Bayerisches Landesamt für
Datenschutzaufsicht

8. Tätigkeitsbericht

2017/2018

8. Tätigkeitsbericht des Bayerischen Landesamts für Datenschutzaufsicht
für die Jahre 2017 und 2018

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 März 2019 – Thomas Kranig, Präsident

Bildnachweis Cover: de.123rf.com – Urheber alicephoto – Dateinummer 40781521

Vorwort

Die Datenschutz-Grundverordnung (DS-GVO) war sicherlich das Top-Datenschutzthema der vergangenen beiden Jahre. Nicht nur Bürger und Unternehmen waren gespannt, was das neue europäische Datenschutzrecht ab dem 25. Mai 2018 mit sich bringt, sondern auch wir als bayerische Datenschutzaufsicht für den nicht-öffentlichen Bereich.

Vorbereitung auf die DS-GVO

Das Jahr 2017 war besonders geprägt von den intensiven Vorbereitungen auf diese neuen gesetzlichen Anforderungen. Durch interne Schulungen, Fachaustausch mit anderen Aufsichtsbehörden und Teilnahme an bzw. Durchführung von Info-Veranstaltungen haben wir uns verstärkt darum bemüht, frühzeitig ein Bild über die EU-Vorgaben zu gewinnen. Wir haben uns dann nicht gescheut, mit Handreichungen und sonstigen Informationen zur DS-GVO öffentlich in Vorträgen, bei ERFA-Kreisen und auf unserer Website Stellung zu verschiedenen Themen zu beziehen. Wir konnten in der Folgezeit wesentlich dazu beitragen, dass die deutschen Datenschutzbehörden im Rahmen der Datenschutzkonferenz (DSK) unserem Veröffentlichungskonzept von Kurzpapieren folgten und abgestimmte Inhalte zur DS-GVO publik machten. Die DSK verständigte sich nach einer weiteren Anregung von uns erstmals auch auf einen gemeinsamen Webauftritt, der von uns entwickelt wurde, unter www.datenschutzkonferenz-online.de abrufbar ist und technisch von uns betreut wird.

Konfrontation mit der Realität

Trotz aller Anstrengungen im Vorfeld wurden wir letztendlich aber im Mai 2018 von der Realität eingeholt: Mit Start der DS-GVO erlebten wir einen regelrechten Ansturm von Beratungsanfragen. Gerade in den ersten Tagen waren wir Land unter, das Telefon klingelte ununterbrochen. Besorgte Personen wollten sich über die neuen Verpflichtungen informieren. An manchen Tagen kamen so viele Anrufe bei uns an, dass alleine das Zählen der Beratungsanfragen gar nicht mehr geordnet möglich war. Nach kurzer Zeit mussten wir daher die Reißleine ziehen und unsere bis dato uneingeschränkte telefonische Erreichbarkeit schweren Herzens durch feste Telefonsprechzeiten auf Vormittag begrenzen. Nur so konnten wir einen einigermaßen geregelten Betriebsablauf, insbesondere bei der Erfassung der Eingänge auf den anderen Kommunikationswegen wie E-Mail und Post weiter gewährleisten.

Unterstützung von Vereinen und KMUs

Durch die DS-GVO rückte der Datenschutz medial in einen völlig neuen Fokus. Es gab nahezu täglich umfangreiche Berichterstattungen zum EU-Datenschutzrecht. Dies führte an mancher Stelle zu erfreulichem Datenschutzbewusstsein, an anderer Stelle jedoch auch zur Fehlinformation und damit resultierender Verunsicherung. Viele Unklarheiten und Befürchtungen haben wir dabei gerade aus dem Kreis der kleineren Organisationen vernommen. Aus diesem Grund haben wir uns entschlossen, vor allem den Vereinen und ehrenamtlich Tätigen eine schnelle und unkomplizierte Hilfestellung bei der Anwendung des neuen Datenschutzrechts zu geben, indem wir zum ersten Mal eine Telefon-Hotline – speziell für das Thema DS-GVO – eingerichtet haben. Die Rückmeldungen hierzu waren äußerst positiv, jedoch der Aufwand für uns nicht zu unterschätzen. Es könnte dennoch eine Option für die Zukunft sein.

Darüber hinaus haben wir aber auch persönlich durch unzählige Veranstaltungen vor Ort in ganz Bayern mit zum Teil mehreren hundert Teilnehmern aktiv und umfassend über die Anforderungen der DS-GVO informiert. So war auch ich als Präsident auf dutzenden Terminen meist abends persönlich als Referent tätig und erklärte möglichst verständlich, dass die DS-GVO nicht ein Bürokratiemonster ist, wie es viele befürchteten. Zusammen mit den Informationen auf unserer Website wollten wir so Ängste

gezielt abbauen und dafür sorgen, dass bayerische Verantwortliche aus dem nicht-öffentlichen Bereich den neuen Vorgaben gerecht werden können. Das scheint uns gelungen zu sein.

Datenschutzkontrollen durch das BayLDA

Auch wenn uns der Trubel durch die DS-GVO reichlich beschäftigte und selbst wir eine Art Anpassungszeit benötigten, hatten wir uns entschieden, durch Datenschutz-Kontrollen nicht nur unserem Ruf als aktiv prüfende Datenschutzaufsichtsbehörde, sondern insoweit auch unserem Auftrag aus der DS-GVO gerecht zu werden. Durch flächendeckende Prüfungen haben wir erneut auf die Wichtigkeit von Cybersicherheit hingewiesen, Schwachstellen auf bayerischen Websites aufgezeigt und die verantwortlichen Betreiber nicht nur sensibilisiert, sondern auch dazu bewegt, die Missstände zu beseitigen. Des Weiteren führten wir auch Kontrollen in vielen anderen Datenschutzbereichen wie der Videoüberwachung, dem Online-Tracking und den Informationspflichten in ganz Bayern durch.

Als Bestätigung unserer Facebook Custom Audience-Prüfung empfanden wir die Entscheidungen des Verwaltungsgerichts Bayreuth und des Bayerischen Verwaltungsgerichtshofs, die unsere Auffassung, dass der Einsatz von Facebook Custom Audience ohne Einwilligung des Nutzers rechtswidrig ist, für zutreffend erklärten.

Überlastung als drohender Dauerzustand

Ob und in welchem Umfang wir künftig aktiv kontrollieren und beraten können, hängt letztendlich entscheidend von unserer Personalstärke ab. Derzeit befinden wir uns in einer schier aussichtslosen Lage: Täglich gehen deutlich mehr Eingaben und Meldungen von Datenschutzverletzungen ein, als wir abarbeiten können, von der enormen Anzahl von Beratungsanfragen ganz abgesehen. Unser Schuldenberg bzw. Arbeitsvorrat wächst stetig, weshalb sich die Wartezeiten auf eine Rückmeldung von uns enorm verlängerten – zur Unzufriedenheit aller Beteiligten. Ein Blick in die Statistiken dieses Tätigkeitsberichts zeigt die dramatische Entwicklung der Fallzahlen. Wenn der bayerische Haushaltsgesetzgeber dem Vorschlag der Bayerischen Staatsregierung für den Doppelhaushalt 2019/2020 folgt und uns keine einzige, weitere Stelle zuerkennen würde, werden wir unsere Prioritäten völlig neu ausrichten müssen, um den dringenden Anforderungen der DS-GVO gerecht zu werden. Die starke Überbelastung insbesondere im Jahr 2018 haben die Mitarbeiter im Hinblick auf die als sicher angesehene Verstärkung durch den nächsten Haushalt ertragen. Auf Dauer wird das nicht gehen.

Sollte es bei dem Vorschlag bleiben, müssen wir unsere Beratungsleistungen für Vereine, Verbände und kleine und mittlere Unternehmen (KMU), aber auch für die sehr innovativen Großunternehmen in Bayern, die Mitwirkung bei Zertifizierungen u. a. weitgehend einstellen. Gerade diese Tätigkeit, in der sich unser (bisheriges) Leitbild verwirklicht hat, dass nämlich jede Beratung, die dazu beiträgt, dass kein Datenschutzverstoß begangen wird, viel mehr wert ist als zahlreiche Sanktionen, wird so nicht mehr möglich sein. Die bisherige Praxis, nämlich niederschwellig und vollziehbar die Anforderungen der DS-GVO zu erläutern, hat uns innerhalb und auch außerhalb von Bayern einen besonderen Ruf als offene und praxisorientierte Aufsichtsbehörde eingebracht (so jedenfalls die uns zugetragenen Reaktionen). Das werden wir mit dem vorhandenen Personal nicht mehr leisten können. Fristen zur Bearbeitung von Beschwerden und gemeldeten Datenschutzverstößen lassen uns nicht mehr viel Spielraum für Beratung.

Besonderheit dieses Tätigkeitsberichts

Künftig werden wir nicht mehr wie bisher im Zyklus von zwei Jahren, sondern gemäß DS-GVO jährlich einen Bericht über unsere Tätigkeit erstellen. Somit ist dies der letzte Tätigkeitsbericht, der relativ umfangreich ausgewählte Sachverhalte aus den vergangenen zwei Jahren darstellt.

Ich möchte mich an dieser Stelle bei allen meinen Mitarbeitern für den enormen Einsatz bedanken, den sie in den letzten beiden Jahren geleistet haben. Ich wünsche ihnen und mir, dass wir in absehbarer Zeit wieder Rahmenbedingen vorfinden werden, die es uns auf Dauer ermöglichen, doch das volle Programm einer motivierten Datenschutzaufsichtsbehörde erfüllen zu können.

Ansbach, im März 2019

Thomas Kranig
Präsident

Inhaltsverzeichnis

Vorwort ... **1**

Inhaltsverzeichnis ... **4**

1 Datenschutzaufsicht im nicht-öffentlichen Bereich ... **10**

1.1 Datenschutz in Bayern ... 10

1.2 Das Bayerische Landesamt für Datenschutzaufsicht ... 10

1.3 Gesetzliche Grundlage für den Tätigkeitsbericht ... 12

2 Zahlen und Fakten ... **14**

2.1 Beschwerden ... 14

2.2 Beratungen ... 16

2.3 Datenschutzverletzungen ... 18

2.4 Abhilfemaßnahmen ... 19

2.5 Europäische Verfahren ... 19

2.6 Förmliche Begleitung von Rechtsetzungsvorhaben ... 20

2.7 Ressourcen ... 20

2.8 Vorträge und Öffentlichkeitsarbeit ... 21

3 Europäische Zusammenarbeit ... **23**

3.1 Verfahren der Zusammenarbeit und Kohärenz ... 23

3.2 Mitwirkung in Subgroups des EDSA ... 24

4 Kontrollen und Prüfungen ... **27**

4.1 Videoüberwachung in Gastronomie und Kinos ... 27

4.2 Kfz-Werkstätten-Kontrolle ... 28

4.3 Patch Management bei WordPress-Websites ... 29

4.4 WordPress GDPR Compliance Plugin ... 31

4.5 Patch Management bei Magento-Websites ... 31

4.6 Informationspflichten bei Bewerbungen ... 32

4.7 DS-GVO-Prüfung bei kleinen und mittleren Unternehmen ... 33

4.8 Rechenschaftspflicht bei Großkonzernen ... 33

4.9 Ransomware bei Arztpraxen ... 34

4.10 HTTPS-Prüfung ... 35

5 Der betriebliche Datenschutzbeauftragte ... **37**

5.1 Erforderlichkeit einer Benennung ... 37

5.2 Überwachungsaufgaben des Datenschutzbeauftragten ... 38

6 Auftragsverarbeitung ... **40**

6.1 Vertrag zur Auftragsverarbeitung und Formulierungshilfe 40
6.2 Abgrenzung Verantwortlicher zu Auftragsverarbeiter 40
6.3 Datenschutzrechtliche Anforderungen an Dienstleister 41
7 Betroffenenrechte 43
7.1 Informationspflichten 43
7.1.1 Informationspflichten in abgestufter Umsetzung 43
7.1.2 Informationspflichten bei Karten-Zahlungen 43
7.1.3 Informationspflichten bei Traueranzeigen 44
7.1.4 Informationspflichten am Telefon 44
7.1.5 Informationspflichten zur Gesprächsaufzeichnung in Callcentern 45
7.1.6 Informationspflichten bei Ärzten 45
7.2 Auskunft 46
7.2.1 Auskunftsrecht bei Ärzten 46
7.2.2 Kopien von Unterlagen bei Auskunft 46
7.3 Berichtigung 47
7.3.1 Allgemeines zum Recht auf Berichtigung 47
7.3.2 Berichtigung eines Werturteils in Versicherungs- oder Arztakten 47
7.4 Löschung 48
7.4.1 Löschung bei Werbung 48
7.4.2 Löschung bei Patientendaten 48
7.5 Datenübertragbarkeit 49
7.5.1 Allgemeines zum Recht auf Datenübertragbarkeit 49
7.5.2 Datenübertragbarkeit bei Ärzten 49
8 Datenschutz im Internet 52
8.1 Bewertungsportale 52
8.2 Datenschutzbestimmungen auf Websites 53
8.3 Cookie-Banner 55
8.4 Kontaktformulare 55
8.5 Fotos auf Websites 56
8.6 WhatsApp 58
8.7 Facebook Custom Audience über die Kundenliste 58
8.8 Facebook-Fanpages 60
8.9 Offline-Tracking 60
9 Steuerberater und Rechtsanwälte 63
9.1 Auftragsverarbeitung bei Steuerberatern 63

9.2 Entsorgung von Akten bei Berufsgeheimnisträgern ... 63
10 Versicherungswirtschaft und Banken ... 66
10.1 Datenweitergabe innerhalb der Versicherungsgruppe ... 66
10.2 Videoidentifizierung und Ausweiskopien ... 67
11 Auskunfteien ... 70
11.1 Bewertung von Auskunfteien nach der DS-GVO ... 70
11.2 Verhaltensregeln der Auskunfteien zu Prüf- und Löschfristen ... 70
12 Werbung und Adresshandel ... 72
12.1 Neue Orientierungshilfe derAufsichtsbehörden ... 72
12.2 Weihnachts-, Neujahrs- und sonstige Glückwunschkarten ... 72
12.3 Zustimmung zur Werbung und Koppelungsverbot ... 72
13 Handel und Dienstleistung ... 75
13.1 Kopieren von Personalausweisen ... 75
13.2 Anlegerdaten in Publikumsgesellschaften ... 76
13.3 Wahrnehmung von Gesellschafterrechten in einer AG ... 76
13.4 Unrichtige Kundendaten bei Energieversorgern ... 77
13.5 Rechnungen vom Energieversorger an Nachlasspfleger ... 78
13.6 Daten bei anerkannten Stellen im Sinne der Luftverkehrs-Ordnung ... 79
13.7 Datenübermittlung von Reisebüros an Reiserücktrittsversicherung ... 79
13.8 Datenübermittlung durch Auftragsverarbeiter aufgrund einstweiliger Verfügung ... 80
13.9 Verweigerung der Herausgabe von Informationen über Datenabruf ... 81
14 Internationaler Datenverkehr ... 84
14.1 Standardvertrag und Auftragskette ... 84
14.2 Genehmigung von Binding Corporate Rules ... 85
15 Beschäftigtendatenschutz ... 88
15.1 Widerruf der Einwilligung zur Veröffentlichung von Mitarbeiterfotos ... 88
15.2 Fragen im Bewerbungsverfahren ... 88
15.3 Videointerviews bei Personalentscheidungen ... 89
16 Gesundheit und Soziales ... 91
16.1 Rechtsgrundlage der Verarbeitung in Arztpraxen ... 91
16.2 Diskretion bei der Anmeldung und im Sprechzimmer ... 91
16.3 Ansprache von Patienten in Arztpraxis ... 92
16.4 Schweigepflichtentbindungserklärung bei Anfragen von Gerichten ... 93
16.5 Abholung von Rezepten und Vereinbarung von Arztterminen durch den Ehepartner ... 93
16.6 Einwilligung für Behandlung durch Heilpraktiker ... 94

16.7 E-Mail-Kommunikation zwischen Arzt und Patient 94
16.8 Verarbeitung von Gesundheitsdaten bei Optikern und Sanitätshäusern 95
16.9 Telefonverzeichnis, Türschilder und Briefkästen im Seniorenheim 95
16.10 Fotos aus Kindertagesstätten für Eltern 96
16.11 Kindernamen in Kindertagesstätten 97
16.12 Elternbeirat kein eigener Verantwortlicher 97
17 Vereine und Verbände 99
17.1 Informationspflicht für Bestandsmitglieder 99
17.2 Umgang mit Kontaktdaten von Vereinsmitgliedern 99
17.3 Feuerwehrvereine 100
17.4 Fotos im Vereinsleben 101
17.5 Datenverarbeitung in einem Drittland durch einen Entwicklungshilfeverein 102
17.6 Informationskampagne zur DS-GVO für Vereine und Ehrenamt 102
18 Wohnungswirtschaft und Mieterdatenschutz 105
18.1 Einzelabrechnungen in Eigentümergemeinschaften 105
18.2 Abrechnungsdaten eines früheren Eigentümers 105
18.3 Weitergabe von Eigentümer-Daten durch den Verwalter an andere Eigentümer 106
18.4 Fotografieren der Wohnung zu Dokumentationszwecken 107
18.5 Datenerhebung von Mietbewerbern 108
19 Videoüberwachung 110
19.1 Dashcams 110
19.2 Videoüberwachung durch Privatpersonen 111
19.3 Videoüberwachung in Schwimmbädern 111
19.4 Videoüberwachung in der Gastronomie 112
20 Fahrzeugdaten 115
20.1 Mustertexte zur Kfz-Halter- und Fahrerinformation 115
20.2 Kameranutzung im Kfz für Forschungszwecke 115
21 Datenschutzverletzungen 118
21.1 Sicherheitslücke bei Hotelbuchungssoftware 119
21.2 Kryptomining auf Webservern 120
21.3 Erpressung nach Cyberangriff 120
21.4 Kundendaten aus Shop-System online einsehbar 121
21.5 Phishing-Attacke bei KRITIS-Einrichtungen 121
21.6 Hacking von eBay-Accounts 122
21.7 Angriffe auf den Login bei Online-Shops 123

21.8 Ransomware-Befall ... 123
21.9 Hacking eines Webhosting-Providers ... 124
21.10 Cyberangriff durch Emotet ... 125
22 Zertifizierung ... 128
23 Technischer Datenschutz und Informationssicherheit ... 130
23.1 Risikoorientierter Ansatz unter der DS-GVO ... 130
23.2 Cybersicherheit als gesetzliche Datenschutzkomponente ... 131
23.3 Datenschutz durch Technikgestaltung ... 132
23.4 Datenschutz-Folgenabschätzung ... 133
23.5 Wirksamkeitsprüfung im Rahmen der Rechenschaftspflicht ... 134
23.6 Facebook-App-Entwickler im Prüffokus ... 134
23.7 HTTPS-Verschlüsselung ... 135
23.8 Browser Fingerprinting ... 136
23.9 E-Mail-Verschlüsselung ... 137
23.10 Löschen unter der DS-GVO ... 138
24 Bußgeldverfahren ... 141
Stichwortverzeichnis ... 143

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 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.

1.2 Das Bayerische Landesamt für Datenschutzaufsicht

Im Berichtszeitraum haben wir durch den Haushaltsgesetzgeber im Rahmen des Doppelhaushalts 2017/2018 und im Nachtragshaushalt 2018 jeweils vier neue Stellen zugewiesen bekommen.

Heute müssen wir feststellen, dass die Anforderungen der DS-GVO an uns als Aufsichtsbehörde und die Anzahl der eingegangenen Beratungsanfragen, Beschwerden sowie Datenschutzverletzungen so gewaltig gestiegen sind, dass ein sehr kurzfristiger erheblicher Stellenzuwachs erforderlich ist, um unserer gesetzlichen Verpflichtung nachkommen zu können. Immerhin unterliegen in Bayern über 700.000 Unternehmen, freiberuflich Tätige, Handwerker u. a. sowie über 90.000 Vereine unserer Kontrolle.

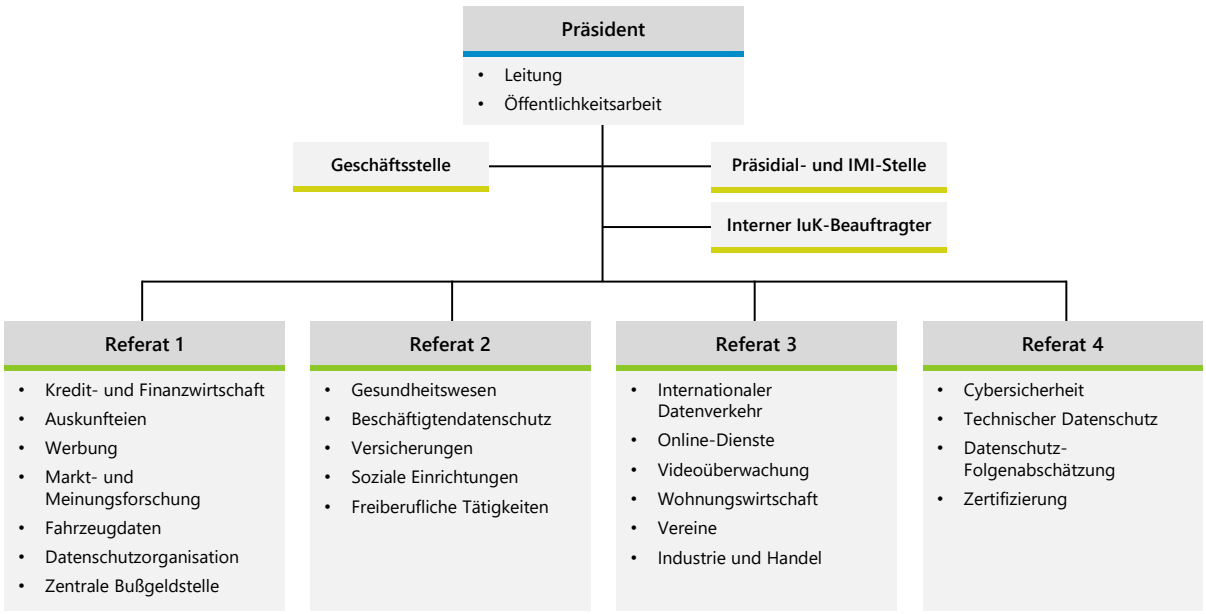
Seit Ende des Berichtszeitraums besteht in unserer Behörde ein Zustand, der nicht nur zu einer gesteigerten Unzufriedenheit bei Bürgern und anfragenden Unternehmen führt, sondern auch bei den eigenen Mitarbeiterinnen und Mitarbeitern. Bei Eingängen ist mittlerweile ein permanentes Sortieren nach deren Dringlichkeit vorzunehmen und dann letztendlich auch zu entscheiden, welche Vorgänge womöglich nicht oder zumindest nicht mehr zeitnah bearbeitet werden können. Deutlich eingeschränkt wurde zudem die telefonische Erreichbarkeit unserer

Mitarbeiter, um die schriftlich eingehenden Anfragen, Beschwerden und Datenschutzverletzungen überhaupt noch erfassen zu können. Dokumentiert wird diese permanente Überlastung der eigenen Mitarbeiterinnen und Mitarbeiter auch durch die sehr ernst zu nehmende Tatsache, dass wir unsere Spitzenposition im bayernweiten Behördenvergleich mit durchschnittlich sehr wenigen Krankheitstagen pro Mitarbeiterin bzw. Mitarbeiter mit einer erschreckenden Geschwindigkeit in die falsche Richtung abbauen. Absichernde Hinweise der Amtsleitung, dass Beschwerden von außen gegen die eigenen Mitarbeiterinnen oder Mitarbeiter wegen zu langer Bearbeitungsdauer der Vorgänge „schon abgelehnt sind, bevor sie eingegangen sind", werden als gut gemeint wahrgenommen, helfen aber nicht wirklich weiter, solange die Mitarbeiterinnen und Mitarbeiter ihren eigenen Anspruch, qualitätsvolle Arbeit leisten zu wollen, noch nicht aufgegeben haben. Um diese schwierige Situation zu meistern, ist es notwendig, den Mitarbeiterinnen und Mitarbeitern eine Perspektive für bessere Rahmenbedingungen geben zu können. Da wir die Aufgabenstellung der DS-GVO an uns und auch die Zahl der Beratungsanfragen, der Beschwerden und der Datenschutzverletzungen nicht steuern können, kann eine Verbesserung im Ergebnis nur darin liegen, dass unser Personalstand angemessen und zeitnah aufgestockt wird.

