelegten Konsistenzmechanismus. Die zuständige Behörde teilt hierzu ihren Entscheidungsentwurf nach einer Vorprüfung, die unter Beteiligung zweier Aufsichtsbehörden aus anderen Mitgliedstaaten erfolgt, dem Europäischen Datenschutzausschuss (EDSA) mit, der seine Stellungnahme zu den verbindlichen Unternehmensregeln abgeben wird. Wenn die BCRs gemäß der Stellungnahme

des EDSA fertiggestellt wurden, genehmigt die zuständige Behörde die BCRs. Inhaltlich wird im Genehmigungsverfahren geprüft, ob die vorgelegten BCR die Mindestanforderungen gemäß Art. 47 Abs. 2 DSGVO erfüllen.

Im Jahr 2019 wurden europaweit durch etwa 20 Konzerne BCR-Verfahren eingeleitet. Wir hatten im Berichtszeitraum in zwei Verfahren, die einmal unter schwedischer und einmal unter französischer Federführung betreut wurden, die Co-Prüfung der BCR übernommen.

IV.

Ausgewählte Sachverhalte

4 Ausgewählte Sachverhalte

4.1 Informationspflichten des Verantwortlichen

Mit Blick auf ihren Regelungszweck und der Schaffung und Erhaltung eines europaweit einheitlichen hohen Datenschutzniveaus, beschränkt sich die Datenschutz-Grundverordnung (DSGVO) nicht auf die bloße Aufstellung materiell-rechtlicher Vorgaben zum datenschutzkonformen Umgang mit personenbezogenen Daten. Zur Sicherung und effektiven Durchsetzung der diesbezüglichen Rechte und Pflichten enthält die Verordnung zudem subjektiv-prozedurale Rechte (sog. Betroffenenrechte), welche die betroffene Person in die Lage versetzen, in großem Umfang die Verarbeitung der sie betreffenden Daten eigeninitiativ zu bestimmen und eventuellen Datenschutzverstößen nachzugehen.

Kodifiziert sind die Betroffenenrechte in Kapitel III der DSGVO. Sie werden durch die Informationspflichten (Art. 12 - 14 DSGVO) eingeleitet. Die Informationspflichten sind wesentlicher Bestandteil und Ausgangspunkt aller Betroffenenrechte, bilden sie doch die Grundlage dafür, dass eine Person von einer sie betreffenden Datenverarbeitung Kenntnis erlangt und entsprechende Dispositionen treffen kann.

Informationsauslösendes Tatbestandsmerkmal der Art. 13 und 14 DSGVO ist die (Daten-)„Erhebung“. Dieser zentrale Begriff findet sich zwar als Unterfall der Datenverarbeitung in Art. 4 Nr. 2 DSGVO, eine Definition desselben enthält die Verordnung indes nicht, wodurch vielfach Unsicherheiten bestehen, in welchen Verarbeitungsstadien der Verantwortliche den Betroffenen zu informieren hat.

Ganz allgemein beschreibt das Erheben den Beginn eines Datenverarbeitungsprozesses. Es ist die Handlung, mit welcher der Verantwortliche erstmals ziel- und zweckgerichtet auf personenbezogene Daten zugreift, in der Absicht einer weiteren Verarbeitung dieser Daten. Dreh- und Angelpunkt der Frage, ob eine Erhebung von Daten vorliegt, ist demnach, ob der Datenbeschaffung ein Verarbeitungszweck zugrunde liegt.

Ist dies nicht der Fall, d. h. besteht bei dem Verantwortlichen keine Verarbeitungsabsicht hinsichtlich der in seine Verfügungsmacht gelangten Daten, kann nicht von einer Datenerhebung gesprochen werden. Gelangen die Daten unverlangt bzw. nicht aufgrund einer gesetzlichen Übermittlungsanordnung in die Verfügungsmacht des Verantwortlichen oder werden sie ihm gar „aufgedrängt", so wird man eine die Informationspflichten nach Art. 13 und 14 DSGVO auslösende Datenerhebung letztlich verneinen müssen. Werden beispielsweise personenbezogene Daten postalisch, telefonisch oder per E-Mail an den Verantwortlichen herangetragen und besteht keine Verarbeitungsabsicht auf Seiten des Verantwortlichen, so muss dieser die betroffene Person hierüber nicht informieren, hat die erlangten Daten jedoch unverzüglich zu löschen.

Eine Information kann auch unterbleiben, wenn der Verantwortliche sich bereits im Besitz der Daten befindet und mit diesen wiederkehrende oder gleichartige Verarbeitungen vornimmt. Bestehen zwischen Vertragsparteien etwa langjährige Geschäftsbeziehungen, so müssen diese sich in der Regel nicht bei jeder neuen geschäftlichen Datenverarbeitung über deren Modalitäten erneut informieren. Nur wenn sich wesentliche Aspekte der Datenverarbeitung ändern bzw. diese zu neuen geänderten Zwecken durchgeführt wird (Art. 13 Abs. 3 DSGVO), löst

dies eine erneute Informationspflicht aus, durch welche dem Betroffenen die diesbezüglichen Änderungen mitgeteilt werden müssen.

4.2 Auskunftsrecht der betroffenen Person

4.2.1 Grundlagen des Auskunftsanspruchs

Als ein die Informationspflichten nach Art. 13 f. Datenschutz-Grundverordnung (DSGVO) konkretisierendes Betroffenenrecht gibt Art. 15 DSGVO der betroffenen Person auf Verlangen ein umfassendes Auskunftsrecht gegenüber dem Verantwortlichen. Von Bedeutung ist dabei insbesondere die Auskunft über die Verarbeitungszwecke und Kategorien der verarbeiteten Daten (Art. 15 Abs. 1 lit. a und b), die Auskunft über eventuelle Empfänger bzw. Empfängerkategorien von Daten (Art. 15 Abs. 1 lit. c) sowie über die geplante Speicherdauer bzw. über die Kriterien, nach denen sich die Speicherdauer richtet (Art. 15 Abs. 1 lit. d).

Das Auskunftsverfahren richtet sich nach den allgemeinen in Art. 12 DSGVO enthaltenen Vorgaben. Ein diesbezüglicher Antrag durch die betroffene Person bedarf keiner besonderen Form, auch nicht inhaltlicher Art. Voraussetzung ist lediglich, dass das Auskunftsbegehren es dem Verantwortlichen ermöglicht, die Informationen aufzufinden, über welche er Auskunft erteilen soll. Mit welchem Aufwand dies für den Verantwortlichen verbunden ist, spielt in diesem Zusammenhang grundsätzlich keine Rolle. Erwägungsgrund 63 der DSGVO schafft für den Verantwortlichen zwar eine Verfahrenserleichterung dahingehend, dass er im Falle einer umfangreichen Datenverarbeitung verlangen kann, dass die betroffene Person präzisiert, auf welche Informationen oder welche Verarbeitungsvorgänge sich ihr

Auskunftsersuchen bezieht. Kann die betroffene Person dies jedoch nicht, so liegt es gleichwohl in der Pflicht des Verantwortlichen, den erforderlichen Verwaltungsaufwand zu betreiben, um eine entsprechende Auskunft erteilen zu können.

4.2.2 Reichweite des Auskunftsanspruchs

Nicht selten gerät das Recht auf Auskunft in Konflikt mit den datenschutzrechtlichen Positionen anderer Personen, mit Geschäftsgeheimnissen bzw. mit den spezialgesetzlich geregelten Rechten auf Akteneinsicht, etwa im Rahmen eines Verwaltungsverfahrens gemäß § 29 Saarländisches Verwaltungsverfahrensgesetz (SVwVfG). Wesentlich ist demnach die Frage nach der Reichweite des Rechts auf Auskunft, d. h. welche Dokumente die betroffene Person, in welcher Form von dem Verantwortlichen hierüber herausverlangen kann.

Was die Reichweite des Auskunftsanspruchs nach Art. 15 DSGVO anbelangt, so besteht nach wie vor eine große Rechtsunsicherheit, welche nach hiesiger Auffassung letztlich nur durch eine normative Klarstellung des europäischen Gesetzgebers gelöst werden kann.

Den wesentlichen Grund für diese Rechtsunsicherheit bildet das bis dato noch nicht abschließend geklärte Zusammenspiel von Art. 15 Abs. 1 DSGVO, dem eigentlichen „Recht auf Auskunft", und Art. 15 Abs. 3 DSGVO, dem sogenannten „Recht auf Kopie".

Gemäß Art. 15 Abs. 3 DSGVO stellt der Verantwortliche dem Betroffenen *„(...) eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung*". Die hiernach herauszugebenden Kopien sind grundsätzlich kostenlos und auf Antrag der betroffenen Person in einem gängigen

elektronischen Format herauszugeben (Art. 15 Abs. 3 S. 2 und 3).

Das Unabhängige Datenschutzzentrum Saarland vertritt in diesem Zusammenhang die Rechtsansicht, dass es sich bei Art. 15 Abs. 1 und Art. 15 Abs. 3 DSGVO nicht um zwei selbstständige und voneinander unabhängige datenschutzrechtliche Anspruchsgrundlagen handelt, sondern vielmehr um ein einheitliches Recht auf Auskunft. Art. 15 Abs. 1 DSGVO statuiert dieses Auskunftsrecht, dessen Modalitäten sodann durch Art. 15 Abs. 3 DSGVO präzisiert werden.

Vertritt man die Gegenauffassung zweier getrennter Anspruchsgrundlagen,[7] so muss auch hiernach konstatiert werden, dass diese dogmatische Einordnung an der Reichweite des Auskunftsanspruchs nichts ändert. Zwar mag man dem Wortlaut von Art. 15 Abs. 3 DSGVO vielleicht auf den ersten Blick entnehmen, dass mit einer „*Kopie der personenbezogenen Daten*" auch eine Ablichtung der jeweiligen Schriftstücke, bis hin zu gesamten Akteninhalten, einhergeht; mit anderen Worten der Verantwortliche eine Ablichtung oder digitale Kopie sämtlicher Informationen schuldet, welche in irgendeiner Art und Weise mit der betroffenen Person in Bezug gebracht werden können, ungeachtet der Frage wie eng dieser Bezug ist.

Bei näherer Betrachtung gilt diese Feststellung jedoch bereits im Rahmen von Art. 15 Abs. 1 DSGVO. Art. 15 Abs. 1 DSGVO beschränkt sich gerade nicht auf die in Buchstabe a) bis h) aufgelisteten Metadaten einer Verarbeitung, sondern bezieht sich daneben auch und gerade auf die personenbezogenen Daten

[7] Vgl. LAG Baden-Württemberg, Urteil vom 20. Dezember 2018 – 17 Sa 11/18, Rn. 196, 203, juris.

selbst; „(…) *Recht auf Auskunft über diese personenbezogenen Daten* ***und*** *auf folgende* [in lit. a-h aufgelisteten] *Informationen"*.

Für die Beantwortung der Frage nach der Reichweite des Auskunftsanspruchs, mithin der Frage was der Verantwortliche der betroffenen Person genau schuldet, ist die dogmatische Einordnung von Art. 15 Abs. 1 DSGVO und Art. 15 Abs. 3 DSGVO folglich von geringer Relevanz. Beide Normen sind bezüglich ihres Bezugsobjekts und des Umfangs der zu beauskunftenden Daten gleichlaufend.

Die potentielle Reichweite des Auskunftsanspruchs sowie des Rechts auf Kopie hat sich demnach anhand anderer Kriterien zu ermitteln.

Nach dem strengen Wortlaut von Art. 15 Abs. 1 DSGVO ist diese Reichweite jedenfalls sehr groß. „Personenbezogene Daten" sind nach der Legaldefinition in Art. 4 Nr. 1 DSGVO „(…) *alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen*". Erfasst von dem Recht auf Auskunft sind demnach nicht nur personenbezogene „Kerndaten" wie Vor- und Zuname, Geburtsdatum und -ort sowie die Wohnanschrift. Auch Sachdaten, welche für sich genommen noch keinen direkten Personenbezug zulassen, werden durch die Verknüpfung mit personenbezogenen Kerndaten zu „personenbezogenen Daten".

Das Unabhängige Datenschutzzentrum Saarland wendet sich jedoch gegen eine sich ausschließlich an dem Wortlaut der Vorschrift orientierende Rechtsansicht, welche als Konsequenz hie-

raus die Pflicht zu einer kostenlosen Übersendung des gesamten Akteninhalts bzw. des vollständigen Inhalts von Geschäftsunterlagen zieht.

Sinn und Zweck des Auskunftsrechts nach Art. 15 DSGVO ist die Kontrollfunktion in Bezug auf die Datenverarbeitung. Der Betroffene soll die Rechtmäßigkeit der Datenverarbeitung nachprüfen können. Hierbei geht es ausschließlich um die Kontrolle der Richtigkeit der Daten und die Legitimität der Verarbeitung. Das Auskunftsrecht will demgegenüber gerade nicht bezwecken, dass der Betroffene durch eine vollständige Kopie (für die betroffene Person) die Rechtmäßigkeit des behördlichen Entscheidungsvorgangs (die Subsumtion in der Sache) kontrollieren kann bzw. auf diesem Wege in den Besitz der vollständigen Geschäftsunterlagen seines Vertragspartners gelangen soll. Hierfür sind die bereichsspezifischen Akteneinsichtsrechte lex specialis, welche sodann auch entsprechende Einschränkungen und Kostenregelungen (Gebühren) vorsehen.

4.3 Auftragsverarbeitung, alleinige und gemeinsame Verantwortlichkeit – Abgrenzung

Der Begriff des Auftragsverarbeiters ist in Art. 4 Nr. 8 Datenschutz-Grundverordnung (DSGVO) definiert als eine Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Weil diese Definition wenig aussagekräftig ist, gibt es nach wie vor eine große Rechtsunsicherheit bei der Abgrenzung der Auftragsverarbeitung zu anderen Rollen bei der Verarbeitung personenbezogener Daten, wie die alleinige oder gemeinsame Verantwortlichkeit. Daher treten datenverarbeitende Stellen regel-

mäßig an die Aufsichtsbehörde mit der Bitte um Einordnung ihrer Tätigkeit heran. Auch unter den Aufsichtsbehörden wird diskutiert, unter welchen Voraussetzungen von einer Auftragsverarbeitung auszugehen ist.

Die zentrale Frage ist dabei, welche Entscheidungsspielräume ein Auftragsverarbeiter haben kann. Hierbei ist einerseits Art. 29 DSGVO von Bedeutung, der die Weisungsgebundenheit des Auftragsverarbeiters bestimmt, andererseits ist Art. 4 Nr. 7 DSGVO zu beachten, der den Verantwortlichen als eine Stelle beschreibt, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmt.

Typischerweise liegt bei der Auftragsverarbeitung ein arbeitsteiliges Handeln zwischen den Beteiligten vor, in dem ein Verantwortlicher eine andere Stelle mit der Durchführung bestimmter Verarbeitungsvorgänge beauftragt, wobei die beauftragte Stelle diese Verarbeitung im Interesse des Verantwortlichen vornimmt, ohne ein eigenes Verarbeitungsinteresse zu haben, das über die Erfüllung der Verpflichtungen gegenüber dem Verantwortlichen hinausgeht.

Zu Abgrenzungsschwierigkeiten kommt es regelmäßig dann, wenn die eingebundene Stelle auch ein über die Vertragserfüllung hinausgehendes eigenes Interesse an der Datenverarbeitung hat oder wenn ihr bestimmte Entscheidungsspielräume eingeräumt sind. Sodann stellt sich die Frage, wie hoch die Anforderungen an den Grad der Mitwirkung im Hinblick auf die Entscheidung über die Zwecke und Mittel der Datenverarbeitung sind, um von einer eigenverantwortlichen Datenverarbeitung auszugehen.

Die Artikel-29-Gruppe, das Vorgängergremium des Europäischen Datenschutzausschusses, hat in diesem Zusammenhang bereits in ihrer Stellungnahme 1/2010 (Working Paper 169) klargestellt, dass die Auftragsverarbeitung auch Fälle umfassen kann, in denen dem Verarbeiter Entscheidungsspielräume hinsichtlich technisch-organisatorischer Fragen eingeräumt werden und es für die Bestimmung der Verantwortlichkeit vor allem auf die Entscheidungsbefugnis hinsichtlich des Zwecks der Verarbeitung ankommt[8].

Von Bedeutung ist in diesem Zusammenhang auch die Entscheidung des EuGH vom 5. Juni 2018 (Rs. C-210/16), wonach der Betreiber einer Facebook-Fanpage gemeinsam mit Facebook für die Datenverarbeitung verantwortlich ist. Der EuGH legt in dieser Entscheidung eine vergleichsweise niedrige Schwelle zur eigenverantwortlichen Datenverarbeitung an, welche bereits dann vorliegen soll, wenn eine natürliche oder juristische Person aus Eigeninteresse Einfluss auf die Verarbeitung personenbezogener Daten nimmt. Dabei wird nicht vorausgesetzt, dass bei mehreren gemeinsam Verantwortlichen jeder für dieselbe Verarbeitung Zugang zu den betreffenden personenbezogenen Daten hat, sondern es genügt insoweit eine Beteiligung an der Entscheidung über die Zwecke und Mittel der Verarbeitung. Der EuGH geht dabei davon aus, dass die Beteiligung nicht gleichmäßig verteilt sein muss und beispielsweise auch allein in der Ermöglichung der Datenverarbeitung bestehen kann.

Auch wenn vor diesem Hintergrund einiges dafür spricht, dass nunmehr sehr häufig von einer eigenen Verantwortlichkeit einer

[8] Working Paper 169/Stellungnahme 1/2010 der Art. 29 Gruppe vom 16. Februar 2010, S. 17 ff., elektronisch abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf

datenverarbeitenden Stelle auszugehen ist, bleibt die Abgrenzung zur Auftragsverarbeitung im Einzelfall schwierig. Dabei ist sehr genau zu prüfen, welche Stelle welche Entscheidungsbefugnisse hat und worauf sich diese beziehen, um hieran anknüpfend eine den aufgestellten Grundsätzen entsprechende Abgrenzung vornehmen zu können.

Auch die Abgrenzung zwischen allein Verantwortlichen und gemeinsam Verantwortlichen ist nicht immer eindeutig vorzunehmen.

Hier bringt das Urteil des Europäischen Gerichtshofes (EuGH) vom 29. Juli 2019 (Rs. C-40/17 „Fashion ID") etwas Licht ins Dunkel, indem klargestellt wird, dass eine gemeinsame Verantwortlichkeit auch hinsichtlich einzelner Verarbeitungsvorgänge vorliegen kann, während hinsichtlich anderer, neben- vor- oder nachgelagerter Vorgänge, auch eine alleinige Verantwortlichkeit bestehen kann. Mithin stellt der EuGH klar, dass jeder Mitverantwortliche sich auf ein eigenes berechtigtes Interesse (bzw. eine eigene Rechtsgrundlage) für die gemeinsam verantworteten Verarbeitungsvorgänge – auch für Datentransfers unter den Verantwortlichen – stützen können muss.

Die Entscheidung wirft aber auch Fragen auf. So werden in dem zu Grunde liegenden Fall unterschiedliche Zwecke der Verantwortlichen festgestellt. Dem EuGH genügte für die Annahme eines gemeinsamen Zwecks – und infolgedessen einer gemeinsamen Verantwortlichkeit für bestimmte Verarbeitungsvorgänge – jedoch bereits die Tatsache, dass die Beteiligten jeweils vergleichbare wirtschaftliche Interessen verfolgen, die sich gegenseitig bedingen.

Es bleibt danach zu prüfen, inwiefern nunmehr jeder auf einer übergeordneten Ebene bestehende gemeinsame Zweck eine gemeinsame Verantwortlichkeit zu begründen vermag.

Fazit/Empfehlung:

Die für die Zuweisung datenschutzrechtlicher Verantwortlichkeit maßgeblichen Kriterien wurden vom EuGH konkretisiert. Die verbleibenden Auslegungsspielräume bedingen jedoch nach wie vor eine gewisse Rechtsunsicherheit.

