

Mitteilung

des Landesbeauftragten für den Datenschutz und die Informationsfreiheit

35. Datenschutz-Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden- Württemberg für das Jahr 2019

Schreiben des Landesbeauftragten für den Datenschutz und die Informationsfreiheit vom 16. Januar 2020, Az.: C 2310/35. TB:

Anbei übersende ich Ihnen meinen 35. Tätigkeitsbericht für den Datenschutz.

Dr. Brink

35. Datenschutz-Tätigkeitsbericht
des Landesbeauftragten für den
Datenschutz und die Informationsfreiheit
Baden-Württemberg
2019



Inhaltsverzeichnis

Vorwort	3
1. Schwerpunkte	7
1.1 Von Baden-Württemberg nach Europa – LfDI evaluiert die DS-GVO	7
1.2 Umfrage zur Umsetzung der DS-GVO im kommunalen Bereich	10
1.3 Datenschutz als KULTuraufgabe	11
1.4 Bodycam – Kontrollbesuche bei Polizeirevieren	17
1.5 Datenpannen in Arztpraxen	20
1.6 E-Mail-Werbung nach UWG – eine Ausnahmeregelung in engen rechtlichen Grenzen	23
1.7 Das Auskunftsrecht nach Artikel 15 Absatz 1 Buchst. c DS-GVO: Volle Transparenz für die Betroffenen gerade auch bei Datenübermittlungen	25
1.8 Art. 15 DS-GVO im Beschäftigtenkontext	26
1.9 Technisch-organisatorischer Datenschutz	28
1.10 Mehr Datenschutz heißt auch mehr Europa!	36
1.11 Aktuelles aus der Bußgeldstelle	40
1.12 Bye Bye Twitter	42
2. Innere Sicherheit	47
2.1. Funkzellen-Abfrage	47
2.2 Eurodac	48
2.3 Schmähesänge im Fußballstadion	49
2.4 Prüfung der Umsetzung von Mitteilungen der Staatsanwaltschaft über den Ausgang des Verfahrens	52
3. Videoüberwachung	56
3.1 Alles fit für die Kontrolle? – Videoüberwachung in Fitnessstudios	56
3.2 Unser täglich` Brot – Videoüberwachung in Bäckereien	57
3.3 Berechtigte Interessen	58
3.4 Orientierungshilfen zur Videoüberwachung	59
4. Verkehr	63
4.1 Verkehr	63
4.2 Behörde setzt auf Postkarte	63
4.3 Entwicklung von Künstlicher Intelligenz (KI) im Bereich Verkehr	64

LfDI BW - 35. Tätigkeitsbericht 2019

5. Justiz	67
5.1 Wie erfüllen Notare ihre datenschutzrechtlichen Informations- und Dokumentationspflichten?	67
5.2 Umsetzung der Richtlinie (EU) 2016/680 im Justizbereich	69
6. Kommunales	73
6.1 Die „Liste der Auffälligen“	73
6.2 Kommunales Netzwerk Datenschutz	74
7. Gesundheit und Soziales	77
7.1 Vorsicht beim Versand von E-Mails	77
7.2 Datenschutz in der ambulanten und stationären Pflege	77
7.3 Die Informationspflicht im Fall der Erhebung personenbezogener Daten bei der betroffenen Person durch Sozialleistungsträger	81
8. Schule und Hochschulen	87
8.1 Nutzungsordnung für die Informationstechnik an einer Schule	87
8.2 Überarbeitung der Broschüre „Datenschutz in Kindertageseinrichtungen“	89
8.3 Überarbeitung der Verwaltungsvorschrift über den Datenschutz an öffentlichen Schulen	90
9. Privater Datenschutz	95
9.1 Arbeitnehmerüberlassung – Verarbeitung im Auftrag ?	95
9.2 Parkraumüberwachung durch private Unternehmen	96
9.3 Datenschutzrechtliche Verantwortlichkeit	97
9.4 Datenschutz bei der Hausverwaltung	99
9.5 Datenschutz in der Kreditwirtschaft	101
9.6 Einwilligungstexte und Datenschutzhinweise am Beispiel von Gewinnspielkarten und Gewinnspielen auf Internetseiten	106
9.7 Auf hoher See	108
9.8 Neues aus dem Bereich internationaler Datenverkehr	109
10. Aus der Dienststelle	113
10.1 Aus der Dienststelle	113
10.2 Presse- und Öffentlichkeitsarbeit	115
Informationen zur Dienststelle	121
Aufbau der Dienststelle	121
Anhang	ab 123

Vorwort

2019 – #DSGVOwirkt!

Im Datenschutz geht es weiter Schlag auf Schlag: Nach dem alles überstrahlenden Stichtag 25. Mai 2018 und dem Beratungsmarathon des ersten Jahres der EU-Datenschutz-Grundverordnung (DS-GVO) legen wir jetzt schon den 2. Tätigkeitsbericht nach dem neuen europäischen Rechtsregime vor.

Seit 2018 ist die DS-GVO in der gesamten EU unmittelbar geltendes Datenschutzrecht, und es bescherte dem Datenschutz eine nie dagewesene Aufmerksamkeit, die sich in einer Flut von Eingaben, Bitten und Beschwerden, in zahlreichen Anfragen nach Beratung, nach Schulung und Begleitung ebenso widerspiegelte wie in einem außergewöhnlich großen Medieninteresse.

Unsere Erfahrung im Jahr 2019: Es lässt nicht nach! Die DS-GVO ist angekommen – und sie geht auch nicht wieder weg!

Die Beschwerdezahlen bleiben auf hohem Niveau, die Beratungswünsche nehmen keineswegs ab, und auch das öffentliche Interesse hält unvermindert an. Für uns besteht kein Zweifel: Die DS-GVO wirkt. Sie wirkt durch ihre klaren, freiheitsfreundlichen Regelungen von Auskunfts-, Berichtigungs- und Löschansprüchen der Bürgerinnen und Bürger, durch klare (und nicht selten aufwändige) Ansagen an die Verantwortlichen (also Unternehmen und Behörden, die persönliche Daten verarbeiten) und nicht zuletzt durch sehr massive Bußgeldandrohungen.

Eine weitere Erkenntnis aus dem vergangenen Jahr: Wir sind zwar mittlerweile eine der am besten ausgestatteten Datenschutz-Aufsichtsbehörden in Deutschland

(und Europa) – aber wir können nicht alles: Beratung und Kontrolle funktionieren je für sich genommen schon wirklich gut – aber nicht gleichzeitig. Wir können – und das haben wir im Jahre 2018 unter Beweis gestellt – beraten, wir können auch – das haben wir mit unseren breit angelegten Kontrollaktionen des Jahres 2019 gezeigt – auch effektiv und mit Augenmaß kontrollieren. Aber beides gleichzeitig geht (noch) nicht. Dafür reicht unser Personalbestand trotz des wirklich hohen persönlichen Einsatzes meiner Kolleg*innen nicht aus. Was etwa bedeutet hat, dass wir 2019 nolens volens unsere Beratungsleistungen zugunsten der Kontrolldichte etwas zurückfahren mussten. Und dass die Wartezeiten bei Eingaben der Bürgerinnen und Bürger immer noch zu lang sind.

Unsere Kernaufgaben (Beratung von Bürgerinnen und Bürgern als sogenannte „Betroffene“ bzw. als für Datenverarbeitung „Verantwortliche“ in Unternehmen, Behörden und Vereinen/Aufklärung und Sensibilisierung der Öffentlichkeit in Fragen des Datenschutzes/Aufsichtsbehördliche Durchsetzung des Datenschutzrechts mit Prüfmaßnahmen und Sanktionen) wurden 2019 ergänzt um die „europäische Dimension“ des neuen Rechts: Als Teil einer europäischen Datenschutzverwaltung koordinieren wir uns mit 48 weiteren Aufsichtsbehörden – die was Verwaltungskultur und Durchsetzungsfähigkeit anbelangt doch deutlich anders „ticken“ als wir. Der Prozess hin zu einer einheitlich agierenden europäischen Datenschutzaufsicht wird sicherlich noch etliche Jahre in Anspruch nehmen. Aber er ist, wie es so schön heißt, alternativlos. Als Behörde sind wir in Europa angekommen und haben dort einen erfreulichen Platz eingenommen: Als deutscher Vertreter in der einflussreichen Social Media-Group des Europäischen Datenschutzausschusses, als Berichterstatter

LfDI BW - 35. Tätigkeitsbericht 2019

zu zentralen Fragestellungen der DS-GVO und als Gesprächspartner für international tätige Unternehmen und Medien.

Im Mittelpunkt unserer Tätigkeit stand und steht weiterhin die Beratungstätigkeit: In tausenden Einzelgesprächen, auf hunderten Veranstaltungen und Seminaren, mittels dutzender Orientierungshilfen in unserem immer wieder erweiterten Internetauftritt („Renner“ ist nach wie vor unser Praxisratgeber [„Datenschutz im Verein“](#)) oder via Twitter, wo wir mit mehr als 5.000 Followern aus der Datenschutzcommunity Millionen von Bürgerinnen und Bürger mit Datenschutzinformationen erreichten. Damit ist jetzt allerdings Schluss: Die durch den Europäischen Gerichtshof und zuletzt durch das Bundesverwaltungsgericht eindeutig bestätigte Rechtslage lässt es nicht mehr zu, als Datenschutz-Aufsichtsbehörde aktiver Teil einer Social Media-Plattform zu sein, die ganz erheblichen Zweifeln hinsichtlich ihrer Datenschutzkonformität ausgesetzt sind. Das ist schade, weil die lebendige Kommunikation auch auf dieser Ebene spannend und ertragreich war, aber da müssen wir konsequent sein – und alle Anstrengungen unternehmen, die so gute und konstruktive Kommunikation auf rechtskonforme und unabhängige andere Kanäle umzusteuern. Klar ist auch: Die neue Rechtslage wird auch Folgen für die Präsenz öffentlicher und nichtöffentlicher Stellen in Social Media haben. So wie es jetzt läuft, kann es nicht bleiben. Wir werden den Dialog hier weiter forcieren und nach guten (zumindest akzeptablen) Lösungen suchen; letztlich gibt die DS-GVO auch hier die Marschrichtung klar vor.

„Wenn es nicht vernünftig ist, dann ist es kein Datenschutz!“ Dieses Motto haben wir auch 2019 beherzigt, etwa bei den Bußgeldern, wo wir unseren Ruf, als Aufsichtsbehörde schnell, konstruktiv, aber auch

konsequent zu handeln bekräftigt haben. Aber wir haben auch nicht die Augen davor verschlossen, dass die DS-GVO als Rechtsnorm nicht in allen Bereichen der Weisheit letzter Schluss ist – und haben maßgeblich für die deutsche Datenschutzkonferenz DSK, aber auch im „Ländle“ mit allen betroffenen Akteuren vom Handwerk über den Mittelstand bis hin zu Wissenschaft und Behörden an der Evaluierung der DS-GVO gearbeitet. Auch die DS-GVO selbst muss besser werden.

Mit Blick auf die Entwicklung des Personals lässt sich sagen: Die Besetzung unserer offenen Stellen stellte kein Problem dar, auch im hart umkämpften Bereich Technik nicht. Der LfDI kann offensichtlich auf eine attraktive Aufgabe und einen guten Ruf bauen, wir sind auch für Kolleg*innen aus der Verwaltung des Landes, für Interessent*innen von anderen deutschen Aufsichtsbehörden und auch für Wechselwillige aus der Privatwirtschaft offensichtlich eine Arbeitsstelle mit Anziehungskraft. Da stärkt uns die nun wiederum vom Parlament beschlossene, im Bundesvergleich einmalig gute Aufstockung des Personals in hervorragender Weise. Wir werden ab 2020 ein Schulungs- und Fortbildungszentrum des Datenschutzes und der Informationsfreiheit aufbauen und unseren Nutzen für die Bürgerinnen und Bürger, aber auch die Betriebe, Unternehmen und Behörden des Landes weiter ausbauen.

Letztlich wird Datenschutz aber nicht (nur) von der Aufsichtsbehörde gemacht, sondern von den Bürgerinnen und Bürgern wahrgenommen (oder eben nicht) und von den verantwortlichen Stellen in Unternehmen und Verwaltungen mehr oder weniger überzeugend gelebt. Welche Bedeutung messen wir als Betroffene und Grundrechtsträger zukünftig unserem Freiheitsrecht auf informationelle Selbst-

LfDI BW - 35. Tätigkeitsbericht 2019

bestimmung zu? Sind wir bloß willige Konsumenten, denen Annehmlichkeiten und „Dabeisein“ wichtiger scheinen als die Chance, selbstbestimmt ins digitale Zeitalter zu schreiten? Ein Grundrecht ohne Grundrechtsträger, die seine Substanz auch wertschätzen, hat keine Zukunft – auch nicht mit einer Europäischen DS-GVO.

Den anhaltenden Schwung der DS-GVO nehmen wir Datenschützer weiterhin optimistisch auf – die Grundlagen für unsere Zuversicht finden sich in diesem Tätigkeitsbericht. Wiederum gilt mein Dank allen meinen Mitarbeiterinnen und Mitarbeitern mit meinem Stellvertreter Herrn Broo an der Spitze für ihre tolle Arbeit, die weit über das Erwartbare hinausgeht – wir Datenschützer sind eben „Überzeugungstäter“. Bedanken darf ich mich an dieser Stelle aber auch bei den Abgeordneten des Landtags Baden-Württemberg, welche unsere Aufgabe auch im Jahr 2019 maßgeblich gestaltet, begleitet und gefördert haben und bei Landesregierung, -Verwaltung und den Kommunen für die immer faire und weitgehend einvernehmliche Zusammenarbeit.

Ihr Landesbeauftragter
Dr. Stefan Brink

LfDI BW - 35. Tätigkeitsbericht 2019

1. Schwerpunkte

1.1 Von Baden-Württemberg nach Europa – LfDI evaluiert die DS-GVO

Das Jahr 2019 stand für uns auch unter dem Zeichen der Evaluierung der DS-GVO. Nach Art. 97 DS-GVO muss zum 25. Mai 2020, also zwei Jahre nach Inkrafttreten der DS-GVO, diese von der Europäischen Kommission evaluiert werden. Zu diesem Zwecke kann sie von den Mitgliedstaaten und den Aufsichtsbehörden Informationen anfordern.

1.1.1 Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden der Länder und des Bundes (Datenschutzkonferenz – DSK) hat sich als Gremium aller deutschen Datenschutzaufsichtsbehörden hierauf vorbereitet, indem sie einen Arbeitskreis eingesetzt hat, die Rückmeldungen aller Aufsichtsbehörden zu koordinieren und zu einem einheitlichen Bericht zusammenzufassen. Der Vorsitz dieses Arbeitsgremiums wurde vom LfDI Baden-Württemberg übernommen.

Von Anfang des Jahres bis hin zur Verabschiedung des Berichtes durch die DSK im November haben wir unter Mitarbeit fünf weiterer Aufsichtsbehörden in insgesamt fünf Sitzungstagen und ständiger Koordinierungsarbeit sowie unter Berücksichtigung der Beschlusslage der DSK und ihrer Arbeitskreise einen Berichtsentwurf gefertigt, welcher zuerst den Grundsatz-Arbeitskreis und sodann die DSK selbst pasierte. Am 06. November 2019 hat die

98. DSK den von uns koordinierten Erfahrungsbericht verabschiedet. Der Bericht ist auf der [Homepage der DSK](#) sowie des [LfDI Baden-Württemberg](#) in deutscher und englischer Sprache abrufbar und wurde durch den DSK-Vorsitz dem Europäischen Datenschutzausschuss (EDSA) zugeleitet.

Neben den gesetzlich für den Fall einer Evaluierungsanfrage durch die Kommission festgelegten Themen des Art. 97 Absatz 2 DS-GVO wurde der Fokus auf etwaigen Änderungsbedarf aufgrund der Anwendungserfahrungen im ersten Jahr gelegt. Dies sowohl bezogen auf bestehende Vorschriften, als auch auf die möglicherweise notwendige Schaffung weiterer Regelungen. Auch die Erwägungsgründe der DS-GVO wurden in die Überlegungen miteinbezogen. Die Frage der Befassung mit etwaigen Problemen bei der Umsetzung der DS-GVO in Bundes- und Landesrecht wurde nicht in den Bericht der DSK miteinbezogen. Dies geschah nach Kenntnis der DSK durch eine Abfrage der Kommission bei den nationalen Innenministerien. Nach Auffassung des LfDI kann sich aus problematischen nationalen Umsetzungsnormen allerdings auch Änderungsbedarf an Öffnungsklauseln der DS-GVO selbst ergeben.

Wesentliche Ergebnisse der DSK wurden in folgenden Schwerpunktthemen behandelt:

Bei den Informations- und Transparenzpflichten nach Art. 13 und 14 DS-GVO haben sich in der Praxis Umsetzungsprobleme gezeigt, z. B. bei telefonischer Datenerhebung. Hier geht es insbesondere um die Frage, ob zunächst eine allgemeinere Information an zentraler Stelle ausreicht und konkrete Informationen nur auf Verlangen nachgereicht werden können. Auch Umfang und Inhalt der Informationspflichten könnten möglicherweise praktikabler und bürgerfreundlicher definiert werden. In der

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

Praxis stellt sich teilweise die Frage nach der Alltagstauglichkeit der Regelungen der DS-GVO. Möglichkeiten zur erleichterten Anwendung der Informationspflichten, die Pflicht zur Meldung von Datenschutzbeauftragten an die Aufsichtsbehörden sowie das Recht auf Kopie nach Art. 15 Absatz 3 DS-GVO wurden in den Fokus genommen.

Eine allgemein umgreifende Sorge vor den Sanktionsmöglichkeiten der DS-GVO führt nach der Erfahrung der Aufsichtsbehörden dazu, dass viele Datenpannen gemeldet werden, welche tatsächlich gar keine Datenpannen sind oder deren Risiken schon längst beseitigt wurden. Daher waren exorbitante Steigerungsraten bei den Meldungen von Datenpannen zu verzeichnen. Mit möglichen Lösungen hat die DSK sich auseinandergesetzt.

Im Bereich der Zweckbindung haben sich in der Praxis vor allem Fragen im Hinblick auf die Rechtsgrundlage und die Voraussetzungen der Weiterverwendung der personenbezogenen Daten bei der Zweckänderung ergeben.

Data protection by design findet in der Praxis kaum Resonanz, da der Anwendungsbereich der DS-GVO Hersteller gerade nicht erfasst. Die DS-GVO stellt mit data protection by design/by default aber Grundsätze auf, die sich in der Sache zwar an Hersteller richten, nimmt diese aber nicht als Verantwortliche in die Pflicht. Daher wird die Frage aufgeworfen, ob auch Hersteller, Lieferanten, Importeure und Verkäufer in die Pflicht genommen werden sollten, so wie es im Produkthaftungsrecht bereits der Fall ist.

Im Schwerpunktthema „Befugnisse der Aufsichtsbehörden und Sanktionspraxis“ haben sich insbesondere Fragen nach dem Begriff des „Verarbeitungsvorgangs“ aus

Art. 58 Absatz 2 lit. b DS-GVO sowie der Zusammenarbeit und des Auskunftsrechts der Aufsichtsbehörden im Bußgeldverfahren als besonders dringlich erwiesen. In einem weiteren in Art. 97 Absatz 2 lit. b DS-GVO aufgeführten Schwerpunkt werden die Erfahrungen der Aufsichtsbehörden mit den Themen „Zuständigkeitsbestimmungen, Zusammenarbeit und Kohärenz“ dargestellt.

Bei der Direktwerbung stellt sich in unterschiedlichen Konstellationen die Frage der Zulässigkeit, welche durch die Schaffung einer spezifischen Rechtsgrundlage gelöst werden könnte.

Eine der zentralen datenschutzpolitischen Herausforderungen unserer Zeit ist das Profiling. Trotz vorhandener Begriffsdefinition wird der Prozess der Profilbildung als solcher von den meisten Normen der DS-GVO – etwa zur automatisierten Entscheidungsfindung – nicht erfasst, sodass eine Beurteilung meist nur nach den allgemeinen Tatbeständen des Art. 6 DS-GVO erfolgt. Die DSK fordert eine Verschärfung des geltenden Rechtsrahmens, um der Nutzung personenbezogener Daten zu Zwecken der Profilbildung effektive und faktisch durchsetzbare Grenzen zu setzen.

Beim Schwerpunkt Akkreditierung könnte durch eine Klarstellung in der DS-GVO eine erhebliche nationale Zuständigkeitsfrage geklärt und die Aufsicht durch die deutschen Datenschutzaufsichtsbehörden sichergestellt werden.

Zum aktuell vorherrschenden Thema in der wissenschaftlichen Auseinandersetzung, der Frage des Datenschutzes im Bereich der Künstlichen Intelligenz und automatisierten Entscheidungsverfahren, übersendete die DSK außerdem ihre [„Hambacher Erklärung zur Künstlichen Intelligenz – Sieben](#)

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

[datenschutzrechtliche Anforderungen](#)“ vom 3. April 2019 an den EDSA. Wenngleich die enthaltenen Forderungen sich vorrangig auf zukünftige Fall- und Normkonstellationen beziehen, haben die deutschen Datenschutzaufsichtsbehörden die Beachtung dieser Grundsätze in den zukünftigen Evaluierungsprozessen als unerlässlich betrachtet.

1.1.2 Beitrag zur Evaluierung des LfDI Baden-Württemberg

Seit dem 25. Mai 2018 ist der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg gesetzlich dazu verpflichtet, die Einhaltung der DS-GVO in Baden-Württemberg zu beaufsichtigen und die Verantwortlichen im Lande zu beraten. Zur Evaluierung der DS-GVO möchte daher auch ich meine Einschätzungen, welche auf der bisherigen praktischen Erfahrung meiner unabhängigen obersten Landesbehörde resultieren, der Europäischen Kommission zur Kenntnis bringen.

Nicht nur aus den Erkenntnissen, welche sich aus fast einem Jahr Vorsitz des Arbeitskreises zur deutschen Evaluierung ergeben, sondern vor allem aus den unzähligen Rückmeldungen, welche dem LfDI aus dem Land zuzugingen – sei es bei Veranstaltungen, Schulungen oder im direkten Austausch mit Verantwortlichen, haben wir einen eigenen [Beitrag zur Evaluierung](#) erarbeitet.

Denn der Kreis der Verantwortlichen in Baden-Württemberg ist mit dem Bundesdurchschnitt nur teilweise vergleichbar. Laut Ministerium für Wirtschaft und Finanzen Baden-Württemberg erwirtschaften kleine und mittlere Unternehmen jeden zweiten Euro Umsatz im Land und beschäftigen zwei Drittel der sozialversicherungspflichtigen Beschäftigten. Der Mittelstand

ist damit das Rückgrat der Wirtschaft in Baden-Württemberg. Außerdem engagiert sich einem Bericht des Ministeriums für Soziales und Integration Baden-Württemberg zufolge fast jeder zweite Baden-Württemberger in seiner Freizeit ehrenamtlich (über 48 Prozent). Damit sind wir Spitzenreiter. Baden-Württemberg ist sowohl Land des Ehrenamtes als auch des Unternehmergeistes und hat damit eigene, spezifische Herausforderungen und Anliegen an einen praxistauglichen Datenschutz.

Um den Erfahrungen der Verantwortlichen und Anwendenden der DS-GVO in Baden-Württemberg Rechnung zu tragen, haben wir am 28. Juni 2019 hierzu eine Anhörung unter dem Banner „[#DS-GVO wirkt \(?\) – 1 Jahr DS-GVO – Praxiserfahrungen und Evaluation](#)“ in Zusammenarbeit mit und in den Räumlichkeiten der Industrie- und Handelskammer Region Stuttgart veranstaltet. Zu Impulsvorträgen geladen waren VertreterInnen aus Aufsicht, Behörden, Wirtschaft, Wissenschaft, Anwaltschaft, Verbänden und Datenverarbeitern. In einem eigens hierzu eingerichteten E-Mail-Postfach wurden außerdem über das ganze Jahr Zuschriften aus allen Bereichen des Landes gesammelt und ausgewertet. Diese landesspezifischen Erkenntnisse bieten ergänzend zum Erfahrungsbericht der DSK einen Beitrag zur Evaluation der DS-GVO durch den europäischen Gesetzgeber.

Insgesamt hat sich gezeigt, dass die Verantwortlichen in Baden-Württemberg sich in vielen Bereichen alltagstauglichere Lösungen wünschen und einige Vorschriften sich nur schwer auf datenverarbeitende Tätigkeiten kleiner Unternehmen oder ehrenamtlicher Arbeit anwenden lassen. Im Vordergrund stehen vor allem Fragen rund um eine mögliche Entlastung bei den Informations-, Transparenz- und Auskunft-

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

pflichten. Er behandelt aber auch Fragen zu Pflichten zur Erstellung von Verarbeitungsverzeichnissen und der Benennung von Datenschutzbeauftragten, außerdem die Einführung und Aufsicht einer Herstellerhaftung sowie Unklarheiten bei der Gemeinsamen Verantwortlichkeit, insbesondere im „Social Media“-Bereich.

Trotz zahlreicher Muster und Praxisratgeber meiner und anderer Aufsichtsbehörden scheint immer noch eine erhebliche Rechtsunsicherheit bei den Verantwortlichen vorhanden zu sein. Wider Erwarten haben sich Sorgen um Sanktionen – zumindest unter unserer Praxis – nicht als vorrangig herausgestellt. Dies mag nicht zuletzt daran liegen, dass wir in Baden-Württemberg immer wieder klargestellt haben, dass es uns daran liegt, dass die Verantwortlichen sich auf den Weg zu einer datenschutzkonformen Verarbeitung gemacht haben. Ca. 75 % der Unternehmen gaben nach Umfrage der DIHK an, die DS-GVO (zumindest bereits teilweise) umgesetzt zu haben. Meine Erfahrungen sind damit im Großen und Ganzen deckungsgleich.

Die Datenschutzaufsicht in Baden-Württemberg orientiert sich am Leitsatz „Wenn es nicht sinnvoll ist, ist es kein Datenschutz“. Unter dieser Zielsetzung soll auch unser Bericht, den wir an den EDSA senden, verstanden werden.

1.2 Umfrage zur Umsetzung der DS-GVO im kommunalen Bereich

Die Kommunen in Baden-Württemberg sind als verantwortliche öffentliche Stellen weiterhin in hohem Maße mit der Umsetzung der neuen Anforderungen aus der Datenschutz-Grundverordnung beschäftigt. Um weiterhin adäquate Beratungsleistungen im kommunalen Bereich zu erbringen, benötigt meine Dienststelle in diesem Zusammenhang verlässliche und

umfassende Informationen, wie gut die Städte und Gemeinden im Land ihre Arbeit an die neuen Anforderungen bereits angepasst haben und wo sie noch nachbessern müssen.

Vor diesem Hintergrund wurde im Sommer 2019 ein umfassender Fragenkatalog an alle 1101 baden-württembergische Kommunen versandt, der den Umsetzungsstand des neuen Datenschutzrechts abfragte. Den Gemeindeverwaltungen wurde ein Online-Katalog mit 50 Fragen vorgelegt, der die wichtigsten Bereiche des neuen Datenschutzrechts zum Inhalt hatte. Die Gemeinden erhielten per E-Mail einen individuellen Teilnahme-Link und hatten in dem Fragenkatalog auch die Möglichkeit, individuelle Antworten zu geben. Im Ergebnis haben 968 Gemeinden (rund 87 %) an der Umfrage teilgenommen. 12 % der Gemeinden haben sich trotz mehrfacher Aufforderung nicht beteiligt, darunter haben 6 % den Umfrage-Link nie aufgerufen.

Die Auswertung der Umfrage zeigt klar, dass sich die Gemeinden insgesamt durch die Anforderungen der Datenschutz-Grundverordnung stark belastet fühlen. Um es an einem Beispiel zu verdeutlichen: Dem Verarbeitungsverzeichnis der verantwortlichen Stelle kommt im Datenschutz eine zentrale Bedeutung zu. Doch fast ein Drittel der Gemeinden hat noch gar nicht begonnen, ein solches aufzustellen. Diese Gemeinden haben somit bislang keine Übersicht über die Verarbeitungstätigkeiten in ihrem Verantwortungsbereich. Mehr als die Hälfte der Gemeinden gaben an, dass es Probleme bei der Erstellung eines Verarbeitungsverzeichnisses gibt.

Zeitgleich mit der Auswertung der Umfrage hat meine Dienststelle eine Broschüre für die baden-württembergischen Gemein-

den veröffentlicht, die den in der Umfrage geäußerten inhaltlichen Beratungsbedarf aufgreift und eine weitere Orientierung im kommunalen Datenschutz bieten soll.

Die Auswertung, die Pressemitteilung sowie die Broschüre „Datenschutz bei Gemeinden“ können [hier](#) abgerufen werden.

Wesentliche Ergebnisse der Umfrage:
Die Kommunikation LfDI und Gemeinden funktioniert, die Kooperationsbereitschaft ist erfreulich hoch.

Die Kommunen sind bereit und willig, sich der „Herausforderung DS-GVO“ zu stellen, aber es fehlt an Know How, Personal und Unterstützung – gerade bei den kleinen Gemeinden.

Der bislang erreichte Stand in Sachen Datenschutz und Datensicherheit ist in vielen Bereichen ungenügend.

1.3 Datenschutz als KULTuraufgabe

Welche Assoziationen haben Bürger und Bürgerinnen, wenn sie an eine beliebige Behörde denken?

Und, um noch einen Schritt weiter zu gehen:

Welche Assoziationen entstehen, wenn sie dabei an eine Behörde denken, deren Hauptaufgabe es ist, sich mit dem Thema Datenschutz zu befassen?

Ob dem Bürger oder der Bürgerin dazu wohl ein Abend mit Sinologinnen zum Themenfeld China einfällt, ein Abend mit der Bundesjustiz- und Verbraucherschutzministerin Dr. Katarina Barley oder gar die Produktion eines Musikvideos, das einen tanzenden Landesbeauftragten präsentiert?

All dies ist nur ein kleiner Ausschnitt dessen, was ich dieses Jahr getan habe.

Gleich zu Beginn des Jahres habe ich gemeinsam mit der Wiener Sängerin Daniela Flickentanz (ja, sie heißt wirklich so), der Hochschule der Medien Stuttgart, und einigen meiner Mitarbeiterinnen und Mitarbeiter ein Musikvideo zum Thema Datenschutz produziert. Von der ersten Kontaktaufnahme bis zum Drehtag lagen ziemlich genau vier Wochen – und diese vier Wochen hatten es ganz schön in sich.

Aber wir haben es geschafft, Mitte Februar 2019 stand das gemeinsam erarbeitete Drehbuch, der Song-Text war angepasst, die Regieanweisungen fertig, sämtliche Requisiten organisiert und nicht zuletzt ist Daniela Flickentanz von Wien nach Stuttgart angereist.

Es konnte also losgehen ...

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

Entstanden ist dabei Datenschutz der ganz anderen Art ...

In unserem Musikvideo wird nicht nur gesungen und getanzt, nein dieses Video gibt – wie ich finde – auf humorvolle und eingängige Weise Handlungsempfehlungen zum Thema Datenschutz – sozusagen ein swingendes How-to.

Welche Behörde kann schon von sich behaupten, ihrem gesetzlichen Beratungsauftrag in Form eines Musikvideos gerecht zu werden ...!?

Sie finden unser Musikvideo auf unserer [Homepage](#) oder auch bei [YouTube](#).

Mein ganz besonderer Dank gilt Daniela Flickentanz und dem hochprofessionellen Team der Hochschule der Medien, Stuttgart, und natürlich meinen experimentierfreudigen Mitarbeitern. Ich bin immer noch begeistert, was wir zusammen erschaffen haben!

Damit sind wir gleich zu Beginn des Jahres mit einer Attraktion eingestiegen – und das war nicht die einzige Attraktion des Jahres 2019!

Im März konnte ich die damalige Bundesjustiz- und Verbraucherschutzministerin Dr. Katarina Barley nach Stuttgart holen. Gemeinsam mit unserem bewährten Kooperationspartner, Hochschule der Medien, Stuttgart, haben wir uns im Rahmen einer Podiumsdiskussion mit dem Thema:

#Doxxing #Datenklau #DigitaleEthik
Unser digitales Leben – alternativlos?!

auseinandergesetzt. Die Veranstaltung war restlos ausgebucht, selbst die zusätzlichen Stehplätze konnten den Andrang und die Begeisterung des Publikums nicht

fangen. Auch diesen Abend können Sie auf [YouTube](#) nachverfolgen.

Im Mai haben wir uns auf den Weg in das Reich der Mitte gemacht – natürlich nur virtuell und akustisch.

CHINA –

Kaiserreich, Terrakottakrieger, Chinesische Mauer, Ming-Dynastie, chinesische Schriftzeichen, die verbotene Stadt, Buddhismus, Chinesischer Tee, Seide, Peking-Oper, ...

Wer fängt bei all diesen Begriffen nicht zu träumen an ...

Jedoch definiert sich die moderne Volksrepublik China nicht nur über diese historischen und kulturellen Güter. Die aktuellen Entwicklungen im Reich der Mitte bieten keinen Anlass mehr um zu träumen – ganz im Gegenteil ... sie weisen dystopische Züge auf. Das Land hat ein Sozialkredit- bzw. Social Scoring-System eingeführt, das auf einem Belohnungs- bzw. Bestrafungssystem basiert. Die Bevölkerung erhält Bonus-Punkte für ein Verhalten, das aus staatlicher Sicht positiv zu bewerten ist. Dazu zählt bspw. die Fürsorge für die Eltern. Umgekehrt werden bei unerwünschtem Verhalten Malus-Punkte in Abzug gebracht. Schon die Nichtbeachtung einer roten Verkehrsampel bietet Anlass das individuelle Punktekontingent zu reduzieren. Sofern eine gewisse Mindestmenge an Punkten unterschritten wird, reagiert der Staat mit Repressalien wie bspw. beim Zugang zu Studien- oder Ausbildungsplätzen, Nutzung von Flügen und Zügen, ... Und das nicht nur für den Verursacher – die Repressalien können sich auf alle Familienmitglieder erstrecken.

All dies geht einher mit umfassender technischer Überwachung gepaart mit sozialer

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

Überwachung durch Nachbarn, Kollegen und „Freunde“... Es steht außer Frage, dass der Umgang mit jemandem, der Schulden hat und dessen Punktekonto eher in den unteren Regionen angesiedelt ist, auch negative Auswirkungen auf den eigenen sozialen Status und damit auch auf die eigene Existenz haben kann. Die Folge davon heißt für die Betroffenen und deren Familien, ggf. zusätzlich zu den bereits genannten Repressalien, soziale Isolation.

Diese Entwicklungen bieten für mich als Freiheitsschützer Anlass zu großer Sorge. Daher war es mir wichtig, über diese Entwicklungen fachkundig zu informieren und mit Interessierten und Fachleuten diese Sachverhalte und die damit verbundenen Auswirkungen kritisch zu hinterfragen und zu diskutieren. Im Mai 2019 habe ich dazu in die Kirche St. Maria in Stuttgart eingeladen.

Unter dem Motto „China – Das Land hinter dem Lächeln“ gewährte uns zunächst Frau Dr. Ricarda Daberkow vom Linden-Museum in die historische Entwicklung einer Jahrtausendealten Kultur Einblick. Nach einer kurzen Pause erläuterte uns Frau Dr. Mareike Ohlberg vom Mercator Institute for China Studies (MERICS) das in der Volksrepublik China bereits praktizierte Social Scoring und dessen Auswirkungen für den Einzelnen im Alltag.

Das Ausmaß, das die staatliche Überwachung im Reich der Mitte bereits jetzt umfasst, konnte an keinem der Zuhörer spurlos vorbeigehen. Umso mehr, da das noch schlummernde Potenzial unermessliche weitere Überwachungsmöglichkeiten bietet, das einer völligen Gleichschaltung und damit der Abschaffung jeglicher Privatsphäre gleichkommt.



Die Vorträge der beiden Sinologinnen und auch die anschließende Diskussion am Buffet mit kleinen chinesischen Köstlichkeiten haben deutlich gemacht, dass Freiheit in jeder Form ein Gut ist, das gar nicht hoch genug geschätzt werden kann. Allerdings wurde auch deutlich, dass all diese Freiheit nicht selbstverständlich ist, sondern, dass jeder von uns jeden Tag dazu beitragen muss, diese Freiheit zu pflegen und zu erhalten.

Ein wenig habe ich mich an einen Abend im letzten Herbst erinnert gefühlt. An diesem Abend habe ich gemeinsam mit den Stuttgarter Innenstadtkinos das Hollywood-Movie „THE CIRCLE“ präsentiert. Dieser basiert auf dem Grundgedanken, dass sich nur der Mensch, der sich ständiger Beobachtung bewusst ist, korrekt verhält. Was bei einem Menschen, der sich unbeobachtet wähnt, nicht immer gewährleistet ist.

Der Preis hierfür heißt PRIVATSPHÄRE!

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

Schockiert weist jeder kritisch denkende Mensch diesen Ansatz weit von sich. Das Reich der Mitte scheint diesen Ansatz nicht nur übernommen, sondern konsequent fortentwickelt zu haben.

Im September 2019 gelang es mir eine Podiumsdiskussion mit Vertreterinnen der Enquete-Kommission „Künstliche Intelligenz“ des Deutschen Bundestages zu präsentieren. Dazu habe ich gemeinsam mit dem Landesbeauftragten von Rheinland-Pfalz, Herrn Prof. Dieter Kugelmann, in das Ernst-Bloch-Zentrum nach Ludwigshafen, eingeladen.

Eines der großen Schlagworte im Jahr 2019 lautete „Künstliche Intelligenz“. Im April 2019 haben meine Kolleg*innen und ich auf der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) die „Hambacher Erklärung zur Künstlichen Intelligenz“ erarbeitet und verabschiedet.

Bereits seit Jahrhunderten träumt der Mensch vom künstlich erschaffenen, in ihrer Intelligenz menschenähnlichen Maschinenwesen. Dafür gibt es in der Literatur und Geschichte viele prominente Vordenker, Forscher und Erfinder. Der griechische Schmiedegott Hephaistos, Leonardo da Vinci und Mary Shelleys Frankenstein seien hier nur exemplarisch genannt.



Mit dem Themenkomplex Künstliche Intelligenz (KI) sind jedoch nicht nur Hoffnungen verbunden – sondern auch viele Befürchtungen und existentielle Bedenken.

Mittelfristig wird es nahezu keinen Lebensbereich mehr geben, auf den KI nicht Einfluss nehmen wird. Ist der Einsatz von Künstlicher Intelligenz doch bereits heute weiter verbreitet als sich viele von uns träumen ließen ...

Der Abend in Ludwigshafen war dazu gedacht, den eingeladenen Referentinnen und ihrer Expertise das Podium zu überlassen. Drei Angehörige der Enquete-Kommission „Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale“ des Deutschen Bundestages, Dr. Petra Sitte (Die Linke), Dr. Anna Christmann (Bündnis 90/Die Grünen), die Sachverständige Lena-Sophie Müller von der Initiative D21 sowie die Professorin Doris Aschenbrenner von der Technischen Universität Delft (NL) boten Einblick in ihre Arbeit und die damit verbundenen gesellschaftlichen Themen. Die an die Podiumsdiskussion anschließenden Fragen und Wortmeldungen des Publikums machten nochmals deutlich, in wie vielen Bereichen KI bereits selbstverständlich zum Einsatz kommt und welche Kon-

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

sequenzen und weitere Fragen sich daraus ergeben.

Letztendlich kristallisierte sich ein wesentlicher Punkt immer wieder heraus. Die zentrale Frage lautet dabei nicht mehr: „Was ist technisch möglich?“ sondern „Was wollen wir als Gesellschaft – in welche Richtung wollen wir uns entwickeln?“.

Es steht außer Frage, dass diese allumfassenden Fragen nicht an einem Abend beantwortet werden können. Aber der Abend war ein guter Auftakt unterschiedlichste gesellschaftliche Gruppen zusammenzubringen und miteinander ins Gespräch zu kommen.

Es ist nie zu früh auf den Wert der Privatsphäre aufmerksam zu machen und das gilt insbesondere für Kinder und Jugendliche. Gemeinsam mit Kooperationspartnern nehme ich mich dieses Themas mit großer Freude jedes Jahr aufs Neue an. Mit einigen der Kooperationspartner ist dabei eine jährlich wiederkehrende und fortwährende Zusammenarbeit entstanden.

Dabei unterstütze ich die Initiative „Datenschutz geht zur Schule“ des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e. V. nicht nur, ich baue diese gemeinsam mit meinen Mitarbeitern und Mitarbeiterinnen aktiv aus. Dazu habe ich meine Kolleginnen und Kollegen der anderen Datenschutzaufsichtsbehörden zu einer gemeinsamen Aktion über die Ländergrenzen hinweg eingeladen. Die länderübergreifende Abstimmung und Koordination lag dabei in Baden-Württemberg.

Die Initiative „Datenschutz geht zur Schule“ sensibilisiert Schülerinnen und Schüler zu einem bewussten Umgang mit dem Internet und den sozialen Medien. Besonders kurzweilig und vor allem anschaulich wird das abstrakte Thema „Datenschutz“ durch

die zahlreichen im Vortrag enthaltenen kurzen Videoclips transportiert.

Anlässlich des Safer Internet Days am 5. Februar 2019 haben wir diverse Aktionstage in verschiedenen Städten und Schulen Baden-Württembergs angeboten und durchgeführt. Die Veranstaltungen boten für Jugendliche die Gelegenheit, bspw. die Grenzen von Big Data, Smart Home und auch die Nutzung und Datenweitergabe beim Einsatz von Messengerdiensten um den Preis der Preisgabe von privaten Informationen und Daten kritisch zu betrachten. Bequemlichkeit versus Privatsphäre wurde zu einem großen Thema. Deutlich wurde auch, dass kostenfreie Angebote nachdrücklich hinterfragt werden sollten. Ist der kostenlos angebotene Messengerdienst tatsächlich kostenlos? Aus welchem Grund bieten viele Unternehmen Kundenkarten und damit verbunden Rabatte und Treueprämien an? Schnell wurde für die Schülerinnen und Schüler klar, dass in der heutigen Zeit kein Unternehmen etwas zu verschenken hat.

Besonders habe ich mich über die begeisterten Rückmeldungen der Jugendlichen, der Lehrerinnen und Lehrer, der Schulleitungen und der Dozentinnen und Dozenten der jeweiligen Aufsichtsbehörden sowie das Presseecho in den regionalen Tageszeitungen gefreut. Macht all dies doch deutlich, wie wichtig und sinnvoll es ist, Kinder und Jugendliche im Umgang mit ihren personenbezogenen Daten im Internet zu sensibilisieren und, welche Herausforderung es auch darstellt, dieses Thema mit einem zielgruppengerechten Wortschatz zu erläutern.

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte



Quelle: erschienen in der Rhein-Neckar-Zeitung vom 6. Februar 2019, Photograph: Helmut Pfeifer

Konkret wurden allein in Baden-Württemberg insgesamt rund 600 Schüler und Schülerinnen in Stuttgart, Esslingen, Ditzingen, Walldorf, Bad Friedrichshall, Ludwigsburg, Ettlingen, Lorch und Pforzheim mit der gemeinsamen und länderübergreifenden Aktion der Aufsichtsbehörden in Kooperation mit dem BvD erreicht.

Deutlich wurde jedoch auch, dass der Bedarf an den Schulen viel, viel höher ist, als wir mit unserer Aktion befriedigen konnten.

Fazit unserer länderübergreifenden Aktion:

Wir werden weitermachen!

Weitere Informationen zu der Initiative Datenschutz geht zur Schule finden Sie auf der [Webseite des BvD](#).

Auch konnten wir die bereits seit 2017 bestehende Kooperation mit der Dualen Hochschule Baden-Württemberg erfolgreich fortsetzen.

Unter Anleitung von Herrn Professor Dr. Tobias Straub, Michael Schlegel und Ivana Marevic entwickelten insgesamt acht studentische Teams Anwendungen

zu der Fragestellung: Wie lassen sich Nutzerinnen und Nutzer von Apps und Internet-Diensten für den Datenschutz sensibilisieren und mit Tools unterstützen? Dabei entwickelten die Teams teils anspruchsvolle Softwarelösungen zur Sensibilisierung der Anwender, zu Schulungszwecken beim Thema Selbstschutz sowie zur Unterstützung von Unternehmen bei der Umsetzung datenschutzrechtlicher Vorgaben, die am Ende des Semesters durch eine Jury, in der auch eine meiner Mitarbeiterinnen vertreten ist, bewertet wurden.

<https://www.dhbw-stuttgart.de/themen/hochschule/meldung/2019/02/studierende-entwickeln-loesungen-fuer-den-datenschutz/>

Eine Fortsetzung der Kooperation zwischen der Dualen Hochschule Baden-Württemberg und meiner Behörde ist bereits mit dem Wintersemester 2019/2020 erneut angelaufen.

Zum Abschluss eines Jahres mit vielen Höhepunkten und Attraktionen konnte ich im Oktober 2019 ein weiteres Mal die Datenschutz-Herbstkonferenz als Schirmherr präsentieren. Veranstalter dieser Fachtagung ist der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V. Die Schirmherrschaft habe ich mir diesmal mit meinen beiden bayrischen Kollegen Thomas Kranig, Präsident des Bayerischen Landesamtes für Datenschutzaufsicht, und Prof. Dr. Thomas Petri, bayrischer Landesbeauftragter für Datenschutz, geteilt. Wie bereits in den letzten beiden Jahren standen die ersten beiden Tage unter dem Motto „Wirtschaft trifft Aufsicht“.

Der dritte Tag der Veranstaltung bot wieder eine Besonderheit. Unter dem Motto (Aufsichts-)Behörde hilft Behörde –

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

„Datenschutz – verstehen und gestalten“ haben wir speziell auf den Kreis der Behördenvertreter zugeschnittenen Fachvorträge und Diskussionen angeboten.



Quelle: BvD e. V./Uli Schneider

Die Herbstkonferenz Datenschutz bietet Fachvorträge, Diskussionen, Expertengespräche, Handlungsleitfäden, Beispiele aus der Praxis für alle, die mit dem Thema Datenschutz befasst sind. Die Formate „Wirtschaft trifft Aufsicht“ und auch „(Aufsichts-)Behörde hilft Behörde“ sind bundesweit einmalig und bieten die Möglichkeit Themen, Fragen und Probleme direkt mit Fachleuten und Vertretern der Aufsichtsbehörden erörtern zu können.

Die Resonanz auf unsere Veranstaltung ist immens. Mit rund 300 Teilnehmern handelt es sich bundesweit um die aktuell am stärksten frequentierte Veranstaltung zum Themenkomplex Datenschutz. In diesem Jahr war der größte Teil der Plätze bereits ausgebucht, bevor das Veranstaltungsprogramm veröffentlicht wurde.

All dies macht deutlich, dass das Thema Datenschutz und der Austausch zwischen Vertretern der Unternehmer und Behörden mit der Aufsichtsbehörde nicht mehr wegzudenken ist!

Wir werden also auch im Herbst 2020 die Datenschutz Herbstkonferenz fortführen.

Für das Jahr 2019 hatte ich das Motto:

Weiter geht's!

Rückblickend kann ich sagen –

das hat sich bewährt –

also bleibe ich auch für das Jahr 2020 dabei!

Weiter geht's!

1.4 Bodycam – Kontrollbesuche bei Polizeirevieren

Seit gut drei Jahren gibt es im Polizeigesetz des Landes eine Rechtsgrundlage für den Einsatz von Bodycams im Streifendienst der Polizei. Nachdem sich die Beschaffung geeigneter Geräte geraume Zeit hingezogen hat, sind diese mittlerweile in der Fläche weitgehend angekommen und im Einsatz. Grund genug, sich die Praxis der Anwendung einmal genauer anzuschauen.

Unsere Erfahrungen aus dem Besuch mehrerer Polizeidienststellen waren gemischt:

Aus Sicht des Datenschutzes geben die technischen und organisatorischen Maßnahmen keinen Anlass zur Kritik. Jedes Polizeirevier hat seine eigenen Geräte, jedes Polizeirevier speichert lokal seine eigenen Aufnahmen, ohne dass Dritte, auch andere Organisationseinheiten des Polizeipräsidiums, darauf zugreifen können. Die Rollen sind klar zugewiesen, die Abläufe strukturiert und transparent. Dieses insgesamt überaus positive Bild wurde leider getrübt, als wir uns willkürlich ausgewählte Filmaufnahmen anzeigen ließen.

Dazu muss man vorausschicken, dass das Polizeigesetz klare Regeln aufstellt, wann diese Technik zu Einsatz kommen darf. Es

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

ist zu unterscheiden: kommen die Polizeibeamtinnen und -beamten im Rahmen ihres Streifendienstes in potenziell gefährliche Situationen, darf die erste Stufe der Bodycam, das sogenannte Pre-Recording, in Gang gesetzt werden. Dabei werden Videosequenzen in einer Länge von 60 Sekunden in einer Schleife aufgenommen. Das heißt, die Kamera zeichnet fortlaufend immer nur insgesamt eine Minute des Geschehens auf. Optisch ist diese Funktionsart an der Kamera sichtbar, wobei immer auch mündlich darauf hingewiesen wird, dass eine Aufzeichnung erfolgt. Hat diese niederschwellige Maßnahme die gewünschte deeskalierende Wirkung, muss die Kamera wieder abgeschaltet werden und die Aufnahme wird automatisch gelöscht.

Tritt der erwünschte Erfolg nicht ein, kann durch erneuten Knopfdruck die dauerhafte Aufnahme und Speicherung des Geschehens aktiviert werden. Neben den letzten 60 Sekunden wird dann solange gespeichert, bis die Kamera wieder ausgeschaltet wird. Auch diese Funktionsart wird optisch sichtbar gemacht. Allerdings ist die gesetzliche Hürde für solche dauerhaften Aufnahmen hoch: es müssen Tatsachen die Annahme rechtfertigen, dass die Speicherung zum Schutz von Polizeibeamten oder Dritten gegen eine Gefahr für Leib und Leben erforderlich ist. Folglich sind Aufnahmen etwa von Ordnungswidrigkeiten oder Beleidigungen grundsätzlich unzulässig. Ebenfalls unzulässig sind Aufnahmen an Orten, die nicht öffentlich zugänglich sind.

Bei Besuchen von insgesamt drei Polizeirevierern wurde eine Reihe von Bodycam-Aufnahmen in Augenschein genommen. Weit überwiegend handelte es sich dabei Situationen, denen möglicherweise körperliche Angriffe vorausgegangen waren. Zum Zeitpunkt und im Verlauf der Aufnahmen wa-

ren diese jedoch jedenfalls abgeschlossen und nichts deutete darauf hin, dass von den betroffenen Personen konkret weitere Angriffe ausgehen würden oder ausgehen konnten. Folgende Beispiele hierzu:

In einem Fall ging es um eine Blutentnahme: die betroffene Person saß auf einem Stuhl und diskutierte mit der Ärztin und den Beamten. Die Blutentnahme erfolgte ohne Gegenwehr. In zwei Fällen wurden ausschließlich Ordnungswidrigkeiten dokumentiert: einmal ging es um „Wildpinkler“, zum anderen um eine wortreiche Auseinandersetzung mit einem Autofahrer, der offenbar den Sicherheitsgurt nicht angelegt hatte, von dem aber keinerlei Aggressivität ausging. In einem weiteren Fall wurde ein Platzverweis dokumentiert, wobei gefilmt wurde, wie ein Beamter in gehörigem Abstand zur betroffenen Person dieser über mehrere Minuten zu Fuß folgte. Häufig waren die Fälle, in denen die betroffene Person bereits mit auf dem Rücken gefesselten Händen bewegungsunfähig auf dem Boden lag; in einem Fall knieten Beamte auf den Rücken des Betroffenen, im anderen Fall lag er rücklings auf dem Boden eines Polizeifahrzeugs. In einem weiteren Fall saß die Person mit angelegtem Sicherheitsgurt auf dem Rücksitz eines Einsatzfahrzeugs, hatte die Beine entspannt übereinandergeschlagen und äußerte sich (sinngemäß) dahin gehend, alles Weitere über sich ergehen zu lassen.