Eine Maßnahme, um die anfallende Arbeit innerhalb der Behörde etwas flexibler bei Ausfällen ausgleichen zu können, haben wir Ende 2018 getroffen: Statt bislang sechs Referate umfasst unsere Organisationsstruktur nunmehr vier Referate. Referatsleitungen können nun innerhalb des Referats besser Schwerpunkte setzen.

Die Bearbeitung grenzüberschreitender Verfahren, die seit der DS-GVO Alltag in unsere Behörde geworden sind, erfordert gute Englischkenntnisse. Bei der Neustrukturierung und personellen Besetzung der Referate wurde daher auch berücksichtigt, dass jedes Referat seine Aufgaben im nationalen als auch im internationalen Bereich eigenständig ohne fremde Übersetzungsleistung erfüllen kann.

Nachfolgend wird unsere Organisation in einem vereinfachten Organigramm dargestellt:



1.3 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 wird deshalb der letzte sein, der einen zweijährigen 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.

2

Zahlen und Fakten

2 Zahlen und Fakten

Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hatten eine Arbeitsgruppe ins Leben gerufen, die Vorschläge für die Vereinheitlichung der Erstellung der Tätigkeitsberichte machen sollte. Insbesondere die statistischen Angaben, die in Art. 59 DS-GVO angesprochen sind, sollten mit einem einheitlichen Verständnis und nach einem gleichförmigen Muster dargestellt werden. Diese Vereinheitlichung dient auch dem Zweck, dass Deutschland bei den jährlichen Abfragen des Europäischen Datenschutzausschusses bei den Aufsichtsbehörden der Mitgliedstaaten ein genaueres Bild abgeben könnte.

Die genannte Arbeitsgruppe schlug für den statistischen Teil vor, dass dieser künftig unter der Überschrift „Zahlen und Fakten" in den Tätigkeitsberichten erscheinen sollte und einheitliche Themenblöcke wie Beschwerden, Datenschutzverletzungen etc. enthält. Auch hat die Arbeitsgruppe notwendigerweise bestimmte Begriffe wie Beschwerde, Beratung usw. definiert, sodass die statistischen Angaben zu diesen Punkten besser vergleichbar werden.

Diese Vereinheitlichung begrüßen und unterstützen wir sehr. Leider kündigte bisher nur etwa die Hälfte der Aufsichtsbehörden an, diesem Vorschlag folgen zu wollen und das auch erst mit dem jeweils (kommenden) Tätigkeitsbericht, der über das Jahr 2019 berichtet. Uns hielt das nicht ab, dieses gute Arbeitsergebnis der Arbeitsgruppe schon in diesem Tätigkeitsbericht zu berücksichtigen und zu versuchen, die Basis für die angestrebte Vereinheitlichung zu schaffen. Auch wenn wir dadurch nicht in allen Bereichen vollständige Zahlen (auf Grund der zum Teil neuen Erhebungsbasis) für diesen Bericht liefern können, so sind die Weichen für den nächsten Bericht bereits gestellt. Wir informieren deshalb an den verschiedenen Stellen, was künftig dort an Statistiken abgebildet bzw. abgehandelt werden soll.

Bezüglich der von den Aufsichtsbehörden bekanntgegebenen Bearbeitungszahlen entstehen immer wieder Diskussionen und Vergleiche in der Öffentlichkeit. Es ist uns daher wichtig, in diesem Zusammenhang auf Folgendes hinzuweisen: Jede Aufsichtsbehörde ist unabhängig und entscheidet in eigener Verantwortung, welche Schwerpunkte sie im Behördenalltag setzen möchte. So kann es geschehen, dass dann, wenn eine Aufsichtsbehörde bspw. eine Prüfung über ordnungsgemäße Auskunftserteilung durchführt, das anschließende Prüfergebnis veröffentlicht und daraufhin viele Menschen feststellen, dass ihrem eigenen Auskunftsbegehren nicht ordentlich Rechnung getragen wird, die Zahl der eingehenden Beschwerden dadurch bei dieser Aufsichtsbehörde erheblich ansteigt. Durch solche öffentlichkeitswirksamen Maßnahmen kann also die Zahl der Anfragen und Beratungen enorm variieren.

Somit halten wir fest: Ausschließlich die statistischen Angaben (auch unsere) für die Beurteilung, wie gut eine Aufsichtsbehörde arbeitet, zu verwenden, kann unter Umständen zu einem nicht-zutreffenden Ergebnis bzw. zu einem verzerrten Bild der Realität führen.

2.1 Beschwerden

Die genannte Arbeitsgruppe hat für diesen Abschnitt Folgendes vorgeschlagen:

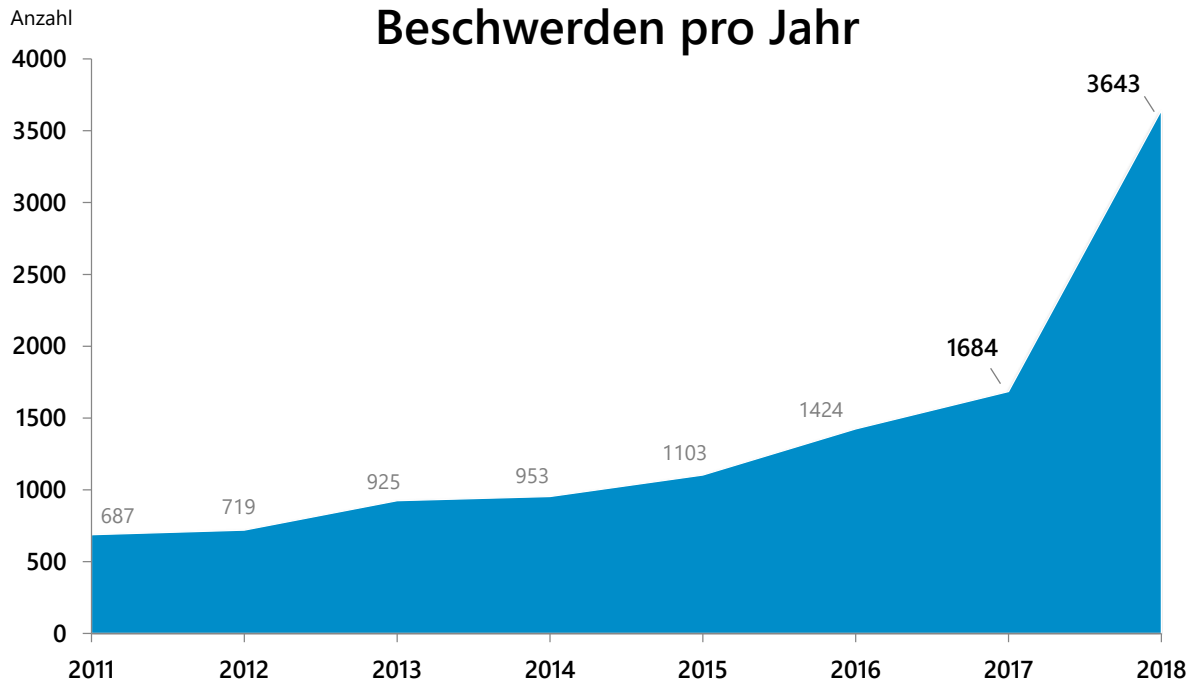
> *„Hier wird eine Übersicht gegeben über die Anzahl von Beschwerden, die im Berichtszeitraum (in Zukunft 12 Monate) eingegangen sind. Als Beschwerden werden bei Eingang solche Vorgänge gezählt, die schriftlich eingehen, bei der eine natürliche Person eine persönliche Betroffenheit darlegt, für die Art. 78 anwendbar ist. Dies schließt Abgaben ein. Telefonische „Beschwerden" können dann gezählt werden, wenn sie verschriftlicht werden (z. B. durch Vermerk)."*

Wir hatten bisher in unseren Tätigkeitsberichten unter Beschwerden alle Eingaben erst dann gezählt, wenn das Verfahren als abgeschlossen gekennzeichnet war. Wir haben nun unsere Zählweise auf die oben genannte Empfehlung umgestellt und insoweit auch die Ermittlung der unten genannten Zahlen angepasst. Auch wenn ein Großteil der Beschwerden aus 2017 und 2018 abgeschlossen werden konnten, ergibt sich durchaus ein nicht zu vernachlässigender Anteil von noch offenen Vorgängen. Dieser Umstand sollte bei Statistik-Vergleichen mit den Vorjahren berücksichtigt werden.

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 künftig nicht mehr als Beschwerden, sondern als Kontrollanregungen. In diesem Bericht konnte diese feine Unterscheidung in der Statistik noch nicht berücksichtigt werden.

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 müssten. 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 Anzahl der Beschwerden aus den vergangen beiden Jahren ist der nachfolgenden Grafik zu entnehmen:



Die Zahl der Beschwerden hat sich auf den ersten Blick mehr als verdoppelt. Diese Tatsache muss nicht bedeuten, dass der Umgang der Verantwortlichen mit personenbezogenen Daten in Bayern deutlich schlechter geworden ist, sondern vielmehr, dass die zahlreichen Veranstaltungen, Presseberichte und Informationsmaterialien dazu geführt haben, dass es 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 müssen wir jedoch dabei eine gewaltige Zunahme an Arbeitslast feststellen, die mit dem bestehenden Personal nicht zu bewältigen ist. Seit über einem Jahr gibt es keinen Monat, bei dem es uns gelingt, mehr Beschwerdeverfahren abzuschließen als neue eingehen. Im Ergebnis bedeutet dies, dass wir zum Ende des Berichtszeitraums einen gewaltigen Arbeitsvorrat in das Jahr 2019 mitgenommen haben. Unter Punkt 2.7 dieses Berichts zeigen wir auf, wie sich die genauen Zahlen der verschiedenen Eingänge im Verhältnis zu unseren Personalressourcen darstellen.

2.2 Beratungen

Die genannte Arbeitsgruppe hat für diesen Abschnitt Folgendes vorgeschlagen:

> *„Hier wird eine Übersicht gegeben über die Anzahl von schriftlichen Beratungen. Dies umfasst summarisch Beratungen von Verantwortlichen, betroffenen Personen und der eigenen Regierung. Ausschließlich (fern) mündliche Beratungen werden ebenso wie Schulungen, Vorträge etc. nicht berücksichtigt."*

Wir hatten in unseren früheren Tätigkeitsberichten unter Beratungen alle Anfragen gezählt – unabhängig davon, ob sie telefonisch, persönlich oder schriftlich eingingen. Diesen Ansatz hielten wir bislang für sehr wichtig, da ein wesentlicher Teil der Anfragen nicht nur per Telefon einging, sondern dort auch persönlich von dem jeweiligen Mitarbeiter aus dem Fachreferat beantwortet wurde. Dies war ein kostenfreier Service, der sicherlich für eine Behörde nicht selbstverständlich war und gerade deshalb sehr gut von Hilfesuchenden angenommen wurde. 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.

Auf Grund der enormen Verunsicherung durch die DS-GVO glühte bei uns förmlich die Telefonleitung: An manchen Tagen im Mai 2018 wurden über 100 telefonische Beratungsanfragen von uns erfolgreich durchgeführt, was einen erheblichen, zeitlichen Aufwand für uns bedeutete. Da unser Behördenalltag drohte dadurch lahmgelegt zu werden, mussten wir unsere telefonische Erreichbarkeit auf vormittags begrenzen und das direkte Verbinden zu den jeweiligen Fachexperten oftmals blocken, damit diese noch ihren anderen Aufgaben nachgehen konnten.

Damit dieser äußerst wichtige Teil unserer Arbeit, der auch den Charakter der Ausrichtung unserer Behörde prägt, nicht aus dem Statistikbereich verschwindet, wollen wir künftig zwar das einheitliche Beratungsschema der Arbeitsgruppe verwenden, aber zusätzlich noch unsere telefonischen Beratungen ausweisen. Zudem werden wir – weil dies sicherlich für einige Interessierte von Relevanz ist – zwischen Beratungen für Bürger und Beratungen für Verantwortliche unterscheiden.

Es findet derzeit eine intensive Diskussion unter den Aufsichtsbehörden über die Frage statt, ob Beratungen überhaupt eine Pflichtaufgabe der Aufsichtsbehörden nach der DS-GVO sind. Unsere eigenen Erfahrungen mit Beratungen waren fast durchweg positiv, da wir insbesondere den anfragenden Verantwortlichen ein Stück Rechtssicherheit vermitteln konnten und auf der

anderen Seite so erfahren haben, welche Bearbeitungen in der Praxis stattfinden oder geplant sind. Wir selbst möchten also gerne weiter an der gelebten Praxis festhalten und eine Behörde sein, die als offene Anlaufstelle für Datenschutzfragen wahrgenommen wird. Damit dieses Beratungsangebot nicht ausgenutzt wird, bestehen wir bei Anfragen von Unternehmensberatungen, Rechtsanwaltskanzleien und externen Datenschutzbüros darauf, dass neben dem Sachverhalt mit der dazugehörigen Frage auch ein eigener Lösungsvorschlag dazu unterbreitet wird.

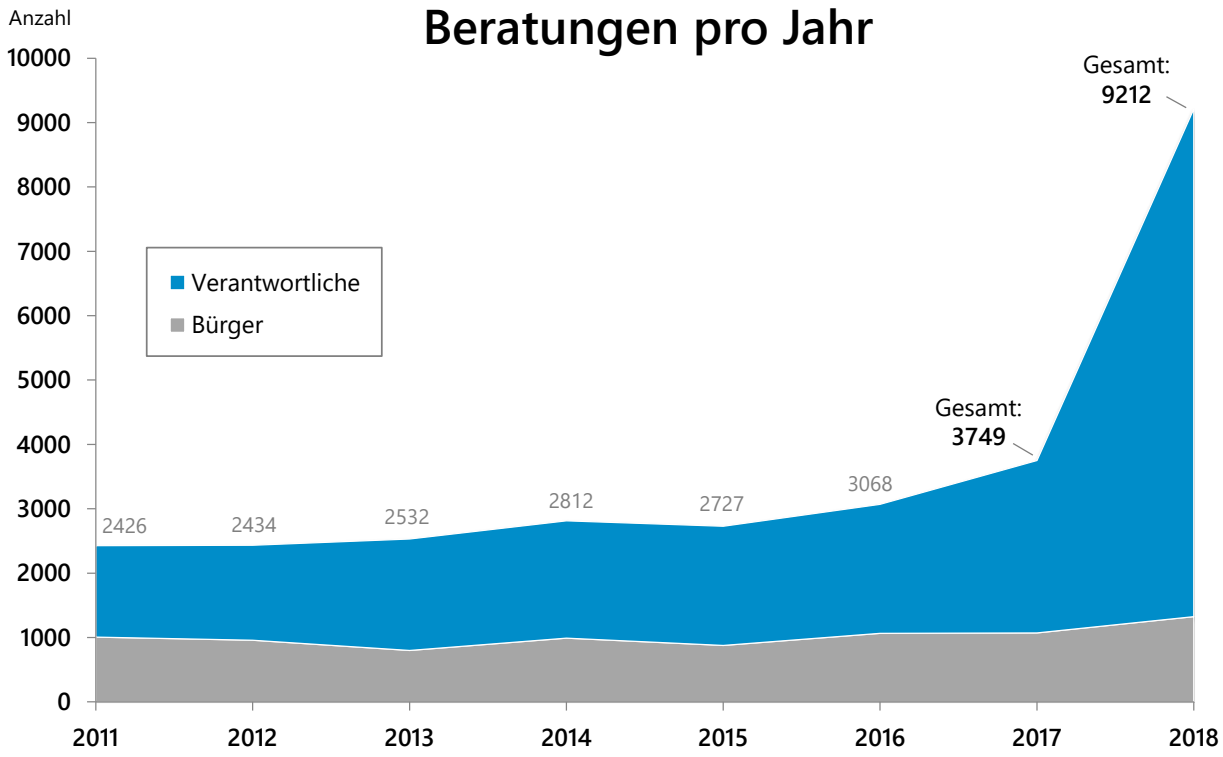
Bei der Begutachtung der Beratungsanfragen ist in den vergangenen zwei Jahren eine exorbitante Steigerung zu erkennen. Auf Grund der Rechtsunsicherheiten bei der Anwendung des neuen Datenschutzrechts war dies mehr als verständlich und eigentlich auch zu begrüßen. Allerdings überforderte uns dieser Zustand alleine von dem Umfang der Anfragen und zwingt uns mittlerweile daher leider zunehmend, sie nun aus Kapazitätsgründen abzulehnen. Das ist für alle Beteiligten als äußerst unbefriedigend einzustufen.

Besonders bedauerlich ist dies dann, wenn unsere Mitarbeiter bei eingehenden Fragen eigentlich schon die Antwort parat haben, aber alleine aus zeitlichen Gründen nicht mehr dazu kommen, diese nach außen zu kommunizieren. Wir hoffen, dass diese Situation nur vorrübergehend ist und wir mittelfristig mit mehr Personal auch wieder mehr Beratungsleistung erbringen können.

Beratungen im Berichtszeitraum

Verantwortliche	2017	2018
Telefonische Beratungen	1774	4329
Schriftliche Beratungen	904	3560

Bürger	2017	2018
Telefonische Beratungen	820	832
Schriftliche Beratungen	251	491



2.3 Datenschutzverletzungen

Die genannte Arbeitsgruppe hat für diesen Abschnitt Folgendes vorgeschlagen:

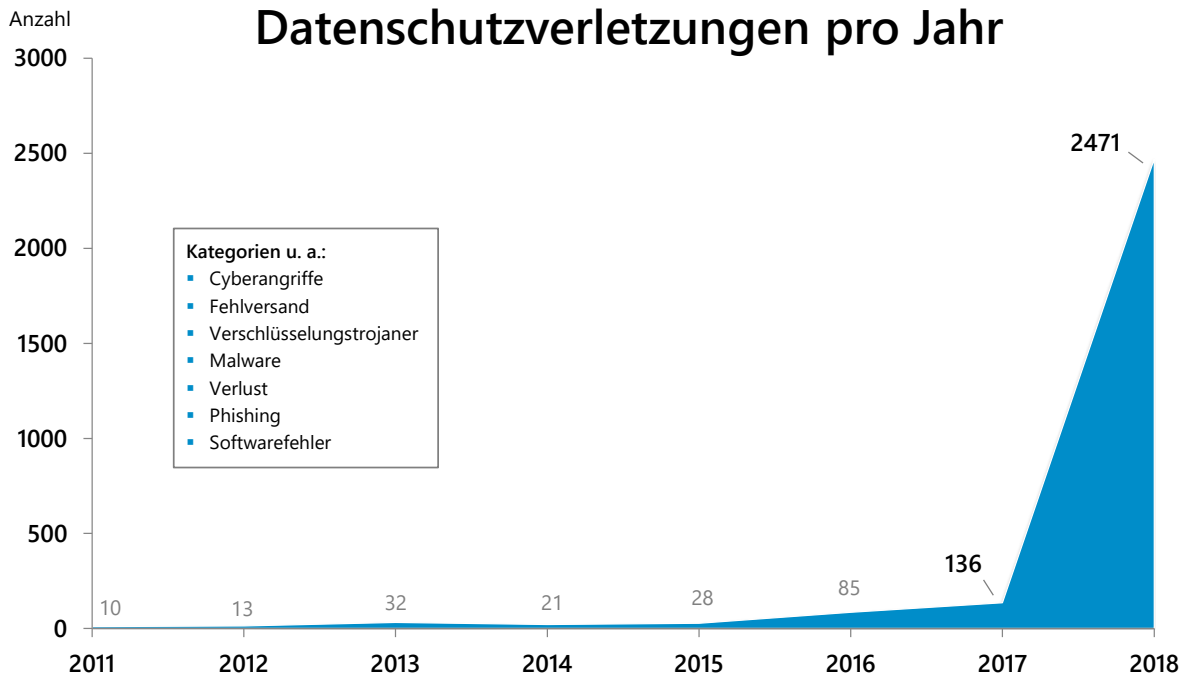
> *„Hier wird eine Übersicht gegeben über die Anzahl schriftlicher, vom jeweils Verantwortlichen eingegangener Meldungen. Soweit zusätzliche Meldepflichten außerhalb von Art. 33 DS-GVO bestehen (z. B. nach TKG bei der BfDI) können diese Zahlen gesondert aufgeführt werden."*

Schon mit dem Inkrafttreten der DS-GVO war für uns erkennbar, dass die Zahl der Meldungen von Datenschutzverletzungen, umgangssprachlich Datenpannen genannt, gewaltig ansteigen dürfte. Wir sahen eine Ursache dafür in der Tatsache, dass die Schwelle der zu meldenden Vorfälle im Verhältnis zu den bisher geltenden Regelungen des BDSG-alt deutlich gesenkt wurde. Im Alltag bedeutet dies für Verantwortliche, dass bei Datenschutzverletzungen seit 25. Mai 2018 häufig die zuständige Aufsichtsbehörde informiert werden muss.

Wir haben deshalb versucht, uns auf verschiedenen Wegen auf den abzusehenden (drohenden) Anstieg vorzubereiten:

- Wir hielten Vorträge, um Verantwortliche über den neuen Umgang mit Datenschutzverletzungen zu informieren.
- Wir nahmen an der Messe it-sa mit einem Standauftritt teil und verteilten dort Informationsmaterialien und Flyer, um Betriebe über die Gesetzesänderung zur Meldepflicht zu unterrichten.
- Wir beantragten mehr Planstellen im bayerischen Haushalt, um auf mittelfristige Sicht die Flut an Vorgängen bewältigen zu können.
- Wir erweiterten den Online-Melde-Service auf unserer Website, um den Verantwortlichen die Meldung von Datenschutzverletzungen nach DS-GVO zu erleichtern. Mittlerweile gehen über drei Viertel der Meldungen bei uns über diesen Service ein.