4.4 Meldungen von Datenpannen

Seit dem Wirksamwerden der Datenschutz-Grundverordnung (DSGVO) ist die Zahl der Meldungen von Datenschutzverletzungen an die Aufsichtsbehörden stark angestiegen. Dies liegt insbesondere an der Ausweitung der meldepflichtigen Tatbestände im Vergleich zur früheren Regelung des Bundesdatenschutzgesetzes (BDSG), darüber hinaus aber auch an einem stärkeren Bewusstsein für datenschutzrechtliche Sachverhalte.

Eine „Datenpanne" liegt nunmehr insbesondere dann vor, wenn Unberechtigte Zugriff auf personenbezogene Daten erhalten haben oder diese zur Kenntnis nehmen konnten. Aber auch der Verlust von Daten, beispielsweise durch versehentliches Löschen oder den Verlust der Zugriffsmöglichkeit, ist als Datenschutzverletzung anzusehen, die eine Meldepflicht auslösen kann.

Art. 33 Abs. 1 DSGVO sieht im Falle einer Verletzung des Schutzes personenbezogener Daten vor, dass der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm

die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde meldet, es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen. Die verantwortliche Stelle muss also nach Bekanntwerden des Vorfalls abwägen, welche Folgen sich aus der Datenschutzverletzung für die betroffene Person ergeben können.

Hierbei spielt es unter anderem eine Rolle, welche Daten von der Verletzung betroffen sind. So ist regelmäßig vom Vorliegen eines Risikos auszugehen, wenn Daten tangiert sind, die zu den besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO zählen.

Als Frist für die Meldung an die Aufsichtsbehörde sieht Art. 33 Abs. 1 DSGVO regelmäßig einen Zeitraum von 72 Stunden vor. Im Falle einer Verzögerung ist diese gegenüber der Aufsichtsbehörde zu begründen. Die Frist beginnt mit dem Bekanntwerden der Datenschutzverletzung, also regelmäßig nach positiver Kenntnisnahme der Datenschutzverletzung durch den Verantwortlichen. Handelt es sich bei dem Verantwortlichen um eine juristische Person, sind für den Zeitpunkt der Kenntnisnahme die allgemeinen Grundsätze der Wissenszurechnung im Unternehmen anzuwenden. Der verantwortlichen Stelle ist demnach die Kenntnis desjenigen Mitarbeiters zuzurechnen, der nach der internen Organisation für die Verarbeitung personenbezogener Daten verantwortlich ist oder von dem dies aufgrund seiner Stellung erwartet werden kann. Die Frist läuft auch an einem Samstag, Sonntag oder Feiertag weiter. Endet die Frist an einem Samstag, Sonntag oder Feiertag, verlängert sie sich auch nicht bis zum nächsten Arbeitstag.

Gerade im Hinblick auf die Einhaltung der Meldefrist muss der Verantwortliche Regelungen treffen, wie bei Bekanntwerden einer Datenpanne zu verfahren ist. Mitarbeiter sind dafür zu sensibilisieren, wann eine Datenschutzverletzung vorliegt oder vorliegen kann, und sie müssen wissen, an welche Stelle sie die bekannt gewordenen Informationen zur Beurteilung, ob ein meldepflichtiger Vorfall gegeben ist, weiterleiten sollen. Hat der Verantwortliche einen Datenschutzbeauftragten benannt, kann diesem die Aufgabe übertragen werden, Datenschutzverletzungen zu bewerten und ggf. die Meldung an die Aufsichtsbehörde vorzunehmen.

Verantwortliche mit Sitz im Saarland haben die Möglichkeit, Datenpannen über ein Online-Formular zu melden, welches auf der Internetseite des Unabhängigen Datenschutzzentrums Saarland vorgehalten wird.[9]

Das Unabhängige Datenschutzzentrum Saarland erfasst alle eingehenden Meldungen und ergreift regelmäßig weitergehende Maßnahmen zur datenschutzrechtlichen Bewertung des Sachverhalts. Die Bewertung umfasst insbesondere auch die Frage, ob neben der Meldung der Datenschutzverletzung an die Aufsichtsbehörde auch eine Benachrichtigung der betroffenen Person angezeigt ist. Hierzu ist die verantwortliche Stelle nach Art. 34 Abs. 1 DSGVO verpflichtet, wenn die Datenpanne voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Ob ein hohes Risiko vorliegt, ist anhand des konkreten Sachverhalts zu beurteilen. Auf Grund

[9] Elektronisch abrufbar unter: https://www.datenschutz.saarland.de/online-services/datenpanne-melden-fuer-verantwortliche/

der Sensibilität der verarbeiteten Daten empfiehlt sich zumindest bei besonderen Kategorien personenbezogener Daten i.S.d. Art. 9 DSGVO regelmäßig eine Benachrichtigung durch die verantwortliche Stelle.

Verhältnismäßig viele Meldungen von Datenschutzverletzungen, die dem Unabhängigen Datenschutzzentrum Saarland seit Mai 2018 gemeldet wurden, stammen aus dem Gesundheitssektor und dem Bereich Kreditwirtschaft.

Dies lässt sich für den Gesundheitsbereich dadurch erklären, dass Gesundheitsdaten unter Art. 9 Abs. 1 DSGVO fallen und daher in diesem Kontext regelmäßig von einem Risiko und damit von einer Meldepflicht auszugehen ist, vor allem dann, wenn Unberechtigte Kenntnis von den sensiblen Daten erhalten haben.

Bei den verantwortlichen Stellen aus dem Gesundheitssektor, die Datenpannen melden, handelt es sich vor allem um Arztpraxen, Krankenhäuser und Abrechnungsunternehmen. Die häufigste Panne stellt dabei die Fehlversendung per Post dar, wobei zum Teil menschliche, zum Teil technische Fehler als Ursache hierfür zu nennen sind. Wo Unterlagen manuell für den Postversand vorbereitet werden, lassen sich menschliche Fehler (z. B. beim Kuvertieren) nicht vollkommen ausschließen. Der Verantwortliche muss jedoch geeignete technische und organisatorische Maßnahmen treffen, um den Versand so sicher und fehlerfrei wie möglich zu gestalten. Dazu gehört vor allem, die Mitarbeiter immer wieder für den sorgsamen Umgang mit Daten von Patienten zu sensibilisieren.

In der überwiegenden Zahl der gemeldeten Datenpannen aus dem Gesundheitsbereich sind die Verantwortlichen zutreffend

von einem hohen Risiko für die Betroffenen ausgegangen und haben dementsprechend die betroffenen Personen informiert.

Im Falle von Kreditinstituten handelt es sich bei Meldungen nach Art. 33 DSGVO ebenfalls überwiegend um postalische Fehlversendungen, beispielsweise von Kontoauszügen. Zwar gehören Daten wie die Bankverbindung selbst nicht zu den in Art. 9 Abs. 1 DSGVO genannten Datenkategorien. Kontoauszüge können jedoch Angaben enthalten, die Rückschlüsse auf besondere Kategorien von Daten zulassen. Darüber hinaus begründet die Offenlegung von Kontodaten gegenüber Unberechtigten eine nicht unerhebliche Missbrauchsgefahr, so dass regelmäßig von einer Meldepflicht auszugehen sein wird. Ob ein hohes Risiko vorliegt und auch eine Benachrichtigung der betroffenen Person erforderlich ist, muss im Einzelfall entschieden werden.

Fazit/ Empfehlung:

Datenpannen, bei denen besonders sensible Daten betroffen sind, verpflichten nicht nur zur Meldung an die Aufsichtsbehörde. Regelmäßig ist auch eine Benachrichtigung der betroffenen Person erforderlich.

4.5 Datenschutz-Folgeabschätzung (DSFA)

Mit einer Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 Datenschutz-Grundverordnung (DSGVO) wird die Verarbeitung personenbezogener Daten in einem folgenabschätzungspflichtigen Verarbeitungsvorgang beschrieben und bewertet. Dabei müssen insbesondere die Risiken für die Rechte und Freiheiten

natürlicher Personen, die durch den Verarbeitungsvorgang auftreten, bewertet und durch geeignete Gegenmaßnahmen ausreichend eingedämmt werden.

Der Verantwortliche für den jeweiligen Verarbeitungsvorgang kann damit nachweisen, dass er geeignete Maßnahmen ausgewählt hat, so dass eine regelungskonforme Verarbeitung möglich ist.

Eine DSFA bezieht sich auf die verarbeiteten Daten, die verwendete Hard- und Software ("System") und die eingesetzten Prozesse eines konkreten Verarbeitungsvorgangs. Für mehrere ähnliche Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige DSFA durchgeführt werden ("kumulierte DSFA", siehe Art. 35 Abs. 1 S. 2 DSGVO).

Die Methode zur Erstellung einer DSFA kann von dem Verantwortlichen frei gewählt werden. Es muss aber sichergestellt werden, dass alle gesetzlichen Mindestanforderungen erfüllt werden. Insbesondere müssen einerseits die Bedrohungen und Risiken für die personenbezogenen Daten und andererseits risikominimierende oder -verhindernde Maßnahmen in einer DSFA dargestellt werden. Hierzu empfiehlt sich die Nutzung einer strukturierten Vorgehensweise, die von den nachstehenden DSFA-Methoden unterstützt wird:

- das "Standard-Datenschutzmodell (SDM)"[10] der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder,

[10] Elektronisch abrufbar unter: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode.pdf

- die "Privacy Impact Assessment (PIA)"[11] der französischen Datenschutzaufsichtsbehörde Commission nationale de l'informatique et des libertés (CNIL).

Mit Hilfe des SDM kann die elektronische Verarbeitung personenbezogener Daten dahingehend geprüft werden, ob sie auf einer ausreichenden Rechtsgrundlage erfolgt (Art. 5 DSGVO). Ferner unterstützt das SDM die Prüfung, ob die personenbezogenen Daten durch eine angemessene Auswahl an technisch-organisatorischen Maßnahmen so verarbeitet werden, dass die Rechte der Betroffenen gewahrt bleiben.

Die Methodik der CNIL unterstützt den Verantwortlichen mit einer umfangreichen Dokumentation und einer Software (PIA-Tool), so dass die Erstellung einer DSFA vollständig in der Software durchgeführt und dokumentiert werden kann.

Art. 35 DSGVO verpflichtet den Verantwortlichen, eine DSFA unter bestimmten Bedingungen durchzuführen. Ändern sich die Risiken im Hinblick auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung, so ist es bei Vorliegen der gesetzlichen Voraussetzungen grundsätzlich erforderlich, eine DSFA auch bei bereits laufenden Verfahren erneut durchzuführen. Eine DSFA kann somit als Bestandteil eines ganzheitlichen Datenschutzmanagementsystems verstanden werden und ist somit als kontinuierlicher Prozess zu etablieren.

4.6 Akkreditierung und Zertifizierung

Mit der europäischen Datenschutz-Grundverordnung (DSGVO) müssen die in der Verordnung enthaltenen Bestimmungen zum

[11] Elektronisch abrufbar unter: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

Datenschutz nunmehr verbindlich in allen Mitgliedstaaten angewendet werden. Eine Möglichkeit den Nachweis zu führen, dass eine Verarbeitung den Vorgaben der DSGVO entspricht, stellt die erfolgreiche Durchführung eines datenschutzspezifischen Zertifizierungsverfahrens dar.

Deutsche Zertifizierungsstellen müssen im Sinne des § 39 Bundesdatenschutzgesetz (BDSG) einen Akkreditierungsprozess durchlaufen. Dieser Prozess wird von der Deutschen Akkreditierungsstelle (DAkkS) in Kooperation mit den Datenschutzaufsichtsbehörden durchgeführt.

Diese Prüfung beinhaltet einen formellen und einen materiellen Teil. Die formellen Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DSGVO basieren auf der internationalen Norm DIN EN ISO/IEC 17065. Sind diese erfüllt, schließt sich eine materielle Prüfung an. Bei dieser Prüfung bedient sich die DAkkS der Fachexpertise der deutschen Datenschutzaufsichtsbehörden. Diese Kooperation ist als öffentlich-rechtliche Vertragsbeziehung im Sinne der §§ 54 ff. VwVfG einzustufen.

Aus diesem Grund wird derzeit im Arbeitskreis "Zertifizierung" der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) eine Kooperationsvereinbarung zwischen den deutschen Datenschutzaufsichtsbehörden und der Deutschen Akkreditierungsstelle (DAkkS) GmbH erstellt, um die Akkreditierungsaufgaben nach Art. 42, 43, 58 DSGVO, § 39 BDSG und § 2 Abs. 3 Akkreditierungsstellengesetz (AkkStelleG) zu regeln.

Der für Frühjahr 2020 geplante Abschluss dieser Verwaltungsvereinbarung fundamentiert die Kooperation zwischen der

DAkkS und den deutschen Aufsichtsbehörden. Die von den Aufsichtsbehörden abgestimmten Akkreditierungskriterien werden dann dem Europäischen Datenschutzausschuss (EDSA) zur Stellungnahme vorgelegt; im Anschluss daran können Zertifizierungsstellen Anträge zur Programmprüfung einreichen. Nach Durchlaufen eines mehrstufigen Akkreditierungsprozesses können dann die Zertifizierungsstellen Produkte, Prozesse und Dienstleistungen im Rahmen eines Audits prüfen und im Falle eines erfolgreichen Ergebnisses ein entsprechendes Zertifikat ausgeben.

4.7 Aktuelle Rechtsprechung im Bereich der Telemedien

Im Bereich der Telemedien wurde das Datenschutzrecht im Berichtszeitraum besonders durch die Entscheidungen des Europäischen Gerichtshofes (EuGH) in Sachen „Fashion ID“[12] und „Planet49“[13] geprägt.

4.7.1 „Fashion ID“

Wie unter Kapitel 4.3 (Auftragsverarbeitung, alleinige und gemeinsame Verantwortlichkeit – Abgrenzung) bereits dargestellt, wurde in Sachen „Fashion ID“ durch den EuGH näher spezifiziert, in welchen Situationen von einer gemeinsamen datenschutzrechtlichen Verantwortlichkeit für einen bestimmten Verarbeitungsvorgang auszugehen ist.

Gegenstand des dortigen Verfahrens war die Einbindung eines „Gefällt mir“-Buttons von Facebook auf der Webseite eines Onlinehändlers. Dadurch, dass der Shopbetreiber diesen Drittinhalt

[12] EuGH, Urteil vom 29. Juli 2019 – C-40/17.

[13] EuGH, Urteil vom 1. Oktober 2019 – C-673/17.

von Facebook auf seiner Webseite einband, erhielt Facebook Informationen über die Besucher des Onlineshops, wie etwa deren IP-Adresse.

Daher war klärungsbedürftig, inwieweit der Shopbetreiber und Facebook für die mit der Einbindung des Buttons einhergehenden Verarbeitungsvorgänge datenschutzrechtlich verantwortlich sind. Denn eine Verantwortlichkeit hat zur Folge, dass für die Verarbeitungsvorgänge einerseits eine Rechtsgrundlage erforderlich ist, andererseits aber auch, dass diverse weitere datenschutzrechtliche Pflichten (z.B. Informationspflichten) zu erfüllen sind.

In seiner Entscheidung hat der EuGH klargestellt, dass eine Verantwortlichkeit eines Beteiligten dann vorliegt, wenn er auf die Verarbeitung „(…) *aus Eigeninteresse auf die Verarbeitung personenbezogener Daten Einfluss* [nehmen kann] *und damit an der Entscheidung über die Zwecke und Mittel dieser Verarbeitung mitwirkt* (…)*“.* [14] Dabei bestehe aber keine Verantwortlichkeit „(…) *für vor- oder nachgelagerte Vorgänge in der Verarbeitungskette, für die sie* [die Person des Verantwortlichen] *weder die Zwecke noch die Mittel festlegt* (…)*“.* [15]

Im gegebenen Fall hatte der EuGH folglich die Verantwortlichkeit des Shopbetreibers für die Erhebung und Übermittlung von Daten der Webseitenbesucher an Facebook durch das Einbinden des Buttons bejaht, weitergehende Verarbeitungen durch Facebook selbst jedoch nicht dem Verantwortungsbereich des Shopbetreibers zugeordnet.

[14] EuGH, Urteil vom 29. Juli 2019 – C-40/17, Rn. 68, juris.

[15] EuGH, Urteil vom 29. Juli 2019 – C-40/17, Rn. 74, juris.

Daher ist insbesondere im Bereich der Telemedien eine Bestimmung der jeweiligen Verantwortlichkeiten immer nur dann möglich, wenn im spezifischen Einzelfall je nach eingesetztem Drittdienst die diesem zugrundeliegenden technischen Abläufe und Einflussmöglichkeiten aller Beteiligten bekannt und geklärt sind. Hier ist der Webseitenbetreiber regelmäßig darauf angewiesen, dass der Diensteanbieter alle erforderlichen Informationen zur Verfügung stellt, die eine datenschutzrechtliche Beurteilung des Dienstes erst ermöglichen. Sind derartige Informationen nicht vorhanden, ist dem Webseitenbetreiber von einer Nutzung des Dienstes abzuraten.

Fazit/Empfehlung:

Drittinhalte sollten auf Webseiten nur eingebunden werden, sofern der Webseitenbetreiber über die für eine datenschutzrechtliche Beurteilung erforderlichen Informationen verfügt.

4.7.2 „Planet49"

In seinem Urteil im Verfahren „Planet49"[16] hat der EuGH nochmals klargestellt, dass, soweit für das Speichern von und den Zugriff auf Cookies in Nutzerendgeräten eine Einwilligung erforderlich ist, diese Einwilligung nur durch ein aktives Tun des Nutzers erteilt werden kann. Ein voreingestelltes Ankreuzkästchen in einem Onlineformular genüge dem regelmäßig nicht. Dies ergibt sich im Rahmen der Datenschutz-Grundverordnung

[16] EuGH, Urteil vom 1. Oktober 2019 – C-673/17.

(DSGVO) bereits aus der Legaldefinition des Begriffs der „Einwilligung" in Art. 4 Nr. 11 DSGVO, nach der eine *„unmissverständlich abgegebene Willensbekundung"* oder eine *„sonstige eindeutige bestätigende Handlung"* erforderlich ist. Erwägungsgrund 32 zur DSGVO legt sogar explizit dar, dass *„angekreuzte Kästchen oder die Untätigkeit einer Person"* keine Einwilligung darstellen. Insoweit war das Urteil aufgrund der recht eindeutigen Rechtslage unter der DSGVO wenig überraschend.

Von besonderer Bedeutung wird hingegen die dem Urteil des EuGH folgende – für Anfang 2020 erwartete – Entscheidung des Bundesgerichtshofes (BGH) in demselben Verfahren sein. Unter Berücksichtigung der Vorgaben des EuGH wird die Entscheidung des BGH voraussichtlich Klarheit im Hinblick auf die (Nicht-)Anwendbarkeit des § 15 Abs. 3 Telemediengesetz (TMG) unter Geltung der DSGVO bringen, und damit auch die Rechtssicherheit für alle Beteiligten im Bereich des Datenschutzes bei Telemedien fördern.

§ 15 Abs. 3 TMG sieht bisher vor, dass unter bestimmten Voraussetzungen Nutzerprofile – etwa von Besuchern einer Webseite – durch Diensteanbieter erstellt werden dürfen, sofern der Nutzer dem nicht widerspricht. Die Erstellung von Nutzungsprofilen erfolgt oftmals mittels Einsatz von Cookies. Das Speichern und der Abruf von Cookies in Nutzerendgeräten ist – abgesehen von einigen Ausnahmen – nach Art. 5 Abs. 3 ePrivacy-Richtlinie jedoch nur mit Einwilligung des Nutzers zulässig.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vertritt daher die Auffassung, dass mit § 15 Abs. 3 TMG die Vorgaben der

ePrivacy-Richtlinie nicht umgesetzt wurden und dieser wegen des – nun vom EuGH nochmals hervorgehobenen – Erfordernisses eines aktiven Tuns bei einer Einwilligung auch keiner richtlinienkonformen Auslegung zugänglich sein dürfte.[17] Solange also keine entsprechende Anpassung des TMG an die klaren Vorgaben an eine wirksame Einwilligung erfolgt, verbleibt für die Beurteilung der Rechtmäßigkeit des Erstellens von Nutzerprofilen mittels Cookies allein der Maßstab der DSGVO.