In fast keinem der von uns in Augenschein genommenen Aufnahmen sahen wir die gesetzlichen Voraussetzungen für den Bodycam-Einsatz, wie sie in § 21 Absatz 6 des Polizeigesetzes (PolG) geregelt sind, als erfüllt an. Hieraus ist zu schließen, dass vielen Polizeibeamtinnen und -beamten offenbar nicht bekannt oder jedenfalls nicht präsent ist, dass Bodycams nicht dazu gedacht sind, jedes polizeilich relevante

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

Geschehen zu dokumentieren, vielmehr die gesetzliche Hürde für den Einsatz der Bodycams verhältnismäßig hoch ist. Die Videodokumentation von Polizeieinsätzen mittels Bodycam kann auch nicht auf eine strafprozessuale Rechtsgrundlage gestützt werden. Die Voraussetzungen des hierfür allein in Betracht zu ziehenden § 100h der Strafprozessordnung liegen regelmäßig nicht vor.

Daneben stellt sich folgendes weiteres Problem: Teilweise erfolgten die Aufnahmen innerhalb von Polizeifahrzeugen oder in Dienstgebäuden. Der Wortlaut des Gesetzes beschränkt den Einsatz von Bodycams dagegen auf polizeiliche Maßnahmen „an öffentlich zugänglichen Orten“. In der einschlägigen Dienstanweisung Bodycam heißt es dazu: „Gemeint sind Orte, die tatsächlich für jedermann zugänglich sind, wie z. B. Straßen, Wege, Plätze, Ladepassagen sowie Bereiche des ÖPNV“. Nun dürften Polizeidienstgebäude und Polizeieinsatzfahrzeuge kaum als öffentlich zugängliche Orte in diesem Sinnen gelten. Formal dürfen Bodycams danach dort auch nicht zum Einsatz kommen, wenngleich Hintergrund für die gesetzliche Regelung eigentlich die Gewährleistung der grundrechtlich geschützten Unverletzlichkeit der Wohnung (Artikel 13 GG) war, was auf die genannten Räumlichkeiten eigentlich nicht zutrifft.

Ein dritter Punkt, der Anlass zur Kritik gibt, ist die praktische Umsetzung der Lösungsregelung. Bodycam-Aufnahmen werden nach ihrer Speicherung verschiedenen Kategorien zugewiesen, je nachdem, zu welchem Zweck sie weiterverarbeitet werden sollen. Insbesondere geht es dabei um die Verwendung in einem Strafverfahren oder einem Verfahren über Ordnungswidrigkeiten. Daneben gibt es noch die Kategorien „Schutz privater

Rechte Dritte“, was nach übereinstimmender Auffassung in der Praxis keinerlei Rolle spielt, und „keine Relevanz“. Insbesondere bezüglich der letztgenannten Kategorie sieht das Gesetz vor, dass die Aufnahmen „unverzüglich, spätestens jedoch nach vier Wochen“ zu löschen sind. Praktisch werden diese Aufnahmen generell vier Wochen lang gespeichert, was zum Teil damit begründet wird, man wolle damit den Betroffenen die Gelegenheit geben, ihren Auskunftsanspruch geltend zu machen. Dies ist zwar grundsätzlich zu begrüßen. Gleichwohl führt diese Praxis zu einer Umkehr des gesetzgeberischen Willens, der das sofortige Löschen („unverzüglich“) als Regel und das längere Speichern („spätestens“) als Ausnahme vorgesehen hat, wobei es hierfür in jedem Einzelfall einer Begründung bedürfte.

Als Fazit kommen wir zu Folgendem:

Die Verantwortlichen sind in der Pflicht, die Polizeibeamtinnen und Polizeibeamten nicht nur einmal, sondern regelmäßig, gegebenenfalls im Rahmen des Einsatztrainings, im rechtmäßigen Umgang mit der Bodycam zu schulen.

Aufgabe der örtlichen Datenschutzbeauftragten ist es, Bodycam-Aufnahmen regelmäßig zu prüfen und steuernd einzugreifen, wenn festgestellt wird, dass rechtliche Voraussetzungen nicht beachtet wurden.

Der Einsatz von Bodycams in Polizeidienstgebäuden und Polizeieinsatzfahrzeugen ist nach derzeitiger Rechtslage unzulässig.

Die Umsetzung der Speicherfristen in der Praxis ist kritisch zu überprüfen und durch interne Maßgaben auf das zulässige Maß zu beschränken.

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

Unsere Besuche und die dabei gewonnenen Erkenntnisse sprachen sich in der Polizei rasch herum. In der Folge kam es zu einem Treffen mit dem Innenministerium/Landespolizeipräsidium. Dabei räumte das Innenministerium ein, dass die polizeiliche Praxis der Kameranutzung, jedenfalls in den von uns geprüften Fällen, auch nach dortiger Auffassung nicht den gesetzlichen Vorgaben entsprochen haben. Es wurde eine Aufarbeitung in Aussicht gestellt, deren Ergebnis uns nach kurzer Zeit erreichte. Darin teilte uns das Landespolizeipräsidium mit, dass man umfangreiche Steuerungsmaßnahmen zur Gewährleistung eines rechtskonformen Kameraeinsatzes veranlasst habe. So habe man die Leiter der örtlichen Polizeipräsidien auf ein Maßnahmenpaket verpflichtet, das Folgendes beinhaltet: Nochmals klargestellt wurde, dass die Strafprozessordnung nicht quasi durch die Hintertür als Rechtsgrundlage für einen allein beweissichernden Einsatz der Bodycams herangezogen werden könne; dies war schon in der entsprechenden Dienstanweisung so festgelegt, wurde in der Praxis aber wohl nicht immer auch so verstanden. Weiter wurde die unverzügliche Löschung von Aufnahmen in den Fällen, in denen diese nicht für weitere strafprozessuale Zwecke oder für Zwecke der Ahndung von Ordnungswidrigkeiten benötigt werden, angeordnet. Damit dürfte die routinemäßige Anwendung der vierwöchigen Maximalspeicherfrist hoffentlich der Vergangenheit angehören. Neben einer verbesserten Dokumentations- und Kontrollpflicht wurde bestimmt, dass der Einsatz der Bodycams in Dienstgebäuden und Dienstfahrzeugen nicht zulässig sei.

Insgesamt war die Reaktion der Polizeiführung auf unsere Prüfungsergebnisse damit konstruktiv und zielführend. Erneut hat sich gezeigt, dass vertrauensvolle Zusammenarbeit zwischen der Polizei Ba-

den-Württemberg und meiner Dienststelle regelmäßig zu greifbaren Ergebnissen im Sinne eines rechtskonformen Umgangs mit personenbezogenen Daten der Bürgerinnen und Bürger führt.

1.5 Datenpannen in Arztpraxen

Eine Vielzahl der auch 2019 an meine Dienststelle gesandten Datenpannenmeldungen betraf Arztpraxen aus Baden-Württemberg. Eine interne Auswertung solcher Meldungen ergab, dass in einer Top 7-Liste der häufigsten Ursachen gemeldeter Pannen der Postfehlversand auf Platz 1 rangierte, der E-Mail-Fehlversand auf Platz 3, die Versendung einer E-Mail mit offenem Adressverteiler auf Platz 5 und der Faxfehlversand auf Platz 7. Der Umstand, dass durch Fehlversand von Arztbriefen, Rezepten oder Röntgenbildern oft auch besonders sensible und schützenswerte Gesundheitsdaten der Patienten in die falschen Hände geraten, gab besonderen Anlass zur gründlichen Befassung mit diesem Thema. Datenpannen, bei denen Arztpraxen Opfer von Cyberangriffen wurden (Platz 2 der Top 7-Liste), sind Gegenstand des Beitrags „Technisch-organisatorischer Datenschutz“ unter Nummer 1.9 dieses Tätigkeitsberichts.

Die seit dem 25. Mai 2018 in Kraft befindliche Datenschutz-Grundverordnung der EU (DS-GVO) regelt in ihrem Artikel 33 Absatz 1 Satz 1, unter welchen Voraussetzungen eine Datenpanne gemeldet werden muss:

„Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.“

Demnach ist die zentrale Voraussetzung für eine solche Meldung eine „Verletzung des Schutzes personenbezogener Daten“. Was darunter zu verstehen ist, ergibt sich aus Artikel 4 Nr. 12 DS-GVO:

Eine „Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“.

Die Meldepflicht nach Artikel 33 Absatz 1 Satz 1 DS-GVO ist demnach weit gefasst. Wenn auch die baden-württembergischen Ärztinnen und Ärzte diese weitreichende Meldepflicht erkennen und erfüllen, ist dies erfreulich. Anhaltspunkte für eine hohe Dunkelziffer an nicht gemeldeten Fällen habe ich – anders als mein Amtsvorgänger unter der Geltung des § 42a des Bundesdatenschutzgesetzes in der alten, bis zum 24. Mai 2018 geltenden Fassung – nicht (vgl. den 32. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Baden-Württemberg für die Jahre 2014/2015, Beitrag Nr. 7.10 Informationspflicht bei Datenschutzverstößen, Drucksache 15/7990 des Landtags von Baden-Württemberg vom 21. Januar 2016, S. 129 ff., im [Internetangebot](#) meiner Dienststelle abrufbar). Es sind im Gegenteil auch nicht meldepflichtige Fälle an mein Amt gemeldet worden, beispielsweise darüber, dass ein Patient einen Teil ihm gehörender Dokumente im Wartezimmer der Praxis liegen gelassen hat.

Gravierende Probleme sind mit solchen vom Gesetz nicht geforderten Meldungen, jedenfalls aus der Sicht meiner Dienststelle, nicht verbunden: Lieber eine Meldung zu viel als eine zu wenig.

Wenn eine Datenpanne – bedauerlicherweise – vorgekommen ist und gemeldet wird, geht es mir insbesondere auch darum, dass Vergleichbares künftig vermieden wird. Nach Artikel 33 Absatz 3 Buchstabe d DS-GVO muss die Meldung an mein Amt „eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen“ enthalten. Daher findet sich in dem von meinem Amt angebotenen – und zur Nutzung auch hier ausdrücklich empfohlenen – [Formular für Online-Meldungen](#) solcher Pannen u. a. die Frage „Welche Gegenmaßnahmen haben Sie bereits eingeleitet, welche weiteren Gegenmaßnahmen sind geplant?“ vor einem großzügig bemessenen Freitextfeld. Hier kann im Fall eines Faxfehlerversands beispielsweise eingetragen werden, dass die Empfehlungen zum Faxversand in meiner [FAQ-Liste zum Datenschutz in der Arztpraxis](#) in der Praxis (erneut) bekannt gemacht sowie die mit dem Faxversand befassten Mitarbeiterinnen und Mitarbeitern geschult und entsprechend angewiesen werden. In anderen Fällen kann es sinnvoll sein, als Gegenmaßnahme wirksame Verschlüsselungen einzuführen und dies in der Meldung mitzuteilen. Fehlern, die auf mangelnde Sorgfalt zurückzuführen sind, kann beispielsweise durch Etablierung gut strukturierter und beherrschbarer Routinen, klare Anweisungen und die Einführung des Vier-Augen-Prinzips für besonders heikle Vorgänge begegnet werden. Bei allen ergriffenen Maßnahmen zur

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

Beseitigung von Fehlerquellen erwarte ich zudem, dass sie in regelmäßigen Zeitabständen sowie überdies anlassbezogen auf ihre Wirksamkeit überprüft und bei Bedarf angepasst werden.

Daneben ist bei Datenpannen in Arztpraxen für mich von besonderer Bedeutung, ob die davon betroffene Person (in vielen Fällen der Patient) zu benachrichtigen ist und benachrichtigt wurde. Artikel 34 Absatz 1 DS-GVO fordert:

„Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.“

Ein solches hohes Risiko ist nach meiner Einschätzung grundsätzlich dann gegeben, wenn Gesundheitsdaten

(im Sinne der Begriffsbestimmung des Artikels 4 Nr. 15 DS-GVO:

„personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“)

Objekte einer meldepflichtigen Datenpanne sind. Viele Datenpannenmeldungen, die etwa den Fehlversand eines Arztbriefs zum Gegenstand hatten, enthielten zu meiner Verwunderung die Aussage, man sehe bei der Arztpraxis keine Benachrichtigungspflicht nach Artikel 34 Absatz 1 DS-GVO, weil das Risiko als gering oder nicht vorhanden betrachtet werde. Solchen lapidaren und rechtlich nicht fundierten Äußerungen bin ich regelmäßig entgegengetreten. Na-

türlich bin ich mir des Umstands bewusst, dass es von dem erwähnten Grundsatz der Benachrichtigungspflicht Ausnahmen geben kann. Beispielsweise dann, wenn ein unbefugter Empfänger fehlgeleiteter Gesundheitsdaten, etwa wegen Verschlüsselung und anderer Einschränkungen, die Klardaten gar nicht zur Kenntnis nehmen konnte. Wenn eine Arztpraxis Anhaltspunkte dafür hat, dass ein solcher Ausnahmefall vorliegt, kann sie dies in ihrer Datenpannenmeldung unter Darstellung des insofern relevanten außergewöhnlichen Sachverhalts und ihrer Erwägungen gerne tun.

Bei Datenpannen in Arztpraxen geht es typischerweise um Gesundheitsdaten. Soweit etwa (auch) genetische Daten oder andere besondere Kategorien personenbezogener Daten i.S.v. Artikel 9 DS-GVO betroffen sind, gilt das hier zu Gesundheitsdaten Gesagte entsprechend. Welche anderen Kategorien hier zu berücksichtigen sind, ergibt sich aus Artikel 9 Absatz 1 DS-GVO:

„Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.“

Diese Ausführungen über die Benachrichtigungspflicht nach Artikel 34 Absatz 1 DS-GVO mit Blick auf Gesundheitsdaten gelten sinngemäß auch für andere Akteure des Gesundheitswesens, wie beispielsweise Krankenhäuser und Pflegeeinrichtungen.

Wer sich vertieft mit den datenschutzrechtlichen Anforderungen bei Datenpannen befassen will, kann beispielsweise die „Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679“ der ARTIKEL-29-DATENSCHUTZGRUPPE (einem [früheren] europäischen Beratungsgremium für den Schutz personenbezogener Daten und der Privatsphäre) studieren, die im [Internetangebot](#) meiner Dienststelle abrufbar sind.

1.6 E-Mail-Werbung nach UWG – eine Ausnahmeregelung in engen rechtlichen Grenzen

E-Mail-Werbung ist grundsätzlich nur mit vorheriger, informierter Einwilligung des Betroffenen erlaubt, es sei denn, dass alle Voraussetzungen des § 7 Absatz 3 des Gesetzes gegen den unlauteren Wettbewerb (UWG) erfüllt sind. Diese Norm stellt somit als Ausnahmeregelung eine gesetzliche Erlaubnis für E-Mail-Werbung auch ohne Zustimmung des Betroffenen dar. Die Beratungs- und Beschwerdepraxis in meiner Behörde zeigt jedoch, dass es die werbenden Unternehmen mit der Einhaltung der Voraussetzungen des § 7 Absatz 3 UWG oft nicht so genau nehmen – und damit gegen Wettbewerbsrecht und folglich auch gegen Datenschutzrecht verstoßen.

E-Mail-Werbung nach § 7 Absatz 3 UWG ist nur dann zulässig, wenn kumulativ alle Voraussetzungen dieser Norm erfüllt werden:

1. Ein Unternehmer muss im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten haben (§ 7 Absatz 3 Nr. 1 UWG).
2. Der Unternehmer verwendet die Adresse zur Direktwerbung für eigene ähn-

liche Waren oder Dienstleistungen (§ 7 Absatz 3 Nr. 2 UWG).

3. Der Kunde hat der Verwendung zu Werbezwecken nicht widersprochen (§ 7 Absatz 3 Nr. 3 UWG).
4. Der Kunde wurde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen (§ 7 Absatz 3 Nr. 4 UWG).

Zu 1.: Bestehende Kunden-Beziehung (Bestandskunde)

Es muss zuvor ein Vertrag zwischen dem werbenden Verantwortlichen und dem beworbenen Kunden geschlossen worden sein. Im Rahmen dieses Vertragsschlusses muss der Unternehmer die E-Mail-Adresse vom Kunden erhalten haben. Auch eine kostenlose Mitgliedschaft etwa in einer Partnerschaftsbörse führt zu einem Vertragsverhältnis über eine Dienstleistung (OLG München, Urteil vom 15. Februar 2018, Az. 29 U 2799/17). Ebenso verhält es sich während eines Probe- oder Schnupper-Abonnements.

Der Wunsch des Kunden, einen Kostenvoranschlag oder ein Angebot erhalten zu wollen, genügt hier jedoch nicht. Tritt der Kunde wirksam vom Vertrag zurück, entfällt von diesem Zeitpunkt an diese Rechtsgrundlage, ebenso bei einer erfolgreichen Anfechtung des Vertrages. § 7 Absatz 3 UWG greift auch nicht (mehr), wenn ein Verbrauchervertrag (§§ 312g, 355 BGB) wirksam widerrufen wurde.

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

Zu 2.: Eigenwerbung für ähnliche Waren oder Dienstleistungen

Der Verantwortliche darf E-Mail-Werbung für eigene – also nicht Werbung für Dritte oder für Produkte bzw. Dienstleistungen Dritter – ähnliche Waren oder Dienstleistungen durchführen. Die E-Mail-Werbung muss also in einem engen Zusammenhang mit dem gekauften Produkt oder der erhaltenen Dienstleistung stehen – in der Praxis der schwierigste Punkt.

§ 7 Absatz 3 UWG ist also regelmäßig keine Rechtsgrundlage für die Zusendung eines allgemeinen Unternehmens-Newsletters mit Angeboten über das gesamte Sortiment bzw. Leistungsangebot des Unternehmens. Die „Ähnlichkeit“ ist vielmehr im Sinne dieser Ausnahmvorschrift eng auszulegen, um die Kunden vor unerbetener Werbung zu schützen.

Doch was ist unter dem Begriff „Ähnlichkeit“ zu verstehen? Hierzu hat das Thüringer Oberlandesgericht (Urteil vom 21. April 2010, Az. 2 U 88/10) ausgeführt: „Die Ähnlichkeit muss sich auf die bereits gekauften Waren beziehen und dem gleichen typischen Verwendungszweck oder Bedarf des Kunden entsprechen; ggf. ist es noch zulässig, Zubehör oder Ergänzungswaren zu bewerben.“

Eine Austauschbarkeit, wie vom Kammergericht Berlin gefordert (Beschluss vom 18. März 2011, Az. 5 W 59/11), sozusagen das Höchstmaß an Ähnlichkeit, ist rechtlich selbstverständlich zutreffend, werbemäßig aber (für beide Seiten) eher weniger interessant: Es macht kaum Sinn, nur für das konkrete Produkt werben zu dürfen, das der Kunde gerade erst gekauft hat (und daher in der Regel nicht unbedingt ein 2. Mal benötigt). Daher spricht das Gesetz auch von „ähnlich“ und nicht von „identisch“.

Unter Berücksichtigung der o. g. Rechtsprechung und einschlägigen Literaturmeinungen sowie zum Zwecke der Entwicklung einer handhabbaren Auslegung ist aus der Sicht des Landesbeauftragten eine Ähnlichkeit der

- beworbenen Ware regelmäßig dann gegeben, wenn
 - ◇ diese der typischen Einsatz- und Verwendungsmöglichkeit der gekauften Ware entspricht oder
 - ◇ es sich um klassisches Zubehör oder Ersatzteile zu der gekauften Ware handelt oder
 - ◇ es sich in einem engen Verwendungszusammenhang um eine verkehrszubehörende Ergänzungsware zu der gekauften Ware handelt.
- beworbenen Dienstleistung regelmäßig dann gegeben, wenn
 - ◇ diese dem typischen Leistungsziel der erbrachten Dienstleistung entspricht oder
 - ◇ es sich um klassisches Zubehör zu der erbrachten Dienstleistung handelt oder
 - ◇ es sich um verkehrszubehörende Zusatz- oder Ergänzungsdienstleistungen zu der erbrachten Dienstleistung handelt.

Entscheidend ist natürlich stets der konkrete Einzelfall. Je öfter ein Kunde beim Unternehmen unterschiedliche Waren und Dienstleistungen einkauft, umso umfangreicher wird natürlich die Werbemöglichkeit.

Beispiele bzgl. Waren und Dienstleistungen finden Sie im Anhang.

Kundenbewertungs- oder Kundenzufriedenheitsanfragen per E-Mail, die stets als Werbung einzustufen sind – und zwar auch

dann, wenn diese Anfragen unmittelbar nach einem Produkterwerb und zusammen mit der Rechnung übersendet werden (Bundesgerichtshof, Urteil vom 10. Juli 2018, Az.: VI ZR 225/17) –, fallen nicht unter § 7 Absatz 3 UWG (wegen eines völlig anderen Zwecks) und sind daher ohne vorherige Einwilligung stets datenschutzwidrig (aber leider weit verbreitet).

Zu 3.: Kein bestehender Werbewiderspruch des Kunden

Der Kunde darf der E-Mail-Werbung zuvor nicht nach Art. 21 Absatz 2 DS-GVO widersprochen haben. Der Kunde muss insbesondere die Möglichkeit haben, dieser werblichen Nutzung seiner E-Mail-Adresse bereits zum Zeitpunkt der Erhebung seiner E-Mail-Adresse, also noch während des Bestellvorgangs im Online-Shop, zu widersprechen. Dies gebietet Artikel 13 Absatz 2 der Datenschutzrichtlinie für elektronische Kommunikation. Näheres hierzu finden Sie im [Tätigkeitsbericht 2014/2015, S. 156 f.](#)

Zu 4.: Hinweis auf jederzeitige Widerspruchsmöglichkeit zu Normaltarifen (Abmeldemöglichkeit)

Jede Werbe-E-Mail muss den leicht auffindbaren und gut lesbaren Hinweis enthalten, dass und wie der Werbung jederzeit zu Normaltarifen widersprochen werden kann. An dieser Stelle hat sich das Angebot eines Abmelde-links bewährt.

Auf die Ähnlichkeit kommt es an: § 7 Absatz 3 UWG ist kein Freibrief für allgemeine Produkt- und Dienstleistungswerbung. Bei jeder/jedem einzelnen Kundin/Kunden muss je nach bisherigem Kaufverhalten (Warenkorb) genau geprüft bzw. abgeklärt werden, für welche ähnlichen Waren und Dienstleistungen geworben werden darf.

1.7 Das Auskunftsrecht nach Artikel 15 Absatz 1 Buchst. c DS-GVO: Volle Transparenz für die Betroffenen gerade auch bei Datenübermittlungen

Das Auskunftsrecht nach Art. 15 DS-GVO gehört zu den zentralen Rechten der Betroffenen. Nur, wenn ich weiß, welche Daten der Verantwortliche über mich gespeichert hat, zu welchen Zwecken er diese verarbeitet und wohin er die Daten übermittelt, kann ich meine Rechte aus Kapitel III der DS-GVO wirksam und vollumfänglich geltend machen. Dennoch gibt es Unternehmen, die gegenüber den Betroffenen behaupten, wählen zu können, ob sie bei Datenübermittlungen die konkreten Empfänger dieser Daten übermitteln oder nur Empfängerkategorien.

Gerade dann, wenn der Verantwortliche personenbezogene Daten an Dritte übermittelt (z. B. im Zuge des Adresshandels vermietet oder verkauft), wächst die Gefahr beim Betroffenen, nicht mehr Herr/Frau über seine Daten zu sein, steigt das Risiko, nicht mehr zu wissen, wer alles im Besitz seiner Daten ist. Der Betroffene will daher genau wissen, wohin welche Daten gegeben wurden.

Im Hinblick auf Datenübermittlungen regelt Art. 15 Absatz 1 Buchst. c DS-GVO:

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

(...)

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;

Beschwerdeführer haben oftmals moniert, dass angefragte Unternehmen in ihrer Auskunft bei Datenübermittlungen lediglich abstrakt die Kategorien von Empfängern der Daten benennen, nicht aber konkret die Unternehmen aufführen würden, auch nicht auf erneute Rückfrage. Sie verwiesen stets auf ihr gesetzliches Wahlrecht, entweder den konkreten Empfänger oder eben nur eine Empfängerkategorie nennen zu dürfen. Teilweise, so etwa ein Adresshändler, würden die Empfänger auch gar nicht dokumentiert.

Diese Sichtweise lehnt der Landesbeauftragte entschieden ab, sie ist mit der DSGVO nicht vereinbar. Allein das Nennen von Kategorien von Empfängern (z. B. Autohäuser, Wirtschaftsauskunfteien, Online-Händler) hilft dem Betroffenen kaum weiter und hat auch mit größtmöglicher Transparenz nichts zu tun.

Wenn es hier überhaupt um ein Wahlrecht gehen würde, stünde dieses außerdem nur dem Betroffenen zu, da es in diesem Abschnitt der DSGVO um dessen Rechte geht.

Entscheidend ist aber, dass es aus dem Grundsatz der Transparenz heraus sowie wegen des Wortlauts der Regelung nicht im Belieben des Verantwortlichen steht, wie konkret er die Auskunft beantwortet.

Soweit Daten schon an Dritte übermittelt worden sind, müssen diese konkret benannt werden. Sind Übermittlungen vorgesehen, genügt es, die Kategorien dieser Dritten aufzuzählen, soweit diese absehbar sind; dies müsste sich aber auch

schon aus den Datenschutzhinweisen nach Art. 13, 14 DSGVO ergeben.

Das Auskunftsrecht nach Art. 15 DSGVO ist sozusagen das „Königsrecht“ der Betroffenen. Hier gilt für die Verantwortlichen beim Beauskunften größte Genauigkeit und Vollständigkeit. Dies betrifft insbesondere auch die konkrete und möglichst genaue Benennung der Empfänger von Daten (Art. 15 Absatz 1 Buchst. c DSGVO). Sobald Datenübermittlungen stattgefunden haben, sind die konkreten Stellen zu nennen, an die Daten übermittelt wurden. Bei geplanten Übermittlungen ist Auskunft über die Empfängerkategorien zu geben. Ein Höchstmaß an Transparenz – wie auch in Art. 5 Absatz 1 Buchst. a, Art. 12 DSGVO festgeschrieben – ist hier für die Verantwortlichen somit das Gebot der Stunde – und kann bei seiner Verletzung massive Folgen bis hin zu Bußgeldern haben.

1.8 Art. 15 DSGVO im Beschäftigtenkontext

Durch die DSGVO wurden die Betroffenenrechte umfassend erweitert. Besondere Bedeutung kommt hierbei dem Recht auf Auskunft und das Recht auf Kopie nach Art. 15 DSGVO, insbesondere im Beschäftigtenkontext, zu. Das Recht auf Auskunft ist hierbei ein fundamentales „Scharnier“ für die weitere Geltendmachung der übrigen Betroffenenrechte. Nur derjenige, der die ihn betreffenden Verarbeitungen kennt, kann in einem zweiten Schritt beispielsweise sein Recht auf Löschung (Art. 17 DSGVO) oder Berichtigung (Art. 16 DSGVO) effektiv vollziehen. Gleichzeitig stellen Auskunftsbegehren von Arbeitnehmern viele Arbeitgeber, besonders bei langen Betriebszugehörigkeiten, vor große Herausforderungen.

1. Recht auf Auskunft

Art. 15 DS-GVO enthält drei selbständige Ansprüche, die sich gegenseitig flankieren. Nach Art. 15 Absatz 1 DS-GVO besteht zunächst das Recht des Betroffenen, von der verantwortlichen Stelle zu erfahren, ob sie betreffende personenbezogene Daten verarbeitet werden.

Weiter kann die betroffene Person Auskunft hinsichtlich gesetzlich näher bestimmten Informationen, wie z. B. Zweck der Verarbeitung, Kategorien der verarbeiteten personenbezogenen Daten, Empfänger bzw. Kategorien von Empfängern der Daten oder Herkunft der Daten, verlangen (vgl. Art. 15 Absatz 1 lit. a bis h DS-GVO).

Daneben besteht gem. Art. 15 Absatz 3 DS-GVO das Recht auf „Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind“.

a) Daten im Beschäftigtenkontext

Im Beschäftigungsverhältnis bestehen unzählige Datenverarbeitungen, welche von (internen) Vermerken, Beurteilungen bis zu Korrespondenzen reichen. Zu beachten ist hierbei, dass den Arbeitnehmer*innen neben Art. 15 DS-GVO auch arbeitsrechtlich das Recht auf Einsicht in ihre Personalakte gem. § 83 BetrVG zusteht, welches allerdings nicht so weitreichend ist, wie Art. 15 DS – GVO. Das Recht auf Auskunft ist damit für die Kontrolle der Rechtmäßigkeit der Datenverarbeitungen, auch im Beschäftigtenkontext, unerlässlich.

b) Recht auf Kopie

Aus den durchgeführten aufsichtsrechtlichen Kontrollverfahren und Beratungsanfragen ist deutlich geworden, dass insbesondere das in Art. 15 Absatz 3 DS-GVO normierte „Recht auf Kopie“ besondere Be-

deutung zukommt und dies von Arbeitnehmern mit besonderem Nachdruck verfolgt wird. Dabei ist hervorzuheben, dass seitens des LAG Baden-Württemberg eine auch medial sehr beachtete Entscheidung (LAG Baden-Württemberg, Urte. v. 20. Dezember 2018 – 17 Sa 11/18) zugunsten einer umfangreichen Auslegung des Begriffs der „Kopie“ getroffen wurde. Demnach habe der Arbeitgeber die gespeicherten personenbezogenen Leistungs- und Verhaltensdaten dem Arbeitnehmer zur Verfügung zu stellen. Dabei sind zunächst der Begriff der „Leistungs- und Verhaltensdaten“ im Beschäftigungsverhältnis sehr offen und lassen kaum Eingrenzungen zu, zum anderen spielte die Entscheidung vor dem Hintergrund von unternehmensinternen Ermittlungen, sodass auch schützenswerte Belange und Anonymität von Hinweisgebern betroffen waren. Die Revision läuft derzeit am BAG unter dem Aktenzeichen 5 AZR 66/19. Es bleibt abzuwarten, ob das BAG den Schutz des Hinweisgebers wegen Art. 15 Absatz 4 DS-GVO den Vorrang vor dem Auskunftsanspruch zugestehen wird oder der Auffassung des LAG folgt.

c) Reichweite und Grenzen des Rechts auf Kopie

In der Praxis stellen hingegen primär pauschal gehaltene Auskunftsbegehren, insbesondere kleinere und mittlere Unternehmen, vor große Herausforderungen. Gerade im Beschäftigtenkontext haben sich nach vielen Jahren der Betriebszugehörigkeit umfänglichste personenbezogene Daten zu unterschiedlichsten Vorgängen angesammelt. Diese Datensätze dürfen aber einer Rechtmäßigkeitskontrolle nicht von vornherein, einzig mit dem Verweis auf den großen Umfang der bestehenden Datenbestände entzogen werden. Systematisch flankiert und ergänzt Art. 15 Absatz 3 den Absatz 1 und nor-

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

miert in Absatz 4 ausdrücklich den Vorbehalt der Beeinträchtigung von „Rechte und Freiheiten anderer Personen“. Legt man das eingangs genannte Ziel der Rechtmäßigkeitskontrolle der Datenverarbeitungen und diese Systematik zugrunde, so wird man im Grundsatz von einem umfassenden Auskunftsrecht und Recht auf Kopie ausgehen können, welches erst nach einer Abwägung der entgegenstehender „Rechte und Freiheiten anderer Personen“, gegebenenfalls durch Schwärzungen, seine Grenzen findet. Verantwortliche Stellen und Adressaten von Auskunftsbegehren müssen demnach, vor der Beauskunftung und dem zur Verfügungstellen der Kopien prüfen und abwägen, ob Rechte anderer Personen, also gegebenenfalls auch die Rechte anderer Arbeitnehmer*innen der Beauskunftung überwiegen oder ihr (temporär) entgegenstehen. Auch die Erwägungsgründe der DS-GVO stellen eine Auslegungshilfe zur Seite. So soll entsprechend Satz 5 des Erwägungsgrunds 63 zur DS-GVO das Auskunftsrecht keine „Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software“ beeinträchtigen. Auch hier können verantwortliche Stellen vor der Beauskunftung abwägen, ob ihre eigenen Geschäftsgeheimnisse der begehrten Auskunft überwiegen. Diese Vorbehalte müssen allerdings nachvollziehbar dokumentiert werden und dürfen nicht dazu führen, dass jegliche Auskunft pauschal verweigert wird.

Das Recht auf Auskunft und auf Kopie nach Art. 15 DS-GVO ist Grundvoraussetzung für die Geltendmachung der weiteren Betroffenenrechte. Der LfDI BW sowie andere Aufsichtsbehörden und Verbraucherorganisationen haben für Betroffene daher Muster zur Orientierung entwickelt, welche auf den Internetauftritten abrufbar sind (zum Beispiel auf [www.baden-wuert-](http://www.baden-wuerttemberg.datenschutz.de)

[temberg.datenschutz.de](http://www.baden-wuerttemberg.datenschutz.de)). Manche Auskunftsbegehren stellen insbesondere viele kleinere und mittlere Unternehmen vor enorme Herausforderungen. Der LfDI wird daher auch künftig, sowohl für Unternehmen im Beratungsfall, als auch betroffenen Personen im Beschwerdefall die jeweiligen Auskunftsbegehren begleiten.

1.9 Technisch-organisatorischer Datenschutz

Unser Technik-Referat hat im Jahr 2019 insgesamt über 25 Vor-Ort-Kontrollbesuche und unzählige schriftliche Kontrollverfahren durchgeführt. Einige der größten Datenpannen in Baden-Württemberg, über die auch in den Medien berichtet wurde – etwa die Hacks des Staatstheaters Stuttgart sowie der Landesmesse Stuttgart – wurden und werden durch das Technik-Referat aufgearbeitet. Durch die große Anzahl an Datenpannen konnten wir interessante Erkenntnisse gewinnen und bestimmte Angriffsmuster feststellen, über die im Folgenden berichtet werden soll.

Aktuelle Bedrohungen

Spear Phishing und Malware

Schadsoftware, die per E-Mail verbreitet wird, ist leider immer noch ein großes Problem in der Praxis. Inzwischen sind Mails mit Schädlingen derart „gut“ gemacht, dass es für Empfänger sehr schwer ist, zu erkennen, dass es sich dabei um einen Angriff handelt. Die Mails werden immer zielgerichteter, mit korrekter Anrede versehen und stammen dabei vermeintlich von Absendern, mit denen die Opfer in der Vergangenheit tatsächlich in Kontakt standen. Man spricht in diesem Zusammenhang auch von „Spear Phishing“. Einer der bekanntesten Vertreter von Malware, der diese Angriffsart nutzt, ist der extrem ge-

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

fährliche „Emotet“, meist in Kombination mit weiterer Schadsoftware wie „Trickbot“ und „Ryuk“.

Auf einem mit Emotet befallenen Rechner werden nicht nur die Adressbücher des betroffenen E-Mail-Clients, sondern auch die E-Mail-Inhalte ausgelesen und auf einen Server der Angreifer kopiert. Damit können diese weitere gezielte Angriffe durchführen, die mit den echten E-Mail-Inhalten täuschend echt erscheinen. Nach einem Emotet-Vorfall ist es daher zwingend, dass sämtliche E-Mails nach sensiblen personenbezogenen Daten, wie Gesundheitsdaten, Bankdaten, Bewerbungsdaten, etc. durchsucht werden und diesen Kontakten eine entsprechende Benachrichtigung über einen Datenabfluss (nach Art. 34 DS-GVO) zugeht. Die Benachrichtigung sollte dabei nicht einfach per E-Mail erfolgen. Zu oft werden solche E-Mails als Spam-Mails klassifiziert und erreichen entweder nicht ihre Empfänger oder werden einfach nicht beachtet. Eine E-Mail-Benachrichtigung stellt insofern keine geeignete Form der Benachrichtigung dar. Betroffene sollten über einen alternativen Kommunikationsweg kontaktiert werden: Telefon, Brief, etc. Unabhängig davon sollte bei einem Emotet-Befall immer eine Anzeige bei der [Zentralen Ansprechstelle Cybercrime](#) der Polizei erstattet werden.

Bei per E-Mail verbreiteter Schadsoftware kommen häufig Word- und Excel-Dokumente mit Makros zur Anwendung. Als erste Sicherheitsmaßnahme sollte eine Sensibilisierung der Mitarbeiter durchgeführt werden. E-Mail-Server sollten zudem so konfiguriert werden, dass sie potenziell schädliche (z. B. Makro-taugliche .docm, .xlsx usw.) und veraltete (z. B. .doc, .xls usw.) Dokumentenformate direkt bei der Einlieferung ablehnen. Als weitere Abhilfemaßnahmen kommt in Betracht, sowohl

E-Mail-Clients als auch Office-Programme in Containern oder Virtuellen Maschinen zu betreiben. Generell ist daher anzuraten, dass E-Mail-Clients nicht als Dokumenten-Management-Systeme für sensible personenbezogene Daten eingesetzt werden. D.h. E-Mails, und vor allem E-Mails mit sensiblen personenbezogenen Daten, sollten nach dem Eingang aus dem E-Mail-Client in eine geeignete Ablage verschoben werden. Eine geeignete Ablage ist dabei z. B. ein verschlüsseltes Dokumenten-Management-System oder zumindest eine verschlüsselte Dateiablage. Auch mit einer durchgehenden Ende-zu-Ende-Verschlüsselung kann das Risiko reduziert werden, dass sensible Daten nach einem erfolgreichen Angriff, z. B. mit Emotet, zu einer Datenpanne mit personenbezogenen Daten werden.

Achtung: Werden regelmäßig (sensible) personenbezogene Daten zwischen Unternehmen, Arztpraxen/Kliniken oder Behörden, etc. ausgetauscht, so entspricht E-Mail ohne Ende-zu-Ende-Verschlüsselung ohnehin nicht dem Stand der Technik.

Die Schadsoftware rund um Emotet ist auch deshalb so gefährlich, weil diese Malware noch weitere Funktionalitäten besitzt. So kommt es häufig auch zur Verschlüsselung des befallenen Systems und der Erpressung durch die Täter: Entweder zahlt der Verantwortliche das Lösegeld, oder er bekommt keinen Zugriff mehr auf seine Daten. Man spricht in diesem Zusammenhang auch von „Ransomware-Angriff“. Nicht selten haben Verantwortliche entweder überhaupt kein Backup ihrer Daten angelegt oder das Backup wurde bei dem Angriff ebenfalls komplett mitverschlüsselt. Es kommt also u. U. zu einem Verlust der Verfügbarkeit personenbezogener Daten und Verantwortliche entscheiden sich mitunter auch, das Lösegeld zu bezahlen

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

(so wurden mit einer ähnlichen Kampagne mittels der Malware „Gandcrab“ in einem Jahr 2 Mrd. Dollar erbeutet). Auch „kleine“ Firmen können bei einem mehrtägigem bis teils mehrwöchigem Ausfall ihres IT-Netzes und den dabei anfallenden Lohnkosten, entgangenen Aufträgen, Strafzahlungen durch nicht eingehaltene Termine, Reputationsverlust, Bußgeldern, Lösegeldforderungen der Hacker, Kosten für spezialisierte IT-Firmen etc. von einem mindestens fünf- bis sechstelligem Schaden ausgehen. **Der unsorgsame Umgang mit E-Mails kann also schnell existenzbedrohend werden.**

Angreifer versuchen bei einem Befall in der Regel Zugriff auf zentrale Systeme wie Domaincontroller zu erlangen und die Schadsoftware im Anschluss auf allen angeschlossenen Systemen zu verbreiten. Daher müssen diese besonders und mit anderen Zugangsdaten abgesichert werden. Ähnliches gilt für Backup-Server: Angreifer versuchen vor dem Verschlüsseln der Daten zuerst alle Backups unbrauchbar zu machen. Daher sollten Backup-Server nicht an zentralen Authentifizierungsdiensten wie Active Directory hängen und ein anderes Betriebssystem nutzen. Clients sollten keine Möglichkeit haben, die Backups zu zerstören oder zu überschreiben. Regelmäßige Offline-Backups erhöhen die Sicherheit.

Empfehlungen:

- Die Nutzer sollten sensibilisiert werden (es sollte auf die aktuellen Gefahren in Bezug auf Spear Phishing hingewiesen werden). Im besten Fall öffnen die Nutzer dann keine schadhaften Anhänge mehr. Falls ein Angriff doch erfolgreich stattfindet, sollten Nutzer aber keine Angst vor Konsequenzen haben und sie sollten den Vorfall umgehend melden.

Es ist wichtig, dass es eine funktionierende Meldekette gibt und befallene Systeme umgehend vom Netz getrennt und (im Fall von Emotet) im Anschluss komplett neu installiert werden.

- Falls es E-Mails mit sensiblen Daten geben sollte, dann sollten diese zeitnah aus dem Postfach gelöscht werden, damit es zu keinen Datenschutz-Problemen durch Malware kommt.
- Backups müssen von der restlichen Umgebung getrennt sein und Backup-Server eigene Authentifizierungen nutzen. Backups sollten auch offline vorhanden sein, damit diese bei einem Vorfall nicht mit verschlüsselt werden. Es sollten Maßnahmen ergriffen werden, damit sich Malware nicht im internen Netz weiter ausbreiten kann. Die Ausführung von Makros sollte standardmäßig deaktiviert sein.

Das BSI hat sehr gute Empfehlungen zu diesem Thema bereitgestellt.

Unzureichende Absicherung des Fernwartungszugangs

Überraschend oft wurden 2019 Datenpannen gemeldet, die über nicht oder nicht ausreichend abgesicherte Fernwartungszugänge erfolgten. Überraschend deshalb, da diese Fernwartungszugänge permanent aktiv waren und teilweise die Zugangs-Passwörter mit abgespeichert oder die Zugänge nicht vor Brute-Force-Angriffen geschützt waren. Einfacher kann man es einem Angreifer letztlich nicht machen. Die Einhaltung der Basis-Anforderungen aus dem Baustein OPS.2.4 Fernwartung des BSI IT-Grundschutz-Kompendiums 2019 hätte derartige Angriffe verhindert. Dort wird unter anderem gefordert: „Die

Initiierung des Fernwartungs-Zugriffs MUSS aus der Institution heraus erfolgen. Der Benutzer des fernadministrierten IT-Systems MUSS dem Fernzugriff explizit zustimmen.“ und „[Es] MÜSSEN alle Kommunikationsverbindungen nach vollzogenem Fernzugriff getrennt werden (Deaktivierung).“. Der Stand der Technik verlangt, dass Verantwortliche zur Erfüllung der Pflichten nach Art. 32 der DS-GVO nicht aus Komfortgründen das Risiko eines permanent aktiven (und offenen) Fernwartungszugangs eingehen. Aber nicht nur Verantwortliche haben dies zu beachten, auch Auftragsverarbeiter, die aus Komfortgründen ihren Kunden einen solchen einfachen Zugang nahelegen, begehen hier einen Verstoß gegen Artikel 28 Absatz 3 Buchstabe f und Artikel 32 der DS-GVO.

Unzureichende Benachrichtigung der Verantwortlichen durch Dienstleister

Stellt ein Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten fest, meldet er diese unverzüglich dem Verantwortlichen. Diese Forderung aus Artikel 33 Absatz 2 der DS-GVO dürfte wohl allen Auftragsverarbeitern bekannt sein. Weniger bekannt ist, wie diese Meldung dem Zweck angemessen durchgeführt werden kann. Der Verantwortliche soll in die Lage versetzt werden, entsprechende Maßnahmen nach Artikel 33 f. DS-GVO ergreifen und entsprechende Gegenmaßnahmen durchführen zu können. Kann eine Meldung über den ansonsten für Werbung verwendeten E-Mail-Verteiler angemessen sein? Nein! Sollte überhaupt eine E-Mail für die Benachrichtigung verwendet werden? Zumindest nicht alleine. Ein zusätzlicher Anruf, Fax oder Einschreiben stellt sicher, dass die Nachricht den Verantwortlichen auch wirklich erreicht und stellt sicher, dass der Auftragsverarbeiter eine geeignete Benachrichtigung des Ver-

antwortlichen auch dokumentieren kann. Es sollte im Auftragsverarbeitungsvertrag geregelt werden, wer und wie bei einer Datenpanne benachrichtigt werden soll.

Hacker-Angriffe auf Online-Konten von Prominenten und Politikern

Anfang Januar 2019 wurde bekannt, dass mehrere Online-Konten deutscher Politiker und Prominenter gehackt und dadurch im Dezember 2018 viele private Daten veröffentlicht wurden („Doxing“). In einer Übersichtsliste waren 994 Politiker und Prominente erwähnt, insgesamt waren aber die Kontaktdaten von weitaus mehr Personen betroffen. „Gehackt“ wurden nur eine mittlere zweistellige Zahl an Social Media-Profilen von Betroffenen. Da viele davon aber ihre Adressbücher zu dem Anbieter der Social-Media-Plattformen hochgeladen haben, hatte der Angreifer Zugriff auf die Kontaktdaten von rund 40.000 Personen. Zudem hat der Angreifer zahlreiche private und intime Nachrichten bzw. Unterhaltungen, die Betroffene auf den Plattformen geführt haben, sowie diverse Dokumente aus Cloud-Speicher-Diensten veröffentlicht. Darunter befanden sich neben privaten Briefen, Rechnungen und Fotos teilweise auch Abbildungen von Ausweisdokumenten.

Diese Dokumente wurden primär auf verschiedenen Plattformen im Internet veröffentlicht, die sich auf die Verbreitung von rechtswidrigen Inhalten spezialisiert haben. Wir konnten teilweise eine Löschung dieser Daten auch im außereuropäischen Ausland erreichen. Die im Raum stehenden hohen Bußgelder waren dabei – auch in Übersee – oftmals ein gutes Argument für die Hosting-Anbieter, die Plattformbetreiber zum Löschen zu bewegen; weitere Verfahren laufen noch. Einige Fälle haben wir zuständigkeitshalber an andere euro-

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

päische Aufsichtsbehörden abgegeben, allerdings bisher noch mit keinem vorzeigbaren Ergebnis.

Der Fall zeigt exemplarisch mehrere Problembereiche auf: So ist das Freigeben von Adressbüchern für Social Media-Plattformen sehr kritisch zu betrachten. Diese Plattformen verwenden die Daten i. d. R. auch zu eigenen Zwecken, beispielsweise zur Profilbildung. Erfolgt die Nutzung der Plattform nicht ausschließlich zu persönlichen oder familiären Tätigkeiten, liegt die Übermittlung der Adressbücher eindeutig im Anwendungsbereich der DS-GVO und bedarf einer Rechtsgrundlage. Da kommt i. d. R. nur die vorherige, freiwillige, aktive, separat erklärte, informierte und widerrufliche Einwilligung der Betroffenen – also aller Kontakte im Adressbuch – in Betracht. Und die hat in aller Regel niemand.

Hacker-Angriffe werden häufig durch schwache oder wiederverwendete Passwörter erleichtert. Unsere [Hinweise zum sicheren Umgang mit Passwörtern](#) haben wir bereits im Tätigkeitsbericht 2018 erwähnt. Eine Zwei-Faktor-Authentifizierung kann den Schutz signifikant erhöhen. Zudem sollte sich jeder überlegen, welche Dokumente er auf welcher Plattform speichert.

Oldies but Goldies?

Neben den oben erwähnten „neuen“ Problemen trafen wir im Jahr der Kontrolle auch wieder auf „alte Bekannte“, also Schwachstellen die bereits in den Vorjahren jeweils ein Thema waren. Ein paar Beispiele:

Akten-/Datenträgervernichtung

Selbst in Zeiten, wo sogar Discounter Büro-Schredder mit Partikelschnitt (P-4) anbieten, kommt es zu Datenpannen mit un-

zureichend vernichteten Akten und Datenträgern. Die DIN 66399 gilt seit 1. Oktober 2012 (siehe dazu 31.TB) und noch immer haben einige verantwortliche Stellen die Entsorgungskonzepte und Bestandsverträge offenbar nicht angepasst, was ggf. zu entsprechenden Bußgeldverfahren führt (siehe hierzu auch Abschnitt „Aktuelles aus der Bußgeldstelle“). Besondere Fundstücke waren dabei mehrere Festplatten vom Flohmarkt, die weder verschlüsselt noch gelöscht waren und sensible Daten enthielten, sowie unzureichend geschredderte Bankunterlagen.

Nachdem Verschlüsselung von Speichermedien zu den grundlegenden Schutzmaßnahmen gehört und die Folgen einer Datenpanne bei Verlust in Form eines möglichen Datenmissbrauchs mildert, sollte idealerweise immer verschlüsselt werden. Dies ist schon alleine deshalb geboten, da je nach Bauart oder Funktionsstörung ggf. gar nicht mehr rückstandsfrei bzw. nicht wiederherstellbar gelöscht werden kann und somit nur noch die physische Zerstörung als Ultima Ratio bliebe.

Nach Artikel 32 Absatz 1 Datenschutzgrundverordnung (DS-GVO) hat die Verantwortliche Stelle (und der ggf. vorhandene Auftragsverarbeiter) unter Berücksichtigung des Stands der Technik geeignete technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten zu treffen. Als Maßnahme wird bspw. die Verschlüsselung personenbezogener Daten genannt. Die Verschlüsselung personenbezogener Daten hat für die Verantwortliche Stelle und/oder den Auftragsverarbeiter noch weitere Vorteile: Sofern eine meldepflichtige „Datenpanne“ vorliegt, müssen auch Betroffene unverzüglich in klarer und einfacher Sprache benachrichtigt werden, wenn ein hohes Risiko für die persönlichen Rechte und Freiheiten entsteht. Eine Be-

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

nachrichtigung des Betroffenen ist jedoch gemäß Artikel 34 Absatz 3 Buchstabe a DS-GVO bei Verlust eines Datenträgers auf dem die Daten nach aktuellem Stand der Technik verschlüsselt wurden in der Regel entbehrlich.

Schließtechnik

Bei Vor-Ort-Begehungen stießen wir immer wieder auf Zweitschlüssel an und in Schränken, IT-Racks (ohne Sonderschließung), in Lagerräumen (teilweise noch mit Brandlast wie Papier/Putzmittel), fehlende Schutzbeschläge und nicht abgeschlossene Türen, die lediglich ins Schloss gezogen wurden. Kurios war der Fall eines IT-Raumes, dessen elektrischer Türöffner eigens über ein Codeschloss zwecks Zutrittskontrolle betätigt wurde, dessen Schlossfalle (ugs. Schnapper) aber auch mit einer größeren Büroklammer einfach geöffnet werden konnte.

Schlüssel, die nicht persönlich ausgehändigt werden und damit unter alleiniger Kontrolle des Empfängers stehen, sind so zu verwahren, dass keine Unbefugten darauf Zugriff haben können. Dabei müssen Aufbewahrungsart und der -ort dem Schutzbedarf des Schlüssels entsprechen. Generell sind fehlende bzw. unzureichende Verfahren bei der Schlüsselverwaltung zu ergänzen. Die Protokollierung der Schlüsselentnahme und -rückgabe wird empfohlen.

Multifunktionsgeräte

Bei Multifunktionsgeräten wurde die Speicherung der Daten lokal bzw. auf Netzlaufwerken sowie die über Browser erreichbaren Schnittstellen geprüft. Teilweise konnten so Dateien auf freigegebenen Netzlaufwerken einfach ausgedruckt werden, obwohl diese dafür nicht vorgese-

hen waren. Die vorgefundene Speicherung von Druckaufträgen über längere Zeit, teilweise über Jahre wurde jeweils nicht benötigt. Die Webschnittstellen von Druckern und Multifunktionsgeräten waren meistens vom Standard-Arbeitsplatzrechner via Browser ansprechbar.