Trotz aller Vorbereitungen trat dann doch ein, was eintreten musste: Die Zahl der Meldungen zu Datenschutzverletzungen explodierte förmlich durch die DS-GVO. Insgesamt 2471 Meldungen gingen im Jahr 2018 ein – sage und schreibe 2376 davon seit dem 25. Mai 2018. Dies ist ein absoluter Rekordwert in unserer Geschichte als bayerische Aufsichtsbehörde.



Die Prognose für 2019 und 2020 verrät bereits, dass die bisherigen Zahlen wohl noch getoppt werden – das liegt an der weiterhin hohen Anzahl eingehender Meldungen. An manchen Tagen erreichen uns bereits über 30 Vorfälle – von Cyberattacken auf bayerische Unternehmen, verschlüsselte Rechner in Arztpraxen bis hin zu fehlversendeten Versicherungsschreiben.

Die neue Meldevorschrift aus Art. 33 DS-GVO zeigt also tatsächlich Wirkung, auch wenn gerade kleineren Unternehmen die Meldeverpflichtung und der Ablauf der Meldung sicher immer noch nicht geläufig sein dürften. Weitere Informationen zu Datenschutzverletzungen und ausgewählten Fallkonstellationen sind im Kapitel 21 dieses Berichts zu finden.

2.4 Abhilfemaßnahmen

Die genannte Arbeitsgruppe hat für diesen Abschnitt vorgeschlagen, die Abhilfemaßnahmen nach Art. 58 Abs. 2 DS-GVO aufzulisten. Im Einzelnen handelt es sich dabei um folgende Maßnahmen:

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

Im Berichtszeitraum, bei dem die DS-GVO ja nur sieben Monate von den insgesamt 24 Monaten angewendet wurde, haben wir noch keine Warnungen, Verwarnungen, Geldbußen und Widerruf von Zertifizierungen erlassen.

Anweisungen und Anordnungen haben wir dagegen schon in manchen Fällen erlassen, die aber bislang noch nicht so erfasst worden sind, dass wir dazu konkrete Zahlen für diese Statistik angeben könnten.

Wir werden deshalb durch die Erweiterung unserer Verwaltungssoftware voraussichtlich im Rahmen des folgenden Tätigkeitsberichts Angaben dazu liefern können.

2.5 Europäische Verfahren

Die genannte Arbeitsgruppe hat für diesen Abschnitt vorgeschlagen, die Anzahl der Verfahren zur Feststellung der Betroffenheit (Art. 56 DS-GVO), der Federführung (Art. 56 DS-GVO) und Anzahl der Verfahren gemäß Kapitel VII DS-GVO (Zusammenarbeit und Kohärenz) aufzulisten.

Um feststellen zu können, ob wir uns bei Verfahren, die in das IMI-System eingestellt sind, als federführende oder betroffene Aufsichtsbehörde melden sollen, war es erforderlich, alle (in englischer Sprache beschriebenen) Vorgänge, die in diesem System eingestellt sind, zu sichten:

Identifizierung der federführenden Aufsichtsbehörde (Art. 56 DS-GVO)	
BayLDA **betroffen** i. S. d. Art. 4 Nr. 22 DS-GVO	193
BayLDA **nicht betroffen** i. S. d Art. 4 Nr. 22 DS-GVO	200
BayLDA **federführende** Aufsichtsbehörde i. S. d. Art. 56 Abs. 1 DS-GVO	3
Bislang noch nicht bearbeitete Fälle	184
Interne Konsultationen	43
Informelle Konsultationen (Art. 60 DS-GVO)	13
Freiwillige Amtshilfeverfahren (Art. 61 DS-GVO)	2
Entscheidungsentwürfe (Art. 60 DS-GVO)	14

Insgesamt 652 Verfahren

Praktisch bedeuten diese Zahlen, dass bei der derzeitigen Nutzung des IMI-Systems eine Person von uns ganztags damit beschäftigt war und ist, zu sichten, ob und in welcher Art und Weise wir betroffen sind und dies entsprechend zu melden.

Dazu kommen die bislang noch nicht detailliert erfassten Fälle, in denen bei uns Beschwerden mit grenzüberschreitender Bedeutung eingereicht wurden, die wir dann (noch) auf Englisch übersetzen und in dieses System eingeben müssen. Es handelt sich auch hierbei um eine nicht geringe Anzahl, über die wir dann sicher im nächsten Tätigkeitsbericht näher berichten können. Unsere Erfahrung mit dem IMI-System zeigt, dass es sich um ein gutes und notwendiges System handelt, um die grenzüberschreitende Zusammenarbeit effektiv zu ermöglichen. Da das Vorhaben derzeit noch am Anfang steht ist davon auszugehen, dass die Zahl der in Zukunft zu beobachtenden und einzustellenden Verfahren (und damit leider auch der Personalaufwand bei uns) dafür deutlich steigen werden.

2.6 Förmliche Begleitung von Rechtsetzungsvorhaben

Die Arbeitsgruppe hat für diesen Abschnitt Folgendes vorgeschlagen:

„Hier werden pauschaliert als eine Gesamtzahl die von Parlament/Regierung angeforderten und durchgeführten Beratungen genannt. Dies soll auch die Teilnahme an öffentlichen Ausschüssen und Stellungnahmen gegenüber Gerichten umfassen."

Diese Arbeitsbereiche wurden mit unserem internen Verwaltungsprogramm noch nicht so erfasst, dass wir sie bereits statistisch auswerten konnten. Wir beabsichtigen daher die Software insoweit fortzuschreiben bzw. anzupassen, dass im nächsten Tätigkeitsbericht – der ja bereits im Frühjahr 2020 erscheinen soll – detaillierte Angaben dazu gemacht werden können.

2.7 Ressourcen

Die genannte Arbeitsgruppe hat für diesen Abschnitt Folgendes vorgeschlagen:

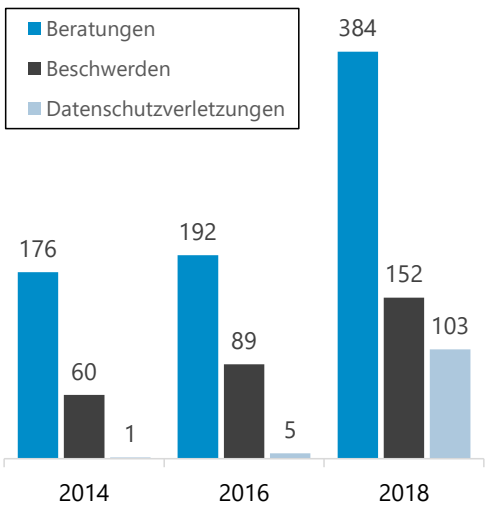
„Hier wird als Freitext in der jeweils geeigneten Form (z. B. orientiert an den Haushaltsplänen) eine Darstellung der Personalsituation in VZÄ gegeben. Wenn möglich, sollte ausgewiesen werden, wie viele VZÄ sich auf DSB, IFG, Presse- und Öffentlichkeitsarbeit und Verwaltung verteilen."

Wir möchten an dieser Stelle die Entwicklung unserer personellen Ausstattung aufzeigen. Im Berichtszeitraum haben wir zwingend erforderliche, neue Planstellen erhalten und damit auch neue Mitarbeiter für unsere Aufgaben gewinnen können. Die Entwicklung sieht wie folgt aus:

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

Um zu verdeutlichen, dass trotz dieses Personalzugewinns das Verhältnis zu den zu bewältigenden Aufgaben dramatisch schlechter wurde und noch immer zunehmender schlechter wird (und wir daher künftig weitere Stellen benötigen), haben wir in der nachfolgenden Grafik das Verhältnis Anzahl der Planstellen zu Anzahl der Vorgänge dargestellt.

Durchschnittliche Vorgänge pro Planstelle



Um uns zumindest etwas zu entlasten, haben wir mit der Regierung von Mittelfranken einen Verbundvertrag abgeschlossen, der zur Folge hat, dass sich die Regierung dankenswerterweise um einige zentrale Dienste wie den Postumlauf und Postversand oder die verwaltungsmäßige Erledigung von Personal- und Haushaltsentscheidungen für uns kümmert. Damit verfolgen wir das Ziel, dass sich unsere eigenen Mitarbeiter mehr dem Datenschutz als der Organisation unseres Landesamts widmen können. Dennoch bindet die (Selbst-)Verwaltung unserer Behörde nicht ganz unwesentliche Anteile unserer eigenen Arbeitszeit, was bei der dünnen Personaldecke durchaus als anstrengend bezeichnet werden darf.

2.8 Vorträge und Öffentlichkeitsarbeit

Die genannte Arbeitsgruppe hat für die Öffentlichkeitsarbeit kein einheitliches Schema erarbeitet. Wir möchten aber an dieser Stelle wie in den vergangenen Berichten kurz darüber berichten, welche Vortragsschwerpunkte wir zuletzt setzten.

Vorträge im Sinne einer Sensibilisierung oder auch Gruppenberatung waren uns auch in diesem Berichtszeitraum ein Hauptanliegen. In den meisten Fällen handelte sich dabei um Veranstaltungen, an denen überwiegend Datenschutzbeauftragte teilnahmen, denen wir dabei unsere Rechtsauffassung nahebringen und erläutern konnten. Ein besonderes Anliegen war es uns wieder, die überwiegend 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, Frankreich, Großbritannien und Liechtenstein Vorträge gehalten.

Den Höhepunkt unserer Vortragsveranstaltungen stellten zweifellos die in den Monaten Juli bis Oktober 2018 zahlreich angebotenen Informationsveranstaltungen für Vereine und ehrenamtlich Tätige dar. Es war durchaus beeindruckend, wenn an heißen Sommerabenden Turnhallen mit bis zu 500 Menschen gefüllt waren, die wissen wollten, welche Anforderungen die DS-GVO an Vereine stellt. Der von den Veranstaltern vorgesehene Zeitrahmen von 90 Minuten wurde regelmäßig um das Doppelte überschritten, um zumindest die allermeisten Fragen zu beantworten. Diese Veranstaltungen, die enorm viel Aufwand für uns bedeuteten, waren dennoch auch ein schönes Erlebnis, da wir in den allermeisten Fällen die Besucher beruhigt nach Hause schicken konnten und sie das, was wir ihnen als notwendige Maßnahmen mit auf den Weg gaben, als nachvollziehbar und verständlich bezeichneten.

Insgesamt hielten wir in beiden Jahren wieder jeweils über 100 Vorträge, um Teilnehmer aus unterschiedlichen Branchen über Datenschutz zu informieren: 2017 waren es 103 Vorträge, 2018 auf Grund der Veranstaltungsreihe für Vereine sogar 137.

Im Rahmen unserer Öffentlichkeitsarbeit erweiterten wir ergänzend unser Angebot auf unserer Website, damit Interessierte einfach und schnell Antworten auf ihre Fragen finden konnten. Dabei war es uns ein besonderes Anliegen, 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

Europäische Zusammenarbeit

3 Europäische Zusammenarbeit

3.1 Verfahren der Zusammenarbeit und Kohärenz

Die Datenschutz-Grundverordnung verpflichtet die europäischen Datenschutzaufsichtsbehörden im Sinne eines europaweit einheitlichen Gesetzesvollzuges zusammenzuarbeiten (Art. 57 Abs. 1 Buchstabe g DS-GVO).

Diese Verpflichtung hat unter anderem zur Folge, dass die Bearbeitung von Beschwerden und anderen Eingaben, denen eine grenzüberschreitende Verarbeitung personenbezogener Daten im Sinne des Art. 4 Nr. 23 DS-GVO zu Grunde liegt, im Rahmen eines Verfahrens der Zusammenarbeit und Kohärenz gemäß den Art. 60 ff. DS-GVO zu erfolgen hat.

Praktisch findet diese Zusammenarbeit der europäischen Datenschutzaufsichtsbehörden seit Mai 2018 über das sog. Internal Market Information System (kurz: IMI-System, zu Deutsch: Binnenmarktinformationssystem) statt. Es handelt sich dabei um ein bereits existierendes System für die europäische Zusammenarbeit von Behörden in anderen Kontexten, das mittlerweile für die Datenschutzaufsichtsbehörden um einen eigenen Bereich erweitert bzw. angepasst wurde.

Alle bei den europäischen Aufsichtsbehörden eingehenden Eingaben werden zunächst dahin gehend geprüft, ob eine grenzüberschreitende Verarbeitung im o. g. Sinne vorliegt. Wenn dem so ist, wird die jeweilige Beschwerde zunächst zum Zwecke der Identifizierung der federführenden Aufsichtsbehörde über das IMI-System den anderen europäischen Aufsichtsbehörden übermittelt. Umgekehrt erhält jede europäische Aufsichtsbehörde seit Mai 2018 täglich eine Vielzahl an Benachrichtigungen des IMI-Systems mit der Information, dass solche Identifizierungsverfahren von anderen europäischen Aufsichtsbehörden über das IMI-System angestoßen wurden. Daraufhin ist zu prüfen, ob wir für die zu Grunde liegenden Eingaben betroffene (vgl. Art. 4 Nr. 22 DS-GVO) oder gar federführende Aufsichtsbehörde im Sinne des Art. 56 Abs. 1 DS-GVO sind und uns entsprechend zurückmelden müssen.

Erst wenn klar ist, welche Aufsichtsbehörde die Federführung innehat, kann das eigentliche Verfahren nach den Art. 60 ff. DS-GVO angestoßen werden. Die federführende Aufsichtsbehörde prüft den Vorgang und entwirft eine Entscheidung. Diese muss den betroffenen Aufsichtsbehörden vorgelegt werden (vgl. Art. 60 Abs. 3 Satz 2 DS-GVO), was ebenfalls über das IMI-System erfolgt. Anschließend kann dann von den betroffenen Aufsichtsbehörden ein maßgeblicher und begründeter Einspruch gegen diesen Entscheidungsentwurf eingelegt werden (Art. 60 Abs. 4 DS-GVO). Sollte es den Aufsichtsbehörden daraufhin nicht möglich sein, sich auf einen Standpunkt zu einigen, so leitet die federführende Aufsichtsbehörde ein Kohärenzverfahren nach den Art. 63 ff. DS-GVO ein, das, wenn zwischendurch keine Einigung erfolgt, durch einen Mehrheitsbeschluss des Europäischen Datenschutzausschusses abgeschlossen und dann von der federführenden Aufsichtsbehörde so zu vollziehen ist.

Das IMI-System bietet auch die Möglichkeit, Anfragen an andere europäische Datenschutzaufsichtsbehörden bzgl. gegenseitiger Amtshilfe (Art. 61 DS-GVO) oder zur Durchführung gemeinsamer Maßnahmen (nach Art. 62 DS-GVO) zu stellen.

Eine praktische Herausforderung, die sich im Rahmen der Zusammenarbeit über das IMI-System stellt, ist die Tatsache, dass man sich unter den europäischen Aufsichtsbehörden geeinigt hat, dass die Arbeitssprache für diese IMI-Verfahren Englisch ist. Das bedeutet für uns wie auch für (fast) alle anderen Aufsichtsbehörden,

dass wir sämtliche Unterlagen, die für die Bearbeitung einer Eingabe entscheidungserheblich sind, zunächst übersetzen müssen. Dies ist meist ein sehr zeitintensives Unterfangen und womöglich auch eine Erklärung dafür, dass bislang in das IMI-System zwar eine Vielzahl von Verfahren zur Identifizierung der federführenden Aufsichtsbehörden (Art. 56 Abs. 1 DS-GVO) eingestellt wurden, gleichzeitig aber verhältnismäßig wenige Entscheidungsentwürfe oder gar finale Entscheidungen vorliegen. Zu einer Streitbeilegung durch den Ausschuss (Art. 65 DS-GVO) ist es bis dato noch kein einziges Mal gekommen.

Für die europäischen Datenschutzaufsichtsbehörden ist diese Art der Zusammenarbeit absolutes Neuland und es bleibt abzuwarten, wie sich die Bearbeitung von grenzüberschreitenden Sachverhalten mit bzw. über das IMI-System und damit der einheitliche Vollzug des europäischen Datenschutzrechts in der Zukunft entwickelt.

Weitere Informationen zum Begriff der federführenden Aufsichtsbehörde finden Sie in den Leitlinien des Europäischen Datenschutzausschusses unter folgendem Link:

edpb.europa.eu/our-work-tools/our-documents/guideline/lead-supervisory-authority_en

3.2 Mitwirkung in Subgroups des EDSA

Der Europäische Datenschutzausschuss (EDSA) dient der Sicherstellung einer europaweit einheitlichen Anwendung der Datenschutz-Grundverordnung (vgl. Art. 70 Abs. 1 Satz 1 DS-GVO). Er besteht aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaates und dem Europäischen Datenschutzbeauftragten oder ihren jeweiligen Vertretern (Art. 68 Abs. 3 DS-GVO).

In der Geschäftsordnung des EDSA (vgl. Art. 72 Abs. 2 DS-GVO) ist vorgesehen, dass der Ausschuss Unterarbeitsgruppen (englisch: Expert Subgroups) einsetzt, die ihn bei der Erfüllung seiner Aufgaben unterstützen sollen (Art. 25 Abs. 1 der Geschäftsordnung des EDSA). Eine ähnliche Organisation und Arbeitsweise war auch für das Vorgängergremium des EDSA, die Artikel-29-Datenschutzgruppe, unter der Datenschutzrichtlinie etabliert. Die Struktur der Unterarbeitsgruppen wurde unter dem Regime der DS-GVO weitestgehend übernommen – lediglich kleinere Änderungen wurden durchgeführt. So gibt es bspw. nun eine IT Users Subgroup, die sich insbesondere mit den technischen Fragen rund um das IMI-System beschäftigt.

Die wichtigsten Aufgaben des EDSA sind die Erarbeitung gemeinsamer Positionen der Aufsichtsbehörden der EU-Mitgliedstaaten zur Interpretation der DS-GVO, z. B. in der Form von Leitlinien und Empfehlungen, sowie bei Bedarf die verbindliche Entscheidung von Einzelfällen, für die Aufsichtsbehörden aus mehreren Mitgliedstaaten zuständig sind.

Die Vertretung der deutschen Datenschutzaufsichtsbehörden in diesen Unterarbeitsgruppen erfolgt, wie auch zuletzt im Rahmen der Art. 29-Gruppe, immer durch eine Vertreterin bzw. einen Vertreter des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) sowie eine Vertreterin bzw. einen Vertreter einer Aufsichtsbehörde eines Landes und einer stellvertretenden Landesvertreterin bzw. eines stellvertretenden Landesvertreters. Hierbei sollen die von der DSK ernannten Vertreterinnen und Vertreter Deutschland als Ganzes repräsentieren und nicht (nur) die eigene Behörde.

Im Berichtszeitraum stellten wir den Landesvertreter in der International Transfer Expert Subgroup sowie eine stellvertretende Landesvertreterin für die Cooperation Expert Subgroup. Die Vertretung werden wir bis auf Weiteres auch aufrechterhalten. Auf diese Weise ist es uns möglich, an der Erstellung von Leitlinien, Empfehlungen und anderen Papieren des EDSA

direkt mitzuarbeiten und die maßgeblichen Entscheidungen auf europäischer Ebene unmittelbar mitzugestalten.

Wir haben zudem in den vergangenen zwei Jahren in den Unterarbeitsgruppen für eine Reihe von Papieren (Leitlinien, interne Arbeitsanweisungen etc.) die sog. Berichterstattung übernommen. Dies beinhaltet insbesondere die Erstellung von Entwürfen und die Koordinierung des Erarbeitungsprozesses sowie die Präsentation der finalen Version vor dem Plenum des EDSA. Daran kann sich sodann auch die Überarbeitung der Papiere nach einer ggf. stattgefundenen öffentlichen Konsultation anschließen.

Auch im Rahmen solcher Unterarbeitsgruppen, für die wir keine förmliche Vertretung innehatten, versuchen wir stets, uns an den Arbeiten zu beteiligen, um so auf die Positionierung der Aufsichtsbehörden zu den von der DS-GVO aufgeworfenen Fragen auf europäischer Ebene Einfluss zu nehmen. Dies geschieht vorrangig durch eine Beteiligung an der innerdeutschen Meinungsbildung zu den angestoßenen Diskussionen und Beiträgen zu Leitlinien und anderen Entwürfen.

Der Austausch mit den anderen europäischen Datenschutzaufsichtsbehörden zu rechtlichen Auslegungsfragen, aber auch praktischen Fragen der Durchführung der DS-GVO, wird nicht nur als sehr hilfreich empfunden, sondern von uns auch als gesetzliche Pflichtaufgabe verstanden.

Da die europäische Zusammenarbeit unter der DS-GVO darüber hinaus einen noch deutlich größeren Stellenwert bekommen hat, als dies schon bisher der Fall war, wird die Beteiligung an den Arbeiten der Expert Subgroups auch in Zukunft einen wichtigen Teil unserer Tätigkeit bilden.

Die Geschäftsordnung des Europäischen Datenschutzausschusses ist auf dessen Homepage unter folgendem Link zu finden:

edpb.europa.eu/node/59

Eine Übersicht über die Unterarbeitsgruppen des EDSA (Expert Subgroups) und den jeweiligen deutschen Vertretungen ist auf der Homepage der Datenschutzkonferenz (DSK) unter folgendem Link abrufbar:

www.datenschutzkonferenz-online.de/media/misc/subgroups.pdf

4

Kontrollen und Prüfungen

4 Kontrollen und Prüfungen

4.1 Videoüberwachung in Gastronomie und Kinos

Anlass und Ziel der Prüfung

Gastronomiebetriebe und Kinos sind bekanntermaßen Orte, an denen sich viele Menschen in ihrer Freizeit aufhalten. Gäste wollen sich dort typischerweise ungezwungen verhalten können. Es besteht daher eine gesteigerte Erwartungshaltung der Gäste dahin gehend, nicht Gegenstand von Überwachungsmaßnahmen zu sein. Gleichzeitig ist auch in diesen Branchen ein verstärkter Einsatz von Videoüberwachungstechnik zu beobachten. Als Zweck der Überwachung geben Unternehmen in aller Regel die Straftatprävention und erleichterte Straftatenaufklärung an. Daneben wird häufig der Kassenbereich überwacht, sodass auch Mitarbeiter von der Videoüberwachung betroffen sind.

Im Rahmen einer schriftlichen Prüfungsaktion haben wir die Videoüberwachungsmaßnahmen von 25 Unternehmen überprüft, davon 19 Gaststätten und 6 Kinos (die jedoch neben dem reinen Kinobetrieb auch noch Gaststättenbereiche betreiben). Auf der Basis der eingegangenen Antworten haben wir schließlich noch Vor-Ort-Prüfungen bei fünf Gaststätten und drei Kinobetrieben durchgeführt.