Fazit/Empfehlung:

Einwilligungen von Nutzern zum Einsatz von Cookies sind nur wirksam, wenn diese ihren Willen durch aktives Tun bekundet haben.

4.8 Orientierungshilfe Telemedien

Da sich der Rechtsanwender im Bereich des Datenschutzes in Telemedien – wie obige Rechtsprechung zeigt – einer Vielzahl juristisch komplexer Problemstellungen ausgesetzt sieht, hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) im Jahr 2019 eine „Orientierungshilfe für Anbieter von Telemedien" veröffentlicht, die insbesondere Webseitenbetreibern Hilfestellung bei der Umset-

[17] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien (Stand: März 2019), S. 4 ff., elektronisch abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf

zung der datenschutzrechtlichen Vorgaben geben soll. Die Orientierungshilfe ist auf dem Internetangebot sowohl des Unabhängigen Datenschutzzentrums Saarland als auch der DSK abrufbar.

4.9 ePrivacy-Verordnung

Die ePrivacy-Verordnung ist ein Gesetzgebungsvorhaben der EU, das ursprünglich zeitgleich mit der Datenschutz-Grundverordnung (DSGVO) in Geltung treten sollte. Sie soll die Regelungen der DSGVO konkretisieren und ergänzen indem sie für den Bereich der elektronischen Kommunikation spezifischere Vorgaben für den Datenschutz aufstellt. Sie wird damit voraussichtlich Regelungen enthalten, die nicht nur, aber insbesondere auch im Bereich der Telemedien von Bedeutung sein werden. Sie soll etwa Regelungen enthalten, aus denen sich ergibt, in welchem Umfang und zu welchen Zwecken das Verhalten von Internetnutzern ausgewertet bzw. nachverfolgt werden darf. Gerade im Bereich der Telemedien wäre hier eine Regelung wünschenswert, die den schutzwürdigen Interessen der Internetnutzer hinreichend Rechnung trägt.

Wie aber die endgültige Fassung der ePrivacy-Verordnung aussehen wird, ist derzeit wieder vollkommen offen. Bereits im Januar 2017 hatte die Kommission einen ersten Entwurf der Verordnung vorgelegt, zu dem sich auch das Europäische Parlament noch im Oktober 2017 positioniert hatte. Seitdem verhandeln die Mitgliedstaaten im Rat der Europäischen Union über ihre Position zur Verordnung – bisher aber ohne Endergebnis. Denn immer wieder kommt es dabei zu Kontroversen zu verschiedenen Regelungen des Verordnungsentwurfes.

Im November 2019 wurde noch damit gerechnet, dass sich der Rat der Europäischen Union bis Ende des Jahres auf eine eigene Position einigen würde. Auch der Ende 2019 von der finnischen Ratspräsidentschaft vorgelegte Kompromissvorschlag konnte jedoch keine Mehrheit unter den Mitgliedstaaten gewinnen. Der Fortgang des Gesetzgebungsverfahrens ist nicht absehbar. Laut einer Äußerung des seit 1. Dezember 2019 amtierenden EU-Kommissars für Binnenmarkt und Dienstleistungen erwägt die neue EU-Kommission sogar einen gänzlich neuen Entwurf zur ePrivacy-Verordnung auszuarbeiten. Bisher ist daher keine verlässliche Aussage darüber möglich, ab wann die ePrivacy-Verordnung gelten wird, und wie ihre Regelungen konkret ausgestaltet sein werden. Es steht jedoch zu befürchten, dass die verbraucher- und datenschutzfreundlicheren Entwürfe von Kommission und Parlament weiter zugunsten wirtschaftlicher Interessen aufgeweicht werden.

4.10 Analysedienste auf Webseiten

Mit Pressemitteilung vom 11. November 2019[18] hatte das Unabhängige Datenschutzzentrum Saarland (UDZ) darauf hingewiesen, dass eine Einbindung von Analysediensten von Drittanbietern auf Webseiten regelmäßig eine Einwilligung der Webseitenbesucher voraussetzt, wenn der Anbieter des jeweiligen Analysedienstes sich (vertraglich) vorbehält, die Daten der Webseitenbesucher auch zu eigenen Zwecken verwenden zu wollen. Denn einerseits liegt dies in der Regel außerhalb des vom Web-

[18] Elektronisch abrufbar unter: https://www.datenschutz.saarland.de/informationsfreiheit/aktuelles

seitenbesucher zu Erwartenden, zudem ist eine Freigabe der Daten für Drittzwecke für die beabsichtigte Analyse nicht erforderlich.

Webseitenbetreiber, die entsprechende Dienste einsetzen, müssen daher vor deren Einsatz überprüfen, ob bzw. unter welchen Voraussetzungen der Dienst diesen Anforderungen entspricht.

4.11 Microsoft Windows 10

Windows ist eines der meist genutzten Betriebssysteme. Seit der Veröffentlichung der neuesten Version Windows 10 häufen sich Fragen bzgl. des datenschutzkonformen Betriebs. Den Schwerpunkt der diesbezüglichen Fragestellungen bildet die Erfassung von sog. Telemetriedaten, die bei der Nutzung dieses Produkts anfallen, sowie deren Übertragung an Microsoft.

Für die Verarbeitung personenbezogener Daten müssen nach Art. 24 Datenschutz-Grundverordnung (DSGVO) geeignete technische und organisatorische Maßnahmen durch den Verantwortlichen umgesetzt werden, um sicherzustellen, dass die Verarbeitung datenschutzkonform erfolgt.

Aus diesem Grund ist es notwendig, dass für jede Verarbeitungstätigkeit unter Nutzung des Betriebssystems Windows 10 geprüft wird, welche personenbezogenen Daten in welchem Umfang verarbeitet werden und welche personenbezogenen Daten für welche Zwecke an Microsoft übermittelt werden. Daran anschließend ist zu prüfen, welche Rechtsgrundlage für die Übermittlung personenbezogener Daten an Microsoft vorhanden ist. Fehlt es an einer solchen, ist die Übermittlung datenschutzrechtlich nicht zulässig.

Für die Übertragung von bei der Nutzung von Windows 10 anfallenden Telemetriedaten an Microsoft konnte bis zum Ende des Berichtszeitraums nicht abschließend geklärt werden, welche Datenkategorien betroffen sind. Eine datenschutzrechtliche Bewertung war unter dieser Voraussetzung nicht möglich.[19] Vor diesem Hintergrund ist die Übertragung von Telemetriedaten durch angemessene (technisch-organisatorische) Maßnahmen zu verhindern. Dabei ist stets sicherzustellen, dass bereits durchgeführte Maßnahmen ihre Wirkung auch nach einem Update des Betriebssystems beibehalten und nicht durch dieses wieder unwirksam werden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) empfiehlt, dass beim Einsatz von Windows 10 für jede Verarbeitungstätigkeit unter Anwendung des Prüfschemas "SDM - Standarddatenschutzmodell Version 2.0" festgestellt wird, ob und welche personenbezogenen Daten an Microsoft übertragen werden und auf welcher Rechtsgrundlage eine Übermittlung datenschutzrechtlich zulässig ist. Verbleibt nach der Betrachtung ein Restrisiko, ist zu prüfen, ob dieses tragbar ist. Im Weiteren empfiehlt die DSK, dass bei allen IT-Projekten der Schutzbedarf nach dem SDM, dem BSI-Grundschutz oder vergleichbaren Normen festgestellt wird. Auf den Ergebnissen dieser Schutzbedarfsanalyse sind entsprechende Anforderungen zu definieren, die einen datenschutzrechtlichen Betrieb auf der Plattform von Windows 10 ermöglichen.

[19] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), Datenschutz bei Windows 10, S. 7, elektronisch abrufbar unter: https://www.datenschutzkonferenz-online.de/media/ah/20191106_win10_pruefschema_dsk.pdf

4.12 Nutzung von WhatsApp im Rahmen kommunaler Bürgerdienste

Die Kommunikationsgewohnheiten der Menschen verändern sich. Diese für den privaten Bereich allgemeingültige Feststellung kann in zunehmender Weise auch auf den öffentlichen Sektor übertragen werden. Zu Recht erwarten die Bürgerinnen und Bürger eine Anpassung des Staates an moderne Medien, vor allem in Bereichen der alltäglichen Leistungsverwaltung.

Verständlich ist in diesem Zusammenhang auch der Wunsch nach einem leichten Kommunikationszugang zu den einzelnen Verwaltungen, welcher sich unseren privaten Kommunikationsgewohnheiten angleicht.

Dass sich eine solche ungezwungene Form der mediengestützten Behördenkommunikation in einem Spannungsverhältnis zu datenschutzrechtlichen Erfordernissen befindet, verwundert nicht. Dies umso weniger aufgrund der Tatsache, dass moderne Messenger-Dienste wie WhatsApp und Facebook-Messenger primär den privaten Bereich im Fokus haben und nicht auf eine Kommunikation zwischen Bürgern und Behörde ausgerichtet sind.

Die Aufgabe einer Datenschutzbehörde besteht jedoch auch in diesem Bereich nicht darin, sich den Entwicklungen des digitalen Zeitalters entgegenzustellen. Sie ist vielmehr dazu berufen, das erwähnte Spannungsverhältnis zu lösen und die verantwortlichen Verwaltungen bei der Einrichtung von modernen Zugangsmöglichkeiten zu ihren Diensten zu unterstützen. In den meisten Fällen kann hierbei eine datenschutzkonforme Lösung gefunden werden.

Vor diesem Hintergrund unterzog unsere Behörde im Berichtzeitraum den behördlichen Einsatz des Messaging-Dienstes „WhatsApp“ im Rahmen kommunaler Bürgerdienste einer rechtlichen Bewertung.

4.12.1 Rahmenbedingungen „WhatsApp“

Bei WhatsApp handelt es sich um einen elektronischen Kommunikationsdienst der in Kalifornien ansässigen WhatsApp Inc. (einer Konzerntochter der Facebook Inc.), welcher sich primär an natürliche Personen richtet. Seit Anfang 2018 stellt die WhatsApp Inc. für die nicht-private Nutzung ein sog. WhatsApp-Business-Konto unter Nutzung der WhatsApp-Business-App zur Verfügung. Hierzu bedarf es der Einrichtung eines sog. „WhatsApp Unternehmens-Accounts“ und es gelten spezielle Nutzungsbedingungen.[20]

Die Verarbeitung personenbezogener Daten (Art. 4 Nr. 1 Datenschutz-Grundverordnung [DSGVO]) bedarf zwingend einer Rechtsgrundlage nach Art. 6 Abs. 1 lit. a - f DSGVO. Für die Einrichtung eines Bürgerdienstes in Form einer elektronischen Kommunikationsplattform zwischen Bürger und Kommune kommt als Rechtsgrundlage Art. 6 Abs. 1 lit. e, Abs. 3 lit. b DSGVO i. V. m. Art. 28 Abs. 2 GG , Art. 117 Abs. 3 SVerf in Betracht. Hiernach können die Gemeinden in Eigenverantwortung den Bereich der örtlichen Öffentlichkeitsarbeit ausgestalten, was grundsätzlich auch den Einsatz moderner Kommunikationsmedien – wie Social-Media-Dienste – umfasst.

[20] WhatsApp Business Nutzungsbedingungen (Stand: 15. Mai 2018), elektronisch abrufbar unter: https://www.whatsapp.com/legal/business-terms/

4.12.2 Verantwortlichkeit für die Datenverarbeitung/Unterscheidung in „Hin-“ und „Rückkanal“

Für die datenschutzrechtliche Bewertung des Einsatzes von WhatsApp im Rahmen kommunaler Bürgerdienste ist – neben der Erfüllung der allgemeinen datenschutzrechtlichen Anforderungen – entscheidend, in welchem Umfang die jeweilige Kommune für die Datenverarbeitung durch WhatsApp verantwortlich ist. In diesem Zusammenhang sind die unterschiedlichen Kommunikationsphasen getrennt voneinander zu bewerten, welche sich vor allem in einen „Hin-“ und einen „Rückkanal“ differenzieren lassen. Der „Hinkanal“ beschreibt die über WhatsApp erfolgende Kontaktaufnahme des Bürgers mit der jeweiligen Kommune während der „Rückkanal“ die hierauf bezogene Antwort der Kommune an den Bürger umfasst.

Von besonderer datenschutzrechtlicher Relevanz an der über WhatsApp geführten Kommunikation zwischen Bürger und Kommune ist vor allem der „Rückkanal“, mithin die Antwort von Seiten der Kommunalverwaltung auf eine aus der Bürgerschaft stammende Anfrage. Der „Hinkanal“ ist – obgleich datenschutzrechtlich nicht unproblematisch – hingegen nicht der Kommune (als Verantwortlicher nach Art. 4 Nr. 7 DSGVO) zurechenbar. Die bloße Eröffnung der Kommunikationsmöglichkeit über WhatsApp durch die Kommune begründet keine Verantwortlichkeit i. S. d. Art. 4 Nr. 7 DSGVO. Verantwortlicher ist hiernach, wer alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sowohl die Zwecke als auch die Mittel der über WhatsApp durchgeführten Verarbeitung werden ausschließlich durch die WhatsApp Inc. festgelegt. Hieran vermag auch der

Umstand nichts zu ändern, dass die Kommunen durch die Möglichkeit einer Kontaktaufnahme über WhatsApp einen Anreiz zur Nutzung des Dienstes setzen. WhatsApp ist vor diesem Hintergrund mit den Diensten eines Telekommunikations- bzw. Postunternehmens zu vergleichen und es steht den betroffenen Personen insofern frei, ihre personenbezogenen Daten über WhatsApp zu übermitteln und die diesbezüglichen Geschäftsbedingungen des Unternehmens zu akzeptieren.

4.12.3 Verantwortlichkeit für den „Rückkanal"/Unterscheidung in Inhalts- und Metadaten

Hinsichtlich der über den Rückkanal mittels WhatsApp übermittelten Daten ist eine Differenzierung hinsichtlich Inhalts- sowie Metadaten vorzunehmen. Inhaltsdaten betreffen den Aussagegehalt der Nachricht an sich, während Metadaten diejenigen Informationen umfassen, welche im Rahmen der technischen Abwicklung der Nachrichtenübersendung anfallen. Unter letztere Datenkategorie fallen beispielsweise die Kontaktdaten von Absender und Empfänger sowie die Zeitpunkte des Sendens und Empfangens der Nachricht.

Die Metadaten werden ausweislich der Allgemeinen Nutzungsbedingungen von WhatsApp gespeichert und ausgewertet.[21]

„Geräte- und Verbindungsdaten. Wenn du unsere Dienste installierst, nutzt oder auf sie zugreifst, erfassen wir geräte- und verbindungsspezifische Informationen. Dazu gehören auch Informationen zu deinem Hardware-Modell und Betriebssystem, Batteriestand, Signalstärke, App-Version, Informationen zum

[21] Die nachfolgend zitierten Passagen beziehen sich auf die rechtlichen Hinweise der WhatsApp Inc., elektronisch abrufbar unter: https://www.whatsapp.com/legal/#payments-in

Browser und Mobilfunknetz sowie zu der Verbindung, einschließlich Telefonnummer, Mobilfunk- oder Internetanbieter, Sprache und Zeitzone sowie IP-Adresse, Informationen zum Gerätebetrieb und Kennungen wie Gerätekennungen (einschließlich individueller IDs für Produkte der Facebook-Unternehmen, die mit demselben Gerät oder Account verknüpft sind).“

Die diesbezügliche Auswertung ist – soweit sie sich nicht für die Diensteerbringung als erforderlich erweist – aus datenschutzrechtlicher Sicht zwar bedenklich, jedoch fehlt es auch bei dieser Datenverarbeitung an einer Verantwortlichkeit der Kommune. Es liegt insbesondere keine gemeinsame Verantwortlichkeit der Kommune und WhatsApp gem. Art. 26 DSGVO vor.

Eine solche gemeinsame Verantwortlichkeit besteht dann, wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen. Zwar ist es im Rahmen einer gemeinsamen Verantwortlichkeit möglich, auch weitgehend eigene Verarbeitungszwecke zu verfolgen und es muss sich auch nicht notwendigerweise um eine gleichberechtigte Verarbeitung beider Kooperationspartner handeln.[22] Die reine Nutzung eines Social-Media-Dienstes führt jedoch noch nicht dazu, dass die Nutzer dieser Dienste Teil der Verarbeitung des Dienstbetreibers werden. Es muss vielmehr ein die Datenverarbeitungen verbindendes Element rechtlicher (vertraglicher) und/oder tatsächlicher Natur hinzutreten, welches die Datenverarbeitungen des Dienstbetreibers (WhatsApp) und des Nutzers (Kommune) miteinander verknüpft.

[22] *Petri*, in: Simitis/Hornung/Spiecker (1. Aufl. 2019), Art. 26 Rn. 14.

Mit Bezug auf die Rechtsprechung des Europäischen Gerichtshofes (EuGH) lassen sich bei der gemeinsamen Verantwortlichkeit dabei vor allem zwei Fallgruppen unterscheiden. So liegt eine gemeinsame Verantwortlichkeit zum einen in Konstellationen vor, in denen ein Verantwortlicher die Ziele eines anderen Verantwortlichen oder sogar ein gemeinsames übergeordnetes Interesse fördert, steuert oder organisiert (vgl. EuGH – „Zeugen Jehovas"[23]).

Die zweite – hier relevante – Fallgruppe sind die Konstellationen, in denen ein Verantwortlicher auf die Verarbeitung eines anderen Verantwortlichen einen steuernden Einfluss hat und von der Verarbeitung bzw. den Verarbeitungsergebnissen des anderen Verantwortlichen profitiert, d. h. einen Nutzen hieraus zieht. In der Entscheidung „FashionID" erkennt der EuGH den steuernden Einfluss darin, dass ein Webseitenbetreiber ein Social Plugin von Facebook in seine Webseite einbindet, das zu einer Erhebung und Übermittlung personenbezogener Daten der Besucher dieser Seite dient.[24] Der Webseitenbetreiber profitiert von dieser Verarbeitung dadurch, dass das Einbinden des Social Plugins es ihm ermöglicht, die Werbung für seine Produkte zu optimieren, indem diese im sozialen Netzwerk Facebook sichtbarer gemacht werden, um so „[…] *in den Genuss eines wirtschaftlichen Vorteils kommen zu können".*[25]

[23] Vgl. EuGH, Urteil vom 10. Juli 2018 – C-25/17 (Zeugen Jehovas).

[24] „Mit der Einbindung eines solchen Social Plugins in ihre Website hat Fashion ID im Übrigen entscheidend das Erheben und die Übermittlung von personenbezogenen Daten der Besucher dieser Seite zugunsten des Anbieters dieses Plug-Ins […] beeinflusst, die ohne Einbindung dieses Plug-Ins nicht erfolgen würden", EuGH, Urteil vom 29. Juli 2019 – C-40/17 (Fashion ID), Rn. 78, juris.

[25] EuGH, Urteil vom 29. Juli 2019 – C-40/17 (Fashion ID), Rn. 80, juris.

In der Entscheidung „Facebook Fanpages" stellt der EuGH fest, dass der Fanpage-Betreiber einen steuernden Einfluss auf die Datenverarbeitung durch Facebook dadurch hat, indem er die Seite einrichtet und so Facebook *„die Möglichkeit gibt, auf dem Computer* […] *der Person die seine Fanpage besucht hat, Cookies zu platzieren* […] *"*[26]. Mittels dieser Cookies wird es Facebook ermöglicht, die Seitenbesucher wiederzuerkennen und so demographische Daten über die Zielgruppe der Fanpage zu erfassen, die dem Seitenbetreiber sodann – nach vorheriger Parametrierung – zur Verfügung gestellt werden und es diesem ermöglichen, sein Informationsangebot so zielgerichtet wie möglich zu gestalten.

