Bayerisches Landesamt für
Datenschutzaufsicht

9. Tätigkeitsbericht

2019

9. Tätigkeitsbericht des Bayerischen Landesamts für Datenschutzaufsicht für das Jahr 2019

Hinweis: Aktualisierte Fassung vom 31.01.2020 (Anpassung in Kapitel 6.3)

Herausgeber:
Bayerisches Landesamt für Datenschutzaufsicht
Promenade 18
91522 Ansbach

Tel.: 0981 180093-0
Fax: 0981 180093-800
E-Mail: poststelle@lda.bayern.de
Web: www.lda.bayern.de

Vorgelegt im Januar 2020 – Thomas Kranig, Präsident

Bildnachweis Cover: de.123rf.com – Urheber melpomen – Dateinummer 117302880

Vorwort

Dieser 9. Tätigkeitsbericht des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA) ist der Erste, dessen Berichtszeitraum sich gemäß der Vorgabe der Datenschutz-Grundverordnung (DS-GVO) nur auf ein Jahr, das Jahr 2019, bezieht. Wie schon in den Vorjahren beinhaltet unser Bericht keine datenschutzpolitischen Ausführungen. Er wiederholt auch nicht die Entschließungen, Beschlüsse, Orientierungshilfen o. ä. der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz – kurz: DSK). Diese sind stattdessen auf der Homepage der DSK jederzeit frei abrufbar (www.datenschutzkonferenz-online.de). Unser Bericht beinhaltet – dem halbierten Berichtszeitraum entsprechend – deutlich weniger Fallbeispiele. Unser Ziel bei der Auswahl der dargestellten Fälle und unseren Entscheidungen dazu war und ist nach wie vor, den Verantwortlichen und betroffenen Personen eine Orientierung zu geben, wie wir die datenschutzrechtlichen Vorschriften in konkreten Fällen auslegen.

Für das BayLDA war das Jahr 2019 insgesamt ein extrem schwieriges Jahr. Es begann damit, dass wir aus unserem bisherigen Dienstgebäude, dem Schloss in Ansbach, ausgezogen sind. Wir konnten dann auf der anderen Straßenseite der Promenade in Ansbach in neu renovierte Räume, die früher einmal eine Zweigstelle der Bayerischen Landesbank beherbergt hatten, einziehen. Trotz intensiver Planung stellte sich der Umzug einer ganzen Behörde als gewaltiger Kraftakt dar. Eine besondere Herausforderung bestand darin, alle Mitarbeiterinnen und Mitarbeiter nicht nur körperlich, sondern „ganzheitlich" mitzunehmen. Es ließ sich nicht vermeiden, dass sich nicht alle durch den Umzug räumlich verbessert haben. Im Juli 2019 erfolgte die Anmietung weiterer Büroräume im 2. Stock des neuen Dienstgebäudes. Die gesamte nunmehr zur Verfügung stehende Bürofläche reicht aber nicht aus, um alle am Ende des Jahres 2019 vorhandenen Mitarbeiterinnen und Mitarbeiter so unterzubringen, wie es die entsprechenden Richtlinien eigentlich vorsehen. Es bleibt deshalb eine nachhaltige Aufgabe, sich um zusätzliche Büroflächen zu bemühen.

Aber auch die fachlichen Anforderungen an uns als Datenschutzaufsichtsbehörde waren 2019 schon alleine auf Grund der erheblichen Anzahl an Beschwerden, Beratungen und gemeldeten Datenschutzverletzungen gewaltig. Die Enttäuschung, dass uns trotz des bereits im Vorjahr 2018 festgestellten gewaltigen Anstiegs dieser Anforderungen im Doppelhaushalt 2019/2020 keine zusätzlichen Stellen bewilligt wurden, konnten wir zum Glück rasch überwinden. Wir erfuhren, dass der Bayerische Staatsminister des Innern, für Sport und Integration, dessen Ressort wir haushaltsrechtlich zugeordnet sind, durch eine interne Umstrukturierung uns einen erheblichen Finanzbetrag zur Verfügung gestellt hat, durch den wir neue – auf Dauer angelegte – Planstellen schaffen konnten. Selbst wenn diese Entscheidung vom März 2019 haushaltsrechtlich erst im Sommer wirksam wurde, so dass die meisten unserer neun neuen Mitarbeiterinnen und Mitarbeiter erst gegen November 2019 den Dienst antreten konnten, war die Aussicht auf diese personelle Aufstockung für die vorhandenen Beschäftigten eine hilfreiche Motivation, um mit der enormen Überlastung besser umgehen zu können. Diese Situation, verschärft durch den Wechsel der Hälfte unserer juristischen Beschäftigten, hatte leider dazu geführt, dass wir unseren gesetzlichen Aufgaben zur Durchführung von Prüfungen und Erlass von Bußgeldbescheiden nur in sehr geringem Umfang nachkommen konnten. Wir gehen davon aus, dass wir diese Aktivitäten in den folgenden Jahren, wenn alle neuen Mitarbeiterinnen und Mitarbeiter eingearbeitet sind, wieder in deutlich größerem Umfang betreiben können.

Der vorliegende Tätigkeitsbericht soll in erster Linie ein Blick zurück auf den Berichtszeitraum sein und darüber informieren, was in dieser Zeit geschehen ist. Das erfahren Sie, verehrte Leserin, verehrter Leser, auf den folgenden Seiten.

Der Bericht soll aber auch dafür verwendet werden, vielen – insbesondere Datenschutzbeauftragten – für die konstruktive Kommunikation zu danken, die uns in die Lage versetzt hat, besser wahrzunehmen, welche Probleme mit der neuen Datenschutz-Grundverordnung „im wirklichen Leben draußen" tatsächlich bestehen.

Ferner soll der Bericht auch dazu dienen, den eigenen Mitarbeiterinnen und Mitarbeitern für ihren hervorragenden Einsatz in einem sehr schwierigen Jahr zu danken. Trotz dieser nicht einfachen äußeren Rahmenbedingungen ist es gelungen, dass sich alle Mitarbeiterinnen und Mitarbeiter als ein Team gesehen, sich gegenseitig unterstützt und über alle Bereiche hinweg ausgezeichnet zusammengearbeitet haben. Herzlichen Dank dafür.

Ansbach, im Januar 2020

Thomas Kranig
Präsident

Inhaltsverzeichnis

Wichtiger Hinweis:

Ausschließlich zum Zweck der besseren Lesbarkeit wird auf die geschlechtsspezifische Schreibweise verzichtet. Alle personenbezogenen Bezeichnungen in diesem Tätigkeitsbericht sind somit geschlechtsneutral zu verstehen.

1

Datenschutzaufsicht im nicht-öffentlichen Bereich

1 Datenschutzaufsicht im nicht-öffentlichen Bereich

1.1 Gesetzliche Grundlage für den Tätigkeitsbericht

Anders als nach der bisherigen Rechtslage verpflichtet Art. 59 DS-GVO jede Aufsichtsbehörde, einen Jahresbericht über ihre Tätigkeit zu erstellen, der eine Liste der Arten der gemeldeten Verstöße und der Arten der getroffenen Maßnahmen nach Art. 58 Abs. 2 enthalten kann.

Dieser Bericht ist deshalb der erste von uns, der nur einen einjährigen Berichtszeitraum umfasst. Aus der Formulierung in der DS-GVO, welche Informationen der Bericht haben kann, ist der Wunsch des Gesetzgebers an die Aufsichtsbehörden zu entnehmen, nicht nur ihre Auffassung zur rechtlichen Beurteilung bestimmter Fallkonstellationen, sondern insbesondere auch statistische Angaben über das tatsächliche Vollzugshandeln darzustellen. Diese Anforderung versuchen wir in den folgenden Ausführungen dieses Tätigkeitsberichts erneut zu erfüllen.

1.2 Datenschutz in Bayern

Art. 51 DS-GVO verpflichtet die Mitgliedstaaten, eine oder mehrere unabhängige Behörden zur Überwachung der Anwendung der DS-GVO einzurichten. Maßgeblich für die konkrete Einrichtung ist das Recht des jeweiligen Mitgliedstaats. Für Deutschland bedeutet dies, dass der Bund für den Bereich seiner Zuständigkeit und die Länder für die Bereiche ihrer Zuständigkeiten entsprechende Aufsichtsbehörden vorsehen müssen. Eine Vorgabe, wie viele Aufsichtsbehörden und für welche Zuständigkeiten Aufsichtsbehörden eingerichtet werden sollen, gibt die DS-GVO nicht vor.

Der bayerische Gesetzgeber hat

- uns, das Bayerische Landesamt für Datenschutzaufsicht (BayLDA), für nicht-öffentliche Stellen in Bayern (Art. 18 BayDSG),
- den Bayerischen Landesbeauftragten für den Datenschutz für die öffentlichen Stellen in Bayern (Art. 15 BayDSG),
- den Medienbeauftragten für den Datenschutz für die Bayerische Landeszentrale für neue Medien, deren Tochtergesellschaften und Anbieter (Art. 20 BayMG) und
- den Rundfunkdatenschutzbeauftragten für den Bayerischen Rundfunk und ausgewählte Beteiligungsunternehmen des Bayerischen Rundfunks (Art. 21 BayRG)

als gleichwertige und gleichrangige Aufsichtsbehörden im Sinne des Art. 51 DS-GVO gesetzlich festgelegt.

Darüber hinaus haben Kirchen, religiöse Vereinigungen oder Gemeinschaften gemäß Art. 91 DS-GVO, wenn sie die dort genannten Voraussetzungen erfüllen, die Möglichkeit eine spezifische Aufsichtsbehörde einzurichten, die dann als Aufsichtsbehörde anzusehen ist, wenn sie die in Art. 51 ff. DS-GVO genannten Voraussetzungen, insbesondere der Unabhängigkeit, erfüllen. Dies wird in Deutschland für die katholische und evangelische Kirche unstrittig angenommen.

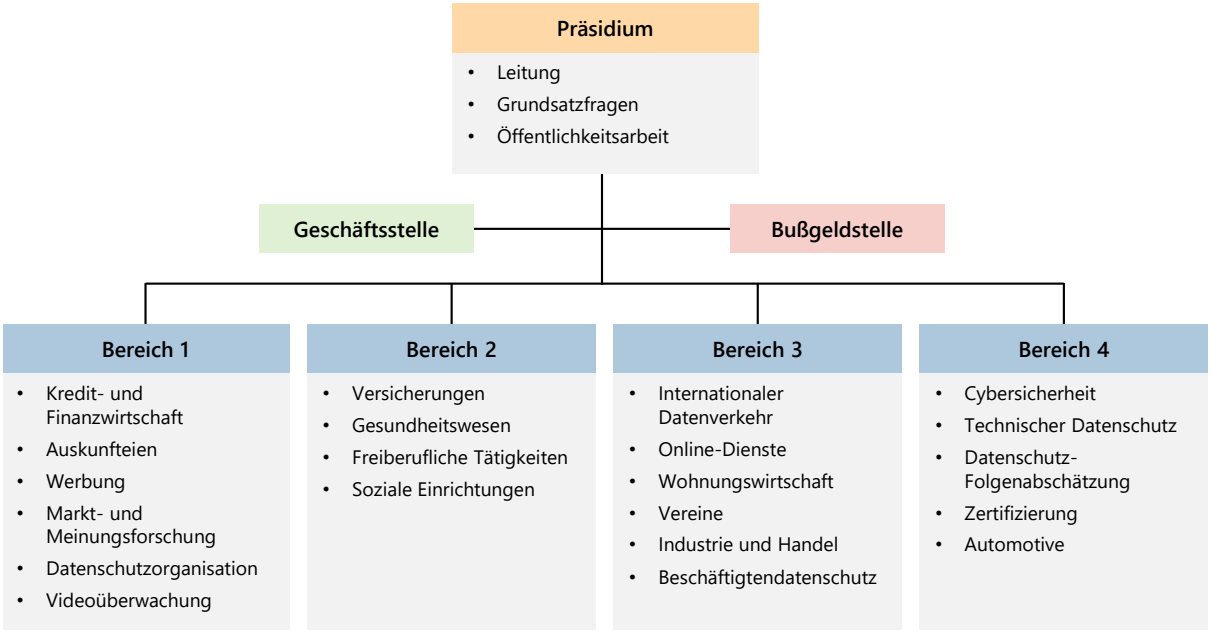
1.3 Das Bayerische Landesamt für Datenschutzaufsicht

Wie oben im Vorwort angesprochen und im Folgenden durch Darstellung der statistischen Angaben belegt, war das Jahr 2019 eine gewaltige Herausforderung. Was Beschwerden, Beratungsanfragen (die wir nach wie vor gerne bearbeiten und beantworten wollen) oder Meldungen von Datenschutzverletzungen inhaltlich und aufwandsmäßig bedeuten, ist uns ziemlich bewusst. Was aber noch auf uns zukommen

wird, konkret durch die Akkreditierung von Zertifizierungsstellen und dann die Zertifizierung selbst (Art. 42 DS-GVO), durch die Einbindung in Verfahren zur Aufstellung von Verhaltensregeln oder Genehmigung von Verhaltensregeln (Art. 40 DS-GVO) oder auch bei Verfahren zur Genehmigung von verbindlichen internen Datenschutzvorschriften (Binding Corporate Rules – BCR, Art. 47 DS-GVO), lässt sich noch nicht wirklich abschätzen. Wir haben uns bei der Auswahl und Aufstockung unseres Personalbestandes daher besonders bemüht, entsprechend ausgebildete Personen für uns zu gewinnen, damit wir auch für die nahe Zukunft gewappnet sind und diese neuen Anforderungen erfüllen können.

Ein erhebliches Maß an Planungsunsicherheit besteht letztendlich aber auch noch darüber, was auf uns zukommt, wenn das Vereinigte Königreich wie anvisiert am 31. Januar 2020 die Europäische Union verlassen wird und sich damit vorbehaltlich noch abzuschließender Verträge von einem Mitgliedstaat der EU zu einem Drittstaat wandelt. Es ist schon heute feststellbar, dass eine große Anzahl von Unternehmen mit dem Gedanken spielen – und es manche auch umgesetzt haben –, ihren Sitz vom Vereinigten Königreich in ein anderes Mitgliedsland EU zu verlegen. Der Großraum München und damit Bayern scheinen insoweit eine besondere Anziehungskraft zu haben. Ferner muss davon ausgegangen werden, dass auch unsere Zuständigkeit für die Durchführung von BCRs durch den Brexit nicht unerheblich steigen dürften, da im Vereinigten Königreich mit die meisten derartiger Verfahren durchgeführt wurden. Die Unternehmen werden versuchen, dieses Instrument für die Datenübermittlung in Drittstaaten beizubehalten, weshalb sie gezwungen sind, eine entsprechende Niederlassung im Bereich der Europäischen Union zu behalten oder zu bekommen.

Nachfolgend wird unsere interne Organisation, mit der wir auch diese Aufgaben stemmen wollen, in einem Organigramm stark vereinfacht dargestellt:



2

Zahlen und Fakten

2 Zahlen und Fakten

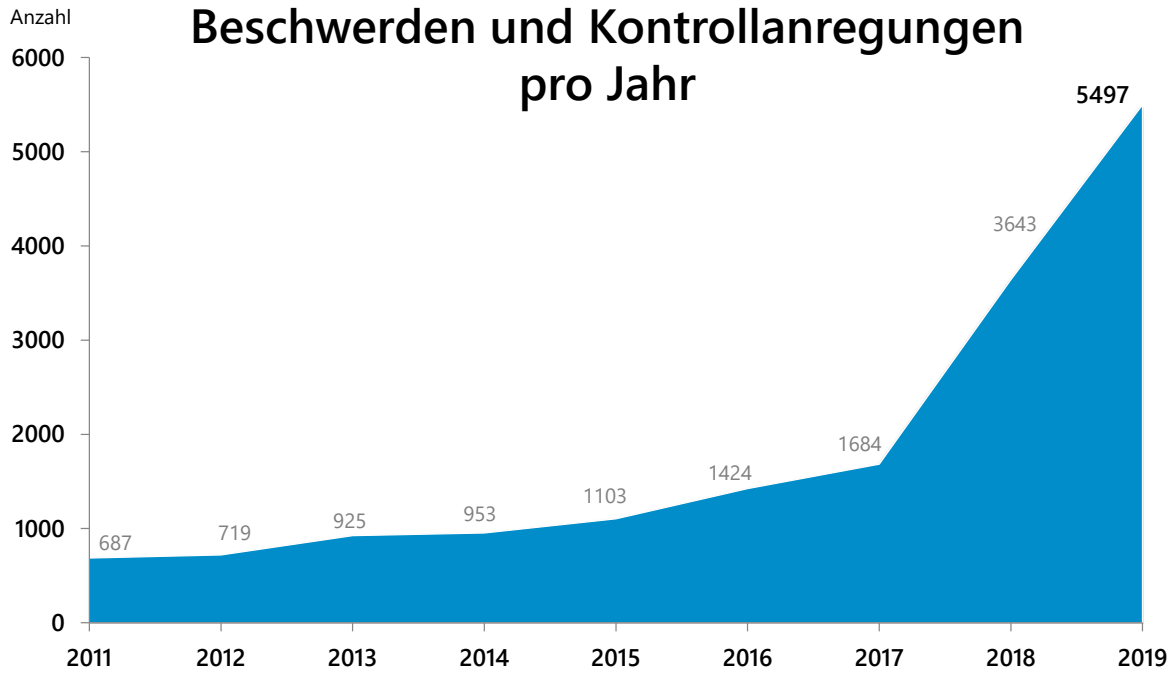
Wie schon im letzten Tätigkeitsbericht dargestellt, hat sich ein größerer Teil der deutschen Datenschutzaufsichtsbehörden auf eine teilweise Vereinheitlichung des statistischen Teils bei der Erstellung der Tätigkeitsberichte verständigt. Dabei sollten die statistischen Angaben, die in Art. 59 DS-GVO angesprochen sind, nach einem gleichförmigen Muster dargestellt werden. Diese Vereinheitlichung soll auch dem Zweck dienen, dass Deutschland bei den jährlichen Abfragen des Europäischen Datenschutzausschusses bei den Aufsichtsbehörden der Mitgliedstaaten ein genaueres Bild abgeben kann.

2.1 Beschwerden

Die Gesamtanzahl der Beschwerden und Kontrollanregungen, die 2019 bei uns eingegangen sind, ist der unten folgenden Grafik zu entnehmen. Als Beschwerden werden dabei solche Vorgänge gezählt, die schriftlich eingehen und bei denen eine natürliche Person eine persönliche Betroffenheit darlegt, für die Art. 78 DS-GVO anwendbar ist. Dies schließt Abgaben ein. Telefonische „Beschwerden" werden dann gezählt, wenn sie verschriftlicht werden (z. B. durch Vermerk).

Unter dem Obergriff „Beschwerden" erhielten wir zuletzt auch eine erhebliche Anzahl von Meldungen über angebliche Datenschutzverstöße, bei denen die Eingabeführer nicht glaubhaft gemacht haben, durch den vorgetragenen Sachverhalt in den eigenen Rechten verletzt zu sein. Diese Eingänge bezeichnen wir nicht als Beschwerden, sondern als Kontrollanregungen.

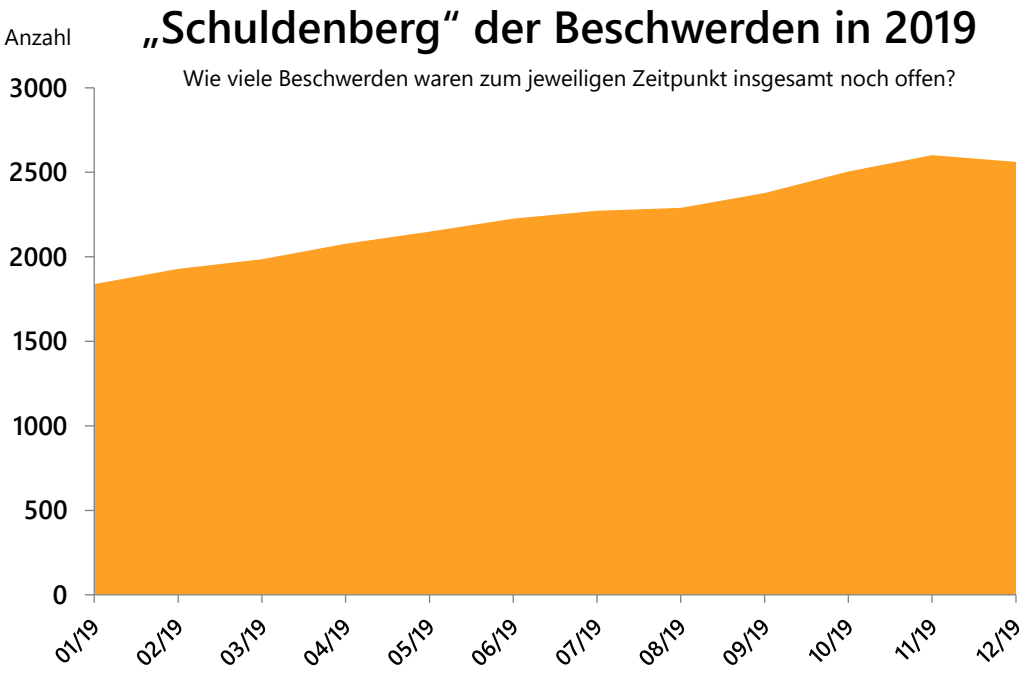
Warum eine getrennte Behandlung zwischen Kontrollanregung und Beschwerde für uns als Behörde nicht nur sinnvoll, sondern auch dringend notwendig ist, zeigt sich schnell: Nach Art. 78 Abs. 2 DS-GVO sind wir gehalten, betroffene Personen innerhalb von drei Monaten über den Stand oder das Ergebnis des Beschwerdeverfahrens in Kenntnis zu setzen. Somit müssen wir bei „echten" Beschwerden rechtzeitig mit der Bearbeitung beginnen. Ansonsten droht der Fall, dass wir dieser Verpflichtung nicht nachkommen und wir uns dadurch der Gefahr einer



(Untätigkeits-)Klage aussetzen. Bei Kontrollanregungen dagegen besteht kein Anspruch darauf, dass wir innerhalb einer bestimmten Frist über den Stand des Verfahrens berichten müssen. Folglich werden Beschwerden vorrangig abgearbeitet, individuell geprüft und entschieden. Bei Kontrollanregungen dagegen erhält der Mitteilende nur eine Bestätigung, dass wir seine Mitteilung als Kontrollanregung erfasst haben und nach pflichtgemäßem Ermessen entscheiden, ob und inwieweit wir dieser Anregung nachgehen.