Eine unnötige Exposition der Geräte sollte stets vermieden werden. Voraussetzung für den datenschutzgerechten Betrieb der Geräte ist, dass die Sicherheitseinstellungen auch aktiviert und sinnvoll konfiguriert werden. Das bedeutet, dass Passwörter zu setzen bzw. Standardpasswörter zu ändern sind und die Webschnittstelle über Filterregeln bspw. bei den Netzkoppelementen nur für dedizierte administrative Rechner erreichbar sind. Sofern geräte-seitig möglich, ist die Transportverschlüsselung zu aktivieren. Außerdem sollte das Gerät in regelmäßige Sicherheitsüberprüfungen und Updates eingebunden werden. Hilfreich ist eine Dokumentation der gewählten Konfiguration, sodass beispielsweise nach einem Update leicht überprüft werden kann, ob alle gewünschten Sicherheitsoptionen auch wirklich noch aktiviert sind.

Bußgelder für technische Verstöße

Besonders erwähnenswert ist aus Sicht des Technik-Referats die Tatsache, dass das erste DSGVO-Bußgeld in Deutschland (noch im Jahr 2018) aufgrund unzureichender Datensicherheit verhängt wurde („Knuddels“-Fall). Fehlende Datensicherheit ist auch im Jahr 2019 der Grund für einen Großteil der von der Bußgeldstelle verhängten Bußgelder. Dies sollte als Signal für die Verantwortlichen gesehen werden, dass Datensicherheit durch die DS-GVO enorm an Bedeutung gewonnen hat und nicht mehr vernachlässigt werden darf!

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

Insgesamt haben wir in diesem Jahr auch festgestellt, dass insbesondere Dienstleister – auf die gerade auch kleinere Unternehmen, Vereine und bspw. Arztpraxen angewiesen sind – viel zu häufig nachlässig in Bezug auf die Datensicherheit agieren. Durch eine Reihe an Datenpannen bei Dienstleistern kam es zu großen Abflüssen personenbezogener Daten von Betroffenen und in einigen Fällen auch zu Schädigungen bei den Verantwortlichen, welche die Dienstleister eingesetzt haben. Aus Sicht des Technikreferats gibt es in diesem Bereich sehr großen Nachbesserungsbedarf.

Beratung

Neben der Kontrolltätigkeit und der Aufarbeitung von Datenpannen war das Technik-Referat auch in der Beratung und der Erarbeitung von Orientierungshilfen aktiv.

Erstellung einer Datenschutzfolgenabschätzung (DSFA) für die E-Akte BW

Die Verpflichtung zur elektronischen Aktenführung tritt nach derzeitiger Gesetzesfassung zum 1. Januar 2022 in Kraft: Ab dann haben gemäß § 6 Absatz 1 EGovG BW die Behörden des Landes ihre Akten elektronisch zu führen. Mit der E-Akte BW geht eine elektronische Datenverarbeitung einher, die eine Vielzahl von personenbezogenen Daten umfasst und insofern für den LfDI ein wichtiges Thema darstellt. Nicht zuletzt muss auch der LfDI auf eine elektronische Aktenführung umstellen. Bereits früh wurde der LfDI von der Stabsstelle „Projekt Landeseinheitliche E-Akte“ des Innenministeriums in die Prüfung eines Sicherheits- und Datenschutzkonzepts eingebunden. Diese Prüfung wurde inzwischen weitestgehend abgeschlossen. Dabei sind noch offene Punkte vorhanden (z. B. Protokollierung vs. Mitarbeiterüberwachung), diese stehen aber einer Einführung der E-Akte BW vorerst nicht entgegen.

Darüber hinaus wird vom LfDI eine Datenschutzfolgenabschätzung (DSFA) für die E-Akte BW erstellt. Diese DSFA soll als Muster von allen Behörden genutzt werden können. Daraus folgt nicht, dass alle Behörden dieselbe DSFA nutzen können. Dafür sind die Verfahren und die Art der personenbezogenen Daten in den einzelnen Behörden zu unterschiedlich. Aber die vom LfDI erstellte DSFA wird sich wohl meist als Vorlage für die behördenspezifischen Verfahren eignen. Sobald die DSFA fertiggestellt ist, soll diese auch öffentlich verfügbar sein und kann als Muster für private Unternehmen dienen (ähnlich dem BayLDA Muster unter https://www.lda.bayern.de/de/thema_dsfa.html). Die DSFA orientiert sich an den ISO/IEC-Normen der 27000- und 29100-Reihe (ISO/IEC 27001, 27002, 27005, 29100, 29134, 29151 und 31000).

Bei der Erstellung der DSFA und dem damit verbundenen Austausch mit den einzelnen Projektgruppen hat sich musterhaft gezeigt, dass eine DSFA ein sehr sinnvolles Verfahren zum Erkennen von Risiken und deren Behandlung ist. Man muss seine Werte kennen, um diese auch angemessen schützen zu können. Passend ist hier ein Zitat von Bundy McGeorge (U.S. National Security Advisor): „Wenn wir unsere Zahnbürsten und Diamanten mit gleichem Eifer schützen, verlieren wir weniger Zahnbürsten und mehr Diamanten.“ (Im Original: “If we guard our toothbrushes and diamonds with equal zeal, we will lose fewer toothbrushes and more diamonds.”). Konkret heißt das, dass mit der Erstellung der DSFA für die E-Akte BW Risiken erkannt wurden aber auch Probleme bei der angedachten Umsetzung einzelner Abhilfemaßnahmen. Und nur wenn eine DSFA vor dem Projektstart durchgeführt wird, können diese Erkenntnisse sinnvoll in den Projektverlauf eingebracht werden.

Praxis

In der Praxis enthalten die bei der Aufsichtsbehörde vorgelegten DSFAs selten eine „Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen“, wie sie in Artikel 35 Absatz 7 Buchstabe c der DS-GVO gefordert wird. Auch die nach Artikel 35 Absatz 7 Buchstabe d der DS-GVO geforderten Abhilfemaßnahmen mit denen den „Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird“ finden in der Praxis kaum Beachtung. Meist beinhalten die vorgelegten DSFAs eine Risikobewertung und Abhilfemaßnahmen für Vertraulichkeit, Verfügbarkeit und Integrität, also den „klassischen“ Zielen aus der Informationssicherheit. Eine Bewertung erfolgt also meist aus der Sicht des Unternehmens – eine Betrachtung aus Sicht der Betroffenen findet leider nicht statt. Gerade diese wird aber vom Datenschutz gerade gefordert.

Videoüberwachung und Türklingeln

Die Werbung gibt es vor: Der Hausbesitzer genießt sein Leben und kann per Videoübertragung und Smartphone-App aus der Ferne dem Postboten die Türe öffnen oder dem vermeintlichen Einbrecher wird klar gemacht, dass er auf Video aufgezeichnet wird. Was kann hier also schon schief gehen? Leider lässt die Sicherheit der Videoübertragung auf das Smartphone oft deutlich zu wünschen übrig. Werden die Hersteller auf die Probleme angesprochen, bleiben diese dabei beeindruckend gelassen – schließlich sind die Hersteller nicht die Verantwortlichen im Sinne der DS-GVO. Der Verantwortliche entscheidet über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten und dies ist nun mal der Betreiber der Kamera – und nicht deren Hersteller. Ob die Vi-

deoübertragung durch unsichere (Vor-) Einstellungen oder Fehler in der Software dabei öffentlich verfügbar oder zu Servern in Drittländern übermittelt werden liegt alleine in der Verantwortung des Betreibers. Der Betreiber der Kamera muss auch darauf achten, keine öffentlichen Räume zu erfassen. Werden Bilder aus öffentlichen Räumen ins Internet übermittelt und für jeden abrufbar, hat dies ein Bußgeld durch die Aufsichtsbehörde zur Folge.

Was kann der Verantwortliche machen? Achten Sie auf die Sicherheit des Produkts, recherchieren Sie vor dem Kauf, informieren Sie sich während der Betriebszeit über mögliche Sicherheitslücken und installieren Sie Software-Updates. Deaktivieren Sie die Übertragung zum Smartphone, wenn Sie nicht unbedingt diese Funktion benötigen. Wenn Sie diese Funktion doch benötigen, sollten Sie sich nach Möglichkeit mit einem VPN ins heimische Netzwerk verbinden und nur darüber mit der Kamera. Der Kamera sollte keine Verbindung mit dem Internet erlaubt werden. So unsinnig sich das auch 2019 lesen mag. Siehe auch TB 2018 Kapitel 3.2.

Videobildauflösung, die DIN EN 62676-4 (bzw. DIN EN 50132-7) und die Frage, ob bei einer Videoüberwachung per se personenbezogene Daten erfasst werden

Alleine mit den technischen Daten der Videoaufnahme lässt sich diese Frage nicht beantworten. Die Beantwortung hängt auch von den Begleitumständen der Videoaufnahme, d. h. den zur Verfügung stehenden Zusatzinformationen, ab. Zunächst aber zu den technischen Daten: (1) Bildauflösung der Kamera, (2) Abstand der Kamera zur erfassten Person, (3) Winkel zwischen Kamera und der erfassten Person und (4) Beleuchtung. Zur Bewertung der Personen-

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

beziehbarkeit von Videoaufnahmen gehen wir im Weiteren von idealen Bedingungen aus, d. h. die Person wird frontal von der Kamera erfasst und die Beleuchtung ist ideal. Die oben genannten Punkte (1) und (2) lassen sich als „Punktdichte“ zusammenfassen und werden bei Videosystemen üblicherweise mit der Einheit mm/Pixel, Pixel/Meter oder Pixel/16 cm (Gesicht) angegeben. Beispiele aus der DIN EN 62676-4 sind in der Tabelle im Anhang zu sehen (Bilder auf Grundlage von <https://www.gov.uk/cast-resources-for-the-crime-prevention-industry>). Dabei kann festgestellt werden, dass ab einer Punktdichte von 16 mm/Pixel, d. h. ein Pixel in der Aufnahme umfasst 16 mm des erfassten Objekts, die dargestellte Person nur mit Zusatzinformationen identifiziert werden kann.

Die DIN EN 62676-4 definiert also, ab welcher Punktdichte Personen überwacht, detektiert, beobachtet, erkannt, identifiziert oder begutachtet werden können. Wie in der Tabelle mit den Abbildungen dargestellt, wird in der DIN EN 62676-4 ab einer Punktdichte von 8 mm/Pixel eine Erkennbarkeit von Personen angenommen. Soweit zu den technischen Daten. Mit Zusatzwissen, das bspw. der Bauleiter auf einer videoüberwachten Baustelle, der Chef im Büro, etc. hat, kann auch bei 16 mm/Pixel vergleichsweise einfach ein Personenbezug herstellbar sein. Führt man diesen Gedanken weiter, so ist auch bei noch geringerer Auflösung eine Einzelfallprüfung erforderlich um festzustellen, ob ein Personenbezug hergestellt werden kann. Zu beachten ist dabei, dass sich aus einer Vielzahl von Zusatzinformationen, wie äußere Erscheinung, mitgeführte Gegenstände, ungewöhnliche Verhaltensweise und/oder durch eine Kombination von Ort, Datum, Zeit, etc. doch eine Personenbeziehbarkeit ergeben kann. Kommt die Einzelfallprüfung allerdings zu dem Schluss, dass kein

Zusatzwissen vorhanden ist, kann unterhalb einer Punktdichte von 16 mm/Pixel von einer Videoüberwachung ohne Personenbezug ausgegangen werden.

1.10 Mehr Datenschutz heißt auch mehr Europa!

Die Stabsstelle Europa wurde in diesem Jahr besonders im Bereich der Grundsatzfragen ausgebaut und gestärkt. Neben dem Bereich der europäischen Zusammenarbeit, der sich in die Mitarbeit in den Gremien des Europäischen Datenschutzausschusses und die Koordinierung der grenzüberschreitenden Verwaltungsverfahren gliedert, sind nun auch die Grundsatzfragen im nationalen Bereich in der Stabsstelle Europa angegliedert. Für den LfDI ist die Stabsstelle die zentrale Koordinierungsstelle dieser Fragen, welche die einheitliche Rechtsanwendung innerhalb und außerhalb des Hauses sicherstellt. Daneben vertritt sie den LfDI bei Vortrags- und Fachveranstaltungen.

1. Europäische Zusammenarbeit

Mit der Geltung der DS-GVO wurde die internationale Zusammenarbeit im Datenschutz auf eine neue Ebene gehoben. Einheitliche verwaltungsinterne Vorschriften sind hierbei genauso wichtig, wie die effiziente und koordinierte Bearbeitung grenzüberschreitender Verwaltungsverfahren.

a) Mitarbeit des LfDI in den Arbeitsgruppen des Europäischen Datenschutzausschusses

Auf europäischer Ebene sind wir in den Arbeitsgremien des Europäischen Datenschutzausschusses beteiligt. Der Europäische Datenschutzausschuss (EDSA) ist die unabhängige europäische Einrichtung,

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

die zur einheitlichen Anwendung der Datenschutzvorschriften in der gesamten Europäischen Union beiträgt und die Zusammenarbeit zwischen den EU-Datenschutzbehörden fördert. Der EDSA besteht aus Vertretern der nationalen Datenschutzbehörden und dem Europäischen Datenschutzbeauftragten (EDSB). Deutschland ist dort mit einem Sitz vertreten. Diesen Sitz nimmt aktuell der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) wahr. Die Wahl des Stellvertreters, der nach § 17 Absatz 1 Satz 1 BDSG Leiter oder Leiterin der Aufsichtsbehörde eines Landes ist, wurde bis dato vom Bundesrat noch nicht erfolgreich durchgeführt. Da dieser Stellvertreter das Stimmrecht in Sachen, in denen die Länder allein das Recht zur Gesetzgebung haben, oder welche die Einrichtung oder das Verfahren von Landesbehörden betreffen, wahrnehmen soll, ist diese Wahl für die effiziente Vertretung der Interessen der Länder unabdingbar – weswegen die unterbliebene Wahl durch den Bundesrat ein schwerwiegendes und kritikwürdiges Versäumnis darstellt.

In den Arbeitsgruppen des EDSA hat der LfDI eine feste Position als Ländervertreter in der Social Media Expert Subgroup inne, die von der Stabsstelle Europa wahrgenommen wird. Diese koordiniert die Stellungnahmen der deutschen Aufsichtsbehörden und bringt die abgestimmten Standpunkte auf europäischer Ebene ein. Neben dieser festen Koordinierungsfunktion nimmt der LfDI aktuell in mehreren Arbeitsbereichen die Position als einfacher oder federführender Berichtersteller wahr:

In der Social Media Expert Subgroup des EDSA ist der LfDI zusammen mit der französischen Datenschutzbehörde (CNIL) federführender Berichtersteller in einem aktuellen Themenbereich. Für die Erstellung

von Guidelines im Bereich der Zusammenarbeit habe ich in der Cooperation Expert Subgroup ebenfalls die federführende Berichterstattung übernommen.

Eine einfache Berichterstellerstellung hatte ich zusammen mit dem Hamburgischen Beauftragten zur Erstellung eines internen Papiers in der Social Media Expert Subgroup inne. Zudem teile ich mir mit Schleswig-Holstein im Bereich der Grundsatzfragen eine solche Position in der Key Provisions Expert Subgroup.

Als Vorsitzender des Arbeitskreises Videoüberwachung der Datenschutzkonferenz habe ich, mithilfe der Berichterstattung durch die Berliner Beauftragte für Datenschutz und Informationsfreiheit, die „Guideline 3/2019 on processing of personal data through video devices“ ermöglicht und diese Fragen auf europäischer Ebene adressiert.

Die bereits 2018 zum Thema vernetzte Fahrzeuge angestoßenen Untersuchungen wurden in diesem Jahr erfolgreich fortgeführt. Auch in diesem Themenbereich hatte ich die deutschen und europäischen Kollegen vorübergehend als Berichtersteller unterstützt.

Guidelines und Opinions des Europäischen Datenschutzausschusses finden Sie unter: https://edpb.europa.eu/edpb_de

b) Grenzüberschreitende Verwaltungsverfahren

Werden grenzüberschreitende Verwaltungsverfahren durchgeführt, so gilt ohnehin gemäß Artikel 60 DS-GVO das Kooperationsprinzip, wonach vorrangig durch Zusammenarbeit ein Konsens erzielt werden soll. Aber auch informelle Kommunikationsmechanismen dürfen in ihrer Bedeutung für die europäische Zusammenarbeit

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

nicht unterschätzt werden. Über die Plattform des Internal Market Information System (IMI) werden alle grenzüberschreitenden Verwaltungsverfahren und auch informelle Anfragen abgewickelt, die den Erfahrungsaustausch der Aufsichtsbehörden ermöglichen. Meine Behörde war 2019 an 123 in diesem System geführten Verfahren beteiligt. Sieben davon haben wir als federführende Aufsichtsbehörde geführt. In 116 Verfahren waren wir betroffene Aufsichtsbehörde, von diesen Verfahren sind 48 in unserem Haus eingegangen und wurden mit den europäischen Behörden geteilt. Wir verzeichnen aktuell ungefähr 15 Eingänge, die in naher Zukunft über das System mit den europäischen Kollegen geteilt werden.

2. Koordinierung einheitlicher Standpunkte auf europäischer und deutscher Ebene

Auf deutscher Ebene vertrete ich die Interessen Baden-Württembergs im Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden der Länder und des Bundes, der Datenschutzkonferenz (DSK). Sie hat die Aufgabe, die Datenschutzgrundrechte zu wahren und zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten. Die Datenschutzkonferenz tagt grundsätzlich halbjährlich in mehrtägigen Sitzungen, wobei seit Geltung der DS-GVO mehrere Sonder- und Zwischenkonferenzen pro Jahr durchgeführt werden.

Arbeitsergebnisse der DSK finden Sie unter: <https://www.datenschutzkonferenz-online.de/>

Die Entscheidungen der DSK werden durch Arbeitskreise vorbereitet. Die Geschäftsordnung der DSK stellt sicher, dass die

Ländervertreter, von denen die Aufsichtsbehörden der Länder in den europäischen Arbeitsgremien vertreten werden, auch in den jeweils thematisch identischen deutschen Arbeitskreisen anwesend sind. Im Rahmen ihrer europäischen Arbeit sind sie an die Standpunkte und Beschlüsse der DSK und die Ergebnisse der Arbeitskreise gebunden. Steht ein einheitlicher Standpunkt zu einem Themengebiet noch aus, so kann dieser gemäß dem Verfahren nach § 18 Absatz 2 Bundesdatenschutzgesetz (BDSG) gebildet werden. Nach § 18 Absatz 2 Satz 4 BDSG ist hierbei im Zweifel die einfache Mehrheit der Stimmen maßgeblich. Durch dieses Verfahren werden einheitliche Standpunkte der deutschen Aufsichtsbehörden und somit die Kohärenz auf deutscher Ebene sichergestellt.

3. Beratungen und Fortbildungen der Stabsstelle EU

Nachdem die Stabsstelle Europa des LfDI im Jahr 2018 bereits zahlreiche Teilnehmerinnen und Teilnehmer geschult hat, ist das Bedürfnis nach Vorträgen zum neuen Datenschutzrecht unter der DS-GVO auch 2019 nicht abgerissen. Innerhalb des Berichtszeitraums wurden in allein 39 Schulungen der Stabsstelle Europa auch in diesem Jahr wieder zahlreiche Interessierte zum Thema Datenschutz sensibilisiert und mit Fachkenntnissen ausgestattet. Nachdem sich nunmehr auch die europäische Rechtsprechung mit dem Thema gezielt auseinander gesetzt hat (Fashion-ID Urteil vom 29. Juli 2019), lag einer der Schwerpunkte dabei auf Schulungen im Social Media-Bereich und der Frage, ob und wie soziale Medien datenschutzkonform genutzt werden können. Durch unsere aktive Mitwirkung in der Social Media Expert Subgroup des Europäischen Datenschutzausschusses (EDSA) können wir wertvolle Arbeitsergebnisse zu den praktischen Fra-

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

gen rund um die Nutzung von Twitter und Co. mitgestalten und diese an die Verantwortlichen in Baden-Württemberg weitergeben. Ein weiterer Fokus lag vergangenes Jahr im nicht-öffentlichen Bereich bei den Fortbildungen für Vereine, die aufgrund ihrer häufig geringen Größe und Manpower auf organisatorischer Ebene im Vorfeld zum Teil große Sorgen bezüglich der Verwirklichung der datenschutzrechtlichen Anforderungen hatten. Durch gezielte Veranstaltungen in diesem Bereich hat der LfDI versucht, den Vereinen diese Ängste zu nehmen. Insbesondere unser Praxisratgeber „Datenschutz im Verein nach der DS-GVO“ (<https://www.baden-wuerttemberg.datenschutz.de/praxisratgeber-datenschutz-im-verein-nach-der-ds-gvo/>) soll durch seine spezifischen Erläuterungen und anschaulichen Beispiele gangbare Wege aufzeigen, wie der Datenschutz im Verein gestaltet werden kann.

Der öffentliche Bereich wurde von der Stabsstelle Europa ebenfalls weiterhin verstärkt geschult. Schnell stellte sich heraus, dass gerade im öffentlichen Bereich oftmals Hinweise für eine rechtmäßige und vor allem praktikable Umsetzung der datenschutzrechtlichen Vorgaben fehlten. Deshalb wurden zahlreiche Veranstaltungen speziell für Behörden unseres Landes durchgeführt, in denen die besonderen Regelungen und Bedürfnisse des Datenschutzes öffentlicher Stellen behandelt wurden. Besonders wertvoll ist in diesem Rahmen auch die Zusammenarbeit zwischen dem LfDI und den Ministerien sowie Regierungspräsidien Baden-Württembergs im Rahmen der von den Ressorts eingerichteten Arbeitskreise. Insbesondere im „Arbeitskreis Datenschutz“ tauscht sich der LfDI regelmäßig mit den behördlichen Datenschutzbeauftragten der vorgenannten Stellen aus und erhält so die Gelegenheit, alltägliche Problemstellungen bei der

Umsetzung der DS-GVO und landes- bzw. bereichsspezifischen Gesetzen im öffentlichen Sektor zu erörtern und gemeinsam mit den anderen Teilnehmer/innen sinnvolle Lösungen für die Praxis zu erarbeiten.

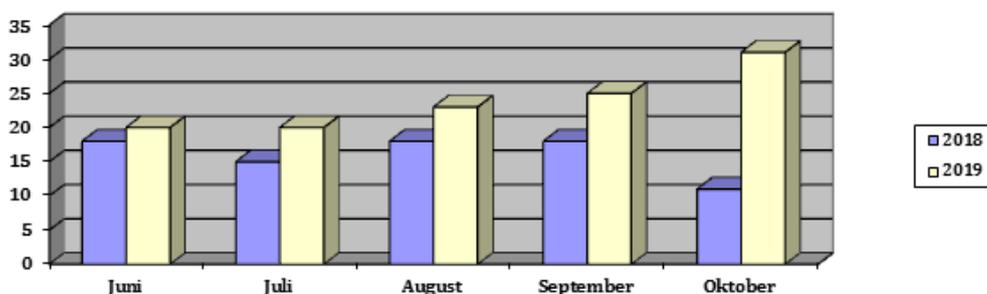
Und zu guter Letzt besteht natürlich auch im eigenen Hause immer wieder die Aufgabe, nicht nur selbst die (neuen) Vorgaben der DS-GVO ordnungsgemäß umzusetzen und zu erfüllen, sondern auch die aktuellen Entwicklungen auf europäischer Ebene oder bei den anderen Aufsichtsbehörden in Deutschland zu beobachten und in die Beratungstätigkeit des LfDI einfließen zu lassen. Aus diesem Grund bietet die Stabsstelle Europa auch intern fortlaufend Inhouse-Schulungen für die eigenen Mitarbeitenden an, in denen zum einen mögliche Veränderungen und neu gewonnene Erkenntnisse zu Grundsatzfragen aus der Datenschutz-Praxis vermittelt werden. Auf diese Weise werden einheitliche Standpunkte innerhalb des LfDI erarbeitet und insbesondere die neuen Mitarbeitenden mit wichtigen Fragestellungen vertraut gemacht.

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

1.11 Aktuelles aus der Bußgeldstelle

Vom 1. Januar 2019 bis 31. Oktober 2019 wurden bei der Bußgeldstelle insgesamt 196 neue Bußgeldverfahren anhängig. Die Anzahl der monatlichen Neueingänge hat sich dabei im Vergleich zum maßgeblichen Vorjahreszeitraum (Anfang Juni bis Ende Oktober) um durchschnittlich 20 % erhöht.

erwirkte Durchsuchungsbeschlüsse, deren Vollzug unmittelbar bevorsteht. Zudem führte die Bußgeldstelle mehrere Kontrollen bei Verantwortlichen durch, die in zwei Fällen zu Bußgeldbescheiden führten.



(berücksichtigt Neueingänge, die nach Wirksamwerden der DS-GVO bis zum Stichtag des jeweiligen Berichts eingingen.)

Die vom Regierungspräsidium Karlsruhe übernommenen Altfälle konnten zwischenzeitlich vollständig erledigt werden. Nach wie vor werden Bußgelder nicht bei jedem Datenschutzverstoß verhängt, sondern vorrangig bei gravierenderen Verstößen. Insgesamt verhängte die Bußgeldstelle zwischen Anfang Januar und Ende Oktober 2019 in 19 Bescheiden Geldbußen in Höhe von insgesamt 242.140,- Euro zzgl. Gebühren in Höhe von insgesamt 12.107,- Euro. Die Geldbußen richteten sich dabei sowohl gegen natürliche Personen als auch gegen kleine und mittelständische Unternehmen. Bußgeldverfahren gegen große Unternehmen befinden sich noch im Ermittlungsstadium. In einer Vielzahl von Fällen führte die Bußgeldstelle Vernehmungen von Zeugen und Betroffenen durch, ließ in mehreren Verfahren durch Gerichtsbeschlüsse und mit Amtshilfe der Polizei Beweismittel beschlagnahmen und

Einzelfälle

Mit Bescheid vom 12. April 2019 verhängte die Bußgeldstelle ein Bußgeld in Höhe von 80.000,- Euro gegen ein mittelständisches Finanzdienstleistungsunternehmen. Dieses hatte bei der Entsorgung von Unterlagen, die personenbezogene Daten zweier Kunden enthielten, nicht die erforderliche Sorgfalt zur Wahrung der Integrität und Vertraulichkeit der Informationen im Sinne des Art. 5 Absatz 1 lit. f DSGVO walten lassen. So wurden die Papiere ohne vorherige Anonymisierung durch Schreddern oder Schwärzen versehentlich im allgemeinen Altpapier entsorgt, wo die Unterlagen von einer Nachbarin entdeckt und an meine Behörde gesandt wurden. Leider ist die unsachgemäße Entsorgung von Unterlagen, die zum Teil sensible personenbezogene Daten enthalten, kein Einzelfall. Vielmehr waren im Berichtsjahr mehrere Bußgeldverfahren wegen Verstößen gegen die Integrität und Vertraulichkeit der Daten gem. Art. 5 Absatz 1 lit. f DSGVO anhängig.

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

gig, von denen die Mehrzahl mit einem Bußgeldbescheid abgeschlossen wurden.

Durch Entscheidung vom 9. Mai 2019 verhängte die Bußgeldstelle erstmals ein Bußgeld gegen einen Polizeibeamten. Dem lag zugrunde, dass der Beamte zu rein privaten Zwecken und unter Verwendung seiner dienstlichen Benutzerkennung über das Kfz-Kennzeichen eines Pkws die Halterdaten einer Zufallsbekanntschaft abfragte. Mit diesen Halterdaten tätigte der Beamte eine sog. SARS-Anfrage bei der Bundesnetzagentur, erlangte so die Telefonnummer seiner Zufallsbekanntschaft und kontaktierte diese anschließend. Dieses Vorgehen stellte einen sog. Exzess dar, welcher der Dienststelle des Polizeibeamten nicht zuzurechnen war. Das in § 28 LDSG normierte Ahndungsverbot bezüglich öffentlicher Stellen war nicht einschlägig, denn weder war die Dienststelle für den Verstoß verantwortlich, noch war der Beamte als eigenständige öffentliche Stelle anzusehen. Es handelte sich vielmehr um einen Verstoß, den der Beamte als Privatperson unter Nutzung dienstlicher Zugriffsbefugnisse beging. Sein Handeln war deshalb nach der DSGVO zu bewerten und wurde mit einem moderaten Bußgeld in Höhe von 1.400,- Euro geahndet. Die Entscheidung zeigt, dass Bedienstete öffentlicher Stellen, ebenso wie Beschäftigte nicht-öffentlicher Stellen, für eigenmächtiges datenschutzwidriges Handeln sanktioniert werden können.

Mit Bescheid vom 24. Oktober 2019 verhängte die Bußgeldstelle ein Bußgeld in Höhe von 100.000,- Euro gegen ein mittelständisches Lebensmittelhandwerksunternehmen, weil dieses die personenbezogenen Daten seiner Bewerber fahrlässig nicht im ausreichenden Umfang gegen den Zugriff durch unberechtigte Dritte schützte. Das Unternehmen hatte auf seiner

Website ein Bewerberportal eingerichtet, über welches Interessenten ihre Bewerbungsunterlagen online einreichen konnten. Jedoch bot das Unternehmen weder eine verschlüsselte Übertragung der Daten an, noch erfolgte die Speicherung der Bewerberdaten verschlüsselt oder passwortgeschützt. Zudem waren die ungesicherten Bewerberdaten mit einer Verknüpfung zu Google versehen, sodass jedermann bei einer Google-Recherche der jeweiligen Bewerbernamen auf deren Bewerbungsunterlagen stoßen und diese ohne Zugriffsbeschränkung abrufen konnte.

Bußgeldkonzept

Die Arbeit der Bußgeldstelle meiner Dienststelle, gemeinsam mit dem Justizariat des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und den Datenschutzaufsichtsbehörden der Länder Berlin und Hessen, führte zur Entwicklung eines deutschen Bußgeldkonzepts für Unternehmen, welches am 16. Oktober 2019 von der [Datenschutzkonferenz](#) veröffentlicht wurde. Das Konzept gilt dabei vorläufig bis zum Erlass europäischer Leitlinien und soll der Harmonisierung der deutschen Sanktionspraxis sowie der Transparenz und Nachvollziehbarkeit für die verantwortlichen Stellen dienen. Da die Geldbußen gem. Art. 83 Absatz 1 DSGVO in jedem Einzelfall wirksam, verhältnismäßig und abschreckend zu sein haben, musste ein Konzept entwickelt werden, welches sowohl den konkreten Tatumständen als auch den sog. täterbezogenen Merkmalen, also insbesondere den wirtschaftlichen Verhältnissen der jeweiligen Verantwortlichen Rechnung trägt. Ein Katalog mit festen Beträgen für bestimmte Verstöße schied damit aus. Das nun veröffentlichte Konzept trägt den wirtschaftlichen Verhältnissen bereits in einem ersten Schritt Rechnung, in welchem die Unternehmen – ähnlich

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

den WpHG-Bußgeldleitlinien II der [BaFin](#) – umsatzbezogen nach Größenklassen kategorisiert werden, um in einem nächsten Schritt einen wirtschaftlichen Grundwert zu bilden. Bei dieser umsatzbezogenen Kategorisierung der Unternehmen ist der funktionale Unternehmensbegriff gemäß ErwG 150 DSGVO heranzuziehen. In einem weiteren Schritt wird dieser Grundwert je nach Schweregrad der Tat mit einem Faktor multipliziert und sodann in einem letzten Schritt anhand weiterer erschwerender oder begünstigender Kriterien, darunter auch die Rentabilität und der Gewinn des Unternehmens, auf den Einzelfall angepasst. Die bisherigen Praxiserfahrungen haben gezeigt, dass das Konzept einerseits die vom europäischen Verordnungsgeber gewollte Erhöhung der Bußgeldbeträge im Vergleich zu Bußgeldern unter dem BDSG a. F. bewirkt. Andererseits erreichen die Bußgelder aber keine unangemessenen Höhen und können von den sanktionierten Unternehmen durchaus nachvollzogen werden. Die zukünftigen Entwicklungen werden zeigen, ob und ggf. inwieweit das Bußgeldkonzept anzupassen ist.

Die praktischen Erfahrungen der ersten 18 Monate seit Wirksamwerden der DSGVO zeigen, dass es sich lohnt, die Beratungsangebote meiner Dienststelle anzunehmen und gesetzliche Vorgaben umzusetzen, um Bußgelder zu vermeiden. Soweit Bußgeldverfahren eingeleitet wurden, erschien in vielen Fällen aufgrund der guten Kooperation mit der Bußgeldstelle und der prompten Umsetzung etwaiger Vorgaben die Verhängung einer Geldbuße nicht mehr notwendig, sodass die Verfahren eingestellt werden konnten. Die bisherige Erfahrung zeigt aber auch, dass in solchen Fällen, in denen eine Sanktionierung geboten ist, die Verstöße mit deutlich höheren Bußgeldern belegt werden als unter dem alten nationalen Rechtsregime.

1.12 Bye Bye Twitter

Am 30. Dezember dieses Jahres musste ich meinen Abschied von der Social Media-Plattform Twitter bekannt geben. Seit dem November twitterte dort unter @lfdi_bw die einzige deutsche Datenschutz-Aufsichtsbehörde mit einem offiziellen Account über eigene News, kommentierte das aktuelle Datenschutz-Geschehen, tauschte sich in teilweise intensiven, aber immer sachbezogenen Diskussionen mit dem Datenschützer-Schwarm auf Twitter aus und war auch für unmittelbare Fragen ansprechbar.

Seit November 2017 setzte der LfDI etwa 3.000 Tweets ab, die Zahl der Follower des Accounts wuchs so auf zuletzt 5.500. Mit meinen Kurznachrichten erreichte ich binnen der letzten zwei Jahre mehrere Millionen Twitternutzer und erhielt tausendfaches Feedback mit Anregungen, Einschätzungen zu unserer Arbeit – erfreulicherweise überwog die freundliche Resonanz deutlich. Gleichzeitig nutzte ich die rege und vor allem schnelle Kommunikation auf dieser Plattform, um mich bei den 150 Personen und Instanzen, denen ich selbst folgte, über aktuelle Datenschutzthemen, Gerichtsentscheidungen und nationale wie internationale politisch-parlamentarische Vorgänge auf dem Laufenden zu halten.

Schon mit der Facebook-Fanpage-Entscheidung des Europäischen Gerichtshofs vom 5. Juni 2018 (C-210/16) verdüsterte sich das Bild für die Nutzer von Social Media: Der EuGH entschied darin, dass auch der Betreiber einer Fanpage neben dem Plattformbetreiber selbst als Verantwortlicher im datenschutzrechtlichen Sinne anzusehen ist – und damit bei Datenschutzverstößen auf der Plattform nicht mehr alleine auf deren Betreiber verweisen und seine Hände in Unschuld waschen kann. Zudem

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

wurde damit klargestellt, dass zwischen den beiden gemeinsam Verantwortlichen ein Vertrag abzuschließen ist (vgl. Art. 26 DS-GVO), in dem die Wahrnehmung von Pflichten etwa gegenüber Betroffenen transparent und eindeutig geregelt werden muss. Und solche Verträge lagen und liegen bis heute nicht in einer datenschutzgerechten Form vor. Damit war seit Mitte des Jahres 2018 jedenfalls für öffentliche und private Betreiber von Facebook-Fanpages klar, dass sie – ganz unabhängig von der Frage, ob die Plattformen die Daten von Mitgliedern und Nicht-Mitgliedern rechtmäßig verarbeiten – ihren Social Media-Auftritt formell rechtswidrig unterhalten. Ob diese Rechtslage auch für andere Plattformen als Facebook gilt, wurde im Folgenden kontrovers diskutiert, lässt sich angesichts der zunehmenden Konvergenz der Social Media-Angebote (ihre Funktionalitäten ähneln sich immer mehr, die darunter liegenden Geschäftsmodelle „wirtschaftliche Verwertung der personenbezogenen Daten der User“ sind identisch) allerdings kaum mehr bestreiten.

Noch prekärer – und noch eindeutiger – wurde die Rechtslage durch die Entscheidung des Bundesverwaltungsgerichts vom 11. September 2019 (BVerwG 6 C 15.18), das die im Wege der Vorabentscheidung vom EuGH im Juni 2018 eingenommene Position in den deutschen Rechtsraum überführte: Damit wurde nicht nur die datenschutzrechtliche Verantwortlichkeit des Fanpagebetreibers bestätigt, sondern zugleich den Aufsichtsbehörden ein Auswahlermessen zugesprochen, zur Beseitigung von Rechtsverstößen beim Betrieb der Plattform wahlweise auf jeden der Verantwortlichen – also auch auf den Nutzer zuzugreifen: „Auch im Bereich des Datenschutzes kann es das Gebot einer effektiven und wirkungsvollen Gefahrenabwehr rechtfertigen, denjenigen Verantwortli-

chen heranzuziehen, dessen Pflichtigkeit sich ohne weiteres bejahen lässt und dem effektive Mittel zum Abstellen des Verstoßes zur Verfügung stehen.“

Damit eröffnet das Bundesverwaltungsgericht ausweislich der am 10. Dezember 2019 veröffentlichten Entscheidungsgründe die Möglichkeit einer „Regulierung um die Ecke“: Die Aufsicht kann bei rechtswidriger Datenverarbeitung auf der Plattform auch auf den Nutzer zugreifen und ihn mit Maßnahmen wie Verwarnungen oder Anordnungen belegen. Ob man das nun Auswahlermessen, Geiselnahme oder Bauernopfer nennt, ist zweitrangig. In der Sache geht es immer darum, einen nicht erreichbaren Störer – den Plattformbetreiber – über einen erreichbaren Störer – den Accountbetreiber – unter Druck zu setzen, das geltende Recht einzuhalten.

Und warum sind die meisten Betreiber von erfolgreichen und reichweitenstarken Plattformbetreibern „nicht erreichbar“? Darauf gibt es eine zweiteilige Antwort: Zunächst einmal hat die DS-GVO dafür gesorgt, dass das neue einheitliche Datenschutzrecht in Europa auch einheitlich umgesetzt wird (Stichwort Kohärenzverfahren zwischen den Aufsichtsbehörden) und hat mittels der sogenannten one stop-shop sichergestellt, dass für jeden Datenverarbeiter eine und nur eine Aufsichtsbehörde zuständig ist und die Ansagen macht. Im Falle von Facebook, Twitter und Co. ist dies die irische Aufsichtsbehörde, welche mit den anderen staatlichen Stelle der Republik Irland den Ruf teilt, besonders ansiedlungs- und wirtschaftsfreundlich zu agieren. Fakt ist, dass es den irischen Kollegen bis heute nicht gelungen ist, auch nur eine wirksame Regulierung gegenüber den Plattformbetreibern zu treffen. Das bedeutet: Andere europäische Aufsichtsbehörden dürfen die Plattformbetreiber nicht wirksam kontrol-

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

lieren, die zuständige Behörde stellt aber keine effektive Kontrolle sicher. Damit liegen Voraussetzungen vor, die das Bundesverwaltungsgericht zur Bedingung der Ausübung von Aufsichtsbefugnissen gegenüber von plattformnutzenden Stellen gemacht hat. Zu denken wäre hierzu an Warnungen an die Nutzer (Art. 58 Abs. 2 lit. a DS-GVO), später auch an Verwarnungen oder sogar Anordnungen, ihre Accounts einzuschränken oder zu schließen (Art. 58 Abs. 2 lit. b und d DS-GVO).

„Schön“ ist das natürlich nicht: Wesentlich naheliegender und „fairer“ wäre es, Datenschutzverstöße an der Quelle abzustellen – zumal die Nutzer der Plattformen uns mit großer Regelmäßigkeit versichern, keinen Einfluss auf die Betreiber ausüben zu können (was wir gut nachvollziehen können). Dennoch: Es sind die Nutzer, welche diese Plattformbetreiber als Dienstleister einsetzen, um ihre Öffentlichkeitsarbeit mit möglichst großer Reichweite und Resonanz zu betreiben (so wie ich das auch bislang via Twitter tat), und dadurch setzen die Nutzer die Grundbedingung dafür, dass viele Interessenten auf die Social Media-Plattformen gelockt werden – und dort ggf. in ihren Rechten verletzt werden.

Zwischenfrage: Aber handeln denn nun die Plattformbetreiber rechtswidrig, verarbeiten sie also Nutzerdaten entgegen den Bestimmungen der DS-GVO? Dazu ist zunächst festzuhalten, dass es gerade Aufgabe der irischen Aufsichtsbehörde ist, dies zu ermitteln und zu bewerten. Wenn dies aber nicht effektiv geschieht, dürfen die übrigen Aufsichtsbehörden die Hände nicht in den Schoß legen und müssen sich – vor dem Hintergrund der Social Media-Nutzung durch verantwortliche Stellen, über die sie selbst die Aufsicht ausüben – ein Bild von der Rechtslage machen. Danach sieht es auf Grundlage der verfügbaren

Informationen, insbesondere der Datenschutzerklärungen der Plattformbetreiber, und vorbehaltlich anderer Erkenntnisse der zuständigen Aufsichtsbehörde überblicksartig wie folgt aus:

So gut wie alle der gängigen Social Media-Plattformen sind derzeit nicht datenschutzkonform nutzbar. Viele Plattformen sammeln Daten von angemeldeten Nutzern und Nichtnutzern, auf der eigenen Website, in den eigenen Apps sowie auf Websites und Apps Dritter. Sie übermitteln nach eigenem Ermessen Daten an Dritte und behalten sich auch den Verkauf aller Daten vor.

Die Verarbeitungen werden weder hinsichtlich der eingesetzten Technologien, noch der betroffenen Datenarten, Verarbeitungszwecke oder Empfänger konkret und abschließend genannt.

Die Verarbeitungen erfolgen weitgehend ohne Rechtsgrundlage: Eine informiert, freiwillig, vorherig, aktiv, für den konkreten Einzelfall und separat erklärte sowie jederzeit zumutbar widerrufliche Einwilligung wird nicht abgefragt. Stattdessen muss man bei der Registrierung zustimmen, dass die Datenschutzrichtlinien „gelten“. Andere Rechtsgrundlagen (Art. 6 Abs. 1 UAbs. 1 lit b–f DS-GVO) sind offensichtlich nicht einschlägig.

Eine Möglichkeit, als Plattform-Nutzer, als Drittwebseiten- oder Drittappbetreiber eine Vereinbarung hinsichtlich der Gemeinsamen Verantwortung (Art. 26 DS-GVO) mit der Plattform abzuschließen, ist oft nicht ersichtlich.

Die Schlussfolgerungen aus diesen Umständen müssen zunächst die Verantwortlichen selbst ziehen und sich darüber klar werden, ob sie zu den von ihnen verfolg-

LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

ten Zwecken unter diesen Umständen Social Media-Plattformen noch weiter nutzen können. Es versteht sich von selbst, dass öffentliche Stellen, die dem Vorbehalt des Gesetzes unterliegen und besondere rechtsstaatliche Bindungen aufweisen, hier wesentlich schneller und strikter vorgehen müssen als nicht-öffentliche Stellen, als Unternehmen und Vereine, die auf diesen Plattformen zumeist aus Werbezwecken unterwegs sind. Der LfDI wird daher zunächst die Behörden des Landes, mit denen bereits seit Mitte 2019 intensive Gespräche geführt werden, auf ihr Verhalten ansprechen und versuchen, im Dialog zu einer Verbesserung der Situation beizutragen. Wie auch immer die Positionen der Behörden dabei sind: So, wie es jetzt ist, kann es auf keinen Fall bleiben.

Damit ist auch die Frage von Alternativen angesprochen – und da sieht es nicht besonders komfortabel aus: Eine datenschutzkonforme Alternative zu Facebook ist weit und breit nicht in Sicht, Facebook ist jedenfalls in Europa quasi ein Monopolist, was sich negativ auf deren Veränderungsbereitschaft auswirken dürfte. Bei Twitter gibt es zwar mit Mastodon einen funktionstüchtigen Konkurrenten mit datenschutzkonformer dezentraler Struktur – dem fehlt es allerdings noch an Reichweite. Ansonsten besteht gerade im öffentlichen Sektor die Chance, durch Aufbau einer eigenen staatlichen Plattform eine autarke und rechtmäßige Alternative zu schaffen. Anfangs wirken solche Gegenmodelle immer etwas unbeholfen – aber das muss ja nicht so bleiben. Und gegenüber öffentlichen Stellen könnte der Gesetzgeber eine Pflichtnutzung der öffentlichen Plattform anordnen und damit für genügend „traffic“ sorgen.

Wie geht es jetzt beim LfDI weiter, wenn er Ende Januar seinen Twitter-Account

schließt? Als Ausgleich für die dann verlorene Reichweite bietet sich ein Bündel an kommunikativen Maßnahmen an: Wir werden unseren vierteljährlichen Newsletter stärken, einen eigenen Podcast aufsetzen und prüfen, ob wir mit einem täglichen E-Mail-Infodienst jene Rückmeldungen, die bisher auf unmittelbare Ansprache via Twitter gegeben werden konnten, einem Kreis von Abonnenten unseres Mail-Services weiter sicherstellen können.

Also: Auch nach Twitter wird der LfDI so kommunikativ, kreativ, responsiv und spontan wie nur irgend möglich bleiben. Wir schaffen das!



LfDI BW - 35. Tätigkeitsbericht 2019 - 1. Schwerpunkte

2. Innere Sicherheit

2.1. Funkzellen-Abfrage

Die Strafprozessordnung (StPO) sieht in § 100g Absatz 3 unter den dort genannten Voraussetzungen die Möglichkeit vor, im Rahmen von Ermittlungsverfahren alle in einer Funkzelle angefallenen Verkehrsdaten zu erheben.

Unter Verkehrsdaten im Sinne des Telekommunikationsgesetzes (TKG) versteht man die Daten, die bei einer Telekommunikation anfallen, also zum Beispiel die Rufnummer der beteiligten Anschlüsse sowie Zeit und Ort eines Gesprächs. Bei der Funkzellenabfrage fordern Ermittler von den Telekommunikationsanbietern alle Verkehrsdaten an, die zu einem bestimmten Zeitraum im Bereich bestimmter Funkzellen registriert wurden, um Straftäter zu identifizieren. Dabei werden regelmäßig unvermeidbar auch Verkehrsdaten Dritter, namentlich solcher Personen erhoben, die sich – ohne Beschuldigte zu sein oder jemals zu werden – in der abgefragten Funkzelle mit ihrem Mobiltelefon aufgehalten haben. § 101a Absatz 6 StPO sieht eine Pflicht zur Benachrichtigung der Beteiligten der betroffenen Telekommunikation vor. Verwiesen wird dabei aber auf die Ausnahmemöglichkeiten nach § 101 Absatz 4 StPO. § 101 Absatz 4 Satz 5 StPO befasst sich mit der Fallgestaltung, dass die Identität einer von einer heimlichen Ermittlungsmaßnahme betroffenen Person nicht bekannt ist, sodass eine Benachrichtigung praktisch nur erfolgen kann, wenn zuvor mittels entsprechender Nachforschungen ihre Identität festgestellt wird. Damit bezieht sich die Norm nicht auf einen Beschuldigten, dessen Identität in diesem Stadium des Ermittlungsverfahrens bereits bekannt ist, sondern auf einen zufällig von der Ermittlungsmaßnahme betroffenen, nicht

tatverdächtigen Dritten. In Bezug auf diese Personengruppe können Nachforschungen den Grundrechtseingriff sowohl für die Zielperson als auch für sonstige Beteiligte vertiefen. Der Gesetzgeber hat daher die in § 101 Absatz 4 Satz 5 StPO vorgesehene Entscheidung den Ermittlungsbehörden übertragen, zumal sich die Identität der betroffenen Personen häufig nur mit hohem Aufwand ermitteln lässt. Regelmäßig berufen sich die Strafverfolgungsbehörden hierauf und verzichten auf die Benachrichtigung.

In Berlin geht man hier neuerdings einen anderen, datenschutzfreundlicheren Weg. Bürger sollen durch die Einführung eines Transparenzsystems besser informiert werden, wenn ihre Handydaten in Ermittlungsverfahren zufällig erfasst wurden. Dieses „Funkzellenabfragen-Transparenz-System“ (FTS) funktioniert so, dass man bei einer eigens bei der Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung eingerichteten Informationsstelle seine Mobilfunknummer in einer „Opt-In-Liste“ (Liste von Interessentebekundungen, vgl. fts.berlin.de) hinterlegen kann. Nach der Registrierung erhält der Handynutzer eine Benachrichtigung über die Erfassung seiner Nummer, wenn diese im Rahmen einer Funkzellenabfrage durch Strafverfolgungsbehörden beim Mobilfunkbetreiber abgefragt wurde. Die Benachrichtigung per SMS erfolgt jedoch erst dann, wenn das Ermittlungsverfahren beendet ist, also entweder Anklage erhoben wurde oder das Verfahren eingestellt wurde. Die Benachrichtigung enthält u. a. Angaben über das Datum, die Uhrzeit, den ungefähren Ort und die rechtlichen Grundlagen der Funkzellenabfrage.

LfDI BW - 35. Tätigkeitsbericht 2019 - 2. Innere Sicherheit

Unter Transparenzaspekten halte ich das FTS für äußerst innovativ und empfehle dringend, die Einführung auch in Baden-Württemberg ernsthaft zu prüfen. Eine erste Kontaktaufnahme mit dem Justizministerium gibt Anlass zu gewisser Hoffnung. Von dort wurde mir zwar mitgeteilt, man wolle erst noch einen Erfahrungsbericht der Berliner Senatsverwaltung abwarten, um dann „gegebenenfalls im Verbund mit den übrigen Landesjustizverwaltungen“ zu entscheiden. Diese Einschränkung dürfte jedoch voraussichtlich zu einer Verschiebung des Einsatzes auf den Sankt Nimmerleinstag führen. Hier fordere ich mehr Mut der Landesregierung, sich an die Spitze zu setzen und im Sinne einer fortschrittlichen, bürgerfreundlichen Verwaltung Zeichen zu setzen.

2.2 Eurodac

Nicht nur auf Bundesebene und auf Ebene der Länder führen Sicherheitsbehörden Dateien mit personenbezogenen Daten. Auch auf europäischer Ebene werden für verschiedenste Zwecke Informationssysteme geschaffen, die die Grundlage für eine effektive Zusammenarbeit der mitgliedstaatlich jeweils zuständigen Behörden bilden.

Dass der Umgang der nationalen Behörden mit personenbezogenen Daten im europäischen Kontext ebenso der Kontrolle bedarf wie bei rein innerstaatlichen Verarbeitungen, liegt auf der Hand. In bestimmten Bereichen hat der europäische Gesetzgeber regelmäßige Kontrollen durch die nationalen Datenschutzaufsichtsbehörden explizit vorgeschrieben. Hiervon sind auch die Aufsichtsbehörden der Länder betroffen, soweit es um die Nutzung dieser Datenbanken durch die jeweilige Länderpolizei geht.

Um dieser Kontrollpflicht nachzukommen, hat sich meine Dienststelle zunächst dem europäischen Fingerabdruck-Identifizierungssystem Eurodac zugewandt.

Zur Unterstützung bei der Ermittlung der Zuständigkeit nach der sog. Dublin-III-Verordnung, die regelt, welcher Mitgliedstaat der EU für die Durchführung eines Asylverfahrens zuständig ist, wurde im Jahr 2000 die Errichtung der Fingerabdruck-Datenbank Eurodac beschlossen, die 2003 den Betrieb aufnahm. Die beiden EG-Verordnungen, die das Verfahren von Eurodac regelten, wurden 2013 durch die ab dem 20. Juli 2015 geltende Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Eurodacs auf den Abgleich mit Eurodac-Daten (ABl L 180 S. 1; nachf.: Eurodac-VO) abgelöst. Die Eurodac-VO dient in erster Linie zur Feststellung der Identität von Personen, die Asyl beantragt haben oder beim illegalen Überschreiten der Außengrenzen der EU aufgegriffen wurden sowie zur Feststellung, ob ein Drittstaatsangehöriger oder Staatenloser, der sich illegal in einem Mitgliedstaat aufhält, bereits in einem anderen Mitgliedstaat einen Asylantrag gestellt hat. In Eurodac werden im Wesentlichen Fingerabdruckdaten gespeichert. Auf Anfrage kann die Information erfolgen, ob die angefragte Person bereits in einem der Mitgliedstaaten einen Asylantrag gestellt hatte.