Hierauf Bezug nehmend stellt der EuGH fest, „[…] *dass der Betreiber einer auf Facebook unterhaltenen Fanpage durch die von ihm vorgenommene Parametrierung u. a. entsprechend seinem Zielpublikum sowie den Zielen der Steuerung oder Förderung seiner Tätigkeiten an der Entscheidung über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Besucher seiner Fanpage beteiligt ist"*.[27]

Anders als im Rahmen einer „Facebook Fanpage", besteht eine solche Auswertungs- und Parametrierungsmöglichkeit nach unseren Erkenntnissen im Rahmen einer Nutzung des Messaging-Dienstes WhatsApp nicht. Die bloße Nutzung von WhatsApp – und damit einhergehend eine u. U. kausale Mitverantwortlichkeit der Kommune für eine Verarbeitung von Daten der den

[26] Vgl. EuGH, Urteil vom 5. Juni 2018 – C- 210/16 (Facebook Fanpages), Rn. 35, juris.

[27] EuGH, Urteil vom 5. Juni 2018 – C- 210/16 (Facebook Fanpages), Rn. 39, juris.

Bürgerdienst nutzenden Personen durch WhatsApp – begründet demnach keine Verantwortlichkeit im datenschutzrechtlichen Sinne.

Die Verantwortlichkeit der Kommunen und sonstiger öffentlicher Stellen beim Einsatz von elektronischen Kommunikationsdiensten erstreckt sich jedoch darauf, einen in technisch-organisatorischer Hinsicht sicheren Übertragungsweg für die versendeten Nachrichten (Inhaltsdaten) anzubieten. Diese Voraussetzungen werden nach hiesiger Einschätzung von WhatsApp – in den jeweils aktuellen Versionen – derzeit erfüllt.

4.12.4 Hinreichende Verschlüsselung der Inhaltsdaten

So ist bei den Inhaltsdaten, sprich dem eigentlichen Kernbestandteil der Kommunikation zwischen der Kommune und der betroffenen Person, von einer hinreichend sicheren Übertragung auszugehen. Die Inhaltsdaten werden laut den Nutzungsbestimmungen der WhatsApp Inc. inhaltsverschlüsselt übertragen und in der Regel nicht auf unternehmenseigenen Servern zwischengespeichert.

Obgleich zumindest in gewissen Fällen eine zeitlich begrenzte Zwischenspeicherung durch das Unternehmen erfolgt, welche der Verantwortliche – soweit ersichtlich – nicht weiter beeinflussen kann,

„Sobald deine Nachrichten (einschließlich deiner Chats, Fotos, Videos, Sprachnachrichten, Dateien und Angaben zu „Standort teilen") zugestellt sind, werden sie von unseren Servern gelöscht. Deine Nachrichten werden auf deinem eigenen Gerät gespeichert. Wenn eine Nachricht nicht sofort zugestellt werden kann (zum Beispiel, wenn du offline bist), können wir sie für bis

zu 30 Tage auf unseren Servern behalten, während wir versuchen, sie zuzustellen. Wenn eine Nachricht nach 30 Tagen immer noch nicht zugestellt wurde, löschen wir sie."

bewirkt die von WhatsApp beschriebene Inhaltsverschlüsselung unseres Erachtens einen hinreichenden Schutz vor Zugriffen auf die derart zwischengespeicherten Inhaltsdaten, auch hinsichtlich etwaiger Zugriffsversuche durch das Unternehmen selbst.

Im Rahmen der gemäß Art. 24 Abs. 1 DSGVO i.V.m. den Erwägungsgründen 75 und 76 DSGVO vorzunehmenden Risikoanalyse ist es demnach gerechtfertigt, wenn die Kommune das von WhatsApp beschriebene Verschlüsselungsverfahren als wesentliches technisches Merkmal der Risikominimierung betrachtet. Dieses Verschlüsselungsverfahren wird durch das Unternehmen eingehend beschrieben und sieht ein asymmetrisches Kryptierungsverfahren vor, d. h. die Kommunikationsdaten werden vor dem Verlassen des Endgerätes verschlüsselt und können nur mit einem allein dem Empfänger zugänglichen privaten Schlüssel entschlüsselt werden.[28]

Auch was die technische Umsetzung des WhatsApp-Angebotes bei den Kommunen angeht, konnten wir keine Verstöße feststellen. Die von uns geprüften Angebote laufen nicht auf einem klassischen Mobilfunkgerät, sondern die WhatsApp-Anwendung wird in einer virtualisierten IT-Umgebung abgeschottet und isoliert betrieben, was einen Zugriff auf Kontaktdaten eines Mobilfunkgerätes (Adressbuch) ausschließt.

[28] *„At no time does the WhatsApp server have access to any of the client's private keys."*; vgl. WhatsApp Encryption Overview – Technical White Paper (Ver. Dez. 2017), elektronisch abrufbar unter: https://www.whatsapp.com/security/

4.12.5 Datenübermittlung in die USA

Letztlich stellt auch eine potentielle Datenübermittlung in die Vereinigten Staaten von Amerika aus datenschutzrechtlicher Sicht hier keinen Hinderungsgrund für den Einsatz des Messaging-Dienstes WhatsApp dar. Die Datenübermittlung in die USA erweist sich derzeit als von den Vorschriften des Art. 44 ff. DSGVO gedeckt. Mit Beschluss vom 12. Juni 2016 hat die Europäische Kommission festgestellt, dass die Vorgaben des EU-US Privacy Shield dem Datenschutzniveau der Europäischen Union entsprechen.[29] Die WhatsApp Inc. ist seit dem 08. März 2018 zertifiziert im Sinne dieses Abkommens,[30] unterfällt demnach dem Anwendungsbereich von Art. 45 Abs. 1 DSGVO.

4.13 Live-Übertragungen von Ratssitzungen über das Internet (Live-Streaming)

Neue Formen der demokratischen Teilhabe in einer digitalen Gesellschaft stellen in datenschutzrechtlicher Hinsicht sowohl die verantwortlichen Stellen als auch die Datenschutzaufsichtsbehörden vor immer neue Herausforderungen. Der Ort der politischen Meinungsbildung verlagert sich zunehmend weg von den öffentlichen Foren, hin in den rein digitalen Bereich des Internets.

Vor diesem Hintergrund beschäftigen sich auch die saarländischen Kommunen mit den rechtlichen Möglichkeiten einer Übertragung der öffentlichen Sitzungen ihrer Gemeinde- und Stadträte über das Internet. Die Herausforderung liegt hierbei

[29] Durchführungsbeschluss (EU) 2016/1250, (Amtsbl. EU, L 207/1).

[30] Elektronisch abrufbar unter: https://www.privacyshield.gov/participant?id=a2zt0000000TSnwAAG

in einem angemessenen Ausgleich zwischen dem Informationsbedürfnis der Öffentlichkeit und den datenschutzrechtlichen Positionen der politischen Akteure.

Dieser Interessenausgleich gestaltet sich umso schwieriger, als eine bereichsspezifische Rechtsgrundlage für eine Verarbeitung personenbezogener Daten in Form einer dauerhaften Übertragung von Bild und Ton einer Gemeinderatssitzung über das Internet (Live-Stream) im saarländischen Recht bis dato fehlt. Während das Kommunalrecht anderer Bundesländer das Anfertigen von Bild-, Film- und Tonaufnahmen im Bereich der kommunalen Parlamente teilweise explizit regelt (vgl. § 64 Abs. 2 Niedersächsisches Kommunalverfassungsgesetz [NKomVG][31] ; § 52 Abs. 3 Hessische Gemeindeordnung [HGO][32] ; § 29 Abs. 5 S. 5 Kommunalverfassung für das Land Mecklenburg-Vorpommern [KV M-V][33]), gründet § 40 Abs. 1 des saarländischen Kommunalselbstverwaltungsgesetzes (KSVG) noch vollständig auf dem tradierten Prinzip der Saalöffentlichkeit, mithin der räumlichen Zugänglichkeit der Ratssitzungen für alle Interessierten sowie für Medienvertreter zum Zwecke der Berichterstattung.

Die Frage, ob und ggf. in welchem Ausmaß diese Saalöffentlichkeit ein überkommenes Konstrukt vergangener Tage darstellt, welches sich den veränderten Lebensumständen, insbesondere

---

[31] Niedersächsisches Kommunalverfassungsgesetz vom 17. Dezember 2010 (Nds. GVBl. S. 576), zuletzt geändert durch Gesetz vom 20. Juni 2018 (Nds. GVBl. S. 113).

[32] Hessische Gemeindeordnung in der Fassung der Bekanntmachung vom 7. März 2005 (GVBl. I, S. 142), zuletzt geändert durch Gesetz vom 21. Juni 2018 (GVBl. S. 291).

[33] Kommunalverfassung für das Land Mecklenburg-Vorpommern vom 13. Juli 2011 (GVOBl. S. 777).

unserem digitalen Informationsbedürfnis – hin zu einer vollumfassenden Medienöffentlichkeit – anpassen muss, stellt sich als derart wesentlich und komplex dar, dass ihre Beantwortung auch im Saarland dem Gesetzgeber vorbehalten sein muss. Letzteres vor allem aufgrund der Tatsache, dass hierbei nicht ausschließlich datenschutzrechtliche Aspekte zu berücksichtigen sind. Ganzheitlich gesehen geht es vielmehr darum „(…) *das wechselseitige Spannungsfeld von Wahrung des Demokratieprinzips, der Funktionsfähigkeit der Vertretung und der Persönlichkeitsrechte von Abgeordneten, Zuschauern* (…) *und Mitarbeitern der Kommunalverwaltung"*[34] aufzulösen, was schwerlich auf untergesetzlicher Ebene geschehen kann. Eine auf die kommunale Selbstverwaltungsgarantie gestützte Satzung oder Ratsordnung, welche die beabsichtigte Datenverarbeitung regelt und als diesbezügliche Verarbeitungsgrundlage fungiert, scheidet unseres Erachtens als Rechtsgrundlage jedenfalls aus.

Auch die allgemeine Datenübermittlungsvorschrift des § 4 Abs. 3 Nr. 2 Saarländisches Datenschutzgesetz (SDSG) stellt keine diesbezüglich hinreichende Rechtsgrundlage dar. Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist hiernach zulässig, wenn „(…) *der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und die betroffene*[n] *Person*[en] *kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat/*[haben] (…)*"*. Hierbei ist bereits fraglich, ob diese allgemeine Übermittlungsbefugnis ne-

[34] *Weidemann*, Von der Saalöffentlichkeit zur Medienöffentlichkeit, KommJur 2017, S. 281 (282).

ben den bereichsspezifischen Regelungen des KSVG, insbesondere des § 40 KSVG, überhaupt Anwendung findet.[35] Darüber hinaus besteht auch kein berechtigtes Interesse der Öffentlichkeit an einer weltweit im Internet abrufbaren Übertragung einer Ratssitzung, mithin auch an einer Übertragung in Länder, welche kein angemessenes Datenschutzniveau aufweisen.[36]

Als hilfsweise Verarbeitungsgrundlage für die Übertragung einer Gemeinderatssitzung via Live-Stream kann jedoch das Institut der Einwilligung nach Art. 6 Abs. 1 S. 1 lit. a DSGVO herangezogen werden, d. h. eine Bild- und Tonaufzeichnung sowie Übertragung mit Wissen und Wollen der hiervon betroffenen Personen. Die Einwilligungen müssen hierbei in informierter Weise erteilt werden, was zwingend eine vorherige Unterrichtung über Art und Umfang der Datenverarbeitung voraussetzt. Den betroffenen Personen müssen dabei die Einzelheiten der beabsichtigten Video- und Tonaufzeichnungen sowie die Übertragungswege im Internet eingehend offengelegt werden.

Ein besonderes Augenmerk ist auch auf die Freiwilligkeit der Einwilligung zu legen. Die Freiwilligkeit ist insbesondere in denjenigen Fällen zu hinterfragen, in welchen zwischen dem Verantwortlichen (der Kommune) und der betroffenen Person ein klares Ungleichgewicht besteht. Ein solches kann im Rahmen eines sozialen Abhängigkeitsverhältnisses (Anstellungsverhältnis) bestehen, was insbesondere auf kommunale Bedienstete und Verwaltungsmitarbeiter zutrifft. Diese sollten demnach in der

[35] Zur alten Rechtslage *Horn*, Moderne Medien in Ratssitzung und Gerichtsverhandlung, ZJS 3/2012, S. 340 (345).

[36] *Horn*, Moderne Medien in Ratssitzung und Gerichtsverhandlung, ZJS 3/2012, S. 340 (345).

Regel außerhalb des Aufnahmebereichs der Kamera platziert werden.

Sind die notwendigen Einwilligungen der Ratsmitglieder für eine Live-Übertragung einer Ratssitzung vorhanden, sind hinsichtlich der Art und Weise der Übertragung weitere datenschutzrechtliche Restriktionen zu beachten. So ist vor allem sicherzustellen, dass von einer Bild- und Tonaufnahme keine der Saalöffentlichkeit angehörenden Zuschauer erfasst werden. Darüber hinaus ist sicherzustellen, dass jegliche Übertragung von Äußerungen Dritter (Zwischenrufe der Zuschauer etc.) und Gespräche der Ratsmitglieder mit persönlichem Inhalt unterbleibt. In organisatorischer Sicht lässt sich dies nur durch eine zeitverzögerte Datenübertragung realisieren, welche es erlaubt, auf entsprechende Äußerungen und Ereignisse zu reagieren und die Übertragung notfalls zu stoppen. Dies erfordert in allen Fällen eine redaktionelle Begleitung während der gesamten Übertragungszeit.

4.14 Nutzung von Geodaten (Luftbilder) zu Zwecken der Einführung einer getrennten Abwassergebühr

Mit Urteil vom 29. Juni 2016 (Az. 1 A 79/15) stellte das Oberverwaltungsgericht des Saarlandes die Nichtigkeit der Gebührenerhebung nach § 4 Abs. 1 und 2 der Abwassergebührensatzung einer saarländischen Stadt fest.

In Konsequenz dieser obergerichtlichen Rechtsprechung sehen sich diese und noch andere Kommunen nunmehr in der Pflicht, den gerichtlichen Vorgaben entsprechende Abwassergebührensatzungen einzuführen bzw. ihre alten Satzungen zu ändern. Viele Kommunen haben sich vor diesem Hintergrund für die

Einführung einer zwischen Schmutz- und Niederschlagswasser gesplitteten Abwassergebühr entschieden. Grundlage der Niederschlagswassergebühr sind dabei in der Regel die Dachflächen und die versiegelten Grundstücksflächen, von denen Regenwasser in die öffentliche Kanalisation eingeleitet wird.

Die betroffenen Kommunen können sich bei der Ermittlung dieser Flächen mehrerer Methoden bedienen, haben jedoch neben dem anfallenden Verwaltungsaufwand dafür Sorge zu tragen, dass die abgabenpflichtigen Flächen innerhalb des Kommunalgebiets auch tatsächlich und in Annäherung ihrer tatsächlichen Flächenmaße erfasst werden.

Neben dem Rückgriff auf verwaltungsinterne Daten (Liegenschafts- und Steuerdaten) sowie auf Selbstauskünfte der abgabenpflichtigen Grundstückseigentümer und -besitzer, erwies sich für die betroffene Stadt auch der Rückgriff auf Bildmaterial des Landesamtes für Vermessung und Geoinformation als geeignete Ermittlungsmethode der abgabenpflichtigen Grundstücksflächen innerhalb des Stadtgebietes.

Bei letzterem Bildmaterial handelt es sich um Luftbildaufnahmen, sogenannte Orthofotos, welche eine farbige, maßstabsgetreue und verzerrungsfreie Abbildung des Stadtgebietes in einer Bildauflösung von 10 cm darstellen. Die diesbezüglichen Fotografien werden durch das Landesamt für Vermessung und Geoinformation für jedermann einsehbar auf der Internetpräsenz „www.geoportal.saarland.de“ bereitgestellt.

Nicht zuletzt aufgrund datenschutzrechtlicher Beschwerden nach Art. 77 Datenschutz-Grundverordnung (DSGVO) war unsere Behörde mit der Frage konfrontiert, ob dieses Fotomaterial zur Ermittlung der in Bezug genommenen Grundstücksflächen

durch die Kommunen verarbeitet werden darf. Die Beschwerdeführer vertraten hierbei insbesondere die Auffassung, eine Verarbeitung solch sensibler Daten wie fotografischer Ansichten ihres Grundeigentums bedinge ihre vorherige Einwilligung.

Die in Bezug genommene Verwendung von Luftaufnahmen durch die hierfür verantwortliche Stadt ist ein anschauliches Beispiel dafür, dass die Rechtmäßigkeit einer Verarbeitung personenbezogener Daten nicht zwingend eine Einwilligung der betroffenen Personen erfordert. Im Rahmen der öffentlichen Verwaltung stellt die Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO vielmehr die Ausnahme dar. Gemäß Art. 6 Abs. 1 lit. e, Abs. 3 S. 1 lit. b DSGVO ist eine Verarbeitung durch Behörden und sonstige öffentliche Stellen rechtmäßig, wenn sie für die Wahrnehmung einer öffentlichen Aufgabe erforderlich ist. Hiernach können sodann auch Verarbeitungen ohne bzw. gegen den Willen der betroffenen Person durchgeführt werden.

Die vorliegende Datenverarbeitung stützt sich auf § 4 Saarländisches Datenschutzgesetz (SDSG)[37] i. V. m. §§ 1 Abs. 1 Kommunalabgabengesetz (KAG)[38], 12 Kommunalselbstverwaltungsgesetz (KSVG)[39]. Eine Datenverarbeitung durch öffentliche Stellen ist hiernach zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der oder des Verantwortlichen liegenden Aufgabe erforderlich ist.

[37] Saarländisches Datenschutzgesetz vom 16. Mai 2018 (Amtsbl. I S. 254).

[38] Gesetz Nr. 1074 – Kommunalabgabengesetz – vom 26. April 1978 in der Fassung der Bekanntmachung vom 29. Mai 1998 (Amtsbl. S. 691), zuletzt geändert durch das Gesetz vom 22. August 2018 (Amtsbl. I S. 674).

[39] Kommunalselbstverwaltungsgesetz in der Fassung der Bekanntmachung vom 27. Juni1997 (Amtsbl. S. 682), zuletzt geändert durch Gesetz vom 15. Juni 2016 (Amtsbl. I S. 840).

Die Regelung und Ausgestaltung der kommunalen Entwässerung ist eine Angelegenheit der örtlichen Gemeinschaft. Die Kommune ist gemäß § 1 Abs. 1 KAG befugt, hierauf bezogene Abgaben (Beiträge und Gebühren) durch Satzung (§ 12 KSVG) zu regeln. Sie hat sich dabei an den Vorgaben der obergerichtlichen Rechtsprechung zur rechtmäßigen Ausgestaltung von Abwassergebühren zu orientieren, welche insbesondere eine sich an objektiven Maßstäben orientierende Belastungsgleichheit der Abgabenpflichtigen und fordert.

In Bezug auf Niederschlagswassergebühren erfordert die rechtmäßige Kalkulation der Gebühr insbesondere die vorherige Ermittlung der versiegelten, bebauten und sonst befestigten Grundstücksflächen. Die bloße Schätzung des versiegelten Bodens erweist sich demgegenüber als gerade nicht ausreichend.[40]

Das von der Stadt gewählte Verfahren einer Flächenermittlung mittels Bildmaterial des Geoinformationssystems stellt sich vor diesem Hintergrund als verhältnismäßige Datenverarbeitung dar. Zwar lassen sich mittels der verarbeiteten Luftbilder keine exakten Informationen über die Entwässerung von Grundstücksflächen ermitteln, da anhand dieser Fotografien selten erkannt werden kann, ob eine Fläche in die städtische Kanalisation entwässert oder das Niederschlagswasser in eine Zisterne geleitet wird oder versickert. Die Verarbeitung der Luftbilder aus dem Geodateninformationssystem verfolgt jedoch auch nicht diesen Zweck. Ziel ist es vielmehr, in einem ersten Schritt die in Betracht kommenden Entwässerungsflächen, einschließlich deren Flä-

[40] OVG Bautzen, Urteil vom 27. März 2001 – 5 D 21/99, NVwZ- RR 2002, S. 371 (372).

chenmaße, zu ermitteln und die jeweilige Entwässerungsart sodann durch eine Anhörung der betroffenen Personen zu konkretisieren.