Die Zahl der Beschwerden ist auch im Jahr 2019 noch einmal gewaltig angestiegen. Wie schon im letzten Bericht ausgeführt, gehen wir davon aus, dass die zahlreichen Veranstaltungen, Presseberichte und Informationsmaterialien dazu geführt haben, dass vielen Bürgern bewusster geworden ist, dass sie Betroffenenrechte haben und diese auch geltend machen können. Die Entwicklung mag daher aus Sicht der Gesellschaft positiv zu bewerten sein, weil ein gesteigertes Datenschutzbewusstsein vorhanden ist. Aus unserer Behördensicht mussten wir jedoch feststellen, die wir diese Arbeitslast mit dem im Jahr 2019 vorhandenen Personal nicht bewältigen konnten. Es gab zuletzt fast keinen Monat, in dem es uns gelang, mehr Beschwerdeverfahren abzuschließen als neue Vorgänge eingingen. Im Ergebnis bedeutet dies, dass wir zum Ende des Berichtszeitraums einen gewaltigen Arbeitsvorrat in das Jahr 2020 mitgenommen und unseren bestehenden „Schuldenberg" kontinuierlich weiter aufgebaut haben. In der unten stehenden Grafik erkennt man die Beschwerden, die insgesamt noch bei uns abgearbeitet werden müssen.

Die schwierige Personalsituation in 2019 und die gestiegene Anzahl von Beschwerden führten leider auch dazu, dass die Laufzeit der Bearbeitung für diese Beschwerden länger geworden ist. Wir mussten eine große Menge an Beschwerden in das Jahr 2020 mithinübernehmen, gehen aber davon aus, dass wir mit dem neuen Personal nach der Einarbeitungsphase wieder zu einer angemessenen Bearbeitungszeit zurückfinden werden.



2.2 Beratungen

Um die Vergleichbarkeit mit den anderen Aufsichtsbehörden sicherzustellen, verstehen wir unter Beratungen nunmehr nur die schriftliche Beantwortung von Anfragen von Verantwortlichen, betroffenen Personen und der eigenen Regierung. Ausschließlich (fern)mündliche Beratungen werden ebenso wie Schulungen, Vorträge etc. nicht mehr berücksichtigt, aber derzeit dennoch von uns separat erfasst.

In der nebenstehenden Tabelle sind die Beratungen im Berichtszeitraum aufgeführt. Wir haben hier, wie in den Vorjahren auch, die telefonischen Auskünfte mitangegeben. Wie man dort und auch in der unteren Grafik erkennen kann, ist die Anzahl der Beratungen im Verhältnis zum letzten Jahr deutlich gesunken. Insbesondere die in der Regel mit geringem Aufwand zu beantwortende Anfragen aus dem Bereich der Vereine und ehrenamtlich Tätigen wurden spürbar weniger, was sich in der Gesamtstatistik widerspiegelt.

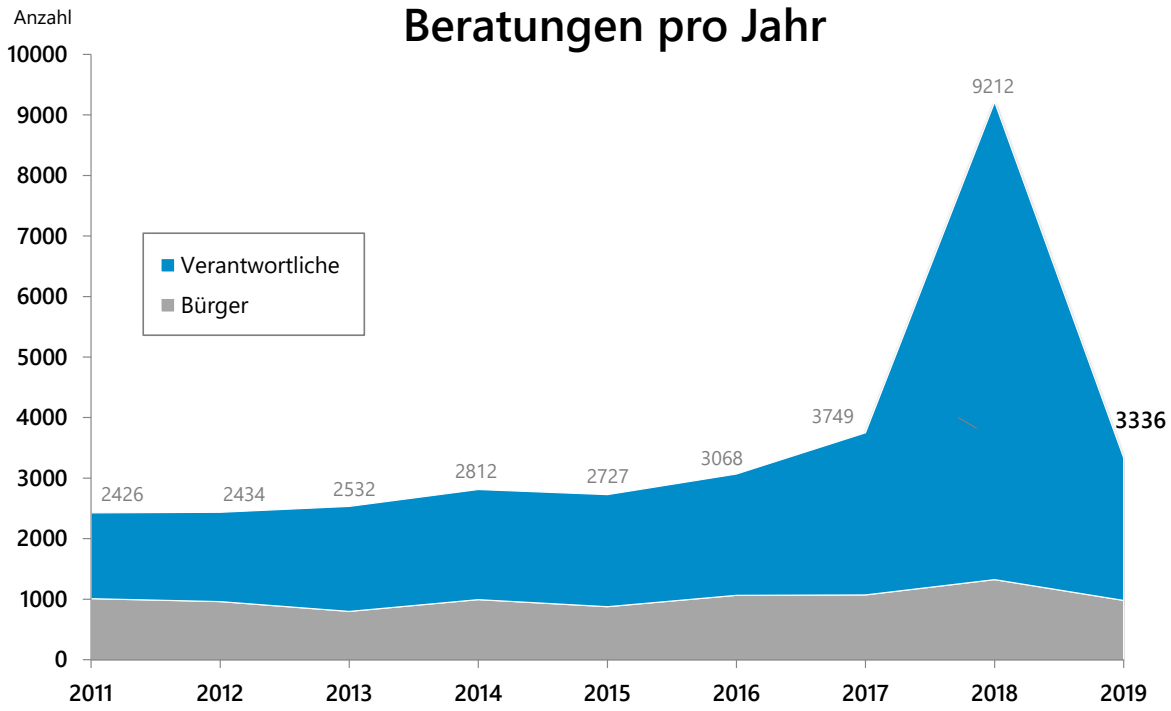
Eine Ursache dafür kann sein, dass wir auf unserer Website die Möglichkeit der Online-Beratung neu angeboten haben. Interessierte Personen können dabei zu bestimmten Themenbereichen Fragen an uns schicken. In diesem Prozess werden Ihnen dann vor Eingabe der Frage die FAQs zu dem ausgewählten Thema angegeben, die wir erstellt haben. Wir werten die Anfragen dazu zwar nicht aus, sind aber überzeugt davon, dass eine erhebliche Anzahl der Anfragenden nach Durchlesen der FAQs schon eine Antwort auf ihre Frage finden und „aussteigen."

www.lda.bayern.de/media/pm2019_7.pdf

Beratungen im Berichtszeitraum

Verantwortliche	2019
Telefonische Beratungen	936
Schriftliche Beratungen	1422

Bürger	2019
Telefonische Beratungen	419
Schriftliche Beratungen	559



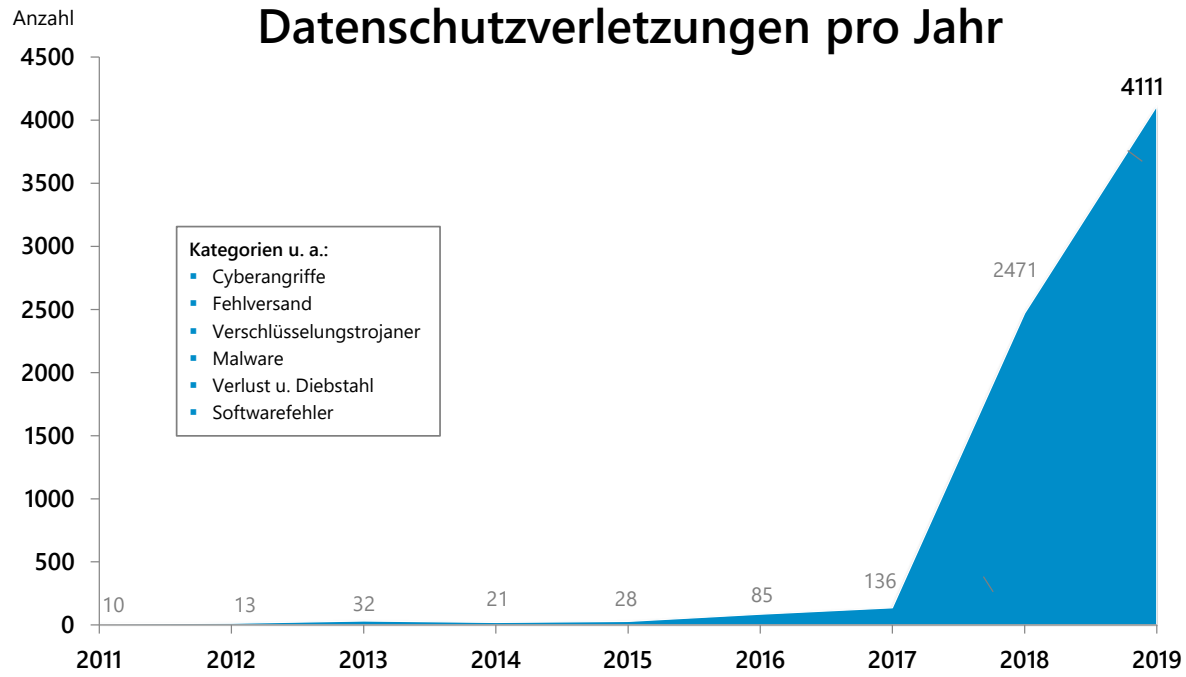
Ein weiterer Grund für den Rückgang der Beratungsanfragen können unsere Informationsveranstaltungen, das gesteigerte Informationsangebot auf unserer Homepage und nicht zuletzt auch die besseren Informationen der jeweiligen Dachverbände sein. Auf der anderen Seite merken wir aber, dass die verbliebenen Anfragen schwierigere Fragestellungen beinhalten und deshalb nach wie vor eine gewaltige Herausforderung darstellen.

Wir sind uns dabei bewusst, dass mit der ausschließlichen Erfassung der schriftlichen Beratungen ein nicht unerheblicher Anteil unserer Arbeit, nämlich die telefonische Beantwortung von Anfragen, statistisch künftig nicht mehr ins Gewicht fällt. Die telefonische Erreichbarkeit und Beantwortung von Anfragen ist uns nach wie vor wichtig. Es ist ein kostenfreier Service, der sicherlich für eine Behörde nicht selbstverständlich ist, aber von Hilfesuchenden sehr gut angenommen wird. Unabhängig davon, ob ein Datenschutzbeauftragter, ein Geschäftsführer, ein Arzt, eine Bürokraft, ein Schüler, ein Bürger, ein Vereinsmitglied etc. anrief – wir waren stets bemüht, uns telefonischen Anfragen anzunehmen.

2.3 Datenschutzverletzungen

Wie schon im letzten Jahr befürchtet und im vergangenen Tätigkeitsbericht prognostiziert, ist die Zahl der Meldungen von Datenschutzverletzungen im Jahr 2019 noch einmal erheblich gestiegen. Die Meldevorschrift aus Art. 33 DS-GVO zeigt tatsächlich Wirkung, auch wenn gerade bei kleineren Unternehmen die Meldeverpflichtung und der Ablauf der Meldung immer noch nicht geläufig sein dürften.

Neben den Beschwerden und den Beratungen prägen daher mittlerweile auch Vorgänge zu Datenschutzverletzungen unseren Arbeitsalltag. In der unten aufgeführten Grafik werden die bei uns eingegangenen Meldungen nach Art. 33 DS-GVO, die von den jeweiligen Verantwortlichen abgegeben wurden, dargestellt. Weitere Informationen zum Thema Datenschutzverletzungen im Allgemeinen sind im Kapitel 17 dieses Berichts zu finden, wenngleich wir dieses Mal von der Darstellung einzelner Fallkonstellationen meldepflichtiger Vorfälle Abstand nehmen.



2.4 Abhilfemaßnahmen

Für diesen Abschnitt haben die Aufsichtsbehörden vorgeschlagen, die Abhilfemaßnahmen nach Art. 58 Abs. 2 DS-GVO aufzulisten. Im Einzelnen handelt es sich dabei um die Maßnahmen, die wir bereits im letzten Tätigkeitsbericht aufführten:

- Warnungen
  (Art. 58 Abs. 2 Buchst. a DS-GVO)
- Verwarnungen
  (Art. 58 Abs. 2 Buchst. b DS-GVO)
- Anweisungen und Anordnungen
  (Art. 58 Abs. 2 Buchst. c - g und j DS-GVO)
- Geldbußen
  (Art. 58 Abs. 2 Buchst. i DS-GVO)
- Widerruf von Zertifizierungen
  (Art. 58 Abs. 2 Buchst. h DS-GVO)

Auch wenn wir es wollten, ist es uns im Jahr 2019 leider nicht gelungen, unser internes Fachverfahren IGOR zur Verwaltung von Vorgängen so zu erweitern, dass die oben genannten Abhilfemaßnahmen statistisch ausgewertet werden können. Wir hoffen, dass uns dies bald gelingt und wir im nächsten Tätigkeitsbericht dazu konkrete Angaben liefern können.

2.5 Europäische Verfahren

Wie im vergangenen Bericht erklärt, ist es für uns erforderlich, die in das IMI-System eingestellten Vorgänge zur Feststellung der Betroffenheit (Art. 56 DS-GVO), der Federführung (Art. 56 DS-GVO) und die Anzahl der Verfahren gemäß Kapitel VII DS-GVO (Zusammenarbeit und Kohärenz) regelmäßig zu sichten. Erst dann kann festgestellt werden, ob und wann wir uns bei Verfahren, die in das IMI-System eingestellt sind, als federführende oder betroffene Aufsichtsbehörde melden sollen bzw. müssen.

Allerdings mussten wir bislang erkennen, dass alleine diese Sichtung im IMI-System und auch die Pflege der IMI-relevanten Vorgänge innerhalb unserer Behörde einen enormen Aufwand bedeuten. Zum Redaktionsschluss dieses Berichts waren wir leider nicht in der Lage, valide Zahlen, aufgeschlüsselt nach den unterschiedlichen Kategorien, zur Verfügung zu stellen. Hintergrund hierbei ist, dass wir seit Beginn der DS-GVO längst eine vierstellige Anzahl an IMI-Vorgängen haben, die uns in irgendeiner Weise tangieren – zusätzlich zu den ohnehin schon in unserer Behörde laufenden Verfahren. Um diesem Umstand Rechnung zu tragen, haben wir bei der Besetzung der neuen Planstellen besonders darauf geachtet, dass eine dauerhafte Begleitung der IMI-Vorgänge von uns gewährleistet werden kann. Auch unser internes Verwaltungsprogramm wurde angepasst, damit wir künftig nicht nur eine statistische Auswertung durchführen, sondern IMI-Vorgänge auch mit einem erhöhten Automatisierungsgrad in unseren Arbeitsalltag integrieren können.

2.6 Förmliche Begleitung von Rechtsetzungsvorhaben

Eine förmliche Begleitung von Rechtsetzungsvorhaben, d. h. Abgabe einer Stellungnahme zu uns betreffenden Gesetzesvorhaben, fand im Jahr 2019 nicht statt.

2.7 Ressourcen

Im Berichtszeitraum haben wir durch den Haushaltsgesetzgeber im engeren Sinne, den Bayerischen Landtag, im Rahmen des Nachtragshaushalts keine neuen Stellen erhalten, aber durch den Bayerischen Staatsminister des Innern, für Integration und Sport, im Zuge einer Haushaltsumschichtung nach Art. 6 des Bayerischen Haushaltsgesetzes im März 2019 die Zusage für Haushaltsmittel bekommen, mit denen wir neun Stellen in der 2. und 3. Qualifikationsebene nicht nur für das Jahr 2019, sondern auf Dauer schaffen konnten.

Im Sommer 2019 standen die Haushaltsmittel dann tatsächlich zur Verfügung, sodass wir zusätzliches Personal einstellen konnten. Von den neun Stellen wurden sieben Stellen ausgeschrieben und die meisten leider erst zum November 2019 besetzt. Zwei Stellen wurden bewusst noch nicht ausgeschrieben und besetzt, um erst die sieben neuen Mitarbeiterinnen und Mitarbeiter zu integrieren. Wir wollen dann feststellen, in welchem Bereich der Bedarf in den nächsten Monaten am größten ist, um zielgerichtet dort weitere Verstärkung einzusetzen. Es sollte damit auch dem neuen Präsidenten die Möglichkeit eingeräumt werden, eigene Schwerpunkte zu setzen.

Erfreulich war die positive Resonanz auf unsere Stellenausschreibungen, was auf der anderen Seite mit einem ziemlichen Aufwand für die Sichtung der Bewerbungsunterlagen und die Durchführung von Vorstellungsgesprächen verbunden war. Die größte Resonanz erfuhren wir bei der Ausschreibung einer Stelle in der Geschäftsstelle, auf die sich alleine 230 Menschen beworben haben.

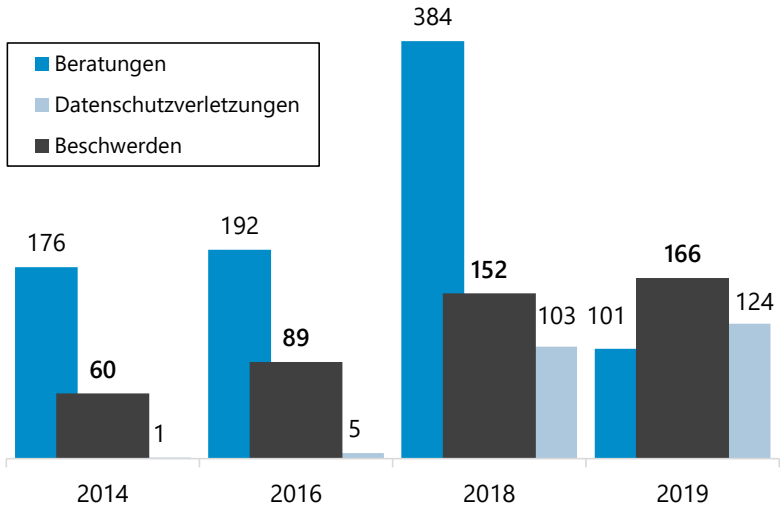
Dass im Laufe des Jahres vier von acht Juristinnen und Juristen das BayLDA vorübergehend oder auf Dauer verlassen haben und ersetzt werden mussten, was mit tatkräftiger Unterstützung des Personalsachgebiets des Bayer Staatsministeriums des Innern sehr gut gelungen ist, erschwerte die Personalsituation im Berichtsjahr für uns erheblich.

Die Personalentwicklung der letzten Jahre sieht wie folgt aus:

- Bis 31.12.2016: 16 Planstellen
- Bis 31.12.2017: 20 Planstellen
- Bis 31.12.2018: 24 Planstellen
- Bis 31.12.2019: 33 Planstellen

Rein rechnerisch hat sich damit die Anzahl der zu bewältigenden Aufgaben auf mehr Schultern verteilt. Wir haben nun zwar deutlich mehr Planstellen als noch vor wenigen Jahren, allerdings muss man sich bewusst machen: Auch deutlich mehr Arbeit. Wie der vorangegangenen Grafik des Schuldenbergs entnommen werden kann, hat sich die Zunahme der Mitarbeiteranzahl noch nicht relevant auf die Anzahl der Erledigungen ausgewirkt, da sich unser neues Personal im Wesentlichen in der Einarbeitung befindet. Entsprechend war die durchschnittliche Anzahl der Vorgänge pro Planstelle besonders bei den Beschwerden auffällig hoch, was dem unten aufgeführten Diagramm zu entnehmen ist.

Durchschnittliche Vorgänge pro Planstelle



2.8 Vorträge und Öffentlichkeitsarbeit

Wir haben auch im Jahr 2019 eine erhebliche Anzahl von Vorträgen gehalten und dabei überwiegend Datenschutzbeauftragte geschult bzw. informiert. Ein besonderes Anliegen war es uns wieder, die meist von den Industrie- und Handelskammern und der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) organisierten ERFA-Kreise in München, Nürnberg, Würzburg, Coburg und Bayreuth zu besuchen und dort die zahlreich vorab eingereichten Fragen zu beantworten.

Um ein Verständnis dafür zu bekommen, wie in anderen Mitgliedstaaten der EU, des Europäischen Wirtschaftsraums (EWR) oder einem Drittstaat mit angemessenem Datenschutzniveau das Verständnis für die DS-GVO ist, haben wir bei Veranstaltungen in der Schweiz, Großbritannien und Liechtenstein Vorträge gehalten bzw. an Veranstaltungen teilgenommen.