Prüffragen

Folgende Fragen waren Schwerpunkt der Prüfung:

- Wie viele Videokameras sind in dem Unternehmen installiert?
- Welche Bereiche werden von den Videokameras erfasst?
- Welche Zwecke werden durch die Videoüberwachung verfolgt?
- Haben die Kameras Zoom-, Schwenk- und/oder Neigetechnik?
- Werden Aufzeichnungen angefertigt und wenn ja,
  - wie lange werden diese gespeichert,
  - wer hat Zugang zu den Aufzeichnungen und
  - an welche Stellen werden diese ggf. weitergegeben?
- Wie wird auf die Videoüberwachung hingewiesen?

Zeitraum

Beginn: Oktober 2017
Abschluss: Februar 2018

Anzahl geprüfte Verantwortliche

25 Unternehmen, davon 19 Gaststätten und sechs Kinos mit Gaststättenbereichen.

Ergebnis

13 der Unternehmen gaben an, keine Videoüberwachung zu betreiben. Zwölf Unternehmen betrieben dagegen in mehr oder weniger großem Umfang Videokameras, die meisten davon auch während der Geschäftszeiten. Bei fünf der geprüften Unternehmen befanden sich Sitzbereiche der Gäste (Cafétische, Barhocker, Sitzecken in Foyers oder Gängen im Kinogebäude) zumindest teilweise im Blickfeld von Kameras – und zwar auch während der Öffnungszeiten. In diesen Fällen haben wir die Beendigung der Überwachung verlangt, da das Interesse der Gäste am Unterbleiben der Überwachung in diesen Bereichen eindeutig überwiegt.

In vier Fällen erfassten Videokameras auch Bereiche, in denen sich Mitarbeiter einen großen Teil der Zeit über aufhalten (Schank-/Thekenbereich sowie, in einem Fall, die Restaurantküche). In diesen Fällen haben wir die Unternehmen aufgefordert, die Überwachung zu beenden oder alternativ die Kameras so auszurichten,

dass die Arbeitsplätze nicht mehr erfasst werden. Als akzeptabel sahen wir es an, wenn nur der unmittelbare Kassenbereich – ohne komplette Erfassung des Mitarbeiters – von der Kamera erfasst wird, wobei als Überwachungszweck unternehmensseitig in diesen Fällen in der Regel die Verhinderung bzw. Aufdeckung von Wechselgeldbetrug angegeben wird.

Alle zwölf schriftlich geprüften Unternehmen wiesen mittels Hinweisschildern auf die Videoüberwachung hin, allerdings nicht immer in einer ausreichend deutlichen Weise (z. T. fehlte die Bezeichnung des Verantwortlichen – stattdessen wurde fälschlicherweise die Firma angegeben, die die Kameratechnik geliefert hatte).

Besonders bemerkenswert war, dass eines der kinobetreibenden Unternehmen in seinen Kinosälen Videokameras betrieb, die auf die Zuschauersitze gerichtet waren; hier erfolgte zwar keine Aufzeichnung, sondern lediglich ein „Monitoring" der Sitzplätze während der ersten Minuten einer Vorführung. Als Zweck gab der Betreiber an, auf diese Weise zu überprüfen, ob mehr Sitzplätze in einer Vorstellung belegt sind als Karten verkauft wurden; auf diese Weise konnte sich der Betreiber Eingangskontrollen zu den einzelnen Kinosälen sparen. Zwar war die Bildqualität verhältnismäßig schwach, sodass die Personen auf den Monitoren in den allermeisten Fällen nicht identifizierbar waren, ferner wurden die Stellen in Kopfhöhe durch Balken verpixelt. Dennoch haben wir diese Überwachung als unzulässig bewertet, da Gäste einer Kinovorführung aufgrund des Freizeitcharakters eine berechtigte Erwartung haben, nicht per Videoüberwachung über mehrere Minuten beobachtet zu werden. Die Maßnahme kann im Hinblick auf die Eingriffsintensität auch nicht als erforderlich angesehen werden, da es für den Betreiber auch andere zumutbare Möglichkeiten gibt, die Erschleichung von Kinovorführungen zu unterbinden – etwa durch Eingangskontrollen oder evtl. durch Lichtschranken oder ähnliche am Markt erhältliche Systeme, mit denen die Belegung von Kinosesseln festgestellt werden kann. Der Betreiber hat die Videobeobachtung seiner Kinosäle umgehend eingestellt.

Als akzeptabel haben wir bei Betreibern großer Kinos in der Regel die Videoüberwachung in Eingangsbereichen, Durchgängen und Foyers angesehen. Dabei forderten wir die Unternehmen auf, die Erforderlichkeit der Maßnahme in der Folgezeit näher zu belegen und zu diesem Zweck für bestimmte Zeiträume die Anzahl und Art an sicherheitsrelevanten Vorgängen in den überwachten Bereichen (insb. etwaige Auseinandersetzungen, ggf. Diebstähle) zu dokumentieren. Auf dieser Grundlage sollte in regelmäßigen Abständen geprüft und uns anhand der Dokumentation nachgewiesen werden, inwieweit in den betreffenden Bereichen tatsächlich eine erhöhte Anzahl derartiger Vorfälle zu beobachten ist.

Vorgefundene Mängelbereiche

- Videoüberwachung von Sitzbereichen/ Gastbereichen: 5 von 25
- Videoüberwachung von permanenten Arbeitsplätzen (Schankbereich, Küche): 4 von 25
- Videoüberwachung in Kinosälen: 1 von 6
- Kein Auftragsverarbeitungsvertrag mit Dienstleister: 1 von 25

4.2 Kfz-Werkstätten-Kontrolle

Anlass und Ziel der Prüfung

Moderne Kraftfahrzeuge generieren immer mehr Daten. Viele davon werden in der Werkstatt für die Inspektion oder die Reparatur benötigt, aber dabei zum Teil an die Kfz-Hersteller übermittelt. Auch auf den ersten Blick rein technische Daten können personenbezogene Daten sein, wenn sie bspw. mit der Fahrgestellnummer oder den Kundendaten verknüpft werden.

Wir wollten daher durch eine schriftliche Prüfung die Verarbeitung von Fahrzeugdaten in Kfz-Werkstätten nachvollziehen und auf die datenschutzrechtliche Relevanz und Vereinbarkeit untersuchen.

Prüffragen

Nachfolgend ein Auszug aus den Prüffragen:

- Welche Daten werden bei einem Werkstattbesuch (z. B. bei Wartung, Reparatur, Unfall) aus dem Fahrzeug erhoben und in den Systemen der Werkstatt gespeichert?
- Auf welcher Rechtsgrundlage werden die Daten verarbeitet?
- Für welchen Zeitraum erfolgt eine Speicherung dieser Daten?
- Wird der Kunde von der Speicherung in Kenntnis gesetzt und wenn ja, wie?
- Werden Fahrzeugdaten an den Hersteller oder sonstige Externe weitergeleitet?
- Falls ja: Zu welchem Zweck werden Daten weitergeleitet (Produktbeobachtung, Produktoptimierung, Bearbeitung von Garantiefällen usw.)?

Zeitraum

Beginn: Juni 2017
Abschluss: Oktober 2017

Anzahl geprüfte Verantwortliche

12

Ergebnis

Das Ergebnis zeigte, dass einige Werkstätten unzureichende Einwilligungen für eine Datenverarbeitung verwendeten. Es muss aus einer solchen Einwilligung ersichtlich sein, welche Daten zu welchem Zweck erhoben und verarbeitet werden sowie wer diese Daten noch erhält.

Auch die Information der Kunden war teilweise unzureichend. Zwar wurde die DS-GVO zum Zeitpunkt der Prüfung noch nicht angewandt, jedoch waren deren Anforderungen bereits längst bekannt. Die DS-GVO schreibt vor, dass ein Kunde in präziser, transparenter, verständlicher und leicht zugänglicher Art und Weise über die Verarbeitung seiner Daten zu informieren ist. Die Werkstätten gaben an, dass Informationen zur Datenverarbeitung entweder in den Betriebsanleitungen oder in den Einwilligungserklärungen vorhanden seien bzw. die Kunden durch Servicemitarbeiter aufgeklärt werden. Hier ist es notwendig, ein Informationsblatt für die Kunden mit dem gesetzlich vorgesehenen Inhalt vorzuhalten, den Kunden mitzugeben oder auf den Werkstatt-Auftrag mit aufzudrucken.

Die zentrale Führung einer elektronischen Service- und Reparaturhistorie beim Automobilhersteller (digitaler Servicenachweis) ist nur aufgrund einer vertraglichen Vereinbarung mit dem Halter oder mit expliziter Einwilligung des Halters zulässig, was nicht überall so praktiziert wurde. Gleiches gilt für die Teilnahme an Vergütungs- und Bonusprogrammen.

Zusammen mit den Verbänden der Kfz-Werkstätten und der Automobilindustrie sollen hierzu in weiteren Gesprächen einheitliche Verfahrensweisen abgestimmt werden, die den datenschutzrechtlichen Anforderungen der DS-GVO genügen.

4.3 Patch Management bei WordPress-Websites

Anlass und Ziel der Prüfung

Nahezu täglich erfährt man aus den Medien von einer Sicherheitslücke bei einem IT-System. Mal ist ein Smartphone unsicher, mal findet man neue Schwachstellen bei Servern. Besonders häufig wird jedoch über gehackte Websites berichtet, die auf Grund einer nicht aktuell gehaltenen Softwareversion angreifbar waren oder sogar noch sind. Wir suchten uns daher als Prüfungsgegenstand den sicheren Einsatz sog. Content Management Systeme (CMS) aus. Mit

diesen Systemen lässt sich der Inhalt von Webseiten oft sehr einfach erstellen, bearbeiten und verwalten. Viele der weitverbreiteten CMS, die meist als Open-Source kostenfrei genutzt werden können, verfügen jedoch über Sicherheitslücken, die je nach Grad der Ausprägung als kritisch einzustufen sind und dadurch den Schutz personenbezogener Daten gefährden. Aus diesem Grund ist es notwendig, durch gezieltes Patch Management vorhandene Lücken zu schließen und die vom Hersteller bereitgestellten, neuesten Versionen einzuspielen, um so den vielfältigen Angriffsmöglichkeiten von Cyberkriminellen präventiv entgegenzutreten. Im Rahmen unserer Prüfung wurde bei ausgewählten Websites evaluiert, ob das eingesetzte CMS "WordPress" eingesetzt wird und hinsichtlich der eingespielten Patches aktuell gehalten ist.

Prüfpunkte

- Version der eingesetzten WordPress-Installation
- Version der eingesetzten WordPress-Plugins
- HTTPS-Implementierung

Zeitraum

Beginn: Februar 2018
Abschluss: August 2018

Anzahl geprüfte Verantwortliche

172 Websites

Ergebnis

Wir mussten feststellen, dass von 172 Websites nur ein Bruchteil WordPress als CMS einsetzten. 18 Verantwortliche nutzten die Software. Alle davon wurden angeschrieben und mit unserem Prüfergebnis konfrontiert, da bei allen Mängeln vorhanden waren. Entweder war die WordPress-Version veraltet, manche Plugins potentiell unsicher oder der Webauftritt hatte keine oder nur unzureichende HTTPS-Verschlüsselung. Besonders erschreckend war, dass sich darunter auch Websites von Verantwortlichen befanden, die auf Grund ihrer beruflichen, herausragenden Position im besonderen Fokus von Cyberkriminellen stehen.

Vier von den 18 Websites hatten jeweils eine stark veraltete WordPress-Version im Einsatz, die sich nicht nur durch zahlreiche längst bekannte Sicherheitslücken auszeichnete, sondern für die auch im Internet öffentlich Anleitungen zum Ausnutzen der Lücken vorzufinden waren.

Sechs von den 18 Websites hatten überhaupt kein SSL-Zertifikat (für HTTPS). Zum Teil konnte sogar der Admin-Bereich unverschlüsselt öffentlich aufgerufen werden konnte. Wenn dann dieser Login für den Admin-Bereich nicht vor klassischen Login-Attacken geschützt ist, wäre es verwunderlich, wenn Cyberkriminelle die Website nicht kapern.

Auf unser Hinwirken wurden die vorgefundenen Mängel abgestellt. Allerdings zeigte eine bislang nicht öffentlich gemachte stichprobenartige Nachprüfung Ende 2018, dass es einzelne Verantwortliche gab, die zwar wegen unser Prüfung im August 2018 auf die sicherste WordPress-Version umgestiegen sind, anschließend (nach Abschluss unserer Prüfung) dann trotz neuer Sicherheitslücken keine Patches mehr durchgeführt haben. Wir prüfen daher, wie die unbelehrbaren Websitebetreiber bei solchen Vorkommnissen nicht mehr nur durch umfassende Prüf- und Informationsschreiben zu kontaktieren sind, sondern ob und wie wegen Verstößen gegen die Sicherheit der Verarbeitung nach Art. 32 DS-GVO auch direkt Bußgeldverfahren einzuleiten sind.

Unser Prüfanschreiben, ein umfassende Informationsblatt sowie den Prüfantwortbogen findet man auf unserer Website:

www.lda.bayern.de/de/kontrollen.html

4.4 WordPress GDPR Compliance Plugin

Anlass und Ziel der Prüfung

Anfang November 2018 wurde eine sehr kritische Sicherheitslücke in einer Erweiterung für WordPress-Installationen bekannt. Das Besondere an der Sicherheitslücke war, dass diese im „WP GDPR Compliance" vorhanden war, mit dem Websitebetreiber eigentlich Vorgaben der DS-GVO einhalten wollten. Das Plugin besaß bis einschließlich Version 1.4.2 diese Lücke, durch die die Angreifer die Website ohne größeren Aufwand übernehmen konnten.

Nach dem Bekanntwerden der Sicherheitslücke wurden zahlreiche Websites von den Kriminellen gekapert, um Daten abzuschöpfen und Schadcode auf der Website zu platzieren. Wir haben daher kurzfristig auf diese Gefährdung reagiert und einen automatisierten Prüflauf bei über 1.000 Websites in Bayern gestartet. Dort begutachten wir, ob WordPress mit dem unsicheren Plugin zum Einsatz kommt und schrieben die betroffenen Verantwortlichen an.

Prüffragen

- In welcher Version wird WordPress als CMS für den Betrieb der Website verwendet?
- Kommt das WP GDPR Compliance Plugin zum Einsatz?
- Falls ja, wurde das Plugin bereits aktualisiert (gepatcht)?

Zeitraum

Beginn: November 2018
Abschluss: Dezember 2018

Anzahl geprüfte Verantwortliche

23 (von über 1.000 automatisiert gescannten Websites)

Ergebnis

Die Prüfung zeigte, dass verhältnismäßig wenige WordPress-Websites in Bayern dieses Plugin einsetzten. Einige davon waren sich über die bestehende Sicherheitslücke nicht im Klaren. Durch unser Hinwirken konnte auf den besagten Websites nicht nur die Sicherheitslücke durch Aktualisieren oder Entfernen des Plugins geschlossen werden, sondern Websitebetreiber auch dahin gehend sensibilisiert werden, welche Verantwortung sie hinsichtlich zu ergreifender Schutzmaßnahmen besitzen.

Alle Prüfinformationen hierzu sind auf unserer Website zu finden:

www.lda.bayern.de/de/kontrollen.html

4.5 Patch Management bei Magento-Websites

Anlass und Ziel der Prüfung

Die bei uns eingehenden Meldungen von Datenschutzverletzungen zeigen, dass die Gefährdungslage bei Online-Shops besonders hoch ist. Veraltete Shop-Systeme weisen oftmals Schwachstellen auf, die Cyberkriminelle gezielt ausnutzen können.

Wir entschlossen uns deshalb, gezielt Online-Shops datenschutzrechtlich zu kontrollieren. Dabei konzentrierten wir uns auf die weit verbreitete Shop-Software Magento und untersuchten deren Installationen dahin gehend, ob alle verfügbaren, wichtigen Sicherheitspatches eingespielt und bekannte kritische Schwachstellen behoben wurden. Des Weiteren wurde überprüft, ob die verantwortlichen Websitebetreiber über einen geregelten Prozess zum Patch Management verfügten sowie die datenschutzrechtlichen Verpflichtungen im Umgang mit Sicherheitsverletzungen im Bedarfsfall umsetzen konnten (Incident Response).

Prüffragen

- Kommt HTTPS in ausreichender Konfiguration zum Einsatz?

- Wird eine aktuelle Magento-Version eingesetzt?
- Wird die Magento-Installation regelmäßig hinsichtlich Updates untersucht?
- Sind alle relevanten Sicherheitspatches installiert?
- Sind sicherheitskritische Verzeichnisse des Webservers öffentlich abrufbar?
- Besteht ein ausreichender Schutz vor Malware und anderen Angriffsarten?
- Besteht ein geregelter Prozess zum Patch Management?

Zeitraum

Beginn: Oktober 2018
Abschluss: Dezember 2018

Anzahl geprüfte Verantwortliche

20 (100 Online-Shops wurden zufällig ausgewählt; 20 von ihnen hatten Magento als Shop-Software aktiv in Verwendung)

Ergebnis

Unsere Prüfung zeigte, dass ein Großteil der Online-Shops über zum Teil gravierende Mängel verfügte. Während die allermeisten Websites zwar mit gängigen HTTPS-Anforderungen kein Problem mehr haben, waren wichtige Sicherheitspatches nicht installiert. In wenigen Fällen gab es Backend-Pfade wie das Administratorenverzeichnis /admin/, die nicht ausreichend geschützt und somit erfolgreich mit bekannten Brute-Force-Versuchen angegriffen werden konnten. Bei den 20 angeschriebenen Online-Shops bestand in 15 Fällen mindestens ein Sicherheitsproblem, das nachgebessert werden musste. Es gab jedoch auch Online-Shops, die vorbildhaft konfiguriert waren, keine offensichtliche Angriffsfläche boten und im Patch Management hochprofessionell agierten.

Umfangreiche Angaben zum Prüfgegenstand sind online abrufbar:

www.lda.bayern.de/de/kontrollen.html

4.6 Informationspflichten bei Bewerbungen

Anlass und Ziel der Prüfung

Unsere Behörde erreichten im Zusammenhang mit dem Umgang personenbezogener Daten im Bewerbungsverfahren zahlreiche Anfragen und Beschwerden. Aus diesem Anlass konzipierten wir eine Prüfungsaktion und richteten diverse Fragen an einige Unternehmen in Bayern. In der schriftlichen Kontrolle forderten wir dabei zudem einige Unterlagen hinsichtlich der Ausgestaltung der Informationspflichten an.

Prüffragen

Nachfolgend stellen wir die Prüfelemente vor:

- Wie kommen Unternehmen als potentielle Arbeitgeber im Bewerbungsverfahren den Informationspflichten gegenüber Bewerbern nach?
- In welchen Fällen werden im Bewerbungsverfahren Rückfragen beim früheren Arbeitgeber gestellt?
- Welche Abteilungen oder Bereiche haben im Unternehmen Zugriff auf die Bewerbungsunterlagen?
- Wie wird sichergestellt, dass die Bewerbungsunterlagen nach Abschluss des Bewerbungsverfahrens in den Abteilungen oder Bereichen wieder gelöscht werden?
- Wann werden die Daten der abgelehnten Bewerber gelöscht?
- Existiert im Verzeichnis der Verarbeitungstätigkeiten ein Eintrag für Bewerbungsverfahren?

Zeitraum

Beginn: Oktober 2018
Abschluss: noch nicht abgeschlossen

Anzahl geprüfte Verantwortliche

15

Ergebnis

Die Prüfung ist noch nicht vollständig abgeschlossen. Es liegen jedoch bereits alle (Erst-) Antworten der Unternehmen vor. Dadurch konnte man zumindest bereits erkennen, dass die Unternehmen bei den abgefragten Aspekten die wesentlichen datenschutzrechtlichen Anforderungen erfüllten. Die Ergebnisse dazu werden auf unserer Website nach Abschluss der Prüfung veröffentlicht.

4.7 DS-GVO-Prüfung bei kleinen und mittleren Unternehmen

Anlass und Ziel der Prüfung

Die DS-GVO verlangt von einem Verantwortlichen, dass die Einhaltung der DS-GVO nachgewiesen wird (Art. 5 Abs. 2 DS-GVO). Diese Rechenschaftspflicht stellt vom Grundsatz her eine "Nachweislast-Umkehr" dar, was bedeutet, dass die Einhaltung der gesetzlichen Anforderungen der Aufsichtsbehörde bei einer Kontrolle dargestellt werden muss. Während dies bei großen Unternehmen in der Regel nur anhand einer systematischen Ausgestaltung der Geschäftsprozesse erreicht werden kann, skaliert die DS-GVO bei kleinen und mittleren Unternehmen recht gut. Die Einhaltung der datenschutzrechtlichen Anforderungen kann deutlich weniger formal erreicht werden. Ziel der Prüfung war daher zu kontrollieren, ob kleine und mittlere Unternehmen die wesentlichen Anforderungen der DS-GVO umsetzen.

Prüffragen

Den kontrollierten Unternehmen wurden in einem schriftlichen Verfahren 20 Fragen gestellt. Nachfolgend ein Auszug daraus:

- Ist ein Datenschutzbeauftragter bestellt und der Aufsichtsbehörde gemeldet?
- Gibt es ein Konzept im Unternehmen, wer bezogen auf den Datenschutz für was zuständig ist?
- Ist ein vollständiges Verarbeitungsverzeichnis vorhanden?
- Existiert ein Löschkonzept?

Zeitraum

Beginn: November 2018
Abschluss: noch nicht abgeschlossen

Anzahl geprüfte Verantwortliche

Insgesamt 15. Sieben Unternehmen davon wurden ausgewählt, zu denen es gehäuft Datenschutzbeschwerden gab. Die anderen acht Unternehmen wurden zufällig ausgewählt.

Vor-Ort-Kontrolle durchgeführt/geplant

Bei 5 von 15

Ergebnis

Die Prüfung ist noch nicht vollständig abgeschlossen. Die Ergebnisse dazu werden auf unserer Website nach Abschluss der Prüfung veröffentlicht.

4.8 Rechenschaftspflicht bei Großkonzernen

Anlass und Ziel der Prüfung

Wie bei der Kontrolle unter Kapitel 4.7 dargestellt, müssen Verantwortliche die Einhaltung der DS-GVO nachweisen können. Wir entschlossen uns daher auch bei Großkonzernen die Einhaltung der Datenschutz-Grundverordnung im Unternehmensalltag zu prüfen.

Prüffragen

Folgende Bereiche standen dabei im Prüffokus:

- Aufbauorganisation
- Ablauforganisation

Bei der Aufbauorganisation wurde die Rolle des Datenschutzes im Organigramm betrachtet. Insbesondere die Rolle des betrieblichen DSB als auch die Rollen der anderen datenschutzrelevanten Akteure im Unternehmen wurden

geprüft, z. B. Informationssicherheit, Rechtsabteilung, interne Revision, Datenschutzkoordinatoren sowie Konzerndatenschutzbeauftragte.