Eine reine Selbstauskunft der Grundstückseigentümer und -besitzer stellt sich demgegenüber zwar als datenschutzrechtlich milderes, jedoch nicht gleich geeignetes Mittel der Gebührenkalkulation dar. Es erscheint bereits fraglich, ob die betroffenen Personen über die notwendigen Informationen der ihnen zuordenbaren Entwässerungsflächen verfügen bzw. in der Lage sind, diese Informationen mit einem vertretbaren Arbeits- und Kostenaufwand zu beschaffen.

Darüber hinaus muss berücksichtigt werden, dass aufgrund des Gebotes der Erhebungsgleichheit erhebliche Anforderungen an die Überprüfung und Kontrolle der über eine reine Selbstauskunft gewonnenen Erkenntnisse gestellt werden müssen. Aufgrund der hohen Fehleranfälligkeit müssten die von den Gebührenpflichtigen eingeforderten Auskünfte zumindest stichprobenartig durch die Kommune kontrolliert und Mithilfe von Karten, Plänen und auch Luftbildern abgeglichen werden,[41] was wiederum eine Verarbeitung personenbezogener Daten impliziert.

Es stellt sich vor diesem Hintergrund als geeignet und erforderlich dar, wenn die Kommune den betroffenen Abgabenpflichtigen bereits mit dem Ersuchen auf Selbstauskunft eigene Ermittlungsergebnisse über die entwässerten Flächen mitteilt, welche auf einer Auswertung von Luftbildaufnahmen beruhen. Hierfür bietet sich der Rückgriff auf vorhandenes Kartenmaterial des

[41] Vgl. OVG Münster, Urteil vom 18. Dezember 2007 – 9 A 3648/04, IBRRS 2008, S. 1322.

Geoinformationssystems des Landesamts für Vermessung und Geoinformation an, da die hierin enthaltenen Luftbildaufnahmen eine Zuordenbarkeit der Boden- und Gebäudebeschaffenheit eines Grundstücks und damit potentieller Entwässerungsflächen, zulassen. Aufgrund der relativ großen Entfernung der Aufnahme zum Bezugsobjekt werden zugleich die datenschutzrechtlichen Positionen der betroffenen Personen gewahrt.

4.15 Telearbeit bei der Polizei

Am 13. Februar 2012 ist die Richtlinie über Telearbeit als ergänzende Arbeitsform in der saarländischen Landesverwaltung in Kraft getreten.

Für die saarländische Polizei wurde erstmals ab August 2018 im Rahmen eines Probebetriebes Telearbeit an wohnortnahen Polizeidienststellen sowie am häuslichen Arbeitsplatz eingerichtet. Auf die Möglichkeit, von dem Telearbeitsrechner auf polizeiliche Informationssysteme zugreifen zu können, wurde aufgrund der hierbei einzuhaltenden hohen IT-Sicherheitsanforderungen, die eine unbefugte Systemnutzung durch Dritte ausschließen muss, vorerst verzichtet.

Ohne die Einbeziehung der Nutzung von polizeilichen Informationssystemen kann die Telearbeitsform jedoch nur von wenigen Polizeibediensteten genutzt werden. Das Landespolizeipräsidium hat daher in einem zweiten Schritt in 2019 die Einführung von Telearbeit am häuslichen Arbeitsplatz unter Nutzung der polizeilichen Informationssysteme geprüft und unsere Dienststelle beratend eingebunden.

Aus datenschutzrechtlicher Sicht war darauf zu achten, dass die bisherigen Rechte-Rollen-Konzepte zu den einzelnen Informa-

tionssystemen übernommen werden. Die Vergabe eines Telearbeitsplatzes sollte den Mitarbeitern keine weitergehenden Berechtigungen als bisher einräumen, vielmehr sollte auch weiterhin nur eine Zugriffsberechtigung zu bestimmten, für die zugewiesene Sachbearbeiterrolle notwendigen Informationssystemen bestehen. Ferner gibt die für die Datenverarbeitung durch die Polizei maßgebende Richtlinie (EU) 2016/680 in Art. 29 i.V.m. Erwägungsgrund (ErwG) 53 vor, dass bei der Verarbeitung personenbezogener Daten für deren Schutz geeignete technische und organisatorische Maßnahmen zu treffen sind. ErwG 60 führt aus, dass der Verantwortliche sicherstellen soll, dass personenbezogene Daten nicht durch Unbefugte verarbeitet werden. Unter Berücksichtigung des Stands der Technik und der Implementierungskosten sind Schutzmaßnahmen zu ergreifen, die mit Blick auf das von der Datenverarbeitung ausgehende Risiko und die Art der zu schützenden personenbezogen Daten angemessen sind.

Wir haben daher das Landespolizeipräsidium dahingehend beraten, dass das IT-Sicherheitskonzept nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[42] aufgebaut werden sollte.

Fazit/ Empfehlung:

Die technisch-organisatorischen Maßnahmen bei der Telearbeit sollten auf dem neuen IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik in seiner aktuellsten Edition aufbauen.

[42] Elektronisch abrufbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/bausteine_node.html

4.16 Lichtbildabgleich in Ordnungswidrigkeitenverfahren

Die personenbezogene Datenverarbeitung durch Behörden im Rahmen der Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten ist ein immer wiederkehrendes Thema der Datenschutzaufsicht im öffentlichen Bereich. Sie stellt zugleich einen besonders sensiblen Teil der Aufsichtstätigkeit dar, gilt es in ihrem Rahmen doch, das staatliche Interesse an einer effektiven Sanktionierung von Gesetzesübertretungen mit den datenschutzrechtlichen Positionen oftmals unbeteiligter Personen in einen angemessenen Ausgleich zueinander zu bringen.

Vor diesem Hintergrund hatte sich unsere Behörde in mehreren Beschwerdefällen mit der rechtlichen Zulässigkeit der im Rahmen von Ermittlungsverfahren in Verkehrsordnungswidrigkeiten bestehenden Verwaltungspraxis eines Lichtbildabgleichs über den Datenbestand der Personal- und Passregister zu befassen. Hierbei wird das Beweisfoto einer Geschwindigkeitsmessanlage (umgangssprachlich „Blitzer“) mit den Lichtbildern verglichen, welche in den Pass- und Ausweisregistern vorgehalten werden und sich in dieser Form auf den Personalausweisen und Reisepässen befinden.

Ihre rechtlichen Grundlagen findet diese Verwaltungspraxis in § 24 Abs. 2 Personalausweisgesetz (PAuswG)[43] und § 22 Abs. 2 Paßgesetz (PaßG). Hiernach dürfen Personalausweis- und Passbehörden anderen Behörden auf deren Ersuchen Daten aus den von ihnen geführten Registern übermitteln, wenn „(…) *die*

[43] 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).

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 (...) *".*

Unsere Behörde ist in diesem Zusammenhang der Rechtsauffassung, dass eine Übermittlung von Passfotos an die Ordnungswidrigkeitenbehörden und ein Lichtbildabgleich durch diese nur dann als rechtmäßig bewertet werden können, wenn sie den das diesbezügliche Verfahren konkretisierenden 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 berücksichtigen.

Nach diesem Erlass ist Voraussetzung für einen Lichtbildabgleich, dass im Vorhinein der Datenübermittlung von der Passbehörde an die ersuchende Ordnungswidrigkeitenbehörde dem Betroffenen (Beschuldigten), unter Vorlage des im Zuge der Verkehrsüberwachung angefertigten Lichtbildes, Gelegenheit zur Stellungnahme nach § 55 Gesetz über Ordnungswidrigkeiten (OWiG) zu geben ist.

Vornehmlicher Zweck dieser vorherigen Anhörung des Betroffenen ist es, dem Verhältnismäßigkeitsgebot dadurch Rechnung zu tragen, dass den Betroffenen Gelegenheit gegeben wird, sich zu der Anschuldigung zu äußern. Er erhält hierdurch die Möglichkeit, der Behörde seine Sicht der Dinge vorzutragen insbesondere, den Tatvorwurf gegen ihn bereits im Ansatz der Ermittlungen zu entkräften. Die vorherige Anhörung gibt dem Betroffenen hingegen nicht die Möglichkeit, einen Lichtbildabgleich bei fortbestehendem Tatverdacht zu verhindern. Folgerichtig ist nach derzeitiger Erlasslage der Betroffene durch die

ersuchende Behörde bereits im Anhörungsbogen darauf hinzuweisen, dass das die Ordnungswidrigkeit dokumentierende Foto mit dem im Pass- oder Personalausweisregister hinterlegten Foto verglichen werden kann, falls er sich nicht äußern möchte.

Grundvoraussetzung für einen Lichtbildabgleich ist demnach, dass zunächst eine Person als „Betroffener" i. S. d. § 66 Abs. 1 Nr. 1 OWiG anzusehen ist. Hierfür muss ein Anfangsverdacht der Begehung einer Ordnungswidrigkeit gegen eine oder mehrere identifizierte Personen vorliegen. Ein Lichtbildabgleich, welcher ohne vorherige Verdachtsmomente erst zur Ermittlung eines potentiell in Betracht kommenden Personenkreises durchgeführt wird, widerspricht nach hiesiger Rechtsauffassung demgegenüber einer verhältnismäßigen Datenverarbeitung.

Als datenschutzwidrig erweist sich demnach eine Verwaltungspraxis, bei welcher die Lichtbilder von Familienangehörigen des Fahrzeughalters ohne vorherige Anhörung dieser Personen zu Zwecken der Fahreridentifizierung herangezogen werden.

4.17 Fotografieren an Schulen und Kindergärten

Ein Thema, das Schulen und Kindergärten wie auch Eltern im Berichtszeitraum zunehmend bewegte, war die Frage nach der Zulässigkeit von Fotos in Schulen und Kindergärten.

4.17.1 Fotos zu privaten Zwecken von Lehrern und Schülern

Fertigen Lehrer, Eltern oder Schüler Fotos für private oder familiäre Zwecke an, auf denen auch Mitschüler oder sonstige Personen zu sehen sind und veröffentlichen sie diese nicht, so greift hier die sogenannte „Haushaltsausnahme". Art. 2 Abs. 2 lit. b

Datenschutz-Grundverordnung (DSGVO) besagt, dass der datenschutzrechtliche Regelungsrahmen keine Anwendung findet, soweit es sich um eine Datenverarbeitung zu rein persönlichen oder familiären Zwecken handelt. Besteht über die Hausordnung der Schule kein entsprechendes Verbot, so ist das Fotografieren zu ausschließlich privaten oder familiären Zwecken auch auf dem Schulgelände gestattet. Ebenso sind Aufnahmen, die während einer Klassenfahrt angefertigt wurden, auch ohne Einwilligung der Betroffenen zulässig, soweit sie zu rein privaten Zwecken genutzt werden und nicht beispielsweise in sozialen Medien veröffentlicht werden.

4.17.2 Klassenfotos, Einzelfotos und Schülerausweise durch externe Fotografen

An vielen Schulen ist die jährliche Anfertigung von Klassenfotos üblich. Werden diese Arbeiten durch einen externen Fotografen durchgeführt, muss mit dem Fotografen eine Vereinbarung getroffen werden, die den Anforderungen des Art. 28 Abs. 3 DSGVO genügt. Die Schule als Verantwortlicher darf dabei nur mit solchen Auftragsverarbeitern zusammenarbeiten, die hinreichende Gewähr dafür bieten, dass geeignete technische und organisatorische Maßnahmen getroffen wurden, um die Verarbeitung im Sinne der DSGVO durchzuführen und die personenbezogenen Daten vor unbefugten Zugriffen zu schützen.

4.17.3 Veröffentlichung von Fotos

Gerade im Bereich der Schulen und Kindergärten hat sich eine verständliche Unsicherheit ergeben, unter welchen Voraussetzungen Fotos von Aktivitäten der Einrichtung veröffentlicht werden dürfen.

Den rechtlich sichersten Weg, sich bei der Veröffentlichung von Fotos datenschutzkonform zu verhalten, stellt derzeit die Einwilligung der einsichtsfähigen Schüler oder ggf. der Erziehungsberechtigten im Sinne von Art. 4 Nr. 11 DSGVO dar. Soweit die Anforderungen an die Einwilligung aus der o.g. Norm erfüllt sind, ist die Datenverarbeitung gem. Art. 6 Abs. 1 lit. a DSGVO legitimiert. Dabei muss die Einwilligung auf den konkreten Zweck bezogen und transparent formuliert sein. Eine „Pauschaleinwilligung" in alle Veröffentlichungen und zu jedem möglichen Zweck erfüllt nicht die Voraussetzungen einer datenschutzkonformen Einwilligung. Die Einwilligung muss so formuliert sein, dass der konkrete Zweck, beispielsweise die Öffentlichkeitsarbeit im Rahmen einer bestimmten Veranstaltung, benannt wird, mögliche Empfänger und Veröffentlichungsplattformen konkret bezeichnet werden (zur Veröffentlichung auf unserer Homepage, zur Weiterleitung an die lokale Presse, etc.) sowie die Löschung der Daten (beispielsweise bis zum Ende des Schuljahres) konkret festgelegt wird. Die Betroffenen müssen sich der Tragweite ihrer Entscheidung bewusst sein, wenn sie in die Veröffentlichung einwilligen. Dies bedeutet, dass besondere Aktivitäten der Schule, die mit einer Veröffentlichung personenbezogener Daten einhergehen, wie beispielsweise die Teilnahme an einer im Fernsehen übertragenen Veranstaltung, einer separaten Einwilligung der Betroffenen bedürfen, die konkret für diesen Zweck formuliert werden muss. Weitere Ausführungen zur Einwilligung können dem Kurzpapier Nr. 20 der Konferenz der unabhängigen Datenschutzbehörden des Bundes

und der Länder (DSK) entnommen werden, das auf unserem Internetangebot abrufbar ist.[44] Wird die Einwilligung in die Veröffentlichung der Fotos von den Erziehungsberechtigten oder einsichtsfähigen Schülern nicht erteilt, so muss der Verantwortliche dies schon beim Anfertigen der Fotos berücksichtigen, indem er die betroffenen Schüler hiervon ausnimmt.

Nicht in allen Fällen bedarf es für die Anfertigung und anschließende Veröffentlichung von Fotos indes einer Einwilligung. Dies vor allem dann nicht, wenn eine im Zuge der Öffentlichkeitsarbeit vorgenommene Veröffentlichung von Fotografien einer schulischen Veranstaltungen als im Interesse der Einrichtung liegend angesehen werden kann. Dieses Veröffentlichungsinteresse ist jedoch eng auszulegen und muss in jedem Einzelfall mit den Interessen der abgebildeten Personen, insbesondere den schutzwürdigen Interessen von Kindern sorgsam abgewogen werden. Wird es bejaht, so ist darauf zu achten, dass die auf den Fotografien abgebildeten Personen nur als Beiwerk zur Örtlichkeit erscheinen und keinesfalls im Fokus der Aufnahmen stehen.

Um den in allen Fällen bestehenden Informationspflichten nach Art. 13 DSGVO zu genügen, sollte weiter darauf geachtet werden, dass bereits in der Einladung zu der Veranstaltung oder durch gut sichtbare Hinweise am Veranstaltungsort die notwendigen Informationen für die Betroffenen bereitgestellt werden. Neben dem Zweck, zu dem die Fotos angefertigt werden umfasst dies auch den Hinweis darauf, dass man beabsichtigt, Fo-

[44] Elektronisch abrufbar unter: https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/datenschutz/ds-gvo/kurzpapiere/Kurzpapier_Nr_20_Einwilligung_nach_der_DSGVO.pdf

tos der Veranstaltung beispielsweise auf der eigenen Homepage zu veröffentlichen. Daneben sind die Betroffenen darüber zu unterrichten, an wen sie sich wenden können, um sich gegen eine Veröffentlichung von Fotos ihrer Person aussprechen zu können. Auch sollten technisch-organisatorische Maßnahmen getroffen werden, die darauf hinwirken, dass eine Indexierung der Webinhalte durch Webcrawler unterbleibt (beispielsweise mittels sog. Robots Exclusion Standard).

Fazit/ Empfehlung:

Die Einwilligung der Erziehungsberechtigten oder einsichtsfähigen Schüler zur Veröffentlichung von Fotos ist datenschutzrechtlich der sicherste Weg diese Datenverarbeitung zu legitimieren.

4.18 Videoüberwachung

Das abstrakte Thema Datenschutz gewinnt für Betroffene und auch für Verantwortliche oftmals erst dann Kontur, sobald es den Betrieb von Kameras betrifft; allein das Vorhandensein einer Kamera – welche in der medialen Darstellung zum Symbolbild der Überwachung oder des Datenschutzes an sich geworden ist – führt vielen Betroffenen überhaupt erst die Möglichkeit einer Datenverarbeitung plastisch vor Augen.

Die Bandbreite der Einsatzmöglichkeiten von Kameras steht dabei in keinem Verhältnis zu dem überwiegenden Gegenstand von Beschwerden, die an das Unabhängige Datenschutzzentrum Saarland herangetragen werden: Wie auch in den vorher-

gehenden Berichtszeiträumen thematisiert das Gros der Beschwerden die Videoüberwachung im nachbarschaftlichen Umfeld.

4.18.1 Kameraeinsatz durch Privatpersonen

Unabhängig ob mobil oder stationär sind Kameras, die von Privatpersonen im öffentlichen Raum zur Wahrnehmung spezifischer Zwecke eingesetzt werden, regelmäßig nach denselben datenschutzrechtlichen Vorgaben zu beurteilen: Die Interessenabwägung nach Art. 6 Abs. 1 lit. f Datenschutz-Grundverordnung (DSGVO) ist als datenschutzrechtliche Richtschnur für Kamerabetreiber maßgebend.

Mobile Kameraeinsätze durch Privatpersonen, wie beispielweise Dashcams, die eingesetzt werden, um ein eventuelles Unfallgeschehen dokumentieren zu können, oder Kameradrohnen[45], wurden im Berichtszeitraum lediglich im Rahmen einer überschaubaren Anzahl an Beschwerden vorgebracht. Gerade für die mittlerweile häufig anzutreffenden Dashcams wird von den Betreibern überwiegend die unzutreffende Ansicht vertreten, dass der Bundesgerichtshof (BGH) in seiner Entscheidung vom 15. Mai 2018 – VI ZR 233/17 – jeglichen Einsatz vorbehaltlos legitimiert habe. Dies ist jedoch mitnichten der Fall. Vielmehr hat der BGH festgestellt, dass schutzwürdige Interessen der übrigen Verkehrsteilnehmer und Passanten dem dauerhaften, anlasslosen Dashcam-Betrieb entgegenstehen.[46] Da die Mehrzahl der

[45] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), Positionspapier zur Nutzung von Kameradrohnen durch nichtöffentliche Stellen (Stand: Januar 2019), elektronisch abrufbar unter: https://www.datenschutz.saarland.de/themen/videoueberwachung/

[46] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), Positionspapier zur Unzulässigkeit von Videoüberwachung aus

Fälle von Dashcam-Einsätzen bei Polizeidienststellen, beispielweise im Rahmen von Verkehrskontrollen oder bei Aufnahme von Unfallgeschehen, zu Tage treten, wurde an das Landespolizeipräsidium im Hinblick auf die Möglichkeit der Sicherung von datenschutzwidrig angefertigten Aufnahmen durch Beschlagnahme von Datenträgern ein Gesprächsangebot übermittelt, auf das eine Antwort bisher noch aussteht.