Im Rahmen unserer Öffentlichkeitsarbeit erweiterten wir fortlaufend unser Angebot auf unserer Website, damit Interessierte einfach und schnell Antworten auf ihre Fragen finden konnten. Dabei war es uns wichtig, die Informationen so herunter zu brechen und mit Mustern zu ergänzen, dass Vereine, Handwerker, freiberuflich Tätige und auch sehr kleine Unternehmen eine effektive praxisorientierte Unterstützung finden konnten.

3

Kontrollen und Prüfungen

3 Kontrollen und Prüfungen

3.1 Safer Internet Day 2019

Unsere Prüfung zur Passwortsicherheit und zum datenschutzkonformen Einsatz von Tracking-Tools offenbart Nachholbedarf bei großen Websites.

Wie bereits in den vorangegangenen Jahren haben wir uns auch 2019 wieder am Safer Internet Day aktiv beteiligt. Unter dem Motto „Together for a better internet" bot der Safer Internet Day vielen Institutionen die Möglichkeit, einen Beitrag für ein sicheres Internet zu leisten. Wir nutzten die Gelegenheit und führten eine umfangreiche Datenschutzkontrolle bei Websites ausgewählter Verantwortlicher durch. Schwerpunkte waren die Umsetzung der datenschutzrechtlichen Anforderungen bezüglich Cybersicherheit und Tracking.

Warum wir diese beiden Themen als Prüfschwerpunkte ausgemacht haben, erklärt sich in unserer Funktion als Aufsichtsbehörde: Spätestens seit Mai 2018 zeichnete sich ab, dass ein häufiges Beschwerdethema bei Bürgern die Information, die Einwilligung und das Setzen von Cookies bei Websites darstellt. Wir haben zahlreiche Eingaben dieser Art erhalten, die sich letztendlich allesamt um Nutzertracking im Internet drehten. Und da wir zudem viele Meldungen über Datenschutzverletzungen nach Art. 33 DS-GVO auf Grund mangelhafter Sicherheit bei Webdiensten registrierten, insbesondere bei der Absicherung der Logins, fiel die Entscheidung leicht, sowohl Tracking als auch Cybersicherheit bei Websites aktiv anzugehen.

Im Rahmen des Cybersicherheitschecks kontrollierten wir, wie Website-Betreiber den Nutzer durch den Registrierungs- und Login-Prozess begleiten und inwieweit sie dabei angemessen mit den Passwörtern ihrer Nutzer umgehen. Im Rahmen der mehrstufigen Prüfung wurden verschiedene Punkte in unterschiedlicher Tiefe untersucht, von der verwendeten Verschlüsselung, der Passwortstärke bis hin zu Absicherungen gegen Angriffsversuche auf Login-Daten.

Bei der Untersuchung im Schwerpunkt Tracking wurden zahlreiche Prüffragen aus dem Bereich der Information und Einwilligung abgehandelt, z. B. „Wird der Nutzer vorab transparent über den Einsatz von Tracking-Tools informiert?", „Werden die Anforderungen an eine wirksame Einwilligung von der Website erfüllt?" und „Kann der Nutzer die Profilbildung durch Tracking-Tools auf der Website selbst durch eigene Einstellungen verhindern?". Hier befanden sich auf Grund konkret vorliegender Beschwerden von Bürgern bereits 40 Websites auf unserer Prüfliste, wobei alle dieser Websites ausschließlich von großen bzw. sehr großen bayerischen Firmen betrieben und verantwortet werden.

Obwohl wir ausschließlich Websites von größeren Unternehmen, zum Teil börsennotierte Großkonzerne, hinsichtlich längst bekannter Sicherheitsanforderungen untersuchten, mussten wir feststellen, dass zahlreiche Defizite vorhanden waren. Die getroffenen Sicherheitsmaßnahmen mussten oft als unzureichend eingestuft werden. In einer umfassenden Ergebnispräsentation haben wir auf unserer Website die einzelnen Ergebnisse zur Verfügung gestellt, bewertet und über den Hintergrund des jeweiligen Prüfpunktes informiert. Da das Ergebnis so ernüchternd ausfiel, werden wir auch weiter aktive Kontrollen im Cybersicherheitsumfeld durchführen und bei Verstößen unser Potential aus dem Maßnahmenkatalog ausschöpfen. Ob dabei allen Verantwortlichen bereits bekannt ist, dass ein Verstoß gegen die Vorschriften aus Art. 32 DS-GVO zur Sicherheit der Verarbeitung mit einer nicht unerheblichen Geldbuße geahndet werden kann, mögen wir nicht beurteilen.

Auch im Bereich Tracking fiel das Ergebnis unserer Prüfung desolat aus: Keine der geprüften Websites erfüllte die Anforderung an eine zulässige Einwilligung nach der DS-GVO, obwohl die Websites Tracking-Tools von Drittanbietern eingebunden hatten und somit eine Datenverarbeitung durch fremde Dienste veranlassten. Einige Website-Betreiber verschwiegen den Einsatz von Tracking-Tools, andere hingegen informierten pauschal über verschiedenste Tools, die zum Teil gar nicht auf der Website eingebunden sind. Im Ergebnis wurde der Nutzer nur selten transparent darüber informiert, ob und welche seiner Daten für welche Zwecke verarbeitet werden. Wir haben uns daher veranlasst gesehen, entsprechende Verfahren gegen die Verantwortlichen einzuleiten und die Verstöße dadurch abzustellen. Weitere Informationen sind den Pressemitteilungen vom 1. und 5. Februar 2019 sowie der dazugehörigen Ergebnispräsentation zu entnehmen.

www.lda.bayern.de/media/pm2019_3_de.pdf

3.2 Videoüberwachung in Shisha-Bars

Beschwerden, die Videoüberwachung zum Gegenstand haben, nehmen quantitativ seit vielen Jahren einen Spitzenplatz in unserer Tätigkeit ein. Regelmäßig erreichen uns Beschwerden über Videokameras in Restaurants, Bars und anderen gastronomischen Einrichtungen. Im Rahmen einer Vor-Ort-Kontrolle haben wir daher im Berichtszeitraum mehrere sog. Shisha-Bars überprüft, gegen die Beschwerden bei uns eingegangen waren.

Die Prüfung ergab insgesamt ein gemischtes Bild. Im Falle einer der überprüften Bars waren im Gastraum, in dem sich wohl vornehmlich junges Publikum aufhält, vier Videokameras angebracht, durch die mehr oder minder der gesamte Gastraum erfasst wurde. Als Grund für die Überwachung gab der Betreiber pauschal Sicherheitsinteressen an. Insbesondere wolle er für den Fall, dass in seiner Bar Straftaten wie beispielsweise Diebstahl begangen werden, entsprechendes Beweismaterial zur Verfügung haben. Ferner habe es vor längerer Zeit einen Einbruchsversuch gegeben. Diese Zwecke vermögen die Videoüberwachung des Gastraums nicht zu rechtfertigen. Wir stellten gegenüber dem Unternehmen klar, dass es in einem gastronomischen Betrieb wie etwa seiner Bar nicht zulässig ist, die Bereiche, in denen sich die Gäste zum Verzehr von Speisen und Getränken oder zum „Relaxen" aufhalten, mit Videokameras zu erfassen.

Als zulässig haben wir lediglich die Erfassung des unmittelbaren Eingangsbereichs und auch dies nur außerhalb der Öffnungszeiten bewertet. Diese Erfassung zum Zwecke der Dokumentation etwaiger Einbruchsversuche kann als ein berechtigtes Interesse des Unternehmens anerkannt werden, so dass die Verarbeitung personenbezogener Daten zu diesem Zweck insoweit datenschutzrechtlich nach Art. 6 Abs. 1 Buchst. f DS-GVO legitimiert ist, dies jedoch begrenzt auf die Zeiten, in denen sich kein Personal vor Ort befindet, so dass etwaige Einbruchsversuche andernfalls somit nicht dokumentiert werden könnten. Was die Speicherdauer betrifft, erachten wir nach wie vor eine Dauer von grundsätzlich bis zu maximal 72 Stunden als ausreichend, da während dieses Zeitraums normalerweise die Auswertung der Videoaufzeichnungen möglich ist.

In einer der Bars wurde zudem der Kassenbereich von einer Videokamera überwacht. Zweck der Überwachung war hier – wie häufig in der Gastronomie und im Handel – die Verhinderung von sog. Wechselgeldbetrug durch Mitarbeiter bzw. Aufdeckung entsprechender Vorgänge. Dies bewerteten wir als zulässig unter der Voraussetzung, dass tatsächlich durch entsprechende Kameraeinstellung gewährleistet ist, dass lediglich der unmittelbare Kassenbereich erfasst wird, nicht jedoch der Mitarbeiter insgesamt.

Bei mehreren der überprüften Bars waren Kameras zudem außen am Gebäude angebracht, die z. T. größere Bereiche des Gehsteigs erfassten. Hier ist höchstens eine Erfassung eines schmalen, unmittelbar an die Gebäudehaut bzw. Eingangstür angrenzenden Bereichs hinnehmbar und nur, sofern gewährleistet ist, dass nicht die gesamte Breite des Gehsteigs erfasst wird, sondern Fußgänger die Möglichkeit haben, den Gehsteig zu nutzen, ohne von den Kameras erfasst zu werden.

Der Erlass förmlicher Anordnungen gegen die im Rahmen dieser Prüfungsaktion von uns überprüften Betriebe war nicht erforderlich, weil die Betriebe unsere mündlich mitgeteilten Hinweise befolgt haben.

3.3 Rechenschaftspflicht beim Einsatz von Tracking-Tools

Viele Unternehmen kennen ihre eigenen Verarbeitungstätigkeiten oft nicht hinreichend und befassen sich nur ungenügend mit den rechtlichen Anforderungen der DS-GVO.

Nach den ernüchternden Ergebnissen der Website-Prüfung im Rahmen des Safer Internet Days 2019, siehe Kapitel 3.1 dieses Berichts, haben wir aufsichtliche Verfahren gegen die Verantwortlichen eingeleitet.

Bei der weitergehenden Prüfung stellte sich heraus, dass sich viele Verantwortliche nicht im Klaren darüber sind, welche Dienste auf ihren Websites überhaupt eingebunden werden. Grund hierfür ist häufig, dass die Betreuung der Websites von Agenturen übernommen wird oder die Marketing-Abteilung des Verantwortlichen selbstständig Tracking-Tools zur Werbefinanzierung in das Webangebot integriert.

Bedauerlicherweise erfolgt dies in vielen Fällen, ohne dass der interne oder externe Datenschutzbeauftragte eingebunden wird. Nicht selten ergab unsere Kontrolle, dass selbst die Geschäftsleitung hiervon keine Kenntnis hatte.

Dies veranlasste uns, die Prüfung umzustellen. Schwerpunkt der Prüfung war nicht mehr nur die Frage, ob für die Einbindung von Tracking-Tools eine Einwilligung eingeholt werden muss oder Art. 6 Abs. 1 Buchst. f) DS-GVO eine ausreichende Rechtsgrundlage ist. Da die Website-Prüfung grundlegende Mängel im Datenschutz-Management zu Tage brachte, prüften wir auch, ob die Verantwortlichen ihrer Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO hinreichend nachgekommen sind.

Wenngleich die Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO eine der wenigen großen Veränderungen des neuen Datenschutzrechts ist, so hätte jeder Verantwortliche in den letzten Jahren die Gelegenheit gehabt, sich hinreichend damit auseinanderzusetzen.

Sowohl auf deutscher als auch europäischer Ebene haben sich die Datenschutzaufsichtsbehörden in mehreren Veröffentlichungen zur Rechenschaftspflicht geäußert, zuletzt in der „Orientierungshilfe für Anbieter von Telemedien".

www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf

Zudem prüften wir seit Oktober 2018 die Rechenschaftspflicht bei Großkonzernen. Ziel dieser Prüfung war es, festzustellen, inwieweit große Unternehmen in der Lage sind, die Einhaltung der gesetzlichen Vorgaben aus der DS-GVO nachzuweisen. Zu diesem Zweck hatten wir einen Prüfkatalog mit 50 Fragen zur Rechenschaftspflicht mit folgenden Schwerpunkten erstellt:

- Aufbauorganisation
- Basis-Anforderungen
- Datenschutzkonforme Verarbeitung
- Umgang mit Betroffenenrechten
- Umgang mit Datenschutzverletzungen

Über diese Prüfung wurde in einer eigenen Pressemitteilung vom 07.11.2018 informiert.

www.lda.bayern.de/media/pm2018_17_de.pdf

Zudem haben wir den vollständigen Prüfkatalog zur Rechenschaftspflicht veröffentlicht:

www.lda.bayern.de/media/pruefungen/201810_rechenschaftspflicht_fragebogen.pdf

Trotz dieser und der zahlreichen Veröffentlichungen der Aufsichtsbehörden insgesamt waren viele Verantwortliche in puncto Rechenschaftsplicht überfordert. Einige Unternehmen waren der Ansicht, es sei damit getan, wenn man der Aufsichtsbehörde die Datenschutzbestimmung der Website ausdruckt oder erklärt, „Werbung ist ein berechtigtes Interesse und deshalb darf man das".

Das dies keinesfalls ausreichend ist, um den Nachweis zu erbringen, dass eine Datenverarbeitung rechtmäßig erfolgt, dürfte auf der Hand liegen. Dabei ist es keine große Herausforderung, die Rechenschaftspflicht zu erfüllen. Die DS-GVO enthält eine Vielzahl von Nachweispflichten, die der Verantwortliche ohnehin erfüllen muss.

Hierzu gehören u. a.

- Verzeichnis über Verarbeitungstätigkeiten (Art. 30 DS-GVO),
- Datenschutz-Folgenabschätzung (Art. 35 DS-GVO),
- genehmigte Verhaltensregeln (Art. 40 DS-GVO),
- Zertifizierung (Art. 42 DS-GVO),
- Meldungen über Datenschutzverletzungen (Art. 33 DS-GVO) sowie
- Verträge zur Auftragsverarbeitung (Art. 28 Abs. 3 DS-GVO).

Darüber hinaus kann die Rechenschaftspflicht durch sonstige Datenschutzdokumentation erfolgen, wie beispielsweise hierdurch:

- Vertragsmanagement
- Konzepte zur Sicherstellung der Betroffenenrechte
- Prozesse der Datenschutzorganisation
- Einführung von Datenschutzrichtlinien
- Interne oder externe Audits
- Mitarbeiterschulungen
- Rechtsgutachten
- Zertifizierungen nach DIN- und ISO-Normen
- Sonstige Aufzeichnungen wie z. B. Berichte, Vermerke oder Protokolle

Sinn und Zweck der Dokumentation ist es, dass der Verantwortliche sich umfassend mit den weitergehenden Anforderungen der DS-GVO auseinandersetzt und prüft, ob eine Datenverarbeitung rechtmäßig erfolgt oder ggf. noch weitere Maßnahmen erforderlich sind, um die rechtmäßige Verarbeitung sicherzustellen.

Im Rahmen des aufsichtlichen Verfahrens haben die meisten Verantwortlichen erheblich nachgebessert, sodass wir das Thema Rechenschaftspflicht abschließen konnten.

Hiervon unberührt bleibt die Frage, ob für den Einsatz von Tracking-Tools zwingend die Einwilligung der Nutzer eingeholt werden muss. Hierzu führen wir das aufsichtliche Verfahren fort bis hin zur Anordnung. Sollte der Verantwortliche mit unserer Entscheidung nicht einverstanden sein, ist mit einer Klage vor dem Verwaltungsgericht zu rechnen.

3.4 Windows 10 und Telemetriedaten

Die Datenübertragung an Microsoft lässt sich mit der Enterprise-Version deaktivieren.

Der Einsatz von Windows 10, insbesondere die Übermittlung von sogenannten Telemetriedaten von einem Windows 10 Rechner an Microsoft, beschäftigt die Datenschutzaufsichtsbehörden schon seit längerer Zeit. Aus diesem Grund hat die Datenschutzkonferenz eine Unterarbeitsgruppe des Arbeitskreises Technik „Windows 10" gegründet, die eine datenschutzrechtliche Bewertung der Datenflüsse an Microsoft erstellen soll.

www.datenschutzkonferenz-online.de/media/dskb/20190403_positionierung_windows_10.pdf

Diese Facharbeitsgruppe hat sich im Dezember 2019 zu einer Laboranalyse von Windows 10, die federführend von uns und dem Bayerischen Landesbeauftragten für den Datenschutz durchgeführt wurde, in Ansbach getroffen. Ebenfalls waren Mitarbeiter von Microsoft eingeladen (von denen über 10 Personen, überwiegend aus dem technischen Bereich, von Microsoft aus den USA gekommen sind), um alle technischen Fragen, die bei der Laboranalyse aufkommen könnten, zu beantworten.

Es wurde ein Testszenario mit einem Windows 10 Rechner, der eine Enterprise-Version (Version 1909) installiert hatte, derart aufgebaut, dass alle Datenflüsse von diesem Rechner noch innerhalb des Labornetzes mittels einer Man-in-the-Middle-Analyse aufgezeichnet wurden. Dabei wurde das System mit von Microsoft offiziell zur Verfügung gestellten Informationen und Tools so konfiguriert, dass das Telemetrielevel „Security" eingestellt war und möglichst alle Datenflüsse deaktiviert werden konnten.

Im Rahmen dieser Labor-Analyse wurde festgestellt, dass die Telemetriedaten von einem Windows 10 Rechner mit der Enterprise-Version komplett deaktivierbar sind. Ausschließlich Aufrufe an (Microsoft-)Server, die aktuelle kryptographische Zertifikate liefern, waren durch diese Konfiguration nicht abschaltbar, da diese für einen tagesaktuellen sicheren Betrieb eines Windows 10-Systems (z. B. bei Rückruf eines ungültig gewordenen SSL-Wurzelzertifikates) erforderlich sind. Auch diese Aufrufe können durch gezielte Systemkonfigurationen unterbunden werden, wenngleich ein solches Vorgehen aus Gründen der Sicherheit keineswegs empfehlenswert ist.

Vom Ergebnis konnte bei diesem Treffen in unserem technischen Labor festgestellt werden, dass die datenschutzrechtlich kontrovers diskutierten Telemetriedaten bei Einsatz der Enterprise Version (und damit auch bei der Education-Version) im überprüften Szenario deaktivierbar sind.

Sollte sich dieses Ergebnis beim realen Einsatz von Windows 10 bei Unternehmen bestätigen, dann stellt zumindest der Umgang mit Telemetriedaten bei Windows 10 Enterprise (auch in verwalteten Umgebungen) keinen datenschutzrechtlichen Hinderungsgrund eines Einsatzes dieses Betriebssystems dar. Wie dagegen der Einsatz von Windows 10 Pro bei Verantwortlichen zu bewerten ist, bei dem die Telemetriedaten zwar reduziert, aber bekanntlich nicht komplett abgeschaltet werden können, könnte möglicherweise ein weiterer Arbeitsauftrag der Datenschutzkonferenz (DSK) werden.

4

Der betriebliche Datenschutzbeauftragte

4 Der betriebliche Datenschutzbeauftragte

4.1 Änderung des BDSG

Gemäß einer Änderung des BDSG ist ein Datenschutzbeauftragter jetzt erst ab 20 Beschäftigten zu benennen.

Am 26. November 2019 trat das Gesetz zur Anpassung des Datenschutzrechts in Kraft. Durch die Gesetzesänderung wurde die bisherige Anzahl von zehn Beschäftigten gemäß § 38 Abs. 1 BDSG auf 20 angehoben. Künftig müssen Betriebe erst einen betrieblichen Datenschutzbeauftragten benennen, wenn 20 oder mehr Mitarbeiterinnen und Mitarbeiter ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Dadurch sollen laut der Gesetzesbegründung vor allem kleinere und mittlere Unternehmen sowie ehrenamtlich tätige Vereine „entlastet" werden.

Dies bedeutet zwar zunächst eine organisatorische Erleichterung. Dennoch sind selbstverständlich die Regelungen des Datenschutzrechts nach wie vor auch in kleineren Betrieben einzuhalten. Ob ein Datenschutzbeauftragter benannt werden muss oder nicht, entbindet nicht von der Pflicht zur Einhaltung des Datenschutzrechts. Weiterhin gilt es zu beachten, dass auch unabhängig von der Anzahl der Beschäftigten ein Datenschutzbeauftragter verpflichtend zu benennen ist, wenn sich dies aus Art. 37 DS-GVO oder § 38 BDSG ergibt. Natürlich kann freiwillig jederzeit ein Datenschutzbeauftragter benannt werden.

In der Praxis wird das dazu führen, dass einige Verantwortliche einen Datenschutzbeauftragten nicht mehr benennen, d. h. auch nicht mehr haben müssen. Die Frage, wie Verantwortliche in diesen Fällen ihren Datenschutzbeauftragten, wenn sie ihn nicht freiwillig weiter beschäftigen wollen, wieder „loswerden", ist keine datenschutzrechtliche, sondern ausschließlich eine arbeits- (für den internen DSB) oder zivilrechtlich (für den externen DSB) zu entscheidende Frage.

www.lda.bayern.de/media/pm/pm2019_15.pdf

4.2 Weiterhin Unsicherheit über Benennungspflicht

Die umstrittene Fragestellung im Zusammenhang mit der Benennungspflicht eines DSB nach BDSG, was „ständig" mit „automatisierter Datenverarbeitung" beschäftigt" bedeutet, wurde durch die Änderung des BDSG nicht gelöst.