In der Ablauforganisation waren datenschutzrelevante Hauptprozesse im Blickfeld:

- Datenschutzkonforme Verarbeitung
- Sicherstellung der Betroffenenrechte
- Umgang mit Datenschutzverletzungen

Die technischen und organisatorischen Maßnahmen stellen in der Prüfung einen besonderen Schwerpunkt dar.

Zeitraum

Beginn: Oktober 2018
Abschluss: noch nicht abgeschlossen

Anzahl geprüfte Verantwortliche

Insgesamt drei Großkonzerne wurden kontrolliert. Die Auswahl der Unternehmen erfolgte unter der subjektiven Annahme, dass diese die DS-GVO schon bestmöglich umgesetzt haben.

Ergebnis

Die Prüfung ist noch nicht vollständig abgeschlossen. Die Unternehmen reichten jedoch allesamt äußerst umfangreiche Unterlagen ein, sodass eine Auswertung noch etwas Zeit in Anspruch nehmen wird. Nachdem die Unternehmen 2019 einer Vor-Ort-Kontrolle unterzogen worden sind, werden wir die Ergebnisse dieser Prüfung evaluieren, das Prüfschema ggf. anpassen oder erweitern und dadurch unseren Standardprüfbogen für große und datengetriebene Unternehmen festlegen.

4.9 Ransomware bei Arztpraxen

Anlass und Ziel der Prüfung

Ransomware, auch Verschlüsselungstrojaner genannt, war auch in Bayern weiterhin aktiv: Durch die Schadsoftware wird der Zugriff auf Daten gesperrt und anschließend Lösegeld gefordert, um die Daten wieder im ursprünglichen Zustand zu erhalten. Meldungen über einen Befall von Arbeitsplatzrechnern bei bayerischen Verantwortlichen erreichten uns wöchentlich (siehe dazu die näheren Ausführungen in Kapitel 21.8).

Betroffen sind nach den eingehenden Meldungen oft Ärzte und kleinere Betriebe, die sich entweder der Gefährdungslage nicht bewusst waren oder nur über unzureichende Sicherheitsmaßnahmen verfügten. Wir entschieden uns deshalb dafür, Ärzte zum Umgang und zur Prävention von Ransomware-Attacken zu kontrollieren. Ziel der Datenschutzprüfung war es, für ein geeignetes und wirksames Backupverhalten bei Ärzten zu sorgen, damit Patientendaten vor der realen Gefahr solcher Kryptotrojaner angemessen geschützt werden.

Prüffragen

- Werden regelmäßige, automatisierte Backups der Patientendaten durchgeführt?
- Mit welcher Software werden Backups durchgeführt?
- Auf welchen Speichermedien werden die Backups gespeichert?
- Wird das Zurückspielen von Backup-Daten getestet?
- Ist das Praxisverwaltungssystem (PVS) an das Internet angeschlossen?
- Befinden sich an das Internet angeschlossene (Recherche-)Rechner in anderen Netzsegmenten als das Praxisverwaltungssystem?
- Sind Netzlaufwerke mit relevanten Patientendaten mit Rechnern verbunden, die an das Internet angeschlossen sind?
- Wurden Awareness-Schulungen durchgeführt, die Internetbedrohungen (z. B. Schadcode, Phishing,...) zum Inhalt hatten?

Zeitraum

Beginn: Oktober 2018
Abschluss: noch nicht abgeschlossen

Anzahl geprüfte Verantwortliche

8 Ärzte

Ergebnis

Bei der ersten Sichtung der eingegangen Antworten war zu erkennen, dass Ärzte meist nicht optimal auf Ransomware-Angriffe vorbereitet sind. So ist das Praxisnetz oft an das Internet angeschlossen, sodass eine Infektion durch Ransomware nicht nur wahrscheinlicher ist, sondern beim Eintreten auch mit einem größeren Schadensausmaß zu rechnen ist. Die Backup-Konzepte waren in einigen Fälle nicht ausreichend. Auch ist zu vermuten, dass auf Grund fehlender Routinen, Übungen und Tests das Einspielen vorhandener Datensicherungen im Ernstfall nicht ohne Weiteres durchgeführt werden kann. Einziger Lichtblick der Prüfung war bisher, dass die Arztpraxen durchgängig von der Gefahrensituation durch Ransomware wussten und ihre Mitarbeiter diesbezüglich sensibilisierten.

4.10 HTTPS-Prüfung

Anlass und Ziel der Prüfung

Verantwortliche müssen beim Betrieb von Websites sicherstellen, dass personenbezogene Daten angemessen geschützt und damit auch sicher übertragen werden. Ein Teil unserer Cybersicherheitsinitiative, die wir im Herbst 2017 gestartet hatten, war, die Transportverschlüsselung bayerischer Websites näher zu begutachten. Hierfür stellten wir einen separaten Online-Service auf unserer eigenen Homepage zur Verfügung. Damit konnten uns Verantwortliche, die ihre eigene Webseite untersuchen lassen wollten, die jeweilige URL mitteilen.

Prüffragen

Prüfgegenstand war die Implementierung und Konfiguration eines HTTPS-Zertifikats nach den gesetzlichen Anforderungen. Nähere Angaben zu den Prüfkriterien sind im Kapitel 23.7 dieses Berichts zu finden.

Zeitraum

Beginn: Oktober 2017
Abschluss: Februar 2018

Anzahl geprüfte Verantwortliche

162 Websites bayerischer Verantwortlicher

Ergebnis

Wir haben sowohl für den Online-Service als auch für die Prüfung als solche sehr positive Resonanz erhalten. Unternehmen, die ihre eigene Website bei uns eingaben, erhielten ein schriftliches Feedback mit dem Ergebnis der Prüfung. Wir teilten dabei gerade vielen kleineren Betrieben mit, dass sie hinsichtlich einer korrekten Umsetzung von HTTPS deutlichen Nachbesserungsbedarf hatten. In zahlreichen Fällen mussten wir anschließend noch Hilfestellung bezüglich des technischen Verständnisses und der Umsetzung der Anforderungen leisten. Dies führte letztendlich dazu, dass wir den Online-Service vorübergehend stilllegen mussten. Eine erneute Aktivierung erscheint erst dann wieder möglich, wenn unsere Behörde über ausreichend Personalressourcen verfügt. Aufgrund der zahlreichen Defizite bei Websites, die wir durch unsere Prüfung bislang feststellten, kann ohne Zweifel festgehalten werden, dass ein solcher Online-Service für alle Beteiligten von Mehrwert ist.

5

Der betriebliche Datenschutzbeauftragte

5 Der betriebliche Datenschutzbeauftragte

5.1 Erforderlichkeit einer Benennung

Die wesentliche Fragestellung für die verpflichtende Benennung eines Datenschutzbeauftragten ist, wie viele Personen in der Regel sowie ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Beim Thema „Benennung eines betrieblichen Datenschutzbeauftragten" erreichte uns immer wieder die gleiche, aber zentrale Frage: Wann ist in einem Unternehmen oder bei einer anderen Stelle jemand „in der Regel" sowie „ständig" mit der automatisierten Verarbeitung personenbezogener Daten „beschäftigt"?

Hierzu wiesen wir zunächst auf Folgendes hin: Ergänzend zu den allgemeinen Vorschriften für die Benennung eines Datenschutzbeauftragten in Art. 37 Abs. 1 DS-GVO hält § 38 Abs. 1 Satz 1 BDSG die in Deutschland aus der Vergangenheit bekannte Regelung aufrecht, dass bei mindestens zehn Personen, die mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, ebenfalls ein Datenschutzbeauftragter zu benennen ist. Dabei kommt es nach dem Gesetzeswortlaut darauf an, dass diese zehn Personen zum einen in der Regel sowie zum anderen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

„In der Regel" stellt als Abgrenzungsmerkmal darauf ab, dass die zehn oder mehr Beschäftigten die übliche personelle Größenordnung des Unternehmens oder des Auftragsverarbeiters bilden; gelegentliche unregelmäßige Aushilfen bleiben dabei außer Betracht.

„Ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt" setzt voraus, dass dies ein Schwerpunkt der Tätigkeit einer Person ist.

Beispiele hierzu: Handwerker, die ein Tablet zur Eingabe der Arbeitszeit beim Kunden nutzen, haben überwiegend mit ihrer handwerklichen Tätigkeit zu tun. Ebenso ist bei Versandmitarbeitern eines Lieferdiensts, die ein Unterschriftspad zur elektronischen Unterschrift des Kunden über ein erhaltenes Paket nutzen, die Tätigkeit regelmäßig weit überwiegend das Zusammenstellen und Ausliefern von Waren. Diese Beispiele zeigen, dass gerade solche Gruppen von Mitarbeitern dann allenfalls untergeordnet mit der automatisierten Verarbeitung personenbezogener Daten von Kunden befasst sind, sodass diese bei der vorher genannten Zehn-Personen-Grenze nicht mitzuzählen sind. Gleiches gilt bspw. auch für Kassenkräfte in Einzelhandelsgeschäften, wenn diese im Schwerpunkt ihrer Tätigkeit Waren über Scanner ziehen, Waren einpacken, anonyme Barkäufe kassieren, eventuell daneben noch Waren einräumen, platzieren sowie Verpackungsmüll wegräumen, und nur untergeordnet personalisierte Kartenzahlungen entgegennehmen.

Beschäftigte der Personal- oder Finanzbuchhaltung zählen hingegen in aller Regel zu den zehn Personen dazu, da hier die vorher aufgelisteten Voraussetzungen erfüllt werden.

Da dieses Thema bei uns gehäuft angefragt wurde, haben wir eine Kurzinformation auf unserer Website als FAQ (Frequently Asked Questions, zu Deutsch: „Häufige Fragen") veröffentlicht:

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

5.2 Überwachungsaufgaben des Datenschutzbeauftragten

Die Hauptverantwortung für die Einhaltung der DS-GVO trägt nicht der Datenschutzbeauftragte, sondern die Leitung eines Unternehmens, eines Vereins oder einer anderen Stelle. Der Datenschutzbeauftragte hat eine Beratungsfunktion und insoweit auch eine Überwachungsfunktion.

Im Berichtszeitraum kam oft die Frage auf, welche Rolle der Datenschutzbeauftragte im Sinne der DS-GVO tatsächlich einnehmen muss.

Nach Art. 39 Abs. 1 Buchstabe b DS-GVO obliegt dem Datenschutzbeauftragten konkret die *Überwachung* der Einhaltung der DS-GVO, anderer Datenschutzvorschriften sowie der Strategien des Verantwortlichen (oder des Auftragsverarbeiters) für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen *Überprüfungen*. In der Praxis stellen sich für Datenschutzbeauftragte daher die Folgefragen, wie diese Überwachungen und Überprüfungen durchzuführen sind und ob damit eventuell sogar umfangreiche Audits durch den Datenschutzbeauftragten, z. B. entsprechend DIN EN ISO 19011 (Leitfaden zur Auditierung von Managementsystemen), veranlasst werden müssen.

Wir meinen dazu, dass in erster Linie der Verantwortliche aufgrund der Pflichten-Zuweisungen in der DS-GVO, wie vor allem der Rechenschaftspflicht nach Art. 5 Abs. 2 und der Sicherstellungspflicht nach Art. 24 Abs. 1 DS-GVO, für die Einhaltung der Datenschutzvorschriften in seinem Unternehmen zu sorgen und dies auch zu kontrollieren hat. Dies kann z. B. durch die Beauftragung der Revision oder der Compliance-Abteilung mit bestimmten Prüfungen, gegebenenfalls auch durch Veranlassung externer Audits wie bspw. nach DIN ISO 19011 erfolgen. Der unabhängige Datenschutzbeauftragte muss in der Gesamtschau überwachen, ob hinreichende Datenschutz- und Datensicherheitsmaßnahmen getroffen wurden und dazu den Verantwortlichen beraten sowie ihm Empfehlungen unterbreiten.

Im veröffentlichten Informationspapier WP 243 des Europäischen Datenschutzausschusses sind entsprechende Angaben unter Nummer 4.1 zu finden:

edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de

6

Auftragsverarbeitung

6 Auftragsverarbeitung

6.1 Vertrag zur Auftragsverarbeitung und Formulierungshilfe

Wie nach dem bisherigen Recht ist auch unter DS-GVO bei der Beauftragung eines Dienstleisters zur Auftragsverarbeitung grundsätzlich ein Vertrag mit datenschutzrechtlichen Regelungen vorgeschrieben.

Mit dem Inkrafttreten der DS-GVO hat sich bezüglich der Pflicht, einen Vertrag zwischen Verantwortlichen und Auftragsverarbeiter für die Auftragsverarbeitung abzuschließen, nichts geändert. Um den Beteiligten hierzu eine Hilfestellung zu geben und zu zeigen, wie die Anforderungen der DS-GVO diesbezüglich umgesetzt werden können, haben wir in Abstimmung mit dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit eine Formulierungshilfe erstellt, die inzwischen auch von anderen Aufsichtsbehörden übernommen wurde.

Die Formulierungshilfe kann für den Praxiseinsatz je nach konkretem Anwendungsfall mühelos ergänzt, gekürzt oder modifiziert zu werden, um dem gegebenen Sachverhalt gerecht zu werden. Die Vorlage kann auf unserer Website abgerufen werden:

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

6.2 Abgrenzung Verantwortlicher zu Auftragsverarbeiter

Veröffentlichungen helfen bei der Einschätzung, ob eine Auftragsverarbeitung vorliegt oder nicht.

Sehr häufig wurden uns verschiedene Sachverhalte detailliert geschildert und dazu die Frage gestellt, was wir als Auftragsverarbeitung mit einem Regelungsbedarf nach Art. 28 Abs. 3 DS-GVO einordnen und was demgegenüber als eine eigenständig (oder gemeinsam mit anderen) zu verantwortende Tätigkeit anzusehen ist.

Weil die früher geltende Datenschutzrichtlinie 95/46/EG die gleichen Definitionen für Verantwortliche und Auftragsverarbeiter hatte wie die Nachfolgeregelung DS-GVO, konnten wir auf die bereits vorhandenen Überlegungen und Beispiele in dem Arbeitspapier Nr. 169 der früheren Artikel-29-Datenschutzgruppe verweisen, die zur ersten Orientierung herangezogen werden können. Das Dokument ist unter dem folgenden Link abrufbar:

ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

Auch die Datenschutzkonferenz der deutschen Aufsichtsbehörden hat in ihrem Kurzpapier Nr. 13 ebenfalls Grundsätze zur Einordnung von Sachverhalten dargestellt und in den dazugehörigen Anhängen A, B und C konkrete Beispiele genannt. Das Kurzpapier ist auf der Website der DSK veröffentlicht:

www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf

Ergänzend dazu haben wir in einem eigenen kurzen FAQ-Papier die genannten Beispielsauflistungen erweitert, um der Praxis noch mehr Orientierung zu geben. Auftragsverarbeitung im datenschutzrechtlichen Sinne liegt nach unserer Auffassung nur in Fällen vor, in denen eine Stelle von einer anderen Stelle im Schwerpunkt mit der Verarbeitung personenbezogener Daten beauftragt wird. Die Beauftragung mit fachlichen Dienstleistungen anderer Art, d. h. mit Dienstleistungen, bei denen nicht die Datenverarbeitung im Vordergrund steht bzw. bei denen die Datenverarbeitung nicht zumindest einen wichtigen (Kern-)Bestandteil ausmacht, stellt unserer Meinung nach keine Auftragsverarbeitung im datenschutzrechtlichen Sinne dar.

Das FAQ-Papier zur Abgrenzung von Auftragsverarbeitung ist auf unserer Website zu finden:

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

6.3 Datenschutzrechtliche Anforderungen an Dienstleister

Im Rahmen der Auftragsverarbeitung sind die datenschutzrechtlichen Anforderungen an Dienstleister nicht disponibel.

Verantwortliche stellten uns die Frage, wie damit umzugehen ist, wenn man sich mit Dienstleistern nicht auf einen Vertrag zur Auftragsverarbeitung einigen kann. Wir haben hierzu festgehalten: Können sich ein Verantwortlicher und ein Auftragsverarbeiter nicht auf den Abschluss oder eine erforderliche Anpassung der Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO verständigen, weil sich z. B. der Auftraggeber weigert, den Vertrag abzuschließen oder einen nach altem Recht bestehenden Vertrag anzupassen, entfällt für den Auftragsverarbeiter die datenschutzrechtliche Grundlage für die Verarbeitung. Daran ändert sich auch dann nichts, wenn Auftraggeber und Auftragnehmer dem gleichen Konzern angehören und/oder dadurch bspw. für Beschäftigte des Auftraggebers oder andere juristische oder natürliche Personen keine Leistungen durch den Auftraggeber erbracht werden können. Dies wäre bspw. bei der Erstellung einer Gehaltsabrechnung durch die „Service-GmbH" eines Konzerns der Fall, wenn es dadurch zu Verzögerungen bei der Auszahlung der Löhne käme. Die Verantwortlichkeit liegt auch hier beim Auftraggeber, der als datenschutzrechtlich Verantwortlicher eine eigene Verpflichtung hat, dafür zu sorgen, dass seine Verarbeitungen rechtskonform erfolgen, gerade auch, wenn er dafür einen Dienstleister einschaltet. Entfällt für den Auftragsverarbeiter die datenschutzrechtliche Grundlage, erfüllt sich für ihn wie für den Auftraggeber ein bußgeldfähiger Tatbestand nach Art. 83 Abs. 4 Buchstabe a i. V. m. Art. 28 DS-GVO.

Bemühten sich im Berichtszeitraum in konkreten Fällen beide Parteien um eine interessensgerechte Anpassung einer Vereinbarung nach § 11 BDSG-alt an die Anforderungen der DS-GVO, konnte für einen vertretbaren Zeitraum von einer aufsichtsrechtlichen Sanktion durch uns abgesehen werden, soweit beide Parteien einigungsbereit und in der Wertung der Gesamtsituation für die betroffenen Personen, deren Daten von der Verarbeitung umfasst sind, keine Nachteile dadurch ersichtlich waren.

7

Betroffenenrechte

7 Betroffenenrechte

7.1 Informationspflichten

7.1.1 Informationspflichten in abgestufter Umsetzung

Die neuen Informationspflichten können situationsgerecht auch in abgestufter Form (mit „Medienbruch“) erfüllt werden.

In der alltäglichen Praxis gibt es zahlreiche Situationen, in denen eine praxistaugliche und angemessene Balance zwischen den Informationspflichten nach Art. 13 und 14 DS-GVO und der Gefahr einer Informationsermüdung bzw. Informationsüberhäufung bei den betroffenen Personen im Hinblick auf deren vielfältige Geschäftsbeziehungen geschaffen werden muss. Nur so können die betroffenen Personen in der Masse situationsgerecht zumindest die wichtigsten Informationen noch bewusst zur Kenntnis nehmen.

Nicht unwesentlich ist dabei die Regelung aus Art. 12 Abs. 1 DS-GVO. Dort finden sich allgemeine Vorgaben darüber, dass geeignete Maßnahmen zu treffen sind, um die (Datenschutz-) Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Wie diese Anforderungen im Alltag umzusetzen sind, hängt tatsächlich sehr stark von der konkreten Datenverarbeitung ab. Der Europäische Datenschutzausschuss (EDSA) hat im „Working Paper 260“ eine gestufte Information für zulässig erachtet. Auf der ersten Stufe bzw. im ersten Schritt müssen immer die Informationen zur Identität des Verantwortlichen und zu den Zwecken der Verarbeitung gegeben werden, soweit diese Informationen nicht ohnehin schon wegen der Art des Kontakts mit der betroffenen Person offenkundig sind (z. B. bei deren Anruf zu einer Terminvereinbarung mit dem Friseur oder Steuerberater). Je nach Art des Kontakts mit der betroffenen Person ist ergänzend noch auf das Bestehen der Betroffenenrechte hinzuweisen, z. B. in Werbeschreiben. Auf zweiter Stufe müssen dann alle Informationen nach Art. 13 bzw. 14 DS-GVO für die betroffene Person erhältlich sein bzw. gegeben werden. Dies kann bspw. per Link zu der entsprechenden Website erfolgen, auf der alle Informationen vorgehalten werden. Möglich ist auch das Bereithalten eines dementsprechenden Informationsblattes, das jederzeit ausgehändigt bzw. übergeben oder zugesandt werden kann.

Wir haben die vielen diesbezüglich anfragenden Verantwortlichen auf die Möglichkeit dieser abgestuften Form mit Medienbruch hingewiesen. Das veröffentlichte Working Paper 260 des EDSA, das diesen zweistufigen Ansatz als zulässig erachtet, kann unter dem folgenden Link heruntergeladen werden:

edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

7.1.2 Informationspflichten bei Karten-Zahlungen

Bei Zahlungsvorgängen mit EC- oder Kreditkarte sind Informationen an die bezahlenden Kunden situationsgerecht auszugeben.

In Handel und Dienstleistung, in Hotels und Gastronomie, bei Veranstaltungen usw., stellt sich die Frage, wie gerade im oft schnell ablaufenden Massengeschäft die Informationen nach Art. 13 DS-GVO sachgerecht an die betroffenen Personen gegeben werden können. Entsprechend erhielten wir Anfragen von Betrieben, welche Ansätze es gibt, um die Kunden beim elektronischen Bezahlen geeignet über den Umgang mit ihren Daten zu informieren.

Hiermit hat sich im September 2018 der „Arbeitskreis Wirtschaft“ der Datenschutzkonferenz

befasst. Empfohlen werden im Ergebnis Hinweisaufkleber, Aufsteller oder kleinere Aushänge im Kassenbereich bzw. am Ladeneingang mit Informationen zu den Verantwortlichen sowie mit einem Internet-Link zu den weiteren Informationen. Ergänzend muss für Interessierte ein vollständiges Info-Blatt an der Kasse bzw. im Laden etc. erhältlich sein.

7.1.3 Informationspflichten bei Traueranzeigen

Bei der Aufgabe von gedruckten Traueranzeigen oder für Online-Medien muss der Veranlasser der Traueranzeige die übrigen darin genannten Personen (z. B. Angehörige) hierzu informieren, nicht etwa die Zeitung oder Dienst selbst.

Datenschutzrechtliche Vorgaben sind auch bei dem Aufgeben von Traueranzeigen zu berücksichtigen: Was in einer solchen Anzeige genau steht und welche Trauernde dabei namentlich genannt werden, liegt im Verantwortungsbereich der Person, die eine Traueranzeige selbst oder über einen Bestatter aufgibt. Wir haben daher festgehalten, dass diese Person (z. B. ein Angehöriger) sich bei den betroffenen Personen vergewissern muss, ob und in welcher Weise sie in der Traueranzeige genannt werden wollen, bevor sie eine Zeitung und gegebenenfalls deren Online-Dienst mit der Veröffentlichung beauftragt.

Die Person, die die Anzeige aufgibt bzw. deren Veröffentlichung verantwortet, muss auch prüfen und die in der Anzeige genannten Personen (z. B. Angehörige) darüber informieren, was vereinbarter Vertragsgegenstand mit dem Medienunternehmen werden soll, z. B. nur eine Zeitungsveröffentlichung oder auch eine Online-Veröffentlichung der Traueranzeige.