Für den Einsatz stationärer Kameras durch Private bleibt für die Frage nach der Anwendung des datenschutzrechtlichen Regelungsrahmen der Erfassungsbereich der Kamera maßgeblich; soweit Kameras im Umfeld von Wohngebäuden mit dem Zweck der Vermeidung von Schadenshandlungen durch Abschreckung beziehungsweise zu deren Verfolgung eingesetzt werden und diese ausschließlich auf das eigene, selbstbewohnte Grundstück ausgerichtet sind, findet diese Überwachung in einem persönlichen und familiären Kontext im Sinne des Art. 2 Abs. 2 lit. c DSGVO und damit außerhalb des datenschutzrechtlichen Regelungsregimes statt. Etwas anderes ergibt sich allerdings dann, wenn Personen im Rahmen ihrer beruflichen Tätigkeit gezwungen sind, sich auf dem privaten Grundstück aufzuhalten und hierbei Objekt einer gezielten Überwachung sind (beispielweise Bezirksschornsteinfeger oder Mitarbeiter von Pflegediensten). In diesem Fall ist eine Videoüberwachung unzulässig. Eine Überwachungsmaßnahme, die über das eigene Grundstück hinausreicht oder auch Eingangs- oder Durchgangsbereiche erfasst, so dass Personen wie Brief-/Paketzusteller oder Mitarbeiter von Lieferservices anlasslos zum Objekt der Videoüberwachung

Fahrzeugen (sog. Dashcams), elektronisch abrufbar unter: https://www.datenschutz.saarland.de/themen/videoueberwachung/

werden, ist hingegen vollumfänglich an den datenschutzrechtlichen Vorgaben zu messen.[47] Sofern ein berechtigtes Überwachungsinteresse zu bejahen und eine Gefährdungslage dokumentiert ist – beispielweise in der Vergangenheit stattgefundene oder zukünftig hinreichend wahrscheinlich zu erwartende Sachbeschädigungen an einer Hausfassade – kann allenfalls die Erfassung eines im Einzelfall geringen adäquaten Toleranzbereichs des öffentlichen Raums zur Zweckerreichung erforderlich sein. Unter dem Gesichtspunkt der Datenminimierung im Sinne des Art. 5 Abs. 1 lit. c DSGVO ist nicht nur eine Beschränkung der Überwachung in räumlicher, sondern auch in zeitlicher Hinsicht zu prüfen, soweit der Eintritt von Schadensereignissen zu bestimmten Tageszeiten wahrscheinlicher ist. Entgegen der oftmals vertretenen Auffassung, dass allein die Anbringung der ohnehin verpflichtenden Hinweisschilder nach Art. 13 DSGVO[48] die Videoüberwachung legitimiert, sind Interessen und Grundrechte/-freiheiten betroffener Personen bei der Interessenabwägung zu berücksichtigen. Überwachungsmaßnahmen, die ganze öffentliche Gehwege oder Straßenzüge erfassen, sind nicht nur nicht zum Schutz des Grundstücks erforderlich im Sinne des Art. 6 Abs. lit. f DSGVO, ihnen stehen regelmäßig auch überwiegende schutzwürdige Interessen der anlasslos erfassten Passanten, Anwohner oder Nachbarn entgegen.

Oftmals wird von Verantwortlichen auch vorgebracht, dass trotz Ausrichtung der Kamera in den öffentlichen Raum durch softwareseitige Maßnahmen, wie Auspixeln oder den Einsatz einer

[47] EuGH, Urteil vom 11. Dezember 2014 – C-212/13, Rn. 33 ff., juris.

[48] Muster für ein Hinweisschild nach Art. 13 DSGVO, elektronisch abrufbar unter: https://www.datenschutz.saarland.de/themen/videoueberwachung

statischen digitalen Maskierung (Privacy-Filter), spezifische Bereiche nicht von der Überwachung betroffen sind und diese daher datenschutzkonform stattfinde; allerdings ist der Einsatz solcher Maßnahmen, die erst nach bereits erfolgter Aufnahme von Bilddaten einsetzen, durch Privatpersonen überwiegend datenschutzrechtlich als problematisch anzusehen. Soweit solche Filter üblicherweise jederzeit über die Benutzeroberfläche des Betriebssystems der Kamera durch den Nutzer de-/aktiviert werden können und den Datenschutzbehörden kein Recht zum unangekündigten Betreten von Privatwohnungen zusteht[49], entzieht sich deren Einsatz einer objektiven externen Kontrolle. In diesbezüglichen Verwaltungsverfahren wird daher regelmäßig die Neuausrichtung der Stabkamera oder die Anbringung einer physischen Abdeckung bei Kuppelkameras als Maßnahme zur Herstellung eines datenschutzkonformen Zustands gefordert.

Einer Vielzahl der Beschwerden im Zusammenhang mit der nachbarschaftlichen Videoüberwachung gehen teils langjährige Auseinandersetzungen voraus. Kamerabetreiber, die sich durch ihre beschwerdeführenden Nachbarn gegenüber der Datenschutzaufsichtsbehörde denunziert glauben, bitten daher erst einmal um Auskunft über die Person des Beschwerdeführers. Angaben zum Beschwerdeführer oder Hinweisgeber werden jedoch gegenüber dem Beschwerdegegner grundsätzlich nicht preisgegeben. Eine Offenlegung der Informationen zur beschwerdeführendenden Person scheidet aus, da der Schutz

[49] Im Gegensatz zum Recht auf Zugang zu den Geschäftsräumen des Verantwortlichen nach Art. 58 Abs. 1 lit f. DSGVO.

diesbezüglicher Angaben zum Informanten im öffentlichen Interesse liegt.[50]

4.18.2 Videoüberwachung im kommerziellen Kontext

Für den Kameraeinsatz durch Unternehmen oder im Zusammenhang mit der wirtschaftlichen Betätigung von Privatpersonen sind datenschutzrechtliche Vorgaben ausnahmslos anwendbar; die Zulässigkeit der Überwachung von Verkaufsflächen, Betriebsgeländen, Geschäftsräumen, Eingangsbereichen etc. ist daher nach Art. 6 Abs. 1 lit. f DSGVO dann anzunehmen, wenn ein berechtigtes Überwachungsinteresse gegeben ist, keine milderen Mittel anstelle der Überwachung in Frage kommen und Interessen und Grundrechte der betroffenen Personen nicht überwiegen.

Die kameragestützte Erfassung besonders schützenswerter Bereiche führt regelmäßig zur Unzulässigkeit der Überwachung: Beispielsweise ist die oft anzutreffende Erfassung von Gastbereichen in Gastronomiebetrieben regelmäßig unzulässig. Diesbezüglich wurden im Berichtszeitraum in zwei Fällen der Videoüberwachung Bußgeldverfahren eingeleitet. Ein Bescheid über ein Bußgeld in Höhe von 2.000,- € ist bereits rechtskräftig. Auch die als Gegenstand einer Beschwerde vorgebrachte kameragestützte Erfassung von Gemeinschaftsräumen und Küche durch einen Vermieter war trotz wiederholt stattgefundener Diebstähle von Einrichtungsgegenständen angesichts der besonderen Schutzwürdigkeit dieses Kernbereichs der privaten Lebensführung datenschutzrechtlich in keiner Weise legitimierbar.

[50] Hessischer Verwaltungsgerichtshof, Beschluss vom 31. Oktober 2019 – 10 B 1869/19.

Einige an das Unabhängige Datenschutzzentrum Saarland adressierte Anfragen thematisierten den gewerblichen Einsatz von Kameradrohnen, um im Auftrag des Kunden spezifische Veranstaltungen wie Familien- oder Unternehmensfeiern zu dokumentieren. Dieser kann – unter gleichzeitiger Beachtung luftverkehrsrechtlicher Vorgaben – nach Art. 6 Abs. 1 lit. f DSGVO zulässig sein; Gäste, Teilnehmer oder erfasste Passanten sind dabei transparent im Sinne des Art. 13 DSGVO – beispielweise durch Hinweisschilder – zu informieren. Gleiches gilt für den Drohneneinsatz soweit dieser für Marketingzwecke stattfindet und die betroffenen Personen situativ nicht in einem schützenswerten oder gar potentiell kompromittierenden Kontext erfasst werden. Soweit die Aufnahmen auf Webseiten veröffentlicht werden, gilt es ein besonderes Augenmerk darauf zu legen, dass die betroffenen Personen über die Art der Veröffentlichung und das Widerspruchsrecht im Sinne des Art. 21 Abs. 1 DSGVO informiert werden.

Werden besondere personenbezogene Daten nach Art. 9 Abs. 1 DSGVO – wie Gesundheitsdaten, Information über weltanschauliche, politische Überzeugungen oder ethnische Zugehörigkeit – im Rahmen des Kameraeinsatzes verarbeitet, spricht dies grundsätzlich gegen die Zulässigkeit der Videoüberwachung. Eine Videoüberwachung, die beispielsweise den Eingangsbereich einer Gebetsstätte oder eines Parteibüros erfasst, wird allenfalls unter den Voraussetzungen des Art. 9 Abs. 2 DSGVO zulässig sein; soweit jedoch das Tragen religiöser oder politischer Symbole bzw. Charakteristika einer betroffenen Person wie deren Hautfarbe oder eine körperliche Beeinträchtigung als Beiwerk und somit nicht zielgerichtet erfasst werden, ist nicht von einer diesbezüglichen Verarbeitungsbeschränkung auszugehen.

4.18.3 Rechtsprechung des Bundesverwaltungsgerichts

Hinsichtlich der im Berichtszeitraum ergangenen gerichtlichen Entscheidungen zum Themenkomplex Videoüberwachung, gebührt vor allem dem Urteil des Bundesverwaltungsgerichts (BVerwG) vom 27. März 2019 – 6 C 2.18 die größte Aufmerksamkeit. Unabhängig davon, dass der Entscheidung eine Anordnung[51] nach Rechtslage vor Geltungsbeginn der DSGVO zugrunde lag, lassen sich der Entscheidung gerade auch Aussagen zur Zulässigkeit der Videoüberwachung nach der Rechtslage ab dem 25. Mai 2018 entnehmen.

Das Gericht führt aus, dass privaten Stellen, soweit diesen ausdrücklich keine Wahrnehmung hoheitlicher Aufgaben zukommt, keine Befugnis zur Verarbeitung personenbezogener Daten auf Grundlage von Art. 6 Abs. 1 lit. e DSGVO zusteht. Dementsprechend kann § 4 BDSG, als ausschließlich im deutschen Recht verankerte Vorschrift zur Videoüberwachung, nicht über die Öffnungsklauseln nach Art. 6 Abs. 2 und 3 DSGVO Wirkung für Videoüberwachungsmaßnahmen durch private Stellen entfalten[52]; allein der unionsrechtliche Rechtsrahmen, regelmäßig in Form der Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO, ist maßgeblich.

Dabei betont das BVerwG, dass für die Auslegung der bis zum 24. Mai 2018 geltenden und der aktuellen Rechtslage vergleichbare Maßstäbe heranzuziehen sind: Das mit der Videoüberwachung verfolgte Verarbeitungsinteresse muss berechtigt sein, es darf keine mildere, weniger eingriffsintensivere, jedoch gleich geeignete Alternative zum Kameraeinsatz geben und es dürfen

[51] Betreffend die Zulässigkeit der Videoüberwachung in einer Zahnarztpraxis.

[52] Vgl. 26. Tätigkeitbericht, 2015/2016, Kapitel 15.1., S. 136 ff.

keine überwiegenden Interessen und Rechte der betroffenen Personen ersichtlich sein.

Für den zu entscheidenden Fall hat das Gericht u. a. festgestellt, dass eine die Überwachung begründende Gefährdungslage (Straftraten in Besucherbereich) nicht ausreichend substantiiert vorgetragen wurde und sich mildere Mittel als die Videoüberwachung aufdrängen (Abschließen von Zugangstüren und Wegschließen von diebstahlgefährdeten Betäubungsmitteln)[53], so dass die verfahrensgegenständliche Videoüberwachung nicht datenschutzrechtlich zulässig betrieben werden konnte.

4.18.4 Orientierungshilfen

Neben den bereits auf dem Internetauftritt des Unabhängigen Datenschutzzentrums Saarland unter der Rubrik Videoüberwachung veröffentlichten Informationsmaterialien der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) steht eine novellierte Fassung der Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen" kurz vor der Veröffentlichung. Darüber hinaus wurde im Berichtszeitraum die öffentliche Konsultation zu den „Guidelines 3/2019 on processing of personal data through video devices" des Europäischen Datenschutzausschusses[54] abgeschlossen. Auch hier ist mit einer zeitnahen Veröffentlichung des finalen Papiers zu rechnen.

[53] Vgl. 27. Tätigkeitbericht 2017/2018, Kapitel 15.2., S. 138 ff.

[54] Elektronisch abrufbar unter: https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-32019-processing-personal-data-through-video_en

4.19 Datenschutz im Verein

Wie im vorangegangenen Berichtszeitraum 2017/2018 war der Themenkomplex des Vereinsdatenschutzes wieder ein Dauerbrenner. Auch wenn die Anzahl der Anfragen gegenüber den Vorjahren leicht rückläufig war, zeigte sich einmal wieder, dass für viele Vereinsvertreter die datenschutzrechtlichen Vorgaben eine Herausforderung sind. Insbesondere in kleineren Vereinen wird es häufig zur Aufgabe eines einzelnen Vertreters gemacht, datenschutzrechtliche Versäumnisse der Vergangenheit im Alleingang auszuräumen.

In diesem Zusammenhang wird oftmals die Datenschutz-Grundverordnung (DSGVO) als Ursache allen Übels ausgemacht. Doch ein zweiter Blick bringt schnell zu Tage, dass wesentliche datenschutzrechtliche Vorgaben auch vor Inkrafttreten der DSGVO bereits Geltung hatten und daher bei konsequenter Beachtung dieser Regelungen in der Vergangenheit nunmehr lediglich ein überschaubarer Anpassungsbedarf bestanden hätte.

Neben der hohen Anzahl an Beratungsanfragen häuften sich nunmehr die Beschwerden Betroffener, die sich durch die von den Vereinen vorgenommene Datenverarbeitung in ihren Rechten verletzt sahen. Dies dürfte insbesondere auf ein steigendes datenschutzrechtliches Bewusstsein zurückzuführen sein und zeigt zugleich, dass rechtswidrige Datenverarbeitungen von den Betroffenen nicht mehr einfach hingenommen werden.

Oftmals lagen diesen Beschwerden die Nichtbeachtung von Betroffenenrechten, insbesondere von Auskunftsersuchen nach Art. 15 DSGVO, zugrunde. Nach dieser Regelung kann dem Grunde nach jede Person von einem Verein Auskunft darüber

verlangen, ob und wenn ja welche Daten zu welchen Zwecken über ihre Person verarbeitet werden. Diese Auskünfte sind von den Vereinen unverzüglich, spätestens aber innerhalb eines Monats zur Verfügung zu stellen (Art. 12 Abs. 3 DSGVO). In den meisten Beschwerdeverfahren hatten die Vereine im Zeitpunkt der Beschwerde überhaupt nicht reagiert und wurden erst nach Intervention durch die Aufsichtsbehörde tätig.

Unsere Dienststelle legt ihr Hauptaugenmerk aber weiterhin auf Aufklärungsarbeit und Beratung von Vereinsvertretern in datenschutzrechtlichen Fragestellungen. In erster Linie wird versucht, wesentliche Grundzüge des Datenschutzrechts zu vermitteln, um innerhalb der Vereine einen datenschutzkonformen Umgang etablieren zu können. Die Aufsichtsbehörde kann dabei erste Anlaufstelle sein. Geht es ins Detail, sind die Vereine selbst gefragt. Aufgabe der Aufsichtsbehörden ist es nämlich nicht, die Datenschutzerklärung auf der Vereinswebseite konkret auszuformulieren bzw. sonstige Datenverarbeitungsprozesse detailliert zu beschreiben. Sofern innerhalb des Vereins also das datenschutzrechtliche Know-how fehlt, muss im Zweifelsfalle fachkundiger Rat eingeholt werden.

4.19.1 Einsicht in die Mitgliederliste

Immer wieder wird an unsere Behörde die Frage gerichtet, unter welchen rechtlichen Voraussetzungen Einsicht in die Mitgliederliste eines Vereins genommen werden darf. So sind beispielsweise einzelne Vereinsmitglieder mit der Arbeit des Vorstands unzufrieden und wollen über ein Mitgliedervotum eine außerordentliche Mitgliederversammlung einberufen. Der Vorstand wiederum fürchtet, dass das unzufriedene Mitglied Stimmung gegen die Vereinsverantwortlichen machen will und verweigert dann die Einsichtnahme.

Dabei ist zu berücksichtigen, dass die einzelnen Mitglieder im Verhältnis zum Verein als Dritte anzusehen sind, da sie für den Verein keine Funktion wahrnehmen, welche die Kenntnisnahme der Mitgliederliste erfordern würde. Da in einer Mitgliederliste personenbezogene Mitgliederdaten wie der Name, die Anschrift, das Geburtsdatum sowie sonstige Angaben enthalten sind, bedarf die Einsichtnahme in diese Listen durch einzelne Mitglieder einer Rechtsgrundlage.

Bei der datenschutzrechtlichen Betrachtung ist insofern der Zweck der Einsichtnahme maßgebend. Beispielsweise bedarf ein Antrag auf Einberufung einer außerordentlichen Mitgliederversammlung im Regelfall der Unterstützung einer bestimmten Anzahl von Vereinsmitgliedern. Um für ihr Anliegen werben zu können und eine ausreichende Unterstützerzahl zu erreichen, sollte dem betreffenden Mitglied Einsicht in die Mitgliederliste gewährt bzw. die Adressliste überlassen werden. Aus datenschutzrechtlicher Sicht wäre diese Datenverarbeitung nach Art. 6 Abs. 1 lit. f DSGVO nicht zu beanstanden, da das Übermittlungsinteresse des Mitgliedes nachvollziehbar ist und nicht ersichtlich ist, weshalb die anderen Vereinsmitglieder ein überwiegendes Interesse daran haben sollten, dass ihre Daten in diesem Kontext nicht offenbart werden.

Es wird empfohlen, von den Mitgliedern, die Einsicht in die Unterlagen begehren, eine schriftliche Erklärung einzuholen, dass die Daten nur zu dem konkret bestimmten Zweck verarbeitet und nicht missbräuchlich genutzt werden. Auch darf Zugang nur zu Kontaktdaten gewährt werden, da beispielsweise die Bankdaten für die Zweckerreichung nicht erforderlich sind.

4.19.2 Anforderungen an Einwilligungserklärungen

Einwilligungserklärungen werden von Vereinsverantwortlichen gerne als Rechtsgrundlage für die Verarbeitung personenbezogener Daten herangezogen. Auch wenn mit der Einholung von Einwilligungserklärungen ein ungleich höherer Aufwand verbunden ist als bei anderen Rechtsgrundlagen, erhoffen sich die verantwortlichen Vereine hierdurch eine größere Rechtssicherheit, da der Betroffene schließlich selbst über seine personenbezogenen Daten entscheiden kann. Eine möglicherweise juristisch komplizierte Abwägung zwischen Verarbeitungsinteressen und schutzwürdigen Interessen der Betroffenen kann dann ausbleiben. Was dabei oftmals übersehen wird ist jedoch der Umstand, dass eine Einwilligung mit Wirkung für die Zukunft jederzeit widerrufen werden kann (Art. 7 Abs. 3 DSGVO). Einwilligungen sollten aus diesem Grund nur bei solchen Datenverarbeitungen eingeholt werden, für die keine andere Rechtsgrundlage in Betracht kommt. Für den Verein elementare Datenverarbeitungen, wie die Mitgliederverwaltung inkl. Beitragseinzug, ist die Einwilligung nicht zu empfehlen, da durch den Widerruf der Einwilligung die Mitgliederverwaltung einzustellen wäre. In diesem Zusammenhang wäre ohnehin zu hinterfragen, ob die Einwilligung überhaupt freiwillig abgegeben werden kann, da bei der Nichterteilung der Einwilligung das Mitgliedschaftsverhältnis nicht zustande kommen würde.

Auf die Möglichkeit des Widerrufs ist außerdem unmissverständlich und ausdrücklich hinzuweisen (Art. 7 Abs. 3 S. 3 DSGVO). In einem konkreten Beschwerdeverfahren hatte der Verein insgesamt vier verschiedene Datenverarbeitungsvorgänge in die Einwilligungserklärung aufgenommen, wies dann aber darauf hin, dass die Einwilligung lediglich zu einzelnen

Punkten widerrufen werden könne. Dies führte in ebenjenen Fällen zur Unwirksamkeit der Einwilligung und damit zur Rechtswidrigkeit der darauf gestützten Datenverarbeitung. Die Einwilligung wurde dahingehend angepasst und konnte im Nachgang rechtmäßig herangezogen werden.