Beim Thema „Benennung eines betrieblichen Datenschutzbeauftragten" erreichten uns nach wie vor Fragen, was unter den Begriffen „ständig", „automatisierte Datenverarbeitung" und/oder „beschäftigt" zu verstehen ist. Insbesondere über die Frage, was unter ständig zu verstehen ist, gibt es unter den deutschen Aufsichtsbehörden (im Gegensatz zu den allermeisten sonstigen Auslegungsfragen) keine einheitliche Auffassung. So wird zum Beispiel vertreten, dass ein Trainer ständig personenbezogene Daten verarbeitet, der regelmäßig einmal in der Woche für eine kurze Zeit die Liste seiner zu trainierende Personen auf seinem Laptop aktualisiert, Mannschaftsaufstellungen erstellt o. ä. Wir vertreten die Auffassung, dass jemand nur dann ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt ist, wenn dies den überwiegenden Anteil seiner Beschäftigung für den Verantwortlichen darstellt.

Die entsprechende Kurzinformation ist auf unserer Website unter FAQ („Muss ein Verein einen Datenschutzbeauftragten benennen?) veröffentlicht:

www.lda.bayern.de/de/faq.html

5

Betroffenenrechte

5 Betroffenenrechte

5.1 Auskunft

Das zentrale Betroffenenrecht, das Recht auf Auskunft, erweist sich in der Praxis nach wie vor als schwer greifbar. Dies spiegelt sich auch durch die hohe Anzahl von Datenschutzbeschwerden wieder, bei denen Betroffene mit der Beauskunftung durch Verantwortliche unzufrieden waren und sich an uns wenden.

Die Sicherstellung der Betroffenenrechte ist eine Kernanforderung der DS-GVO an Verantwortliche – im Alltag beginnen diese häufig mit dem Wunsch eines Betroffenen, sein Recht auf Auskunft geltend zu machen. Da wir sehr viele Datenschutzbeschwerden erhalten, wenn die Betroffenen nicht mit der Sicherstellung Ihrer Rechte zufrieden sind, haben wir im folgenden sieben „No-Go's" aufgeschrieben, die von Verantwortlichen und auch Betroffenen unbedingt zu vermeiden sind:

No-Go 1: Ignorieren von Auskunftsbegehren bei Identitätszweifeln

Bestehen Zweifel an der Identität des Betroffenen, können gemäß Art. 12 Abs. 6 DS-GVO Informationen als Nachweis der Identität angefordert werden. Die pauschale Behauptung von Zweifeln an der Identität genügt nicht, um Auskunftsbegehren per se unbeantwortet zu lassen.

Beispiel Telefax: Auch Anfragen per Telefax ohne Absenderkennung müssen vom Verantwortlichen bearbeitet werden. Von einer Identifikationssicherheit kann grundsätzlich auch im Falle eines Telefaxes mit Absenderkennung nicht zweifelsfrei ausgegangen werden, da die Möglichkeit der Fälschung besteht.

No-Go 2: Auskunft über ausschließlich Stammdaten als personenbezogene Daten

Die bloße Beauskunftung von Stammdaten der betroffenen Person genügt nicht, um den Anforderungen des Art. 15 DS-GVO gerecht zu werden. Zu den personenbezogenen Daten gehören neben den Stammdaten unter anderem auch die Folgenden:

- Daten, welche Rückschlüsse auf das Konsumverhalten des Betroffenen geben (Einkäufe, Bestellungen, etc.)
- Kontodaten
- Körperliche Merkmale
- Interne Vermerke und Bewertungen
- Gesprächs- und Telefonvermerke

Bei einer großen Menge von personenbezogenen Daten kann der Verantwortliche eine Präzisierung der Anfrage anfordern.

No-Go 3: Einreichen der Beschwerde vor Verstreichen der Frist

Nicht zu vernachlässigen ist, dass nach Art. 12 Abs. 3 DS-GVO der Verantwortliche dazu verpflichtet ist, der betroffenen Person die sie betreffenden Informationen „unverzüglich, in jedem Fall aber innerhalb eines Monats" zur Verfügung zu stellen. Ist aufgrund der Komplexität und Anzahl der Anträge eine Auskunft nicht innerhalb eines Monats möglich, kann eine Fristverlängerung von zwei Monaten unter Angabe der Gründe geltend gemacht werden. „Unverzüglich" bedeutet nicht, dass eine Reaktion auf die Anfrage sofort zu erfolgen hat, sondern dass die Anfrage „ohne schuldhaftes Zögern" zu bearbeiten ist. Die Aufsichtsbehörde kann nur tätig werden, wenn die Reaktion innerhalb der Monatsfrist ausbleibt oder die Auskunft unvollständig oder nicht rechtmäßig erfolgt ist.

No-Go 4: Zweck des Rechts auf Auskunft außer Acht lassen

Durch das Recht auf Auskunft haben betroffene Personen die Möglichkeit, die Rechtmäßigkeit der Verarbeitung ihrer personenbezogenen Daten zu überprüfen. Auf Basis dieses Wissens können weitere Betroffenenrechte, wie beispielsweise das Recht auf Berichtigung gemäß Art. 16 DS-GVO, ausgeübt werden. Mit dem Recht auf Auskunft sollen ausschließlich Datenschutzziele verfolgt werden. Dieses Recht soll nicht zur Sammlung von Beweisen für andere bestehende Konflikte dienen.

No-Go 5: Geltendmachung des Rechts auf Auskunft gegenüber dem Anwalt der Gegenseite

Ein Auskunftsrecht aus Art. 15 DS-GVO gegenüber Rechtsanwälten, die nicht für den/die Auskunft-Begehrende(n) tätig wurden (sondern z. B. für die gegnerische Partei) besteht gemäß § 29 Abs. 1 Satz 2 BDSG i. V. m. § 43a Abs. 2 BRAO nicht, weil die erwünschten Informationen einer gesetzlichen Verschwiegenheitspflicht unterfallen. Das datenschutzrechtliche Auskunftsrecht liefert somit keine Möglichkeit, um vom Anwalt der Gegenseite die Offenlegung von Informationen zu erzwingen (siehe auch das anschließende Kapitel 5.2 dieses Berichts).

No-Go 6: Beschwerde ohne beweiskräftige Nachweise

Wir als Datenschutzaufsichtsbehörde wissen zunächst nicht, welche Daten der Verantwortliche konkret speichert und verarbeitet. Sind betroffene Personen der Auffassung, die Auskunft ist nicht richtig oder nicht vollständig, benötigen wir beweiskräftige Nachweise, welche die Aussage des Verantwortlichen widerlegen, um ihm gegenüber darauf Bezug nehmen zu können.

No-Go 7: Berufung auf unverhältnismäßigen Aufwand ohne Darlegung der Umstände

Bei Berufung auf einen unverhältnismäßigen Aufwand i.S.d. § 34 Abs. 1 Nr. 2 BDSG ist der Verantwortliche dazu verpflichtet, der betroffenen Person die konkreten Umstände darzulegen, welche den unverhältnismäßigen Aufwand begründen.

www.lda.bayern.de/de/thema_auskunft.html

5.2 Kein Auskunftsrecht gegenüber gegnerischem Rechtsanwalt

Gegenüber dem Rechtsanwalt der Gegenpartei besteht regelmäßig kein Auskunftsrecht, soweit die begehrten Informationen dessen Verschwiegenheitspflicht unterfallen.

Mitunter wenden sich betroffene Personen, die in Rechtsstreitigkeiten verwickelt sind, an den Rechtsanwalt der Gegenpartei und verlangen Auskunft nach Art. 15 DS-GVO hinsichtlich ihrer bei diesem Anwalt gespeicherten personenbezogenen Daten.

Aus unserer Sicht darf diesem Auskunftsverlangen in der Regel nicht nachgekommen werden. Denn das Auskunftsrecht ist gemäß Art. 23 Abs. 1 Buchst. g DS-GVO i.V.m. § 29 Abs. 1 Satz 2 BDSG ausgeschlossen, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift geheim gehalten werden müssen. Hierzu zählen insbesondere solche Informationen, die der berufsrechtlichen Verschwiegenheitspflicht unterfallen, also grundsätzlich alles, was dem Rechtsanwalt in Ausübung seines Berufs bekannt geworden ist (§ 43a Abs. 2 Berufsrechtsanwaltsordnung).

Etwas anderes gilt nur dann, wenn es sich um Tatsachen handelt, die offenkundig sind oder die ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Diese Voraussetzungen dürften jedoch nur selten erfüllt sein.

Das Auskunftsrecht eines Mandanten gegenüber seinem eigenen Rechtsanwalt bleibt selbstverständlich hiervon unberührt.

6

Datenschutz im Internet

6 Datenschutz im Internet

6.1 Facebook Fanpages

Betreiber von Facebook Fanpages haben nach derzeitigem Stand keine Möglichkeit, diese datenschutzkonform zu betreiben und müssen deshalb damit rechnen, Adressat von Anordnungen der Aufsichtsbehörden zu werden.

Der EuGH hat sich bereits mit Urteil vom 5. Juni 2018 (C-210/16) zur gemeinsamen Verantwortlichkeit von Facebook und Fanpage-Betreibern geäußert. Nach der Entscheidung des EuGH kann der Fanpage-Betreiber nicht mehr allein auf die datenschutzrechtliche Verantwortung von Facebook verweisen, sondern ist für die Einhaltung des Datenschutzes gegenüber den Fanpage-Besuchern (mit-)verantwortlich.

Das bedeutet konkret, dass sowohl Facebook als auch die Fanpage-Betreiber ihrer Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO nachkommen müssen. Jeder Fanpage-Betreiber muss sicherstellen, dass die seiner Verantwortung unterliegenden Verarbeitungstätigkeiten gem. Art. 6 Abs. 1 DS-GVO rechtmäßig sind. Dies gilt auch in den Fällen, in denen der Fanpage-Betreiber die Verarbeitungstätigkeiten nicht unmittelbar selbst ausführt, sondern durch Facebook durchführen lässt.

Das Problem ist, dass der Fanpage-Betreiber ohne hinreichende Kenntnis über die Verarbeitungstätigkeiten nicht in der Lage ist, zu bewerten, ob die Verarbeitung rechtmäßig erfolgt. Aus diesem Grund hat die Datenschutzkonferenz sich schon mehrfach zu Facebook-Fanpages positioniert und gefordert, dass Facebook entsprechend nachbessert, sodass die Fanpage-Betreiber ihrer Verantwortlichkeit entsprechend den Anforderungen der DS-GVO gerecht werden können.

Auch wir sind der Auffassung, dass ein datenschutzkonformer Betrieb einer Fanpage nicht möglich ist, solange Facebook diesen Pflichten nicht nachkommt. Daran ändert auch der Umstand nichts, dass Facebook im Oktober 2019 das „Page-Controller-Addendum", die Vereinbarung gem. Art. 26 DS-GVO, erheblich geändert und ergänzt hat.

Die Pflicht, eine Vereinbarung gem. Art. 26 Abs. 1 DS-GVO abzuschließen, ist zunächst nur eine formale Anforderung. Sie entbindet jedoch nicht davon, dass der Fanpage-Betreiber seine weiteren datenschutzrechtlichen Anforderungen, insbesondere seine Rechenschaftspflicht erfüllt.

Da nach derzeitigem Stand leider nicht davon auszugehen ist, dass die für Facebook in Europa federführend zuständige Aufsichtsbehörde dieser Situation abhilft, müssen Fanpagebetreiber als Mitverantwortliche damit rechnen, Adressat von aufsichtsbehördlichen Anordnungen zu werden.

www.datenschutzkonferenz-online.de/media/dskb/20180905_dskb_facebook_fanpages.pdf

6.2 Einsatz von Tracking-Tools

Die Datenschutzkonferenz hat zum Einsatz von Tracking-Tools eine „Orientierungshilfe Telemedien" veröffentlicht.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder veröffentlichte am 26. April 2018 eine Positionsbestimmung zur Anwendbarkeit des Telemediengesetzes (TMG) für nicht-öffentliche Stellen ab dem 25. Mai 2018. Ziel dieser Positionsbestimmung war es, den Website-Betreibern zu verdeutlichen, welche datenschutzrechtlichen Anforderungen beim Einsatz von Tracking-Tools auf Websites gelten.

Zahlreiche Beratungsanfragen verdeutlichten, dass eine einheitliche Positionsbestimmung der deutschen Aufsichtsbehörden nötig war. Immerhin herrschte viel Rechtsunsicherheit beim Verhältnis zwischen DS-GVO und dem bereichsspezifischen nationalen Recht, wie dem Telemediengesetz.

Nachdem die Positionsbestimmung veröffentlicht wurde, beschlossen die Datenschutzbehörden, eine Konsultation von betroffenen Wirtschaftsverbänden und Unternehmen durchzuführen. Anhand der Stellungnahmen im Konsultationsverfahren wurde die Positionsbestimmung konkretisiert und ergänzt.

Website-Betreiber können nunmehr die wesentlichen Anforderungen beim Einsatz von Tracking-Tools in der „Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien" nachlesen.

Besonders wichtig für Website-Betreiber ist, dass

- nicht jeder Einsatz von Cookies einwilligungsbedürftig ist,
- es nicht auf den Einsatz von Cookies ankommt, sondern sich die datenschutzrechtlichen Anforderungen immer an der Verarbeitungstätigkeit orientieren und
- die Voraussetzungen des Art. 6 Abs. 1 Buchst. f) DS-GVO anhand einer dreistufigen Prüfung zu ermitteln sind und der alleinige Hinweis, Direktwerbung sei ein berechtigtes Interesse, nicht ausreichend ist.

Außerdem erhalten Website-Betreiber wichtige Hinweise zur datenschutzkonformen Gestaltung eines sog. „Cookie-Banners". Die dort genannten Anforderungen gelten für den Fall, dass eine Einwilligung des Nutzers eingeholt werden muss.

www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf

6.3 Google Analytics

(Aktualisierte Fassung vom 31.01.2020)

Beim Einsatz von Google Analytics gelten neue Anforderungen. Die Datenschutzaufsichtsbehörden verlangen seit Geltung der DS-GVO die Einwilligung des Nutzers.

Wer eine Website betreibt, möchte in der Regel wissen, wie häufig diese besucht wird, ob es regelmäßige Nutzer gibt, aus welchen Ländern diese kommen und wie das Nutzungsverhalten auf der Seite ist. Dies wird allgemein als Reichweitenmessung bzw. Analytics bezeichnet. Eines der am häufigsten verwendeten Tools zur Reichweitenmessung ist Google Analytics.

Daher verwundert es nicht, dass uns zahlreiche Beschwerden wegen des Einsatzes von Google Analytics vorliegen. Viele Nutzer beschweren sich darüber, dass Google Analytics auf der Website nicht deaktiviert werden kann, keine Einwilligung eingeholt wird und über den Einsatz der Tools gar nicht oder nur unzureichend informiert wird.

Die Datenschutzaufsichtsbehörden des Bundes und der Länder haben in der „Orientierungshilfe für Anbieter von Telemedien" zusammengefasst, unter welchen Anforderungen der Einsatz von Tools zur Reichweitenanalyse und zum Tracking rechtmäßig ist.

Dennoch berufen sich weiterhin viele Website-Betreiber bei der Einbindung von Google Analytics oder vergleichbaren Analysewerkzeugen auf alte, längst überholte und zurückgezogene Veröffentlichungen der deutschen Aufsichtsbehörden.

Das Tool Google Analytics wurde jedoch in den vergangenen Jahren fortentwickelt und mit Geltung der DS-GVO änderte sich auch zwangsläufig die rechtliche Bewertung. Website-Betreiber müssen daher sorgfältig prüfen, wie Google Analytics eingesetzt, also konfiguriert wurde,

und welche rechtlichen Anforderungen daraus resultieren.

Beispielsweise ist die sog. „Datenfreigabe“ an Google standardmäßig aktiviert. Unter Berücksichtigung der „Orientierungshilfe für Anbieter von Telemedien“ bedeutet das Folgendes: Räumt der Website-Betreiber Google die Möglichkeit ein, die Daten der Webseitenbesucher zu eigenen Zwecken zu verwenden, erfordert dies eine Einwilligung der Nutzer.

Website-Betreiber, die Nutzer ohne Vorliegen einer Einwilligung tracken, begehen einen Datenschutzverstoß, der mit einer empfindlichen Geldbuße geahndet werden kann.

Neben der Frage, ob Google Analytics rechtmäßig eingesetzt wird oder nicht, sollte der Website-Betreiber auch prüfen, ob er hinreichend über Google Analytics in den Datenschutzbestimmungen informiert.

Im Übrigen gilt dies nicht nur für Google Analytics, sondern auch für Tracking-Dienste anderer Anbieter.

www.lda.bayern.de/media/pm/pm2019_14.pdf

Hinweis:
Das Kapitel 6.3 des Tätigkeitsberichts in der Fassung vom 28.01.2020 stellte einen veralteten Redaktionsstand dar. Aus diesem Grund wurde das Kapitel mit der Fassung vom 31.01.2020 aktualisiert. Dieser Stand entspricht auch unserer Hausmeinung.

7

Steuerberater und Rechtsanwälte

7 Steuerberater und Rechtsanwälte

7.1 Anfertigung von Ausweiskopien durch Steuerberater

Steuerberater haben unabhängig von der tatsächlichen Durchführung einer Risikoanalyse das Recht, Kopien von Personalausweisen zur Identitätsprüfung anzufertigen.

Steuerberater sind nach dem Geldwäschegesetz in Ausübung ihres Berufs verpflichtet, die Identität ihrer Vertragspartner zu identifizieren (§ 2 Abs. 1 Nr. 12 i.V.m. § 10 Abs. 1 Nr. 1 GWG). Geschieht dies mittels Vorlage eines Personalausweises, so hat der Steuerberater das Recht, diesen zu kopieren (§ 12 Abs. 1 Satz 1 Nr. 1 i.V.m. § 8 Abs. 2 Satz 2 GWG). Dieses Recht besteht unabhängig von der Frage, ob der Steuerberater im Vorfeld eine Risikoanalyse durchgeführt hat. Zwar ist der Steuerberater auch zur Durchführung einer Risikoanalyse gesetzlich verpflichtet (§ 4 Abs. 1, Abs. 2, § 5 GWG) und handelt bei Nichtbeachtung dieser Pflicht ordnungswidrig (§ 56 Abs. 1 Nr. 2 GWG). Die Identifizierungspflicht bleibt hiervon jedoch unberührt.

Denn selbst wenn der Steuerberater bei Durchführung der Risikoanalyse zu dem Ergebnis kommt, dass nur ein geringes Risiko besteht, müssen vereinfachte Sorgfaltspflichten erfüllt werden (§ 14 Abs. 1 Satz 1 GWG). Die Identitätsprüfung kann – nicht muss – in diesem Fall auch durch Vorlage anderer Dokumente erfolgen (§ 14 Abs. 2 Satz 1 Nr. 2 GWG).

8

Versicherungswirtschaft und Banken

8 Versicherungswirtschaft und Banken

8.1 Auskunftsrecht gegenüber Versicherungsunternehmen

Wir halten die in der Versicherungsbranche übliche, gestufte Beantwortung von Auskunftsersuchen auch vor dem Hintergrund neuerer Rechtsprechung für zulässig.

Mit Urteil vom 26. Juli 2019 hat das OLG Köln (Az.: 20 U 75/18) entschieden, dass sich das Auskunftsrecht eines Versicherungsnehmers gegenüber seinem Versicherungsunternehmen nicht nur auf die sogenannten „Stammdaten" beschränkt. Vielmehr müsse das Versicherungsunternehmen auch Auskunft über Gesprächsvermerke und Telefonnotizen erteilen, soweit darin Aussagen des Versicherungsnehmers oder Aussagen über den Versicherungsnehmer enthalten seien.

www.justiz.nrw.de/nrwe/olgs/koeln/j2019/20_U_75_18_Urteil_20190726.html

Gleichwohl gehen wir davon aus, dass sich dieses Urteil mit der bisherigen Praxis der Versicherungsunternehmen bei der Beantwortung von Auskunftsersuchen vereinbaren lässt. Soweit ein Versicherungsnehmer nur pauschal Auskunft über seine gespeicherten personenbezogenen Daten verlangt, darf sich das Versicherungsunternehmen in einem ersten Schritt mit der Beauskunftung der Stammdaten begnügen. Eine weitergehende Beauskunftung hat erst dann zu erfolgen, wenn das Auskunftsersuchen vom Versicherungsnehmer entsprechend präzisiert wird. Hierfür spricht auch Erwägungsgrund 63 Satz 7 zur DS-GVO.

8.2 Kein Auskunftsrecht hinsichtlich Geschäftsgeheimnissen

Eine Verpflichtung zur Offenlegung der genauen Berechnungsgrundlage hinsichtlich der Erhebung eines Risikozuschlags besteht nicht.

In einer Beschwerde wandte sich ein Versicherungsnehmer an uns, da ihm von seinem Versicherungsunternehmen Auskunft über die Berechnungsgrundlage hinsichtlich eines veranlassten Risikozuschlags in der Krankheitsvollkostenversicherung verweigert worden war.