LfDI BW - 35. Tätigkeitsbericht 2019 - 2. Innere Sicherheit

2015 wurde der Anwendungsbereich der Eurodac-VO dahingehend erweitert, dass auch den Strafverfolgungsbehörden der Zugriff auf die Eurodac-Datenbank zum Zwecke der Strafverfolgung und Gefahrenabwehr ermöglicht wurde, soweit es sich um terroristische Straftaten oder sonstige schwere Straftaten handelt (Artikel 19 Absatz 1 in Verbindung mit Artikel 1 Absatz 2 Eurodac-VO). Im Einzelfall bedarf die Abfrage eines begründeten Antrags, der die formalen und inhaltlichen Voraussetzungen des Artikels 20 Absatz 1 Eurodac-VO erfüllt:

- Formal müssen zunächst andere Dateien (nationale Fingerabdruck-Datenbanken, PRÜM-Recherche, Visa-Informationssystem) abgefragt werden („Abfrage-Kaskade“).
- Inhaltlich muss es um terroristische oder sonstige schwere Straftaten gehen (1),
- der Abgleich muss konkret erforderlich sein (2) und
- es müssen hinreichende Gründe vorliegen, welche annehmen lassen, der Abgleich werde wesentlich zur Verhütung, Aufdeckung oder Ermittlung einer der fraglichen Straftaten beitragen (3).

Das Vorliegen dieser Voraussetzungen regelmäßig zu prüfen obliegt den Datenschutzaufsichtsbehörden (Artikel 30 Absatz 1, Artikel 32 Absatz 2, Artikel 33 Absatz 2 Eurodac-VO).

Im Rahmen unserer Prüfung ließen wir uns vom Landeskriminalamt Baden-Württemberg die (standardisierten) Anträge auf Eurodac-Recherchen aus dem Jahr 2018 vorlegen. Es handelt sich insgesamt um 16 Vorgänge. In keinem Fall ergaben sich für uns Anhaltspunkte, die Zweifel am Vor-

liegen der rechtlichen Voraussetzungen für den Datenbankabgleich begründet hätten:

- In allen Fällen war vor Antragstellung die „Abfrage-Kaskade“ durchlaufen worden. Inhaltlich ging es in allen Fällen um Maßnahmen der Strafverfolgung.
- Den Anträgen lagen folgende Delikte zugrunde: Beteiligung an einer kriminellen Vereinigung, Terrorismus, Bandendiebstahl, Menschenhandel und Tötungsdelikte (1).
- Die Abgleiche erfolgten einzelfallbezogen, wobei jeweils hinreichende Gründe für die Annahme bestanden, dass der Abgleich Informationen erbringen könnte, die wesentlich zur Verfolgung dieser Straftaten beitragen würden (2).
- Schließlich bestand in allen Fällen der begründete Verdacht, dass die Betroffenen einer Personenkategorie zuzuordnen waren, die von der Eurodac-VO erfasst werden (3).

Im Ergebnis war der Umgang der Polizei mit diesem Informationssystem deshalb nicht zu beanstanden.

2.3 Schmähgesänge im Fußballstadion

Wer sich Fußballspiele im Fernsehen anschaut, bekommt neben dem eigentlichen Spielgeschehen auf dem Rasen regelmäßig auch einen Einblick in das Zuschauerverhalten – in Bild und Ton. Stadionbesucher sind insofern für eine unbegrenzte Öffentlichkeit grundsätzlich erkenn- und im Zweifel auch identifizierbar. Bild- und Tonaufnahmen von Sportveranstaltungen sind fester Bestandteil des Angebots öffentlicher und privater Fernsehsender. Kein Stadionbesucher käme auf die Idee,

LfDI BW - 35. Tätigkeitsbericht 2019 - 2. Innere Sicherheit

solche Übertragungen unter dem Gesichtspunkt des Datenschutzes in Frage zu stellen. Anders wird es aber bisweilen dann gesehen, wenn ein Verein das Stadiongeschehen optisch und gegebenenfalls auch akustisch dokumentiert, oder wenn dies durch die Polizei geschieht. Hier steht die nicht unberechtigte Sorge im Hintergrund, dass diese Aufnahmen im Einzelfall für den jeweils Betroffenen nachteilige Maßnahmen verwendet werden. So auch in einem Fall, in dem wir uns mit einer Beschwerde befassen mussten, in dem es um die Bild- und Tonerfassung von „Schmähgesängen“ im Stadion eines Fußballvereins der 1. Bundesliga ging.

Ein baden-württembergischer Fußballverein schaffte in der Vergangenheit auch aufgrund des finanziellen Engagements einer Privatperson den Aufstieg in die 1. Bundesliga. Dies stand wiederholt in der Kritik und führt zu massiven Anfeindungen des Mäzens durch Fans von Gastvereinen, die sich in unflätigen Beleidigungen äußerten. Weder der Verein noch der Adressat der Beleidigungen wollten dies weiter hinnehmen. Um dagegen vorzugehen, wurden Bild- und Tonaufnahmen, die während des Spiels mit entsprechenden technischen Einrichtungen des Vereins gemacht wurden, herangezogen. Dazu muss man wissen, dass der Deutsche Fußballbund die Vereine der 1. und 2. Bundesliga sowie der 3. Liga und der Regionalligen zur Vorhaltung einer Videoüberwachungsanlage in ihren Stadien verpflichtet, welche der Polizei zur Nutzung zur Verfügung gestellt werden muss. Nicht vorgeschrieben und nicht üblich sind dagegen Mikrofone. Dass ein solches im gegenständlichen Stadion installiert ist, hängt offenbar mit den örtlichen Besonderheiten zusammen. Wie dem auch sei, jedenfalls kam es bei einem Fußballspiel wieder zu den – leider üblichen – üblen Beleidigungen. Die Polizei nahm

dies zum Anlass, aus den Videoaufnahmen des Gästefanblocks einzelne Personen, die sich an den Beleidigungen beteiligt hatten, herauszugreifen und deren Daten sowohl dem Verein als auch dem Verletzten mitzuteilen. Der Verein verhängte daraufhin Stadionverbote und der Verletzte stellte Strafantrag wegen Beleidigung.

Datenschutzrechtlich handelt es sich bei den Bild- und Tonaufnahmen um personenbezogene Daten. Für den Personenbezug reicht es aus, dass eine Person, deren konkrete Identität (noch) nicht feststeht, durch Verknüpfung mit Zusatzinformationen letztlich doch identifiziert werden kann. Vorliegend war es so, dass die Polizei einzelne Personen aus dem Gästefanblock, die sich ersichtlich an den Beleidigungen beteiligt hatten, mithilfe sog. szenekundiger Beamte des Gastvereins ermitteln konnte. Die Beteiligung an den Beleidigungen konnte nachgewiesen werden, indem die Tonaufnahmen mit den Lippenbewegungen verglichen wurden. Der Verein und der Verletzte erhielten dann die Informationen von der Polizei, damit sie ihre Rechtsansprüche geltend machen konnten. Der Personenbezug der Bild- und Tonaufnahmen konnte hier für alle drei Verantwortlichen angenommen werden, da sie jeweils über rechtliche Mittel verfügten, die es ihnen erlauben, die betreffenden Personen anhand von Zusatzinformationen, über die Dritte (szenekundige Beamte bzw. Polizei) verfügten, bestimmen zu lassen (hierzu: EuGH, Urteil vom 19.10.2016, C-582/14, Celex-Nr. 62014CJ0582, Rn. 47, 49).

Für die Frage der datenschutzrechtlichen Rechtfertigung dieser Datenverarbeitungen war seitens der Polizei Folgendes festzustellen:

Die Polizei nimmt sowohl Aufgaben der Gefahrenabwehr als auch der Strafverfolgung wahr. Im einen Fall richten sich die Grund-

LfDI BW - 35. Tätigkeitsbericht 2019 - 2. Innere Sicherheit

lagen für die Datenverarbeitung nach dem Polizeigesetz, im anderen Fall nach der Strafprozessordnung. Im Einzelfall ist bei doppelunktionalen Maßnahmen anhand des (erkennbaren) Grunds oder Ziels des polizeilichen Handelns und gegebenenfalls dessen Schwerpunkts zu bestimmen, ob die streitbefangenen Maßnahmen der Gefahrenabwehr oder der Strafverfolgung dienen. Im gegebenen Fall war das etwas kompliziert, was daran liegt, dass das Polizeigesetz bei Fußballveranstaltungen zwar grundsätzlich Bild- und Tonaufnahmen zulässt, aber eben nur zu dem Zweck, im Gefahrenfall rechtzeitig eingreifen zu können, um die Gefahr abzuwehren. Nun wurde seitens der Polizei aber eingeräumt, bei Beleidigungen während des Fußballspiels nicht unmittelbar einschreiten zu wollen, da dies das Risiko einer Eskalation beinhaltet. Die Tonaufnahmen waren damit rein strafprozessual motiviert. Auf das Polizeigesetz als Rechtsgrundlage für die Tonaufnahmen konnte man sich deshalb nicht berufen. Vielmehr wurde insoweit auf die Ermittlungsgeneralklausel des § 163 der Strafprozessordnung (StPO) abgestellt, die nach Auffassung der Polizei auch Grundlage für Tonaufnahmen sein kann. Dies ist zwar nicht unumstritten, konnte aber von uns nicht völlig ausgeschlossen werden. Insbesondere kam aus unserer Sicht die Spezialregelung des § 100f StPO (Akustische Überwachung außerhalb von Wohnraum) hier nicht zum Tragen, da es, als die Schmähesänge erfasst wurden, noch keinen Beschuldigten im rechtlichen Sinne gab. Da aber jedenfalls der Anfangsverdacht einer Straftat (Beleidigung) im Raum stand, war gegen § 163 Absatz 1 Satz 2 StPO („Ermittlungen jeder Art“) als Grundlage für die Tonaufnahmen nichts zu erinnern. Die (optische) Videoüberwachung als solche konnte dagegen auf § 21 Absatz 1 Satz 2 Nummer 2 des Polizeigesetzes (PolG) gestützt werden („wenn auf

Grund der Art und Größe der Veranstaltungen und Ansammlungen erfahrungsgemäß erhebliche Gefahren für die öffentliche Sicherheit entstehen können“).

Seitens des Vereins war von Folgendem auszugehen:

Nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f der Datenschutz-Grundverordnung (DS-GVO) ist eine Verarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Hier kamen wir zum Ergebnis, dass der Verein berechtigt war, Bild- und Tonaufnahmen vom Stadiongeschehen herzustellen und von der Polizei die Namen derjenigen zu erheben, die gegen die Stadionordnung verstoßen hatten.

Dem Verein steht das Hausrecht am Stadiongelände zu. Es beinhaltet die Befugnis, darüber zu entscheiden, wer sich im Stadionbereich aufhält. Der Inhaber des Hausrechts ist daher berechtigt, die zu dessen Wahrung erforderlichen Maßnahmen zu ergreifen, d. h. Störer zu verweisen und ihnen das Betreten für die Zukunft zu untersagen, mithin ein Hausverbot auszusprechen. Eine Beobachtung zur Wahrnehmung des Hausrechts dient sowohl einem präventiven als auch einem repressiven Zweck, indem zum einen Verstöße gegen die Hausordnung oder gar Straftaten auf dem Gelände durch Abschreckung verhindert und zum anderen die Verfolgung zivilrechtlicher Ansprüche oder die Strafverfolgung durch die Auswertung des aufgenommenen Bildmaterials zum Zweck der Beweissicherung ermöglicht werden (OVG Lüneburg, Urteil vom 29. September 2014 – 11 LC 114/13 –, juris).

LfDI BW - 35. Tätigkeitsbericht 2019 - 2. Innere Sicherheit

Das Interesse des Vereins daran, sein Hausrecht wahrnehmen zu können, kann als in diesem Sinne berechtigt anerkannt werden. Nach § 11 Nummer 7 Buchstabe d der Allgemeinen Ticket Geschäftsbedingungen (ATGB) der TSG 1899 Hoffenheim sind (u. a.) obszön anstößige oder provokativ beleidigende Parolen untersagt. Verstöße hiergegen kann der Verein gemäß § 11 Nummer 9 und 10 ATGB sanktionieren, bis hin zu einem Stadionverbot. Die Durchsetzung des Hausrechts erfordert hier die Verarbeitung personenbezogener Daten in einer Form, die geeignet ist, den Nachweis der Rechtsverletzung rechtssicher zu erbringen. Entscheidend kommt es somit auf das Ergebnis einer Interessenabwägung an. Hierzu ist zu sagen, dass das Interesse insbesondere derjenigen, die vorsätzlich gegen die ihnen bekannten und von ihnen akzeptierten Geschäftsbedingungen verstoßen, daran, im Falle eines Verstoßes hiergegen von Sanktionen unbehelligt zu bleiben, eher als gering zu bewerten ist. Dass Bild- und Tonaufnahmen auf dem Stadiongelande erfolgen, wird in § 11 Nummer 8 ATGB hingewiesen; dies ist deshalb jedem Stadionbesucher als bekannt zuzurechnen. Auch darf der Umstand, dass in Fußballstadien eine Videoüberwachung stattfindet, allgemein, jedenfalls aber bei regelmäßigen Besuchern von Fußballspielen, als bekannt vorausgesetzt werden (Erwägungsgrund 47 der DS-GVO). Zum anderen erfolgen die Beleidigungen öffentlich und für einen unbestimmten Kreis wahrnehmbar, was im Übrigen gerade beabsichtigt ist und insofern zu einer deutlichen Minderung der Schutzbedürftigkeit führt (vgl. auch: BVerfG, Beschluss vom 9. Oktober 2002 – 1 BvR 1611/96 –, BVerfGE 106, 28-51; EuGH, Urteil vom 04.05.2017, C-13/16, Celex-Nr. 62016CJ0013). Zudem handelt es sich bei Beleidigungen um Straftaten. Die Grundrechte auf Privatheit und Datenschutz sind

kein Deckmantel, unter dem Rechtsverstöße grundsätzlich folgenlos begangen werden könnten.

Seitens des Verletzten war ebenfalls davon auszugehen, dass er die Daten derjenigen, gegen die er Strafantrag wegen Beleidigung stellen wollte, auf der Grundlage des Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f DS-GVO berechtigt erheben konnte.

Die Befugnis der Polizei, die Namen der Betroffenen dem Verein bzw. dem Verletzten bekannt zu geben, entnehmen wir § 475 Absatz 4 StPO bzw. §§ 406e, 385 Absatz 3 StPO.

Letztlich kamen wir so zum Ergebnis, dass keiner der Verantwortlichen sich datenschutzrechtlich fehlerhaft verhalten hat.

2.4 Prüfung der Umsetzung von Mitteilungen der Staatsanwaltschaft über den Ausgang des Verfahrens gem. § 482 StPO (MiStrA Nr. 11)

Da die Speicherung personenbezogener Daten in polizeilichen Dateien bei Verfahrenseinstellungen regelmäßig Gegenstand datenschutzrechtlicher Prüfungen durch unsere Behörde ist und wir in der Vergangenheit im Rahmen von Einzelfallprüfungen bereits mehrfach Datenspeicherungen im polizeilichen Auskunftssystem POLAS feststellen konnten, die aufgrund der staatsanwaltschaftlichen Einstellungsverfügung hätten gelöscht sein müssen, entschieden wir uns, die polizeiliche Speicherungs- und Lösungspraxis solcher Verfahren anhand von Stichproben einmal genauer zu betrachten.

In unsere Prüfung sollten Verfahrensakten einbezogen werden, die von der Staatsan-

LfDI BW - 35. Tätigkeitsbericht 2019 - 2. Innere Sicherheit

waltschaft nach § 170 Absatz 2 der Strafprozessordnung (StPO) wegen erwiesener Unschuld oder deshalb eingestellt wurden, weil kein Straftatbestand erfüllt war. Nach § 482 Absatz 2 Satz 1 StPO unterrichtet die Staatsanwaltschaft die Polizeibehörde, die mit der Angelegenheit befasst war, über den Ausgang des Verfahrens. Aufgrund dieser Mitteilung entscheidet die Polizei über die weitere Speicherung im polizeilichen Auskunftssystem POLAS. Die Speicherung von Daten aus Ermittlungsverfahren in POLAS ist jedoch nur zulässig, wenn ein Tatverdacht begründet werden kann. Dies ist nicht der Fall, wenn der Tatverdacht durch die staatsanwaltschaftliche Entscheidung ausgeräumt wurde.

Für die Speicherung von Daten aus Ermittlungsverfahren ist vorrangig § 38 des Polizeigesetzes (PolG) maßgeblich. In Absatz 2 heißt es dort: „Zur Vorbeugenden Bekämpfung von Straftaten ist die Speicherung, Veränderung und Nutzung personenbezogener Daten bis zu einer Dauer von zwei Jahren erforderlich, wenn auf Grund tatsächlicher Anhaltspunkte der Verdacht besteht, dass die betroffene Person eine Straftat begangen hat. Ein solcher Verdacht besteht nicht, wenn die betroffene Person im Strafverfahren rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens gegen sie unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt ist und sich aus den Gründen der Entscheidung ergibt, dass die betroffene Person die Straftaten nicht oder nicht rechtswidrig begangen hat.“

Für unsere Prüfung forderten wir bei insgesamt fünf Staatsanwaltschaften jeweils zehn Verfahrensakten aus dem Bereich der allgemeinen Abteilungen an, die in den Monaten September bis November 2018 zuletzt (insgesamt und endgültig) aus den oben genannten Gründen beendet

wurden. Unter den uns von den Staatsanwaltschaften zugesandten Akten befanden sich jedoch auch Verfahren, die zwar nach § 170 Absatz 2 StPO eingestellt wurden, aber deshalb, weil die Tatbestandsmäßigkeit, Rechtswidrigkeit oder Schuld nicht nachgewiesen werden konnte. Da in diesen Fällen der Verdacht, dass die Straftat begangen wurde, in der Regel nicht ausgeräumt wird und ein Restverdacht nach § 38 Absatz 2 Satz 1 PolG begründet werden kann, ist bei dieser Art der Einstellung eine Speicherung der Daten bis zu einer Dauer von zwei Jahren zulässig. Sofern tatsächliche Anhaltspunkte vorliegen, dass die Person auch künftig eine Straftat begehen wird, können die Daten gemäß § 38 Absatz 3 PolG auch darüber hinaus gespeichert werden.

Da uns von einer Staatsanwaltschaft ausschließlich Verfahrensakten übersandt wurden, die mit der Begründung beendet wurden, dass Tatbestandsmäßigkeit, Rechtswidrigkeit oder Schuld nicht nachweisbar waren, forderten wir von dieser nochmals zehn weitere Akten mit den zu prüfenden Einstellungsbegründungen nach. Vereinzelt befanden sich unter den von den anderen Staatsanwaltschaften übersandten Akten aber auch Verfahren, die aufgrund eines Verfahrenshindernisses eingestellt wurden, z. B. weil kein Strafantrag gestellt wurde oder bereits Verjährung eingetreten war. Ein Verfahren wurde gem. §§ 374, 376 StPO wegen mangelnden öffentlichen Interesses auf den Privatklageweg verwiesen.

Wir entschlossen uns, nicht nur die ausschließlich unseren Prüfungskriterien entsprechenden Vorgänge bei den Polizeipräsidien anzufragen, sondern uns nebenbei auch anzusehen, wie die Polizei in den anderen Vorgängen hinsichtlich einer weiteren Datenspeicherung entschieden hat-

LfDI BW - 35. Tätigkeitsbericht 2019 - 2. Innere Sicherheit

te. Von den insgesamt 60 übersandten Verfahrensakten schlossen wir vorab aber 16 Fälle aus, weil die Strafanzeigen nicht von der Landespolizei sondern von anderen Behörden oder Privatpersonen direkt an die Staatsanwaltschaft gesandt wurden, die Staatsanwaltschaft selbst das Ermittlungsverfahren eingeleitet hatte oder weil sich das Ermittlungsverfahren lediglich gegen unbekannt Personen gerichtet hatte. Hinsichtlich der übrigen 44 Verfahren, wandten wir uns an insgesamt sechs Polizeipräsidien mit der Bitte, uns Auskunft über bestehende Datenspeicherungen zu diesen Vorgängen sowie die jeweiligen Speichermodalitäten zu geben.

Unter den angefragten 44 Verfahren befanden sich 29 Verfahren, die wegen erwiesener Unschuld oder deshalb eingestellt wurden, weil das angezeigte Verhalten laut der Staatsanwaltschaft keinen Straftatbestand erfüllt hatte. Von diesen Verfahren wurden seitens der Polizei nur insgesamt 18 Vorgänge mittels einer Strafanzeige der Staatsanwaltschaft vorgelegt, darunter auch drei Verkehrsstraftaten. In den anderen Verfahren wurde offenbar bereits seitens der Polizei davon ausgegangen, dass keine Strafbarkeit der Beschuldigten oder keine Straftat vorlag und die Anzeige lediglich in Berichtsform der Staatsanwaltschaft vorgelegt, sodass erst gar keine Datenspeicherungen in POLAS veranlasst wurden. Verkehrsstraftaten werden grundsätzlich nicht in POLAS gespeichert.

Erfreulicherweise konnten wir feststellen, dass keines der angefragten Ermittlungsverfahren, die aufgrund des Tenors der staatsanwaltschaftlichen Einstellungsverfügung nicht weiter gespeichert werden durften, in POLAS gespeichert war.

Zu den aus anderen Gründen zur Einstellung gekommenen Verfahren lagen über-

wiegend Datenspeicherungen in POLAS vor, wogegen grundsätzlich keine Einwände erhoben werden konnten. Allerdings fiel auch hier wieder auf, dass teilweise zu lange Speicherfristen vergeben wurden, insbesondere wenn die Ermittlungsverfahren in der Verbunddatei „Kriminalaktennachweis“ (KAN) gespeichert wurden. Über dieses Problem hatten wir bereits in unserem 34. Tätigkeitsbericht im Zusammenhang mit der Kontrolle der Vergabe des ermittlungsunterstützenden Hinweises „HWA0“ berichtet. Für die nun festgestellten Fälle wurde jeweils eine zehnjährige Speicherfrist festgesetzt, was in Anbetracht der hier zugrundeliegenden Sachverhalte und insbesondere aufgrund der Ausführungen in der staatsanwaltschaftlichen Einstellungsverfügung unverhältnismäßig lang war. So wurde z. B. im Fall eines angezeigten Körperverletzungsdelikt in der Einstellungsverfügung ausgeführt, dass nicht festgestellt werden könne, ob der Beschuldigte angegriffen oder sich lediglich gegen einen Angriff verteidigt habe. In einem anderen Fall war der Beschuldigte wegen Erpressung zur Anzeige gebracht worden. In der Einstellungsverfügung teilte die Staatsanwaltschaft mit, dass die Nachrichten lediglich Hinweise enthalten hätten, die darauf hindeuteten, der Beschuldigte habe möglicherweise versucht, die Geschädigte zu erpressen oder zumindest zu nötigen, der Inhalt der Nachrichten sei jedoch nicht eindeutig gewesen. In einem anderen Fall wegen schwerer räuberischer Erpressung hatte die Staatsanwaltschaft ausgeführt, dass die Aussagen der Beteiligten widersprüchlich und die Angaben der Geschädigten teilweise nicht glaubhaft seien. Aufgrund der zugrundeliegenden Sachverhalte und insbesondere die Formulierungen der Staatsanwaltschaft sehen wir eine zehnjährige Speicherfrist in diesen Fällen als unverhältnismäßig an. Bei der Entscheidung über die Speicherfrist muss

LfDI BW - 35. Tätigkeitsbericht 2019 - 2. Innere Sicherheit

grundsätzlich immer der Einzelfall betrachtet werden, auch wenn für Erpressungsdelikte nach § 38 PolG i. V. m. § 5 Absatz 2 Nummer 2 DVO PolG grundsätzlich eine zehnjährige Speicherfrist zulässig wäre.

Wir teilten den zwei zuständigen Polizeipräsidiien unsere Auffassung hinsichtlich der gewählten Speicherfristen mit und baten darum, die Vergabe der Speicherfristen nochmals kritisch zu prüfen. Ein Polizeipräsidium teilte uns bereits schriftlich mit, dass es unsere Auffassung teile und eine Reduzierung der Speicherfrist veranlasst habe. Die schriftliche Antwort des anderen Polizeipräsidiiums steht momentan noch aus.

Die angesprochenen Fälle zeigen, dass bei der Speicherung von Verfahren, die seitens der Staatsanwaltschaft eingestellt werden, oftmals auch die begründete Einstellungsverfügung relevant sein kann, um bei der Festlegung der Speicherfrist die Verhältnismäßigkeit zu wahren. Die Übermittlung einer begründeten Einstellungsverfügung seitens der Staatsanwaltschaft ist jedoch nicht in jedem Fall vorgesehen. In § 482 Absatz 2 StPO heißt es für die Staatsanwaltschaft: „Sie unterrichtet die Polizeibehörde in den Fällen des Absatzes 1 über den Ausgang des Verfahrens durch Mitteilung der Entscheidungsformel, der entscheidenden Stelle sowie des Datums und der Art der Entscheidung. Die Übersendung der Mitteilung zum Bundeszentralregister ist zulässig, im Falle des Erforderns auch des Urteils oder einer mit Gründen versehenen Einstellungsentscheidung.“

Die Frage, in welchen Fällen die Übersendung einer begründeten Einstellungsverfügung erforderlich erscheint, ist offen. Im Rahmen unserer Prüfung interessierte uns deshalb, ob die MAV seitens der Staatsanwaltschaft elektronisch oder in Papierform von der Staatsanwaltschaft übersandt

wurde und ob die Einstellungsverfügung mit Gründen versehen war. Den von der Staatsanwaltschaft übersandten Akten konnten wir entnehmen, dass in den meisten Verfahren eine MAV mit Gründen an die Polizei verfügt wurde, den Polizeipräsidiien in den noch gespeicherten Fällen aber immer nur dann eine begründete Einstellungsverfügung vorlag, wenn die Verfügung in Papierform ergangen ist. In der Mehrzahl der Verfahren wurde die Verfügung lediglich elektronisch versandt und ein Einstellungskürzel übermittelt, welches in den betreffenden Fällen den Einstellungsgrund „Verfahrenshindernis“ oder „Tatbestandsmäßigkeit, Rechtswidrigkeit oder Schuld nicht nachweisbar“ stand. Lediglich in einem Fall wurde mitgeteilt, dass neben der elektronischen MAV auch eine in Papierform eingegangen sei.

Unsere Prüfung hat gezeigt, dass es bei der Umsetzung der MAVs keine grundsätzlichen Probleme im Zusammenhang mit den polizeilichen Speicherungen in POLAS gibt und die Ermittlungsverfahren, die aufgrund der staatsanwaltschaftlichen Einstellungsverfügung keine weitere Speicherberechtigung hatten, auch aus POLAS gelöscht wurden.

Allerdings zeigt sich immer wieder, dass für die Festlegung der Speicherfrist jeder Einzelfall genau bewertet und geprüft werden muss, ob die festgelegte Speicherfrist anhand der besonderen Umstände des Einzelfalls wirklich verhältnismäßig ist. Im Zweifel sollte, falls eine begründete Einstellungsverfügung der Staatsanwaltschaft nicht übermittelt wurde, diese angefordert und in die Entscheidung mit einbezogen werden.

LfDI BW - 35. Tätigkeitsbericht 2019 - 3. Videoüberwachung

3. Videoüberwachung

3.1 Alles fit für die Kontrolle? – Videoüberwachung in Fitnessstudios

Zahlreich sind die wiederkehrenden Beschwerden über Kameras in Fitnessstudios. Selbst in Umkleidebereichen werden noch immer Kameras angebracht. Die schriftliche Kontrolle fünf zufällig ausgewählter Betriebe, bestätigen den Eindruck einer flächendeckenden Überwachung der Hobbysportler jedoch nur teilweise.

Bereits im 33. Tätigkeitsbericht haben wir ausführlich über den rechtlichen Rahmen der Überwachung von Fitnessstudios berichtet. Die hohe Anzahl der Beschwerden legte den Eindruck nahe, dass in fast allen Studios eine Überwachung mit Kameras stattfindet. Anlasslos kontrolliert wurden nun fünf zufällig ausgewählte Studios unterschiedlicher Größe, Lage und Ausrichtung.

Drei Studios teilten uns mit, keine Überwachungskameras einzusetzen. In einem kleinen Fitnessstudio im ländlichen Raum mit nur vier Vollzeitkräften wird ein Großteil der Trainingsfläche permanent überwacht. Ob die Überwachung der Freizeitsportler auch erforderlich ist, ist bislang unklar. Die Argumentation, wonach bei einem Verzicht auf die Kameras ein zusätzlicher Personalaufwand von bis zu 560 Stunden wöchentlich entstehen würde und letztlich der Betrieb eingestellt werden müsste, konnte uns nicht überzeugen. Ist Datenschutz für die Betreiber ein Fremdwort? – Ganz und gar nicht. Der Austausch mit der Datenschutzbeauftragten zeigt vielmehr, dass man sich in dem kleinen Betrieb sehr wohl mit dem neuen Recht auseinandergesetzt hat. Möglicherweise besteht hier ein Miss-

verständnis im Hinblick auf die Reichweite der Verkehrssicherungspflicht. Zum Schutz der Kunden vor jedweder Unannehmlichkeit und jedem erdenklichem Unglück sind auch Betreiber von Fitnessstudios nicht verpflichtet. Passen Sie also immer gut auf sich selbst auf, wenn Sie Sport treiben! Bei dem fünften kontrollierten Studio handelt es sich um einen Franchisenehmerin mit 24-Stunden-Betrieb. Zunächst hatten wir die Franchisegeberin angeschrieben. Deren Rechtsanwalt verwies uns an die Franchisenehmerin. Vertragliche Vorgaben hinsichtlich einer möglichen Videoüberwachung würden nicht gemacht. Ob ein Franchisenehmer seiner Mandantin Videokameras einsetze oder nicht, liege nicht in der Sphäre seiner Mandantin. Die Antwort der Franchisenehmerin steht noch aus. Es würde uns nicht überraschen, wenn wir demnächst einen Brief von einem alten Bekannten bekämen: Dem bereits erwähnten Rechtsanwalt, diesmal unter dem Briefkopf einer von ihm geführten Datenschutz-GmbH. Ausweislich des Internetauftritts handelt sich dabei um den Datenschutzbeauftragten der Franchisenehmerin.

Die DS-GVO hat den Bußgeldrahmen bei Datenschutzverstößen beträchtlich erhöht. Dies scheint sich in der Fitnessbranche aber noch nicht herumgesprochen zu haben. Nach wie vor erhalten wir Beschwerden von Sportlern, die eine Videoüberwachung in Umkleidebereichen anzeigen. Eine Überwachung greift hier in die Intimsphäre der Sportler ein, weshalb es sich um einen der intensivsten Eingriffe in Persönlichkeitsrechte handelt. Die schutzwürdigen Interessen der Betroffenen überwiegen in diesen Bereichen. Eine Datenverarbeitung ist daher auch bei dokumentierten Überwachungsinteressen rechtswidrig.

LfDI BW - 35. Tätigkeitsbericht 2019 - 3. Videoüberwachung

Auch wenn weiterhin viele Beschwerden eingehen, zeigen die bereits durchgeführten Kontrollen: Die Betreiber von Fitnessstudios sind in Sachen Datenschutz zwar nicht alle top fit, aber lernfähig. Wir bleiben am Ball.

3.2 Unser täglich' Brot – Videoüberwachung in Bäckereien

Seit Jahren gehen Beschwerden über die Videoüberwachung von Beschäftigten in Bäckereien bei uns ein. Dieses Jahr haben wir genauer hingeschaut: Bei Kontrollen vor Ort und in schriftlicher Form.

In 26 Bäckereien waren wir unangekündigt vor Ort. Bei fünfzehn Betrieben haben wir schriftliche Kontrollen durchgeführt. Wann ist die Überwachung zulässig? Eine Verkäuferin erklärte es uns folgendermaßen: „Ich dachte immer, wegen der Sicherheit darf man überwacht werden. Aber wenn ich jetzt überfallen werde, dann hilft mir das auch nicht. Das geht viel zu langsam. Es heißt dann auch immer ‚man muss das jetzt unterschreiben‘. Aber ich denke, dass ich das nicht muss. Doch was soll man dann bei der Arbeit machen? Ich sage immer: Es gehört Vertrauen dazu.“ Damit fasste sie die wichtigsten Aspekte kurz und prägnant zusammen. Ausführlich und in Fachsprache finden Sie dazu mehr in unseren Veröffentlichungen zur Videoüberwachung.

Ergebnis der Kontrollen vor Ort:

Der mit der Überwachung verfolgte Zweck war überwiegend unklar. Die Verhaltens- und Leistungskontrolle und Aufklärung von Mitarbeiterdiebstählen wurde nur in wenigen Fällen als Zweck ausdrücklich angegeben. Eine Information der Beschäftigten

ist überwiegend nicht erfolgt. Meist sind Hinweisschilder vorhanden. Allerdings entsprechen diese in der Regel nicht den Anforderungen der Aufsichtsbehörden.

Ergebnis der schriftlichen Kontrollen:

Nahezu alle Betriebe, die Kameras zum Einsatz bringen, möchten mit den Aufnahmen Straftaten von Beschäftigten aufklären oder verfolgen. Dokumentierte Anhaltspunkte für einen konkreten Verdacht konnten bislang nicht in einem Fall nachgewiesen werden oder sind völlig unzureichend.

Kleinere Bäckereien verzichten häufig auf Kameras – und das auch dann, wenn die Chefin nicht immer vor Ort ist. Eine Verkäuferin erklärte uns: „Wir haben keine Kameras und die brauchen wir auch gar nicht. Unser Chef vertraut uns. Wir haben einen prima Chef.“ Mangels Anhaltspunkten für einen Verstoß haben wir den Inhaber leider nicht kennengelernt. Wenn seine Mitarbeiter so von ihm sprechen, muss er ein sehr zufriedener Mensch sein.

Bei einigen Betrieben mit vielen Filialen hat die Überwachung von Beschäftigten regelrecht System. Eine Firma im Bereich der Sicherheitstechnik ist auf Überwachung spezialisiert und zählt gleich mehrere Filialketten zu seinen Kunden. Anstelle seiner Kunden erklärte uns der Geschäftsführer die Notwendigkeit seiner Produkte am Telefon: „Einfach gestrickte Hausfrauen sollen nicht in die Kasse langen. Häufig wurden die vom Mann verlassen. Wenn man Kinder hat, muss man sich da überlegen, ob man die Milch für 1,10 Euro oder für 80 Cent kauft. Das sind Leute, die finanzielle Not haben. Die nehmen Geld raus so gut es geht. Die denkt sich: Das tut keinem weh, der Chef kommt eh mit dem Porsche vorgefahren. Wenn es raus

LfDI BW - 35. Tätigkeitsbericht 2019 - 3. Videoüberwachung

kommt, entschuldigen die sich meist und es kommt nicht zur Anzeige.“ Der hier vorgetragene Generalverdacht gegen sämtliche Mitarbeiterinnen in den Betrieben seiner Kundschaft ist selbstverständlich alles andere als die gesetzlich geforderten zu dokumentierenden Anhaltspunkte für die Begründung eines Verdachts. Und aus der Verantwortung sind die Bäckereibetriebe mit einer Stellungnahme der Sicherheitsfirma freilich nicht. Verantwortlich im Sinne der Datenschutz-Grundverordnung ist und bleibt die Bäckerei selbst. Soweit uns ein Auftragsverarbeitungsvertrag vorgelegt wurde, werden auch hier ganz entscheidende Fragen offen gelassen: Technisch-organisatorische Maßnahmen zum Schutz der Daten – Fehlanzeige. Die kontrollierten Betriebe müssen davon ausgehen, dass wir uns mit solchen Antworten nicht zufrieden geben.

Manche Kunden ziehen Konsequenzen. Eine Kundin teilte uns im Rahmen Ihrer Beschwerde mit: „Seit einigen Wochen kaufe ich nicht mehr bei diesem Bäcker ein. Zuvor war ich fast täglich dort.“

Während viele kleine, inhabergeführte Bäckereien ohne Überwachung auskommen, verlässt sich eine ganze Reihe von Filialbetrieben auf fragwürdige Geschäftsmodelle der Sicherheitstechnik. Mitarbeitende werden grundlos unter Generalverdacht gestellt. Dem begegnen wir mit aufsichtsrechtlichen Maßnahmen und in einigen Fällen auch mit Bußgeldverfahren.

3.3 Berechtigte Interessen

Den Betreibern von Videokameras bereitet es selten Schwierigkeiten, ein Interesse an einer Überwachung von Personen vorzutragen. Sie möchten sich häufig vor Einbrüchen, Diebstählen, Vandalismus oder Übergriffen schützen. Viele Betreiber tun

sich aber sehr schwer damit, ein berechtigtes Interesse gegenüber der Aufsichtsbehörde ausreichend zu begründen und darzulegen.

Eine Voraussetzung einer rechtmäßigen Videoüberwachung ist, dass die Überwachungsmaßnahme der Wahrung eines berechtigten Interesses des Verantwortlichen oder eines Dritten dient. In Betracht kommt hierbei der Schutz vor Einbrüchen, Diebstahl, Vandalismus oder Übergriffen. Dies sind gängige Ziele einer Videoüberwachung. Da ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage ideeller, wirtschaftlicher oder rechtlicher Natur sein kann, sind diese Interessen auch generell schutzwürdig. Berechtigt ist ein Überwachungsinteresse aber nur dann, wenn es rechtmäßig, hinreichend klar formuliert und nicht rein spekulativ ist (vgl. Stellungnahme 06/2014 der Artikel-29-Datenschutzgruppe zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG (WP 217), S. 32, S. 70.). Das Bundesverwaltungsgericht führt in seinem Urteil vom 27. März 2019 (Az. 6C 2.18, Rn. 28) dazu aus:

„Die Gesichtspunkte der Verhinderung und Aufklärung von Straftaten stellen grds. berechtigte Interessen i.S.v. § 6b Absatz 1 Nr. 3 BDSG a.F. dar (redaktionelle Anmerkung: Das berechtigte Interesse findet sich jetzt in Art. 6 Absatz 1 Buchstabe f DSGVO). Sie können eine Videoüberwachung jedoch nur dann als objektiv begründbar rechtfertigen, wenn eine Gefährdungslage besteht, die über das allgemeine Lebensrisiko hinausgeht. Eine solche Gefährdung kann sich nur aus tatsächlichen Erkenntnissen ergeben; subjektive Befürchtungen oder ein Gefühl der Unsicherheit reichen nicht aus.“

LfDI BW - 35. Tätigkeitsbericht 2019 - 3. Videoüberwachung

Für Betreiber einer Videoüberwachung bedeutet das Folgendes: Beschädigungen, Vorfälle in der Vergangenheit oder andere Ereignisse, die eine Gefahrenlage objektiv begründen können, müssen gegenüber der Aufsichtsbehörde nachgewiesen werden. Ein solcher Nachweis kann sich nur aus einer konkreten Beschreibung entsprechender Vorfälle ergeben. Mindestens sollte dazu die Art des Ereignisses, der Ort, der Zeitpunkt und die Häufigkeit von Vorfällen angegeben werden. Eine Beschreibung sollte so genau wie möglich erfolgen, beispielsweise mit Datum und Uhrzeit. Auch die Angabe der Schadenshöhe, eine Beschreibung des beschädigten Objekts, Schadensmeldungen bei einer Versicherung oder Anzeigen bei der Polizei helfen dabei, die Bedeutung des eigenen Überwachungsinteresses zu begründen und beispielsweise gegenüber bloßen Bagatelldelikten abzugrenzen. Konkrete Vorfälle müssen dabei nicht beim Überwachenden selbst stattgefunden haben. In bestimmten Fällen kann sich eine Gefahrenlage auch daraus ergeben, dass – mit gewissem zeitlichem Zusammenhang – vergleichbare Vorfälle oder Übergriffe in der unmittelbaren Nachbarschaft stattgefunden haben. Hier sind Vorfälle nachzuweisen, aus welchen sich eine zeitliche, sachliche und örtliche Verbindung zum eigenen Überwachungsinteresse ergibt. Nur im Ausnahmefall ist der Nachweis einer rein abstrakten Gefahrenlage ausreichend. Beispielsweise wenn eine Situation vorliegt, die nach allgemeiner Lebenserfahrung typischerweise gefährlich ist. Beispielsweise in Ladengeschäften, die wertvolle Ware verkaufen (z. B. Juweliere) oder die im Hinblick auf Vermögens- und Eigentumsdelikte besonders gefährdet sind (z. B. Tankstellen).

Subjektive Befürchtungen oder ein Gefühl der Unsicherheit begründen für sich genommen kein berechtigtes Interesse an ei-

ner Videoüberwachung. Als Gefühl ist „Sicherheit“ nicht fassbar. Gefühle lassen sich nicht in Zahlen fassen oder empirisch nachweisen. Eine Person kann sich an einem bestimmten Orten unsicher fühlen, obwohl eine Gefahr tatsächlich nicht besteht oder rational begründet ist. Dem, der sich unsicher „fühlt“, kann dabei nicht automatisch das Recht zugestanden werden, ganz real in Persönlichkeitsrechte Dritter einzugreifen. Würde ein nicht messbares Gefühl für einen solchen Eingriff ausreichen, könnten Überwachungsmaßnahmen laufend verschärft und Videoüberwachungen uferlos in öffentliche Räume ausgedehnt werden. Das Recht der Betroffenen auf informationelle Selbstbestimmung wäre nahezu entwertet. Eine gefühlsorientierte Behauptung würde ausreichen, um es zu beschränken. Das Interesse, die gefühlte Sicherheit zu erhöhen, kann daher nur neben ein tatsächlich begründbares Interesse treten. Aus dem gleichen Grund rechtfertigt auch eine vermeintlich abschreckende Wirkung von Videoüberwachung für sich genommen keinen dauerhaften und anlasslosen Eingriff in Rechte Dritter.

Ein berechtigtes Interesse an einer Videoüberwachung muss konkret vorliegen und nachweisbar begründet sein. Vorfälle, Ereignisse und Beschädigungen sind daher zu dokumentieren (Datum, Art und Ort des Vorfalls, Schadenshöhe, etc.). Strafanzeigen und Versicherungsmeldungen sollten zum Nachweis des Überwachungsinteresses aufbewahrt werden.

3.4 Orientierungshilfen zur Videoüberwachung

Der Betreiber einer Videoüberwachung ist verpflichtet die Vorschriften des Datenschutzes einzuhalten. Die rechtliche Prüfung einer Anlage ist von Fall zu Fall verschieden und nicht unbedingt leicht.

LfDI BW - 35. Tätigkeitsbericht 2019 - 3. Videoüberwachung

Der Betreiber muss unbestimmte Rechtsbegriffe auslegen, Dokumentations- und Transparenzvorschriften beachten, alternative Maßnahmen prüfen, schutzwürdigen Interessen von Betroffenen erkennen und diese im Einzelfall mit seinen eigenen Überwachungsinteressen abwägen. Um den Betreibern die Einhaltung gesetzlicher Vorschriften zu erleichtern und ihnen Wege zu einem rechtmäßigen Einsatz von Videokameras aufzuzeigen, veröffentlichen und überarbeiten die Aufsichtsbehörden laufend Orientierungshilfen zu den unterschiedlichsten Themen. Besonders der bundesweite Arbeitskreis zur Videoüberwachung – der unter der Leitung Baden-Württembergs steht – liefert in seinem Arbeitsbereich kontinuierlich neues und aktualisiertes Informationsmaterial.

Videoüberwachung durch öffentliche Stellen in Baden-Württemberg

Graffiti an der Rathauswand, eine beschädigte Parkbank oder ein vermüllter Schulhof. Ungebührliches Verhalten oder Vandalismus verursacht Kosten und ist – häufig auch für Anwohner – ärgerlich. Um dem zu begegnen, wird oft und schnell die Installation einer Videoüberwachungsanlage in Betracht gezogen oder gar im Gemeinderat beschlossen. „Was spricht schon dagegen? Kameras überwachen uns ja auch sonst auf Schritt und Tritt.“, mögen sich Entscheider denken.

Dabei muss einer öffentlichen Stelle bewusst sein, dass sie mit Videoüberwachungen in Grundrechte von gefilmten Personen eingreift. Dieser Eingriff kann nur rechtmäßig erfolgen, wenn eine Datenverarbeitung die Voraussetzungen einer Rechtsgrundlage erfüllt. In Baden-Württemberg ist seit Juni 2018 die Zulässigkeit einer Videoüberwachung öffentlich zugänglicher Räume in § 18 LDSG geregelt. Die Norm weicht an einigen Stellen von der Vorgängervor-

schrift ab. Auf unserer Webseite haben wir zur Anwendung der Vorschrift eine Orientierungshilfe veröffentlicht. Sie unterstützt öffentliche Stellen dabei, eine Videoüberwachung rechtskonform nach den Vorgaben der DS-GVO und des § 18 LDSG einzurichten. Die Vorschriften werden erläutert, die Voraussetzungen einer transparenten Hinweisbeschilderung aufgezeigt und auf technisch-organisatorischen Schutzmaßnahmen hingewiesen.

Einsatz von Bodycams durch private Sicherheitsunternehmen

Private Sicherheitsunternehmen rüsten ihre Beschäftigten mittlerweile mit beweglichen Körperkameras, sogenannten Bodycams aus. Als Überwachungszwecke führen sie den Schutz von Beschäftigten vor Übergriffen oder Beschaffung von Beweismitteln für zivilrechtliche Ansprüche an. Viele erhoffen sich eine abschreckende oder deeskalierende Wirkung der Kameras. Der private Einsatz von Bodycams birgt dabei einige datenschutzrechtliche Risiken. Bei einem Einsatz an öffentlichen Orten besteht die Gefahr, dass Betroffene von ihren Grundrechten nur noch eingeschränkt Gebrauch machen. Zudem müssen Passanten detaillierte Film- oder Tonaufnahmen befürchten, wenn mit Bodycams ausgerüstete Sicherheitskräfte Streifengänge auf einem gut besuchten Gelände unternehmen oder eine Menschenmenge durchqueren. Je nach Befestigung und Verwendung der Kamera kann es dabei auch zu verdeckten Datenverarbeitungen und Überwachungsmaßnahmen kommen. Der Einsatz einer Bodycam durch private Sicherheitsunternehmen ist an Art. 6 Absatz 1 Buchstabe f DS-GVO zu messen. Was aus Sicht der Aufsichtsbehörden bei einem solchen Einsatz von Körperkameras zu beachten ist, können Sie in unserer Orientierungshilfe nachlesen. Diese ist auf unserer [Webseite](#) veröffentlicht.

Leitlinien des Europäischen Datenschutz-Ausschusses zur Videoüberwachung

Auf europäischer Ebene hat der Europäische Datenschutzausschuss im Juli 2019 eine Leitlinie zur Videoüberwachung angenommen. Nachdem das Verfahren zur Öffentlichkeitsbeteiligung abgeschlossen ist, wird der Inhalt der Leitlinie auf Videoüberwachungsanlagen in ganz Europa angewendet. Die Leitlinie wird die Auslegung der DS-GVO für Videoüberwachungen maßgeblich mitbestimmen. Das Dokument wird auf der Webseite der Datenschutzkonferenz (www.datenschutzkonferenz-online.de) veröffentlicht.

Videoüberwachung durch nicht-öffentliche Stellen

An die europäische Leitlinie zur Videoüberwachung wird sich im kommenden Jahr die Veröffentlichung einer aktualisierten Fassung der Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ anschließen. Die Orientierungshilfe wird die Vorschriften des BDSG, der DS-GVO und aktuelle Gerichtsentscheidungen systematisch darstellen und praxisnahe Hinweise für die Prüfung der gesetzlichen Tatbestände geben. Sie wird darüber hinaus eine Vielzahl einzelner Fallkonstellationen enthalten und die Voraussetzungen einer Videoüberwachung im Beschäftigungsverhältnis behandeln.



LfDI BW - 35. Tätigkeitsbericht 2019 - 3. Videoüberwachung

4. Verkehr

4.1 Verkehr

Im Bereich Verkehr ist vor allem nach der Einführung der Datenschutz-Grundverordnung (DS-GVO) ein immenser Anstieg der Beschwerden über Bußgeldverfahren zu verzeichnen gewesen. Sensibilisiert durch die DS-GVO haben sich nicht wenige Bürger erstmals gefragt, ob die Ordnungsbehörden gegen datenschutzrechtliche Regelungen verstoßen, wenn sie die Betroffenen mittels Geschwindigkeitsüberwachungsanlagen erfassen oder wenn der gemeindliche Vollzugsdienst von Falschparkern die Kennzeichen fotografiert.

Die Datenverarbeitung der Bußgeldstelle erfolgt zu Zwecken der Verfolgung und Ahndung von Ordnungswidrigkeiten. In diesem Bereich ist nicht die Datenschutz-Grundverordnung, sondern die Richtlinie RL (EU) 2016/680 einschlägig, die anders als die DS-GVO, nicht unmittelbar gilt, sondern erst in innerstaatliches Recht umgesetzt werden musste. Die Umsetzung erfolgte durch das Landesdatenschutzgesetz für Justiz- und Bußgeldbehörden (LDSG-JB) vom 15. Mai 2019. Das Landesdatenschutzgesetz für Justiz- und Bußgeldbehörden regelt, dass besondere Rechtsvorschriften des Bundes oder des Landes vorgehen. Das Ordnungswidrigkeitsverfahren ist spezialgesetzlich im Gesetz über Ordnungswidrigkeiten (OWiG) geregelt und dieses verweist wiederum auf die Regelungen der Strafprozessordnung. Insofern haben die Bußgeldbehörden und die Mitarbeiter des Ordnungsamtes ähnliche Befugnisse wie die Strafverfolgungsbehörden. Sie dürfen einen Tatbestand ermitteln und Beweise erheben.

So ärgerlich die Knöllchen auch sind, nicht jede für den Bürger ungewollte Datener-

hebung durch die Bußgeldbehörden ist auch ein Datenschutzverstoß. Die Radarkontrollen zur Geschwindigkeitsmessung und auch die Fotos von Falschparkern sind durch den Ermittlungsgrundsatz der Bußgeldbehörden gedeckt.

4.2 Behörde setzt auf Postkarte

Die Führerscheinstelle eines Landratsamts verschickte wohl aus Kostengründen Postkarten an Antragsteller. Auf diesen Postkarten standen nicht nur das Aktenzeichen und der Name der Sachbearbeitung bei der Führerscheinstelle, sondern vorgedruckt und zum Ankreuzen auch, welche Unterlagen noch bei der Führerscheinstelle vorzulegen seien. Dies reichte von ärztlichen Bescheinigungen über das Sehvermögen bis zu sonstigen ärztlichen Bescheinigungen und Gutachten für die Erteilung oder Verlängerung von Fahrerlaubnissen nach der Fahrerlaubnisverordnung. Handschriftlich konnten noch offene Gebühren und weitere Mitteilungen an die Antragstellenden eingetragen werden.

Besonders pikant war in dem Fall, der meiner Behörde gemeldet wurde, dass dem Antragsteller handschriftlich auf der Postkarte mitgeteilt wurde, er könne nicht als Begleitperson für das begleitete Fahren eingetragen werden.

Durch die offene Postkarte wurden die vertraulichen Vorgänge zwischen Bürgerinnen und Bürgern und der Verwaltung auf eine Art und Weise verarbeitet, die die Kenntnisnahme unbeteiligter Dritter von diesem Verfahren ermöglicht. Damit wurde die Vertraulichkeit und Integrität von besonders schutzwürdigen Gesundheitsdaten verletzt. Die Regelungen der Datenschutz-Grundverordnung besagen, dass Daten nur in der Art und Weise verarbeitet werden dürfen, die eine angemessene Sicherheit der personenbezogenen Daten

LfDI BW - 35. Tätigkeitsbericht 2019 - 4. Verkehr

gewährleistet. Das bedeutet, dass Maßnahmen zu ergreifen sind, die vor einer Kenntnisnahme der Daten durch Unbefugte schützt.