7.1.4 Informationspflichten am Telefon

Bei Telefongesprächen können die Informationspflichten situations- und bedarfsgerecht in abgeschichteter Form ausreichend erfüllt werden.

Häufig wurden uns Fragen zur sachgerechten Umsetzung der Informationspflichten nach Art. 13 DS-GVO bei Telefongesprächen gestellt, z. B. über was bei einem Anruf alles informiert werden muss und ob sogar eine Bandansage am Telefon abgespielt werden sollte, die dann vorab über die Datenverarbeitung informiert.

Wir haben auch hier versucht, möglichst schnell für Klarheit zu sorgen: Es ist zunächst zu unterscheiden, ob eine Person selbst bei der betreffenden Stelle anruft und von sich aus ein konkretes Anliegen vorträgt (wie z. B. Notruf bei einer Rettungsleitstelle, Anruf zur Terminvereinbarung mit der Hausbank oder mit einem Handwerksbetrieb) oder ob die betroffene Person angerufen wird.

Im ersten Fall, Anruf durch die Person selbst, verfügt diese Person regelmäßig schon über die Informationen zum Verantwortlichen und zum Zweck des Anrufs, sodass sich weitergehende Datenschutzinformationen in dem Telefongespräch zur Speicherung der Daten aus dem Anruf grundsätzlich erübrigen. Bei entsprechenden Nachfragen der anrufenden Person zu den weiteren Informationen nach Art. 13 DS-GVO oder bei einer beabsichtigten Speicherung der Daten auch für andere Zwecke (wie spätere Werbung) sind die ergänzenden Informationen entsprechend Art. 13 DS-GVO zu erteilen. Das kann durch die Zusendung eines Informationsblattes, Hinweis auf einen Link im Internet oder das Abspielen einer Bandaufzeichnung erfolgen.

Ruft ein Unternehmen oder eine andere Stelle bei einer Person an, muss diese Person jedenfalls über die Identität des Verantwortlichen und die Zwecke des Anrufs informiert werden,

soweit dies nicht schon wegen bestehender geschäftlicher oder sonstiger Beziehungen klar ist. Situations- und bedarfsgerecht sind die weiteren Informationen nach Art. 13 DS-GVO zur Verarbeitung personenbezogener Daten auch hier durch Zusendung eines Informationsblattes, Hinweis auf einen Link im Internet oder das Abspielen einer Bandaufzeichnung anzubieten.

7.1.5 Informationspflichten zur Gesprächsaufzeichnung in Callcentern

Eine Aufzeichnung von Telefongesprächen in Callcentern bedarf der informierten Einwilligung der externen Gesprächspartner.

Die Aufzeichnung von Telefongesprächen ist datenschutzrechtlich in aller Regel auch unter der DS-GVO nur mit informierter Einwilligung (insbesondere für welche Zwecke und Dauer die Aufzeichnung erfolgt) auch des externen Gesprächspartners zulässig. Eine datenschutzrechtlich wirksame Einwilligung im Sinne von Art. 4 Nr. 11 DS-GVO setzt voraus, dass der externe Gesprächspartner vor Beginn der beabsichtigten Aufzeichnung gefragt wird, ob er mit der Aufzeichnung einverstanden ist, und falls er einverstanden ist, gebeten wird, sein Einverständnis bspw. durch Aussprechen eines „Ja" oder durch eine andere aktive bestätigende Handlung (etwa durch das Betätigen einer bestimmten Telefontaste) eindeutig zum Ausdruck zu bringen.

Wir teilten Anfragenden mit, dass die bloße Einräumung einer Widerspruchsmöglichkeit mit dem anschließenden Fortsetzen des Telefonats keine datenschutzrechtlich wirksame Einwilligung im Sinne der DS-GVO darstellt.

Da der datenschutzrechtlich Verantwortliche nachweisen können muss, dass die betroffene Person eine wirksame Einwilligung erteilt hat (Art. 7 Abs. 1 DS-GVO), muss er auch nachweisen können, dass die betroffene Person die Einwilligung „in informierter Weise" abgegeben hat (vgl. Art. 4 Nr. 11 DS-GVO), z. B. durch genaue Festlegungen der Gesprächsführung für die Beschäftigten der Callcenter zur Information der externen Gesprächspartner.

Hinsichtlich weiterer Informationen verwiesen wir auf den Beschluss der Datenschutzkonferenz vom 23.03.2018, der auf der offiziellen DSK-Website abrufbar ist:

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

7.1.6 Informationspflichten bei Ärzten

Patienten müssen nicht unterschreiben, dass sie Datenschutzinformationen in der Arztpraxis zur Kenntnis genommen haben.

In vielen Arztpraxen bestand große Verunsicherung, ob man Patienten Datenschutzhinweise aushändigen und anschließend unterschreiben lassen muss, um den neuen Anforderungen der DS-GVO gerecht zu werden. Nach unserer Auffassung können Arztpraxen ihre nach Art. 13 DS-GVO bestehenden Informationspflichten erfüllen, indem sie die zu erteilenden Informationen in ihrer Praxis, bspw. im Wartebereich oder bei der Anmeldung, als Flyer oder Handout bereitlegen. Eine Unterschrift des Patienten, die Informationen erhalten zu haben, ist nicht erforderlich.

In dem Beschluss der DSK vom 5. September 2018 wurde festgehalten, dass der Verantwortliche, um seinen Nachweispflichten gegenüber der Aufsichtsbehörde nachzukommen, das Aushändigen der Information vermerken oder einen konkreten Verfahrensablauf betreffend der Umsetzung der Informationspflicht dokumentieren kann, aus dem hervorgeht, wie die Patientin oder der Patient die Informationen *im Regelfall* erhält. In diesem Beschluss wurde zudem festgehalten, dass eine Verweigerung der Behandlung wegen einer bloßen Verweigerung

der ja ohnehin nicht erforderlichen Unterschrift durch den Patienten nicht mit der DS-GVO vereinbar ist.

Der Beschluss der DSK vom 5. September 2018 ist online abrufbar:

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

7.2 Auskunft

7.2.1 Auskunftsrecht bei Ärzten

Patienten, die ihr Recht auf Auskunft gelten machen, ist eine vollständige Übersicht der Daten in verständlicher Form von den Arztpraxen zu geben, ohne dass dabei medizinische Fachbegriffe erläutert werden müssen.

Viel Unsicherheit verursachte das Verhältnis des Auskunftsanspruchs nach Art. 15 DS-GVO zu dem Recht auf Einsichtnahme in die Patientenakte nach § 630 g BGB.

Zunächst hielten wir fest, dass der Auskunftsanspruch nach Art. 15 DS-GVO sämtliche bei dem Verantwortlichen gespeicherte personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO umfasst. Der Erwägungsgrund 63 stellt dabei klar, dass Art. 15 DS-GVO auch die eigenen gesundheitsbezogenen Daten umfasst, etwa Daten in Patientenakten. Somit sind Informationen wie bspw. Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen, enthalten.

Verlangen kann der Antragssteller nach Art. 15 DS-GVO eine vollständige Übersicht dieser Daten in verständlicher Form, d. h. in einer Form, die es ihm ermöglicht, von diesen Daten Kenntnis zu erlangen und zu prüfen, ob sie richtig sind und der DS-GVO gemäß verarbeitet werden. Das bedeutet aber nicht, dass ein Arzt einem Auskunft begehrenden Patienten in der Patientenakte stehende Fachbegriffe oder sonstige Kurzbezeichnungen erläutern muss.

Als Einschränkung einer Auskunftspflicht nach Art. 15 DS-GVO könnte es unserer Meinung nach sinnvoll sein, die Regelung des § 630 g Abs. 1 Halbsatz 2 BGB analog heranzuziehen (Einschränkung aus erheblichen therapeutischen Gründe oder sonstigen erheblichen entgegenstehenden Rechten Dritter).

7.2.2 Kopien von Unterlagen bei Auskunft

Das Auskunftsrecht über gespeicherte personenbezogene Daten begründet keinen allgemeinen Anspruch auf Kopien von Dokumenten oder Akten.

Wir wurden oft gefragt, ob vollständige Kopien von Akten im Rahmen von Auskunftsersuchen von Verantwortlichen angefertigt und herausgegeben werden müssen. Der datenschutzrechtliche Auskunftsanspruch nach Art. 15 DS-GVO betrifft nach dem Wortlaut von dessen Abs. 1 eine Auskunftserteilung über die personenbezogenen Daten, die vom Verantwortlichen verarbeitet werden. Das bedeutet aber nicht regelmäßig die Herausgabe von allen Dokumenten, E-Mails etc., in denen z. B. der Name der betroffenen Person und eventuelle weitere Informationen über diese Person enthalten sind.

Nach Art. 15 Abs. 3 DS-GVO ist nur eine „Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind", zur Verfügung zu stellen. Es ist hier jedoch nicht die Rede von Kopien der betreffenden Akten, von sonstigen Unterlagen usw.

Hierzu verwiesen wir auch auf das Urteil des Europäischen Gerichtshofs (EuGH) vom 17.07.2014, Az. C-141/12 und C-372/12, in dem u. a. Folgendes ausgeführt wird:

„…In Fällen wie denen, die zu den Ausgangsverfahren geführt haben, folgt aus der in Rn. 48 des vorliegenden Urteils gegebenen Antwort, dass nur die Daten, die in der Entwurfsschrift über denjenigen … wiedergegeben sind, und die Daten, die gegebenenfalls in der Entwurfsschrift enthaltenen rechtlichen Analyse wiedergegeben sind, „personenbezogene Daten" im Sinne von Art. 2 Buchstabe a der Richtlinie 95/46 sind. Folglich bezieht sich das Auskunftsrecht, auf das sich dieser Antragsteller gemäß Art. 12 Buchstabe a der Richtlinie 95/46 und Art. 8 Abs. 2 der Charta berufen kann, ausschließlich auf diese Daten … Zur Wahrung dieses Auskunftsrechts genügt es, dass dieser Antragsteller eine vollständige Übersicht dieser Daten in verständlicher Form erhält, d. h. in einer Form, die es ihm ermöglicht, von diesen Daten Kenntnis zu erlangen und zu prüfen, ob sie richtig sind und der Richtlinie gemäß verarbeitet werden, so dass er gegebenenfalls die ihm in der Richtlinie verliehenen Rechte ausüben kann."

Wegen der gleichgelagerten Regelung in Art. 15 Abs. 1 DS-GVO im Vergleich zur früheren EU-Datenschutzrichtlinie (dort Art. 12) sehen wir die vom EuGH in der zitierten Entscheidung aufgestellten Maßstäbe weiterhin als zutreffend an.

Manche bereichsspezifische Vorschriften gehen über den datenschutzrechtlichen Auskunftsanspruch nach Art. 15 DS-GVO hinaus, wie z. B. § 630g BGB mit einem Recht von Patienten auf elektronische Abschriften der Patientenakte, allerdings gegen Kostenerstattung.

7.3 Berichtigung

7.3.1 Allgemeines zum Recht auf Berichtigung

Das Recht auf Berichtigung ist ein zentrales Datenschutzrecht für betroffene Personen.

Im Berichtszeitraum haben wir zahlreiche Anfragen, aber auch Beschwerden erhalten, die im Schwerpunkt von den Betroffenenrechten handelten. Das gemäß Art. 16 DS-GVO neue Recht für betroffene Personen, vom Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen, war dabei jedoch eher nicht so häufig Thema. Wir stellen daher in den nachfolgenden Ausführungen lediglich eine ausgewählte Fallkonstellation dar. Andere Berichtigungssachverhalte sind im Tätigkeitsbericht z. B. noch in Kapitel 13.4 und 13.5 zu finden.

7.3.2 Berichtigung eines Werturteils in Versicherungs- oder Arztakten

Gespeicherte Werturteile sind einem Berichtigungs- bzw. Löschanspruch zugänglich.

Auch im Sinne von Art. 2 Abs. 1 DS-GVO gespeicherte bzw. verarbeitete Meinungsäußerungen, Beurteilungen und Werturteile, die sich auf eine bestimmte oder bestimmbare betroffene Person beziehen, sowie Darstellungen des privaten oder beruflichen Verhaltens dieser Person werden von der Begriffsdefinition der personenbezogenen Daten nach Datenschutzrecht mit erfasst. Der Begriff der personenbezogenen Daten umfasst schließlich alle Informationen, die über eine Bezugsperson etwas aussagen oder mit ihr in Verbindung zu bringen sind.

Somit müssen gespeicherte Werturteile über eine Person wie „unverschämt", „zahlungsunwillig", „schleppende Zahlungsweise" im Falle eines

Bestreitens durch die beurteilte Person von dem Verantwortlichen entweder hinreichend belegt werden können oder je nach Sachverhalt berichtigt bzw. sogar gelöscht werden.

Bei Fragestellungen dieser Art kann auch auf die bisherige Rechtsprechung, z. B. die Urteile des Bundesgerichtshof (BGH) vom 23.06.2009 („spickmich") und vom 22.02.2011 verwiesen werden:

openjur.de/u/31109.html
openjur.de/u/163862.html

7.4 Löschung

7.4.1 Löschung bei Werbung

Die Löschung der Postadresse verhindert nicht automatisch die spätere Zusendung von Postwerbung.

Wenn betroffene Personen von Unternehmen unerwünschte, personalisierte Postwerbung erhalten, wünschen sie vom Absender oftmals gleichzeitig eine Löschung ihrer Postadresse und die Gewähr, künftig von solcher Werbung des Absenders verschont zu bleiben. Entsprechende Beschwerden erhalten wir hierzu gehäuft.

Für die Umsetzung der Betroffenenrechte ist im Zweifelsfall von der betroffenen Person klarzustellen bzw. bei ihr zu klären, was sie mit ihrer Willenserklärung bewirken möchte. Möchte sie vorrangig von einer werblichen Ansprache durch das Unternehmen verschont bleiben, ist dafür die Aufnahme ihrer Kontaktdaten in eine Werbesperrdatei bei diesem Unternehmen das richtige Mittel zur Berücksichtigung ihres Willens. Bei der (datenschutzrechtlich zulässigen) Nutzung von Fremddaten kann dann durch Abgleich mit der Werbesperrdatei sichergestellt werden, dass die Kontaktdaten dieser betroffenen Person nicht verwendet werden.

Wünscht eine betroffene Person ausdrücklich und allein eine Löschung aller Daten, sollte sie darauf hingewiesen werden, dass sie bei einem künftigen – rechtlich zulässigen – Einsatz von Fremddaten eventuell wieder Werbung erhalten kann.

7.4.2 Löschung bei Patientendaten

Patientendaten sind nicht in jedem Fall auf Wunsch der betroffenen Person zu löschen.

Wegen des Rechts auf Löschung von personenbezogenen Daten erreichten uns im Gesundheitsbereich einerseits Anfragen von Arztpraxen, wie mit einem Löschungswunsch von Patienten umgegangen werden soll. Andererseits beschwerten sich Patienten, weil ihr Arzt die Patientendaten nicht unverzüglich und vollständig gelöscht hat.

Hier ist festzuhalten, dass personenbezogene Daten nicht in jedem Fall auf Wunsch der betroffenen Person zu löschen sind, sondern dass der Löschung stets eine Prüfung vorausgehen muss, ob die Voraussetzungen für einen Löschungsanspruch vorliegen. Denn die betroffene Person hat (nur) dann ein Recht auf Löschung, wenn eine der in Art. 17 Abs. 1 DS-GVO genannten Voraussetzungen vorliegt.

Danach sind personenbezogene Daten insbesondere zu löschen, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind (Art. 17 Abs. 1 Buchstabe a DS-GVO). Eine Löschpflicht besteht hier auch ohne Aufforderung durch den Betroffenen.

Sollte für die Erreichung des Zwecks, für den die Daten erhoben wurden, die Aufbewahrung noch notwendig sein, muss bzw. darf nicht gelöscht werden. Dies kann insbesondere dann der Fall sein, wenn die Gesundheitsdaten wichtige Informationen enthalten, von denen davon ausgegangen werden kann, dass für diese auch nach Ablauf gesetzlicher Aufbewahrungsfristen

das Interesse des Berechtigten an der Speicherung das an der Löschung überwiegt, bspw. im Hinblick auf Medikamentenunverträglichkeiten. Gemäß Art. 17 Abs. 3 DS-GVO dürfen Daten zudem nicht gelöscht werden, wenn für diese eine gesetzliche Pflicht zur Aufbewahrung besteht. Insbesondere nach § 630 f Abs. 3 BGB besteht eine gesetzliche Aufbewahrungsfrist von 10 Jahren nach Abschluss der Behandlung. Darüber hinaus gibt es Normen, die eine weitergehende Aufbewahrung gebieten, wie bspw. § 28 Abs. 3 RöV.

Eine Ausnahme von der Verpflichtung zur Löschung kann sich zudem aus Art. 17 Abs. 3 Buchstabe e DS-GVO ergeben, da die objektive Verjährungsfrist für Schadensersatzansprüche wegen Körper- oder Gesundheitsverletzungen gemäß § 199 Abs. 2 BGB dreißig Jahre nach Vornahme des potentiell schadensträchtigen Verhaltens beträgt. Hier ist eine Abwägung unter Berücksichtigung der Interessen des Betroffenen und der Wahrscheinlichkeit der Geltendmachung von Ansprüchen („erforderlich") vorzunehmen. Eine Aufbewahrung aller Patientendaten für die Dauer von 30 Jahren wegen drohender Schadensersatzansprüche wäre nicht datenschutzkonform. Erforderlich ist hier eine individuelle Risikobewertung.

Grundsätzlich muss jeder Verantwortliche, d. h. auch jeder Arzt, sich selbst darüber vergewissern, welche Aufbewahrungsfristen er für welche personenbezogenen Daten seiner Patienten hat. Wir als Datenschutzaufsichtsbehörde gaben hier bislang nichts vor, sondern verlangten im Zuge einer möglichen Prüfung der Rechenschaftspflicht den Nachweis, auf welcher Rechtsgrundlage Daten noch verarbeitet (gespeichert) werden.

7.5 Datenübertragbarkeit

7.5.1 Allgemeines zum Recht auf Datenübertragbarkeit

Das Recht auf Datenübertragbarkeit ist eines der neuen Instrumente der DS-GVO und soll den betroffenen Personen bessere Kontrolle über ihre Daten bieten.

Das in Art. 20 DS-GVO verankerte Recht auf Datenübertragbarkeit, das meist auch unter Recht auf Datenportabilität bekannt ist, stärkt die Rechte der betroffenen Personen gerade im Bereich digitaler Dienste, wie z. B. bei sozialen Netzwerken. Zweck der Vorschrift ist es primär, den Wettbewerb um datenschutzfreundliche Produkte und Dienstleistungen zu fördern.

Im Berichtszeitraum beschäftigten wir uns also mit diesem neuen Recht, um zu sehen, wo die Vorschrift im Alltag tatsächlich Anwendung findet. Es haben sich dann jedoch kaum relevante Fragestellungen bei unserer Behörde durch Bürgereingaben hierbei ergeben. Wir gehen davon aus, dass dieses Thema künftig mehr Bedeutung in unserem Datenschutzalltag erfahren könnte.

7.5.2 Datenübertragbarkeit bei Ärzten

In der Regel besteht kein Anspruch auf Datenportabilität für Patienten gegenüber Ärzten oder medizinischen Laboren.

In einem uns geschilderten Fall verlangte ein Patient von einem medizinischen Labor unter Verweis auf sein Recht auf Datenübertragbarkeit die Laborrechnung in einem maschinenlesbaren Format, um die Angaben für seine eigenen Zwecke bequem weiter verarbeiten zu können.

Wir haben darauf hingewiesen, dass personenbezogene Daten, die auf der Rechtsgrundlage des Art. 9 Abs. 2 Buchstabe h DS-GVO verarbeitet werden (wie z. B. die Verarbeitung von Patientendaten in einem medizinischen Labor),

nicht vom Recht auf Datenübertragbarkeit erfasst sind. Dieses Recht besteht nämlich dagegen nach Art. 20 Abs. 1 Buchstabe a DS-GVO dann, „sofern die Verarbeitung auf einer Einwilligung gemäß Art. 6 Abs. 1 Buchstabe a oder Art. 9 Abs. 2 Buschstabe a oder auf einem Vertrag gemäß Art. 6 Abs. 1 Buchstabe b beruht".

Hinzu kommt, dass sich das Recht auf Datenübertragbarkeit dem Wortlaut nach nur auf diejenigen personenbezogenen Daten bezieht, die die betroffene Person einem Verantwortlichen bereitgestellt hat. Diejenigen Daten, die also eine Arztpraxis bzw. im konkreten Sachverhalt das medizinische Labor bei der Bearbeitung des Laborauftrages generiert hat (wie z. B. die Laborwerte, die Rechnungsdaten etc.), sind vom Recht auf Datenübertragbarkeit nicht erfasst.

8

Datenschutz im Internet

8 Datenschutz im Internet

8.1 Bewertungsportale

Die datenschutzrechtlichen Anforderungen bei sogenannten Bewertungsportalen haben sich durch die DS-GVO nicht wesentlich verändert.

Wir waren in der Vergangenheit mehrfach und regelmäßig mit datenschutzrechtlichen Fragestellungen im Zusammenhang mit Bewertungsplattformen für Personen bestimmter Berufsgruppen befasst. Am bekanntesten dürften Bewertungsplattformen für Lehrer und Ärzte sein. Auch die Rechtsprechung hat sich in den letzten Jahren mit deren datenschutzrechtlichen Zulässigkeit auseinandergesetzt und hierzu einige richtungsweisende Urteile gefällt.

Nach der Rechtsprechung des Bundesgerichtshofs (BGH vom 23.09.2014, Az.: VI ZR 358/13, BGH vom 20.02.2018, Az.: VI ZR 30/17) zu einem Arztbewertungsportal ist die Speicherung der personenbezogenen Daten der Ärzte zum Zweck der Übermittlung zulässig und ein Löschungsanspruch mithin nicht gegeben. Im Ergebnis wurde die datenschutzrechtliche Zulässigkeit auf datenschutzrechtliche Rechtsgrundlagen gestützt, nach denen eine Abwägung zwischen dem Recht auf informationelle Selbstbestimmung des bewerteten Arztes nach Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG und dem Recht auf Kommunikationsfreiheit nach Art. 5 Abs. 1 GG der Bewertenden und des Portalbetreibers stattzufinden hat:

> *„Nach § 29 Abs. 1 Satz 1 Nr. 1 BDSG ist die Erhebung und Speicherung personenbezogener Daten zum Zweck der Übermittlung zulässig, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung oder Speicherung hat. Der wertausfüllungsbedürftige Begriff des „schutzwürdigen Interesses" verlangt eine Abwägung des Interesses des Betroffenen an dem Schutz seiner Daten und des Stellenwerts, den die Offenlegung und Verwendung der Daten für ihn hat, mit den Interessen der Nutzer, für deren Zwecke die Speicherung erfolgt, unter Berücksichtigung der objektiven Wertordnung der Grundrechte (...) Dabei hat eine Abwägung zwischen dem Recht der Klägerin auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, Art. 8 Abs. 1 EMRK auf der einen Seite und dem Recht der Beklagten sowie der Interessen der Portalnutzer (vgl. Art. 7 Buchstabe f Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ABl. Nr. L 281 S. 31) auf Kommunikationsfreiheit nach Art. 5 Abs. 1 GG, Art. 10 Abs. 1 EMRK auf der anderen Seite zu erfolgen, bei der zudem die mittelbare Drittwirkung des beiden Seiten zustehenden Grundrechts aus Art. 12 Abs. 1 GG zu berücksichtigen ist (...). Nach den Feststellungen des Berufungsgerichts ist auch im vorliegenden Fall davon auszugehen, dass die Beklagte in dem von ihr betriebenen Internetportal die über Ärzte gespeicherten personenbezogenen Daten – also die sogenannten Basisdaten verbunden mit Noten und Freitextkommentaren – zum Abruf bereit stellt. Für ein auf diese Funktion beschränktes Bewertungsportal hat der Senat entschieden, dass die Speicherung der personenbezogenen Daten der Ärzte zulässig und ein Löschungsanspruch nach § 35 Abs. 2 Satz 2 Nr. 1 BDSG mithin nicht gegeben ist (...)."*

Bereits im Tätigkeitsbericht 2013/2014 haben wir unter Punkt 7.5 die Grundzüge der datenschutzrechtlichen Bewertung derartiger Plattformen vorgestellt.