Gem. Art. 15 Abs. 1 i. V. m. Abs. 3 DS-GVO hat die betroffene Person das Recht, von dem Verantwortlichen eine Auskunft über ihre personenbezogenen Daten, die verarbeitet werden, zu verlangen. Die Grenzen dieses Auskunftsrechts finden sich in Art. 15 Abs. 4, Art. 23 Abs. 1 DS-GVO i. V. m. § 29 Abs. 1 BDSG. Hiernach darf das Recht auf Auskunft die Rechte und Freiheiten anderer Personen nicht beeinträchtigen. Das Recht des Versicherers auf Wahrung seines Geschäftsgeheimnisses ist hierunter zu fassen. Die kalkulatorischen Grundlagen des Risikozuschlags sind als Geschäftsgeheimnis zu bewerten (vgl. § 2 GeschGehG) und unterliegen somit nicht der Auskunftspflicht.

9

Werbung und Adresshandel

9 Werbung und Adresshandel

9.1 Werbeprofiling bei Kreditinstituten

Kreditinstitute haben vermehrt die Daten ihrer Kunden zu Werbezwecken ausgewertet und sich zur Rechtfertigung dazu auf Art. 6 Abs. 1 f DS-GVO berufen.

Im Jahr 2019 wurden wir mehrfach auf Fälle aufmerksam, in denen Kreditinstitute die Daten ihrer Kunden neben dem Zweck der Vertragsdurchführung auch zum Zweck der Bildung eines umfangreichen Werbeprofils verarbeiten. In diese werbliche Verarbeitung wurden unter anderem Daten aus Beratungsgesprächen, Nutzungsdaten aus Online-Banking und Banking-Apps, Daten aus laufenden Verträgen und die Auswertung von Zahlungsverkehrsdaten einbezogen. Gestützt wurde diese Verarbeitung jeweils auf eine Interessensabwägung nach Art. 6 Abs. 1 Buchst. f DS-GVO.

Allerdings ist in aller Regel nicht davon auszugehen, dass bei einer derart umfassenden Profilbildung die werblichen Interessen des Kreditinstituts die berechtigten Interessen der Kunden an einem Ausschluss der Verarbeitung überwiegen. Daher sind wir der Ansicht, dass eine solche Verarbeitung nur in Verbindung mit einer Einwilligung des Kunden rechtskonform zu verwirklichen ist.

Ganz besonders gilt dies hinsichtlich der teilweise praktizierten Auswertung von Zahlungsverkehrsdaten, da z. B. die Angaben zum Verwendungszweck aus Überweisungen und Lastschriften oftmals auch besondere Kategorien von personenbezogenen Daten enthalten können (z. B. bei Zahlung von Mitgliedsbeiträgen an politische Parteien und Gewerkschaften oder Begleichung von Arztrechnungen). Bei dieser Art von besonders geschützten Daten verbietet Art. 9 DS-GVO generell, dass diese auf Basis einer Interessensabwägung im Sinne des Art. 6 Abs. 1 Buchst. f DS-GVO verarbeitet werden.

Näheres zu diesem Thema kann auf der Website der Datenschutzkonferenz dem Kurzpapier Nr. 3 sowie Ziffer 1.3.1 der Orientierungshilfe der Aufsichtsbehörden zur Direktwerbung entnommen werden.

www.datenschutzkonferenz-online.de/orientierungshilfen.html

9.2 Werbung per E-Mail oder SMS

Werbung per E-Mail oder SMS kann bei Bestandskunden auf der Basis des Art. 6 Abs. 1 Buchst f DS-GVO erfolgen, ansonsten nur mit Einwilligung der betroffenen Personen.

Seit Geltung der Datenschutz-Grundverordnung erreichen uns viele Beschwerden zum Thema E-Mail-Werbung. Ausgangslage ist ein Vertrag, bei dem die betroffene Person, z. B. in einem Online-Portal, ihre E-Mail-Adresse angibt, um Ware zu bestellen und die nachfolgende Korrespondenz mit dem Unternehmen über diesen Kommunikationsweg abwickeln zu können. In der Folgezeit verschickt das Unternehmen Werbemails an diese E-Mail-Adresse, obwohl der Kunde im Rahmen des Bestellvorgangs hierzu keine (aktive) Einwilligung erteilt hat.

Die Verwendung von E-Mail-Adressen oder Telefonnummern für die Zusendung von E-Mail- oder SMS-Werbung ist – falls bisher keine Geschäftsbeziehung mit dem Empfänger bestand ("Neukundenwerbung") – nur erlaubt, wenn hierfür eine ausdrückliche Einwilligung gegeben ist. Dies gilt sowohl für Verbraucher (B2C – business to customer) als auch für Unternehmen (B2B – business-to-business).

Ausnahmsweise ist bei bestehenden Kundenbeziehungen („Bestandskunden") E-Mail- oder SMS-Werbung zulässig, wenn die elektronischen Kontaktdaten im Zusammenhang mit der Vertragsabwicklung (Verkauf einer Ware oder Dienstleistung) erlangt worden sind, (nur) für eigene ähnliche Waren oder Dienstleistungen geworben wird, dem bisher nicht widersprochen wurde und bei der Erhebung der elektronischen Kontaktdaten – sowie aus Gründen der leichteren Nachweisbarkeit bei jeder Werbe-Mail bzw. Werbe-SMS – klar und deutlich auf das Widerspruchsrecht hingewiesen wurde bzw. wird.

Weitere Voraussetzung ist auch hier die Erfüllung der gesetzlichen Informationspflichten, d. h. bei Erhebung der E-Mail-Adresse muss der Verantwortliche die betroffene Person u. a. über die künftige Verwendung der E-Mail-Adresse zu Werbezwecken in Kenntnis setzen. Entsprechende Informationen in den Datenschutzhinweisen des Unternehmens genügen grundsätzlich den gesetzlichen Vorgaben.

Vermehrt treffen wir in letzter Zeit auf die Situation, dass das werbende Unternehmen bereits im unmittelbaren Anschluss an das Eingabefeld zur E-Mail-Adresse seiner Informationspflicht nachkommt und auf die Verwendung zu Werbezwecken sowie auf das entsprechende Widerspruchsrecht bereits an dieser Stelle hinweist. Wir sehen darin keine (vorausgefüllte) Einwilligung der betroffenen Person, sondern lediglich eine Information über eine im Zusammenhang mit dem Vertragsabschluss geplante Verwendung personenbezogener Daten für den Versand von Werbung, sofern die weiteren rechtlichen Voraussetzungen der o. g. Ausnahmevorschrift eingehalten werden.

Auch sehen wir den Anwendungsbereich für das sogenannte Koppelungsverbot nach Art. 7 Abs. 4 DS-GVO nicht eröffnet, weil der Interessent die Ware auch dann erwerben kann, wenn er der vorangekündigten E-Mail-Werbung widerspricht.

10

Handel und Dienstleistung

10 Handel und Dienstleistung

10.1 Übermittlung von E-Mail-Adressen durch Online-Versandhändler an Postdienstleister

Eine Weitergabe von E-Mail-Adressen an Postdienstleister ist im Rahmen des Onlineversandhandels nur mit Einwilligung des Kunden zulässig.

Es scheint immer noch einige Händler im Bereich des Onlineversandhandels zu geben, die die E-Mail-Adressen ihrer Kunden ohne deren Einwilligung an den Postdienstleister weitergeben, den sie mit der Auslieferung der bestellten Ware an den Kunden beauftragen. Dadurch werde es dem Paketdienst ermöglicht, den einzelnen Kunden stets über den aktuellen Stand des Versandes zu informieren, wird hier händlerseitig typischerweise argumentiert. Der Händler erachtet dies regelmäßig als „Serviceleistung" – Kundenbeschwerden werden deshalb oftmals nicht ernst genommen.

Die Datenschutzkonferenz veröffentlichte bereits am 23. März 2018 einen Beschluss, der hierzu eine Positionierung enthält:

www.datenschutzkonferenz-online.de/media/dskb/20180323_dskb_mail_adressen.pdf

Aus datenschutzrechtlicher Sicht ist die Übermittlung der E-Mail-Adresse an den Postdienstleister nur bei Vorliegen einer Einwilligung des Kunden zulässig. Unproblematisch ist es natürlich, wenn der Onlinehändler bereits selbst die Zustellinformationen bzw. einen Link in der eigenen Bestellbestätigung zur Verfügung stellt. Eine Übermittlung an den Paketdienst wird damit hinfällig.

10.2 Kontaktaufnahme durch Energieversorger ohne Vertragsverhältnis

Die Verarbeitung personenbezogene Daten zur Kontaktaufnahme durch den Energieversorger kann auch ohne ein bestehendes Vertragsverhältnis zulässig sein.

Auch im Berichtszeitraum gingen erneut in erheblicher Anzahl Beschwerden gegen Energieversorger bei uns ein.

In einigen Fällen schilderte uns der Beschwerdeführer, dass der Energieversorger ihn weiterhin kontaktiere, obwohl er das Eigentum an der Immobilie bereits aufgegeben habe und demnach nicht länger Vertragspartner sei. Daher sei die weitere Verarbeitung seiner Daten rechtswidrig.

Diese Annahme ist in der dargestellten Konstellation meistens unrichtig, weil für den Energieversorger eine gesetzliche Verpflichtung nach § 36 Energiewirtschaftsgesetz und der Grundversorgungsordnung für Strom bzw. Gas besteht, den Kunden, der den Strom- oder Erdgaszähler nutzt, zu ermitteln. Datenschutzrechtliche Ermächtigungsgrundlage für die Verarbeitung ist hier Art. 6 Abs. 1 Buchst. c DS-GVO. Die Kontaktierung des bei dem Unternehmen zuletzt bekannten Nutzers stellt daher keinen Datenschutzverstoß dar.

10.3 Verarbeitung personenbezogener Daten aufgrund von Namensverwechslungen

Personenbezogene Daten müssen vor einer weiteren Verarbeitung insbesondere hinsichtlich ihrer Richtigkeit überprüft werden. Dabei muss die betroffene Person eindeutig identifiziert werden können.

Hintergrund zahlreicher Beschwerden waren nach wie vor Namens- bzw. Personenverwechslungen. Eine von uns bearbeitete Beschwerde hatte zum Inhalt, dass ein Handelsunternehmen zwei Anfragen zu einer Person bei einer Auskunftei gestellt hat, obwohl der Beschwerdeführer nie eine Geschäftsbeziehung zu dem Unternehmen hatte.

In seiner Stellungnahme teilte uns der Verantwortliche mit, dass ein Kunde dort angefragt habe, ein Kundenkonto für seine Firma eröffnen zu wollen. Da die Firma des Kunden ein Konto noch nicht eröffnet hatte, sei die übliche Abfrage bei der Auskunftei nicht möglich gewesen. Man habe daher versucht, den Kunden als Privatperson bei der Auskunftei anzufragen. Die Abfrage habe einen Treffer zu einer namensgleichen Person ergeben, die jedoch in einem anderen Ort wohnte. Man glaubte, sich vertippt zu haben und wiederholte den Vorgang am Folgetag – wiederum mit dem gleichen Ergebnis. Eine Mitarbeiterin teilte daraufhin mit, dass sie den Kunden persönlich kenne und sie auch den Wohnort wisse. Es folgte eine weitere Abfrage gemäß den Angaben der Mitarbeiterin.

Im Ergebnis wurden hier drei Anfragen bei Auskunfteien gestellt, ohne die betroffene Person vorher eindeutig identifiziert bzw. sie zur Verifizierung ihrer Daten aufgefordert zu haben. Im Hinblick auf die Verarbeitung der Daten des Beschwerdeführers wurde gegen den Grundsatz der Rechtmäßigkeit nach Art. 5 Abs. 1 Buchst. a DS-GVO i. V. m. Art. 6 Abs. 1 DS-GVO verstoßen, da es für diese Person keine Rechtsgrundlage für die Durchführung einer Bonitätsabfrage gab. Wir haben dem Unternehmen gegenüber eine Verwarnung nach Art. 58 Abs. 2 Buchst. b DS-GVO ausgesprochen und dieses ausdrücklich darauf hingewiesen, dass künftig erst dann Abfragen durchzuführen sind, wenn die Identität hinreichend geprüft und verifiziert wurde.

11

Internationaler Datenverkehr

11 Internationaler Datenverkehr

11.1 Privacy Shield

Der seit dem 1. August 2016 geltende EU-U.S. Privacy Shield ist in Kraft und kann als Grundlage für die Übermittlung personenbezogener Daten an zertifizierte US-Unternehmen verwendet werden.

Seit 1. August 2016 kann der sog. EU-U.S. Privacy Shield als Grundlage für die Übermittlung personenbezogener Daten an solche US-Unternehmen verwendet werden, die eine Privacy-Shield-Zertifizierung besitzen. Mit der Zertifizierung verpflichtet sich das jeweilige Unternehmen zur Einhaltung grundlegender Datenschutzprinzipien; flankiert wird die Zertifizierung durch die Aufsicht des US-Handelsministeriums und der Federal Trade Commission, einer US-Bundesbehörde. Die Zertifizierung hat eine Gültigkeitsdauer von einem Jahr und kann beim US-Handelsministerium erneuert werden. Durch den sog. Privacy-Shield-Beschluss aus dem Jahr 2016 hat die Europäische Kommission anerkannt, dass das Privacy-Shield-System für die daran teilnehmenden – derzeit rund 5.000 – US-Unternehmen ein angemessenes Datenschutzniveau liefert. Es handelt sich bei diesem Beschluss um die Feststellung eines angemessenen Datenschutzniveaus im Sinne von Art. 45 DS-GVO. Damit dürfen personenbezogene Daten, die der DS-GVO unterfallen, an US-Unternehmen, die eine gültige Zertifizierung besitzen, übermittelt werden. Neben den Standarddatenschutzklauseln (ehemals „Standardvertragsklauseln") stellt der Privacy Shield das wohl wichtigste Instrument zur Legitimierung der Übermittlung personenbezogener Daten in die USA dar.

Wie in dem Angemessenheitsbeschluss der Europäischen Kommission vorgesehen, findet jedes Jahr eine sog. Gemeinsame Überprüfung („Joint Review") der praktischen Erfahrungen mit der Anwendung des Privacy Shield statt. An der Überprüfung nehmen neben der Europäischen Kommission und den Vertretern der US-Verwaltung auch Vertreter des Europäischen Datenschutzausschusses statt, mithin der Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten. Die dritte derartige Überprüfung fand im Herbst 2019 statt. Im Anschluss an die diesjährige Überprüfung zog die Europäische Kommission eine insgesamt positive Bilanz zum Funktionieren des Privacy Shield, sah aber auch noch Verbesserungsbedarf. Insbesondere hält die Kommission es für erforderlich, dass die Federal Trade Commission ihre Kontrolltätigkeit gegenüber den zertifizierten Unternehmen intensiviert.

Die Datenschutzaufsichtsbehörden ihrerseits kamen nach der diesjährigen Überprüfung zu einem differenzierteren Bild. Der Bericht des Europäischen Datenschutzausschusses (EDSA) ist abrufbar unter:

edpb.europa.eu/our-work-tools/our-documents/eu-us-privacy-shield-third-annual-joint-review-report-12112019_en

Einerseits erkannten sie an, dass es Verbesserungen bei der Kontrolle und Durchsetzung des Privacy Shield durch die zuständigen US-Behörden gegeben hat. Dennoch äußerte der EDSA noch signifikante Zweifel zu einer Reihe wichtiger Fragen. So ist nach wie vor aus Sicht des EDSA unklar, ob die so genannte Ombudsperson, die für die Bearbeitung von Beschwerden betroffener Personen im Hinblick auf etwaige Datenzugriffe durch US-Sicherheitsbehörden zuständig ist, mit einem ausreichenden Maß an Befugnissen ausgestattet ist sowie über ein Maß an Unabhängigkeit in der Ausübung dieser Befugnisse verfügt, das den Anforderungen der EU-Grundrechtecharta genügt. Auch im Hinblick auf die geltenden US-Regelungen zu den Datenzugriffsbefugnissen der US-Sicherheitsbehörden (Artikel 702 FISA sowie der sog. Executive Order 12333) sah der EDSA noch offene

Fragen, insbesondere weil weite Teile der existierenden US-Dokumente zu diesen Fragestellungen von der US-Seite im Rahmen der bisherigen Gemeinsamen Überprüfungen des Privacy Shield mit Verweis auf deren Einstufung als sicherheitsrelevant und daher geheim den Vertretern des EDSA nicht offengelegt wurden.

Hinzuweisen ist auch darauf, dass der Privacy Shield, jedenfalls mittelbar, auch Gegenstand eines derzeit vom Europäischen Gerichtshof verhandelten Vorlageverfahrens („Schrems II") ist, bei dem für die ersten Monate 2020 mit einem Urteil zu rechnen ist. Auch wenn das konkrete Verfahren nicht unmittelbar die Gültigkeit der Privacy-Shield-Entscheidung zum Gegenstand hat, ist es nicht ausgeschlossen, dass der EuGH in seinem Urteil auch relevante Aussagen zum Privacy Shield treffen könnte. Selbst eine Ungültigerklärung des Privacy Shield durch den EuGH im Rahmen des anstehenden Urteils kann nach Ansicht einiger Beobachter zumindest nicht völlig ausgeschlossen werden. Im Rahmen des vorgenannten vom EuGH verhandelten Verfahrens („Schrems II") ist der EuGH aufgrund einer Vorlage des obersten Gerichts aus Irland (Irish High Court) aufgerufen, über die Gültigkeit der EU-Standarddatenschutzklauseln für Übermittlungen an Auftragsverarbeiter (Kommissionsbeschluss 2010/87/EU vom 15.02.2010) zu entscheiden.

Für die Rechtsanwender – also Unternehmen und andere Stellen, die personenbezogene Daten in die USA übermitteln – bleibt festzuhalten, dass der Privacy Shield als Instrument nach wie vor Gültigkeit besitzt, so dass er als Grundlage für Datenübermittlungen in die USA verwendet werden kann. Die Datenschutzbehörden haben nicht die Möglichkeit, von sich aus den Privacy-Shield-Beschluss für unwirksam zu erklären.

Unternehmen – und auch die Datenschutzbehörden – müssen sich bewusst sein, dass im Rahmen des Schrems-II-Verfahrens vor dem Europäischen Gerichtshof möglicherweise auch die Gültigkeit des Privacy Shield auf dem Prüfstand steht. Sollte der EuGH die Standardvertragsklauseln und den Privacy Shield für ungültig erklären, könnten Unternehmen und andere Akteure, die personenbezogene Daten in die USA übermitteln, abgesehen von Einzelverträgen, die von der Aufsichtsbehörde zu genehmigen wäre, wohl auf keine wirksame Rechtsgrundlage mehr berufen.

12

Beschäftigtendatenschutz

12 Beschäftigtendatenschutz

12.1 Mitteilung von Überstunden an Vorgesetzte

Es ist datenschutzrechtlich nicht zu beanstanden, wenn die Personalbuchhaltung den jeweiligen Vorgesetzten und der Geschäftsführung Mitteilungen über Überstunden der betreffenden Mitarbeiter zukommen lässt.

Wir wurden angefragt, ob es zulässig sei, dass unregelmäßige oder regelmäßige Mitteilungen der Personalbuchhaltung über die Überstunden der Mitarbeiter an den jeweiligen Vorgesetzten und die Geschäftsführung erfolgen.

Der Arbeitgeber darf gemäß § 26 Abs. 1 Satz 1 BDSG mit Mitarbeiterdaten umgehen, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. Diese Voraussetzungen dürften hier erfüllt sein. Wenn Vorgesetzte und ggf. auch die Geschäftsführung von der Personalbuchhaltung die jeweiligen Überstunden der ihnen unterstehenden Mitarbeiter mitgeteilt bekommen, halten wir dies für vertretbar. Anhand der Überstunden können die Vorgesetzten erkennen, wie stark die einzelnen Mitarbeiter belastet sind und ggf. eine Umverteilung der Aufgaben vornehmen. Bei einer großen Zahl von Überstunden könnten sie auch auf deren Abbau hinwirken. Gegebenenfalls könnte auch die Einstellung neuer Mitarbeiter für bestimmte, besonders belastete Bereiche in Betracht kommen.

12.2 Fragerecht des Arbeitgebers bezüglich Gesundheit

Der Arbeitgeber darf nach gesundheitlichen Einschränkungen des Beschäftigten fragen, soweit diese für die Verrichtung der geschuldeten Arbeitsleistung relevant sind.

Wenn in einem Unternehmen Mitarbeiter schwere körperliche Tätigkeiten (heben oder tragen) verrichten, muss es dem Arbeitgeber aufgrund seiner Fürsorgepflicht möglich sein, Kenntnis von gesundheitlichen Einschränkungen dieser Mitarbeiter zu nehmen.

Die Erhebung dieser Informationen durch den Arbeitgeber ist zulässig. Einschlägige datenschutzrechtliche Rechtsgrundlage ist § 26 Abs. 3 BDSG. Danach darf der Arbeitgeber besondere Kategorien personenbezogener Daten seiner Mitarbeiter im Sinne des Art. 9 Abs. 1 DS-GVO für Zwecke des Beschäftigungsverhältnisses u. a. verarbeiten, wenn dies zur Erfüllung von Pflichten aus dem Arbeitsrecht erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person am Ausschluss der Verarbeitung überwiegt. Bei den Einschränkungen beim Heben und Tragen handelt es sich um Gesundheitsdaten, die in Art. 9 Abs. 1 DS-GVO aufgeführt sind. Aufgrund der Fürsorgepflicht gegenüber seinen Mitarbeitern hat der Arbeitgeber dafür zu sorgen, dass bei der Verteilung von Aufgaben auf die körperlichen Einschränkungen bestimmter Mitarbeiter Rücksicht genommen wird. Dazu muss er von diesen Einschränkungen Kenntnis nehmen dürfen. Da dies auch im Interesse der betreffenden Mitarbeiter geschieht, stehen keine überwiegenden schutzwürdigen Interessen letzterer der Datenverarbeitung entgegen.