Es liegt eigentlich auf der Hand, dass vertrauliche Informationen im Behördenverkehr grundsätzlich in geschlossenen Briefumschlägen zu verschicken sind.

Meine Behörde hat in diesem Fall nicht um Stellungnahme gebeten, sondern das Landratsamt unmittelbar angewiesen, die Kommunikation von Verwaltungsvorgängen ab sofort ausschließlich vor dem Zugriff Dritter geschützt durchzuführen und für Mitteilungen an die Beteiligten in einem Verwaltungsverfahren einen geschlossenen Umschlag zu benutzen sowie von der Versendung offener Postkarten abzusehen.

Der Landrat hat diese Weisung sofort umgesetzt.

4.3 Entwicklung von Künstlicher Intelligenz (KI) im Bereich Verkehr

Die erste Datenschutzfolgenabschätzung, die meine Behörde begleitete, fand im Bereich Verkehr statt.

Ein Automobilzulieferer entwickelt für seine Kunden Algorithmen für das autonome Fahren. Um diese jedoch zu trainieren, werden reale Fahr- und Verkehrsbedingungen benötigt. Andernfalls kommt es zu Fehlern im System, was zu fatalen Fehlern der autonom fahrenden Fahrzeuge führen kann.

In unserem Fall werden Videodaten aus Autos heraus aufgenommen. Hierbei werden zwangsläufig personenbezogenen Daten erfasst, seien es Personen auf den Gehwegen und an Ampeln, Fahrradfahrer oder andere

Verkehrsteilnehmer, sowie Kfz-Kennzeichen. Obwohl eine Identifikation der Personen oder der Kfz-Halter überhaupt nicht gewollt ist, kann die Datenerfassung nicht ohne eine Rechtsgrundlage für die Datenerhebung erfolgen. Die Zulässigkeit der Datenverarbeitung ergibt sich in diesem speziellen Einzelfall aus einem die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegenden, berechtigten Interessen des Automobilzulieferers im Sinne von Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f DS-GVO.

Bei der Interessenabwägung zugunsten des Automobilzulieferers fanden viele Faktoren Berücksichtigung, wie beispielsweise die Persönlichkeitsrelevanz, der zeitliche und räumliche Umfang, ein nur kleiner zugriffsberechtigter Personenkreis, dass die Daten nicht an Dritte herausgegeben werden sowie die eingesetzten technischen und organisatorischen Maßnahmen. Wichtig für die Interessenabwägung war noch, dass die Betroffenenrechte gewahrt werden, indem die Aufnahmefahrzeuge mit Kamerasymbol und der Information über den Verantwortlichen gekennzeichnet sind. Somit können die betroffenen Verkehrsteilnehmer von ihrem Widerspruchrecht vor Ort Gebrauch machen, indem die Sequenzen direkt im Fahrzeug gelöscht werden. Die Löschung der Videodaten ist auch im Nachhinein bei Angabe von Ort und Zeit möglich.

Die Durchführung einer Datenschutz-Folgenabschätzung ist ebenfalls in die Interessenabwägung einzubeziehen.

Die Entwicklung und Erforschung von neuer Technik soll nicht am Datenschutz scheitern, jedoch ist die Entwicklung und Forschung auch kein Freifahrtschein, datenschutzrechtliche Grundlagen und Regelungen über Bord zu werfen. Werden da-

LfDI BW - 35. Tätigkeitsbericht 2019 - 4. Verkehr

tenschutzrechtliche Grundsätze, welche die Datenschutz-Grundverordnung uns vorgibt, beachtet und sind sie Teil des Forschungsvorhabens und -verfahrens (Privacy by design), dann kann dies das Vertrauen der Bürgerinnen und Bürger in neue Technologie stärken und zu einem nicht zu unterschätzenden Wettbewerbsvorteil führen.



LfDI BW - 35. Tätigkeitsbericht 2019 - 4. Verkehr

LfDI BW - 35. Tätigkeitsbericht 2019 - 5. Justiz

5. Justiz

5.1 Wie erfüllen Notare ihre datenschutzrechtlichen Informations- und Dokumentationspflichten? – Kontrollkampagne

Um in Erfahrung zu bringen, wie Verantwortliche mit in der Datenschutz-Grundverordnung (DS-GVO) enthaltenen Informations- und Dokumentationspflichten umgehen, hat meine Dienststelle im Rahmen einer anlasslosen Kontrollkampagne im Mai 2019, also nach knapp einem Jahr seit Geltung der Datenschutz-Grundverordnung, zwanzig zufällig ausgewählte Notare aufgefordert, zum einen nachzuweisen, wie sie ihren Informationspflichten gegenüber den von einer Datenerhebung Betroffenen gemäß den Artikeln 13, 14 DS-GVO nachkommen und zum anderen, ihr Verzeichnis von Verarbeitungstätigkeiten gemäß Artikel 30 DS-GVO vorzulegen.

Ablauf der Kontrollkampagne:

Die Verpflichtung, meiner Dienststelle die angeforderten Unterlagen auf Anfrage vorzulegen, ergibt sich bzgl. der Verzeichnisse von Verarbeitungstätigkeiten aus der in Artikel 30 Absatz 4 DS-GVO ausdrücklich genannten Vorlagepflicht und bzgl. der Datenschutzinformationen gemäß den Artikeln 13, 14 DS-GVO aus der allgemeinen Unterstützungspflicht des § 26 Landesdatenschutzgesetz (LDSG), der auch Notare zur Kooperation verpflichtet.

Wie bereits erwähnt, bestanden die genannten Informations- und Dokumentationspflichten zu Beginn der Kontrollaktion bereits seit knapp einem Jahr. Meine Dienststelle ist deshalb davon ausgegangen, dass die Notare – die Organe der Rechtspflege und Träger eines öffentlichen

Amtes sind – die entsprechenden Unterlagen bereits Monate vor der Kontrollaktion meiner Dienststelle erstellt haben, sodass sie diese ohne großen Aufwand an meine Dienststelle übersenden können und dies aufgrund ihrer, meiner Dienststelle gegenüber bestehenden Unterstützungs- und Vorlagepflicht auch tun.

Tatsächlich haben fünfzehn der zwanzig Notare innerhalb der von meiner Dienststelle gesetzten dreiwöchigen Frist bzw. einige Tage später die erbetenen Unterlagen vorgelegt.

Von den fünf anderen Notaren haben drei innerhalb der Frist um eine Fristverlängerung gebeten, aber nur in einem dieser Fälle wurden die Unterlagen innerhalb der verlängerten Frist vorgelegt.

Zwei der Notare haben auf die Aufforderung meiner Dienststelle überhaupt nicht reagiert und mussten an die Erledigung erinnert werden, die daraufhin in einem der beiden Fälle auch unverzüglich erfolgte. Selbst Anfang November, also mehr als 5 Monate nach der ersten Aufforderung meiner Dienststelle, lagen trotz mehrmaliger Erinnerungen unter Hinweis auf die Unterstützungspflicht in zwei Fällen weder die Datenschutzinformationen gemäß den Artikeln 13 und 14 DS-GVO noch das Verzeichnis der Verarbeitungstätigkeiten gemäß Artikel 30 DS-GVO und in einem Fall nur das Verzeichnis der Verarbeitungstätigkeiten vor.

Unabhängig davon, ob die verzögerte Vorlage in den einzelnen Fällen darauf zurückzuführen ist, dass die Notare ihren nach der Datenschutz-Grundverordnung bestehenden Informations- und Dokumentationspflichten oder „nur“ der meiner Dienststelle gegenüber bestehenden Unterstützungs- bzw. Vorlagepflicht nicht

LfDI BW - 35. Tätigkeitsbericht 2019 - 5. Justiz

nachgekommen sind, handelt es sich dabei um erhebliche Verstöße gegen datenschutzrechtliche Pflichten. Da gegen öffentliche Stellen gemäß § 28 LDSG keine Geldbußen verhängt werden können, stellen die vorgeschilderten Verstöße gegen datenschutzrechtliche Regelungen durch einzelne Notare als Träger eines öffentlichen Amtes und Rechtspflegeorgan zwar keine Ordnungswidrigkeiten dar. Da ein derartiges Verhalten jedoch nicht akzeptabel ist, habe ich sowohl das Ministerium der Justiz und für Europa als oberste Aufsichtsbehörde der Notare als auch die Notarkammer Baden-Württemberg aufgefordert, dafür Sorge zu tragen, dass die Notare künftig sowohl ihren Informations- und Dokumentationspflichten als auch den meiner Dienststelle gegenüber bestehenden Verpflichtungen nachkommen.

Inhaltliche Kontrolle der Datenschutzinformationen für Betroffene gemäß den Artikeln 13 und 14 DS-GVO:

Die vorgeschilderten Umstände, dass einige der Notare die angeforderten Unterlagen verspätet bzw. selbst Monate nach Anforderung durch meine Dienststelle noch nicht vorgelegt hatten, und die dadurch entstandene Verzögerung haben dazu geführt, dass bislang lediglich die inhaltliche Überprüfung der Datenschutzinformationen für Betroffene nach Artikel 13 und 14 DS-GVO durchgeführt werden konnte, die Prüfung der Verzeichnisse der Verarbeitungstätigkeiten, die sehr umfangreich sind, jedoch erst im Lauf des Jahres 2020 erfolgen kann.

Die Informationspflichten verantwortlicher Stellen gemäß den Artikeln 13 und 14 DS-GVO, die weit über die bisherige (nationale) Rechtslage hinausgehen, bilden die Grundlage für die Ausübung der Betroffenenrechte. Nur wenn eine betroffene Person weiß, dass personenbezogene Daten

über sie verarbeitet werden, kann sie ihre Betroffenenrechte, wie z. B. ihr Auskunftsrecht, auch sinnvoll und effektiv ausüben. Worüber die Betroffenen zu informieren sind, ergibt sich bei Erhebung von personenbezogenen Daten bei der betroffenen Person aus Artikel 13 DS-GVO und, wenn die personenbezogenen Daten nicht bei der betroffenen Person selbst sondern bei Dritten erhoben werden, aus Artikel 14 DS-GVO.

In beiden Fällen müssen, soweit keine Ausnahmenvorschriften greifen, u. a.

- der Name und die Kontaktdaten des Verantwortlichen,
- die Kontaktdaten des ggf. bestellten Datenschutzbeauftragten (wobei Notare einen solchen immer bestellen müssen),
- die Zwecke, für die die Daten erhoben werden sollen bzw. erhoben worden sind, sowie die Rechtsgrundlage für die Verarbeitung,
- ggf. die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten,
- die geplante Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer und etwa,
- die Betroffenenrechte (Auskunfts-, Berichtigungs-, Löschungs-, Einschränkungs- und Widerspruchsrechte sowie das Recht auf Datenübertragbarkeit)

angegeben werden.

Bei der Durchsicht der meiner Dienststelle von Notaren vorgelegten Datenschutzinformationen ist vor allem Folgendes aufgefallen:

Bei einigen der Notare bezogen sich die vorgelegten Datenschutzinformationen lediglich auf die Erhebung personenbezogener Daten im Zusammenhang mit Zugriffen auf die Website des Notars. Die Erhebung personenbezogener Daten durch den Notar im Rahmen der eigentlichen Notartätigkeit, also etwa im Zusammenhang mit der Erstellung von Urkundsentwürfen, der Beurkundung und dem Vollzug von Urkundsgeschäften oder der Durchführung von Beratungen, die von der Informationspflicht der Artikel 13 und 14 DS-GVO ebenfalls erfasst wird, war in diesen Datenschutzinformationen dagegen nicht angesprochen.

Darüber hinaus scheint es vor allem zum Thema Datenschutzbeauftragter Unklarheiten zu geben. So waren in mehreren der vorgelegten Datenschutzinformationen bzgl. der Datenschutzbeauftragten lediglich die allgemeine E-Mail-Adresse/ Telefon- und Telefaxnummer des Notariats angegeben, sodass eine unmittelbare Kontaktaufnahme eines Betroffenen mit dem Datenschutzbeauftragten nicht möglich wäre. Der Datenschutzbeauftragte muss jedoch direkt kontaktierbar sein. Daher ist in den Datenschutzinformationen mindestens eine gesonderte, direkt dem Datenschutzbeauftragten zugewiesene E-Mail-Adresse anzugeben.

In manchen Fällen wurde als Datenschutzbeauftragter jeweils ein Notarkollege innerhalb der gleichen Sozietät genannt. Notare in einer Sozietät bzw. einer Bürogemeinschaft können sich jedoch nicht gegenseitig als Datenschutzbeauftragte benennen. Ein Notar als Verantwortlicher kann sich auch nicht in eigener Sache als Datenschutzbeauftragter bestellen. Dies würde zu Interessenkollisionen führen und ließe sich nicht mit der Funktion und Aufgabe eines Datenschutzbeauftragten vereinbaren (Artikel 38 und 39 DS-GVO). Notare in einer Sozietät oder Bürogemein-

schaft sind sowohl für den Bereich ihres Amtes als auch für den wirtschaftlichen und organisatorischen Bereich die verantwortliche Stelle. Eine gegenseitige Benennung als Datenschutzbeauftragter würde im wirtschaftlichen und organisatorischen Bereich dazu führen, dass der jeweils tätig werdende Datenschutzbeauftragte bei Erfüllung seiner Aufgaben als Datenschutzbeauftragter für einen Kollegen jeweils auch sich selbst berät bzw. kontrolliert. Werden beispielsweise Fragen zur Datenverarbeitung im gemeinsamen Datenverarbeitungssystem behandelt oder geht es um eine Implementierung im gemeinsam genutzten IT-System, kann ein Mitglied der Sozietät/Bürogemeinschaft nicht frei von eigener Betroffenheit beraten oder kontrollieren. Hier sind unabhängige und fachlich versierte eigene Datenschutzbeauftragte zu bestellen.

Da die Kontrollkampagne nicht, wie geplant, im Jahr 2019 abgeschlossen werden konnte, aber auch wegen der bereits jetzt festgestellten Datenschutzverstöße, wird sich meine Dienststelle auch im Jahr 2020 verstärkt mit Notaren befassen.

5.2 Umsetzung der Richtlinie (EU) 2016/680 im Justizbereich

Bereits in meinem letzten Tätigkeitsbericht hatte ich angesprochen, dass die Datenschutz-Grundverordnung für strafrechtliche und ordnungswidrigkeitenrechtliche Verfahren keine und auch im Bereich des Justizvollzugs nur äußerst selten Anwendung findet, und dass für diese Bereiche statt dessen die Richtlinie (EU) 2016/680 datenschutzrechtliche Vorgaben enthält. Eine Richtlinie muss – anders als die unmittelbar geltende Datenschutz-Grundverordnung – durch nationales Recht umgesetzt werden und zwar, soweit dies nicht durch Bundesrecht erfolgt, durch Landesrecht.

LfDI BW - 35. Tätigkeitsbericht 2019 - 5. Justiz

Auf Landesebene ist diese Umsetzung für die Justiz- und Bußgeldbehörden vor allem durch das seit dem 6. Juni 2019 geltende Landesdatenschutzgesetz für Justiz- und Bußgeldbehörden und durch die am gleichen Tag in Kraft getretene Änderung des Justizvollzugsgesetzbuchs erfolgt.

Landesdatenschutzgesetz für Justiz- und Bußgeldbehörden (LDSG-JB)

Das Landesdatenschutzgesetz für Justiz- und Bußgeldbehörden ist anwendbar auf die Datenverarbeitung der ordentlichen Gerichte in Strafsachen, der Staatsanwaltschaften und auch für die Verarbeitung personenbezogener Daten zur Ahndung von Ordnungswidrigkeiten und zur Vollstreckung von Bußgeldern durch alle hierfür zuständigen öffentlichen Stellen des Landes. Anders als teilweise vermutet wird, gilt das Gesetz im Bußgeldbereich damit nicht nur für datenschutzrechtliche Ordnungswidrigkeiten, für die meine Dienststelle zuständig ist.

Das Landesdatenschutzgesetz für Justiz- und Bußgeldbehörden regelt auch die Zuständigkeit und die Befugnisse meiner Dienststelle im Anwendungsbereich des Gesetzes.

Über die Umsetzung der Richtlinie (EU) 2016/680 hinaus enthält das Gesetz aber auch Regelungen, die nicht unmittelbar der Umsetzung der Richtlinie dienen, wie z. B. unter welchen Voraussetzungen die Videoüberwachung in Gefangenenvorführräumen von Gerichtsgebäuden zulässig ist und eine Vorschrift, die es im Außendienst tätigen Justizbediensteten unter bestimmten Voraussetzungen erlaubt, in Gefahrensituationen Geräte mit einer Mithörfunktion zu benutzen.

Wie bereits in meinem letzten Tätigkeitsbereich ausgeführt, wurden meine Bedenken bzgl. der Videoüberwachung inhaftierter Personen, die wegen einer Verhandlung vom Gefangenentransporter der Justizvollzugsanstalt in die Vorführzelle des Gerichts, von dort zum Gerichtssaal und wieder zurückgebracht werden müssen, teilweise bereits im überarbeiteten Entwurf des Landesdatenschutzgesetzes für Justiz- und Bußgeldbehörden vom Juli 2018 berücksichtigt.

Zum Zeitpunkt des letzten Tätigkeitsberichts war mir dagegen noch nicht bekannt, dass auch meiner Forderung nachgekommen wurde, den im Entwurf vorgesehenen Hinweis auf den Einsatz von Videotechnik richtlinienkonform zu konkretisieren. In § 5 Absatz 6 LDSG-JB wird nun dementsprechend ausdrücklich auf die §§ 55 und 56 des Bundesdatenschutzgesetzes verwiesen, in denen die in der Richtlinie (EU) 2016/680 genannten Informations- und Benachrichtigungspflichten umgesetzt worden sind.

Gegen die im Entwurf des Gesetzes vorgesehene Rechtsgrundlage für den Einsatz einer Mithörfunktion bei mobilen Alarmgeräten, die es im Außendienst tätigen Justizbediensteten (z. B. Gerichtsvollziehern) erlauben sollte, in Gefahrensituationen zu ihrem Schutz mittels geeigneter Geräte heimlich Tonaufnahmen zu fertigen, hatte ich ebenfalls massive Bedenken geäußert (vgl. 34. Tätigkeitsbericht, 5.1.1).

Leider ist die Regelung nicht ersatzlos gestrichen worden. Im Vergleich zur Entwurfsfassung sind die Zulässigkeitsvoraussetzungen für die Anfertigung von heimlichen Tonaufnahmen im nun geltenden § 6 LDSG-JB jedoch erheblich verschärft worden.

Während im Ausgangsentwurf vorgesehen war, dass bei Vorliegen einer nicht näher konkretisierten Gefahr zum Schutz des Justizbediensteten verdeckte Tonaufnahmen am Einsatzort angefertigt und an eine Leitstelle übermittelt werden können, regelt § 6 LDSG-JB, dass Justizbedienstete nur bei einer dringenden Gefahr für Leben, Gesundheit oder Freiheit ausschließlich zu ihrem Schutz Tonaufnahmen am Einsatzort fertigen und an eine Leitstelle übermitteln können. Die Maßnahme darf – anders als im Ausgangsentwurf vorgesehen – jedoch nur dann verdeckt durchgeführt werden, wenn Anhaltspunkte dafür bestehen, dass der Zweck der Maßnahme gefährdet wäre, wenn die betroffene Person bei Beginn oder im Verlauf der Maßnahme darüber informiert würde.

Änderung des Justizvollzugsgesetzbuchs

Der Justizvollzug erfolgt zu Zwecken der Strafvollstreckung und/oder zum Schutz vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Damit dient er Zwecken, auf die die Richtlinie (EU) 2016/680 Anwendung findet. Vor allem um diese im Justizvollzug umzusetzen, war eine Änderung des Justizvollzugsgesetzbuchs erforderlich. Manchmal verarbeitet eine Justizvollzugsanstalt aber auch zu anderen Zwecken personenbezogene Daten. In diesen seltenen Fällen findet die Datenschutz-Grundverordnung Anwendung, weshalb das Justizvollzugsgesetzbuch auch an die Datenschutz-Grundverordnung anzupassen war.

Die Änderung des Justizvollzugsgesetzbuchs ist ebenfalls – wie auch das Landesdatenschutzgesetz für Justiz- und Bußgeldbehörden – am 6. Juni 2019 in Kraft getreten.

Da sowohl das Landesdatenschutzgesetz für Justiz- und Bußgeldbehörden als auch die Änderung des Justizvollzugsgesetzbuchs erst seit wenigen Monaten gelten, kann – aufgrund der wenigen Erfahrungen, die bislang mit diesen Gesetzen vorliegen – noch keine Aussage darüber getroffen werden, ob sich die vorgenommene Umsetzung der Richtlinie (EU) 2016/680 bzw. die Anpassung an die Datenschutz-Grundverordnung in der Praxis bewähren oder, ob bzw. in welchen Punkten weiterer Änderungsbedarf besteht.



LfDI BW - 35. Tätigkeitsbericht 2019 - 5. Justiz

6. Kommunales

6.1 Die „Liste der Auffälligen“

Durch entsprechende Presseberichterstattung wurden wir darauf aufmerksam, dass die Stadt Tübingen „kreative“ Wege im Umgang mit Migranten geht. Diese werden nämlich, sofern der Stadt zu Ohren kommt, dass Personen aus dieser Gruppe mit dem Gesetz in Konflikt kommen, in einer sogenannten „Liste der Auffälligen“ erfasst und gespeichert. Wer auf der Liste steht, muss damit rechnen, häufiger die Unterkunft wechseln zu müssen und bei Behördenkontakten unter besonderer Beobachtung zu stehen.

Um prüfen zu können, ob diese besondere Form der Datenverarbeitung die datenschutzrechtlichen Voraussetzungen erfüllt, wandten wir uns mit einem detaillierten Fragenkatalog an die Stadt. Deren Stellungnahme war alles andere als befriedigend. Nicht nur wurden zum Teil falsche Rechtsgrundlagen angegeben. Soweit zutreffend auf die Vorschrift des Landesdatenschutzgesetzes (LDSG) betreffend die Datenverarbeitung zu anderen Zwecken (§ 5 LDSG) verwiesen wurde, wurde diese falsch wiedergegeben und hinsichtlich ihrer Anwendungsvoraussetzungen unzutreffend bewertet. Was die Sachverhalte angeht, die zur Aufnahme in die Liste führen, blieb unklar, was die Stadt etwa unter „Gefährderanzeigen“ oder „Vorfällen mit Gefährdungspotenzial“ genau versteht. Auf die Frage, woher die Daten stammen, hieß es: „Es handelt sich ausschließlich um Informationen, die der Verwaltung vorliegen“. An einer Stelle wurde angegeben, dass eine Weitergabe der Informationen aus der Liste nicht erfolge, an anderer Stelle heißt es, dass das Integrationsmanagement in den Unterkünften informiert werde. Zur Frage, ob die Betroffenen über

ihre Datenschutzrechte informiert worden seien, verwies die Stadt auf angebliche Einschränkungen des Auskunftsrechts „nach Art. 15, Absatz 1 lit. c) und e) [DS-GVO]“, die es so überhaupt nicht gibt. Eine nach Artikel 35 Absatz 3 Buchstabe b der Datenschutz-Grundverordnung (DS-GVO) vor der Erstellung der Datei zwingend erforderliche Datenschutz-Folgenabschätzung wurde erst noch in Aussicht gestellt. Der angeblich vorhandene Eintrag in das Verzeichnis der Verarbeitungstätigkeiten wurde uns trotz Aufforderung bis heute nicht vorgelegt.

In einem erneuten Schreiben baten wir die Stadt, sich auf eine Rechtsgrundlage festzulegen und das Vorliegen deren Voraussetzungen nachzuweisen. Aus unserer Sicht kam allenfalls § 5 Absatz 1 Nummer 2 2. Alternative LDSG in Betracht, wonach personenbezogene Daten, die zu einem bestimmten Verwaltungszweck erhoben wurden, abweichend hiervon auch genutzt werden dürfen, wenn dies „zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte und Freiheiten einer anderen Person erforderlich ist“. Die Stadt machte geltend, die in der Liste erfassten Migranten stellten eine Gefahr für die Beschäftigten der Stadt dar. Unsere Frage ging dahin, ob es konkrete Anhaltspunkte dafür gebe, dass die gelisteten Personen gegenüber städtischen Bediensteten jemals auffällig geworden seien. In ihrer Antwort ging die Stadt hierauf nicht ein und verwies lediglich auf statistische Erhebungen über die Rückfallwahrscheinlichkeit bei Gewaltdelikten. Auf unsere sonstigen Fragen wurde dagegen nicht mehr eingegangen. Nachdem wir das gegenüber dem Oberbürgermeister monierten und auf die gesetzliche Pflicht der Stadt hingewiesen hatten, uns in unserer Arbeit zu unterstützen, erhielten wir überraschend nachrichtlich ein Schreiben des Oberbürgermeisters

LfDI BW - 35. Tätigkeitsbericht 2019 - 6. Kommunales

an den Innenminister des Landes, in dem er sich wortreich über uns beschwerte: Wir würden immer nur weitere Fragen stellen, für die Fachleute in seinem Haus sei nicht mehr erkennbar, welche Antworten wir erwarteten, was wir wollten, sei rechtlich nicht zulässig und vom Aufwand nicht zu leisten. Uns wurde unterstellt, indem wir das Vorgehen der Stadt im Hinblick auf die Beachtung datenschutzrechtlicher Vorschriften prüfen und damit unserem gesetzlichen Auftrag nachkommen, würden wir städtische Mitarbeiter gefährden.

Dies ist absurd. Zutreffend ist vielmehr, dass wir bis heute wegen des unkooperativen Verhaltens der Stadt nicht in der Lage sind, konkret festzustellen, ob das, was dort vor sich geht, legal ist, oder der Stadt eventuell beratend zur Seite zu stehen, um eine rechtmäßige Datenverarbeitung möglich zu machen.

Die Verweigerungshaltung der Stadt ist nicht nur unverständlich, sie gibt uns auch Anlass, weitere Maßnahmen zu ergreifen, die uns nach der Datenschutz-Grundverordnung zu Gebote stehen. Die Sache bedarf einer Klärung.

6.2 Kommunales Netzwerk Datenschutz

Sein zehnjähriges Bestehen feierte das Kommunale Netzwerk Datenschutz an der Verwaltungshochschule Kehl. Das Netzwerk ist ein landesweiter Zusammenschluss kommunaler behördlicher Datenschutzbeauftragter, die sich schon seit 2009 zweimal jährlich zu einer Konferenz in der Hochschule treffen.

Waren es anfangs nur etwa 20 Personen, sind es jetzt schon mehr als 120 Mitglieder. Sie kommen sowohl aus kleineren Gemein-

den wie auch aus großen Städten, Landratsämtern und selbstständigen Behörden wie beispielsweise einer Hafenverwaltung. Obwohl Experten im Datenschutz haben sie immer wieder neue Datenschutzprobleme und Fragen. Diese erörtern sie zunächst im Fachkreis gemeinsam, versuchen diese zu lösen, bevor sie sich an den LfDI wenden. „Alte Hasen“ mit jahrelanger Praxiserfahrung können so Neueinsteigern helfen und den Einstieg in die schwierige Materie erleichtern.

Zwar gibt es Arbeitsgemeinschaften auch bei den kommunalen Spitzenverbänden. Aber übergreifend treffen sich Praktikerrinnen und Praktiker nur in diesem Kehler Netzwerk. Gerade der Erfahrungsaustausch unabhängig von der Größe der Behörde ist dabei sehr gewinnbringend. Ein solches Netzwerk kann auch als Vorbild für andere Organisationen und Zusammenschlüsse (Vereine, Schulen) dienen.

Wichtiges Element der Netzwerkarbeit ist der durch die Konferenzen entstehende persönliche Kontakt. So tauschen sich die Mitglieder permanent über ein Intranet-Portal des Netzwerkes aus. Auf diesem werden speziell Informationen für kommunale Datenschutzbeauftragte in Baden-Württemberg bereitgehalten. Die Unterlagen kommen von den Mitgliedern und können von diesen selbst hochgeladen werden.

Der LfDI unterstützt nach besten Kräften die Arbeit dieses Netzwerkes. Er gibt die Möglichkeit, ausgewählte Fragen, die im Kreise der Konferenzteilnehmer nicht beantwortet werden konnten, beim LfDI einzureichen. Soweit es dem LfDI möglich war, sandte seine Behörde auch Referentinnen und Referenten zu den Tagungen.

LfDI BW - 35. Tätigkeitsbericht 2019 - 6. Kommunales

Träger des Netzwerkes ist die Kehler Akademie e. V., eine der beiden Fort- und Weiterbildungseinrichtungen der Hochschule Kehl.



LfDI BW - 35. Tätigkeitsbericht 2019 - 6. Kommunales

7. Gesundheit und Soziales

7.1 Vorsicht beim Versand von E-Mails

Neben der rechtlichen Frage, ob E-Mails mit personenbezogenen Daten – wenn die betroffene Person hierin eingewilligt hat – unverschlüsselt versandt werden dürfen, ist darauf zu achten, dass beim Versand von E-Mails besondere Sorgfalt aufgebracht wird.

Meine Dienststelle hatte sich im Berichtszeitraum mit mehreren Beschwerden im Zusammenhang mit dem Versand von E-Mails durch Sozialleistungsträger zu befassen.

In einem Fall hatte ein Jobcenter ausnahmsweise – auf ausdrücklichen Wunsch eines Leistungsbeziehers aufgrund der Dringlichkeit seiner Angelegenheit – einen Bescheid per (unverschlüsselter) E-Mail an den Leistungsbezieher senden wollen. Aufgrund dessen, dass E-Mail-Adressen häufig unterstrichen dargestellt werden, wurde von der Mitarbeiterin des Jobcenters ein Unterstrich in der E-Mail-Adresse nicht erkannt und die E-Mail-Adresse dadurch falsch geschrieben. Diese „falsche“ E-Mail-Adresse existierte, sodass ein (unbekannter) Namensvetter des Leistungsbeziehers die E-Mail samt Bescheid erhielt. Die betroffene Behörde hat den Sachverhalt zum Anlass genommen, eine Dienstanweisung „Datenschutz“ zu erlassen und die Mitarbeitenden zum Thema „E-Mailing“ zu informieren, um das Bewusstsein für den Datenschutz zu schärfen.

In einem weiteren Fall hatte ein Mitarbeiter eines Jugendamts per E-Mail über einen Zuständigkeitswechsel innerhalb seiner Dienststelle informiert. Leider schrieb er alle Empfänger „offen“ an, anstatt diese

in „Bcc“ zu setzen. So konnten alle Empfänger erkennen, wer noch die E-Mail erhalten hatte und damit auch, wer Kontakt zum Jugendamt hat.

Auch hier hat die betroffene Behörde in der Folge die Mitarbeitenden bezüglich der Thematik sensibilisiert.

In einem dritten Fall ging es darum, dass ein Jugendamt eine Nachricht per E-Mail an einen Elternteil und nachrichtlich an einen vom Jugendamt beauftragten Jugendhilfeträger versandt hatte. So wurde dem beauftragten Jugendhilfeträger die E-Mail-Adresse des Elternteils bekannt – hierin hatte der Elternteil nicht eingewilligt.

So schnell und einfach eine E-Mail versandt ist, birgt diese Unkompliziertheit auch gewisse Risiken. Daher ist beim Versand von E-Mails Sorgfalt angebracht. Durch Verschlüsselung von E-Mails kann, wie z. B. im Fall des Jobcenters, verhindert werden, dass Dritten sensible Sachverhalte bekannt werden.

7.2 Datenschutz in der ambulanten und stationären Pflege

Häusliche Krankenpflege

Im Berichtszeitraum waren wir mit der Frage befasst, inwieweit im Rahmen der häuslichen Krankenpflege zur Abrechnung einer aufwändigen Wundversorgung sensible Gesundheitsdaten wie Fotos der zu versorgenden Wunde an die Krankenkasse übermittelt werden dürfen. Ferner war zu klären, ob diese Daten allein von sog. „Wundmanagern“ der Krankenkasse ausgewertet werden dürfen, ohne den Medizinischen Dienst der Krankenkassen (MDK) einzuschalten.

LfDI BW - 35. Tätigkeitsbericht 2019 - 7. Gesundheit und Soziales

Die häusliche Krankenpflege nach § 37 des Fünften Buches Sozialgesetzbuch (SGB V) umfasst die im Einzelfall erforderliche Grundpflege, Behandlungspflege und hauswirtschaftliche Versorgung. Auf ärztliche Verordnung wird u. a. die Wundversorgung als Behandlungspflege durch einen ambulanten Pflegedienst durchgeführt. Der Pflegedienst rechnet die erbrachten Leistungen anschließend im Rahmen der vertraglichen Vereinbarungen mit der Krankenkasse des Patienten ab.

Bei der Wundversorgung ist allerdings zwischen einer regulären Versorgung zu unterscheiden, die einen durchschnittlich hohen Aufwand erfordert, und einer aufwändigen Versorgung, die einen zeitintensiven Aufwand erfordert. Für eine sog. „aufwändige Wundversorgung“ sehen die vertraglichen Vereinbarungen mit der Krankenkasse eine höhere Vergütung vor. Dementsprechend erfordert die Abrechnung dieser aufwändigeren Leistung auch einen aussagekräftigen Nachweis.

Als vertragliche Abrechnungsgrundlage für die höhere Vergütung einer aufwändigen Wundbehandlung diente bisher ein konkretes zwischen Krankenkasse und den Pflegeverbänden abgestimmtes Antragsformular. Dieses Formular sah u. a. vor, dass zu den Unterlagen eine „aussagekräftige Darstellung der aufwändigen Wundversorgung im Rahmen eines zeitgemäßen Wundmanagements“ eingereicht wird. Dies wurde von einigen ambulanten Pflegediensten so verstanden, dass sie zusammen mit dem Antragsformular bei der Krankenkasse als Nachweis einer aufwändigen Wundbehandlung zusätzlich umfangreiche Unterlagen einreichen müssten; typischerweise reichten die Pflegedienste neben Wundbefunden, Wundprotokollen auch Fotos der Wunde ein. Für die Übermittlung der „notwendigen Unter-

lagen“ sah das Antragsformular vor, dass sich der Pflegedienst von dem Versicherten eine Einwilligung einholt. Die vom Pflegedienst übersandten Unterlagen wertet die Krankenkasse dann im Normalfall mithilfe von bei ihr angestellten, speziell ausgebildeten, sog. „Wundmanagern“ aus. Eine Weiterleitung an den Medizinischen Dienst der Krankenversicherung (MDK) findet nur ausnahmsweise statt.

In diesem Zusammenhang stellte uns ein Träger der ambulanten Pflege die Frage, ob dieses Verfahren datenschutzrechtlich zulässig sei.

Wir erörterten das Verfahren daraufhin mit der betreffenden Krankenkasse. Unsere Prüfung führte zu den folgenden wesentlichen datenschutzrechtlichen Erwägungen: Zweifelhaft ist, ob die in Rede stehende Erhebung von Sozialdaten überhaupt in Form einer Einwilligungserklärung gerechtfertigt werden kann. Die Vorschriften des § 284 SGB V regeln abschließend, in welchen Fällen die Krankenkasse berechtigt ist, Sozialdaten zu erheben. Eine darüber hinausgehende Datenverarbeitung auf der Grundlage einer Einwilligung ist demgegenüber – was der nationale Gesetzgeber gemäß Artikel 9 Absatz 2 Buchstabe a) und Absatz 4 der Datenschutz-Grundverordnung (DS-GVO) bei besonderen Kategorien personenbezogener Daten, insbesondere bei Gesundheitsdaten bestimmen kann – ausgeschlossen. Allerdings erlauben die Bestimmungen in § 284 Absatz 1 Satz 1 Nummer 4 und Nummer 8 SGB V die Erhebung von Sozialdaten insoweit, als dies zur Prüfung der Leistungspflicht der Krankenkasse bzw. zur Abrechnung mit den Leistungserbringern erforderlich ist. Im Fall der Abrechnung einer aufwändigen Wundversorgung benötigt die Krankenkasse die zusätzlichen Daten, um festzustellen, ob statt einer regulären tatsächlich eine aufwändige Wundversorgung

LfDI BW - 35. Tätigkeitsbericht 2019 - 7. Gesundheit und Soziales

erforderlich war und durchgeführt wurde mit der Folge, dass sie dem Pflegedienst gegenüber hierfür zur Zahlung einer entsprechend höheren Vergütung verpflichtet wäre. Die Pflicht zur Kostenerstattung ergibt sich in der Regel aus Anspruchsvoraussetzungen, die dem Grunde und der Höhe nach vorliegen müssen. Die Frage, in welcher Höhe die Krankenkasse zur Zahlung eines Zuschlags verpflichtet ist, ist daher von den Befugnisnormen des § 284 Absatz 1 Satz 1 Nummer 4 und Nummer 8 SGB V umfasst, die die Vorschriften der Datenschutz-Grundverordnung als spezifische mitgliedstaatliche Bestimmungen gemäß Artikel 6 Absatz 1 Buchstabe e) und Absatz 3 Satz 3 DS-GVO sowie gemäß Artikel 9 Absatz 2 Buchstabe h) und Absatz 4 DS-GVO konkretisieren.

Des Weiteren stellten wir gegenüber der Krankenkasse bezüglich des Umfangs der erhobenen Daten klar, dass die Erhebung von rein medizinischen Daten zur Feststellung, ob eine aufwändige Wundversorgung vorliegt, jedenfalls nicht mit dem Erlaubnistatbestand des § 284 Absatz 1 Nummer 4 und Nummer 8 SGB V gerechtfertigt werden könne.

Im Laufe unserer Prüfung ergab sich, dass die Krankenkasse, wenn ein Antrag auf Feststellung einer aufwändigen Wundversorgung gestellt wird, zu dessen Glaubhaftmachung ausschließlich pflegerische Informationen zur Wundversorgung erwarten würde. Diese seien Angaben wie die Anzahl und Ausdehnung der Wunden, der Zeitaufwand für den Wundverbandswechsel, die Reinigung und Desinfektion sowie die Durchführung des Wundverbands. Keinesfalls würde sie medizinische Informationen von dem Pflegedienst benötigen, die im Rahmen der häuslichen Krankenpflege nur vom verordnenden Arzt bzw. in schwierigen Fällen vom MDK zu beurteilen seien.

Aufgrund dessen hatten wir der Krankenkasse aufgegeben, in dem verwendeten Antragsformular klarzustellen, dass sie als weitere Angaben lediglich die pflegerischen Aspekte der Wundversorgung zur Leistungsbeurteilung benötigt, nicht hingegen weitere aussagekräftige Unterlagen über medizinische Aspekte. Außerdem teilten wir der Krankenkasse unsere Auffassung mit, dass sie diese weiteren Angaben nicht auf Basis einer Einwilligung, sondern auf der Grundlage der §§ 284 Absatz 1 Nummer 4 und Nummer 8 SGB V i.V.m. Artikel 6 Absatz 1 Buchstabe e), Absatz 3 Satz 3, Artikel 9 Absatz 2 Buchstabe h), Absatz 4 DS-GVO erheben könne.

Die Krankenkasse hat auf unsere Hinweise das Antragsformular, das Gegenstand ihrer Verträge mit den Pflegeverbänden war, in Abstimmung mit ihren Vertragspartnern geändert.

Auf dem Formular kommt nunmehr insbesondere – was wir ausdrücklich begrüßen – klar zum Ausdruck, dass:

- die Krankenkasse zur Prüfung, ob eine aufwändige Wundversorgung erforderlich ist, keine zusätzlichen Unterlagen in Form von Wundprotokollen oder gar Fotos von der Wunde benötigt und dass
- die Krankenkasse unter „aussagekräftige Darstellung der aufwändigen Wundversorgung im Rahmen eines zeitgemäßen Wundmanagements“ Angaben zur Anzahl der Wunden, deren Ausdehnung, den Zeitaufwand sowie pflegerische Aspekte wie Reinigung, Desinfektion sowie die Durchführung des Wundverbands erwartet.

Allerdings ist entgegen der Ankündigung der Krankenkasse auf dem uns vorgelegten angepassten Formular noch immer die Einholung einer Einwilligungserklärung vorgesehen. Dies wird Gegenstand

LfDI BW - 35. Tätigkeitsbericht 2019 - 7. Gesundheit und Soziales

weiterer Erörterung mit der Krankenkasse sein.

Das Verfahren der Krankenkasse, dass grundsätzlich bei ihr angestellte sog. „Wundmanager*innen“ prüfen, ob dem Pflegedienst eine höhere Vergütung für eine aufwändige Wundversorgung zusteht und nur im Ausnahmefall der MDK mit einer Begutachtung beauftragt wird, gab übrigens keinen Anlass zur Kritik: Eine Krankenkasse ist nach § 275 Absatz 1 SGB V zwar verpflichtet, in bestimmten Fällen eine gutachtliche Stellungnahme des MDK einzuholen. Allerdings ergibt sich hieraus nicht, dass sie im Rahmen der Prüfung der Frage, ob eine aufwändige Wundversorgung erforderlich ist, stets eine solche gutachtliche Stellungnahme in Auftrag geben müsste. Die Krankenkasse hat vielmehr einen Beurteilungsspielraum, der es ihr erlaubt, die Beteiligung des MDK auf die Ausnahmefälle zu beschränken, in denen es sich um schwierige medizinische Fragestellungen handelt, und die Prüfung in einfach gelagerten Fällen selbst vorzunehmen.

Anforderung von Personallisten durch die Heimaufsichtsbehörden

Ein Verband, der auch die Interessen von Pflegeeinrichtungen vertritt, hat uns im Berichtszeitraum gebeten, die Praxis der baden-württembergischen Heimaufsichtsbehörden zu überprüfen, wonach diese von den stationären Pflegeeinrichtungen im Rahmen ihrer Prüftätigkeit Listen von den dort beschäftigten Pflegekräften mit deren Klarnamen und Qualifikation anfordern. Fraglich war in diesem Zusammenhang auch, ob die Heimaufsichtsbehörden diese Art von Personallisten nicht nur im Rahmen der jährlichen oder anlassbezogenen Qualitätsprüfungen, sondern auch im Rahmen der halbjährlich stattfindenden sog. Änderungsanzeigen anfordern dürfen.

Die Heimaufsichtsbehörden haben nach der Vorschrift des § 10 des baden-württembergischen Wohn-, Teilhabe- und Pflegegesetz (WTPG) u. a. die Aufgabe, die persönliche und fachliche Eignung der in einer stationären Pflegeeinrichtung Beschäftigten zu überprüfen. Um eine stationäre Pflegeeinrichtung betreiben zu dürfen, muss der Träger der Einrichtung sicherstellen, dass die Zahl der Beschäftigten und ihre persönliche und fachliche Eignung für die von ihnen zu leistende Tätigkeit ausreicht (vgl. § 10 Absatz 3 Nummer 3 WTPG). Sofern dies nicht sichergestellt ist, haben die Heimaufsichtsbehörden den gesetzlichen Auftrag, geeignete Maßnahmen nach dem Wohn-, Teilhabe- und Pflegegesetz zu ergreifen, so z. B. ein Beschäftigungsverbot auszusprechen.

Das für die Heimaufsichtsbehörden zuständige Ministerium für Soziales und Integration legte uns gegenüber schlüssig und überzeugend dar, dass für die Aufgabenerfüllung der Heimaufsichtsbehörden Personallisten erforderlich seien, die nicht nur die Initialen der Beschäftigten, sondern die Klarnamen sowie die Qualifikation der Beschäftigten enthalten. Die Heimaufsichtsbehörden müssten bei der Überprüfung, ob eine stationäre Einrichtung die Vorgaben des Wohn-, Teilhabe- und Pflegegesetz erfüllt, auch die Vorschrift des § 4 Absatz 1 der Landespersonalverordnung einbeziehen. Danach dürfen bei Personen, die in einer stationären Einrichtung beschäftigt sind, keine Tatsachen vorliegen, die die Annahme rechtfertigen, dass sie für die von ihnen ausgeübten Tätigkeiten persönlich ungeeignet sind. Ungeeignet ist insbesondere, wer wegen (in der Landespersonalverordnung näher umschriebener) Straftaten rechtskräftig verurteilt worden ist.

LfDI BW - 35. Tätigkeitsbericht 2019 - 7. Gesundheit und Soziales

Die Heimaufsichtsbehörden erhalten über die sog. Mitteilungen in Strafsachen der Gerichte oder Staatsanwaltschaften Kenntnis über strafrechtliche Verurteilungen, die die persönliche Eignung der Beschäftigten einer stationären Einrichtung in Frage stellen (vgl. § 13 Absatz 2 Satz 1, § 14 Absatz 1 Nummer 5 des Einführungsgesetzes zum Gerichtsverfassungsgesetz und Nummer 28 der Anordnung des Bundesministeriums der Justiz und für Verbraucherschutz und der Landesjustizverwaltungen über die Mitteilungen in Strafsachen vom 27. März 2019) ausschließt. Diese Mitteilungen gleichen die Heimaufsichtsbehörden sodann mit den vorliegenden Personallisten ab und ergreifen dann erforderlichenfalls die notwendigen Maßnahmen. Lägen den Heimaufsichtsbehörden indes keine Personallisten der einzelnen Einrichtungen mit Klarnamen vor, so wäre eine Zuordnung der Mitteilungen zu den einzelnen Personen bzw. Einrichtungen nicht möglich. Uns gegenüber wurde überdies plausibel dargestellt, dass den Heimaufsichtsbehörden ein gleich geeignetes und milderer Mittel, um den Überwachungspflichten aus dem Wohn-, Teilhabe- und Pflegegesetz nachzukommen, nicht zur Verfügung steht.

Bislang war ebenfalls die Frage strittig, ob die baden-württembergischen Heimaufsichtsbehörden berechtigt sind, die Personallisten von den Einrichtungen nicht nur im Rahmen der jährlichen oder anlassbezogenen Qualitätsprüfung nach § 17 WTPG anzufordern, sondern auch im Rahmen der Änderungsanzeigen nach § 11 Absatz 3 WTPG, die das Ministerium für Soziales und Integration laut seiner Orientierungshilfe für die Heimaufsichtsbehörden in Baden-Württemberg zumindest halbjährlich erwartet. Diesbezüglich verständigte sich das Ministerium für Soziales und Integration mit den Heimaufsichtsbehörden darauf, dass diese im Rahmen der Änderungsan-

zeigen nach § 11 Absatz 3 WTPG vorerst – das heißt jedenfalls bis zu einer ggf. entsprechenden gesetzlichen Klarstellung im Wohn-, Teilhabe- und Pflegegesetz – keine Personallisten mit Namen und Qualifikation der Beschäftigten anfordern würden.

7.3 Die Informationspflicht im Fall der Erhebung personenbezogener Daten bei der betroffenen Person durch Sozialleistungsträger: Die Neuerungen der DS-GVO

Die datenschutzrechtlichen Informationspflichten bilden die Grundlage für die Ausübung der Betroffenenrechte (insbesondere der Artikel 15 ff. der Datenschutz-Grundverordnung [DS-GVO]). Nur wenn die betroffene Person weiß, dass personenbezogene Daten über sie verarbeitet werden, kann sie diese Rechte auch ausüben. Oder wie es der Erwägungsgrund 60 zur Datenschutz-Grundverordnung formuliert: Die Grundsätze einer fairen und transparenten Verarbeitung machen es erforderlich, dass die betroffene Person über die Existenz des Verarbeitungsvorgangs und seiner Zwecke unterrichtet wird. Im Bereich des Sozialrechts zählen darüber hinaus Aufklärung, Beratung und Auskunft ohnehin zu den Grundpflichten der Leistungsträger (vgl. §§ 13–15 des Ersten Buchs des Sozialgesetzbuchs [SGB I]). Der Erfüllung der datenschutzrechtlichen Informationspflichten durch Sozialleistungsträger kommt daher eine wichtige Bedeutung zu.

Schon vor Geltung der Datenschutz-Grundverordnung gab es Informationspflichten der Sozialleistungsträger: Früher war es jedoch ausreichend, wenn sie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung, die Identität der verantwortlichen Stelle und ggf. über Kate-

LfDI BW - 35. Tätigkeitsbericht 2019 - 7. Gesundheit und Soziales

gorien von Empfängern unterrichtet; ansonsten war nur noch darauf hinzuweisen, ob der Betroffene zur Auskunft verpflichtet, die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen oder die Angabe freiwillig ist (vgl. § 67a Absatz 3 des Zehnten Buchs des Sozialgesetzbuchs [SGB X] in der bis zum 24. Mai 2018 geltenden Fassung). Die in der Datenschutz-Grundverordnung geregelten Informationspflichten gehen wesentlich über die bisherige Rechtslage hinaus.

Mit Artikel 23 DS-GVO wurde in der Datenschutz-Grundverordnung allerdings auch die Möglichkeit eröffnet, durch Gesetzgebungsmaßnahmen – in gewissem Umfang – Beschränkungen der Informationspflichten vorzunehmen. Von dieser Möglichkeit hat der Bundesgesetzgeber für den Bereich des Sozialdatenschutzes Gebrauch gemacht, nämlich mit den Regelungen des § 82 SGB X in Bezug auf die Informationspflicht im Fall der Erhebung von personenbezogenen Daten bei der betroffenen Person (Artikel 13 DS-GVO) und mit § 82a SGB X in Bezug auf die Informationspflicht in dem Fall, dass die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden (Artikel 14 DS-GVO).

Nicht nur die Sozialleistungsträger hatten sich mit den dargestellten gesetzlichen Neuerungen zu befassen, auch für meine Dienststelle war im Bereich des Sozialdatenschutzes die Thematik der Informationspflichten (insbesondere im Fall der Erhebung von personenbezogenen Daten bei der betroffenen Person [Artikel 13 DS-GVO]) seit Geltung der Datenschutz-Grundverordnung ein Schwerpunkt:

So hatte meine Dienststelle mehrere Beschwerden betreffend die Erfüllung der Informationspflicht zu bearbeiten. Das The-

ma wird also durchaus in der Öffentlichkeit wahrgenommen. Bei den Beschwerden ging es in erster Linie darum, dass der Verantwortliche noch gar keine Informationen erstellt hatte.

Darüber hinaus war die Thematik einer der Schwerpunkte bei zwei von meiner Dienststelle durchgeführten Kontrollen bei einem Sozialamt und bei einem Versorgungsamt.

Die Befassung mit den Informationspflichten zeigte, dass die Erstellung korrekter und gleichzeitig für die betroffene Person verständlicher Informationen nicht ganz einfach ist.

Aufgrund der gewonnenen Erkenntnisse hat meine Dienststelle daher den Beitrag „Besonderheiten zur Informationspflicht nach Artikel 13 der Datenschutz-Grundverordnung für Sozialleistungsträger“ erstellt, um den Verantwortlichen die Erstellung der Informationen etwas zu erleichtern. Der Beitrag ist auf der [Internetseite](#) meiner Dienststelle abrufbar.

Auf einige Einzelheiten der Informationspflicht nach Artikel 13 DS-GVO soll im Folgenden kurz eingegangen werden:

Artikel 13 Absatz 1 Buchstabe a DS-GVO: Mitteilung des Namens und der Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters

Beim Verantwortlichen handelt es sich nicht um den (gesamten) Stadt- oder Landkreis oder – wie teilweise in den von mir überprüften Informationen ausgeführt wurde – um den (behördlichen) Datenschutzbeauftragten. Wer Verantwortlicher ist, ist zunächst in Artikel 4 Nr. 7 DS-GVO gesetzlich definiert. Für den Bereich des Sozialdatenschutzes gibt es außerdem

LfDI BW - 35. Tätigkeitsbericht 2019 - 7. Gesundheit und Soziales

eine Spezialvorschrift in § 67 Absatz 4 SGB X: Danach ist bei der Verarbeitung von Sozialdaten durch einen Leistungsträger Verantwortlicher der Leistungsträger (vgl. § 67 Absatz 4 Satz 1 SGB X). Wichtig ist hierzu die Regelung des § 67 Absatz 4 Satz 2 SGB X:

„Ist der Leistungsträger eine Gebietskörperschaft, so sind der Verantwortliche die Organisationseinheiten, die eine Aufgabe nach einem der besonderen Teile dieses Gesetzbuchs funktional durchführen.“

Dies kann beispielsweise das Jobcenter (für den Bereich des Zweiten Buchs des Sozialgesetzbuchs) oder die Wohngeldstelle (für den Bereich des Wohngeldgesetzes) sein.