4.19.3 Informationspflichten bei Ehrungen

Im Berichtszeitraum wollte ein Sportverband von uns eine rechtliche Einschätzung darüber erhalten, wie mit datenschutzrechtlichen Informationspflichten im Sinne der Art. 12 ff. DSGVO im Zusammenhang mit der Ehrung von verdienten Vereinsmitgliedern umzugehen sei. Stellt ein Mitgliedsverein des Sportverbandes einen Ehrungsantrag an den Verband, werden neben dem vollständigen Namen und der Anschrift die wesentlichen Verdienste dieser Person übermittelt. Hierbei stellte sich die Frage, ob und wie die zu ehrende Person durch den Verband über die sie betreffende Datenverarbeitung zu informieren ist.

Da der Sportverband die personenbezogenen Daten nicht direkt beim Betroffenen, sondern beim jeweiligen Verein, in dem der Betroffene Mitglied ist, erhebt, müsste er nach Art. 14 Abs. 1, Abs. 3 lit. a oder b DSGVO dem Betroffenen grundsätzlich innerhalb eines Monats nach der Datenübermittlung oder zum Zeitpunkt der ersten Kommunikation mit der betroffenen Person u.a. mitteilen, für welchen Zweck und von welcher Stelle er die Daten erhoben hat. Dies würde nach Ansicht des Verbandes jedoch den gewünschten Überraschungseffekt der Ehrung zunichtemachen.

Nach Einschätzung des Verbandes könnte die Information der betroffenen Person durch den Mitgliedsverband nach Art. 14

Abs. 5 lit. c DSGVO in Verbindung mit § 29 Abs. 1 Bundesdatenschutzgesetz (BDSG) unterbleiben. Hiernach bestehe die Pflicht zur Information insbesondere dann nicht, soweit durch ihre Erfüllung Informationen offenbart würden, die ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Vorliegend überwiege das Geheimhaltungsinteresse des Mitgliedsverbandes, nämlich die betroffene Person mit der Ehrung überraschen zu können, das Interesse der betroffenen Person, über die Datenverarbeitung gemäß Art 14 DSGVO informiert zu werden. Insbesondere würden nur die von der betroffenen Person im sozialen Raum bereits bekannten personenbezogenen Daten weitergegeben und vom Mitgliedsverband für die Ehrung verwendet.

Dieser Auffassung konnten wir uns nicht anschließen, da dieser Auslegung ein unzutreffendes Verständnis der Vorschriften des Art. 14 Abs. 5 lit. c DSGVO und des § 29 Abs. 1 BDSG zugrunde liegt.

Nach Art. 14 Abs. 5 lit. c DSGVO entfallen die Informationspflichten des Art. 14 DSGVO, wenn eine Rechtsvorschrift die Erhebung oder zweckändernde Offenlegung bestimmter Daten ausdrücklich regelt, da dann die betroffene Person anhand einer solchen Rechtsvorschrift einen hinreichenden Überblick über die Datenverarbeitung erlangen kann. Eine solche ausdrückliche Rechtsvorschrift zur Erhebung von Daten durch den Verband zum Zwecke der Ehrung existiert nicht.

Auch die in Bezug genommene Vorschrift des § 29 Abs. 1 BDSG, die auf Art. 23 Abs. 1 lit. i DSGVO beruht, kann in dem Fall einer Ehrung durch einen Verband die Informationspflichten nicht entfallen lassen. Es ergibt sich bereits aus der Formulierung der

Vorschrift, dass ihr Anwendungsbereich sehr eng auszulegen ist und das Geheimhaltungsinteresse das Informationsbedürfnis deutlich überwiegen muss. Allein die Ermöglichung eines Überraschungseffekts oder die Verhinderung eines Gefühls von Enttäuschung haben kein derart großes Gewicht, so dass die Abwägung zwischen den widerstreitenden Interessen eindeutig zu Lasten des Verbandsinteresses ausfällt.

Auch kann die Information nicht im Hinblick auf die Regelung des Art. 14 Abs. 5 lit. b S. 1 Hs. 2 Alt. 2 DSGVO unterbleiben. Nach dieser Vorschrift gelten die Vorgaben für die Informationspflichten auch dann nicht, wenn die Erteilung der Informationen voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt. Ziel der Verarbeitung ist die Ehrung eines Mitglieds durch den Dachverband, wobei das Mitglied von der Ehrung überrascht werden soll. Die Ehrung als solche wäre durch die Erteilung der Information keineswegs gefährdet, sondern allenfalls das Überraschungsmoment, der allerdings nur einen Nebenzweck darstellt. Dass bereits Nebenzwecke der eigentlichen Verarbeitung zu einem Ausschluss der Informationspflichten führen sollen, würde der Bedeutung der Informationspflichten nicht gerecht werden.

Daneben finden nach Art. 14 Abs. 5 lit. a DSGVO die Vorschriften über die Informationspflichten bei der Dritterhebung keine Anwendung, wenn die betroffene Person bereits über die Information verfügt. Die Vorschrift entspricht der Ausnahme in Art. 13 Abs. 4 DSGVO und setzt eine positive Kenntnis voraus und nicht lediglich eine Prognose. Da nach Art. 14 DSGVO der Sportverband Adressat der Informationspflichten ist und dieser darüber aufzuklären hat, welche Datenkategorien er bei wem und zu

welchem Zweck erhoben hat, müssten diese Informationen der betroffenen Person bereits vor dem Zeitpunkt der Übermittlung vorliegen, um gemäß Art. 14 Abs. 5 lit. a DSGVO nicht nachträglich informieren zu müssen. Eine frühzeitige Information, beispielsweise in Form eines Datenschutzhinweises, welcher an alle angeschlossenen Mitglieder versendet wurde, ist seitens des Sportverbandes in dem uns vorgelegten Fall jedoch nicht erfolgt.

Im Ergebnis konnte sich der Sportverband auf keine Ausnahmevorschrift berufen und war verpflichtet, von der Datenverarbeitung betroffene Personen umfassend über diese zu informieren.

4.20 Datenschutzrechtliche Bewertung telefonischer Werbeansprachen

Bereits im 27. Tätigkeitsbericht unserer Behörde[55] wurde eine Beschwerde eines Betroffenen über unverlangte Werbeanrufe durch ein Versicherungsunternehmen dargestellt, welche eine Anordnung unserer Dienststelle zur Folge hatte.

Das Versicherungsunternehmen machte als Rechtsgrundlage eine im Rahmen eines Online-Gewinnspiels erteilte Einwilligung des Betroffenen nach Art. 6 Abs. 1 lit. a Datenschutz-Grundverordnung (DGSVO) geltend. Der Betroffene habe in einem Online-Formular neben seinem Namen und der Adresse auch seine Telefonnummer eingetragen und eine Checkbox angekreuzt, wonach er mit postalischer und telefonischer Werbung einverstanden sei. Zudem sei dem Betroffenen eine E-Mail an die eingetragene Adresse mit der Bitte um Bestätigung der Teilnahme

[55] Elektronisch abrufbar unter: https://www.datenschutz.saarland.de/ueber-uns/taetigkeitsberichte

gesendet worden, woraufhin eine solche Bestätigung durch Anklicken des in der Mail angegebenen Links erfolgt sei (sog. Double-opt-in-Verfahren).

Wir sahen hingegen eine Einwilligung nach Art 6 Abs. 1 lit. a DSGVO als nicht nachgewiesen an und verwiesen u.a. auf eine Entscheidung des Bundesgerichtshof (BGH) vom 10. Februar 2011 (Az. I ZR 164/09), wonach nicht zwingend von einem Zusammenhang zwischen der in einem Online-Formular eingetragenen E-Mail-Adresse und der angegebenen Telefonnummer ausgegangen werden könne. Daher sei das Double-opt-in-Verfahren nicht zum Nachweis einer in dem zu Grunde liegenden Fall zu prüfenden Einwilligung in Werbeanrufe geeignet.

Da auch keine andere Rechtsgrundlage – insbesondere nicht Art. 6 Abs. 1 lit. f DSGVO – gegeben war, wurde dem Unternehmen die Verarbeitung personenbezogener Daten für Zwecke des telefonischen Direktmarketings untersagt, soweit diese über Online-Gewinnspiele generiert werden und keine nachgewiesene Einwilligung der hiervon betroffenen Personen vorliegt. Die Löschung dieser Daten wurde ergänzend verfügt.

Hiergegen erhob das Versicherungsunternehmen Klage beim Verwaltungsgericht des Saarlandes und machte geltend, entsprechende Einwilligungen zur telefonischen Werbeansprache würden vorliegen. Aus Sicht des klagenden Unternehmens seien die in der Rechtsprechung entwickelten strengen Anforderungen an den Nachweis einer wettbewerbsrechtlichen Einwilligung nach § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG) nicht auf eine datenschutzrechtliche Einwilligung im Sinne des Art. 6 Abs. 1 lit. a in Verbindung mit Art. 4 Nr. 11 DSGVO übertragbar. Die DSGVO dürfe mithin nicht derart aus-

gelegt werden, dass eine telefonische Direktwerbung ausschließlich mit ausdrücklicher Einwilligung erlaubt sei, diese sei mithin aufgrund des berechtigten Interesses nach Art. 6 Abs. 1 lit. f DSGVO zulässig.

Das Verwaltungsgericht des Saarlandes wies die Klage mit Urteil vom 29. Oktober 2019 (Az. 1 K 732/19) ab und folgte unserer Rechtsauffassung, wonach das Double-opt-in keine geeignete Möglichkeit darstellt, eine Einwilligung in die Nutzung der erlangten Telefonnummer zu Werbeanrufen durch den Anschlussinhaber nachzuweisen, so dass sich das verantwortliche Unternehmen nicht auf eine Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO berufen kann.

Das Gericht sieht auch die Rechtsgrundlage des Art. 6 Abs. 1 lit. f DSGVO nicht anwendbar, weil Art. 13 Abs. 3 der Richtlinie 2002/58/EG (ePrivacy-Richtlinie) (ebenso wie die in Vorbereitung befindliche Verordnung) eine eindeutige Regelung im innerstaatlichen Recht vorsehe, wonach telefonische Direktwerbung entweder dann verboten ist, wenn keine Einwilligung der betreffenden Person vorliegt oder dann, wenn die betreffende Person es abgelehnt hat, zu Werbezwecken angerufen zu werden. Durch die verbindliche Vorgabe dieser beiden Möglichkeiten zur Umsetzung des unionsrechtlichen Schutzes komme eine Interessenabwägung als Rechtsgrundlage nicht in Betracht.

Es sei auch kein Vorrang der DSGVO gegenüber der ePrivacy-Richtlinie ersichtlich, der eine andere Bewertung rechtfertigen würde. Das Verwaltungsgericht stellt weiterhin klar, dass – auch wenn man eine Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO für anwendbar hielte – es an einem berechtigten Interesse mangele, weil ein solches nur im Falle von legalen Interes-

sen angenommen werden könne. Dies sei vorliegend abzulehnen, weil die gegenständliche Werbeansprache in Widerspruch zur ePrivacy-Richtlinie stehe.

Fazit/Empfehlung:

Die Verwendung der Telefonnummer zur telefonischen Werbeansprache bedarf einer Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO in Verbindung mit Art. 4 Nr. 11 DSGVO . Das Double-opt-in-Verfahren ist nicht geeignet zum Nachweis einer solchen Einwilligung.

4.21 Einsicht in die Patientenakte

Im Gesundheitsbereich werden naturgemäß sehr sensible personenbezogene Daten verarbeitet. Daher ist es vielen Patienten ein wichtiges Anliegen, über den Inhalt der Behandlungsdokumentation, also ihrer Patientenakte, informiert zu sein. Immer wieder wenden sich Patienten an das Unabhängige Datenschutzzentrum Saarland und bitten um Unterstützung, weil ihr behandelnder Arzt keine Einsicht in die Patientenakte gewähren will oder sich weigert, eine Kopie der Akte zur Verfügung zu stellen. Dabei existieren mehrere Rechtsvorschriften, auf die sich ein entsprechender Anspruch des Patienten stützen lässt.

So enthält zum einen das Bürgerliche Gesetzbuch (BGB) mit § 630g eine Regelung, die einen Anspruch auf Einsicht in die Patientenakte und auf Erhalt elektronischer Abschriften der Akte im Rahmen des Behandlungsvertrags zwischen Behandelndem und Patient begründet.

Auch § 10 Abs. 2 der Berufsordnung für die Ärztinnen und Ärzte des Saarlandes verpflichtet den Arzt berufsrechtlich dazu, dem Patienten Einsicht in die Behandlungsdokumentation zu gewähren und auf Verlangen Kopien herauszugeben.

Für Krankenhäuser im Saarland existiert mit § 13 Abs. 7 Saarländischen Krankenhausgesetz (SKHG) zudem eine spezialgesetzliche Regelung, die dem Patienten ein Recht auf kostenfreie Auskunft über die gespeicherten persönlichen Daten sowie die Möglichkeit der Einsichtnahme in die Behandlungsdokumentation der Klinik einräumt.

Hinzu kommt seit dem Wirksamwerden der Datenschutz-Grundverordnung (DSGVO) der allgemeine Auskunftsanspruch, den gemäß Art. 15 DSGVO jede von einer Datenverarbeitung betroffene Person gegenüber dem Verantwortlichen hat.

Während die Vorschriften aus Berufsordnung und SKHG inhaltlich § 630g BGB ähneln, unterscheiden sich die BGB-Vorschrift und Art. 15 DSGVO insbesondere in zwei Aspekten:

- Während § 630g Abs. 2 BGB es dem Arzt erlaubt, dem Patienten die Kosten für die Kopie seiner Akte in Rechnung zu stellen, normiert Art. 15 Abs. 3 DSGVO einen Anspruch auf eine erste kostenfreie Kopie.
- § 630g Abs. 1 BGB schränkt den Anspruch ein für den Fall, dass erhebliche therapeutische Gründe einer (vollständigen) Einsichtnahme entgegenstehen. Eine vergleichbare Beschränkung des Auskunftsanspruchs nach Art. 15 DSGVO existiert dagegen nicht.

In welchem Verhältnis § 630g BGB und Art. 15 DSGVO zueinander stehen, wird von den datenschutzrechtlichen Aufsichtsbehörden unterschiedlich beurteilt.

Das Unabhängige Datenschutzzentrum Saarland stellt derzeit bei der Bearbeitung von Anfragen oder Beschwerden in diesem Zusammenhang darauf ab, welches Anliegen der betroffene Patient im konkreten Fall verfolgt. Geht es dem Patienten vorrangig um die Verarbeitung seiner personenbezogenen Daten (z.B. Empfänger, Speicherdauer), kann von einem Auskunftsersuchen nach Art. 15 DSGVO ausgegangen werden. Steht dagegen der Inhalt des Behandlungsverlaufs im Vordergrund, wie beispielsweise in Fällen, in denen der Patient seine Akte bei einem Wechsel der Praxis zum neuen Arzt mitnehmen möchte und deshalb eine vollständige Kopie benötigt, erscheint § 630g BGB als einschlägige Rechtsgrundlage, zumal der Umfang der Datenkopie, die nach Art. 15 Abs. 3 DSGVO verlangt werden kann, nach wie vor umstritten ist.

Fazit/Empfehlung:

Patienten haben ein Recht darauf, ihre Behandlungsakte einzusehen und eine Kopie davon zu erhalten. Der Anspruch kann nur in Ausnahmefällen abgelehnt werden.

5.1 Durchführung von Vor-Ort-Prüfungen
5.2 Prüfung Rechenschaftspflichten bei Großunternehmen
5 3 Prüfung Body-Cam

V.

Ausgewählte Prüfungen

5 Ausgewählte Prüfungen

5.1 Durchführung von Vor-Ort-Prüfungen

Im Berichtszeitraum wurden von unserer Dienststelle mehrere Prüfungen zum Beschäftigtendatenschutz durchgeführt. Meist sind die Prüfungen anlassbezogen, das heißt wir haben aus dem Kreise der Beschäftigten des zu prüfenden Unternehmens einen Hinweis auf datenschutzrechtliche Verstöße erhalten. Dabei ist im Vorfeld eine Vor-Ort-Prüfung abzuwägen, ob wir uns bei dem zu prüfenden Unternehmen anmelden oder nicht. Besteht die Gefahr, durch die Ankündigung der Prüfung den behaupteten datenschutzrechtlichen Verstoß nicht mehr überprüfen zu können, wird der Kontrollbesuch ohne vorherige Ankündigung durchgeführt.

Im Vorfeld der Prüfung werden durch die beteiligten Mitarbeiter des Unabhängigen Datenschutzzentrums Saarland der genaue Prüfgegenstand, der Prüfablauf und die Aufgabenverteilung festgelegt.

So stellen wir uns und unser Anliegen zunächst vor Ort vor, überreichen Hinweisblätter zu unseren Befugnissen und kommen unserer Informationsverpflichtung nach Art. 13 Datenschutz-Grundverordnung (DSGVO) nach.

Gem. Art. 58 Abs. 1 S. 1 lit. e und f DSGVO in Verbindung mit § 40 Abs. 5 Bundesdatenschutzgesetz (BDSG) haben die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen der zuständigen Aufsichtsbehörde Zugang zu den Räumlichkeiten, einschließlich aller Datenverarbeitungsanlagen und -geräte sowie Zugang zu allen personenbezogenen

Daten und Informationen zu gestatten, die zur Erfüllung der Aufgaben der Aufsichtsbehörde erforderlich sind.

Nachdem der Prüfungsablauf mit den Verantwortlichen vor Ort abgesprochen ist, wird zunächst auf die formellen Anforderungen der DSGVO Bezug genommen und in der Regel die Vorlage des Verzeichnisses der Verarbeitungstätigkeit gem. Art. 30 DSGVO, das Vorliegen einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO oder zumindest einer Risikobewertung, die getroffenen technisch-organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten gem. Art. 32 DSGVO, die Gewährleistung der Betroffenenrechte, vorgegebene Löschfristen etc. durch uns angefordert. Nach Sichtung des formellen Teils wird der konkrete Anlass der Prüfung in Augenschein genommen. So haben wir beispielsweise ein GPS-System, das eine Überwachung von Beschäftigten ermöglicht, oder ein hausinternes Informationssystem, das benutzt wurde, um die Leistung der jeweiligen Mitarbeiter im Haus vergleichbar zu machen, überprüft. Dabei lassen wir uns vom Ansprechpartner vor Ort die Funktionsweise und die technischen Auswertungsmöglichkeiten erörtern und stellen gezielte Nachfragen, um zu einer ersten Einschätzung gelangen zu können, ob die getroffenen Maßnahmen datenschutzkonform sind.

Noch vor Ort erstellen wir eine Kurzzusammenfassung der Prüfung und erörtern diese mit den Verantwortlichen.

Im Anschluss an die Prüfung erfolgt die datenschutzrechtliche Auswertung durch das Prüfteam sowie die Erstellung eines Prüfberichts, der den Ablauf der Prüfung widerspiegelt und datenschutzrechtliches Verbesserungspotential aufzeigt.

Der Prüfbericht wird dem Verantwortlichen des Unternehmens mit der Gelegenheit zur Stellungnahme zugesandt. Wurden bei der Prüfung datenschutzrechtliche Verstöße festgestellt, werden in der Regel Abhilfemaßnahmen nach Art. 58 Abs. 2 DSGVO ergriffen, um datenschutzrechtliches Fehlverhalten zukünftig abzustellen. Zur Prüfung, ob zusätzlich zu oder anstelle von solchen Maßnahmen eine Geldbuße zu verhängen ist, erfolgt erforderlichenfalls eine Abgabe an unsere Bußgeldstelle.