12.3 Zugriff auf das E-Mail-Postfach ausgeschiedener Mitarbeiter

Wenn in einem Unternehmen die private Internet- und E-Mail-Nutzung untersagt ist, ist es für den Arbeitgeber möglich, auf das E-Mail Postfach eines ausgeschiedenen Mitarbeiters zuzugreifen.

Ein Unternehmen, in dem die private Nutzung von Internet und E-Mail untersagt ist, fragte nach, ob es auf das E-Mail-Postfach eines ausgeschiedenen Mitarbeiters zugreifen darf, da sich eingegangene E-Mails, die zu laufenden Geschäftsvorgängen gehören, in diesem E-Mail Postfach befinden würden.

Sofern, wie im konkret vorliegenden Fall, die private Nutzung von Internet und E-Mail untersagt ist, richtet sich die Zulässigkeit von Zugriffen des Arbeitgebers auf das E-Mail-Postfach des ausgeschiedenen Mitarbeiters nach § 26 Abs. 1 Satz 1 BDSDG. Danach ist der Umgang des Arbeitgebers mit Mitarbeiterdaten für Zwecke des Beschäftigungsverhältnisses zulässig, wenn er für die Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist. Die dienstlichen E-Mails stehen dem Arbeitgeber zu, so dass er darüber nach Ausscheiden des betreffenden Mitarbeiters verfügen kann. Wenn zudem E-Mails aus dem Postfach für die weitere Bearbeitung von Geschäftsvorgängen benötigt werden, muss dem Arbeitgeber der Zugriff möglich sein. Sollte er auf eine E-Mail mit privatem Inhalt stoßen, dürfte er diese allerdings nicht zur Kenntnis nehmen und müsste sie entweder an den ausgeschiedenen Mitarbeiter übermitteln oder löschen. Eine Einwilligung des ausgeschiedenen Mitarbeiters ist in einem solchen Fall nicht erforderlich.

Wir haben diesen Fall zum Anlass genommen, zu empfehlen, dass Postfächer ausgeschiedener Mitarbeiter möglichst zeitnah gelöscht werden, sodass Absender eine Fehlermeldung erhalten und sich um den neuen und richtigen E-Mail Kontakt kümmern müssen oder können.

12.4 Backgroundscreening über Bewerber

Potentielle Arbeitgeber dürfen sich nicht bei Facebook über Bewerber informieren.

Wir wurden gefragt, ob sich ein Arbeitgeber im Rahmen eines Bewerbungsverfahrens Informationen zu Bewerbern aus Facebook beschaffen darf.

Maßgeblich ist § 26 Abs. 1 Satz 1 BDSG. Danach darf der Arbeitgeber Daten von Beschäftigten - dazu zählen auch Bewerber, § 26 Abs. 8 BDSG - verarbeiten, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich ist. Diese Erforderlichkeit wird bei solchen Quellen im Internet bejaht, die einen beruflichen Bezug aufweisen, also z. B. XING oder LinkedIn, weil Mitglieder dieser Netzwerke dort bewusst Informationen über sich im beruflichen Kontext einstellen. Diese Informationen sind deshalb auch für potentielle Arbeitgeber bestimmt, die für ihre Entscheidung hinsichtlich der Eignung eine Rolle spielen können.

Bei Facebook betreffen die Inhalte mehr den persönlichen Bereich, weshalb eine Erforderlichkeit für die Entscheidung über die Begründung des Beschäftigungsverhältnisses zu verneinen ist, auch wenn der Facebook-Account öffentlich zugänglich ist.

13

Gesundheit und Soziales

13 Gesundheit und Soziales

13.1 Übermittlung von Patientendaten an Strafverfolgungsbehörden

Ärzte und Psychotherapeuten sind nicht zur Herausgabe von Patientendaten gegenüber den Strafverfolgungsbehörden verpflichtet und dürfen diese Daten auch nur in Ausnahmefällen von sich aus übermitteln.

Wir erhielten Eingaben von Ärzten, die von der Polizei oder Staatsanwaltschaft zur Herausgabe von Patientendaten aufgefordert werden. Umgekehrt haben manche Ärzte bei uns nachgefragt, ob sie von sich aus Patientendaten an diese Stellen weitergeben dürfen, beispielsweise, wenn sie den Verdacht hegen, dass der Patient eine Straftat begangen hat.

Da Ärzte und Psychotherapeuten gemäß § 53 Abs. 1 Satz 1 Nr. 3 StPO zur Zeugnisverweigerung berechtigt sind, unterliegen die von ihnen angefertigten Unterlagen mit den Patientendaten insoweit dem Beschlagnahmeverbot des § 97 Abs. 1 StPO. Die Herausgabe dieser Unterlagen an die Strafverfolgungsbehörden ist auch bei Vorliegen eines Durchsuchungsbeschlusses nur bei Entbindung von der Schweigepflicht durch den Patienten oder auf freiwilliger Basis des Arztes möglich.

Voraussetzung für die Freiwilligkeit ist, dass der Arzt bzw. Psychotherapeut von der Strafverfolgungsbehörde über das Beschlagnahmeverbot belehrt wurde. Ist dies der Fall, enthält die freiwillige Herausgabe der Daten einen konkludenten Verzicht des Berufsgeheimnisträgers auf sein Zeugnisverweigerungsrecht. Hiervon unberührt bleibt die mögliche Strafbarkeit des Arztes oder Psychotherapeuten nach § 203 StGB.

Aufgrund der in den jeweiligen Berufsordnungen festgeschriebenen Schweigepflicht ist die Offenbarung von Patientendaten durch den Arzt oder Psychotherapeuten nicht ohne weiteres möglich. Soweit keine Entbindung von der Schweigepflicht vorliegt, muss die Offenbarung von Patientendaten zum Schutz eines höherwertigen Rechtsguts erforderlich sein. Dies ist nicht immer der Fall, wenn der Berufsgeheimnisträger lediglich den Verdacht hegt, dass sich der Patient in irgendeiner Weise strafbar gemacht hat.

Dagegen ist die Offenbarung der Patientendaten zulässig, wenn der Verdacht einer der in § 138 StGB genannten, schwerwiegenden Straftaten im Raum steht, da sich anderenfalls der Berufsgeheimnisträger aufgrund einer unterbliebenen Mitteilung selbst strafbar machen könnte. Die mit der Offenbarung der Daten notwendigerweise verbundene Zweckänderung ist in diesem Fall durch § 24 Abs. 2 BDSG i.V.m. §§ 24 Abs. 1 Nr. 1, § 22 Abs. 1 Nr. 1 d BDSG gerechtfertigt.

13.2 Berichtigung von ärztlichen Diagnosen

Die Prüfung der Richtigkeit einer ärztlichen Diagnose fällt nicht in unserem Zuständigkeitsbereich. Macht ein Patient in diesem Zusammenhang sein Berichtigungsrecht geltend, obliegt ihm die Beweislast für das Vorliegen der Unrichtigkeit.

Uns erreichen Anfragen von Patienten, die die Richtigkeit der von ihrem Arzt gestellten Diagnose anzweifeln und in diesem Zusammenhang eine Berichtigung ihrer Daten nach Art. 16 DS-GVO wünschen.

Die fachliche Richtigkeit einer Diagnose ist keine Frage des Datenschutzes. Soweit noch

nicht – z. B. durch unanfechtbare Entscheidung eines Gerichts – feststeht, ob eine gestellte Diagnose tatsächlich unrichtig ist, fällt diese Prüfung folglich nicht in unsere Zuständigkeit.

Anders sieht es aus, wenn es darum geht, ob Tatsachen, die der vom Arzt erstellten Diagnose zu Grunde legen, unrichtig sind. Für die erfolgreiche Geltendmachung eines Anspruchs auf Berichtigung dieser Tatsachen reicht es allerdings nicht, dass der betroffene Patient lediglich die Richtigkeit der Diagnose bestreitet. Er muss in seinem Antrag auf Berichtigung vielmehr konkret darlegen, inwiefern die ihn betreffenden Tatsachen unrichtig sind und wie eine Berichtigung aussehen sollte. Dem verantwortlichen Arzt obliegt sodann die umfassende Prüfung der gespeicherten Daten und gegebenenfalls eine Berichtigung der Tatsachen und eine Überarbeitung der Diagnose.

Wird eine Patientenakte entsprechend berichtigt, muss neben dem ursprünglichen Inhalt erkennbar bleiben, wann die Korrektur vorgenommen wurde (§ 630f Abs. 1 Satz 2 BGB).

14

Vereine und Verbände

14 Vereine und Verbände

14.1 Mitgliederverwaltung

Rechtsgrundlage für die Verarbeitung personenbezogener Daten zum Zwecke der Mitgliederverwaltung im Verein ist Art. 6 Abs. 1 Buchst. b DS-GVO.

Viele Vereine vertreten immer noch die Auffassung oder vermuten, dass sie für die Verarbeitung personenbezogener Daten im Rahmen der Mitgliederverwaltung eine Einwilligung von der betroffenen Person einholen müssten. Eine Einwilligung wird für diesen Verarbeitungszweck jedoch grundsätzlich nicht benötigt. Denn gemäß Art. 6 Abs. 1 Buchst. b DS-GVO ist geregelt, dass die Verarbeitung personenbezogener Daten zulässig ist, wenn sie zur Erfüllung eines Vertrages erfolgt. Da das Mitgliedschaftsverhältnis ein vertragsähnliches Rechtsverhältnis ist (vgl. BGHZ 110, 323, 327), ist die Verarbeitung für Zwecke, die zur Durchführung des Mitgliedschaftsverhältnisses erforderlich sind, auf Grundlage von Art. 6 Abs. 1 Buchst. b DS-GVO zulässig. Gleiches gilt aber auch für Verarbeitungstätigkeiten, die zur Erreichung weiterer Zwecke erforderlich sind, die als solche hinreichend deutlich als Vereinszwecke in der Satzung des Vereins angelegt sind.

Es erreichten uns im Berichtszeitraum eine Reihe von Anfragen von Vereinen, anhand derer wir erkannten, dass die Bedeutung der datenschutzrechtlichen Informationspflichten in diesem Zusammenhang oftmals noch missverstanden wird. Die datenschutzrechtlichen Informationen nach Art. 13 und Art. 14 DS-GVO sind nicht zu verwechseln mit der Einwilligung nach Art. 7 DS-GVO. Art. 13 DS-GVO stellt keine Rechtsgrundlage für die Datenverarbeitung dar, sondern soll sicherstellen, dass der Verantwortliche die betroffene Person über die Verarbeitung transparent und in einer nachvollziehbaren Weise informiert.

Einige Vereine lassen sich den Erhalt der Informationen nach Art. 13 DS-GVO durch Unterschrift bestätigen – werten dies dann aber als Einwilligung nach Art. 7 DS-GVO. So wird uns oft die Frage gestellt, ob eine Mitgliedschaft noch möglich sei, wenn das potenzielle Mitglied generell keine „Einwilligung" in die Verarbeitung seiner personenbezogenen Daten erteilt.

Wie bereits ausgeführt, steht mit Art. 6 Abs. 1 Buchst. b DS-GVO bereits eine einschlägige Rechtsgrundlage zur Verfügung. Dass die betroffene Person ihre Einwilligung verweigert, führt deshalb nicht zur Unzulässigkeit der Verarbeitung personenbezogener Daten im Rahmen der Mitgliederverwaltung bzw. zum Ausschluss aus dem Verein. Vereine sollten davon Abstand nehmen, für Zwecke der Mitgliederverwaltung und für andere von der Vereinssatzung hinreichend klar abgedeckte Verarbeitungszwecke Einwilligungen der Mitglieder einzuholen.

Auch ein „Bestätigenlassen" des Erhalts der nach Art. 13 DS-GVO zu erteilenden Informationen durch Unterschrift ist nicht erforderlich. Jedoch muss der Verein in der Lage sein, im Rahmen der Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO) nachzuweisen, dass er den Mitgliedern ordnungsgemäß die nach Art. 13 DS-GVO zu erteilenden Informationen zur Verfügung gestellt hat. Dieser Nachweis kann unkompliziert z. B. dadurch erbracht werden, dass die Informationen auf dem (vom Neumitglied ausgefüllten) Formular enthalten sind, mit dem die Mitgliedschaft im Verein beantragt wird.

14.2 Öffentlicher Aushang der Klageschrift eines Mitglieds in einem Verfahren gegen den Verein

Es ist nicht zulässig, eine von einem Vereinsmitglied verfasste Klageschrift, die allein vom Vereinsvorstand zu bearbeiten ist, allen Mitgliedern des Vereins im Wortlaut bekanntzugeben.

Ein Mitglied eines Schrebergartenvereins beschwerte sich bei uns darüber, dass der Vereinsvorstand eine von ihm verfasste und an das Registergericht gerichtete Klageschrift, die dem Vereinsvorstand vom Gericht mit dem Ersuchen um Stellungnahme zugeleitet worden war, auf dem Vereinsgelände in einem Schaukasten – nebst einigen augenscheinlich vom Vorstand stammenden handschriftlichen Anmerkungen – ausgehängt hatte. Das klagende Mitglied fühlte sich dadurch an den Pranger gestellt. In der Klageschrift hatte der Beschwerdeführer beantragt, einen bestimmten Beschluss der Mitgliederversammlung des Vereins gerichtlich für nichtig zu erklären.

Das Aushängen der Klageschrift war nach unserer Auffassung datenschutzrechtlich nicht zulässig. Auch wenn es für den Verein zulässig wäre, die Mitglieder darüber zu informieren, dass ein bestimmter Beschluss gerichtlich durch ein Mitglied angefochten worden ist, so ist es jedenfalls nicht erforderlich, die entsprechende Klageschrift des klagenden Mitglieds in vollem Wortlaut allen anderen Mitgliedern bekannt zu geben. Es war Aufgabe des Vorstands, die vom Gericht angeforderte Stellungnahme zu verfassen und dem Gericht zu übermitteln; dass hierfür eine wie auch immer geartete Information (potentiell) aller Vereinsmitglieder über den Inhalt der Klageschrift erforderlich gewesen wäre, war nicht erkennbar.

Wir haben daher dafür gesorgt, dass das Schreiben aus dem Schaukasten entfernt wurde.

15

Wohnungswirtschaft und Mieterdatenschutz

15 Wohnungswirtschaft und Mieterdatenschutz

15.1 Angebot eines Mess- und Abrechnungsdienstleisters an Beiräte einer Wohnungseigentümergemeinschaft

Die Verarbeitung personenbezogener Daten von Verwaltungsbeiräten durch einen Mess- und Abrechnungsdienstleister für Werbezwecke ist datenschutzrechtlich unzulässig.

Wir erhielten eine Beschwerde, in der moniert wurde, dass ein Dienstleistungsunternehmen, das mit dem Mess- und Abrechnungsdienst in einer Eigentümergemeinschaft betraut war, mehrere Verwaltungsbeiräte der Eigentümergemeinschaft kontaktiert habe, um der Eigentümergemeinschaft ein Angebot zu unterbreiten. Das Unternehmen erläuterte den Beiräten in diesem Schreiben, dass es vermute, dass der von der Eigentümergemeinschaft bestellte Verwalter künftig einen anderen (gesellschaftsrechtlich mit dem Verwalter verbundenen) Abrechnungsdienstleister mit dem Mess- und Abrechnungsdienst betrauen werde; vor diesem Hintergrund wolle das Unternehmen der Eigentümergemeinschaft ein neues Angebot für die künftige Zusammenarbeit unterbreiten und habe sich daher entschlossen, dieses Angebot direkt den einzelnen Verwaltungsbeiräten zu unterbreiten.

Das von uns zur Stellungnahme aufgeforderte Unternehmen teilte uns mit, dass es nur deshalb mit den Beiräten kommuniziert habe, um den Umfang der Datenverarbeitung möglichst gering zu halten und nicht sämtliche Eigentümer anschreiben zu müssen. Es wurde in diesem Zusammenhang die Meinung geäußert, dass sich die Datenverarbeitung auf die Durchführung und Abwicklung des zu Grunde liegenden Vertragsverhältnisses beschränkt habe.

Nach unserer Auffassung war dieses Unternehmen im Rahmen seiner Tätigkeit als Mess- und Abrechnungsdienstleister datenschutzrechtlich als Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DS-GVO für den Verwalter der Eigentümergemeinschaft und nicht als Verantwortlicher nach Art. 4 Nr. 7 DS-GVO tätig. Die Kontaktdaten der Verwaltungsbeiräte und anderen Eigentümer waren dem Dienstleister durch den Verwalter im Rahmen der Beauftragung mit der Ablesung und Abrechnung der Gas- und Warmwasser-Verbrauchsdaten zur Verfügung gestellt worden.

Als datenschutzrechtlich Verantwortlichen sehen wir in solchen Fällen grundsätzlich den von der Eigentümergemeinschaft bestellten Verwalter an, da dieser gemäß § 28 Abs. 3 WEG die Aufgabe hat, eine Abrechnung zu erstellen. Der Verwalter hatte sich zur Erfüllung dieser originären Verwalteraufgabe des Abrechnungsdienstleisters bedient. Als Auftragsverarbeiter war der Dienstleister nicht berechtigt, personenbezogene Daten der einzelnen Wohnungseigentümer, die ihm vom Verwalter zur Durchführung der Ablesung und Abrechnung überlassen worden waren, für eigene (Werbe-)Zwecke zu verarbeiten. Die dem Abrechnungsdienstleister vom Verwalter im Rahmen des Vertrags zur Auftragsverarbeitung nach Art. 28 Abs. 3 DS-GVO überlassenen Adressdaten der Wohnungseigentümer wurden dem Dienstleister nicht zum Zweck der Werbung zur Verfügung gestellt, sondern lediglich, damit dieser im Auftrag des Verwalters die Ablesung durchführt und die abgelesenen Daten dem Verwalter dann zur Durchführung der Abrechnung nach § 28 Abs. 3 WEG in aufbereiteter Form zur Verfügung stellt. Auch der Umstand, dass zivilrechtlich ein Vertragsverhältnis zwischen dem Abrechnungsdienstleister und der Eigentümergemeinschaft besteht, ermächtigt den Dienstleister nicht dazu, einzelne Eigentümer oder Verwaltungs-

beiräte für eigene Werbezwecke zu kontaktieren, denn insoweit muss zwischen der Eigentümergemeinschaft als solcher und den einzelnen Eigentümern – zu denen der Dienstleister gerade kein Vertragsverhältnis hat – unterschieden werden.

Mithin hat der Dienstleister Daten, die ihm als Auftragsverarbeiter anvertraut waren, entgegen den Weisungen des Verantwortlichen – des Verwalters – verarbeitet, wodurch er insoweit selbst zum Verantwortlichen wurde (Art. 28 Abs. 10 DS-GVO). Eine Rechtsgrundlage für die Verarbeitung der (Kontakt-)Daten der Verwaltungsbeiräte stand ihm aus den vorgenannten Gründen nicht zur Verfügung, so dass die Verarbeitung nach Art. 5 Abs. 1 Buchst. a DS-GVO den Grundsatz der Rechtmäßigkeit verletzte.

15.2 Veröffentlichung von Unterlagen eines Rechtsstreits auf dem Internetportal der Wohnungseigentümer

Die Bereitstellung von Unterlagen hinsichtlich eines Rechtsstreits innerhalb der Wohnungseigentümergemeinschaft stellt für den Verwalter eine gesetzliche Verpflichtung nach § 27 Abs. 1 Nr. 7 WEG dar.

Eine Wohnungseigentümerin beschwerte sich bei uns darüber, dass der Verwalter auf einem für die Kommunikation mit den Wohnungseigentümern verwendeten webbasierten Portal Unterlagen zu einem Rechtsstreit veröffentlicht habe, den die Beschwerdeführerin gegen die Eigentümergemeinschaft führte. Sie hielt es nicht für zulässig, dass auf diese Weise die Informationen über den Rechtsstreit allen Eigentümern in der Eigentümergemeinschaft zur Kenntnis gegeben wurden. Sie forderte deshalb vom Verwalter die Entfernung bzw. Löschung dieser Unterlagen vom Portal.

Diese Eingabe verdeutlicht exemplarisch unsere Beobachtung, dass bei manchen Wohnungseigentümern offenbar Fehlvorstellungen über die notwendigen Informationsflüsse innerhalb einer Eigentümergemeinschaft bestehen.

Aus datenschutzrechtlicher Sicht bestehen hinsichtlich der Bereitstellung der Informationen, die im Zusammenhang mit dem Rechtsstreit stehen, keine Bedenken. Denn der Verwalter hatte nach § 27 Abs. 1 Nr. 7 WEG im vorliegenden Fall sogar die rechtliche Verpflichtung, die Wohnungseigentümer unverzüglich darüber zu unterrichten, dass ein Rechtsstreit im Sinne von § 43 WEG zwischen der Eigentümergemeinschaft und einem einzelnen Eigentümer anhängig ist. Die Verarbeitung der Daten der Beschwerdeführerin – d. h. die Bereitstellung der Informationen betreffend den Rechtsstreit – erfolgte deshalb zur Erfüllung dieser rechtlichen Verpflichtung und war damit nach Art. 6 Abs. 1 Buchst. c DS-GVO zulässig.

Ein Anspruch auf Löschung von dem (nur) für Wohnungseigentümer zugänglichen Portal bestand damit nicht.