Mit dem nach Artikel 13 Absatz 1 Buchstabe a DS-GVO anzugebenden Vertreter ist im Übrigen nicht etwa der Leiter des Jobcenters oder der Leiter der Wohngeldstelle gemeint, sondern der Vertreter im Sinne von Artikel 4 Nr. 17 DS-GVO. Dies ist eine in der Union niedergelassene natürliche oder juristische Person, die gemäß Artikel 27 DS-GVO bestellt wurde. Artikel 27 DS-GVO sieht vor, dass ein nicht in der Union niedergelassener Verantwortlicher oder Auftragsverarbeiter ggf. einen Vertreter in der Union als Ansprechpartner benennt. Diese Regelung dürfte daher bei der Verarbeitung von Sozialdaten durch öffentliche Stellen keine Bedeutung haben.

Artikel 13 Absatz 1 Buchstabe c DS-GVO: Mitteilung der Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie der Rechtsgrundlage für die Verarbeitung

Als Rechtsgrundlage für die Verarbeitung kommt bei Sozialleistungsträgern insbesondere Artikel 6 Absatz 1 Buchstabe e und Absatz 3 DS-GVO in Verbindung mit

Vorschriften des nationalen Rechts in Betracht. Bei unseren Prüfungen kam es vor, dass nur die „alt bewährten“ Regelungen im Sozialgesetzbuch genannt wurden, während die „neuen“ Vorschriften der Datenschutz-Grundverordnung „vergessen“ wurden.

Des Weiteren ist es an dieser Stelle wichtig, die Vorschriften im nationalen Recht (z. B. im SGB X) möglichst präzise anzugeben. Nun gibt es Fälle, in denen es nicht möglich ist, in verständlicher Weise alle Rechtsgrundlagen in einer Gesamtinformation anzugeben. Dann kann ausnahmsweise bei den Informationen nach Artikel 13 DS-GVO eine pauschalere Zitierweise genügen mit einem Verweis auf die Angabe der genauen Grundlagen in den Formularen, z. B. in folgender Weise:

„Die Datenverarbeitung durch das Sozialamt stützt sich insbesondere auf Artikel 6 Absatz 1 Buchstabe e und Absatz 3 DS-GVO i. V. m. §§ 67 ff. SGB X sowie auf spezialgesetzliche Regelungen. Die genauen Rechtsgrundlagen finden sich in den einzelnen Formularen.“

In den einzelnen Formularen sind dann die jeweils passenden Rechtsnormen zu benennen.

Artikel 13 Absatz 1 Buchstabe e DS-GVO: Gegebenenfalls Mitteilung der Empfänger oder der Kategorien von Empfängern personenbezogener Daten

Wer Empfänger ist, ist in Artikel 4 Nr. 9 DS-GVO gesetzlich definiert. Danach ist der Begriff des „Empfängers“ weiter als der des „Dritten“ (Artikel 4 Nr. 10 DS-GVO). Insbesondere ist auch der Auftragsverarbeiter „Empfänger“ und daher anzugeben.

LfDI BW - 35. Tätigkeitsbericht 2019 - 7. Gesundheit und Soziales

Bei dieser Information sind außerdem die (auf die Öffnungsklausel in Artikel 23 DS-GVO gestützten) Spezialregelungen in § 82 Absatz 1 SGB X zu beachten.

Artikel 13 Absatz 2 Buchstabe b und c DS-GVO

Hier wird empfohlen, immer auch den betreffenden Artikel der Datenschutz-Grundverordnung zu nennen (z. B. beim Auskunftsanspruch der betroffenen Person Artikel 15 DS-GVO), damit die betroffene Person bei Interesse selbst Genaueres nachlesen kann.

Artikel 13 Absatz 2 Buchstabe e: Mitteilung, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte

Die Regelung entspricht derjenigen des § 67a Absatz 3 Satz 3 SGB X in der bis zum 24. Mai 2018 geltenden Fassung.

Im Rahmen unserer Beratungstätigkeit wurden wir ferner auf einen besonderen Klärungsbedarf der Leistungsträger im Bereich der Kinder- und Jugendhilfe im Hinblick auf den Umfang ihrer Informationspflichten aufmerksam gemacht. Hier erschien ihnen fraglich, ob etwa § 62 Absatz 2 Satz 2 des Achten Buchs des Sozialgesetzbuchs (SGB VIII) ihre Informationspflichten abschließend regelt oder ob die weitergehende Regelung in Artikel 13 DS-GVO der nationalen Vorschrift vorgeht. Die Regelung in § 62 Absatz 2 SGB VIII lautet:

„Sozialdaten sind beim Betroffenen zu erheben. Er ist über die Rechtsgrundlage der

Erhebung sowie die Zweckbestimmungen der Erhebung und Verwendung aufzuklären, soweit diese nicht offenkundig sind.“ Die Regelung ist nicht geändert worden, obwohl das Achte Buch des Sozialgesetzbuchs seit Geltung der Datenschutz-Grundverordnung und erst recht seit ihrem Erlass bereits mehrfach Änderungen erfahren hat. Insbesondere sieht das inzwischen von Bundestag und Bundesrat beschlossene Zweite Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (in Art. 129; Gesetzentwurf: BT-Drs. 19/4674, S. 1 ff.) lediglich redaktionelle Änderungen von § 62 Absatz 2 SGB VIII vor. Demgegenüber wurde durch Artikel 24 des Gesetzes zur Änderung des Bundesversorgungsgesetzes und anderer Gesetze vom 17. Juli 2017 (BGBl. I 2541, 2558) die vor dem Inkraft-Treten des Datenschutz-Grundverordnung geltende allgemeine Bestimmung in § 67a Absatz 3 SGB X a. F. (s. zu ihr schon oben) zur Informationspflicht im Fall der Erhebung von Sozialdaten beim Betroffenen mit der Begründung (s. Beschlussempfehlung und Bericht des Ausschusses für Arbeit und Soziales, BT-Drs. 18/12611, S. 102 f.) aufgehoben, dass der dortige Regelungsgehalt künftig nach Art. 13 DS-GVO unmittelbar gelte. Diese Gesetzgebung könnte man dahingehend verstehen, dass der Gesetzgeber, indem er § 62 Absatz 2 Satz 2 SGB VIII trotz der vorgenommenen anderweitigen Änderungen jeweils aufrechterhalten hat, die Anwendung von Artikel 13 DS-GVO etwa mit Blick auf die Öffnungsklausel in Artikel 23 DS-GVO ausschließen wollte.

Insbesondere in Bezug auf die Änderungen des § 62 SGB X durch das Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz EU ist jedoch weder dem Wortlaut der geänderten Vorschrift noch der Be-

LfDI BW - 35. Tätigkeitsbericht 2019 - 7. Gesundheit und Soziales

gründung zum Gesetzentwurf (BT-Drs. 19/4674, S. 397) ein solches gesetzgeberisches Ziel, die Informationspflichten aus Artikel 13 DS-GVO einzuschränken, zu entnehmen. Vielmehr soll es sich bei den Änderungen des § 62 Absatz 2 SGB VIII der Gesetzesbegründung zufolge lediglich um eine redaktionelle Anpassung „an die Begriffsbestimmungen aus Artikel 4 der Verordnung (EU) 2016/679“ handeln. Zugleich fügt das Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz EU (durch Art. 129 Nr. 5 Buchst. a] bb]) in § 68 Absatz 1 SGB VIII ausdrücklich einen Passus ein, dem zufolge die Informationspflichten nach Artikel 13 und 14 DS-GVO im Fall der Datenerhebung durch Beistandschaft, Amtspflegschaft oder Amtsvormundschaft nur eingeschränkt gelten sollen, wobei in der Gesetzesbegründung ausdrücklich auf die Voraussetzungen der Öffnungsklausel in Art. 23 DS-GVO für diese Fallkonstellation eingegangen wird (BT-Drs. 19/4674, S. 398 f.). Hieraus lässt sich der Umkehrschluss ziehen, dass der Gesetzgeber grundsätzlich auch im Bereich des Achten Buch des Sozialgesetzbuchs von der Geltung der Informationspflichten der Datenschutz-Grundverordnung ausgeht. Ohnehin bestünden Zweifel, dass ein allgemeiner Ausschluss der Informationspflicht nach Artikel 13 DS-GVO durch die aktuelle Fassung von § 62 Absatz 2 Satz 2 SGB VIII den Anforderungen des Artikel 23 DS-GVO an eine zulässige Beschränkung entsprechen würde, sodass auch deswegen nicht von einem entsprechenden Willen des Gesetzgebers ausgegangen werden kann.

Der Erfüllung der datenschutzrechtlichen Informationspflichten kommt im Bereich des Sozialrechts eine wichtige Bedeutung zu. Die Frage ausreichender datenschutzrechtlicher Information ist hier durchaus Gegenstand öffentlicher Wahrnehmung. Die in der Datenschutz-Grundverordnung

geregelten Informationspflichten der Sozialleistungsträger gehen dabei wesentlich über die Anforderungen der früheren Rechtslage hinaus. Dadurch ist die Erstellung korrekter und gleichzeitig für die betroffene Person verständlicher Informationen nicht ganz einfach. Auch ist die Konkurrenz von Vorschriften des Sozialgesetzbuchs mit den Regelungen der Datenschutz-Grundverordnung zuweilen schwer zu lösen. Besonders wichtig ist aus meiner Sicht in jedem Fall eine möglichst präzise Angabe der Rechtsgrundlage für die Datenverarbeitung, damit der Betroffene wenigstens im Ansatz nachvollziehen kann, ob die Datenverarbeitung durch den Sozialleistungsträger rechtmäßig ist.



LfDI BW - 35. Tätigkeitsbericht 2019 - 7. Gesundheit und Soziales

8. Schule und Hochschulen

8.1 Nutzungsordnung für die Informationstechnik an einer Schule

Fernmeldegeheimnis contra Schulrecht. Darf eine Schule speichern, welcher Schüler welche Internet-Seite besucht hat? Um hier Fallstricken zu entgehen, sollte sich jede Schule um dieses Thema kümmern.

Eine Anfrage erreichte mich, ob eine Schule speichern dürfe, welche Schülerin oder welcher Schüler welche Internet-Seite besucht hat, ob also die die Internetnutzung betreffenden Verkehrsdaten (auch „Verbindungsdaten“ genannt) gespeichert werden dürfen.

Wenn eine Schule im Sinne des Telekommunikationsgesetzes (TKG) Diensteanbieter ist, so muss sie nach § 88 TKG das Fernmeldegeheimnis gemäß Artikel 10 Absatz 1 des Grundgesetzes wahren. Dabei ist zu beachten, dass eine Verletzung des Fernmeldegeheimnisses gemäß § 206 des Strafgesetzbuchs (in den dort näher umschriebenen Begehungsformen) mit einer Freiheitsstrafe bis zu 5 Jahren bestraft werden kann. Dem Fernmeldegeheimnis unterfallen der Inhalt der Telekommunikation und ihre näheren Umstände; dazu gehört insbesondere schon die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis ist bereits bei jeder Speicherung von Verkehrsdaten tangiert, insbesondere also bei Speicherung der Information, wann welche Internetseite besucht hat oder – wenn die Schule den Schülern auch E-Mail-Adressen zuteilt – wer an wen eine E-Mail geschrieben hat.

Es ist davon auszugehen, dass eine Schule dann zum Diensteanbieter im Sinne des Telekommunikationsgesetzes wird, wenn sie die private Internet- oder E-Mail-Nutzung über die schulische Informationstechnik erlaubt oder duldet. Hierfür genügt es bereits, wenn sie den Internetzugang zur Verfügung stellt und dabei die private Nutzung nicht ausdrücklich untersagt. Denn auf diese Weise wirkt sie zumindest teilweise geschäftsmäßig bei der Erbringung von Telekommunikationsdiensten mit. Für eine geschäftsmäßige Erbringung von Telekommunikationsdiensten ist nämlich nach dem Telekommunikationsgesetz keine Gewinnerzielung notwendig, sondern es genügt ein nachhaltiges Angebot von Telekommunikation für Dritte (vgl. § 3 Nummer 6 und 10 TKG).

Gewährt somit eine Schule die private Nutzung bzw. liegen keine expliziten Regelungen hierzu an der Schule vor, so muss die Schule das Fernmeldegeheimnis wahren und darf grundsätzlich keine Verbindungsdaten speichern. Solche Speicherungen dürfen nur insoweit vorgenommen werden, als sie ausnahmsweise von §§ 96 ff. TKG zugelassen werden, etwa weil sie zum Aufbau oder zur Aufrechterhaltung der Telekommunikation, zur Entgeltabrechnung oder zur Beseitigung von Störungen erforderlich sind. Werden zu diesen besonderen Zwecken ausnahmsweise Verbindungsdaten gespeichert, darf nach dem datenschutzrechtlichen Zweckbindungsgrundsatz (Artikel 5 Absatz 1 Buchstabe b) DS-GVO) in diese Daten allerdings auch nur insoweit Einblick genommen werden, als dies zur Verfolgung gerade dieser Zwecke erforderlich ist.

Nun tragen jedoch die Lehrkräfte nach § 38 Absatz 6 des Schulgesetzes Baden-Württemberg (SchG) die unmittelbare pädagogische Verantwortung für die Erzie-

LfDI BW - 35. Tätigkeitsbericht 2019 - 8. Schule und Hochschulen

hung und Bildung der Schüler. Die Schulleitung wiederum leitet und verwaltet nach § 41 SchG die Schule und ist weisungsbe-rechtigt gegenüber den Lehrkräften. Aus diesen Verantwortlichkeiten kann in be-gründeten Einzelfällen ein (von §§ 96 ff. TKG nicht erfasster) pädagogischer Bedarf zur Überprüfung von Kommunikationsda-ten entstehen, z. B. wer wann welche In-ternet-Seite besucht hat.

Diesem Bedarf kann die Schule jedoch nicht nachkommen, wenn sie dem Fernmelde-geheimnis unterliegt; die Verpflichtung zur Einhaltung des Fernmeldegeheimnisses steht dann vielmehr den Anforderungen des Schulgesetzes an die Schule entgegen.

Dieses Dilemma zwischen pädagogischer Verantwortung und Fernmeldegeheimnis lässt sich auflösen, wenn die Schule nicht als Diensteanbieter im Sinne des Telekom-munikationsgesetzes auftritt und damit nicht mehr dem Fernmeldegeheimnis nach § 88 TKG unterliegt. Sobald die Schule explizit den Schülern die private Kommu-nikation untersagt (und diese auch nicht duldet), ist sie nicht mehr als Dienstean-bieter im Sinne des Telekommunikations-gesetzes anzusehen. In der Folge dürfen die Schülerinnen und Schüler die Informa-tionstechnik der Schule nur noch im Rah-men der schulischen Nutzung verwenden. Zur Umsetzung gegenüber den Schülerin-nen und Schülern ist eine Nutzungsord-nung der Schule erforderlich, welche die private Nutzung untersagt. Dazu kann die Schule auf § 23 Absatz 2 SchG zurückgrei-fen und eine entsprechende Schulordnung erlassen, in welcher noch Weiteres gere-gelt werden kann.

Gegenüber den Lehrkräften (und anderen Bediensteten der Schule) gilt hinsichtlich des Fernmeldegeheimnisses übrigens das-selbe: Sobald ihnen die private Nutzung er-

laubt oder sie geduldet wird, unterliegt die Schule dem Fernmeldegeheimnis mit den oben beschriebenen Folgen. Bei Lehrkräf-ten und sonstigen Bediensteten kann aller-dings die Nutzung der Informationstechnik nicht auf der Grundlage des § 23 Absatz 2 SchG geregelt werden; diese Norm findet als Generalklausel nur bei Maßnahmen im Bereich von „erzieherischen Aufgaben“ und somit nur im Verhältnis zu Schülern Anwendung. Eine Untersagung der priva-ten Nutzung gegenüber Lehrkräften kann dagegen im Wege der Dienstanweisung erfolgen. Soll allerdings den Bediensten die private Nutzung gestattet werden, ohne dass die Schule auf die nach §§ 96 ff. TKG erlaubten Verarbeitungen der Ver-bindungsdaten beschränkt sein soll, so empfiehlt es sich, eine entsprechende Dienstvereinbarung mit dem Personalrat zu treffen. Darin kann etwa geregelt wer-den, dass eine Lehrkraft die Informations-technik der Schule auch privat nutzen darf, sofern sie schriftlich zusichert, mit der Speicherung der Verbindungsdaten ein-verstanden zu sein. Zu regeln wäre darin weiterhin, wann im Einzelfall zu welchen vorab definierten Zwecken eine Einsicht durch wen in welche gespeicherten Verbin-dungs- und Bestandsdaten unter welchen weiteren Bedingungen zulässig sein soll.

Auch dann, wenn eine Speicherung von Verbindungsdaten (etwa aufgrund Aus-schlusses der privaten Nutzung in der Nut-zungsordnung) grundsätzlich erlaubt ist, sind bei der konkreten Verarbeitung der Daten weitere datenschutzrechtliche An-forderungen einzuhalten. So ist die Infor-mationspflicht nach Art. 13 bzw. 14 DS-GVO zu beachten. Außerdem muss die maximale Speicherdauer an der Erforder-lichkeit zu dem mit der Speicherung ver-folgten Zweck orientiert sein. Zugang zu den Daten darf nur der möglichst klein zu haltende Kreis von Personen haben, deren

LfDI BW - 35. Tätigkeitsbericht 2019 - 8. Schule und Hochschulen

Zugriff zur Erreichung des Zwecks erforderlich ist (z. B. Schulleitung und Administratoren). Ein Zugriff darf nur unter Beachtung der Datensparsamkeit sowohl in sachlicher (welche Datenarten?) als auch in zeitlicher Hinsicht (wird in der ganzen „Historie“ recherchiert oder nur bezüglich eines bestimmten „Tatzeitraums“?) erfolgen. Dabei darf der heimliche Zugriff nur dann erfolgen, wenn mit dem offenen Zugriff der verfolgte Zweck nicht erreicht werden kann; wird der heimliche Zugriff unter diesem Gesichtspunkt vorgenommen, hat in der Regel eine nachträgliche Benachrichtigung zu erfolgen, sobald diese ohne Vereitelung des Zwecks möglich ist.

Eine Nutzungsordnung für die Informationstechnik ist an einer Schule ein Muss, um das Dilemma zwischen Fernmeldegeheimnis und pädagogischer Verantwortung der Schule aufzulösen.

8.2 Überarbeitung der Broschüre „Datenschutz in Kindertageseinrichtungen“ im Hinblick auf die Datenschutzgrundverordnung

„Datenschutz ist Grundrechtsschutz. Datenschutz ist Kinderschutz.“ So lautet der Slogan im Vorwort der vom Kultusministerium Baden-Württemberg herausgegebenen Broschüre „Datenschutz in Kindertageseinrichtungen“. Diese hat das Kultusministerium gemeinsam mit uns und dem unter anderem für Baden-Württemberg zuständigen Regionalverantwortlichen für den Datenschutz der Evangelischen Kirche in Deutschland im Hinblick auf die Neuerungen der Datenschutz-Grundverordnung aktualisiert.

In Bezug auf die Verarbeitung personenbezogener Daten durch Kindertagesstätten erhält unsere Dienststelle laufend zahlrei-

che Beratungswünsche und Beschwerden. Bereits hieraus wird deutlich, dass es in diesem Bereich vielfach erhebliche Unsicherheiten in Bezug auf die Anforderungen des Datenschutzes gibt. Um diesen entgegenzuwirken, hatte das Kultusministerium bereits im Jahr 2012 gemeinsam mit freien Trägerverbänden, den kirchlichen Datenschutzbeauftragten und meiner Dienststelle eine viel nachgefragte Broschüre „Datenschutz in Kindertageseinrichtungen“ herausgegeben, zuletzt in dritter Auflage im Jahr 2015 (zur Erstauflage s. bereits den 31. Tätigkeitsbericht meiner Dienststelle 2012/2013, Nr 8.1.1, S. 115).

Die Änderungen, welche die Datenschutz-Grundverordnung mit sich gebracht hat, wirken sich auch im Bereich der Kindertagesstätten aus. Gleichzeitig betont die Datenschutz-Grundverordnung an vielen Stellen die besondere Schutzbedürftigkeit von Kindern im Hinblick auf den Datenschutz (vgl. etwa die Erwägungsgründe 38 und 75 sowie Art. 6 Absatz 1 Buchst. f) letzter Halbsatz DS-GVO). Daher erschien es geboten, die Broschüre im Hinblick auf die Neuerungen der Datenschutz-Grundverordnung erneut zu überarbeiten.

Die Neufassung der Broschüre behält die bewährte Gliederung in Informationen für Eltern, Informationen für Erzieherinnen und Erzieher sowie Informationen für die Träger von Kindertagesstätten bei, geht aber jeweils auf die neuen Rechtsgrundlagen ein.

Dabei werden in der neuen Auflage die Eltern wie bisher insbesondere über ihre Datenschutzrechte gegenüber der Kindertageseinrichtung aufgeklärt:

- Welche personenbezogenen Daten darf die Kindertageseinrichtung erheben und wann benötigt sie eine Einwilligung?

LfDI BW - 35. Tätigkeitsbericht 2019 - 8. Schule und Hochschulen

- Wann müssen diese Daten wieder gelöscht werden?
- Welchen Anspruch auf Auskunft über die Daten der Kinder haben die Eltern?

Darüber hinaus enthält die Broschüre Informationen für Erzieherinnen und Erzieher zur Unterstützung ihrer Arbeit in den Kindertageseinrichtungen. Behandelt werden u. a. die praxisrelevanten Fragen, was im Aufnahme- bzw. Betreuungsvertrag gefragt werden darf, wie mit Beobachtungsbögen und der Bildungs- und Entwicklungsdokumentation, Ton- und Videoaufzeichnungen sowie Fotos umzugehen ist, unter welchen Umständen Listen mit den Kontaktdaten der Kinder bzw. ihrer Eltern erstellt und herausgegeben werden dürfen sowie welche personenbezogenen Daten zwischen Kindertageseinrichtungen und Schule ausgetauscht oder an Behörden bzw. sonstige Dritte weitergeben werden dürfen. Neu eingefügt wurden insoweit Ausführungen zu den besonderen Kategorien personenbezogener Daten und zu den Meldepflichten bei Datenpannen.

Der Abschnitt mit den Informationen für die Träger von Kindertagesstätten enthält wie bisher Ausführungen dazu, was im Aufnahme- oder Betreuungsvertrag berücksichtigt werden muss und wie die Träger dem Recht der Eltern auf Auskunft über gespeicherte Daten nachkommen können. Neu aufgenommen wurden Erläuterungen zum Verzeichnis der Verarbeitungstätigkeiten und zur Datenschutz-Folgenabschätzung.

Besonders hilfreich für die Praxis dürften die überarbeiteten Muster für Einwilligungen (zum Aushang, zur Weitergabe und zur Veröffentlichung von Fotos, zur Veröffentlichung sonstiger personenbezogener Daten, zur Erfassung von Daten zur Bildungs- und Entwicklungsdokumentation

sowie zu Ton- und Videoaufzeichnungen) sein. Im Hinblick auf die Belehrungspflichten insbesondere aus Artikel 13 Absatz 2 und Artikel 14 Absatz 2 DS-GVO wird den Kindertagesstätten außerdem ein neu erarbeitetes Muster-Beiblatt zur Information über Rechte nach der Datenschutz-Grundverordnung zur Verfügung gestellt.

Die Broschüre ist [elektronisch](#) und in Papierform über die Seiten „Kindergärten und andere Kitas in Baden-Württemberg“ des Kultusministeriums erhältlich.

Datenschutz und Pädagogik ergänzen sich. Sowohl beim Datenschutz als auch in der Pädagogik stehen die Würde des Menschen nach Artikel 1 unseres Grundgesetzes (GG) und die freie Entfaltung der Persönlichkeit nach Artikel 2 GG im Zentrum. Deswegen unterstützt die neu aufgelegte Broschüre die Kindertageseinrichtungen sowie die Erzieherinnen und Erzieher beim Datenschutz und bietet damit auch Rüstzeug für die pädagogische Arbeit mit dem Kind.

8.3 Überarbeitung der Verwaltungsvorschrift über den Datenschutz an öffentlichen Schulen durch das Kultusministerium Baden-Württemberg und deren Umsetzung

Nachdem das Land das Landesdatenschutzgesetz an die Datenschutz-Grundverordnung angepasst hatte, konnte das Kultusministerium die Verwaltungsvorschrift über den Datenschutz an öffentlichen Schulen überarbeiten. Gemäß § 26 Absatz 2 LDSG hat mich das Kultusministerium hierzu rechtzeitig beteiligt. Während ich die Überarbeitung der Verwaltungsvorschrift und die Einbeziehung meiner Dienststelle durch das Kultusministerium

LfDI BW - 35. Tätigkeitsbericht 2019 - 8. Schule und Hochschulen

grundsätzlich begrüße, sind aus meiner Sicht gleichwohl noch erhebliche Defizite beim Vollzug der Verwaltungsvorschrift und namentlich bei dem Umfang der den Schulen zur Erfüllung der datenschutzrechtlichen Anforderungen zur Verfügung gestellten Ressourcen festzustellen.

Mit dem Erlass einer Verwaltungsvorschrift über den Datenschutz an öffentlichen Schulen (im Folgenden: VwV) unterstützt das Kultusministerium die Schulen, indem es die datenschutzrechtlichen Vorgaben in Bezug auf öffentliche Schulen konkretisiert und dadurch deren Handeln vereinheitlicht sowie vereinfacht. Zuletzt hatte das Kultusministerium die Verwaltungsvorschrift mit Wirkung zum 1. Januar 2015 aktualisiert (vgl. hierzu den [32. Tätigkeitsbericht 2014/2015](#) meiner Dienststelle, Nr. 8.1 / S. 141 f.). Das Inkrafttreten der Datenschutz-Grundverordnung und in dessen Folge die Neufassung des Landesdatenschutzgesetzes brachten die Notwendigkeit einer Überarbeitung auch der Verwaltungsvorschrift mit sich.

Dem ist das Kultusministerium mit dem Erlass der unter dem 4. Juli 2019 neu gefassten Verwaltungsvorschrift, in dessen Entwurf es mich ordnungsgemäß eingebunden hat, nachgekommen. Der Änderungsbedarf war dabei erheblich; nur beispielhaft können hier wesentliche Neuerungen aufgezählt werden:

- Neu sind etwa die Ausführungen über die Informationspflicht bei der Datenerhebung (Nummer 1.2 VwV). Ein Großteil der Stammdaten wird bereits bei Aufnahme der Schülerinnen und Schüler erhoben. Die neu geschaffene Anlage 2 zur Verwaltungsvorschrift gibt den Schulen hierzu das Muster eines Schul-Aufnahmebogens an die Hand, an dem sich die Schulen nach

Nummer 2.2.1 (vorletzter Satz) zu orientieren haben. Dort befinden sich Ausführungen zur Erfüllung der datenschutzrechtlichen Informationspflicht, die noch durch ein separates – ebenfalls neu entwickeltes – Merkblatt „Betroffenenrechte“ ergänzt wird. In dem Muster wird außerdem in vorbildlicher Weise kenntlich gemacht, zu welchen Angaben die Eltern der Schüler verpflichtet sind und welche Angaben nur freiwillig zu tätigen sind.

- Grundlegend überarbeitet bzw. neu eingeführt wurden etwa die Hinweise zur Zulässigkeit von Datenverarbeitungen (Nummer 1.1 VwV), zur Verarbeitung besonderer Kategorien personenbezogener Daten (Nummer 1.4 VwV), zur Datenlöschung und Einschränkung der Verarbeitung sowie zur Datenübertragbarkeit (Nummer 1.5 VwV) und zum Auskunftsweg (Nummer 1.6 VwV).
- Hilfreiche Erläuterungen erhalten die Schulen durch die Verwaltungsvorschriften außerdem zum Verzeichnis von Verarbeitungstätigkeiten (Nummer 1.8 VwV) einschließlich einer Auflistung der regelmäßig zumindest einzutragenden Computerprogramme (Nummer 1.8.3 VwV), zur Notwendigkeit und Durchführung einer Datenschutz-Folgeabschätzung (Nummer 1.9 VwV) und zur Meldung von Datenpannen (Nummer 1.10 VwV).
- Für besonders wichtig erachte ich die Anordnung einer regelmäßigen Belehrung des gesamten Kollegiums der Schule zum Datenschutz, welche nach Nummer 1.7.2 VwV einmal pro Jahr erfolgen muss. Zum Nachweis der Belehrung wird den Schulen ein Formular in Anlage 3 zur Verwaltungsvorschrift zur Verfügung gestellt.

LfDI BW - 35. Tätigkeitsbericht 2019 - 8. Schule und Hochschulen

Allerdings sehe ich bei der Umsetzung der Verwaltungsvorschrift noch Verbesserungspotenzial:

- Wie in der Verwaltungsvorschrift (Nummer 1.11.3 und 1.11.5 VwV) erwähnt, ist es gemäß Artikel 37 DS-GVO öffentlichen Stellen vorgeschrieben, einen Datenschutzbeauftragten zu benennen und dies mir zu melden, wobei die Schule z. B. mein Online-Portal verwenden kann. Leider ergab jedoch eine Auswertung, dass mir nur von gut 800 öffentlichen und privaten Schulen solche Meldungen vorliegen, bei rund 3800 öffentlichen und ca. 720 privaten Schulen in Baden-Württemberg (Statistisches Landesamt, Allgemeinbildende Schulen bzw. berufliche Schulen, Gesamtüberblick Schuljahr 2018/2019). Das ist ein sehr geringer Anteil und wird zu Kontrollaktionen meiner Behörde führen.
- Die Datenschutzerklärungen von diversen Internet-Auftritten der Schulen enthalten keine Angaben nach Artikel 13 Absatz 1 Buchstabe b DS-GVO zum Datenschutzbeauftragten. Solche Angaben in den Internet-Auftritten der Schulen könnten jedoch auch die Effizienz des Datenschutzes an Schulen erhöhen, v. a. da ich dadurch bei Beschwerden von Eltern, Schülerinnen bzw. Schülern oder Lehrkräften besser mit den Datenschutzbeauftragten zusammenarbeiten könnte. Durch die Angabe der Kontaktdaten des Datenschutzbeauftragten im Internetauftritt können auch die Betroffenen einfacher unmittelbar mit dem Datenschutzbeauftragten der Schule in Verbindung treten, welcher, da näher an der Schule, häufig schneller als ich die datenschutzrechtlichen Probleme beheben kann.
- Bereits in meinem letzten Tätigkeitsbericht 2018 bin ich in Kapitel 8.1 auf die fehlenden personellen und finanziellen Ressourcen bei der Bestellpflicht von Datenschutzbeauftragten eingegangen (Tätigkeitsbericht 2018, S. 111). Im Stellenplan des Nachtragshaushalts 2018/2019 des Kultusministeriums (Kapitel 0404 Staatliche Schulämter Titel 422 01) finden sich nun 26 neue Stellen für Datenschutzbeauftragte, welche an den Schulämtern angesiedelt werden sollen. Über neue Stellen für Datenschutzbeauftragte freue ich mich sehr. Geht man aber davon aus, dass die Schulämter für rd. 3100 öffentliche Schulen verantwortlich sind (Statistisches Landesamt, Allgemeinbildende Schulen, Gesamtüberblick Schuljahr 2018/2019; für Gymnasien und berufliche Schulen sind nicht die Schulämter, sondern die Regierungspräsidien verantwortlich), ist durchschnittlich einer dieser Datenschutzbeauftragten für rd. 120 Schulen zuständig, sofern keine Datenschutzbeauftragten aus den Kollegium der Schulen benannt wurden.

Nimmt der Datenschutzbeauftragte seine Aufgaben gemäß Artikel 39 DS-GVO ernst, so muss er die Lehrkräfte an diesen rd. 120 Schulen zum Datenschutz sensibilisieren, beraten und schulen sowie die Einhaltung der Datenschutz-Grundverordnung und anderer Datenschutzvorschriften an der Schule überwachen und er muss frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden sein. Außerdem können ihn betroffene Personen, d. h. hier Eltern, Schülerinnen bzw. Schüler und Lehrkräfte, an diesen rd. 120 Schulen zu allen mit der Verarbeitung personenbezogener Daten stehenden Fragen zu Rate ziehen. Eine solche Aufgabenlast

LfDI BW - 35. Tätigkeitsbericht 2019 - 8. Schule und Hochschulen

ist von den aktuell bestellten Datenschutzbeauftragten nicht zu bewältigen.

Bei einer großen Menge an Schulen in der Zuständigkeit eines einzelnen Datenschutzbeauftragten besteht daher ein Widerspruch zu Artikel 38 Absatz 2 DS-GVO, wonach der Verantwortliche die zur Erfüllung erforderlichen Ressourcen zur Verfügung stellen muss.

Zur weiterhin hier vorliegenden Problematik des Interessenkonflikts (vgl. Artikel 38 Absatz 6 DS-GVO) für die Mitarbeiter des Schulamts in der Funktion des Datenschutzbeauftragten einer Schule verweise ich auf Kapitel 8.1 meines Tätigkeitsberichts 2018 auf S. 111.

Die Verwaltungsvorschrift Datenschutz an öffentlichen Schulen erleichtert den Schulen die Umsetzung des Datenschutzes. Allerdings müssen den Schulen zur weiteren Umsetzung deutlich mehr Ressourcen zur Verfügung gestellt werden, damit insbesondere die gesetzlich vorgeschriebenen Datenschutzbeauftragten effektiv tätig werden können.



LfDI BW - 35. Tätigkeitsbericht 2019 - 8. Schule und Hochschulen

9. Privater Datenschutz

9.1 Arbeitnehmerüberlassung – Verarbeitung im Auftrag ?

Eine Auftragsverarbeitung gem. Art. 28 DS-GVO wird zwischen verantwortlichen Stellen (leider) oftmals vereinbart, um vermeintlichen Anforderungen der DS-GVO nachzukommen, auch wenn im konkreten Fall überhaupt keine Auftragsverarbeitung vorliegt. Werden Beschäftigtendaten von verschiedenen Unternehmen erhoben oder übermittelt, sind mit Blick auf den Beschäftigtendatenschutz die Datenverarbeitungen besonders sensibel und genauer zu betrachten.

Im Rahmen eines Kontrollbesuchs eines Personaldienstleisters schilderte uns der betriebliche Datenschutzbeauftragte nachfolgende Problematik, die wir bei der Vor-Ort-Kontrolle umgehend richtig stellen konnten:

Das Geschäftsmodell der verantwortlichen Stelle ist das sog. „Personalleasing“, also als „Verleiher“ die Arbeitnehmerüberlassung von Leiharbeiter*innen entsprechend des Arbeitnehmerüberlassungsgesetzes (AÜG). Im Zuge des Einsatzes der Leiharbeiter*innen bei anderen Unternehmen, den „Entleihern“, seien in der Vergangenheit oftmals Auftragsverarbeitungsvereinbarungen gem. Art. 28 DS-GVO seitens der Entleihunternehmen zugesandt worden, um damit den datenschutzrechtliche Anforderungen der DS-GVO vor dem Hintergrund der Arbeitnehmerüberlassung zu genügen. Nach Art. 88 DS-GVO i. V. m. § 26 Absatz 8 Nr. 1 BDSG sind Beschäftigte im Sinne des Gesetzes „Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeiterinnen und Leiharbeiter im Verhältnis zum Entleiher“. Dies soll klarstellen, dass Leih-

arbeiter*innen nicht nur gegenüber Ihrem Arbeitgeber, sondern auch gegenüber dem Unternehmen, bei welchem sie eingesetzt sind, datenschutzrechtlich als Beschäftigte gelten.

Dies ist darauf zurück zu führen, dass es zu einer Vielzahl von Verarbeitungen, zwischen dem „Verleiher“ und „Entleiher“ über die Leiharbeiter*innen kommt und beide sich demnach an die Voraussetzungen des Art. 88 DS-GVO i. V. m. § 26 Absatz 1 BDSG halten müssen. Das bedeutet aber auch, dass eine Auftragsverarbeitungsvereinbarung gem. Art. 28 DS-GVO beim „Personalleasing“ überhaupt nicht in Frage kommt. Der „Verleiher“ verarbeitet keine personenbezogenen Daten auf Weisung, unter Kontrolle oder für Zwecke des Entleihers, wie es Art. 28 DS-GVO voraussetzen würde.

Das Gegenteil ist der Fall: „Entleiher“ und „Verleiher“ verarbeiten die personenbezogenen Daten Leiharbeiter*innen meistens für ihre eigenen oder gemeinsame Zwecke und Absichten und somit gerade nicht im Auftrag oder auf Weisung der anderen Vertragspartei. „Verleiher“ und „Entleiher“ sind somit selbst jeweils als eigene Verantwortliche anzusehen oder gemeinsam verantwortlich.

Für die Durchführung der Arbeitnehmerüberlassung von Leiharbeiter*innen kommt eine Auftragsverarbeitungsvereinbarung gem. Art. 28 DS-GVO zwischen „Verleiher“ und „Entleiher“ nicht in Frage. Die beteiligten Unternehmen müssen ihre (beabsichtigten) Verarbeitungen der personenbezogenen Daten der Beschäftigten eigenständig auf ihre Rechtmäßigkeit überprüfen und entsprechende Vorkehrungen treffen.

LfDI BW - 35. Tätigkeitsbericht 2019 - 9. Arbeitswelt

9.2 Parkraumüberwachung durch private Unternehmen

Ein in unserem Zuständigkeitsbereich ansässiges Unternehmen überwacht bundesweit die Einhaltung der Benutzungsordnungen von privaten Parkplätzen und Parkhäusern. Immer wieder wenden sich Personen, die wegen eines „Parkverstoßes“ von diesem Unternehmen in Anspruch genommen werden, an unsere Behörde, weil sie darin einen Datenschutzverstoß sehen.

Eine derartige Beschwerde ist grundsätzlich zulässig. Allerdings können wir die Angelegenheit nur datenschutzrechtlich überprüfen. Ob die – angebliche – Forderung des Unternehmens begründet ist, müssen ggf. die Zivilgerichte entscheiden.

Das Überwachungsunternehmen kann die Kfz-Halterdaten eines seiner Meinung nach rechtswidrig abgestellten Fahrzeugs über das Kraftfahrtbundesamt oder die Zulassungsstelle beschaffen. Dazu muss glaubhaft gemacht werden, dass dem Eigner des Parkraums u. U. ein Rechtsanspruch im Zusammenhang mit dem Betrieb des Fahrzeuges zusteht. Das Überwachungsunternehmen kann diese Angaben nutzen bzw. nutzen lassen, um diese – vermeintlichen – Ansprüche durchzusetzen. Das ist nach dem Datenschutzrecht zulässig.

Für den Fall, dass eine Person erwiesenermaßen „falsch“ geparkt hat, darf das Unternehmen eine angemessene Zeit diesen Vorgang auch nach Abschluss des Kostenerhebungsverfahrens speichern, um im Wiederholungsfall schärfere Sanktionen zu ergreifen bzw. von Kulanzentscheidungen abzusehen. Dazu muss es aber nach Art. 21 Absatz 1 der EU-Datenschutzgrundverordnung im Falle des Widerspruchs der betroffenen Person beweisen, dass diese tatsächlich einen von der Firma verwalte-

ten Parkplatz zu Unrecht genutzt hat bzw. dass dadurch ein Schaden eingetreten ist. Der Fahrer des Fahrzeuges kann in der Regel nur in Anspruch genommen werden, wenn er mit Befahren des Parkplatzes die Allgemeinen Geschäftsbedingungen, die eine Vertragsstrafe für rechtswidriges Parken vorsehen, konkludent akzeptiert hat. Das Bestehen einer Forderung gegenüber dem Halter, der das Fahrzeug nicht selbst abgestellt hat, setzt voraus, dass dem Inhaber des Parkplatzes nach den §§ 861, 823 Absatz 1 des Bürgerlichen Gesetzbuches ein konkreter Schaden durch die „Besitzentziehung“ des Parkplatzes entstanden ist.

Kann dem Fahrer bzw. dem Halter ein derartiger Anspruch nicht nachgewiesen werden, sind deren Daten nach Beendigung des Beitreibungsverfahrens in der Datei, auf die die Mitarbeiterinnen und Mitarbeiter des Überwachungsunternehmens zur Bearbeitung derartiger Fälle Zugriff nehmen können, zu löschen. Die Fortsetzung der Speicherung für einen angemessenen Zeitraum ist nur zulässig, wenn der Anspruch begründet war und das Unternehmen sich vorbehalten hat, im Wiederholungsfall eine höhere Vertragsstrafe zu verlangen bzw. von einer Kulanzentscheidung abzusehen.

Ungeachtet dessen ist das Unternehmen verpflichtet, auch nach dem endgültigen Abschluss des Vorgangs die Daten noch für eine angemessene Dokumentationsfrist gesperrt vorzuhalten, denn das EU-Datenschutzrecht unterscheidet zwischen Datenlöschung und Datenvernichtung. Letztere ist erst zulässig, wenn keine Rückfragen bzw. Rechtsstreitigkeiten wegen der Datenverarbeitung mehr zu erwarten sind bzw. nationale Aufbewahrungsvorschriften das Vorhalten der Angaben nicht mehr vorschreiben. Allerdings dürfen diese dann nur noch so gespeichert sein, dass ledig-

lich die Geschäftsleitung oder der betriebliche Datenschutzbeauftragte darauf Zugriff nehmen können. Die Angaben dürfen dann nur noch für das Finanzamt, für Datenschutzkontrollen oder für zu erwartende gerichtliche Verfahren genutzt werden.

Diese Fälle zeigen, dass Unternehmen durch das Datenschutzrecht nicht gehindert sind, ihnen zustehende Ansprüche zivilprozessual durchzusetzen, dass aber für diesen Zweck erhobene Daten grundsätzlich dann nicht mehr weiterverarbeitet werden dürfen, wenn das Verfahren abschließend entschieden ist. Das Anlegen „Schwarzer Listen“ ist durch das EU-Datenschutzrecht untersagt.

9.3 Datenschutzrechtliche Verantwortlichkeit

In der Praxis werden zunehmend ursprünglich dem Verantwortlichen obliegende Aufgaben an externe Dienstleister übertragen. Dabei ergeben sich häufig Schwierigkeiten hinsichtlich der Abgrenzung von Verantwortlichkeiten. Die datenschutzrechtliche Verantwortlichkeit eines Dienstleisters für Aktenvernichtungen ist nicht zwangsläufig zu verneinen.

Anlass für die erneute Auseinandersetzung mit diesem Thema war eine Datenpannenmeldung, bei der es um die Frage ging, ob ein Dienstleister für die Aktenvernichtung beim Aufstellen eines Einwurf-Containers selbst überprüfen muss, dass dieser verschlossen aufgestellt wird oder ob es stets dem Auftraggeber obliegt, dies bei Anlieferung des Containers zu überprüfen.

Adressat der Datenschutzgrundverordnung ist primär der Verantwortliche, also die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die alleine oder gemeinsam mit anderen über

die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (vgl. Art. 4 Nr. 7 DS-GVO). Verstößt er gegen die DS-GVO, so kann er nicht nur Adressat von Geldbußen und anderen Sanktionen werden (Art. 83 und 84 DS-GVO), sondern haftet gegenüber der oder den Personen, die durch diese Verstöße einen materiellen oder immateriellen Schaden erleiden (Art. 82 Absatz 1 DS-GVO). Dieser Schadensersatzanspruch richtet sich vorrangig gegen den Verantwortlichen, kann aber unter Umständen auch den Auftragsverarbeiter treffen, auch wenn dessen Haftung durch Art. 82 Absatz 2 beschränkt wurde:

Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

Für die Haftungsfrage ist also entscheidend, ob ein Verantwortlicher oder ein Auftragsverarbeiter den Schaden verursachte. Eine Exkulpierungsmöglichkeit steht ausschließlich dem Auftragsverarbeiter offen. Wenngleich der Auftragsverarbeiter vom Verantwortlichen im Grundsatz klar zu trennen ist, können sich in Grenzfällen durchaus schwierige Abgrenzungsfragen stellen.

Auftragsverarbeiter ist nach Art. 4 Nr. 8 DS-GVO eine Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Nach Art. 29 DS-GVO darf ein

LfDI BW - 35. Tätigkeitsbericht 2019 - 9. Arbeitswelt

Auftragsverarbeiter personenbezogene Daten nur nach Weisung des Verantwortlichen verarbeiten. Dabei steht dem Auftragsverarbeiter nur ein sehr begrenzter Gestaltungsspielraum bei einer Datenverarbeitung zur Verfügung. Grundsätzlich wird dem Auftragsverarbeiter nicht die eigentliche Aufgabe übertragen, sondern nur eine Hilfstätigkeit. Deshalb wird die Verarbeitungstätigkeit des Auftragsverarbeiters grundsätzlich dem Verantwortlichen zugerechnet. Dies ergibt sich insbesondere auch aus Art. 28 DS-GVO, welcher dem Verantwortlichen die Prüfung der Geeignetheit des Auftragsverarbeiters auferlegt.

Häufiges Paradebeispiel für das Vorliegen einer Auftragsverarbeitung ist die Hinzuziehung eines Dienstleisters für die Aktenvernichtung. Die Löschung von magnetischen und optischen Datenträgern (z. B. Magnetbändern, Disketten, CDs, DVDs, Sticks) bzw. die Vernichtung von Datenträgern aller Art, insbesondere von nicht mehr benötigten Papierunterlagen, stellt eine typische Datenverarbeitung dar. Seit Inkrafttreten der DS-GVO gibt es eine bezeichnende Zunahme von Dienstleistern, welche eine DS-GVO-konforme Aktenvernichtung anbieten. Insbesondere wird damit geworben, dass sich „um alles gekümmert wird“. Gerade kleine und mittelständische Unternehmen nehmen dieses Angebot verständlicherweise gerne an, um sich zumindest bezüglich der Datenlöschung keine Sorgen mehr machen zu müssen. Vergessen wird dabei, dass der Verantwortliche auch dann die Verantwortung für die Einhaltung der Datenschutz-Vorschriften trägt, wenn er einen Auftragsverarbeiter mit der Vernichtung von Datenträgern mit personenbezogenen Daten beauftragt (Art. 5 Absatz 2 DS-GVO). Ihm obliegen Überprüfung und Einhaltung der Vorgaben der DS-GVO. Dies gelingt ihm nur, wenn er dem Dienstleister klare Weisungen erteilt hinsichtlich

der Löschung, aber auch bezüglich der Zwischenlagerung und dem Transport (bis zur Vernichtung) sowie Ort und Zeitpunkt der Vernichtung (z. B. vor Ort beim Verantwortlichen oder in der Betriebsstätte des Auftragsverarbeiters) festlegt. Sind diese Angaben mit dem Dienstleister nicht oder nur schwer verhandelbar, muss sich der Verantwortliche die Frage stellen lassen, ob hier noch von einer Auftragsverarbeitung gesprochen werden darf und ob er einen geeigneten Dienstleister ausgewählt hat. Zu beachten ist hierbei der weniger bekannte Art. 28 Absatz 10 DS-GVO:

Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.

Ein Dienstleister, der selbstständig darüber entscheidet, wie er die Daten vernichtet, lagert und/oder transportiert, begibt sich in die Position eines Verantwortlichen. Er kann sich seiner Verantwortlichkeit selbst dann nicht entziehen, wenn formal ein Auftragsverarbeitungsvertrag geschlossen wird, dieser aber in der Realität nicht „gelebt“ wird. Ein solcher Vertrag kann zwar einen Rechtschein setzen, der für eine Auftragsverarbeitung spricht, ist aber nicht konstituierend. Bedeutet: Man kann mittels dieses Vertrages keinen Auftragsverarbeiter kreieren, der tatsächlich keiner ist – sondern selbst die Rolle des Verantwortlichen eingenommen hat.

Die Fassade des Paradebeispiels für Auftragsverarbeitung bröckelt. Inzwischen spricht einiges dafür, dass nicht mehr jeder Dienstleister auch „nur“ Auftragsverarbeiter ist. Entscheidend ist vielmehr, wer tatsächlich die Art der durchzuführenden Datenverarbeitungen und den Umgang

mit den zu löschenden personenbezogenen Daten festlegt. Je weniger Einfluss das Unternehmen oder die Behörde auf den Dienstleister hat, desto weniger kann man von einer Auftragsverarbeitung sprechen. Dass dieser Trend durchaus kritisch zu sehen ist, liegt auf der Hand: Die Privilegierung für die Datenübertragung vom Unternehmen oder der Behörde auf den Dienstleister entfiel, es bedürfte mithin einer eigenständigen Rechtsgrundlage. Eventuell wäre sogar an eine Gemeinsame Verantwortlichkeit (Art. 26 DS-GVO) zu denken. Der LfDI rät, hier klare Regelungen zu treffen und diese für beide Seiten ungünstige Rechtslage zu vermeiden.

9.4 Datenschutz bei der Hausverwaltung

Hausverwaltungen verarbeiten eine Vielzahl personenbezogener Daten sowohl von Wohnungseigentümern als auch von Mietern. Gerade im Hinblick auf die Wohnungseigentümergeinschaft herrscht bei Verwaltern oft die Ansicht vor, dass Eigentümerdaten großzügig weitergegeben werden dürften, weil in der Wohnungseigentümergeinschaft kein Datenschutzrecht gelte. Diese Ansicht ist unzutreffend.

Weitergabe von Daten innerhalb einer Wohnungseigentümergeinschaft

Die Wohnungseigentümergeinschaft begründet zwischen ihren Mitgliedern ein zivilrechtliches Schuldverhältnis mit gegenseitigen Rechten und Pflichten. Da den Wohnungseigentümern aufgrund dieses Schuldverhältnisses rechtliche Ansprüche gegeneinander entstehen können, müssen sie in der Lage sein, einander notfalls vor den Zivilgerichten verklagen zu können. Jeder Wohnungseigentümer hat daher ein berechtigtes Interesse, die Namen und ladungsfähigen Anschriften aller anderen

Miteigentümer zu erfahren. Der Verwalter ist aufgrund seines mit der Wohnungseigentümergeinschaft geschlossenen Verwaltervertrags verpflichtet, jedem Miteigentümer auf Verlangen eine Liste der Namen und Anschriften der übrigen Miteigentümer zur Verfügung zu stellen. Hierfür bedarf es weder der Einwilligung der einzelnen Miteigentümer noch eines Beschlusses der Eigentümerversammlung.

Anders verhält es sich mit den E-Mail-Adressen und sonstigen Kontaktdaten der Wohnungseigentümer. Diese sind für rechtliche Auseinandersetzungen zwischen den Mitgliedern der Gemeinschaft nicht notwendig. Die Weitergabe dieser Daten durch den Verwalter ist daher weder zur Erfüllung des Verwaltervertrags noch zur Wahrung berechtigter Interessen der Miteigentümer erforderlich. Der Verwalter darf die Kontaktdaten daher nicht ohne Einwilligung aller betroffenen Eigentümer weitergeben.