5.2 Prüfung Rechenschaftspflichten bei Großunternehmen

Die Rechenschaftspflicht ist eines der gewichtigsten und umfangreichsten Gebote der Datenschutz-Grundverordnung (DSGVO). [56] Die Rechenschaftspflicht hat dabei zwei Bestandteile:

1. die Pflicht zur Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 DSGVO) und

2. den Nachweis, dass der Verantwortliche diese Pflicht befolgt (Art. 5 Abs. 2 DSGVO).

Der Nachweis wird mittels einer Dokumentation geführt, für die es zwar keine bestimmte Form gibt, die jedoch an verschiedenen Stellen der DSGVO konkretisiert wird. Beispiele für die erweiterten Dokumentationspflichten sind etwa das Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO mit erweiterten Dokumentationspflichten nach Art. 30 Abs. 1 S. 2 und Abs. 2 sowie Abs. 3 DSGVO), die Meldung von Datenschutzverletzungen (Art. 33 DSGVO mit erweiterten Dokumentationspflichten

[56] *Jaspers/Schwartmann/Hermann*, in: Schwartmann/Jaspers/Thüsing/Kugelmann (2018), DS-GVO/BDSG, Art. 5 Rn. 72 ff.

nach Art. 33 Abs. 5 DSGVO) oder die Datenschutz-Folgeabschätzung (Art. 35 DSGVO mit erweiterten Dokumentationspflichten nach Art. 35 Abs. 7 DSGVO).

Die Aufsichtsbehörden haben wiederum nach Art. 57 Abs. 1 lit. a DSGVO die Aufgabe, die Anwendung der DSGVO zu überwachen und durchzusetzen, wobei die Überwachung der DSGVO nicht nur die konkrete Kontrolle von Datenverarbeitungsvorgängen meint, sondern auch die Einhaltung der datenschutzrechtlichen Vorschriften im Allgemeinen, wie zum Beispiel die Erfüllung der Rechenschaftspflichten.

Zudem haben die Aufsichtsbehörden nach Art. 57 Abs. 1 lit. h DSGVO die Aufgabe, die Untersuchungen über die Anwendung der DSGVO durchzuführen. Damit ist auch eine präventive Kontrolle von Amts wegen gemeint.

Schlussendlich liegt es nach Art. 57 Abs. 1 lit. d DSGVO auch im Aufgabenbereich der Aufsichtsbehörden die Verantwortlichen für die ihnen auferlegten Pflichten zu sensibilisieren. Dies meint, dass die Aufsichtsbehörden frühzeitig aufklären und auf eine datenschutzkonforme Verarbeitung hinwirken.

Vor dem Hintergrund dieser Aufgabenbereiche der zuständigen Aufsichtsbehörden hatte das Unabhängige Datenschutzzentrum, nachdem die DSGVO sechs Monate anwendbar war, insgesamt drei der größten saarländischen Unternehmen einen Fragekatalog mit 50 Einzelfragen zu insgesamt sechs Teilbereichen der Rechenschaftspflicht zugesandt.

Ziel dieser anlasslosen Prüfung war es zunächst, festzustellen, wie der Stand der Umsetzung der Vorgaben der DSGVO nach

sechsmonatiger Anwendung ist und inwieweit die Unternehmen den Nachweis für die Einhaltung der gesetzlichen Anforderungen erbringen können.

Es handelte sich insoweit um eine anlasslose Querschnittsprüfung mit folgenden wesentlichen Ergebnissen in den abgefragten Themenkomplexen:

Der erste Themenkomplex stellte auf das Grundkonzept der datenschutzrechtlichen Umsetzung (insbesondere Art. 24 DSGVO) und die Einbindung des Datenschutzbeauftragten ab (Art. 37ff DSGVO) ab. Dies kann bei großen Organisationseinheiten mit sehr vielen Mitarbeitern in den verschiedenen Unternehmensbereichen und/oder mehreren Standorten bzw. Niederlassungen durchaus problematisch werden. Allerdings zeigten sich hierbei wenige Defizite.

Der zweite Themenkomplex betraf das Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO). Da dieses alle Verarbeitungstätigkeiten beinhalten soll, bildet es das Herzstück eines jeden Datenschutzmanagementsystems. Das Verzeichnis der Verarbeitungstätigkeiten soll beispielsweise die Zwecke der Verarbeitung (Rechtsgrundlage), Kategorien betroffener Personen und personenbezogener Daten sowie eventuelle Datenübermittlungen und die dazugehörigen Empfänger enthalten, aber auch Löschfristen für Datenkategorien. Bei diesem Themenkomplex haben sich erste Schwächen offenbart. Offensichtlich war nicht ganz klar, was konkret unter einer Verarbeitungstätigkeit zu verstehen ist. Der Begriff Verarbeitungstätigkeit orientiert sich an dem Zweck, zu dem eine Verarbeitungstätigkeit durchgeführt wird. Hier reichte die Spannweite von 5 bis zu 139 Verarbeitungstätigkeiten, wobei bei lediglich fünf angegebenen Verarbeitungstätigkeiten angesichts der Größe der geprüften

Unternehmen davon ausgegangen werden konnte, dass das Verzeichnis nicht vollständig war.

Der dritte Themenkomplex betraf das einheitliche Risikomodell. Die DSGVO verfolgt einen risikobasierten Ansatz, d.h. der Verantwortliche muss bei seiner Datenverarbeitung eigenverantwortlich Risiken für die Rechte und Freiheiten natürlicher Personen berücksichtigen (z.B. Art. 24 Abs. 1, Art. 25 Abs.1, Art. 32 bis 36 DSGVO). Hier stand bereits zu befürchten, dass die Abgrenzung zu Unternehmensrisiken schwer fällt. Dies hängt damit zusammen, dass dieser Ansatz im Rahmen des Datenschutzes neu ist. Bisher hat man sowohl aus technischer als auch aus betriebswirtschaftlicher Sicht immer das Risiko für das Unternehmen betrachtet. Nunmehr muss man im Prinzip die gleichen Instrumente auf die Rechte und Freiheiten betroffener Personen anwenden, wobei das bereits seit langem bekannte Unternehmensrisiko an dieser Stelle eben keine Rolle spielt.

Der größte Themenkomplex betraf die datenschutzkonforme Verarbeitung von personenbezogenen Daten. Hier war zu erwarten, dass es aufgrund der Vielzahl unbestimmter Rechtsbegriffe in der DSGVO zu Schwierigkeiten kommt. Vor allem die datenschutzrechtlichen Themen Einwilligung, Datenschutz-Folgeabschätzung, Löschkonzept sowie technisch und organisatorische Maßnahmen bereiteten die meisten Probleme.

Die DSGVO sieht vor, dass die Verarbeitung personenbezogener Daten untersagt ist, es sei denn, es liegt eine Legitimationsgrundlage vor (Art. 6 Abs. 1 S. 1 DSGVO). Die Einwilligung (Art. 4 Nr. 11 DSGVO) ist eine Möglichkeit die Verarbeitung von personenbezogenen Daten zu legitimieren (Art. 6 Abs. 1 S. 1 lit. a DSGVO). Allerdings ist deren Umsetzung aufgrund gesetzlicher

Vorgaben (u.a. Art. 7 DSGVO) nicht einfach zu handhaben. Zudem hat sich gezeigt, dass die Abgrenzung zu anderen Legitimationsgrundlagen, wie etwa die Datenverarbeitung aufgrund eines Vertrages (Art. 6 Abs. 1 S. 1 lit. b DSGVO), schwerfällt.

Die Datenschutz-Folgenabschätzung (Art. 35 DSGVO) ist ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten betroffener Personen. Sie ist zwingend durchzuführen, wenn voraussichtlich ein hohes Risiko besteht. Die Feststellung, ob voraussichtlich ein hohes Risiko vorliegt, ist offensichtlich nicht immer einfach. Bei dieser sog. Schwellwertanalyse werden Eintrittswahrscheinlichkeit und Schwere der potentiellen Schäden betrachtet. Die Bestimmung der Eintrittswahrscheinlichkeit anhand pauschaler Eintrittszyklen ist aber ohne weitere Erwägungen nicht ausreichend.

Bei der Erstellung eines Löschkonzepts ist zu berücksichtigen, dass Daten nur solange gespeichert werden dürfen, wie dies für den Zweck der Verarbeitung notwendig ist (Art. 5 Abs. 1 lit. e DSGVO, ErwG 39). Dabei sind aber auch Aufbewahrungspflichten, etwa aus dem Steuer- und Handelsrecht zu beachten (§ 257 Abs. 1 Nr. 1 Handelsgesetzbuch [HGB] und § 147 Abs. 1 Nr. 2 bis 4, Abs. 3 Abgabenordnung [AO] bzw. § 14b Umsatzsteuergesetz [UStG]). Daher ist die Erstellung eines solchen schematischen Löschkonzeptes komplex.

Unter die von den Verantwortlichen zu ergreifenden technischen und organisatorischen Maßnahmen nach Art. 24 f. und 32 DSGVO fallen Fragen der Sicherheit personenbezogener Daten. Hierzu gibt es zahlreiche ISO-Normen, deren Umsetzung zwar auch aus Sicht der IT-Sicherheit geboten, aber ebenfalls nicht trivial ist. Folglich ergaben sich hier ernsthafte Schwierigkeiten.

Bei dem fünften Themenkomplex, dem Umgang mit Betroffenenrechten (Art. 12 ff. DSGVO), also z.B. Information der betroffenen Personen bei Datenerhebung oder Erteilung von Auskünften aufgrund von Anfragen betroffener Personen, zeichnete sich ein deutlich positiveres Bild. Auch dies war abzusehen, da gerade Großunternehmen unmittelbar mit der Ausübung von Betroffenenrechten konfrontiert waren. Lediglich bei den Datenschutzerklärungen auf den Webseiten zeigten sich Schwächen.

In dem letzten Themenkomplex, dem Umgang mit Datenschutzverletzungen nach Art. 33 f. DSGVO, hat offensichtlich die Meldepflicht dazu geführt, dass man sich schon im Vorfeld einiges an Gedanken gemacht hat. Bei der Verarbeitung von personenbezogenen Daten kann es immer wieder zu Datenpannen kommen. Entweder durch Hackerangriffe oder einfach nur aufgrund von Versehen einzelner Mitarbeiter können personenbezogene Daten abhandenkommen und/oder verloren gehen. Wenn dies der Fall ist, muss unverzüglich, spätestens aber binnen einer Frist von 72 Stunden eine Meldung bei der zuständigen Aufsichtsbehörde und bei hohen Risiken auch der betroffenen Personen erfolgen. Diese 72-Stunden-Frist (Art. 33 Abs. 1 S. 1 DSGVO) bereitet offenbar Kopfzerbrechen, vor allem was die Berechnung der Frist und die Maßnahmen zu deren Einhaltung betrifft.

Im Ergebnis kann man festhalten, dass das Gesamtbild differenziert zu betrachten ist. Dies war zum Teil aber auch nicht anders zu erwarten. Auch nach der zweijährigen Übergangszeit waren viele Fragen offen und der Umgang mit den auslegungsbedürftigen Vorschriften schwierig. Daher war das Ziel der Prüfung

folglich nicht, Verstöße festzustellen und zu sanktionieren, sondern den Stand der Umsetzung festzustellen und an problematischen Stellen die verantwortlichen Unternehmen insoweit zu sensibilisieren, dass diese die von uns erkannten Problembereiche ernsthaft angehen müssen. Außerdem sind seitens der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) weitere Publikationen und damit weitere Hilfestellungen geplant. Einige strittige Fragen werden sich aber erst klären, wenn hierzu höchstrichterliche Rechtsprechung vorliegt.

5.3 Prüfung Body-Cam

Im Jahre 2016 wurde im Saarländischen Polizeigesetz (SPolG) eine Rechtsgrundlage für den Einsatz von Video- und Tontechnik zum Schutz der Beamten geschaffen (Gesetz Nr. 1889 zur Änderung des Saarländischen Polizeigesetzes vom 18. Mai 2016, Amtsbl. 2016, 440). Die Vollzugspolizei kann nunmehr nach § 27 Abs. 3 SPolG in öffentlich zugänglichen Räumen personenbezogene Daten kurzzeitig speichern (Vorabaufnahme) und durch die offene Anfertigung von Bild- und Tonaufzeichnungen erheben, soweit dies zum Schutz von Polizeivollzugsbeamtinnen oder Polizeivollzugsbeamten oder Dritten zur Abwehr einer konkreten Gefahr erforderlich ist. Auf entsprechende Maßnahmen ist durch Schilder oder in sonstiger geeigneter Form hinzuweisen. In § 27 Abs. 6 SPolG ist zudem bestimmt, dass die im Rahmen einer solchen Maßnahme getätigten Aufzeichnungen, soweit sie nicht zur Verfolgung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung erforderlich sind, unverzüglich zu löschen sind.

Die Formulierung „Vorabaufnahme“ soll laut Gesetzesbegründung ermöglichen, dass eine Bildaufzeichnung für einen definierten Zeitraum bereits vor einer manuellen Aufzeichnungsauslösung, also anlasslos, verfügbar gehalten wird. Erst bei manueller Auslösung der Aufzeichnung bei einer konkreten Gefährdungssituation wird in der Folge dann das kurze Zeitfenster der Vorabaufnahme endgültig mitgespeichert. Diese Funktion soll den Polizeibeamten vor Ort die Möglichkeit geben, bereits das Entstehen einer Gefahrensituation zu dokumentieren. Zwar lässt das Gesetz durch die Verwendung des Begriffs „kurzzeitig“ offen, wie lange der Zeitraum der Vorabaufnahme (oder auch Pre-Recording) zulässigerweise sein darf. In der Errichtungsanordnung des Landespolizeipräsidiums wurde jedoch für diese Pre-Recording-Funktion eine Dauer von nicht mehr als 30 Sekunden als Höchstfrist festgelegt. Ebenso ergibt sich aus der Gesetzesbegründung, dass im Rahmen der Vorabaufnahme im Gegensatz zur nachfolgenden Aufnahme nur Bild- und nicht auch Tonaufnahmen zulässig sind.

Auf der Grundlage dieser neuen Befugnis werden durch die saarländische Polizei vornehmlich im Wach- und Streifendienst sog. Body-Cams eingesetzt. Eine Body-Cam oder Körperkamera ist eine kleine Filmkamera, die nah am Körper, meist im Schulterbereich, getragen wird. Mit ihr können Bild- und Tonaufzeichnungen des unmittelbaren Umfelds ihres Trägers gefertigt werden.

Die Bedienung der Kamera selbst ist hierbei relativ einfach. Mit dem Einschalten der Kamera muss der einsetzende Polizeibeamte allerdings auch die tatsächliche Gefahrenlage einschätzen. Er muss dabei bewerten, ob der Einsatz der Kamera in ihrer relativ hohen Eingriffsintensität für den Betroffenen mit Bild- und

Tonaufzeichnung, auch gegenüber anderen polizeilichen Einsatzmitteln verhältnismäßig ist. Darüber hinaus muss er die Person, die aufgezeichnet werden soll, laut und deutlich auf das Einschalten der Body-Cam hinweisen. Nach Rückkehr in die Dienststelle sind die Aufnahmen von der Body-Cam mit Hilfe einer speziellen Bearbeitungs-, Verwaltungs- und Archivierungssoftware zu exportieren. Der Datenexport gewährleistet die gleichzeitige Löschung der Daten auf der Kamera selbst. Sodann sind die exportierten Daten hinsichtlich ihrer strafrechtlichen Relevanz zu sichten und zu bewerten.

Darüber hinaus ist aus datenschutzrechtlicher Sicht ebenso bedeutsam, dass durch einen landesweiten Einsatz im bürgernahen Alltagsgeschäft der Polizeibeamten auch davon ausgegangen werden muss, dass eine Vielzahl nichtbeteiligter Personen ohne ihr Wissen aufgezeichnet werden.

Mithin hielten wir es aufgrund der uns gesetzlich zugewiesen Verpflichtung, die Einhaltung der datenschutzrechtlichen Bestimmungen zu überwachen, nach Einsatz eines mehr als einjährigen landesweiten Wirkbetriebes für geboten, eine stichprobenartige Prüfung durchzuführen. Schwerpunkte der Prüfung sollten die Einhaltung der festgelegten technischen und organisatorischen Maßnahmen, insbesondere die Umsetzung der Hinweispflichten an die Betroffenen bei Aufzeichnung, die Einhaltung der Speicherbegrenzungen und Speicherfristen und die Umsetzung und Nachvollziehbarkeit von Datenexporten sein.

Das Ergebnis der Prüfung von Body-Cam-Aufzeichnungen im öffentlich-zugänglichen Bereich zeigt auf, dass schon bei der Umsetzung der technisch-organisatorischen Maßnahmen erhebliche Defizite zu Tage getreten sind. In vielen Fällen konnte nicht mehr festgestellt werden von welchem Polizeibeamten die

Aufnahmen getätigt wurden. Speicherfristen wurden nicht eingehalten und in erheblichem Maß überschritten, Datenexporte waren zum Teil nicht nachvollziehbar.

Mit der Regelung für den Betrieb von Körperkameras im Landespolizeipräsidium wurde dem Polizeibeamten ein hohes Maß an Eigenverantwortung nicht nur für die Erstellung einer zulässigen Body-Cam-Aufzeichnung, sondern auch für die zulässige weitere Datenverarbeitung übertragen. Aus hiesiger Sicht sollte zumindest hinsichtlich der weiteren Datenverarbeitung nach Rückkehr des Polizeibeamten in die Dienststelle eine deutliche Entlastung durch automatisierte systemseitige Lösungen herbeigeführt werden.

Anlagenverzeichnis

Anhang 1: Verzeichnis der Rechtsgrundlagen

BDSG – Bundesdatenschutzgesetz: Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das durch Artikel 12 des Gesetzes vom 20. November 2019 (BGBl. I S. 1626) geändert worden ist.

BGB – Bürgerliches Gesetzbuch: neugefasst durch Bek. v. 2.1.2002 I 42, 2909; 2003, 738; zuletzt geändert durch Art. 1 G v. 21.12.2019 I 2911

DSGVO – Datenschutz-Grundverordnung: Verordnung (EU) 2016/679 des Europäischen Parlamentes 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. ABI. Nr. L 314, S. 72 und ABI. 2018 Nr. L 127, S. 2).

ePrivacy-Richtlinie: 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 Kommunikation (Abl. L 201 S. 37), zuletzt geändert durch Art. 2 ÄndRL 2009/136/EG vom 25.11.2009 (ABl. L 337 S. 11, ber. 2013 ABl. L 241 S. 9, ber. 2017 ABl. L 162 S. 56).

JI-RL – JI-Richtlinie: 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 (Amtbl. EU L 119/89).

JVollzDSG – Justizvollzugsdatenschutzgesetz: Saarländisches Justizvollzugsdatenschutzgesetz vom 4. Dezember 2019 (Amtsblatt I 2020, S. 79)

PaßG – Paßgesetz: Paßgesetz vom 19. April 1986 (BGBl. I S. 537), zuletzt geändert d. Gesetz v. 7. Juli 2017 (BGBl. I S. 2310)

SDSG – Saarländisches Datenschutzgesetz: Gesetz zur Anpassung des Saarländischen Datenschutzgesetzes an die Verordnung (EU) 2016/679 vom 16. Mai 2018 (Amtsbl. I S. 254).

SPolG – Saarländisches Polizeigesetz: Gesetz Nr. 1889 zur Änderung des Saarländischen Polizeigesetzes vom 18. Mai 2016 (Amtsbl. 2016, S. 440).

TMG – Telemediengesetz: Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 11 des Gesetzes vom 11. Juli 2019 (BGBl. I S. 1066) geändert worden ist.

UNABHÄNGIGES
DATENSCHUTZ
ZENTRUM SAARLAND

Die Landesbeauftragte für Datenschutz und Informationsfreiheit

Fritz-Dobisch-Str. 12 • 66111 Saarbrücken
Postfach 10 26 31 • 66026 Saarbrücken

Telefon 0681 94781 – 0
Telefax 0681 94781 – 29

E-Mail poststelle@datenschutz.saarland.de

www.datenschutz.saarland.de
www.informationsfreiheit.saarland.de