Mit Geltung der DS-GVO war nun eine Welle weiterer Eingaben/Anfragen bewerteter Personen, insbesondere von Ärzten, festzustellen, die

das Erfordernis einer grundsätzlichen datenschutzrechtlichen Neubewertung von Arztbewertungsportalen gesehen haben bzw. einen Löschungsanspruch ihrer personenbezogenen Daten auf der Grundlage der Vorschriften der DS-GVO geltend gemacht haben.

In den Vorschriften der DS-GVO findet sich allerdings eine nahezu gleich lautende Rechtsgrundlage für eine rechtmäßige Verarbeitung personenbezogener Daten wie dies in den Vorschriften des BDSG-alt der Fall war und die Grundlage für die Beurteilung der grundsätzlichen datenschutzrechtlichen Zulässigkeit gewesen ist. Eine Verarbeitung ist nunmehr rechtmäßig, wenn

> *„die Verarbeitung [...] zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich [ist], sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen"*

(Art. 6 Abs. 1 Buchstabe f DS-GVO).

Art. 17 Abs. 3 Buchstabe a DS-GVO bestimmt, dass ein Recht auf Löschung personenbezogener Daten nicht besteht,

> *„soweit die Verarbeitung erforderlich ist zur Ausübung des Rechts auf freie Meinungsäußerung und Information"*.

Vor dem Hintergrund dieser rechtlichen Bestimmungen der DS-GVO und der seitens des BGH in seinen Entscheidungen angestellten Überlegungen und aufgestellten Abwägungskriterien sehen wir derzeit keine Veranlassung, aufgrund der Geltung der DS-GVO von der bisherigen datenschutzrechtlichen Bewertung eines Arztbewertungsportals abzuweichen.

Wir werden aber beobachten, ob und wie die Rechtsprechung in Zukunft über Anträge auf Löschung von Profilen in Arztbewertungsportalen auf der Grundlage der DS-GVO entscheidet und unser Prüfverhalten daran orientieren.

8.2 Datenschutzbestimmungen auf Websites

Websitebetreiber haben nach DS-GVO zahlreiche, zum Teil auch neue Informationspflichten, die sie auf ihrer Website berücksichtigen müssen.

Einen wahren Ansturm an Anfragen und Eingaben hatten wir zu der Thematik des Bereitstellens einer gesetzeskonformen Datenschutzerklärung für einen Internetauftritt zu verzeichnen. Teilweise konnte man den Eindruck gewinnen, dass Informationspflichten in Form von Datenschutzerklärungen als ein vollkommen neues Thema wahrgenommen werden und erst mit Geltung der DS-GVO geschaffen worden sind und eine dahin gehende Verpflichtung nicht schon nach der bisherigen Rechtslage bestanden habe. Oder aber die neue Rechtslage wurde zum Anlass genommen, unliebsamen Websitebetreibern, die nicht rechtzeitig eine Überarbeitung/Anpassung einer bereits vorhandenen Datenschutzerklärung bis zum 25. Mai 2018 vorgenommen hatten, durch eine Beschwerde bei der Datenschutzaufsichtsbehörde zumindest etwas Ärger zu bereiten. Wieder andere, nämlich Verantwortliche von Internetauftritten selbst, richteten eine Vielzahl an entsprechenden Beratungsanfragen an uns, „was denn aufgrund der DS-GVO bezüglich ihrer Datenschutzerklärung veranlasst sei" bzw. „wie eine nach den Vorschriften der DS-GVO gesetzeskonforme Datenschutzerklärung für ihren Internetauftritt auszusehen habe".

Grundsätzlich bemühen wir uns natürlich immer, konkreten Eingaben zu unzulässig einzustufenden Datenschutzerklärungen die angemessene Aufmerksamkeit zu widmen. Auf solche Nachfragen geben wir entsprechende Hinweise für eine aus unserer Sicht zutreffende Umsetzung der Vorschriften der DS-GVO im Hinblick auf die Gestaltung einer Datenschutzerklärung im Internetauftritt. Allerdings wird dies nicht so weit gehen können, dass wir für einen

konkreten Internetauftritt eine Datenschutzerklärung erstellen oder eine entsprechende Vorlage liefern. Es verbleibt dabei, dass es der Verantwortung des für den Internetauftritt Verantwortlichen obliegt, den vom Gesetzgeber vorgegebenen gesetzlichen Regelungen zu entsprechen. Denn ohne eine umfassende, konkrete Überprüfung des jeweiligen internen Umgangs mit den personenbezogenen Daten der Nutzer beim Verantwortlichen und ohne technische Überprüfung des Internetauftritts ist bspw. kaum eine Aussage dazu möglich, welchen Inhalt die konkrete Datenschutzerklärung haben muss, um vollständig und inhaltlich richtig zu sein.

Insofern wurden Anfragende und Verantwortliche eines Internetauftritts auf die gesetzlichen Regelungen der Art. 12 ff. DS-GVO verwiesen bzw. darauf hingewiesen und ihnen aufgetragen, eine bereits nach bisherigem Recht vorhandene Datenschutzerklärung inhaltlich an den Maßgaben der Art. 13, 14 DS-GVO zu messen und anzupassen bzw. bei einer neu zu formulierenden Datenschutzerklärung den Inhalt auf die in Art. 13, 14 DS-GVO genannten Punkten abzustimmen.

Die genannten Vorschriften der DS-GVO benennen die Punkte, die – individuell abgestimmt auf den konkreten Internetauftritt – eine Datenschutzerklärung enthalten muss. Nicht vorgegeben sind die Wortwahl oder bestimmte Formulierungen. Die Informationen sollen aber „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ zur Verfügung gestellt werden (Art. 12 Abs. 1 Satz 1 DS-GVO) und dienen dazu, eine faire und transparente Verarbeitung zu gewährleisten (Art. 5 Abs. 1 Buchstabe a DS-GVO, ErwGr. 60). Dieses Ziel im Blick, kann eine Datenschutzerklärung durchaus durch den Diensteanbieter selbst formuliert werden.

In aller Regel trifft die Informationspflicht jeden Websitebetreiber, selbst wenn der Internetauftritt recht einfach gehalten sein mag und z. B. lediglich der Information des Nutzers dient und nicht einmal eine Möglichkeit der Eingabe von personenbezogenen Daten bietet (z. B. durch ein Kontaktformular, einen Registrierungsvorgang). Hintergrund für diese Einschätzung ist, dass mit dem Aufruf einer Website zumindest die Erhebung und Nutzung der IP-Adresse des Nutzers als technische Steuerungsinformation zur Übertragung von Informationen zwischen dem Diensteanbieter (bzw. dem mit dem Hosting der Website beauftragten Hosting-Unternehmen) und dem Nutzer erforderlich ist und die IP-Adresse des Nutzers ein datenschutzrechtlich relevantes Datum ist. Über die Verarbeitung der IP-Adresse ist der Nutzer zu informieren, sofern diese vom Hosting-Unternehmen an den Diensteanbieter fließen bzw. die Möglichkeit eines Abrufs auf Seiten des Diensteanbieters besteht.

Einzig in dem speziellen Fall, dass die IP-Adressen einzig beim Hosting-Unternehmen verbleiben, dort in erster Linie zu Sicherheitszwecken verarbeitet werden und nicht an den Diensteanbieter fließen bzw. von diesem abgerufen werden können, würden wir in der Verarbeitung der IP-Adressen durch das Hosting-Unternehmen keine Auftragsverarbeitung für den Diensteanbieter erkennen und eine kurzfristige IP-Adressenspeicherung noch der Vermittlung eines Telekommunikationsdienstes durch das Hosting-Unternehmen und damit den Regelungen des Telekommunikationsgesetzes zurechnen (siehe hierzu die Informationen in unserem Internetauftritt unter „Fragen und Antworten“, „Hosting keine Auftragsverarbeitung“).

www.lda.bayern.de/de/infoblaetter.html

Vielfältig wurden wir bei unserer Arbeit auf im Internet frei abrufbare Textgeneratoren für die Erstellung von Datenschutzerklärungen aufmerksam gemacht. Sofern diese als „Anregung“ verstanden werden, welche konkreten Elemente eine Datenschutzerklärung in der Praxis überhaupt enthalten kann bzw. als Formulierungshilfe genutzt werden, ist gegen derartige Angebote sicherlich nichts einzuwenden. Allerdings

ist bei der Nutzung genau darauf zu achten, dass die damit erstellte Datenschutzerklärung auf den individuellen Internetauftritt abgestimmt ist, die tatsächlich stattfindende Verarbeitung personenbezogener Daten korrekt wiedergegeben wird und die gelieferte Vorlage einer Datenschutzerklärung ggf. konkretisiert wird. Dies hatten wir bereits in unserem 6. Tätigkeitsbericht 2013/2014 unter Punkt 7.6 festgehalten:

www.lda.bayern.de/media/baylda_report_06.pdf

8.3 Cookie-Banner

Vorhandene Cookie-Banner auf Websites erfüllen meist nicht die Anforderungen für eine ausreichende Information und wirksame Einwilligung.

Auf vielen Websites sind sog. „Cookie-Banner" eingebunden. Mit diesen Bannern soll eine Einwilligung des Nutzers eingeholt und über die Datenverarbeitung informiert werden. Eine Vielzahl dieser Cookie-Banner erfüllt die datenschutzrechtlichen Anforderungen nicht. Zwar kann durch eine vorgeschaltete Abfrage beim ersten Aufruf einer Website oder einer Web-App grundsätzlich eine wirksame Einwilligung eingeholt werden. Dabei sind jedoch folgende Anforderungen zu beachten:

- Beim erstmaligen Öffnen einer Website, erscheint das Banner bspw. als eigenes HTML-Element. In der Regel besteht dieses HTML-Element aus einer Übersicht aller einwilligungsbedürftigen Verarbeitungsvorgänge, die unter Nennung der beteiligten Akteure und deren Funktion ausreichend erklärt und über ein Auswahlmenü aktiviert werden können. Aktivieren bedeutet in diesem Zusammenhang, dass die Auswahlmöglichkeiten nicht voreingestellt sein dürfen.
- Das Banner blockiert zunächst alle Skripte einer Website oder Web-App, die potenziell Nutzerdaten erfassen.
- Erst wenn der Nutzer seine Einwilligung durch eine aktive Handlung wie zum Beispiel das Setzen eines Häkchens im Banner oder den Klick auf eine Schaltfläche abgegeben hat, darf die Datenverarbeitung stattfinden.
- Diese Aktion des Nutzers, die Abgabe der Einwilligung, wird vom Verantwortlichen gespeichert, damit bei einem weiteren Aufruf der Website das Banner nicht erneut erscheint und die Einwilligung zu Beweiszwecken gesichert ist. Zur Erfüllung der Nachweispflichten des Art. 7 Abs. 1 DS-GVO ist es gem. Art. 11 Abs. 1 DS-GVO nicht erforderlich, dass die Nutzer dazu direkt identifiziert werden. Eine indirekte Identifizierung (vgl. ErwGr. 26) ist ausreichend.
- Da eine Einwilligung widerruflich ist, muss eine entsprechende Möglichkeit zum Widerruf implementiert werden.
- Verantwortliche müssen sicherstellen, dass die Einwilligung nicht nur das Setzen von Cookies umfasst, sondern alle einwilligungsbedürftigen Verarbeitungstätigkeiten, wie z. B. Verfahren zur Verfolgung der Nutzer durch Zählpixel oder Canvas Fingerprinting.

Nur wenn die oben genannten Anforderungen erfüllt sind, liegt eine wirksame Einwilligung vor.

8.4 Kontaktformulare

Kontaktformulare können unter Berücksichtigung weniger Anforderungen mühelos auf Websites zur Verfügung gestellt werden.

Im Rahmen der wahrgenommenen Rechtsunsicherheit durch die DS-GVO haben sich manche Websitebetreiber entschieden, das Kontaktformular vorübergehend oder sogar dauerhaft von der Website zu entfernen. Andere Verantwortliche hatten die Kontaktformulare auf der

Website belassen und die Verarbeitung der eingegebenen Daten dabei auf eine Einwilligung gestützt. In beiden Fällen wiesen wir jeweils darauf hin, dass Kontaktformulare an sich ohne weiteres auf Websites eingebunden werden können, wenn folgende Punkte beachtet werden:

- Grundsätzlich bedarf es keiner Einwilligung durch den Nutzer, da die Datenverarbeitung auf eine Interessenabwägung nach Art. 6 Abs. 1 Buchstabe f DS-GVO gestützt werden kann. Der Verantwortliche hat ein berechtigtes Interesse daran, Nutzeranfragen, die über das Kontaktformular eingehen, zu beantworten.
- Falls das Kontaktformular vom Nutzer verwendet wird, um sich über angebotene Waren und Dienstleistungen zu informieren, kann die Verarbeitung zu diesem Zweck auf Art. 6 Abs. 1 Buchstabe b DS-GVO gestützt werden (zur Erfüllung eines Vertrags).
- Eine Einwilligung ist dann erforderlich, wenn besondere Kategorien personenbezogener Daten gem. Art. 9 Abs. 1 DS-GVO verarbeitet werden. Das kann z. B. der Fall sein, wenn über das Formular Gesundheitsdaten für die Terminvergabe bei einem Arzt abgefragt werden, das Kontaktformular für die Anmeldung bei einer religiösen Vereinigung oder politischen Partei genutzt wird oder der Nutzer Anhänge hochladen kann, die Rückschlüsse auf Daten zur Religion, ethnischen Herkunft, sexuellen Orientierung etc. zulassen.
- Weiterhin sollten Verantwortliche überprüfen, welche Daten im Kontaktformular als Pflichtfelder ausgestaltet und welche Angaben dagegen optional sind. Der Verantwortliche sollte nur solche Eingaben als Pflichtfelder festlegen, die tatsächlich erforderlich sind, um die Anfrage zu beantworten. „So viel wie nötig, so wenig wie möglich" – dieses Prinzip sollte auch bei der Gestaltung des Kontaktformulars gelten. Das leitet sich nicht nur aus dem Grundsatz zur Datensparsamkeit ab, sondern auch aus dem Grundsatz Privacy by Default. Das beutet bspw., dass das Geburtsdatum oder die Anschrift des Nutzers nicht nötig sind, wenn das Kontaktformular für ein Online-Portal genutzt wird, bei dem sich jeder pseudonym anmelden kann.

8.5 Fotos auf Websites

Es ist nicht immer eine Einwilligung erforderlich, um Fotos im Web zu veröffentlichen.

Seit dem 25. Mai 2018 hat sich auch der Rechtsrahmen für die Anfertigung und Verarbeitung von Fotos geändert. Für die Praxis, wie mit Fotos auf Websites umzugehen ist, hat dies aber an sich keine wesentlichen Auswirkungen mit sich gebracht. Derzeit wird jedoch intensiv deutschlandweit diskutiert, ob sich die Veröffentlichung von Fotos noch nach den Vorschriften des Kunsturhebergesetzes (KUG) richten kann. Wir vertreten als BayLDA die Auffassung, dass das KUG durch die Regelungen der DS-GVO verdrängt wird und nicht mehr anwendbar ist. Somit richtet sich die Verarbeitung von Fotos nach den Vorschriften der DS-GVO, es sei denn, die Fotos werden zu journalistischen, künstlerischen oder literarischen Zwecken verarbeitet. In diesem Fall gelten – vereinfacht gesagt – nur noch die Regelungen zum Datengeheimnis und zur Datensicherheit (vgl. Art. 38 BayDSG).

Im Ergebnis hat die DS-GVO für Website-Betreiber in puncto Fotos keine wesentlichen Änderungen ergeben. Dennoch war die Rechtsunsicherheit groß. Uns erreichten unzählige Anfragen von Websitebetreibern zur Veröffentlichung von Fotos.

Die Verarbeitung von Fotos, insbesondere die Veröffentlichung im Internet, ist rechtmäßig, wenn

- dies gemäß Art. 6 Abs. 1 Buchstabe b DS-GVO in einem Vertrag vereinbart wurde, z. B. bei der Hochzeitsfotografie oder Modelverträgen,
- die abgebildete Person gem. Art. 6 Abs. 1 Buchstabe a DS-GVO eingewilligt hat oder
- die berechtigten Interessen des Verantwortlichen gem. Art. 6 Abs. 1 Buchstabe f DS-GVO überwiegen.

Um auf Nummer sicher zu gehen, empfehlen wir grundsätzlich eine Einwilligung für die Veröffentlichung von Fotos einzuholen. Das schafft nicht nur Transparenz, sondern auch Rechtssicherheit, da die Veröffentlichung auch in jedem Fall rechtmäßig ist.

Liegt keine Einwilligung vor, bedeutet dies aber keinesfalls, dass die Veröffentlichung verboten ist. Ganz im Gegenteil: Wir sind der Auffassung, dass z. B. ein Verein in fast allen Fällen die Veröffentlichung auf Art. 6 Abs. 1 Buchstabe f DS-GVO stützen kann, weil er ein berechtigtes Interesse daran hat, über das Vereinsgeschehen zu informieren und die abgebildete Person durch die Veröffentlichung nicht besonders beeinträchtigt ist.

Auf Grund der vielen Anfragen speziell zum Thema „Fotos im Vereinsleben" beleuchten wir in dem ergänzenden Kapitel 17.4 in diesem Tätigkeitsbericht die dortigen Besonderheiten näher.

Zu beachten ist stets auch der Zweck der Veröffentlichung und der Kontext, in dem das Foto erscheint. Beispielsweise wäre es nicht mehr im Rahmen der Interessenabwägung zulässig, ein Foto eines Passanten auf der Straße zu veröffentlichen, um Werbung für einen Markenturnschuh zu schalten. Hier überwiegen die Interessen des Betroffenen, da er nicht damit rechnet, dass sein Bild für Werbezwecke veröffentlicht wird.

Außerdem sollten Verantwortliche mit Fotos von Kindern besonders achtsam umgehen. Jede Veröffentlichung im Internet birgt die Gefahr, dass Fotos de facto nicht mehr gelöscht werden können, sondern allenfalls das Wiederfinden z. B. über Suchmaschinen erschwert wird. Denn ein Löschen für immer ist bei Veröffentlichungen im Internet die absolute Ausnahme. Aus diesem Grund sind Verantwortliche auf der sicheren Seite, wenn sie vorab die Einwilligung der Eltern einholen.

Eine Einwilligung ist in jedem Fall dann erforderlich, wenn (mindestens) eines der folgenden Kriterien erfüllt ist:

- Das Foto erfasst die Intimsphäre der betroffenen Person (hier überwiegen in der Regel die Interessen der betroffenen Person).
- Beschäftigte werden auf dem Foto veröffentlicht (hier ist auf die Rechtsprechung des Bundesarbeitsgerichts abzustellen, nach der im Beschäftigtenverhältnis eine schriftliche Einwilligung eingeholt werden soll).
- Die betroffene Person wird in einer Situation dargestellt, die diskreditierend sein kann oder die Gefahr einer Diskriminierung birgt (z. B. Partyfotos, Nacktfotos).
- Auf dem Foto werden Situationen dargestellt, die z. B. Rückschluss auf Religion, Gesundheit, Sexualleben oder sexuelle Orientierung ermöglichen (vgl. Art. 9 Abs. 1 DS-GVO).

8.6 WhatsApp

Hinsichtlich des Einsatzes von WhatsApp im beruflichen Umfeld bestehen große Datenschutzbedenken.

Nicht erst seit Geltung der DS-GVO herrscht bei Bürgern und Unternehmen große Verunsicherung bezüglich des Einsatzes von Messenger-Diensten. Vor allem WhatsApp ist seit langer Zeit in der öffentlichen Kritik. Befeuert wird die Diskussion um den Messenger durch die mittlerweile zahlreichen Datenschutzbeschwerden, die seit dem 25. Mai 2018 bei den Aufsichtsbehörden eingegangen sind. Die Beschwerden befassen sich nahezu immer mit denselben Problemen: Betroffene Personen erhalten keine Auskunft über die gespeicherten Daten, Löschanträge werden nicht umgesetzt und die Einwilligung im Messenger ist unwirksam. Dennoch wollen Unternehmen die Kommunikation zum Kunden und innerhalb des Unternehmens so einfach wie möglich gestalten.

Wir empfehlen eingehend zu prüfen, ob für die Kommunikation auf andere Messenger als WhatsApp gesetzt bzw. umgestellt werden kann. Grund hierfür ist, dass WhatsApp viele Informationen zur Kommunikation innerhalb der Facebook-Unternehmensgruppe teilt – und in Zukunft womöglich die Daten aller Dienste verschmelzen möchte. Zum aktuellen Umgang mit den Kundendaten gibt WhatsApp umfangreiche Informationen in den Nutzungsbedingungen und Datenschutzbestimmungen. Alternativen zu WhatsApp sind z. B. Threema, SIMSme, Wire, Hoccer und Chiffry.

Sollten Verantwortliche dennoch nicht auf WhatsApp verzichten wollen, sind folgende Anforderungen zu berücksichtigen:

- WhatsApp darf von Berufsgeheimnisträgern grundsätzlich nicht eingesetzt werden (Ausnahmen nur unter ganz speziellen Voraussetzungen möglich).
- Für die interne Unternehmenskommunikation sollte der Einsatz von WhatsApp grundsätzlich unterbleiben.
- Nachrichtenverläufe über WhatsApp sollten nicht archiviert werden.
- Automatische Speicherung der Nachrichten im internen Speicher, insbesondere der Anhänge, sollte vermieden werden, wenn weitere Apps auf dem mobilen Gerät installiert sind, denen Zugriff auf den internen Speicher gestattet wird (Gefahr eines unberechtigten Zugriffs und Fehlversand von Anhängen).
- WhatsApp sollte von einem separaten Smartphone oder über eine Container-Lösung/Mobile Device Management betrieben werden.
- Soweit der Zugriff auf das Telefonbuch gewährt wird, muss sichergestellt werden, dass nur Kontakte (z. B. Kunden/Klienten) im Telefonbuch gespeichert sind, die ihre Einwilligung erteilt haben.