15.3 Bekanntgabe einer Wohnungsdurchsuchung an Verwaltungsbeiräte

Die ausschließlich telefonische Weitergabe einer Information durch einen Verwalter einer Eigentümergemeinschaft an die Verwaltungsbeiräte unterfällt nicht dem Datenschutzrecht, sofern der Verwalter die in Rede stehende Information nicht automatisiert oder in einem Dateisystem verarbeitet.

Wir erhielten im Berichtszeitraum verhältnismäßig viele Beschwerden, die die Bekanntgabe bestimmter Informationen durch Verwalter von Eigentümergemeinschaften an Verwaltungsbeiräte betrafen. Aus diesen Beschwerden wird erkennbar, dass manche Wohnungseigentümer

sich nicht im Klaren darüber sind, welche Stellung ein Verwaltungsbeirat in der Eigentümergemeinschaft hat.

In einem Fall beschwerte sich ein Eigentümer darüber, dass der Verwalter „mehrere andere Eigentümer" darüber informiert habe, dass die Polizei eine Hausdurchsuchung in seiner Wohnung durchgeführt habe. Als wir den Verwalter zur Stellungnahme aufforderten, stellte sich heraus, dass die Polizei im Rahmen einer Wohnungsdurchsuchung die Tür zu der Wohnung des Beschwerdeführers aufbrechen musste, da ein anderer Zugang nicht möglich war. Die Polizei hatte den Verwalter kontaktiert und versucht zu eruieren, ob eine Möglichkeit bestehe, die Wohnung zu betreten, ohne die Tür aufbrechen zu müssen, was jedoch nicht möglich war, da der Verwalter keinen Schlüssel zu der Wohnung hatte. Da es sich bei der Wohnungstür um Gemeinschaftseigentum handelte, hatte der Verwalter es für angemessen angesehen, die zwei für die Eigentümergemeinschaft bestellten Verwaltungsbeiräte darüber zu informieren, dass die Polizei die Wohnungstür aufbrechen werde und somit die im Gemeinschaftseigentum stehende Tür beschädigt werden würde.

Wir haben dieses Vorgehen im vorliegenden Fall als zulässig bewertet, da der Verwaltungsbeirat gemäß § 29 Abs. 2 WEG die Aufgabe hat, den Verwalter bei der Durchführung seiner Aufgaben zu unterstützen. Vor diesem Hintergrund wäre es zumindest nicht zu beanstanden, wenn der Verwalter es aufgrund des durch den Polizeieinsatz verursachten Schaden am Gemeinschaftseigentum angezeigt erachtet hat, die Verwaltungsbeiräte über den Vorgang zu informieren.

Unabhängig davon war schon mehr als fraglich, ob die Mitteilung der entsprechenden Information durch den Verwalter an die Beiräte, dass eine Wohnungsdurchsuchung durch die Polizei in der Wohnung des Beschwerdeführers stattfinden werde. überhaupt eine der DS-GVO unterfallende Verarbeitung darstellt. Der Verwalter war nämlich durch die Polizei telefonisch über den bevorstehenden Einsatz informiert worden und hat diese Information lediglich ebenfalls telefonisch an die Beiräte weitergegeben, ohne sie jedoch in irgendeiner Weise automatisiert oder aber in einem Dateisystem zu verarbeiten. Mangels einer automatisierten Verarbeitung oder einer Verarbeitung personenbezogener Daten in einem „Dateisystem" im Sinne von Art. 4 Nr. 16 DS-GVO unterfiel die Weitergabe dieser Information durch den Verwalter an die Beiräte gemäß Art. 2 Abs. 1 DS-GVO nicht dem Anwendungsbereich des Datenschutzrechts.

Der Fall verdeutlicht exemplarisch, dass nicht jede Weitergabe personenbezogener Daten dem Anwendungsbereich des Datenschutzrechts unterfällt.

16

Videoüberwachung

16 Videoüberwachung

16.1 Zweckbindung für Verwendung von Videoaufnahmen

Bei der Verwendung von Videoaufzeichnungen für einen anderen Zweck als den ursprünglichen geplanten muss dem Grundsatz der Zweckbindung besondere Aufmerksamkeit zugemessen werden.

Ein Mitarbeiter eines Reinigungsunternehmens beschwerte sich darüber, dass er bei einem Reinigungseinsatz in einem Schwimmbad von den dort installierten Videokameras erfasst wurde und diese Aufnahmen seinem Arbeitgeber vorgelegt wurden.

Das Reinigungsunternehmen reinigte unter Einsatz mehrerer Mitarbeiter regelmäßig in den frühen Morgenstunden die Schwimmhalle eines Schwimmbadbetreibers. Ein Mitarbeiter des Reinigungsunternehmens beschwerte sich bei uns darüber, dass ihn sein Arbeitgeber eines Tages zu sich gerufen und ihm Videoaufzeichnungen aus der Schwimmhalle vorlegte, in denen er sowie eine weitere Mitarbeiterin bei der Durchführung der Reinigungsarbeiten zu sehen waren. Der Arbeitgeber erklärte, diese Aufnahmen vom Schwimmbadbetreiber mit dem Hinweis vorgelegt erhalten zu haben, dass auf den Aufnahmen zum einen zu sehen sei, dass das Reinigungsunternehmen nur zwei statt der versprochenen drei Mitarbeiter zum Reinigen einsetze. Zum anderen bemängelte der Schwimmbadbetreiber anhand der Aufnahmen gegenüber dem Reinigungsunternehmen, dass die Mitarbeiter die Reinigungsarbeiten „nicht ordentlich" bzw. in ungenügender Qualität durchführten.

Das Reinigungsunternehmen als Arbeitgeber der eingesetzten Mitarbeiter schloss sich diesen Vorwürfen zwar nicht an und machte den eingesetzten Mitarbeitern aus diesem Anlass keine Vorhaltungen. Dennoch fühlte sich der Beschwerdeführer dadurch, dass der Schwimmbadbetreiber die Aufnahmen seinem Arbeitgeber – der Reinigungsfirma – vorgelegt und anhand dieser Aufnahmen seine Arbeitsleistung bemängelt habe, in seinen Rechten verletzt. Er monierte insbesondere, dass er nicht erwartet hatte, dass er beim Ausführen der Reinigung gefilmt würde und die entsprechenden Aufnahmen seinem Arbeitgeber vorgelegt würden.

Aufgrund dieser Beschwerde forderten wir den Schwimmbadbetreiber auf, zu erklären, für welche Zwecke die in der Schwimmhalle betriebene Videoüberwachung durchgeführt wird, sowie in welcher Weise er die betroffenen Personen über diese Zwecke informierte. Der Betreiber erklärte, die Videoanlage sei nur während der Nacht in Betrieb und diene der Prävention gegen unbefugtes Betreten der Schwimmhalle – etwa durch Einbrecher – sowie dazu, in solchen Fällen Täter zu identifizieren, um gegen sie etwaige (Schadensersatz-)Ansprüche verfolgen und Strafverfolgungsmaßnahmen einleiten zu können. Entsprechend wurde mittels „Hinweisschildes" über die Videoüberwachung informiert. Da die Reinigungskräfte ihre Arbeiten noch zu einem Zeitpunkt verrichteten, in dem die Anlage scharf geschaltet war, waren sie von den Kameras erfasst worden.

Nach unserer Bewertung hatte der Schwimmbadbetreiber dadurch, dass er die Aufnahmen dem Reinigungsunternehmen vorgelegt hat, gegen den datenschutzrechtlichen Grundsatz der Zweckbindung gemäß Art. 5 Abs. 1 Buchst. b DS-GVO verstoßen. Der ursprüngliche Zweck, dem die Anfertigung von Videoaufnahmen diente, lag in der Prävention und Verfolgung von Einbrüchen sowie der Verfolgung damit zusammenhängender zivilrechtlicher Ansprüche gegen die Täter. Im vorliegenden Fall wurden die Aufnahmen durch den Betreiber indes zu einem ganz anderen Zweck verwendet, nament-

lich dazu, die Leistung des Reinigungsunternehmens – und der von diesem eingesetzten Mitarbeiter – anhand der Aufnahmen zu bemängeln. Dieser Verwendungszweck ist vom o. g. ursprünglichen Zweck der Videoüberwachung – also dem Zweck, zu dem die Daten erhoben wurden – gänzlich verschieden und somit muss bei Zugrundelegung der in Art. 6 Abs. 4 DS-GVO geregelten Kriterien als mit dem ursprünglichen Zweck unvereinbar angesehen werden.

Die Verarbeitung personenbezogener Daten zu einem Zweck, der mit dem Erhebungszweck unvereinbar ist, ist gemäß Art. 6 Abs. 4 DS-GVO nur zulässig, wenn diese Verarbeitung aufgrund einer Rechtsvorschrift des EU-Rechts oder des mitgliedstaatlichen Rechts (zu einem der in Art. 23 DS-GVO aufgezählten Zwecke) ausdrücklich erlaubt ist oder wenn die betroffene Person hierzu eingewilligt hat. Mangels einer Einwilligung der gefilmten Mitarbeiter konnte die Verarbeitung daher nur zulässig sein, wenn eine Rechtsvorschrift eine derartige Zweckänderung erlaubte. Zu prüfen ist hierbei vor allem § 24 BDSG – die Vorschrift, die die Verarbeitung zu einem unvereinbaren neuen Verarbeitungszweck regelt.

Die Voraussetzungen des § 24 BDSG waren im vorliegenden Fall jedoch nach unsere Bewertung nicht erfüllt. Zwar erlaubt § 24 Abs.1 Nr. 2 BDSG die Verarbeitung für einen neuen, unvereinbaren Zweck, soweit sie zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist, aber nur, sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen. Vorliegend könnte man zwar argumentieren, dass der Schwimmbadbetreiber durch die Vorlage der Aufnahmen an die Reinigungsfirma letzterer nachweisen wollte, dass diese die Reinigungsarbeiten in einer ungenügenden Qualität erbrachte. Dies kann als „Ausübung zivilrechtlicher Ansprüche" angesehen werden, so dass der Anwendungsbereich des § 24 Abs. 1 Nr. 2 BDSG zwar grundsätzlich eröffnet ist. Jedoch überwogen bei der nach dieser Vorschrift durchzuführenden Interessenabwägung die Interessen der gefilmten Mitarbeiter des Reinigungsunternehmens am Unterbleiben einer solchen Datenverarbeitung. Denn letztlich war die komplette Reinigungstätigkeit der betroffenen Mitarbeiter per Video aufgezeichnet worden, was letztlich einer weitgehenden Komplettüberwachung ihrer Arbeitsleistung – jedenfalls im Rahmen des Arbeitseinsatzes in diesem Schwimmbad – gleichkommt. Jedenfalls eine solche Komplettüberwachung des Verhaltens und der Leistung von Beschäftigten ist, auch nach den in der arbeitsgerichtlichen Rechtsprechung entwickelten Maßstäben, unzulässig.

Diese Wertung muss auch bei der Anwendung des § 24 Abs. 1 Nr. 2 BDSG und der dort durchzuführenden Interessenabwägung durchschlagen. Damit war die Vorlage der Aufnahmen durch den Schwimmbadbetreiber an die Reinigungsfirma unzulässig. Wir haben aus diesem Anlass gegenüber dem Schwimmbadbetreiber mit einer Verwarnung reagiert, die dieser akzeptiert hat.

16.2 Kamerafahrten durch Apple

Apple veranlasst Videoaufnahmen von Straßen und Häusern zur Verbesserung der eigenen Kartendienste.

Uns erreichten zahlreiche Anfragen und Beschwerden von Bürgern, die von Fahrzeugen mit speziellen Kameras berichteten. Dahinter steckte ein Projekt von Apple mit dem Ziel, eigene Dienste wie Apple Maps zu verbessern.

Bereits im Frühjahr 2019 informierte uns Apple darüber, dass eine aus ungefähr 80 Fahrzeugen bestehende Fahrzeugflotte im Zeitraum von Juli bis September 2019 in deutschen Städten und Gemeinden unterwegs sein wird. Apple stellte uns ein umfangreiches Konzept vor und erklärte, dass in den Fahrzeugen neben Kameras und Sensoren auch Computer verbaut wurden. Die Aufnahmen würden mittels starker Verschlüsselung nach Stand der Technik bereits im

Fahrzeug verschlüsselt und danach auf Festplatten gespeichert. Die verschlüsselten Daten wurden erst bei Apple in den USA wieder entschlüsselt und weiterverarbeitet. Bevor die Daten durch Apple weiterverarbeitet würden, würden Gesichter und KFZ-Kennzeichen verpixelt. So sind laut dem Konzept in fast allen Fällen keine Personen direkt zu erkennen und damit nicht unmittelbar zu identifizieren.

Ungeachtet dessen haben betroffene Personen jederzeit – auch nachdem die Aufnahmefahrten beendet wurden – die Möglichkeit der Verarbeitung ihrer Hausansicht zu widersprechen. Ein Widerspruch ist möglich auf der Apple-Website maps.apple.com/imagecollection oder per E-Mail an MapsImageCollection@apple.com.

maps.apple.com/imagecollection

Übrigens plant Apple derzeit nicht das sogenannte „Look-Around"-Feature in Deutschland anzubieten. Dieses Feature ermöglicht es, über das Internet eine 3D-Darstellung der Aufnahmen anzusehen, wie es beispielsweise bei Google Street View möglich ist.

www.lda.bayern.de/media/pm/pm2019_9.pdf

17

Datenschutzverletzungen

17 Datenschutzverletzungen

17.1 Allgemeines zu den gemeldeten Vorfällen

Mit der DS-GVO stieg die Anzahl der Meldungen nach Art. 33 DS-GVO rapide an und blieb bis zum Ende des Berichtsjahres auf einem hohen Niveau bestehen.

Unmittelbar nach dem Beginn der Anwendbarkeit der DS-GVO im Mai 2018 konnten wir einen starken Anstieg von Meldungen über Datenschutzverletzungen von Verantwortlichen registrieren. Bereits im letzten Tätigkeitsbericht wagten wir deshalb die Prognose, dass der eingeleitete Trend auch in den darauffolgenden Jahren Bestand haben werde. Zurückblickend auf das Berichtsjahr 2019 stellen wir fest, dass diese Einschätzung zutreffend war. Wir haben uns mittlerweile an den Umstand gewöhnt, sodass die Bearbeitung von Datenschutzverletzungen einen großen Anteil unserer täglichen Arbeit einnimmt und wir an vielen Tagen über 20 Meldungen erhalten.

Wir versuchen deshalb nach wie vor, die bei uns gemeldeten Vorfälle bestimmten Kategorien zuzuordnen, damit einerseits eine zielgerichtete Bearbeitung durch einen für den Fachbereich spezialisierten Mitarbeiter gefördert wird und anderseits auch von uns bewusst wahrgenommen werden kann, wo Schwerpunkte bezüglich unserer Präventionsarbeit gesetzt werden sollten. Cyberangriffe, Verschlüsselungstrojaner, Malware, Verlust, Diebstahl, Software- und Buchungsfehler sowie Fehlversendungen sind dabei die mit Abstand häufigsten Kategorien. Weit über die Hälfte der uns gemeldeten Datenschutzverletzungen betreffen Sachverhalte, die ein eher „normales" Risiko für die betroffenen Personen besitzen und für die oftmals auch durch uns keine weiteren Abhilfemaßnahmen mehr vorgeschlagen werden müssen. Sicherheitsvorkommnisse mit einem hohen Risiko für die betroffenen Personen bleiben – aus der Sicht aller Beteiligten zum Glück – die Ausnahme, wenngleich auch hier ein Anstieg im Jahr 2019 festzustellen ist. Hintergrund dazu ist, dass gerade bei Angriffen über das Internet eine gezielte Schadensabsicht besteht, während bei vielen anderen Datenpannenkategorien mit den Daten der betroffenen Personen im Idealfall meist „nichts" passiert. Spitzenreiter bezüglich der reinen Anzahl der Meldungen bleibt unverändert die Kategorie Fehlversendung.

Eine Erkenntnis, die 2019 gewonnen wurde, ist die Tatsache, dass Cyberattacken mittlerweile einen erheblichen, zum Teil auch existenzbedrohenden Schaden für die Opfer darstellen. Opfer sind in den uns gemeldeten Fällen sowohl die gehackten Unternehmen als auch die betroffenen Personen, deren Daten für verschiedene kriminelle Zwecke verwendet werden. Oft haben die Hacker die Absicht, gezielt an persönliche Daten heranzukommen, z. B. Daten von Patienten, Mitgliedern, Beschäftigten und Kunden, da der Wert dieser Daten mittlerweile auch dort wahrgenommen wird. Die Erpressung von Verantwortlichen mit einer Lösegeldforderung, sei es durch die vollständige Verschlüsselung mittels Ransomware oder durch eine entwendete Kopie von Kundendaten, ist bereits ein alltägliches Szenario. Im Berichtszeitraum mussten wir dabei sogar Fälle feststellen, bei denen der ganze Betrieb stillstand und manche Mitarbeiter zum Teil einige Zeit zu Hause bleiben mussten. Keine Seltenheit war es, dass gerade kleine Betriebe, KMUs und Arztpraxen Opfer solcher Angriffe wurden.

Wir haben uns auf Grund dieser Entwicklung entschieden, unseren gesetzten Schwerpunkt „Cybersicherheit" weiter zu verfolgen und – soweit es die Personalkapazitäten erlauben – auch auszubauen. Das vergangene Jahr hat uns bestätigt, dass es einen erheblichen Bedarf an Unterstützung im nicht-öffentlichen Bereich gibt. Viele Vorfälle hätte man durch Basis-Schutzmaßnahmen wie das regelmäßige Einspielen

von Sicherheitsupdates und das richtige Durchführen von Datensicherungen ohne großen Aufwand vermeiden können. Unser Ziel wird daher bleiben, Verantwortliche mit Präventionstipps zu unterstützen, um die Angriffsfläche nachhaltig zu reduzieren und ein angemessenes Schutzniveau zu erreichen. Dies dient letztendlich allen Beteiligten – den Verantwortlichen, den betroffenen Personen und auch der zuständigen Datenschutzaufsichtsbehörde.

17.2 Arbeitskreis der DSK zu Datenschutzverletzungen

Die Datenschutzkonferenz hat einen Arbeitskreis gegründet, bei dem ein einheitliches Verständnis für die Meldepflicht nach Art. 33 DS-GVO erarbeitet werden soll.

Bei der Auswertung eines europaweit tätigen Versicherungsunternehmens wurde erkennbar, dass die Auffassungen der Datenschutzaufsichtsbehörden in Europa, aber auch in Deutschland zu der Frage, welche Datenschutzverletzungen nach Art. 33 DS-GVO der Aufsichtsbehörde zu melden sind, sehr unterschiedlich sind. Ursache dafür mag sein, dass das Verständnis darüber, wann bei einer Datenschutzverletzung kein Risiko für die Rechte und Freiheiten einer betroffenen Person vorliegt, weit auseinander geht.

Ziel dieser Arbeitsgruppe, die von uns geleitet wird, ist es, zunächst innerhalb der deutschen Aufsichtsbehörden möglichst klare Kriterien dafür zu ermitteln, wann eine Meldepflicht besteht. Ein weiterer Schritt wird dann sein, mit dieser Auffassung nach Europa zu gehen und zu erreichen suchen, dass auch auf dieser Ebene ein gemeinsames Verständnis entsteht.

18

Technischer Datenschutz und Informationssicherheit

18 Technischer Datenschutz und Informationssicherheit

18.1 Gesundheitsdaten im Web

Eine Berichterstattung über tausende medizinische Bilddaten im Internet führte auch nach Bayern.

Im September 2019 veröffentlichte der Bayerische Rundfunk einen Artikel, der sich mit über das Internet aufrufbaren medizinischen Daten beschäftigte. Es seien weltweit Millionen radiologische Bilddaten von sogenannten PACS-Servern abrufbar, von denen einige Systeme auch in Deutschland stehen würden.

Wir haben daraufhin Anhaltspunkte hinsichtlich eines Betreibers eines solchen Systems in unserer Zuständigkeit wahrgenommen. Im Rahmen unserer aufsichtlichen Tätigkeit und Prüfroutinen haben wir medizinische Bilddaten ohne Passwortschutz vorgefunden. Es stellte sich heraus, dass dieses System ein falsch konfigurierter Rechner eines Arztes in Bayern war, der diesen – nachdem wir ihn kontaktiert hatten – unmittelbar vom Internet trennte. Im Rahmen einer anschließenden forensischen Untersuchung des Vorfalls haben wir auch den betroffenen Rechner vom verantwortlichen Arzt persönlich erhalten und analysiert. Es wurden dabei keine Anhaltspunkte gefunden, die Rückschlüsse ermöglichten, dass kriminelle Personen auf den Rechner bzw. die medizinische Daten zugegriffen hatten.

Da der betroffene Arzt bei uns eine Meldung nach Art. 33 DS-GVO durchgeführt hatte, wurde auf Grund der Einschränkungen durch die Bußgeldvorschriften des neuen BDSG kein Ordnungswidrigkeitsverfahren eingeleitet (§ 43 Abs. 4 BDSG).

Die betroffenen Patienten mussten zudem nicht gemäß Art. 34 DS-GVO informiert werden, da nicht von einem hohen Risiko hinsichtlich deren Rechte und Freiheiten ausgegangen werden konnte. Hintergrund hierbei war, dass es letztendlich im Ergebnis der Untersuchungen keine nachhaltigen Anhaltspunkte für einen Zugriff auf die Daten mit dem Ziel einer missbräuchlichen Verwendung gab.