Dies gilt auch bei der Weiterleitung von E-Mails im Rahmen von Diskussionen und Auseinandersetzungen innerhalb der Wohnungseigentümergeinschaft unter Beteiligung des Verwalters. Wenn ein Eigentümer den Verwalter per E-Mail auf einen Missstand aufmerksam macht, dem er abhelfen oder der in der Eigentümerversammlung besprochen werden soll, so bestimmt sich die Frage, ob der Verwalter diese E-Mail den anderen Miteigentümern unter Offenlegung der Identität des Absenders weiterleiten darf nach dem Ergebnis der Interessenabwägung gemäß Artikel 6 Absatz 1 Unterabsatz 1 lit. f DS-GVO. Selbst wenn hiernach die Weitergabe des nicht anonymisierten E-Mail-Textes im Einzelfall zulässig sein sollte, ist die Übermittlung der E-Mail-Adresse selbst im Zweifel ohne Einwilligung des betroffenen Eigentümers rechtswidrig. Auch hier müs-

LfDI BW - 35. Tätigkeitsbericht 2019 - 9. Arbeitswelt

sen die Hausverwalter daher ganz genau hinsehen.

Weitergabe von Daten an externe Stellen wie Handwerker

Der Hausverwalter gibt in der Praxis häufig auch Kontaktdaten an externe Stellen weiter, vor allem an Handwerker. Auf diese Weise soll gewährleistet werden, dass dieser mit dem Wohnungsnutzer, sei es ein Eigentümer oder ein Mieter, zeitnah einen Reparaturtermin vereinbaren kann. Häufig stößt die Weitergabe aber bei der betroffenen Person auf Unmut, etwa weil diese zwar damit einverstanden gewesen wäre, telefonisch, nicht jedoch per E-Mail vom Handwerksbetrieb kontaktiert zu werden.

Die Weitergabe der Kontaktdaten findet ihre Rechtsgrundlage regelmäßig in Artikel 6 Absatz 1 Unterabsatz 1 lit. b DSGVO, d.h. die Übermittlung muss für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich sein. Handelt es sich beim betroffenen Wohnungsnutzer um den Eigentümer, so kommt hierfür der Verwaltervertrag in Betracht. Damit der Verwalter vertragsgemäß eine zeitnahe Reparatur in die Wege leiten kann, gibt er die Telefonnummer des Eigentümers an den Handwerksbetrieb weiter, die er zu Vertragsbeginn vom Eigentümer zu diesem Zweck erhalten hat. Im Rahmen seiner Informationspflichten nach Artikel 13 DSGVO muss der Verwalter den Eigentümer schon bei der Erhebung der Telefonnummer auf die Möglichkeit der Weitergabe an Handwerker zwecks Vereinbarung von Reparaturterminen hinweisen. Hingegen sollte der Verwalter, wenn er im Lauf der Zeit vom Eigentümer eine E-Mail erhält, dessen E-Mail-Adresse nicht ohne dessen Einwilligung des Eigentümers an Handwerker weitergeben, denn eine solche Weitergabe wäre angesichts der zu diesem

Zweck hinterlegten Telefonnummer nicht ohne Weiteres erforderlich.

Deutlicher wird die Problematik bei der Mietverwaltung. Der Mietinteressent teilt dem Vermieter, dem von diesem beauftragten Makler oder dem die Mieterauswahl vorbereitenden Hausverwalter oft eine Vielzahl von Kommunikationsdaten mit, um überhaupt bei der Mieterauswahl berücksichtigt zu werden. Kommt das Mietverhältnis dann zustande, so ist der Verwalter im Besitz jeweils der dienstlichen und privaten Festnetz- und Mobilfunknummer des Mieters sowie seiner E-Mail-Adresse und ggf. der Faxanschlussnummer seiner Eltern. Wird in der Wohnung eine Reparatur fällig, so wählt der Verwalter leider oft „zielsicher“ dasjenige Kontaktdaten aus, unter dem der betroffene Mieter am schlechtesten zu erreichen ist oder er verzichtet gänzlich auf die Auswahl und gibt gleich alle Kontaktdaten ohne Einverständnis des Mieters weiter.

Auch hier ist die Weitergabe eines Kontaktdaten erforderlich, nämlich zur Erfüllung des zwischen Mieter und Vermieter geschlossenen Mietvertrags. Erforderlich ist dabei aber nur das Kontaktdaten, unter dem der Mieter erreichbar ist und erreichbar sein will. Liegen dem Verwalter mehrere Kontaktdaten vor, darf er diese nicht alle übermitteln, sondern muss sich auf das für den Zweck notwendige beschränken. Auf welches von mehreren dem Verwalter vorliegenden Kontaktdaten dies zutrifft, hat dieser selbst kraft seiner datenschutzrechtlichen Verantwortlichkeit zu ermitteln. Zu diesem Zweck empfiehlt es sich, den Mieter einfach zu fragen, unter welchem Kontaktdaten er für Handwerker erreichbar sein will. Nur wenn der Verwalter auf diese Frage in angemessener Zeit keine Antwort erhält, darf er selbst entscheiden, welches Kontaktdaten er dem

Handwerksbetrieb übermittelt. Die Informationspflicht nach Artikel 13 DS-GVO gilt auch gegenüber dem Mieter.

Der Hausverwalter hat bei der Weitergabe von Kontaktdaten der Wohnungsnutzer die Grundsätze der Erforderlichkeit und der Datenminimierung zu beachten.

Benennung eines Datenschutzbeauftragten durch eine Wohnungseigentümergeinschaft

Hausverwalter bieten den ihnen vertraglich verbundenen Wohnungseigentümergeinschaften zuweilen an, für sie neben der Verwaltung der Wohnanlage auch die Aufgaben eines Datenschutzbeauftragten zu übernehmen. Die dafür entstehenden Kosten sollen dann vollständig der Gemeinschaft auferlegt werden. Dieses Vorgehen bedarf kritischer Betrachtung.

Eine Wohnungseigentümergeinschaft ist regelmäßig nicht zur Benennung eines Datenschutzbeauftragten verpflichtet. Insbesondere sind in der Gemeinschaft in der Regel gerade nicht zehn oder mehr Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt, was nach § 38 Absatz 1 Satz 1 BDSG eine Benennungspflicht auslösen würde. Dies dürfte für gewöhnlich auch dann nicht der Fall sein, wenn die Wohnungseigentümer keinen Verwalter bestellt haben, sondern das gemeinschaftliche Eigentum selbst verwalten.

Bestellt die Wohnungseigentümergeinschaft hingegen einen Verwalter, so ist dieser selbst Verantwortlicher im datenschutzrechtlichen Sinn. Er wird auch nicht als Auftragsverarbeiter für die Gemeinschaft tätig, denn der Verwalter unterliegt nach der üblichen Vertragsgestaltung nicht den Weisungen der Wohnungseigentü-

gemeinschaft und wird von dieser auch nicht überwacht. Der Verwalter verarbeitet personenbezogene Daten daher nicht im Auftrag der Gemeinschaft für diese, sondern in eigener Verantwortung zur Durchführung seiner eigenen Geschäftstätigkeit. Ist beispielsweise aufgrund der Anzahl der beim Verwalter in der Regel ständig mit der Verarbeitung personenbezogener Daten beschäftigter Personen die Benennung eines Datenschutzbeauftragten geboten, so trifft diese Pflicht nicht die Wohnungseigentümergeinschaft, sondern den Verwalter selbst.

Ein Verwalter, der aufgrund rechtlicher Vorgaben einen Datenschutzbeauftragten benennt, um die Einhaltung des Datenschutzes in seinem Betrieb zu gewährleisten, hat mithin keine Veranlassung, dessen Tätigkeit gegenüber den Wohnungseigentümern als Dienstleistung für diese zu deklarieren und sie sich von der Gemeinschaft vergüten zu lassen. Ebenso wenig erscheint es angemessen, wenn der Verwalter sonstige Aufwendungen, die der Erfüllung datenschutzrechtlicher Vorgaben im Rahmen seiner Geschäftstätigkeit dienen, der Gemeinschaft als Datenschutz-Service in Rechnung stellt.

Die Wohnungseigentümergeinschaft sollte stets prüfen, ob sie selbst zur Benennung eines Datenschutzbeauftragten verpflichtet ist.

9.5 Datenschutz in der Kreditwirtschaft

Kopieren von Personalausweisen bei Kreditinstituten

Die Praxis von Kreditinstituten, bei der Eröffnung eines Kontos den Personalausweis des Kunden zu fotokopieren, sorgt bei vielen schon seit langem für Irritation. Den-

LfDI BW - 35. Tätigkeitsbericht 2019 - 9. Arbeitswelt

noch bleibt dieses Vorgehen auch unter Geltung der DS-GVO rechtmäßig.

Indem die Bank den Personalausweis kopiert und die Kopie aufbewahrt, verarbeitet sie die im Ausweis abgedruckten personenbezogenen Daten. Nach Artikel 6 Absatz 1 lit. c DS-GVO ist eine solche Verarbeitung unter anderem rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, erforderlich ist. Die maßgebliche rechtliche Verpflichtung ist dem Geldwäschegesetz (GwG) zu entnehmen. Kreditinstitute gehören gemäß § 2 Absatz 1 Nr. 1 GwG zu den Stellen, die Verpflichtungen nach dem Geldwäschegesetz unterliegen. Sie haben nach § 10 Absatz 1 Nr. 1 und Absatz 3 Satz 1 Nr. 1 den Vertragspartner bei Begründung der Geschäftsbeziehung zu identifizieren. Dabei kann die Überprüfung der Identitätsdaten gemäß § 12 Absatz 1 Satz 1 Nr. 1 GwG anhand eines amtlichen Ausweises, wie insbesondere des Personalausweises, erfolgen. § 8 Absatz 2 Satz 2 GwG stellt klar, dass die Bank das Recht und die Pflicht hat, vollständige Kopien des zur Identitätsprüfung vorgelegten Ausweisdokuments anzufertigen oder es vollständig optisch digitalisiert zu erfassen. Die Kopien sind nach § 8 Absatz 4 Satz 1 GwG fünf Jahre lang aufzubewahren.

In diesem Zusammenhang soll nicht unerwähnt bleiben, dass § 11 Absatz 4 Nr. 1 GwG die Daten nennt, die im Rahmen der Identifizierung des Kunden zu erheben sind. Einige der auf den Personalausweis aufgedruckten Angaben, wie z. B. die Körpergröße und Augenfarbe, sowie die für die Verwendung der Online-Funktion unter Umständen benötigte Zugangsnummer gehören nicht dazu. Häufig wird daher darauf hingewiesen, dass das vollständige Kopieren des Personalausweises ohne Schwärzungen einzelner nicht benötigter Angaben

dem Grundsatz der Datenminimierung aus Artikel 5 Absatz 1 lit. c DS-GVO widerspreche. Dieser Einwand ist richtig, steht aber im Ergebnis der Anwendbarkeit des § 8 Absatz 2 Satz 2 GwG nicht entgegen. Zwar genießt die Datenschutzgrundverordnung einschließlich des Grundsatzes der Datenminimierung grundsätzlich Anwendungsvorrang gegenüber Vorschriften des nationalen Rechts. Die Kopierpflicht aus § 8 GwG dient jedoch der Umsetzung von Artikel 40 Absatz 1 lit. a der Vierten Geldwäscherichtlinie (2015/849). Hiernach regeln die Mitgliedstaaten, dass Kreditinstitute eine Kopie der im Rahmen der Identifizierung der Kunden erhaltenen Dokumente anfertigen und aufbewahren. Da die Identifizierung anhand eines ungeschwärzten Ausweisdokuments erfolgt ist, kommt somit auch nur eine vollständige Kopie für die Erfüllung der Aufbewahrungspflicht in Betracht. Artikel 40 Absatz 1 lit. a der Vierten Geldwäscherichtlinie ist insoweit im Verhältnis zur Datenschutz-Grundverordnung eine vorrangige Spezialvorschrift. Die Bank muss daher keine Schwärzung einzelner Angaben in der Ausweiskopie akzeptieren. Zwar ist es aus der Sicht des Datenschutzes wenig erfreulich, dass Unternehmen auch solche personenbezogenen Ausweisdaten speichern, die für Ihre Geschäftstätigkeit nicht ohne Weiteres erforderlich sind. Angesichts der vorgenannten Gesetzeslage müssen die Datenschutzaufsichtsbehörden aber das vollständige Kopieren des Personalausweises durch Banken im Rahmen der Identifizierung nach dem Geldwäschegesetz hinnehmen.

Bankkunden müssen zu Beginn der Geschäftsbeziehung akzeptieren, dass die Bank eine vollständige Kopie ihres Personalausweises anfertigt und aufbewahrt.

Bonitätsprüfungen in der Versicherungswirtschaft

Ebenso wie andere Unternehmen sind auch Banken und Versicherungen berechtigt, vor Abschluss eines finanziell riskanten Vertrags bei einer Auskunft eine Bonitätsauskunft zu ihrem Kunden einzuholen. Das Vorliegen der entsprechenden Risikolage ist dabei jedoch sorgfältig zu prüfen.

Holt ein Versicherungsunternehmen eine Bonitätsauskunft zu einem Kunden ein, um sich von seiner finanziellen Leistungsfähigkeit zu überzeugen, so verarbeitet es hierbei schutzwürdige personenbezogene Daten. Eine solche Verarbeitung ist nach Artikel 6 Absatz 1 lit. f DS-GVO rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Ein berechtigtes Interesse des Versicherers kommt regelmäßig nur in Betracht, wenn dieser sich durch die Bonitätsprüfung vor einem kreditorischen Ausfallrisiko schützen will, wenn er also sicherstellen will, dass er seine eigene vertragliche Leistung nicht ohne hinreichende Aussicht auf Erhalt der Gegenleistung des Kunden erbringt. Dabei ist die maßgebliche Leistung des Versicherers nicht erst die Geldleistung im Schadensfall. Vielmehr stellt bereits der abstrakte Versicherungsschutz ab Beginn der Vertragslaufzeit eine Leistung des Versicherers dar, unabhängig davon, ob es zu einem Schadensereignis und in der Folge zu einer Schadensersatzleistung seitens des Versicherers kommt. Ein überwiegendes schutzwürdiges Gegeninteresse des Versicherungsnehmers ist in der Regel nicht gegeben.

Ein finanzielles Ausfallrisiko besteht für den Versicherer jedoch nicht, wenn der

Versicherungsnehmer seine Prämienzahlung vollständig im Voraus leistet. Dies ist in der Regel der Fall bei der Haftpflichtversicherung für Mofas. Hier gilt der Versicherungsschutz nur für ein Jahr. Der Versicherungsnehmer erhält für diesen Zeitraum ein Versicherungskennzeichen, dessen Gültigkeitsdauer bereits an der Schriftfarbe eindeutig erkennbar ist. Sollte der Versicherungsnehmer daher nach Ablauf des Versicherungszeitraums ohne Haftpflichtversicherung mit dem Mofa fahren, so kommt eine Haftung des Versicherungsunternehmens nicht in Betracht. Dessen finanzielles Risiko ist daher durch die im Voraus entrichtete Prämienzahlung abgedeckt. Unter diesen Umständen hat der Versicherer kein berechtigtes Interesse daran, bei einer Auskunft eine Bonitätsauskunft zum Versicherungsnehmer abzurufen.

Die Datenschutzaufsichtsbehörde wird die Einholung von Bonitätsauskünften bei Auskunfteien weiterhin kritisch begleiten.

Scoring

Nach den Erkenntnissen der Verbraucherzentralen ist es in Zeiten der Niedrigzinsen offenbar weit verbreitet, auf Pump zu kaufen und sich dazu zu verschulden. Diese Einstellung bringt das Risiko der massiven Überschuldung mit sich. Das wiederum veranlasst die Unternehmen, sich vor Vertragsabschlüssen durch Einholen eines Scorewertes von der Kreditwürdigkeit des Vertragspartners zu überzeugen. Dieser soll mit Hilfe eines komplizierten Berechnungsverfahrens etwas über das künftige Zahlungsverhalten der betroffenen Person aussagen.

Art. 22 Absatz 2 DS-GVO lässt es zu, dass Entscheidungen über den Abschluss oder die Erfüllung eines Vertrages ausschließ-

LfDI BW - 35. Tätigkeitsbericht 2019 - 9. Arbeitswelt

lich auf der Grundlage eines automatisiert errechneten Scorewertes getroffen werden. Auch können Scorewerte zusammen mit anderen Parametern zur Gewinnung einer derartigen Prognose genutzt werden, wenn für ein solches Verfahren im konkreten Fall ein berechtigtes Interesse i. S. des Art. 6 Absatz 1 lit. f DS-GVO besteht.

Die Berechnung bzw. Nutzung eines Scorewertes ist nur rechtmäßig, wenn die Vorschriften des Datenschutzes sowohl bei den den Scorewert berechnenden Stellen, bei denen, die diesen dazu Informationen übermittelt haben, wie auch bei den Verantwortlichen, die den Scorewert letztlich nutzen, eingehalten werden bzw. eingehalten worden sind. Deswegen ist die Einbeziehung rechtswidrig verarbeiteter Daten und solcher, deren Speicherung inzwischen unzulässig geworden ist, grundsätzlich nicht erlaubt. Das betrifft insbesondere höchstpersönliche Angaben i. S. d. Art. 9 DS-GVO. Auch müssen die Angaben inhaltlich richtig sein. Problematisch ist, ob auch Daten aus sozialen Netzwerken miteinbezogen werden dürfen. Das ist allenfalls bei Informationen zu akzeptieren, die die betroffene Person selbst „für jedermann zugänglich“ ins Netz gestellt hat bzw. die Behörden und Gerichte berechtigterweise öffentlich bekanntmachen können (z. B. Schuldnerverzeichnis der Vollstreckungsgerichte nach § 882 f Absatz 1 Satz 1 Nr. 4, § 882 g Absatz 2 Nr. 2 ZPO, Entscheidungen im Insolvenzverfahren z. B. § 30 InsO).

Für die Berechnung des Scorewertes dürfen nur Daten genutzt werden, die dafür unter Zugrundelegung eines wissenschaftlich mathematisch-statistischen Verfahrens nachweislich erheblich und geeignet sind. Das Verfahren muss im Einklang mit dem Stand der Wissenschaft für die Analyse, ob die betroffene Person aufgrund ihrer Merkmale zu einer bestimmten Vergleichsgruppe, deren Bonität bekannt ist, gehört,

tauglich sein. Auch müssen die statistischen Vergleichswerte aktuell sein. Ferner muss eine ausreichende Tatsachengrundlage für die Prognose bestehen.

Die Ermittlung des Wahrscheinlichkeitswertes darf nicht maßgeblich auf sog. Anschriftendaten beruhen. Gemeint sind die Eigenschaften des Wohngebäudes (Alter und Art), sowie das Zahlungsverhalten der Bewohner der Straße und des Gebäudes, wo die betroffene Person lebt.

Trifft ein Verantwortlicher eine automatisierte Entscheidung i. S. des Art. 22 Absatz 2 lit. a DS-GVO, also ausschließlich gestützt auf einen Scorewert, kann die betroffene Person nach Art. 22 Absatz 3 DS-GVO die Überprüfung der Entscheidung einschließlich des dabei verwendeten Scorewertes unter Darlegung ihres eigenen Standpunktes durch eine natürliche Person verlangen.

Ansonsten gilt Folgendes:

Gegenüber Auskunftseien können die betroffenen Personen nach Art. 15 Absatz 1 DS-GVO, Erwägungsgrund 63, verlangen, darüber informiert zu werden, welche Daten für die Berechnung von sie betreffenden Scorewerten gespeichert sind und woher das Unternehmen diese erhalten hat (Art. 15 Absatz 1 lit. g DS-GVO). Dabei kann sich die Auskunftsei nicht damit begnügen, lediglich die Kategorie, der die gespeicherten Daten angehören, zu benennen (vgl. Art. 15 Absatz 1 lit. b DS-GVO). Nach der im Einklang mit Art. 22 Absatz 3 DS-GVO stehenden, bisher zum Scoring ergangenen Rechtsprechung des BGH besteht ein Anspruch auf Auskunft, welche konkreten Einzel-Daten gespeichert sind, damit fehlerhafte Angaben noch vor ihrer Benutzung korrigiert und Missverständnisse aufgeklärt werden können, was bei der bloßen Offenbarung

LfDI BW - 35. Tätigkeitsbericht 2019 - 9. Arbeitswelt

von Datenkategorien so nicht möglich wäre.

Nach der neueren Rechtsprechung muss auch Werturteilen ein überprüfbarer, zutreffender Tatsachenkern zugrunde liegen. Dazu müssen die Stellen, die Scorewerte berechnen oder verwenden, zumindest mitteilen, welche Umstände maßgeblich waren, dass die betroffene Person nicht als „uneingeschränkt kreditwürdig“ bewertet wurde. Außerdem ist auf Anfrage darüber zu informieren, welche Daten in bereits berechnete Scorewerte Eingang gefunden haben, an wen bislang welche Scorewerte übermittelt worden sind, weshalb die gespeicherten oder verwendeten Angaben geeignet sein sollen, einen realistischen Scorewert zu bestimmen, und welche berechtigten Interessen für die Verwendung von Informationen aus sozialen Netzwerken bestehen sollen.

Nach Art. 18 Absatz 1 DS-GVO hat die betroffene Person das Recht, gegen die für die Scorewertberechnung gespeicherten Daten bei der Auskunft Widerspruch zu erheben und zu verlangen, dass diese auf ihre Richtigkeit hin überprüft werden. Kann die Auskunft deren Richtigkeit nicht beweisen, müssen die Angaben entweder nach Art. 16 DS-GVO berichtigt oder nach Art. 17 Absatz 1 lit. d DS-GVO gelöscht werden.

Aufgrund von Art. 21 Absatz 1 DS-GVO kann die betroffene Person der Verarbeitung ihrer Daten widersprechen. Will sie das im Zusammenhang mit einer Scorewertberechnung tun, muss sie gegenüber dem Verantwortlichen substantiiert schutzwürdige Belange vortragen, die bei der Berechnung und Übermittlung eines Scorewertes verletzt werden können oder wurden. Ein Scorewert verletzt das Persönlichkeitsrecht eines Menschen bzw. dessen Recht an der ungehinderten Ausübung

seines Berufes nach Art. 12 GG, wenn die Bewertung den unzutreffenden Eindruck vermittelt, die betroffene Person sei nicht uneingeschränkt kreditwürdig, obwohl es keine Gründe für eine derartige Annahme gibt. Die betroffene Person kann geltend machen, dass das Berechnungsergebnis evident unzutreffend sei oder dass nicht aktuelle, unrichtige, einredebehaftete, für die Berechnung unzulässige oder ungeeignete Angaben bzw. bislang rechtswidrig verarbeitete Daten genutzt worden sind. Auch kann der Scorewertberechnung die sachliche Basis fehlen, wenn kein ausreichendes Datenmaterial zur Verfügung steht oder wenn wichtige relevante Tatsachen, z. B. Schuldenfreiheit – außer Acht bleiben oder geblieben sind bzw. wenn (Teil)-Werturteilen, Schätzdaten und Pauschalbewertungen keine tragfähigen Fakten zugrunde liegen. Ferner kann eingewandt werden, der Auskunftsei fehle für die Verarbeitung von Erkenntnissen aus den sozialen Netzwerken das berechtigte Interesse bzw. es würde den Anschriftendaten ein zu großes Gewicht beigemessen werden. Nicht zuletzt kann vorgetragen werden, bei der Berechnung handle es sich um ein Phantasieprodukt, weil die Auskunftsei sich nicht in der Lage sehe, das Zustandekommen der Berechnung nachvollziehbar zu erläutern. Im Falle eines derartigen Widerspruchs muss der Verantwortliche gem. Art. 21 Absatz 1 Satz 2 DS-GVO unter Widerlegung der Einwendungen beweisen, dass es akzeptable Gründe für die beanstandete Scoreberechnung gibt, welche die Interessen der betroffenen Person überwiegen.

Die Datenschutzaufsichtsbehörde wird auch künftig sehr genau darauf achten, dass die Vorgaben der EU-Datenschutzgrundverordnung bei der Berechnung und Nutzung von Scorewerten beachtet werden.

LfDI BW - 35. Tätigkeitsbericht 2019 - 9. Arbeitswelt

9.6 Einwilligungstexte und Datenschutzhinweise am Beispiel von Gewinnspielkarten und Gewinnspielen auf Internetseiten

Die Praxis der Aufsichtsbehörde zeigt, dass viele Gewinnspiele leider oftmals zum Sammeln von personenbezogenen Daten benutzt werden. Nach Art. 6 Absatz 1 Buchst. a DS-GVO wird für das Sammeln von personenbezogenen Daten auch bei Gewinnspielen die Einwilligung des Betroffenen notwendig. Daher werden die Gewinnspiele auch in der Regel mit der Einwilligung zur Werbung, z. B. direkt auf einer Postkarte, abgedruckt.

Die Einholung der Einwilligung nach Art. 7 DS-GVO richtet sich hierbei nach den Grundsätzen des Artikels 5 mit EG 39 sowie Art. 12 DS-GVO. Den Ausgangspunkt bildet somit die Transparenz der Datenverarbeitung. Ferner muss mittels geeigneter technischer und organisatorischer Maßnahmen gem. Art. 24 und 32 DS-GVO die Einwilligung zur Werbung ausreichend von der Einwilligung zur Teilnahme am Gewinnspiel abgegrenzt werden. Idealerweise kann der Kunde auswählen, zu welchen Themen er auf welchen Wegen Werbung erhalten möchte.

Die Gewinnspiele und Einwilligungen müssen daher einige Voraussetzungen erfüllen, damit die Einwilligung zur Werbung nach Art. 7 Absatz 2 DS-GVO herangezogen werden kann. Sie muss in verständlicher, leicht zugänglicher Form und in einer klaren und einfachen Sprache sowie transparent und verständlich erfolgen.

In den durchgeführten Kontrollen und zahlreichen Anfragen im Kontext von Gewinnspielen sind uns folgende datenschutzrechtlich relevanten Problemfelder aufgefallen:

Rücksendung in einem Briefumschlag:

Sobald sich personenbezogene Daten auf einer Gewinnspielkarte befinden, die über die bloße Adresse hinausgehen, sollte der Gewinnspielteilnehmer deutlich darauf hingewiesen werden, dass aus datenschutzrechtlichen Gründen ein Briefumschlag verwendet werden sollte, um unberechtigte Einsichtnahmen in die Adresse und die weiteren personenbezogenen Daten des Gewinnspielteilnehmers zu verhindern. Besser ist es natürlich, direkt einen Rückumschlag für die zurückzusendende Antwort beizulegen.

Schriftgröße:

Bei den durchgeführten aufsichtsrechtlichen Überprüfungen sind zudem zahlreiche Einwilligungen und Gewinnspiele mit einer Schriftgröße im Millimeterbereich aufgefallen. Stattdessen muss die Einwilligung zur Werbung transparent und verständlich erfolgen. Dazu gehört selbstverständlich eine angemessene – auch ohne Lupe lesbare – Schriftgröße. Laut der Norm DIN 5008 ist es zugunsten der Lesbarkeit sogar sinnvoll, im Fließtext keine Schriftgröße kleiner als 10 Punkt zu verwenden. Ein deutlicher Kontrast und eine ausreichende Schärfe, also eine schwarze, deutlich sichtbare Schrift, sind für die Lesbarkeit ebenso zwingend. Zumindest im Internet lässt sich die Schrift ja durchaus eigenhändig vergrößern.

Einwilligung in Werbung und Verlosung, gleichzeitige Einwilligung für den gesamten Werbebereich auf allen Kontaktwegen:

Das Trennungsgebot wurde durch ein Urteil des BGH (1.2.2018 – Az. III ZR 196/17) kürzlich leider aufgehoben. Zuvor konnte man (zwingend) zwischen den einzelnen Kontaktwegen und Werbefeldern auswählen. Trotzdem sollte auch nach neuer Rechtslage der Gewinnspielteilnehmer die

Möglichkeit haben, einzelne Kommunikationswege und einzelne Werbefelder zu streichen oder einzeln auswählen zu können. Oftmals soll stattdessen die Einwilligung für die Werbung gleichzeitig für SMS, Anrufe auf dem Festnetz, Anrufe auf dem Handy und Werbemails erfolgen.

Einwilligung zu Werbung und Verlosung, Rechtsverbindlichkeit:

Wenn die Einwilligungen auf der Postkarte für das Gewinnspiel von der Einwilligung in die Datenverarbeitung zu Werbezwecken nicht klar getrennt sind, ist nach Art. 7 Absatz 2 Satz 2 DS-GVO diese Einwilligung unwirksam. Eine Möglichkeit, das Gewinnspiel von der Werbeeinwilligung zu trennen, sind unterschiedliche Kästchen, die vom Gewinnspielteilnehmer angekreuzt werden können.

Die Einwilligung zur Werbung ist freiwillig:

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

Eine Einwilligung ist demnach nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht, der auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hingewiesen wurde (so bereits zum BDSG-alt: OLG Frankfurt am Main, 24.01.2018 – 13 U 165/16). Die

Einwilligung muss also stets für den konkreten Fall und in Kenntnis der Sachlage erteilt werden (BGH, Urt. v. 25.10.2012, I ZR 169/10, juris Rn. 24; zum alten Recht), um wirksam zu sein.

Weitergabe der Daten an Dritte:

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

Datenschutzhinweise für Gewinnspiele:

Im Rahmen der Datenverarbeitungen zur Durchführung des Gewinnspiels trifft die verantwortliche Stelle bereits bei Erhebung der personenbezogenen Daten die Informationspflicht des Art. 13 DS-GVO. Daher müssen die Datenschutzhinweise neben der Einwilligung abgedruckt werden. Lässt sich dies auf Grund des Umfangs etwa auf einer Postkarte nicht darstellen, ist ein Hinweis auf die Datenschutzhinweise auf der Internetseite des Anbieters (z. B. als Link) im Wege eines sog. „Medienbruchs“ nach heutiger Meinung grundsätzlich denkbar.

Für den Kunden sollte es ersichtlich sein, was mit seinen Daten geschieht und wann diese wieder gelöscht werden. Die Datenschutzhinweise zum Gewinnspiel sollten einen eigenen Abschnitt in den allgemeinen Datenschutzhinweisen der verantwortlichen Stelle erhalten.

LfDI BW - 35. Tätigkeitsbericht 2019 - 9. Arbeitswelt

9.7 Auf hoher See

Um auf gesundheitliche Probleme von Passagieren einer Kreuzfahrt vorbereitet zu sein, wollte ein Reiseveranstalter den Gesundheitszustand der Passagiere erfragen. Die Suche nach einer Rechtsgrundlage für diese Verarbeitung war schwieriger als erwartet.

Ein baden-württembergisches Reiseunternehmen, das u. a. Kreuzfahrten anbietet, wollte einige Monate vor Abfahrt des Schiffes einen Fragebogen an die Passagiere versenden, auf dem verschiedene Fragen zum Gesundheitszustand beantwortet werden sollten. Die Fragen waren teilweise offen formuliert, so wurde bspw. pauschal nach Operationen und stationären Behandlungen in den vergangenen fünf Jahren und nach regelmäßiger Medikamenteneinnahme gefragt.

Als Grund wurde angegeben, dass die Kreuzfahrt auch in abgelegene Gewässer führe und eine medizinische Evakuierung (bspw. per Hubschrauber) tagelang unmöglich sein könne. Daher sei es notwendig, den Gesundheitszustand der Reisenden vorab zu prüfen und evtl. Vorkehrungen zu treffen. Auch müsse vor Abfahrt des Schiffes geprüft werden, ob besondere Medikamente mitgeführt werden müssen. Da Gesundheitsdaten zu den besonders sensiblen Daten nach Art. 9 DS-GVO zählen, musste sowohl eine Rechtsgrundlage nach Art. 6, als auch nach Art. 9 DS-GVO vorliegen. Art. 9 Absatz 2 DS-GVO bietet hier verschiedene Möglichkeiten:

- Die Verarbeitung ist zum Zweck der Gesundheitsvorsorge auf der Grundlage des europäischen oder deutschen Rechts notwendig (zzgl. weiterer Voraussetzungen), oder

- die Verarbeitung ist zum Schutz lebenswichtiger Interessen der Person nötig und die Person kann aus körperlichen oder rechtlichen Gründen aktuell keine Einwilligung abgeben, oder
- es liegt eine Einwilligung vor.

Daneben gibt es weitere Regelungen für verschiedene Fälle, die hier jedoch keine Rolle spielten.

Unsere Prüfung ergab nun Folgendes: Eine Verarbeitung zum Zweck der Gesundheitsvorsorge lag hier sicherlich vor. Allerdings ließ sich kein (europäisches oder deutsches) Gesetz finden, das es Reiseunternehmen vorschreibt, den Gesundheitszustand ihrer Kunden zu überprüfen. Auch Nachfragen beim Seeärztlichen Dienst in Hamburg und einer Reederei ergaben hier keine weiteren Erkenntnisse.

Zwar ist das Reiseunternehmen verpflichtet, seinen Kunden „in Schwierigkeiten [...] Beistand zu gewähren“ (§ 651q BGB), dies bedeutet aber nicht, dass sich hieraus bereits eine Pflicht für den Kunden ergibt, Gesundheitsdaten preiszugeben. Ausreichend wäre es vielmehr, wenn der Kunde vor Reisebeginn die Möglichkeit hat, freiwillig bestimmte Angaben zu machen.

Auch die zweite Möglichkeit war hier nicht anwendbar. Möglicherweise ließe sich argumentieren, dass die Verarbeitung zum Schutz lebenswichtiger Interessen nötig wäre. Allerdings sind die Passagiere durchaus in der Lage, eine Einwilligung abzugeben (wenn sie es denn möchten), da sie weder ohnmächtig sind, noch eine besondere rechtliche Situation vorliegt. Eine besondere Notlage, bei der man auf eine Einwilligung verzichten könnte, liegt hier also nicht vor.

Als einzige Rechtsgrundlage blieb somit die Einwilligung nach Art. 9 Absatz 2 Buchstabe a DS-GVO übrig. Das Reiseunternehmen hat sich bereit erklärt, dies so umzusetzen.

Abschließend sei darauf hingewiesen, dass Reiseunternehmen darauf achten sollten, ihre Kundschaft vorab über mögliche Gesundheitsgefahren aufzuklären und Hilfe, Beratung oder sonstige Unterstützung anzubieten. Ob und in welchem Ausmaß man dieses Angebot in Anspruch nimmt, bleibt dann aber jedem selbst überlassen.

Wenn ein Reiseunternehmen vor einer Kreuzfahrt Gesundheitsdaten der Passagiere erheben möchte, kommt als Rechtsgrundlage aktuell nur eine freiwillige und informierte Einwilligung (Art. 6 Absatz 1 S. 1 Buchstabe a in Verbindung mit Art. 9 Absatz 2 Buchstabe a DS-GVO) in Frage.

9.8 Neues aus dem Bereich internationaler Datenverkehr

Die DS-GVO ergänzt die bereits aus dem bisherigen Recht bekannten Instrumente für einen Transfer personenbezogener Daten in Länder außerhalb der EU (Drittländer) um neue Ansätze und Instrumente. Themen aus den Vorjahren setzten sich fort, etwa der EU-US Privacy Shield.

Nach wie vor erreichen uns immer wieder Beratungsanfragen zu folgender Konstellation aus dem Bereich der internationalen Auftragsdatenverarbeitung: Ein Verantwortlicher in der EU oder dem europäischen Wirtschaftsraum (EWR) beauftragt einen Auftragsverarbeiter in der EU oder dem EWR, der seinerseits einen Unterauftragsverarbeiter in einem Drittstaat einschalten möchte. Die Standardvertragsklauseln der europäischen Kommission für

die Übermittlung von einem Verantwortlichen in der EU an einen Auftragsverarbeiter in einem Drittland (Beschluss 2010/87/EU-Standardvertrag für Auftragsdatenverarbeiter LINK) sind zwar übergangsweise bis zur Änderung oder Aufhebung durch die Kommission weiter anwendbar (Artikel 46 Absatz 5 Satz 2 DS-GVO), erfassen diese Konstellation jedoch nicht. Stattdessen setzen sie voraus, dass ein Verantwortlicher in der EU einen Auftragsverarbeiter in einem Drittstaat unmittelbar selbst beauftragt. Für einen genehmigungsfreien Transfer personenbezogener Daten in der eingangs geschilderten Konstellation ist es deshalb erforderlich, dass der Verantwortliche in der EU die Auftragsverarbeiter im Drittstaat selbst beauftragt und mit diesen – gegebenenfalls vertreten durch weitere Auftragsverarbeiter in der EU – den Standardvertrag für Auftragsdatenverarbeiter abschließt.

Zur Auslegung der Fallgruppen des Artikels 49 der DS-GVO (z. B. Drittstaaten-transfer auf der Grundlage einer Einwilligung des Betroffenen oder zur Wahrung zwingender berechtigter Interessen des Verantwortlichen) gibt es zwischenzeitlich ein Arbeitspapier des Datenschutzausschusses, das wertvolle Hinweise zur Auslegung des Artikel 49 enthält (Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679).

Verbindliche interne Datenschutzvorschriften (engl.: binding corporate rules bzw. BCR) erfreuen sich stetig wachsender Beliebtheit als Instrument zum Transfer personenbezogener Daten in Drittstaaten innerhalb einer Unternehmensgruppe. Die DS-GVO sieht vor, dass BCR im Kohärenzverfahren durch den Datenschutzausschuss von allen europäischen Aufsichtsbehörden behandelt werden. Um dem Rechnung zu tragen, wurde das bis-

LfDI BW - 35. Tätigkeitsbericht 2019 - 9. Arbeitswelt

lang vereinbarte informelle Verfahren der gegenseitigen Anerkennung angepasst. Sämtliche Datenschutzaufsichtsbehörden und das Sekretariat des europäischen Datenschutzausschusses erhalten nunmehr den Entwurf der BCR mit der Gelegenheit zur inhaltlichen Prüfung bereits vor Eröffnung des eigentlichen Kohärenzverfahrens. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg hat im Berichtszeitraum als federführende Aufsichtsbehörde und als Co-Prüfer an mehreren BCR-Verfahren mitgewirkt.

Die DS-GVO sieht in Artikel 46 Absatz 2 lit. e und f mit genehmigten Verhaltensregeln und genehmigten Zertifizierungsmechanismen neue Instrumente für einen Drittstaatentransfer vor, die der europäische Datenschutzausschuss zurzeit durch die Erstellung entsprechender Arbeitspapiere noch mit Leben erfüllt. Am 23. Januar 2019 hat die europäische Kommission nach Beteiligung des Datenschutzausschusses eine Angemessenheitsentscheidung für Japan erlassen. Die dritte gemeinsame Überprüfung der Angemessenheitsentscheidung für die USA (EU-US Privacy Shield) durch die europäische Kommission und die amerikanische Seite unter Beteiligung der europäischen Aufsichtsbehörden im Herbst dieses Jahres hat einerseits Fortschritte ergeben – so finden etwa von Seiten der amerikanischen Aufsicht vermehrt anlassunabhängige Kontrollen bei den (selbst) zertifizierten amerikanischen Unternehmen statt –, andererseits gibt es weitere zahlreiche offene Fragen und erheblichen Verbesserungsbedarf. So hat etwa die europäische Seite bislang keinen Zugang zu sämtlichen Informationen und Dokumenten, die eine belastbare Aussage über das Funktionieren der Rechtschutzmechanismen für Betroffene aus Europa erlauben würden.

Das kommende Jahr verspricht gerade in Bezug auf den internationalen Datentransfer spannend zu werden. Ende 2016 hatten eine irische und zwei französische Bürgerrechtsorganisationen Klagen gegen die Angemessenheitsentscheidung der EU-Kommission zum EU-US Privacy Shield erhoben. Während eine dieser Klagen zwischenzeitlich als unzulässig abgewiesen wurde (Digital Rights Ireland, Az. T-670/16), ist die Klage von La Quadrature du Net (Az. T 738/16) noch anhängig. Ebenfalls 2016 brachte die irische Datenschutzaufsichtsbehörde die Standardvertragsklauseln der EU-Kommission für Auftragsdatenverarbeiter vor das zuständige irische Gericht (High Court). Der High Court legte Mitte 2018 dem Europäischen Gerichtshof (EuGH) Fragen zu den Standardvertragsklauseln vor (Vorabentscheidungsersuchen vom 9. Mai 2018, Az. C-311/18). Diese beziehen sich auf den Einsatz der Standardvertragsklauseln für Datenübermittlungen in die USA. Auch in diesem Verfahren ist in absehbarer Zeit mit einem Urteil, das möglicherweise weitreichende Aussagen zur Zulässigkeit des Datentransfers in Drittstaaten enthalten wird, zu rechnen. Nicht unwahrscheinlich, dass allen Beteiligten ein „Safe Harbor II“ droht ...

Der im März 2018 durch den US-Kongress verabschiedete sogenannte Cloud Act erlaubt es US-amerikanischen Strafverfolgungsbehörden unter bestimmten Voraussetzungen, die Offenlegung von außerhalb der USA gespeicherten Kundendaten durch US-Provider zu verlangen. Der europäische Datenschutzausschuss hat am 10. Juli 2019 eine erste Stellungnahme und rechtliche Einschätzung zu den Auswirkungen des Cloud Act auf die Datenverarbeitung in Europa vorgelegt. Danach liegen bei auf den Cloud Act gestützten Herausgabeverlangen, die nicht auf eine wirksame internati-

LfDI BW - 35. Tätigkeitsbericht 2019 - 9. Arbeitswelt

onale Übereinkunft wie etwa ein Rechtshilfeabkommen gestützt werden können, die Voraussetzungen für einen Drittstaaten-transfer nach dem 5. Kapitel der DS-GVO sowie die allgemeinen datenschutzrechtlichen Anforderungen an die Rechtmäßigkeit der Datenverarbeitung, insbesondere nach Artikel 6 DS-GVO, allenfalls in Ausnahmefällen vor.

Datenübermittlungen in Drittländer sind mit Risiken für die informationelle Selbstbestimmung der Betroffenen verbunden. Deshalb sollten datenverarbeitende Stellen sorgfältig prüfen, ob sie Leistungen in Anspruch nehmen, die mit einem Transfer personenbezogener Daten in Länder außerhalb der EU und des europäischen Wirtschaftsraums verbunden sind. In jedem Fall empfehlen wir bei einem Transfer in Drittstaaten dringend, für die technisch-organisatorischen Sicherheitsmaßnahmen höchste Standards, z. B. eine starke Verschlüsselung, zugrunde zu legen und Datenschutzerklärungen über die Art und Weise und den Umfang vorgesehener Datenverarbeitungen in Drittländern sorgfältig zu lesen. Bleiben insoweit offene Fragen, raten wir von der Nutzung solcher Angebote ab.



LfDI BW - 35. Tätigkeitsbericht 2019 - 9. Arbeitswelt

10. Aus der Dienststelle

10.1 Aus der Dienststelle

Im letzten Tätigkeitsbericht hatte ich die Herausforderungen dargestellt, welche das Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO) sowie das Inkrafttreten des Landesdatenschutzgesetzes für die Dienststelle als solche und insbesondere auch für die Mitarbeiter*innen mit sich brachten. Mittlerweile haben wir uns zwar weitgehend konsolidiert und sind auf allen Gebieten arbeitsfähig.

Dies bedeutet aber nicht, dass wir uns nun gemütlich zurücklehnen könnten. Neben den in den Fachreferaten nach wie vor hohen Fallzahlen, die zeitgerecht abzuarbeiten den Kolleg*innen alles abverlangt, war auch in den Bereichen Personal, Haushalt und Organisation von ‚business as usual‘ überhaupt keine Rede.

Mein Ziel, für mehr Fluktuation beim Personal zu sorgen, damit die Kolleg*innen auch die Welt außerhalb des Datenschutzes kennenlernen und, neben der persönlichen Entwicklung, so unter anderem auch die Voraussetzungen für die Übernahme von Führungsfunktionen schaffen, wurde schneller und umfangreicher erfüllt als erwartet. Das hängt sicherlich auch damit zusammen, dass der Datenschutz in Zeiten der Digitalisierung mittlerweile einen anderen Stellenwert bekommen hat – und wohl auch mit unserer besseren „Sichtbarkeit“. Da ist es kein Wunder, dass auch andere Stellen auf uns und unsere Arbeit aufmerksam werden – und versuchen, an unserem Know-how (und leider auch an unserem hervorragenden „Personalkörper“) zu partizipieren. Abordnungen an Bundesministerien und in die Verwaltungsgerichtsbarkeit sowie Versetzungen an Hochschulen und andere Landesbehörden zeigen, dass hier ein Mentalitätswandel bei den anderen öffentlichen Stellen, aber natürlich auch bei den Beschäftigten der Dienststelle eingetreten ist. So ungern ich die Kolleginnen und Kollegen ziehen lasse – für die Betroffenen freut mich das natürlich auch, und ich sehe darin die Chance, unsere hier gewonnene Datenschutzkompetenz mittels solcher Multiplikatoren in die Fläche zu tragen – eine ‚win-win-Situation‘!

Wie die Landesverwaltung insgesamt spüren auch wir immer deutlicher die Entwicklungen auf dem Arbeitsmarkt, auf dem der öffentliche Dienst mit der Wirtschaft um die besten Köpfe konkurriert. Dabei zeigt sich aber, dass das Interesse am Thema Datenschutz, nicht zuletzt auch befeuert durch die Datenschutz-Grundverordnung, manche*n doch dazu führt, lukrative private Angebote zugunsten einer spannenden und verantwortungsvollen Aufgabe auf einem gesellschaftlich relevanten Gebiet des öffentlichen Rechts auszuschlagen – acht Neueinstellungen konnte die Dienststelle im Jahr 2019 verzeichnen. Und damit sind wir komplett besetzt.

Mit Blick darauf, dass der Landtag meiner Dienststelle mit dem Doppelhaushalt 2020/2021 erneut 10 Stellen zugesprochen hat, wofür ich außerordentlich dankbar bin, bin ich optimistisch, weitere Kolleg*innen für die Mitarbeit an dieser Aufgabe gewinnen zu können.

LfDI BW - 35. Tätigkeitsbericht 2019 - Aus der Dienststelle

Apropos Haushalt: Meinem vielfach geäußerten Wunsch, die meiner Dienststelle zur Verfügung stehenden bescheidenen Sachmittel weiter strukturell zu erhöhen, ist der Landtag jetzt nachgekommen. Um 75.000 EUR wurde der Ansatz erhöht, für die Jahre 2020/2021 zudem um jeweils zusätzlich 20.000 EUR aufgestockt. Dies macht es nun möglich, dringend benötigte Investitionen auf verlässlicher Basis tätigen zu können. Des Weiteren wurde die Personalausgabenbudgetierung eingeführt, welche die dezentrale Budgetverantwortung auf den Bereich der Personalausgaben erweitert und zusätzliche Flexibilisierungsmöglichkeiten schafft. Das werden wir intensiv nutzen.

Daneben wurden wir mit Blick auf den 2020 ins Haus stehenden Umzug in neue Räumlichkeiten ausreichend mit entsprechenden Sachmitteln bedacht. Damit können die Dienst- und Veranstaltungsräume im neuen Domizil modern und beschäftigtenfreundlich ausgestattet werden. Sicher trägt dies zur Steigerung der Motivation der Kolleg*innen bei, zumal die durch den stetigen Personalzuwachs entstandene Raumsituation mittlerweile an der Grenze des Zumutbaren angelangt ist.

Auch organisatorisch hat sich einiges getan. Zur Vorbereitung auf die Einführung der landeseinheitlichen E-Akte BW in der Dienststelle wurde die Einführung des landeseinheitlichen Aktenplans als Voraussetzung hierfür vorgebracht. Die Umsetzung, die nun im Januar 2020 erfolgt, beschleunigt zudem die Prozesse in der Registratur der Dienststelle, die durch die hohen Fallzahlen besonders belastet ist. Deren Entlastung durch Veränderungen in der Ablauforganisation, insbesondere auch durch digitale Maßnahmen, war ein weiterer Schwerpunkt der Arbeit im organisatorischen Bereich.

Insgesamt macht die Digitalisierung also auch vor meiner Dienststelle nicht Halt. Die Beteiligungsprozesse intern wurden so umgestellt, dass sie papierlos erfolgen können, die Telearbeit wurde institutionalisiert und ausgebaut, zuletzt auch das mobile Arbeiten eingeführt. Des Weiteren wurden das Angebot an elektronischen Verwaltungsleistungen auf der Homepage der Dienststelle erweitert und erste Vorbereitungen für die Migration der IuK der Dienststelle zur IT Baden-Württemberg (BITBW) getroffen, die im Jahr 2020 beginnen und bis Q1/2021 abgeschlossen sein soll.

Auch sonst hat sich die Dienststelle der Landesverwaltung weiter zugewandt und nimmt an den bestehenden interministeriellen Arbeitsgruppensitzungen zu Querschnittsthemen teil. Den Austausch empfinde ich als sehr gewinnbringend und möchte mich an dieser Stelle bei den Ministerien dafür bedanken, dass die Dienststelle und ihre Belegschaft so offen im Kreis der Obersten Landesbehörden aufgenommen wurden. Wir werden uns auch bei diesen Stellen konstruktiv und hilfreich einbringen.

Unsere Dienststellenstatistik finden Sie im Anhang.

10.2 Presse- und Öffentlichkeitsarbeit

*Meine Stelle für Presse- und Öffentlichkeitsarbeit informierte auch im Berichtsjahr wieder zum einen Datenschutz- und Informationsfreiheitsinteressierte über aktuelle und öffentlich relevante Themen. Zum anderen ist sie der zentrale Ansprechpunkt für Journalist*innen um aktuelle Fragen zu beantworten. Aber auch Anfragen aus der Bevölkerung, insbesondere dann, wenn datenschutzrechtliche Themen die Schlagzeilen beherrschen, werden hier beantwortet.*

Pressearbeit



Die in den letzten Jahren weiter ansteigende Zahl von Anfragen der Medien, seien es Interviewanfragen, datenschutzrechtliche Fragen oder die Bitte um eine aktuelle Stellungnahme, belegt die steigende Bedeutung des Datenschutzes. Dabei nimmt nicht nur die Zahl der Anfragen kontinuierlich zu, immer breiter wird auch das Themenspektrum, zu dem meine Dienststelle um Auskunft oder Stellungnahme gebeten wird. Diese bezogen sich in erster Linie auf Fragen zu Bußgeldverfahren, Anzahl der Beschwerden und Anfragen, Evaluation der DS-GVO, Patientendatenschutz sowie Hackerangriffen.

Pressemitteilungen datenschutzbezogener Themen sowie Veranstaltungen wurden auch im Berichtsjahr der Öffentlichkeit durch Pressemitteilungen bekanntgegeben. In Bezug auf die Pressemitteilungen war vor allem die Ergebnisse der Kommunalumfrage ein wichtiges Thema, aber auch Mitteilungen zur Künstlichen Intelligenz (KI), das erste Bußgeld gegen einen Polizeibeamten sowie unsere Kontrollmaßnahmen haben zu einem großen Presseecho geführt.

Zudem fanden am 4. Februar 2019 und am 4. November 2019 Pressekonferenzen statt. Die thematischen Aufhänger waren jeweils die Vorstellung des 34. Datenschutz-Tätigkeitsberichts sowie die Vorstellung der Ergebnisse der Datenschutz-Umfrage bei den Gemeinden in Baden-Württemberg.

LfDI BW - 35. Tätigkeitsbericht 2019 - Aus der Dienststelle



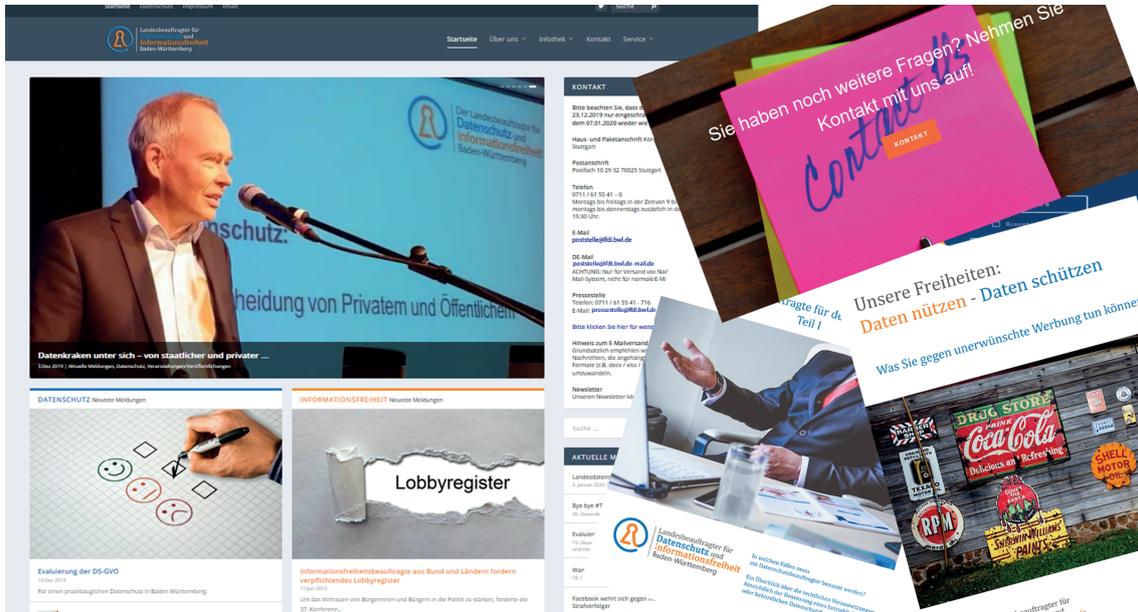
Datum	Name
04.11.	Ergebnisse der kommunalen Datenschutz-Umfrage des LfDI liegen vor Ergebnisse der Kommunalumfrage Präsentation der Ergebnisse der Kommunalumfrage Broschüre Gemeinden (Stand Dezember 2019)
09.10.	Zum Einsatz von Cookies und Cookie-Bannern
09.09.	Datenschutzbeauftragte stärken Unternehmen
19.08.	Künstliche Intelligenz – und ihre Folgen
31.07.	Gemeinden in Baden-Württemberg benötigen mehr Unterstützung bei der Umsetzung des Datenschutzes
30.07.	Datenschutzverletzungen bereiten zunehmend Sorge
28.06.	Datenpannen bei Melderegisterauskünften
18.06.	Erstes Bußgeld gegen Polizeibeamten
03.06.	Kino-Session mit dem Landesbeauftragten
24.05.	Die ersten IFG-Days Baden-Württemberg
22.04.	Mehr Licht! – Gemeinsame Verantwortlichkeit sinnvoll gestalten
09.04.	Transparenz schützt Wissenschaftsfreiheit
08.04.	Kontrollmaßnahmen zur DSGVO stehen fest
20.03.	Diskussion mit Bundesjustizministerin Katarina Barley
11.03.	Schulstunden der etwas anderen Art
28.02.	LfDI Baden-Württemberg verhängt Bußgeld gegen früheren Juso-Landeschef

LfDI BW - 35. Tätigkeitsbericht 2019 - Aus der Dienststelle

14.02.	Studierende entwickeln Lösungen für den Datenschutz
11.02.	Keep cool beim kalten Brexit
04.02.	LfDI Dr. Stefan Brink stellt den 34. Tätigkeitsbericht zum Datenschutz vor
30.01.	Bundesweite Kooperation der Aufsichtsbehörden unterstützt BvD-Initiative
22.01	Aufräumen nach dem Polit-Hack

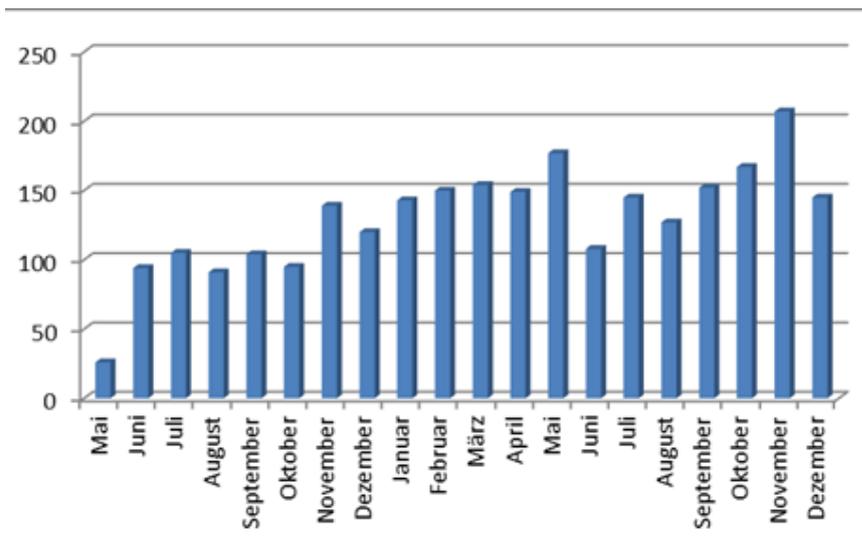
LfDI BW - 35. Tätigkeitsbericht 2019 - Aus der Dienststelle

Internetauftritt



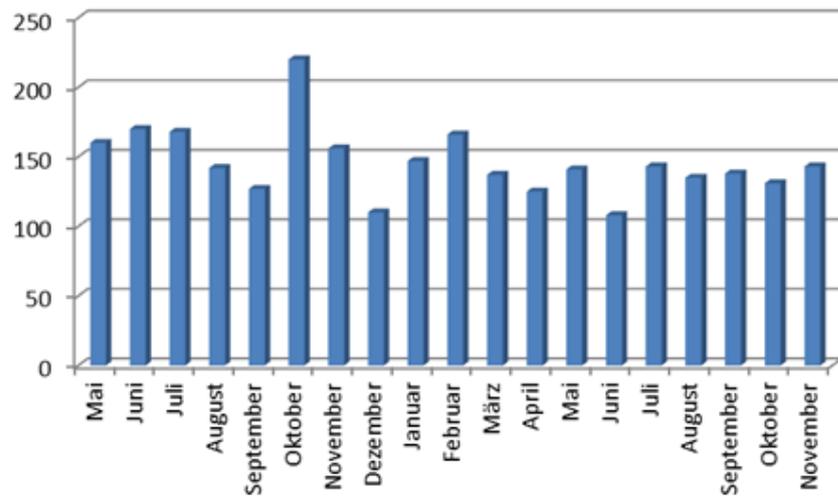
Der Internetauftritt meiner Dienststelle wird offensichtlich bundesweit genutzt und lässt, nach Rückäußerungen der Nutzer, den Schluss zu, sehr geschätzt zu sein. Neben dem Abruf von aktuellen Informationen, Broschüren und Merkblätter werden vor allen Dingen auch unserer Kontaktformulare rege genutzt:

Eingangszahlen Online-Beschwerdeformular:



LfDI BW - 35. Tätigkeitsbericht 2019 - Aus der Dienststelle

Eingangszahlen „Meldung einer Verletzung des Schutzes personenbezogener Daten nach Art. 33 DS-GVO“ Mai 2018 bis Dezember 2019:



Kontaktdaten der Datenschutzbeauftragten:

Seit Mai 2018 wurden meiner Dienststelle per Online-Formular ca. 32.000 Kontaktdaten von Datenschutzbeauftragten gemeldet.

FAQs



Damit Sie sich schnell und unkompliziert einen Überblick über unsere Themen verschaffen können, haben wir in einer Extra-Rubrik auf unserer Webseite oft gestellte Fragen mit den dazugehörigen Antworten zusammengefasst:

- [Datenschutz in der Arztpraxis](#)
- [Cookies und Tracking](#)
- [Fotografieren und Datenschutz – Wir sind im Bild!](#)
- [Informationsfreiheit](#)
- [Kommunen](#)
- [Datenschutz in der Pflege](#)

LfdI BW - 35. Tätigkeitsbericht 2019 - Aus der Dienststelle

- [Sozialleistungen](#)
- [Vereine](#)
- [Veröffentlichung von Fotos speziell für Vereine](#)

Dieser Abschnitt wird regelmäßig um weitere FAQs ergänzt. Es lohnt sich daher, hier immer wieder vorbeizuschauen.

Newsletter

LANDESBEAUFTRAGTER FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT BADEN-WÜRTTEMBERG

NEWSLTR

Der Newsletter meiner Dienststelle wird mehrmals im Jahr publiziert und hat in der Zwischenzeit über 3.500 Abonnent*innen.

Der Newsletter kann hier abonniert werden:

<https://www.baden-wuerttemberg.datenschutz.de/newsletter-anmeldung/>

Publikationen

Im zurückliegenden Zeitraum wurden wieder wichtige neue Broschüren und Muster veröffentlicht. Auf meinem Internetauftritt findet man unter der Rubrik „Infothek“ zahlreiche verschiedene Materialien mit Erläuterungen, Definitionen und Hinweisen zu den einzelnen Vorschriften und deren Umsetzung.

Besonders empfehlen möchte ich die Lektüre der folgenden Ratgeber meiner Dienststelle:

- [Broschüre „Auftragsverarbeitung nach DS-GVO“](#)
- [Broschüre „Betroffenenrechte“](#)
- [Praxisratgeber „Der Beauftragte für den Datenschutz“ – Teil I und Teil II](#)
- [Broschüre „Fotografieren und Datenschutz – Kompakt und praxisorientiert“](#)
- [Ratgeber zum Beschäftigten-Datenschutz](#)
- [Orientierungshilfe „Datenschutz im Verein nach der DS-GVO“](#)
- [Praxisratgeber für Vereine](#)
- [Videoüberwachung durch öffentliche Stellen in Baden-Württemberg](#)
- [Broschüre „Was Sie gegen unerwünschte Werbung tun können“](#)

Für Ihr Feedback zu unserer Presse- und Öffentlichkeitsarbeit haben wir immer ein offenes Ohr! Mein Team wird unter der E-Mail-Adresse pressestelle@lfdi.bwl.de die Kommentare aufgreifen, zu den Vorschlägen und Anregungen Stellung nehmen und Fragen beantworten. Wir wollen unser digitales Angebot mit der Unterstützung der Nutzer nicht nur gut, sondern besser machen.

LfDI BW - 35. Tätigkeitsbericht 2019 - Aus der Dienststelle

Informationen zur Dienststelle

Aufbau der Dienststelle

Die Dienststelle des Landesbeauftragten für den Datenschutz und die Informationsfreiheit verfügt über 53,5 Planstellen und ist in sechs Referate und die Stabsstelle Europa gegliedert. Die jeweiligen Leiter/-innen und ihre Themenschwerpunkte sind der nachstehenden Übersicht zu entnehmen. Bitte wenden Sie sich bei Anfragen an unsere Telefonzentrale (0711 / 61 55 41 – 0).



Telefonzentrale: 0711 / 61 55 41 - 0

Die Telefonzentrale ist montags bis freitags in der Zeit von 9 bis 12 Uhr und montags bis donnerstags zusätzlich in der Zeit von 14 bis 15:30 Uhr besetzt.

Telefax: 0711 / 61 55 41 - 15

E-Mail: poststelle@lfdi.bwl.de

LfDI BW - 35. Tätigkeitsbericht 2019 - Aus der Dienststelle

Dienststellenstatistik

Bezeichnung	2016	2017	2018	2019
Beschwerden				
– öffentlicher Bereich	840	1186	1188	972
– nicht-öffentlicher Bereich	1208	1872	2714	2785
Kontrollen				
– öffentlicher Bereich	12	23	5	39
– nicht-öffentlicher Bereich	4	32	8	72
Beratungen				
– öffentlicher Bereich	878	991	1492	1289
– nicht-öffentlicher Bereich	637	795	2948	2553

LfDI BW - 35. Tätigkeitsbericht 2019 - Anhang

Tabellen zu Beitrag 1.6 „E-Mail-Werbung nach § 7 Absatz 3 UWG“

Beispiele bzgl. Waren:

Gekaufte Ware	Waren mit entsprechenden typischen Einsatz- und Verwendungsmöglichkeiten	Klassisches Zubehör oder Ersatzteile	Verkehrsübliche Ergänzungsware
Herrenschuh	Andere Herrenschuhe	Einlegesohle, Schnürsenkel	Schuhputzmittel
Kinderfahrrad	Dreiräder, Roller, Laufräder	Kinder-Fahrradhelme, Luftpumpen, Fahrradkörbe	Fahrradversicherung, Diebstahlschutz, Fahrradfinanzierung
Damen-Wintermantel	Damen-Winterjacken	---	Handschuhe, Schal, Mütze
Laserdrucker	Tintenstrahldrucker	Farbkartuschen	Papier
Eintrittskarte für eine Oper	Eintrittskarten für klassische Musik und Ballett	---	Fahrkarte, Kartengutscheine
			
E-MAIL-WERBUNG NACH § 7 ABS. 3 UWG ZULÄSSIG			

Beispiele bzgl. Dienstleistungen:

Erbrachte Dienstleistung	Dienstleistungen mit entsprechenden, typischen Leistungszielen	Klassisches Zubehör	Verkehrsübliche Zusatz- oder Ergänzungsdienstleistungen
Druck von Visitenkarten (online)	Druck von Briefpapier oder Briefumschlägen	Visitenkartenetui, Visitenkartenständer	Personalisiertes Bedrucken von Gegenständen
Onlinebuchung Pauschalreise nach Nizza (Flug, Hotel)	Pauschalreisen nach Frankreich	Reiserücktrittsversicherung	Mietwagen, Ausflugsapakete
Online-Handy-Vertrag	Andere Telekommunikations-Verträge	Handy, Ladekabel, Musik- oder Filmflat, Handysersatzteile	Handyversicherung
Online-Mietwagen-Vertrag	Andere Mietwagen-Verträge	Miete Navigationsgerät, Miete Kindersitz	Hotelübernachtung
Online-Fotoentwicklung (auf Papier)	Andere Fotoentwicklungen	Fotoalbum, Fotokleber	Druck von Fotobüchern, Postern, Kalendern
			
E-MAIL-WERBUNG NACH § 7 ABS. 3 UWG ZULÄSSIG			

LfDI BW - 35. Tätigkeitsbericht 2019 - Anhang

Tabellen zu Beitrag 1.9 „Technisch-organisatorischer Datenschutz“

	Überwachen	Detektieren	Beobachten	Erkennen	Identifizieren	Überprüfen
Punktdichte (mm/Pixel)	80	40	16	8	4	1
						

Die einzelnen Kategorien sind nach der DIN EN 62676-4 (<https://www.din.de/de/service-fuer-anwender/din-term>) wie folgt definiert:

Überwachen	Ermöglicht das Anschauen der Anzahl, Ausrichtung und Geschwindigkeit von Bewegungen von Menschen über einen großen Bereich, vorausgesetzt, ihre Anwesenheit ist der Bedienperson bekannt.
Detektieren	Ermöglicht der Bedienperson, zuverlässig und leicht zu ermitteln, ob irgendein Ziel, wie z. B. eine Person, anwesend ist oder nicht.
Beobachten	Ermöglicht es, charakteristische Einzelheiten von Individuen, wie z. B. auffällige Kleidung, zu sehen, während eine Ansicht von Aktivitäten im Umfeld eines Vorfalles gewährt wird.
Erkennen	Ermöglicht der Bedienperson das Erkennen eines Individuums.
Identifizieren	Ermöglicht die zweifelsfreie Identifizierung eines Individuums.
Überprüfen	Ermöglicht auch bei schwierigen Kontrastverhältnissen die zweifelsfreie Identifizierung eines Individuums.

LfDI BW - 35. Tätigkeitsbericht 2019 - Anhang

Ergebnisse der Anhörung
des Landesbeauftragten für den Datenschutz und die
Informationsfreiheit Baden-Württemberg
vom 28. Juni 2019 bei der IHK Stuttgart
zur
Evaluierung der DS-GVO

-

„Wenn es nicht sinnvoll ist, dann ist es kein Datenschutz.“

- Für einen praxistauglichen Datenschutz in Baden-Württemberg -

LfDI BW - 35. Tätigkeitsbericht 2019 - Anhang

Inhalt

Vorwort	3
1. Informations-, Auskunft- und Transparenzpflichten	5
Lösungsansätze.....	6
2. Verarbeitungsverzeichnis	7
Lösungsansätze.....	7
3. Benennungspflicht von Datenschutzbeauftragten.....	8
Lösungsansätze.....	9
5. Herstellerhaftung - „privacy by design“	10
Lösungsansätze.....	11
5. Unklarheiten bei der Gemeinsamen Verantwortlichkeit, insbesondere im „social media“-Bereich	12
Lösungsansätze.....	12
Fazit	14

LfDI BW - 35. Tätigkeitsbericht 2019 - Anhang

Vorwort

Seit dem 25. Mai 2018 ist der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW) gesetzlich dazu verpflichtet, die Einhaltung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, kurz: die Datenschutz-Grundverordnung - DS-GVO in Baden-Württemberg zu beaufsichtigen und die Verantwortlichen im Lande zu beraten.

Art. 97 Abs. 1 DS-GVO sieht vor, dass die EU-Kommission dem EU-Parlament und dem Rat bis zum 25. Mai 2020 einen Bericht über die Bewertung und Überprüfung der DSGVO vorlegt. Art. 97 Abs. 3 DS-GVO gibt der Kommission hierfür das Recht, Informationen unter anderem auch von den Aufsichtsbehörden anzufordern. Hierzu möchte auch der LfDI Baden-Württemberg seine Einschätzungen, welche aus der bisherigen praktischen Erfahrung seiner unabhängigen obersten Landesbehörde resultieren, zur Kenntnis geben und nimmt die Gelegenheit wahr, Anregungen zur Evaluierung der DS-GVO zu unterbreiten.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz - DSK) hat sich mit ihrem „Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden“ vom 06. November 2019, welche vom LfDI Baden-Württemberg mitgetragen wurde, bereits mit dem aus ihrer Erfahrung mit der Anwendung der DS-GVO resultierenden Änderungsvorschlägen an den Europäischen Datenschutzausschuss gewandt. Den Vorsitz des eigens hierzu eingesetzten Projekt-Arbeitskreises der DSK hatte der LfDI Baden-Württemberg inne.

Die Sicht der Aufsichtsbehörden ist sicherlich wichtig und für die EU-Kommission hilfreich – nicht wenig wichtig sind aber die Erfahrungen, welche die Verantwortlichen und Anwendenden der DS-GVO in Baden-Württemberg gesammelt haben – buchstäblich am eigenen Leibe. Um diesen Erfahrungen Rechnung zu tragen, hat der LfDI Baden-Württemberg am 28. Juni 2019 eine Anhörung unter dem Banner „#DSGVO wirkt (?) – 1 Jahr DSGVO – Praxiserfahrungen und Evaluation“ in Zusammenarbeit mit der Industrie- und Handelskammer Region Stuttgart veranstaltet. Zu Impulsvorträgen geladen waren Vertretungen aus Aufsicht, Behörden, Wirtschaft, Wissenschaft, Anwaltschaft, Verbänden und Datenverarbeitern. In einem eigens hierzu eingerichteten E-Mail-Postfach wurden außerdem über das ganze Jahr Zuschriften aus allen Bereichen des Landes gesammelt und ausgewertet – auch von dieser „niedrigschwelligen“ Möglichkeit, Kritik und Anregungen zur DS-GVO abzugeben, haben zahlreiche Institutionen wie Verbände und Vereine, aber auch viele Privatpersonen Gebrauch gemacht.

Der Kreis der Verantwortlichen in Baden-Württemberg ist mit dem Bundesdurchschnitt nur teilweise vergleichbar. Laut Ministerium für Wirtschaft und Finanzen Baden-Württemberg erwirtschaften beispielsweise kleine und mittlere Unternehmen jeden zweiten Euro Umsatz im Land und beschäftigen zwei Drittel der sozialversicherungspflichtigen Beschäftigten. Der Mittelstand ist damit das Rückgrat der Wirtschaft in Baden-Württemberg - und trägt in entscheidendem Maße zur wirtschaftlichen Entwicklung bei. Außerdem engagiert sich einem Bericht des Ministeriums für Soziales und Integration Baden-Württembergs zufolge fast jeder zweite Baden-Württemberger in seiner Freizeit ehrenamtlich in Vereinen und Verbänden: über 48 Prozent der Bürgerinnen und

LfDI BW - 35. Tätigkeitsbericht 2019 - Anhang

Bürger tun dies. Baden-Württemberg ist damit bundesweit Spitzenreiter. Daraus ergeben sich auch ganz eigene, spezifische Herausforderungen und Anliegen an einen praxistauglichen Datenschutz. Diese landesspezifischen Erkenntnisse sollen - neben dem Erfahrungsbericht der DSK - einen Beitrag zur Evaluation der DS-GVO durch den europäischen Gesetzgeber bieten.

Insgesamt hat sich gezeigt, dass die Verantwortlichen in Baden-Württemberg sich in vielen Bereichen alltagstauglichere Lösungen wünschen und einige Vorschriften nur schwer auf datenverarbeitenden Tätigkeiten kleiner Unternehmen oder ehrenamtlicher Arbeit anwendbar sind. Im Vordergrund stehen vor allem Fragen rund um eine mögliche Entlastung bei den Informations-, Transparenz- und Auskunftspflichten, aber auch bei Fragen der Gemeinsamen Verantwortlichkeit und der Auftragsdatenverarbeitung. Trotz zahlreicher Muster und Praxisratgeber meiner Dienststelle und anderen Aufsichtsbehörden scheint hier immer noch eine gewisse Rechtsunsicherheit bei den Verantwortlichen vorhanden zu sein. Wider Erwarten haben sich Sorgen um Sanktionen – zumindest unter der Praxis in Baden-Württemberg – nicht als vorrangig herausgestellt. Dies mag nicht zuletzt daran liegen, dass in Baden-Württemberg immer wieder klargestellt wurde, dass Beratung vor Bestrafung geht – und dass viele Verantwortliche sich auf den Weg zu einer datenschutzkonformen Verarbeitung gemacht haben. Ca. 75% der Unternehmen im Lande gaben nach Umfrage der DIHK an, die DSGVO (zumindest bereits teilweise) umgesetzt zu haben. Meine Erfahrungen sind damit im Großen und Ganzen deckungsgleich.

Die Datenschutzaufsicht in Baden-Württemberg orientiert sich am Leitsatz „Wenn es nicht sinnvoll ist, dann ist es kein Datenschutz“. Unter dieser Zielsetzung soll auch der vorliegende Bericht verstanden werden. Er spiegelt die Stimmen aus dem Land wieder, welche meine Dienststelle bei ihrer täglichen Arbeit und im Laufe des gesamten Evaluierungsprozesses vernommen hat. Dieser Bericht ist eine Zusammenstellung von Erfahrungen und Anregungen der Verantwortlichen und Betroffenen im Land. Als Aufsichtsbehörde sehen wir uns in der Pflicht, der europäischen Ebene auch diese Stimmen zu Gehör zu bringen

Dr. Stefan Brink

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

LfDI BW - 35. Tätigkeitsbericht 2019 - Anhang

1. Informations-, Auskunfts- und Transparenzpflichten

Die DS-GVO bringt Verpflichtungen, die kleine Vereine nun ebenso treffen wie Konzerne wie Apple, Amazon, Google, Microsoft oder Facebook. Darunter zahlreiche Pflichten, welche die Bundesgesetzgebung bislang nicht kannte. Der LfDI Baden-Württemberg erhält zahlreiche besorgte Anfragen und Beschwerden aus Vereinen, die sich überfordert fühlen oder Sanktionsandrohungen bei Fehlverhalten fürchten. Beratung alleine reicht den Vereinen im Land nicht aus, es werden tatsächliche Entlastungen gefordert. Vereine und kleine Unternehmen können sich im Gegensatz zu größeren Unternehmen häufig externe Experten nicht leisten.

Viele kleine und mittlere Unternehmen sowie ehrenamtlich Tätige haben in der Praxis erhebliche Schwierigkeiten, die gesetzlich vorgesehenen Informationspflichten umfassend zu erfüllen. Es gilt zu vermeiden, dass gerade das Ehrenamt zu einem haftungsrechtlichen Risiko für die Verantwortlichen wird. Gleichzeitig muss die Einhaltung des Datenschutzniveaus im Sinne aller Bürgerinnen und Bürgern gewährleistet werden. Hier muss mithilfe der im Laufe der Anwendung der DS-GVO gewonnenen Erkenntnisse auf Dauer ein praktikabler und sinnvoller Ausgleich gefunden werden.

Gerade bei kleinen Unternehmen, deren Datenverarbeitung hauptsächlich im Rahmen von Kundenbeziehungen stattfindet, scheint die Erfüllung der Informationspflichten oft mit unverhältnismäßig hohem Aufwand verbunden oder schlichtweg nicht realisierbar zu sein. Im Rahmen von Unternehmen-Kunden-Beziehungen sind dem beauftragenden Kunden oft viele der informationspflichtigen Daten bereits bekannt. Hierzu wird jedoch selten zum Beispiel die Rechtsgrundlage der Datenverarbeitung zählen. Fraglich scheint allerdings, ob diese bei jeder Auftragserteilung tatsächlich von Interesse ist. Betroffene klagen an dieser Stelle häufig über eine ungewollte Informationsflut. Zu überlegen wäre, ob unter Berücksichtigung des risikobasierten Ansatzes die Beauftragung beispielsweise eines Handwerksbetriebs mit risikoarmer Datenverarbeitung nur erleichterten Regulierungen unterworfen werden sollte.

Das Prinzip „one size fits all“ funktioniert gerade bei den Informations- und Transparenzpflichten in der Praxis nicht. Eine Überlegung wäre daher, ob für Verantwortliche, deren Kerntätigkeit nicht die Datenverarbeitung ist, Ausnahmen geschaffen werden könnten. Unterschiede sind im Alltag auch dort deutlich erkennbar, wo im Rahmen von geschäftlichen Beziehungen viele Informationen bereits vorhanden sind und eine gewisse Augenhöhe der Beteiligten vorherrscht. Bei vielen vertrags- oder vertragsähnlichen Verhältnissen werden Datenschutzvorgaben oft als bürokratische Belastung ohne Mehrwert gesehen.

Informationspflichten müssen „leicht zugänglich“ sein. Hierdurch sollte jedoch gerade kein Informationsüberschuss entstehen, welcher dazu verleitet, die Informationen gar nicht mehr wahrzunehmen, da die Unterscheidung zwischen essentiellen Informationen und solchen, die nicht vorrangig von Interesse sind, schwer fällt. Dies kann im Einzelfall eher zu einem Mangel an als zur Förderung der Transparenz führen. Dieser Entwicklung ist entgegenzusteuern.

Generelle Ausnahmen von Verantwortlichen-Pflichten bergen allerdings immer die Gefahr, dem Ziel der Vorschrift selbst zuwider zulaufen. Bei jeglicher erleichternden Änderung müsste daher darauf geachtet werden, die Grenzen so deutlich zu ziehen, dass die eigentliche Zielgruppe der größeren datenverarbeitenden Unternehmen oder Unternehmen mit datenverarbeitender Kerntätigkeit nicht unter die Ausnahmevorschriften fallen können.

LfDI BW - 35. Tätigkeitsbericht 2019 - Anhang

Auch die Auskunftspflicht nach Art. 15 DS-GVO stellt Verantwortliche oft vor große Herausforderungen. Teilweise wurde von einer Pervertierung des Auskunftsrechts als Instrument der „Selbstjustiz“ berichtet. Tatsächlich sind - vor allem im Austausch mit öffentlichen Stellen, aber auch in unserer eigenen Arbeit als auskunftspflichtige Stelle – immer wieder Auslegungsfragen vor allem zum Recht auf Kopie begegnet. Hier ist unklar, wie weit dieses reicht und ob mit dem Begriff der „Kopie“ ein Anspruch auf Aushändigung in Papierform eingerechnet. Die Unterscheidung zwischen der „Auskunft über diese personenbezogenen Daten“ nach Abs. 1 S. 1, der Auskunft über „die Kategorien personenbezogener Daten, die verarbeitet werden“ nach Abs. 1 S. 1 lit. b und der „Kopie der personenbezogenen Daten“ nach Abs. 3 S. 1 fällt Verantwortlichen sowohl im öffentlichen als auch im nichtöffentlichen Bereich gleichermaßen schwer.

Lösungsansätze

- Gleichgang der Ausnahmenregelungen der Art. 13 und 14 DS-GVO
- Anhebung oder Differenzierung der Risikostufe in Art. 13 und 14 DS-GVO
- Ausnahmen bei Informationspflichten beispielsweise für die Datenverarbeitung zu privilegierten Zwecken, zugunsten von Unternehmen, deren Datenverarbeitung nicht Zweck der Geschäftstätigkeit ist oder zugunsten der Geheimhaltungsinteressen des Verantwortlichen
- Einführung einer 250-Personen-Grenze (ähnlich Art. 30 Abs. 5 DS-GVO) für Informationspflichten
- Einführung von Definitionen und Differenzierung der Pflichten von Kleinunternehmen und Kleinen und Mittleren Unternehmen (KMU), beispielsweise nach Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinunternehmen sowie der kleinen und mittleren Unternehmen (Az. K(2003) 1422)
- Streichung des Entstehens der Informationspflichten „zum Zeitpunkt der Erhebung“ für bestimmte Fallkonstellationen
- Zulassung des sog. Medienbruchs für risikoarme Fallkonstellationen und gesetzliche Normierung der notwendigen Informationen im zweistufigen Verfahren
- Änderung der Fristen für die Bereitstellung von Informationen in Alltagsgeschäften unter Berücksichtigung des Zwecks der Regelungen zu Informationspflichten
- Standardisierung von Datenschutzerklärungen auf Internetseiten
- Die „Notwendigkeit“ bei den Informationspflichten von den „jeweiligen Umständen“ abhängig machen, um auf Alltagssituationen eingehen zu können
- Klarstellung, dass eine Angabe einer Kategorie von Empfängern auch ausreichend ist, wenn der Verantwortliche den Empfänger konkret kennt
- Klarstellung des Verhältnisses von Transparenzpflichten und Betriebs- und Geschäftsgeheimnissen
- Begrenzung des Auskunftsanspruchs beispielsweise über eine Verhältnismäßigkeitseinrede, weitere Schärfung der Missbrauchseinrede Art. 12 Abs. 5 S. 2 „bei offenkundig unbegründeten Anträgen“, begriffliche Klarstellung oder Streichung Rechts auf „Kopie“

LfDI BW - 35. Tätigkeitsbericht 2019 - Anhang

2. Verarbeitungsverzeichnis

Die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten stellt für kleine und mittlere Unternehmen häufig eine schwer zu bewältigende Herausforderung dar.

Zwar hält die DS-GVO mit Art. 30 Abs. 5 DS-GVO eine Ausnahmenvorschrift von der Verpflichtung für Unternehmen oder Einrichtungen bereit, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien gemäß Artikel 9 DS-GVO bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DS-GVO einschließt.

Diese Ausnahmeregelung ist für kleine und mittlere Unternehmen allerdings in der Praxis so gut wie nie einschlägig. Die Gegenausnahmen hierzu sind so weitreichend, dass kaum ein Unternehmen von dieser Ausnahme profitiert. Bei der Beschäftigung von etwas weniger als 250 Mitarbeitern ist eine lediglich gelegentliche Verarbeitung personenbezogener Daten kaum möglich. Jeder Betrieb, der Arbeitnehmer beschäftigt, verarbeitet zwangsläufig zumindest deren Daten zur Durchführung des Beschäftigungsverhältnisses - auch Gesundheitsdaten im Rahmen der Fehltagverwaltung oder die Religionszugehörigkeit im Rahmen der Steuerverwaltung. Die Ausnahme scheitert spätestens an der „gelegentlichen“ Verarbeitung im Sinne von „Häufigkeit“. Dies dürfte nicht das gesetzgeberische Ziel gewesen sein. Die einzige Möglichkeit, dieser unerwünschten Folge entgegenzutreten, ist die Einschränkung der Gegenausnahme des Art. 30 Abs. 5 DS-GVO. Bei dieser „missglückten Rückausnahmeregelung“ wird dringend Anpassungsbedarf gesehen.

Der eigentlich vorgesehene risikobasierte Ansatz greift hier nicht durch. „One size fits all“ scheint auch hier nicht zu funktionieren. Für Verantwortliche wäre es nachzuvollziehen, wenn beispielsweise stärker auf eine datenverarbeitende Kerntätigkeit abgestellt würde und für andere Verantwortliche geringere Anforderungen gelten würden, z.B. bei Geschäftsbeziehungen. Hier würde eine Differenzierung anhand der Kerntätigkeit dem eigentlichen Ziel der Vorschrift mehr Rechnung tragen. Im Gegenzug könnte die Schwelle der Mitarbeiterzahl gesenkt werden.

Lösungsansätze

- Ersatz der Häufigkeitsvoraussetzung des Art. 30 Abs. 5 DS-GVO durch Abstellen auf Datenverarbeitung als Kerntätigkeit des Unternehmens (beispielsweise ähnlich Art. 37 Abs. 1 lit. b DS-GVO)
- Schaffung privilegierter Verarbeitungskategorien beispielsweise für Geschäftsbeziehungen
- Sensible Kategorien personenbezogener Daten nach Art. 9 DS-GVO als einzige Rückausnahme
- Erhöhung der Risikostufe

LfDI BW - 35. Tätigkeitsbericht 2019 - Anhang

3. Benennungspflicht von Datenschutzbeauftragten

Der Ruf nach der Abschaffung der Benennungspflicht für Datenschutzbeauftragte ist wohl landesweit am häufigsten zu hören. Der Nutzen der Benennungspflicht insgesamt und der Meldepflicht an die Datenschutzaufsichtsbehörden wird häufig in Frage gestellt, vor allem wenn es um kleinere Vereine oder Unternehmen geht.

Das Ziel der Harmonisierung des Rechts auf europäische Ebene wird hier oft als nicht erreicht angesehen. Weite Öffnungsklauseln stehen in der Kritik, unterschiedliche Rechtsanwendung kann bis hin zu Wettbewerbsnachteilen führen. Häufig wird auch hier eine Stärkung des risikobasierten Ansatzes, die Erleichterung für risikoarme Datenverarbeitungen und die Fokussierung auf Qualität und Quantität der Datenverarbeitungen gefordert.

Seit der nationale Gesetzgeber die Anhebung der Personengrenze im Bundesdatenschutzgesetz von zehn auf zwanzig umgesetzt hat, ist es zunächst ruhiger um das Thema geworden. Allerdings werden die Verantwortlichen bald feststellen, dass eine fehlende Benennungs- oder Meldepflicht sie nicht von ihren Aufgaben als datenschutzrechtlich Verantwortliche befreit.

Bei dieser Diskussion ist zu bedenken, dass die Datenschutzbeauftragten für eine kompetente datenschutzrechtliche Beratung sorgen, um Datenschutzverstöße schon im Vorfeld zu vermeiden und nicht zuletzt das Sanktionsrisiko gering zu halten. Oft wird vergessen, dass auch beim Wegfall der Benennungspflicht die Pflichten des Datenschutzrechts bestehen bleiben, die interne Beratung und der angelernte Sachverstand jedoch wegfällt. Ein Wegfall würde kurzfristig als Entlastung empfunden werden, allerdings würde beim Aufkommen der nächsten datenschutzrechtlichen Fragestellung eine interne Rückgriffsmöglichkeit entfallen und der LfDI könnte die Einzelfall-Betreuung sämtlicher Vereine in Baden-Württemberg auch mit massiven Personalaufstockungen nicht gewährleisten.

Die Meldepflicht an die Aufsichtsbehörde ist ebenso kein Selbstzweck. Die grundlegende Abschaffung der Meldepflicht der Datenschutzbeauftragten würde die Kontrolle der Aufsichtsbehörden in diesem Bereich erschweren. Der Meldepflicht kommt zudem eine Selbstkontroll-Funktion - auch hinsichtlich des Aufbaus einer Datenschutzorganisation - zu. Ein Datenschutzbeauftragter stellt die Wahrung der Rechte von Beschäftigten und Bürgern sicher, deren Daten verarbeitet werden. Datenschutzbeauftragte bieten die Chance, Knowhow zu verbreiten, ohne auf eher pauschal arbeitende Dienstleister angewiesen zu sein.

Nach dem auch den Regelungen der Art. 37 ff. DS-GVO zugrunde gelegten risikobasierten Ansatz muss ein Datenschutzbeauftragter nur dann benannt werden, wenn dies wegen des Risikos erforderlich ist. Die Feststellung des Risikos wird allerdings von eher starren Voraussetzungen abhängig gemacht. Dem risikobasierten Ansatz könnte hier durchaus größeres Gewicht verliehen werden.

Bayern hat die Meldepflicht für Amateursportvereine, Musikkapellen und sonstige vor allem durch ehrenamtliches Engagement getragene Vereine aufgehoben. Sollte sich dies als vereinbar mit deutschem und europäischem Datenschutzrecht erweisen, wäre darüber nachzudenken, hier eine gesetzliche Klarstellung solcher Möglichkeiten in den Gesetzestext aufzunehmen, um eine europaweite Erleichterung herbeizuführen. Allerdings müssten Möglichkeiten gefunden werden, wie die Beratung zur Einhaltung der bestehenden Pflichten trotzdem gewährleistet werden könnten, beispielsweise durch Einrichtung einer zentralen Beratungsstelle mit entsprechender Ausrüstung.

LfdI BW - 35. Tätigkeitsbericht 2019 - Anhang

Lösungsansätze

- Ausnahmeregelungen für ausschließlich ehrenamtlich tätige, nicht wirtschaftliche Vereine
- Ausnahmeregelungen für Kleinunternehmen, verbunden mit einer entsprechenden Legaldefinition
- Angleichung der Bestellpflicht im öffentlichen und nichtöffentlichen Bereich, stattdessen Differenzierung der Pflichten anhand von Unternehmensgröße oder Branche
- Einrichtung einer zentralen Beratungsstelle für von der Bestellpflicht befreite Verantwortliche

LfDI BW - 35. Tätigkeitsbericht 2019 - Anhang

5. Herstellerhaftung - „privacy by design“

Die DS-GVO stellt mit Privacy by Design / Privacy by Default Grundsätze auf, die sich an Hersteller richten, nimmt Hersteller aber nicht als solche in die Pflicht. Es sollten auch Hersteller, Lieferanten, Importeure, Verkäufer usw. in die Pflicht genommen werden, so wie dies im Produkthaftungsrecht (ProdHaftG bzw. RL 85/374/EWG) bereits der Fall ist.

Beim Begriff „Datenschutz durch Technikgestaltung“ (Privacy by Design), der im Artikel 25 Abs. 1 DS-GVO für den Verantwortlichen vorgeschrieben ist, stellt sich in der Praxis der Adressatenkreis als nicht weitreichend genug heraus. Da Verantwortliche in der Regel nicht selbst Software entwickeln und in weiten Teilen Standard- und Anwendungssoftware von Herstellern bzw. Anbietern, zum Teil sogar von solchen mit globaler, nationaler oder regionaler Monopol- oder zumindest marktbeherrschender Stellung, beziehen und nutzen müssen, läuft diese Forderung häufig ins Leere. Sie sollte daher auch die Hersteller von Software zur Einhaltung dieses datenschutzfördernden Designprinzips verpflichten. In der Praxis trifft dies insb. auf Hersteller von komplexer Software wie z. B. Betriebssystemen, Datenbankmanagementsystemen, Standard-Office-Paketen oder sehr speziellen Fachanwendungen, zu.

Betriebssysteme etwa sind auf dem Markt nur in begrenzter Anzahl vorhanden, sodass Verantwortliche, die Server, Desktop-Computer, Notebooks, Tablets, Smartphones oder ähnliche Geräte betreiben, auf eines derjenigen zurückgreifen müssen. In der Regel sind diese beim Kauf durch den Anwender schon vorinstalliert. Nach derzeitiger Rechtslage ist es die Pflicht der Verantwortlichen, etwaige datenschutzrechtlich relevante Schwachstellen, Fehlkonfigurationen, aus ihrer Sicht unerwünschte Funktionen, etc. zu finden und abzustellen. Den Hersteller trifft keine Pflicht, seine Produkte ohne diese Fehler auszuliefern. Ähnlich verhält es sich in Alltagssituationen, etwa bei haustür-Schließsystemen via Smartphone-App oder anderen „smart home“ Anwendungen. Zwischen der dafür zuständigen App und dem möglicherweise in einem Drittland ohne angemessenes Datenschutz-Niveau befindlichen Hersteller findet Datenverkehr statt. Setzt ein Unternehmen derartige Systeme ein, ist es selbst Verantwortlicher und muss Datenverarbeitungen verantworten, die es nicht durchschauen kann. Der Hersteller ist nicht effektiv greifbar. Setzt eine Privatperson im Rahmen privat-familiärer Tätigkeit derartige Systeme ein, ist ein Verantwortlicher i.S.d. DS-GVO schon nicht vorhanden. Die Pflichten der DS-GVO treffen niemanden, gehen also ins Leere.

Die bisherige Rechtslage widerspricht dem Ansatz von „data protection by design“ bzw. „by default“. Entgegen Erwägungsgrund 78 S. 4 DS-GVO werden Hersteller in keiner Weise ermutigt, „das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen“. Damit bestehen nicht nur erhebliche Lücken im Bereich des Schutzes personenbezogener Daten, sondern es kommt zu einer Potenzierung von technischem und bürokratischem Aufwand bei dem Versuch, dezentral Mängel zu beseitigen, die zentral verursacht werden. Dies belastet alle Verantwortlichen und Auftragsverarbeiter, wobei KMU überproportional belastet werden.

LfDI BW - 35. Tätigkeitsbericht 2019 - Anhang

Die Rechtslage widerspricht so auch dem über die RL 85/374/EWG harmonisierten Produkthaftungsrecht. Danach haften Hersteller, Importeure, Lieferanten, etc. für Schäden, die durch ihre Produkte entstehen. Diese bereits harmonisierte Rechtslage müsste in den Bereich des Schutzes personenbezogener Daten zu übertragen werden. Für datenschutzrechtlich relevante Produkte muss daher auch der Hersteller in die Verantwortung genommen werden.

Über die Position der DSK hinausgehend vertritt der LfDI Baden-Württemberg die Auffassung, dass die Durchsetzung einer wie beschrieben angepassten Rechtslage nur dann möglich wäre, wenn die Datenschutz-Aufsichtsbehörden auch zur Kontrolle der Einhaltung des Datenschutzes bei Herstellern, Importeure, Lieferanten, etc. befugt wären.

Lösungsansätze

- Einfügen einer an der Produkthaftungs-Richtlinie orientierten Hersteller-Definition in den allgemeinen Begriffsbestimmungen und Aufnahme in sämtliche Verantwortlichen-Pflichten sowie
- in die Verpflichtungen zur Zusammenarbeit mit den Aufsichtsbehörden und in die Zuständigkeits-, Aufgaben- und Befugnis- Normen der Aufsichtsbehörden sowie in die Sanktionsmöglichkeiten zum Zwecke der wirksamen Rechtsdurchsetzung

LfDI BW - 35. Tätigkeitsbericht 2019 - Anhang

5. Unklarheiten bei der Gemeinsamen Verantwortlichkeit, insbesondere im „social media“-Bereich

Das Inkrafttreten der DS-GVO hat insbesondere beim Betrieb von Internetseiten und der Benutzung von sozialen Medien für massive Verunsicherung gesorgt.

Fragen rund um die Gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO sowie der Abgrenzung zur Auftragsdatenverarbeitung nach Art. 28 DS-GVO sind die Folge. Häufig wird im Falle der Ablehnung einer Verarbeitung im Auftrag eine Gemeinsame Verantwortlichkeit unterstellt, die aber regelmäßig nicht vorliegt.

Eine Umfrage meiner Behörde bei den Gemeinden in Baden-Württemberg hat zum Thema „Weitergabe von Online-Nutzungsdaten“ ergeben, dass fast jede Gemeinde eine Website hat und über die Hälfte davon Inhalte oder Elemente von Dritten (z.B. Google/Facebook) in die Seite einbindet. Dies hat oftmals zur Folge, dass das gesamte Nutzungsverhalten von Website-Besuchern an Dritte ohne ersichtliche Rechtsgrundlage weitergegeben wird.

In anderen Konstellationen wird mit der Einwilligung als Rechtsgrundlage gearbeitet. Das eigentliche Ziel des Nutzerschutzes scheint in der Praxis durch Einwilligungs-Buttons und Banner nicht erreicht zu werden, sondern führt im Gegenteil eher zu Abwehrreaktionen. Bei sogenanntem „Tracking“ oder „Targeting“ auf Websites durch Drittanbieterwerkzeuge oder Webanalysetools stellt sich oft die Frage nach der Rechtsgrundlage und der Erfüllung der Informationspflichten.

Gerade beim Betrieb von Seiten auf sozialen Medien stellt sich nach den neusten Entscheidungen des EuGH zur Kategorisierung als Gemeinsame Verantwortlichkeit für die Seitenbetreiber die Frage, wie sie die daraus entspringenden Pflichten realisieren sollen. Oft besteht in der Praxis für die Profil-Inhaber nicht die Möglichkeit, auf die gemeinsame Datenverarbeitung Einfluss zu nehmen und Zweck und Mittel festzulegen, geschweige denn dies transparent zu machen. Selbst wenn die Möglichkeit besteht, ist den gemeinsam Verantwortlichen im Rahmen des Art. 26 ohne weitere Hilfestellung der Aufsichtsbehörde - wie beispielsweise durch unser „Vertragsmuster für eine Vereinbarung nach Art. 26 DS-GVO“ - nicht klar, welche wesentlichen Inhalte festzulegen sind, sodass eine Vielzahl ungenügender Vereinbarungen besteht und Betroffenen die Klarheit über den korrekten Ansprechpartner fehlt. Die Regelung des Art. 26 DS-GVO wird häufig als defizitär beschrieben. Es wird Präzisierungsbedarf auch bezüglich der Transparenzanforderungen sowie des Rechtsverhältnisses der Verantwortlichen untereinander gesehen.

Lösungsansätze

- Klarere Abgrenzungskriterien zwischen Gemeinsamer Verantwortlichkeit nach Art. 26 DS-GVO und Auftragsdatenverarbeitung nach Art. 28 DS-GVO
- Klarstellung dahingehend, dass der erfüllte Tatbestand einer Gemeinsamen Verantwortlichkeit keine Rechtsgrundlage für den Datenaustausch zwischen den beteiligten Verantwortlichen darstellt
- Orientierung des Betroffenenrechts anhand der Organisationspflicht und Beschränkung der Reichweite der gemeinsamen Haftung auf ein adäquates Maß

LfDI BW - 35. Tätigkeitsbericht 2019 - Anhang

- Klarstellung, dass eine Gemeinsame Verantwortlichkeit für eine gesamte Anwendung oder auch für ein gesamtes Projekt bestehen, daneben aber auch nur einen Teilbereich des gesamten Verarbeitungssystems betreffen kann
- Klarstellung, wann eine Gemeinsame Verantwortlichkeit vorliegen kann, beispielsweise
 - wenn zwei oder mehr Verantwortliche darüber entscheiden, welche Personen an der Datenverarbeitung beteiligt sind und Zugang zu den Daten haben,
 - welche Kategorien von personenbezogenen Daten erhoben werden sollen,
 - wie die personenbezogene Daten erhoben werden sollen,
 - aufgrund welcher Rechtsgrundlage die Datenverarbeitung vorgenommen werden soll,
 - welche technischen und organisatorischen Maßnahmen ergriffen werden sollen,
 - wann personenbezogenen Daten gelöscht werden;
 - den Anlass für eine Datenerhebung geben, oder
 - bei einer gemeinsamen Verarbeitung personenbezogener Daten eigene individuelle Ziele verfolgen
- Klarstellung, dass Gemeinsam Verantwortliche die regelmäßige Überprüfung ihrer gegenseitigen Pflichten vereinbaren können
- Normierung einer der Auftragsverarbeitung ähnlichen Regelung zu den wesentlichen Inhalten einer Vereinbarung zur gemeinsamen Verantwortlichkeit
- Förderung weiterer Guidelines auf europäischer Ebene

LfDI BW - 35. Tätigkeitsbericht 2019 - Anhang

Fazit

Bei aller Kritik darf man nicht vergessen, welche Vorteile das neue Datenschutzrecht bietet. Man hat nun, vor allem auch gegenüber anderen Wirtschaftsräumen, ein einheitliches europäisches Instrument. Die Bürgerrechte sind dadurch eindeutig gestärkt worden. Die DS-GVO ist also ein Erfolgsmodell - mit Verbesserungspotenzial.

Die Europäische Kommission braucht für ihre Aufgabe der Fortentwicklung des Datenschutzrechts alle Erfahrungen aus der Anwendung der DS-GVO; nicht nur aus aufsichtsbehördlicher Sicht, sondern umfassend. Hierzu leisten wir einen Beitrag.

Der LfDI ist sich des Umstandes bewusst, dass die Chancen auf tatsächliche Gesetzesänderungen auf EU-Ebene nach den langen Verhandlungen beim Zustandekommen der DS-GVO und den aktuellen Erfahrungen aus den Verhandlungen zur ePrivacy-Verordnung eher begrenzt sind. Nichts desto trotz sehen wir es als unsere Aufgabe, die Anwendung der DS-GVO vor Ort weiterhin zu beobachten und ein offenes Ohr für die Anliegen und Probleme der Verantwortlichen in Baden-Württemberg zu haben - und die so gewonnen Erkenntnisse an die Gesetzgeber im Land, im Bund und in Europa weiter zu tragen.

Stichwortverzeichnis

A

Akkreditierung 10
Akten-/Datenträgervernichtung 34
Aktenvernichtung 102
Ambulanter Pflegedienst 82
Arztpraxen 22
Auftragsverarbeiter 101
Auftragsverarbeitung 99
Auskunftsbegehren 30
Auskunftsrecht 27

B

Befugnisse der Aufsichtsbehörden und Sanktionspraxis 10
Beschäftigtendatenschutz 99
Betroffenenrechte 28, 30, 66, 70, 85, 95, 122
Bodycams 19
Bonitätsprüfung 106
Bußgeld 72, 117
Bußgelder 35
BvD 18

D

Data protection by design 10
Datenpannen 10, 22
Datenschutzhinweis 110
Dienstvereinbarung zur Nutzung von Informationstechnik 92
Direktwerbung 10

E

Eigenwerbung 26
Einwilligung 110
E-Mail 81
E-Mail-Werbung 25
Emotet 31
Eurodac 50
Europäische Datenschutzausschuss (EDSA) 38
Europäischer Datenschutzausschuss 38

F

Fernmeldegeheimnis 91
Fernwartung 32
Funkzellen 49

G

Geldwäschegesetz 106
Gesundheit 112
Gewinnspiele 111

LfDI BW - 35. Tätigkeitsbericht 2019 - Anhang

H

Häusliche Krankenpflege 81
Hausverwalter 105
Hausverwaltung 103
Heimaufsichtsbehörden 84

I

Informationspflichten 85
Informations- und Transparenzpflichten 9

J

Jobcenter 81
Jugendamt 81

K

Kindertageseinrichtungen 93
Kontrollbesuch 19
Kultusministerium 94
Kundenbewertung 26
Künstliche Intelligenz 10

M

Malware 30
Messengerdienste 17

N

Nutzungsordnung 91

P

Parkraumüberwachung 100
Personalausweiskopie 105
Phishing 30
Polizei 19
Pre-Recording 20
Private Internet- oder E-Mail-Nutzung 91

R

Recht auf Auskunft und auf Kopie 30
Reiseveranstalter 112

S

Schule 94
Schulische Informationstechnik 91
Schulrecht 91
Social Media 39
Sozialleistungsträger 81

T

Technisch-organisatorischer Datenschutz 22, 30, 126

LfdI BW - 35. Tätigkeitsbericht 2019 - Anhang

U

Umfrage 12
Unlauterer Wettbewerb (UWG) 25

V

Verantwortlichkeit 101
Vernetzte Fahrzeuge 39
Versicherungsunternehmen 107
Verwaltungsvorschrift über den Datenschutz an öffentlichen Schulen 94
Videoüberwachung 37

W

Werbewiderspruch 27
Werbung 25, 125
Wohnungseigentümergeinschaft 103, 105
Wundmanager 81

Z

Zweckbindung 10