Bei vergleichbaren Fällen wäre dies dann anders zu bewerten, wenn die Daten im Internet frei zugänglich auftauchen oder in krimineller Absicht (z. B. Erpressung) verwendet werden – dann wäre eine Meldung nach Art. 34 DS-GVO an alle betroffenen Patienten erforderlich.

18.2 Anforderungen an starke Passwörter

Passwörter können auch heute noch ein wirksamer Schutzmechanismus sein, wenn die Nutzer achtsam und die Passwörter stark sind.

Gleich zu Beginn des Jahres 2019 standen Personen des öffentlichen Lebens im Mittelpunkt einer Cybersicherheitsbetrachtung, nachdem eine unbefugte Person umfangreiche persönliche Informationen über diese im Internet veröffentlicht hatte („Doxing-Skandal"). Diesen Vorfall nahmen wir zum Anlass, um im Rahmen des jährlichen Safer Internet Days eine Prüfung von Online-Dienstanbietern durchzuführen, wie diese ihre Nutzer bei der Handhabung mit Zugangsdaten unterstützen sowie wie robust deren Systeme gegen Cyberkriminelle ausgestattet sind (siehe Kapitel 3.1 dieses Berichts). Informationen zu dieser Prüfung finden sich unter:

www.lda.bayern.de/media/sid_ergebnis_2019.pdf

In diesem Zusammenhang haben wir uns darauf verständigt, dass wir gegenüber Anbietern von Online-Diensten gezielt von starken Passwörtern für die Nutzer sprechen. Pauschale Aussagen zu bestimmten Längen und Komplexitäten von Passwärtern (z. B. acht Stellen mit Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen)

sehen wir nicht mehr als zielführend an, da gemäß dem risikoorientierten Ansatz der DS-GVO konkrete Umstände (z. B. Online-Angriffe möglich oder nicht), die Arten der Speicherung (wie bcrypt-Hashverfahren samt Salt zur Umwandlung eines Klartextpassworts vor dessen Speicherung) und auch der Einsatz von Mehrfaktorauthentifizierungsverfahren zwangsläufig zu berücksichtigen sind.

Als Empfehlung können wir trotzdem folgende Best-Practice-Aussagen treffen, die gerade für Anbieter von Online-Diensten allerdings nicht neu sein sollten:

- Mindestlänge von zehn Zeichen bei hoher Zeichenkomplexität (Groß-/Kleinbuchstaben, Ziffern, Sonderzeichen)
- Falls geringe Passwortkomplexität: Erhöhung der Mindestlänge (z. B. 20 Zeichen)
- Speicherung mit geeigneten gesalzenen Hashverfahren wie z. B. bcrypt anstatt SHA- oder MD5-Verfahren
- Zwei-Faktor-Authentifizierung (z. B. mittels App), insbesondere bei hohem Risiko der Verarbeitung

Durchaus empfehlenswert ist in diesem Zusammenhang auch der Passwort-Check des Bayerischen Staatsministeriums für Digitales, der innerhalb des eigenen Browsers ein eingegebenes Passwort auf dessen Stärke bewertet.

www.stmd.bayern.de/service/passwort-check

18.3 Beschwerden zum Tesla Sentry Mode

Der Tesla-Diebstahlschutz in öffentlich zugänglichen Raum ist Thema von Datenschutzbeschwerden und wird deshalb aufsichtlich von uns geprüft.

Wir haben im Jahr 2019 vermehrt Beschwerden wegen Tesla-Fahrzeugen erhalten, bei denen uns die Beschwerdeführer berichteten, dass diese – teils weil sie einen neugierigen Blick ins Innere des Fahrzeugs geworfen haben – von der Displayanzeige der Umfelderfassung des Fahrzeugs irritiert gewesen seien.

Die datenschutzrechtliche Frage bei dieser Überwachungstechnik – Sentry Mode genannt – ist, ob eine Umfeldüberwachung eines Tesla-Fahrzeugs, bspw. auf dem Parkplatz eines Supermarkts, durch die vorhandenen hochauflösenden Kameras des Fahrzeugs zulässig ist. Zentral ist dabei auch zu klären, ob die Aufzeichnung durch die Fahrzeuge schon bei einer Näherung an das Fahrzeug stattfindet oder erst, nachdem dieses mittels Bewegungssensoren ein Rütteln oder eine starke Beschleunigung (z. B. bei einem Auffahrunfall) festgestellt hat. Da es aufgrund der Beeinträchtigung des Persönlichkeitsrechts bei einer anlasslosen Videoüberwachung von öffentlich zugänglichen Flächen regelmäßig datenschutzrechtlich unzulässig ist, derartige Aufnahmen anzufertigen (z. B. bei Dashcams), beabsichtigen wir im Rahmen einer Kontrolle, u. a. eigene Analysen an einem Tesla-Fahrzeug im Jahr 2020 durchzuführen, um insbesondere den Einsatz des Sentry Modes auf Grund der vorhandenen Beschwerden datenschutzrechtlich abschließend zu bewerten.

Wer als Tesla-Fahrer jetzt schon auf Nummer sicher gehen und keinen datenschutzrechtlichen Verstoß riskieren möchte, sollte diese Funktion entweder nicht oder nur auf dem eigenen Grundstück ohne Blick auf einen öffentlichen Bereich (z. B. öffentliche Straße) aktivieren.

18.4 Umgang mit Bedrohungen durch Emotet

Klassische Virenscanner bieten nach wie vor kaum Schutz vor Emotet – der Sicherheitsfaktor Mensch bleibt gerade bei E-Mail-Kommunikation ein Schlüsselfaktor.

Auch im Jahr 2019 blieb die Bedrohungslage durch Schadsoftware für Betriebe und Bürger allgemein hoch. Besonders hervorgehoben hat sich dabei die Malware Emotet, die bei vielen bei uns eingegangenen Meldungen zur Verletzung der Sicherheit nach Art. 33 DS-GVO die Ursache war.

Emotet stellt seit Längerem eine der größten Bedrohungen im Internet dar, da dieser Trojaner in der Regel aufgrund seiner sogenannten polymorphen Struktur von signaturbasierten Virenscannern nicht erkannt wird. Dies führt dazu, dass Nutzer im Posteingang direkt mit der gefährlichen E-Mail konfrontiert werden, anstatt dass diese wie bei anderen Schädlingen herausgefiltert werden. Nutzer, die eine solche authentisch aufbereitete, aber eben gefälschte Mail erhalten, öffnen oft das enthaltene Word-Dokument im Anhang oder klicken auf einen Link. Damit wird dann der Download des eigentlichen Emotet-Schadcodes samt automatischer Ausführung auf dem System ausgelöst.

Während Emotet im Jahr 2014 noch als Banking-Trojaner fungierte, ist dessen Funktionalität heute weit umfassender. Man kann sagen, dass jedes mit Emotet infizierte System Teil eines weltumfassenden Emotet-Botnetzes wird, das von Cyberkriminellen für verschiedene Angriffe – je nach Geschäftsmodell – verwendet wird. So kommt es bei manchen Systemen, teils erst nach Wochen, nachdem auf einen Link einer Mail geklickt wurde, zu einer Verschlüsselung von Dateien samt Lösegeldforderung (Ransomware), während bei anderen Systeme die E-Mail-Kommunikation samt Adressbücher abgezogen wird, um damit weitere Systeme zu infizieren. Es ist ebenfalls möglich, dass sich der Schadcode im lokalen Netzwerk weiterverbreitet, dort weitere Systeme infiziert und diese zum Bestandteil des Botnetzes macht.

Die meisten solcher Meldungen nach Art. 33 DS-GVO erhielten wir von Unternehmen, die mit einem Emotet infiziert wurden, der die E-Mail-Kommunikation ausleitet, die dann im Namen des betroffenen Unternehmens für weitere automatisierte Angriffe verwendet werden. Die Unternehmen wurden hierbei von bestehenden Kommunikationspartnern darauf hingewiesen, dass sie eine vermeintliche E-Mail samt Schadcode(link) von diesen erhalten hätten.

Die bei uns registrierten Emotet-Meldungen umfassten im Prinzip alle Sektoren und Unternehmensgrößen, sowohl mittelständische und kleine Unternehmen als auch Ärzte oder Rechtsanwälte. Wir haben uns deshalb veranlasst gesehen, im Rahmen einer Pressemitteilung vor einer entsprechenden Infektionswelle zu warnen:

www.lda.bayern.de/media/pm/pm2019_15.pdf

18.5 E-Mail-Kommunikation zwischen Berufsgeheimnisträgern und betroffenen Personen

Soweit in E-Mails von Berufsgeheimnisträgern (z. B. Rechtsanwälten) an betroffene Personen auch sensible Daten Dritter enthalten sind, entscheidet das Risiko, wie diese verschlüsselt werden müssen.

Berufsgeheimnisträger (z. B. Rechtsanwälte, Ärzte) kommunizieren mit ihren Mandanten oder Patienten weiterhin häufig per E-Mail. Dies ist auch grundsätzlich möglich, da bspw. Anwälte gemäß Art. 6 Abs. 1 Satz 1 Buchst. f DS-GVO insoweit ein berechtigtes Interesse an der effizienten Abwicklung ihres Schriftverkehrs geltend machen können.

Allerdings haben Rechtsanwälte dann auch nach Art. 32 DS-GVO geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. In diesem Zusammenhang ist zu berücksichtigen, dass Berufsgeheimnisträger hinsichtlich aller Informationen, die ihnen in Ausübung ihres Berufs bekannt geworden sind, zur Verschwiegenheit verpflichtet sind (§ 43a Abs. 2 Bundesrechtsanwaltsordnung). Ein Verstoß hiergegen stellt sogar eine Straftat nach § 203 Abs. 1 Nr. 3 Strafgesetzbuch dar.

Aus diesem Grund müssen Berufsgeheimnisträger unserer Auffassung nach beim Versand von E-Mails grundsätzlich auf das Vorhandensein einer Transportverschlüsselung achten. Bei einem hohen Risiko für die Rechte und Freiheiten ist zusätzlich eine Inhaltsverschlüsselung (beispielsweise mittels PGP oder SMIME) vorzusehen.

Ein Absenken des angemessenen Schutzniveaus bei einem hohen Risiko hin zu einer bloßen Transportverschlüsselung ist zwar mit Zustimmung der betroffenen Person möglich; dies gilt jedoch nur insoweit, als hiervon ausschließlich Daten der betroffenen Personen enthalten sind. Soweit E-Mails eines Berufsgeheimnisträgers auch sensible personenbezogene Daten Dritter mit einem hohen Risiko (z. B. zu der gegnerischen Partei bei einem Rechtsanwalt) enthalten, ist zwingend eine Inhaltsverschlüsselung vorzunehmen.

Der sendende Berufsgeheimnisträger muss bei Versand von Daten von Dritten sich zudem vergewissern, dass der E-Mail-Provider des Empfängers (d. h. der der betroffenen Person) die Inhalte der E-Mail nicht zu Werbezwecken auswertet. Sollte dies der Fall sein, wie es bspw. bei vielen Freemail-Providern der Fall ist, ist unabhängig vom Risiko eine Inhaltsverschlüsselung vorzunehmen.

18.6 Cyberabwehr Bayern

Die Cyberabwehr Bayern soll künftig einen engen und schnellen Fachaustausch zwischen den staatlichen Akteuren im Bereich Cybersicherheit gewährleisten.

Vor dem Hintergrund einer zunehmenden und überregionalen Bedrohungslage aus dem Cyberraum hat die Bayerische Staatsregierung beschlossen, zum 01.01.2020 die „Cyberabwehr Bayern“ ins Leben zu rufen.

www.stmi.bayern.de/med/aktuell/archiv/2019/191105mr/

Dabei handelt es sich um eine ausschließlich behördeninterne Informations- und Kooperationsplattform für alle bayerischen Landesbehörden mit Cybersicherheitsaufgaben. Die Teilnehmer der Cyberabwehr Bayern sind daher das Cyber-Allianz-Zentrum (CAZ) im Bayerischen Landesamt für Verfassungsschutz, die Zentrale Ansprechstelle Cybercrime (ZAC) im Bayerischen Landeskriminalamt, die Zentralstelle Cybercrime der Generalstaatsanwaltschaft Bamberg (ZCB), das Landesamt für Sicherheit in der Informationstechnik (LSI), das Bayerische Landesamt für Datenschutzaufsicht (LDA) und der Bayerische Landesbeauftragte für den Datenschutz (LfD).

Dieses Gremium hält regelmäßig gemeinsame Lagebesprechungen ab, um aktuelle cybersicherheitsrelevante Ereignisse zu erörtern, aus der jeweils behördenspezifischen Perspektive zu bewerten und sich maßnahmenorientiert abzustimmen. Dadurch werden Kompetenzen gebündelt, Ressourcen effizienter eingesetzt und Reaktionszeiten – insbesondere in Krisenlagen – verkürzt sowie ein breiterer Überblick über die aktuelle Cyberlage ermöglicht.

19

Bußgeldverfahren

19 Bußgeldverfahren

19.1 Zentrale Bußgeldstelle

Organisatorisch haben wir im Jahr 2019 unsere mit zwei Personen besetzte Zentrale Bußgeldstelle (ZBS) geschaffen. Die Personen der ZBS arbeiten ausschließlich in diesem Bereich und nicht mehr, wie früher, teilweise auch im aufsichtlichen Bereich.

19.2 Bußgeldverfahren

Nach wie vor erreichen uns viele Fälle, die den Einsatz von Dash-Cams, Videoüberwachung des öffentlichen Raums durch Private oder Veröffentlichungen personenbezogener Daten im Internet ohne Einwilligung der Betroffenen – v. a. auf Social-Media Plattformen wie Facebook, Instagram und WhatsApp – betreffen.

Insgesamt haben wir ca. 100 Bußgeldverfahren abgeschlossen, eines davon mit einem Bußgeldbescheid nach der DS-GVO. Darüber hinaus befinden sich derzeit einige Verfahren bereits im Stadium der Anhörung und werden in absehbarer Zeit in den Erlass eines Bußgeldbescheides münden.

Die Bußgeldverfahren bezogen sich auch in diesem Berichtszeitraum teilweise noch auf die alte Rechtslage, da die Datenschutzverstöße noch vor dem 25. Mai 2018 begangen wurden. Für Handlungen, die vor dem 25. Mai 2018 beendet wurden, gilt aufgrund des sog. Meistbegünstigungsprinzips des § 4 Abs. 3 des Gesetzes über Ordnungswidrigkeiten (OWiG) zumeist noch die alte – mildere – Rechtslage weiter, sodass auf diese Sachverhalte die Bußgeldvorschrift des § 43 Bundesdatenschutzgesetz alte Fassung anzuwenden ist. Inzwischen handelt es sich aber in der überwiegenden Mehrheit an Fällen um Bußgeldverfahren nach der DS-GVO.

Die jeweiligen Sachverhalte wurden unserer Zentralen Bußgeldstelle auf verschiedenen Wegen zur Kenntnis gebracht: Unmittelbar durch die betroffenen Personen, über die Polizei oder durch Abgaben der Staatsanwaltschaft nach Abschluss des dortigen strafrechtlichen Ermittlungsverfahrens gemäß § 43 OWiG zur Prüfung der datenschutzrechtlichen Ordnungswidrigkeiten in eigener Zuständigkeit.

Wegen der Überlastung unserer Behörde (siehe Vorwort dieses Berichts) konnte eine Abgabe von den jeweiligen aufsichtlichen Fachbereichen nur in einem geringen Umfang erfolgen, da schließlich auch die Aufbereitung eines festgestellten Verstoßes für die Bußgeldstelle mit einem Aufwand verbunden ist. Durch eine interne Dienstanweisung und Verfahrensbeschreibung soll in Zukunft erreicht werden, dass bußgeldrelevante Verstöße, die im aufsichtliche Verfahren festgestellt wurden, vermehrt an die Bußgeldstelle abgegeben werden können.

19.3 Datenabruf für private Zwecke

Beschäftigte von öffentlichen Stellen, die von dienstlichen Geräten personenbezogene Daten für private Zwecke abrufen, werden nicht zu Verantwortlichen.

Weiterhin galt es für uns verschiedenste Probleme, die die neue Rechtslage mit sich bringt, zu lösen. So wurde beispielsweise im Berichtszeitraum in Zusammenarbeit mit dem Bayerischen Landesbeauftragten für den Datenschutz (BayLfD) die Zuständigkeit für Bußgeldverfahren gegen Mitarbeiter öffentlicher Stellen, die unzulässig Datenabrufe zu privaten Zwecken vornehmen, wie folgt geklärt:

Datenabrufe durch Mitarbeiter öffentlicher Stellen aus behördlichen Datenbanken – wie bei-

spielsweise aus polizeilichen Recherchesystemen – sind nur dann erlaubt, wenn ein dienstlicher Anlass dafür besteht.

Kern des behandelten Problems ist die Frage, ob ein Mitarbeiter einer öffentlichen Stelle bei einem Datenabruf aus einem behördlichen Abfragesystem ohne dienstlichen Anlass, d. h. zu rein privaten Zwecken, selbst zum Verantwortlichen im Sinne des Art. 4 Nr. 7 DS-GVO wird – mit der Konsequenz der Anwendbarkeit des Art. 83 DS-GVO – oder Teil der verantwortlichen öffentlichen Stelle bleibt, sodass die Bußgeldvorschrift des Art. 23 des Bayerischen Datenschutzgesetzes (BayDSG) anzuwenden ist. Wenn man der ersten Auffassung folgen würde, würde der behördliche Mitarbeiter den unzulässigen Datenabruf als nicht-öffentliche Stelle durchführen, sodass wir für die Ahndung des Verstoßes zuständig wären.

Nach übereinstimmender Ansicht des BayLfD und uns wird ein Mitarbeiter einer öffentlichen Stelle, der Datenabrufe zu rein privaten Zwecken vornimmt, nicht zum selbstständigen Verantwortlichen im Sinne des Art. 4 Nr. 7 DS-GVO, sondern bleibt Teil der verantwortlichen Behörde. Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO ist, wer über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der einzelne Mitarbeiter einer öffentlichen Stelle entscheidet jedoch nicht selbst über die grundsätzlichen Zwecke und Mittel der Abfragesysteme, vielmehr verwendet er lediglich die ihm zur Verfügung gestellten Programme. Darüber hinaus regelt Art. 3 Abs. 2 BayDSG auf Grundlage der in Art. 4 Nr. 7 DS-GVO enthaltenen Spezifizierungsklausel, dass Verantwortlicher für die Verarbeitung personenbezogener Daten im Sinne der DS-GVO die für die Verarbeitung zuständige öffentliche Stelle ist.

Auch ein Vergleich mit den in der DS-GVO enthaltenen Regelungen zum Auftragsverarbeiter stützt dieses Ergebnis: Ein Auftragsverarbeiter ist nicht berechtigt, Zwecke und Mittel der Datenverarbeitung zu bestimmen. In Fällen, in denen der Auftragsverarbeiter in rechtswidriger Weise seine Befugnisse überschreitet, regelt Art. 28 Abs. 10 DS-GVO, dass er für diese Verarbeitung als eigener Verantwortlicher im Sinne der DS-GVO haftbar wird. Dies ist vergleichbar mit einem Behördenmitarbeiter, der seine Befugnisse überschreitet. Eine dem Art. 28 Abs. 10 DS-GVO entsprechende Regelung zur eigenen Verantwortlichkeit von Behördenmitarbeitern bei Datenverarbeitungen zu privaten Zwecken fehlt jedoch, sodass davon auszugehen ist, dass der Gesetzgeber eine solche gerade nicht regeln wollte.

In der Konsequenz bedeutet dies, dass mangels Verantwortlichkeit des den Datenabruf tätigenden Mitarbeiters nicht die Verwirklichung einer Ordnungswidrigkeit nach Art. 83 DS-GVO, sondern nur die Verwirklichung einer Ordnungswidrigkeit nach Art. 23 BayDSG in Betracht kommt.

Die Zuständigkeit für die Ahndung einer solchen Ordnungswidrigkeit nach Art. 23 BayDSG ergibt sich aus § 36 Abs. 2 OWiG in Verbindung mit der (Bayerischen) Zuständigkeitsverordnung (ZustV).

Im Bereich der Polizei sind nach § 91 Abs. 3 ZustV die dem Staatsministerium des Innern, für Sport und Integration unmittelbar nachgeordneten Polizeidienststellen für die Verfolgung der Ordnungswidrigkeit zuständig. Im Übrigen kommt meist § 87 Abs. 1 Satz 1 ZustV zur Anwendung, wonach diejenige Verwaltungsbehörde zuständig ist, der der Vollzug der Rechtsvorschrift obliegt, gegen die sich die Zuwiderhandlung richtet. Das ist diejenige öffentliche Stelle, in deren Bereich der Verstoß gegen Art. 23 BayDSG begangen wurde.

Dieses Ergebnis ist in Hinblick auf eine so mögliche Harmonisierung des disziplinarrechtlichen Vorgehens und der Verfolgung der Ordnungswidrigkeit aus Art. 23 BayDSG auch sachgerecht.

Stichwortverzeichnis

R

S

T

U

V

W

Z

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 18
91522 Ansbach

Tel.: 0981 180093-0
Fax: 0981 180093-800
E-Mail: poststelle@lda.bayern.de
Web: www.lda.bayern.de