8.7 Facebook Custom Audience über die Kundenliste

Der Bayerische Verwaltungsgerichtshof bestätigt unsere Anordnung hinsichtlich Facebook Custom Audience.

Wir hatten uns bereits mehrfach zu den Anforderungen an einen zulässigen Einsatz von Marketing-Tools in Tätigkeitsberichten, Pressemitteilungen und sonstigen Veröffentlichungen geäußert. Auf Basis dieser Informationen untersuchten wir in einer Großprüfung bei über 40 Unternehmen in Bayern, ob und in welcher Weise das Marketing-Werkzeug „Facebook Custom Audience“ eingesetzt wurde.

Das Ergebnis unserer Prüfung war, dass bei den meisten Unternehmen ein Verstoß gegen datenschutzrechtliche Pflichten vorlag. In vielen Fällen haben die Unternehmen nach entsprechender Belehrung durch uns auf die weitere Nutzung des weit verbreiteten Marketing-Tools verzichtet. Eines der geprüften Unternehmen weigerte sich jedoch, unseren Aufforderungen nachzukommen. Daraufhin haben wir eine Anordnung erlassen und das Unternehmen darin aufgefordert, das „Facebook Custom Audience über die Kundenliste" nicht mehr einzusetzen. Die sofortige Vollziehung wurde von uns dabei angeordnet. Gegen diese Anordnung klagte das Unternehmen.

Im Eilverfahren in der ersten Instanz bestätigte das VG Bayreuth unsere Auffassung. Im Berufungsverfahren entschied der Bayerische Verwaltungsgerichtshof, dass unsere Anordnung rechtmäßig ergangen sei und bestätigte folgende Auffassung von uns:

- Das eingesetzte Hash-Verfahren SHA-256 ist nicht geeignet, um personenbezogene Daten zu anonymisieren.
- Für die Frage, ob ein Verhältnis über eine Auftragsverarbeitung vorliegt, kommt es nicht auf die vertraglichen Vereinbarungen der Parteien an, sondern auf die tatsächlichen Abläufe der Datenverarbeitung.
- Im konkreten Fall ist Facebook im Rahmen des Dienstes „Custom Audience über die Kundenliste" nicht Auftragnehmer des Unternehmens, sondern eine eigene verantwortliche Stelle.
- Das Hochladen der Kundenliste stellt eine Übermittlung personenbezogener Daten dar.
- Diese Übermittlung kann nicht auf die Rechtsgrundlage des Art. 6 Abs. 1 Buchstabe f DS-GVO gestützt werden. Insbesondere überwiegen die schutzwürdigen Interessen der Nutzer, sodass die Übermittlung nicht auf eine Interessenabwägung gestützt werden kann. Zwar hat der Werbetreibende ein berechtigtes Interesse an zielgerichteter Werbung; diesem Interesse stehen jedoch die überwiegenden, schutzwürdigen Interessen der Betroffenen gegenüber, die insbesondere nicht damit rechnen, dass ihre E-Mail-Adresse an Facebook übermittelt wird.
- Daher ist der Einsatz nur aufgrund einer vorigen informierten Einwilligung des Nutzers zulässig.

Das Verfahren „Facebook Custom Audience" ermöglicht es Unternehmen, ihre Kunden, die zugleich Nutzer von Facebook sind, auf dem sozialen Netzwerk gezielt bewerben zu lassen. Um auf Facebook werben zu können, erstellt ein Unternehmen (z. B. Online-Shop) eine Liste seiner Kunden und Interessenten mit Name, Wohnort, E-Mail-Adresse und Telefonnummer. Diese Kundenliste wird dann im Facebook-Konto des Online-Shops an Facebook hochgeladen. Zuvor werden die Kundendaten unter Einsatz eines sogenannten Hash-Verfahrens in feste Zeichenketten umgewandelt (z. B. Max Mustermann = dddfab9b5b8a360150547065daff114ff218b39c8b0986b761075977aeeca3c3). Danach gleicht Facebook die Kundenliste mit allen Facebook-Nutzern ab und kann so feststellen, welcher Kunde des Online-Shops auch Mitglied bei Facebook ist. Der Online-Shop kann somit eine oder mehrere Werbekampagne(n) auf Facebook für seine Kunden starten. Er wählt eine bestimmte Zielgruppe aus, die die Werbung erhalten soll. So kann der Online-Shop vorgeben, dass z. B. Frauen zwischen 20 und 30 Jahren, die viel Sport treiben und über ein durchschnittliches Einkommen verfügen, Werbung in ihrem Facebook-Account von dem Online-Shop erhalten.

Grundlage für unsere Anordnung sowie für die Entscheidungen der Gerichte war die Rechtslage vor dem 25. Mai 2018, also vor Geltung der DS-GVO. Allerdings berücksichtigte unsere Anordnung schon vorsorglich die neue Rechtslage

nach der DS-GVO. Da es im Kern des Rechtsstreits um die Frage ging, ob das Interesse am Einsatz des Marketing-Tools den schutzwürdigen Interessen der Betroffenen überwiegt, ist die Entscheidung auch nach der neuen Rechtslage – der DSVO – relevant.

8.8 Facebook-Fanpages

Fanpage-Betreiber haben auf Facebook eine datenschutzrechtliche Verantwortung gegenüber den Fanpage-Nutzern.

Mit Urteil vom 5. Juni 2018 hat der EuGH, Aktenzeichen C-210/16, entschieden, dass eine gemeinsame Verantwortlichkeit von Facebook und Fanpage-Betreibern besteht. Das bedeutet u. a., dass Fanpage-Betreiber nicht mehr allein auf die datenschutzrechtliche Verantwortung von Facebook verweisen können, sondern selbst für die Einhaltung des Datenschutzes gegenüber den Fanpage-Nutzern mitverantwortlich sind.

Die Entscheidung hat zu großer Verunsicherung geführt, weil die Folgen einer Verarbeitung gemeinsam Verantwortlicher nach der DS-GVO zum Teil unklar sind. Aus diesem Grund hat die DSK folgende Anforderungen für Fanpage-Betreiber formuliert:

- Der Fanpage-Besucher muss transparent und in verständlicher Form darüber informiert werden, welche Daten zu welchem Zwecken durch Facebook und die Fanpage-Betreiber verarbeitet werden. Dies gilt sowohl für Personen, die bei Facebook registriert sind, als auch für nicht registrierte Besucherinnen und Besucher des sozialen Netzwerks.
- Diese Informationspflichten können Fanpage-Besucher nur dann erfüllen, wenn sie darauf hinwirken, dass Facebook ihnen die erforderlichen Informationen zur Verfügung stellt.
- Fanpage-Betreiber müssen gemeinsam mit Facebook in einer Vereinbarung festlegen, wer von ihnen welche Verpflichtung der DS-GVO erfüllt. Diese Vereinbarung muss in wesentlichen Punkten den Betroffenen zur Verfügung gestellt werden, damit diese ihre Betroffenenrechte wahrnehmen können.

Außerdem hat die DSK einen Fragenkatalog formuliert. Dieser Fragenkatalog ist Bestanteil eines Beschlusses der DSK zu Facebook-Fanpages vom 5. September 2018. Die dort aufgeführten Fragen müssen von Facebook und Fanpage-Betreibern beantwortet werden können. Sollte dies nicht möglich sein, kann die Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO nicht erfüllt und ein datenschutzkonformes Betreiben der Fanpage nicht dargelegt werden.

Siehe Urteil des EuGH:

curia.europa.eu/juris/liste.jsf?language=de&num=C-210/16

Siehe Beschluss der DSK vom 5. September 2018:

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

8.9 Offline-Tracking

Verantwortliche müssen sich auch bei Offline-Tracking-Verfahren im Klaren darüber sein, dass Hash-Verfahren nicht zur Anonymisierung von personenbezogenen Daten führen.

Nicht nur im Einzelhandel, sondern auch an vielen Bahnhöfen, Flughäfen oder Veranstaltungsorten werden Offline-Tracking-Verfahren zur Kundenfrequenz-Messung eingesetzt. Dabei werden Kunden und Besucher über ihr Smartphone oder sonstige mobile Geräte erfasst. Durch mehrere Router werden hierbei die MAC-Adressen, in einigen Fällen auch weitere Geräte-

daten der Besucher erhoben und ggf. über einen längeren Zeitraum gespeichert. Dies ermöglicht es dem Verantwortlichen zu messen, wie viele Besucher einen bestimmten Ort passieren, wie lange sie sich dort aufhalten und welche dieser Besucher zum wiederholten Male vorbeikommen.

Zahlreiche Dienste zum Offline-Tracking sind derart ausgestaltet, dass die gehashten MAC-Adressen auf unbestimmte Zeit gespeichert und evtl. mit weiteren Daten zusammengeführt werden. Dies geschieht deshalb, weil Betreiber des Offline-Tracking meist davon ausgehen, es handle sich bei den gehashten Daten um anonymisierte Daten. Wir vertreten hierzu jedoch eine andere Auffassung: Bei der MAC-Adresse handelt es sich um ein personenbezogenes Datum, da hier die MAC-Adresse einem bestimmten Gerät zugeordnet ist und der Nutzer des Geräts mittelbar bestimmt werden kann. Zwar wird in der Regel die MAC-Adresse unter Verwendung eines Hash-Verfahrens verändert – das Hash-Verfahren führt jedoch nicht zu einer Anonymisierung der Daten. Diese Auffassung wurde durch einen Beschluss des Bayerischen Verwaltungsgerichtshofs vom 26. September 2018 bestätigt.

Siehe Beschluss des BayVGH:

gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2018-N-25018

Verantwortliche, die Verfahren zum Offline-Tracking einsetzen, müssen daher sicherstellen, dass die Datenverarbeitung aufgrund einer Rechtsgrundlage oder einer Einwilligung erfolgt. In der Praxis sind uns keine Fälle bekannt, in denen tatsächlich eine wirksame Einwilligung eingeholt wurde. Auch Hinweise gem. Art. 12 ff. DS-GVO zum Einsatz des Offline-Tracking fehlen regelmäßig.

9

Steuerberater und Rechtsanwälte

9 Steuerberater und Rechtsanwälte

9.1 Auftragsverarbeitung bei Steuerberatern

Die Beauftragung von Steuerberatern ist in der Regel keine Auftragsverarbeitung.

Steuerberater sind nach unserer Auffassung nach dem insoweit geltenden Fachrecht (Steuerberatungsgesetz) als Freiberufler selbständig, weisungsunabhängig und eigenverantwortlich tätig und unterliegen dementsprechend auch einer strafbewehrten persönlichen Geheimhaltungspflicht (vgl. dazu § 57 Steuerberatungsgesetz, § 203 Abs. 1 Nr. 3 des Strafgesetzbuches). Das widerspricht der Weisungsgebundenheit im Sinne von Art. 28 Abs. 3 Buchstabe a DS-GVO. Des Weiteren ist den Steuerberatern eine gewerbliche Tätigkeit außerhalb des Steuerberaterrechts grundsätzlich untersagt (§ 57 Abs. 4 Nr. 1 Steuerberatungsgesetz).

In dem DSK-Kurzpapier Nr. 13 zur Auftragsverarbeitung nach der DS-GVO heißt es auf Seite 4 deshalb wie folgt:

> *„Keine Auftragsverarbeitung, sondern die Inanspruchnahme fremder Fachleistungen bei einem eigenständig Verantwortlichen, für die bei der Verarbeitung (einschließlich Übermittlung) personenbezogener Daten eine Rechtsgrundlage gemäß Art. 6 DS-GVO gegeben sein muss, sind beispielsweise in der Regel die Einbeziehung eines Berufsgeheimnisträgers (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer)…"*

Siehe DSK-Kurzpapier Nr. 13:

www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf

Auch wenn Steuerberater nur die Lohnbuchhaltung für einen Mandanten durchführen, müssen sie dafür aufgrund des Steuerberaterrechts die eigene Verantwortung übernehmen und können sich nicht, wie allgemeine Dienstleister zur Lohnabrechnung, auf Weisungen von Mandanten berufen.

Steuerberater arbeiten deshalb aus unserer Sicht regelmäßig eigenverantwortlich aufgrund eines Mandantenvertrags und dürfen von den Mandanten im Rahmen der Erforderlichkeit für ihre Tätigkeit personenbezogene Kunden- und/oder Arbeitnehmerdaten erhalten.

9.2 Entsorgung von Akten bei Berufsgeheimnisträgern

Besondere Sorgfalt ist bei der Entsorgung von Akten bei Berufsgeheimnisträgern geboten – maßgeblich ist hier nach wie vor die DIN 66399.

Die Vernichtung von Datenträgern regelt die DIN 66399, welche je nach Art und Sensibilität der zu vernichtenden Daten eine Zuordnung in 3 Schutzklassen und 7 Sicherheitsstufen vorsieht. Bei Akten von Berufsgeheimnisträgern handelt es sich häufig um besondere Kategorien personenbezogener Daten i. S. d. Art. 9 DS-GVO, die darüber hinaus einem strafrechtlich sanktionierten Berufsgeheimnis unterliegen. Der Schutzbedarf der Daten ist deshalb sehr hoch (Schutzklasse 3). In diesem Bereich sind für die Vernichtung von Papierdatenträgern die Sicherheitsstufen P4 bis P7 vorgesehen.

Sollen die anfallenden Papierschnipsel im normalen Hausmüll/Papiertonne entsorgt werden, sehen wir einen Schredder mit Sicherheitsstufe P5 als erforderlich an. Zum einen ist die Sicherheitsstufe P5 ohnehin nach der DIN 66399 empfohlen für Datenträger mit geheim zuhaltenden Daten (d. h. für Daten, die einem Berufsgeheimnis unterliegen). Zum anderen wäre die Mindest-Sicherheitsstufe P4 auch deshalb nicht ausreichend, weil sich z. B. in der Abfalltonne einer Kanzlei überwiegend Papierschnipsel aus

dieser Kanzlei befinden, was eine etwaige Rekonstruktion erleichtern könnte.

10

Versicherungswirtschaft und Banken

10 Versicherungswirtschaft und Banken

10.1 Datenweitergabe innerhalb der Versicherungsgruppe

In einigen Fällen ist bei Datenweitergabe durch Versicherungen keine Einwilligung erforderlich.

Uns erreichen viele Beschwerden, in denen eine Datenweitergabe durch Versicherungen ohne entsprechende Einwilligung der Versicherten bemängelt wird. In vielen Bereichen sind die Versicherungsunternehmen auf eine Einwilligungs- und Schweigepflichtentbindungserklärung der Versicherten angewiesen, da es bisher keine entsprechende gesetzliche Rechtsgrundlage zur Datenverarbeitung gibt (z. B. bei der Datenerhebung zur Leistungsfallprüfung). Daneben bestehen jedoch einige Konstellationen, in denen für eine Datenverarbeitung keine Einwilligungserklärung erforderlich ist.

Für die Versicherungsbranche gibt es bereits seit 2012 Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft, die auf der Basis des bis zum 25. Mai 2018 geltenden § 38a BDSG genehmigt waren und denen fast alle deutschen Versicherungsunternehmen beigetreten sind.

Diese Verhaltensregeln von 2012 (auch „Verhaltenskodex" oder auf Englisch „Code of Conduct" genannt) wurden im Hinblick auf die DS-GVO geprüft, in materiell-rechtlicher Hinsicht an die neue Rechtslage angepasst und in neuer Fassung am 1. August 2018 vom Gesamtverband der Deutschen Versicherungswirtschaft (GDV) verabschiedet. Auch der neuen Fassung unterwerfen sich zunehmend mehr Versicherungsunternehmen.

Die deutschen Datenschutzaufsichtsbehörden stimmen überein, dass die Versicherungsunternehmen durch die Anwendung dieser Verhaltensregeln die Vorgaben der DS-GVO für die Versicherungswirtschaft branchenspezifisch datenschutzrechtlich zulässig konkretisieren. Da die Verhaltensregeln aber nichts über eine nach Art. 41 DS-GVO vorzusehende Kontrollstelle aussagen, konnten sie nicht durch die zuständige Aufsichtsbehörde als förmliche Verhaltensregeln im Sinne des Art. 40 DS-GVO genehmigt werden. Im Folgenden werden sie daher als „Regelwerk" bezeichnet.

Aus der DS-GVO und dem Regelwerk ergeben sich insbesondere folgende Konstellationen, in denen auch ohne Einwilligung der Versicherten personenbezogene Daten offengelegt oder übermittelt werden dürfen:

- **Gemeinsam nutzbare Stammdaten der Versicherten**

  Gemäß Art. 9 des Regelwerks dürfen die Stammdaten der Versicherten in einem von Mitgliedern der Versicherungsgruppe gemeinsam nutzbaren Datenverarbeitungsverfahren verarbeitet werden.

  Wenn eine betroffene Person mit mindestens einem Unternehmen einer Versicherungsgruppe einen Vertrag geschlossen hat, dürfen auch die anderen Unternehmen dieser Versicherungsgruppe auf die Stammdaten der betroffenen Person zugreifen, soweit dies für den jeweiligen Zweck erforderlich ist (Art. 9 Abs. 1 und 2 des Regelwerks).

  Unter diese Stammdaten fallen die allgemeinen Daten der betroffenen Person wie Name, Adresse, Geburtsdatum, Kundennummer, Angaben über die Art der bestehenden Verträge (wie Vertragsstatus, Beginn- und Ablaufdaten, Versicherungsnummern) und Werbe- und andere Widersprüche, vgl. Ziff. II „Begriffsbestimmungen" des Regelwerks.

- **Auftragsverarbeitung**

  Neben diesem gemeinsamen Zugriff auf die Stammdaten durch ein gemeinsam nutzbares Verarbeitungsverfahren können die Unternehmen einer Versicherungsgruppe gemäß Art. 21 des Regelwerks auch im Rahmen einer Auftragsverarbeitung im Sinne des Art. 28 DS-GVO ein anderes Unternehmen der Versicherungsgruppe mit der Verarbeitung personenbezogener Daten ihrer Versicherten beauftragen.

  Dies geschieht häufig, um wesentliche Inhalte der Versicherungsverträge, wie insb. die Vertrags- und Leistungsbearbeitung, zentral in der Versicherungsgruppe wahrzunehmen. Für diese Auftragsverarbeitung ist keine Einwilligung der betroffenen Versicherten erforderlich, da es sich nicht um eine Datenübermittlung handelt. Vielmehr bleibt das Unternehmen, das Vertragspartner der betroffenen Person ist, Verantwortlicher im Sinne der DS-GVO, sodass sich die betroffenen Personen insb. zur Ausübung ihrer Betroffenenrechte stets an ihren Vertragspartner wenden können.

  Art. 28 DS-GVO stellt hohe Anforderungen an die zwischen dem verantwortlichen Unternehmen und dem Auftragsverarbeiter zu schließende Vereinbarung zur Auftragsverarbeitung, um den Schutz der personenbezogenen Daten der betroffenen Personen sicherzustellen. Art. 21 des Regelwerks konkretisiert diese Anforderungen der DS-GVO und verpflichtet die Versicherungsunternehmen u. a. dazu, stets eine aktuelle Liste der Auftragsverarbeiter bereitzuhalten. Gemäß Art. 21 Abs. 3 Satz 5 des Regelwerks muss bei Erhebung personenbezogener Daten bei der betroffenen Person grundsätzlich über diese Dienstleisterliste informiert werden. Außerdem können die Versicherten von ihrem Vertragspartner auch über diese Dienstleister gemäß Art. 23 Abs. 3 Satz 4 des Regelwerks Auskunft verlangen. In der Regel ist die Dienstleisterliste online in den Datenschutzhinweisen der jeweiligen Versicherungsunternehmen enthalten und somit jederzeit für die Versicherten einsehbar.

- **Datenübermittlung zur Vertragserfüllung**

  Soweit es sich nicht um besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DS-GVO handelt (insb. Gesundheitsdaten), können personenbezogene Daten außerdem gemäß Art. 22 Abs. 1 des Regelwerks an Dienstleister übermittelt werden, soweit dies zur Erfüllung des Versicherungsvertrags erforderlich ist. Hierunter fällt vor allem auch die Übermittlung an Sachverständige zur selbstständigen Begutachtung des Versicherungsfalls.

  Gesundheitsdaten und andere besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DS-GVO dürfen zur Vertragserfüllung nur auf Grundlage einer Einwilligungs- und Schweigepflichtentbindungserklärung übermittelt werden (Art. 22 Abs. 10 des Regelwerks).

10.2 Videoidentifizierung und Ausweiskopien

Durch Onlineübertragung kann eine Fernidentifikation von Personen durchgeführt werden.

Bei reinem Online- oder Telefon-Banking stellt sich die Frage, wie eine sichere Identifizierung von Personen für die Kundenvertragsbeziehung sowie die gesetzlich vorgeschriebene Geldwäscheprüfung nach dem Geldwäschegesetz

möglichst verbraucherfreundlich durchgeführt werden kann.

Identifikationsverfahren mit Medienbruch, wie das Postident-Verfahren bei einer Postfiliale, haben den Nachteil einer zeitlichen Verzögerung und schaffen Probleme für mobilitätseingeschränkte Menschen. Der Einsatz des „elektronischen Personalausweises" zur Online-Identifikation ist in der Praxis noch wenig verbreitet. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat deshalb in ihrem Rundschreiben Nr. 3/2017 (GW) vom 10.04.2017 an alle Kreditinstitute ein Verfahren zur Online-Videoidentifizierung dargestellt, das bei Einhaltung der darin genannten Rahmenbedingungen die finanzaufsichtlichen und geldwäscherechtlichen Identifizierungsanforderungen aus BaFin-Sicht erfüllt.

Für eine Teilnahme an dem Videoidentifizierungsverfahren müssen betroffene Personen ihr ausdrückliches Einverständnis dazu erklären, dass der gesamte Identifizierungsprozess sowie Fotos der Person und ihres Ausweisdokuments aufgezeichnet werden. Andernfalls müssen sie ein anderes Identifizierungsverfahren gegenüber ihrem Vertragspartner wählen.

Wenn die von der BaFin vorgegebenen Rahmenbedingungen eingehalten werden, haben auch wir aus Sicht des Datenschutzes keine Bedenken gegen diese Art der Identifikation.

Siehe BaFin-Rundschreiben:

www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1703_gw_videoident.html

11

Auskunfteien

11 Auskunfteien

11.1 Bewertung von Auskunfteien nach der DS-GVO

Auskunfteien dürfen auch unter Geltung der DS-GVO finanzrelevante Daten zu Verbrauchern speichern und bei berechtigten Anfragen übermitteln.

Die Geschäftstätigkeit der Auskunfteien kann auch nach der DS-GVO datenschutzkonform durchgeführt werden.

Nach Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO ist eine Verarbeitung personenbezogener Daten rechtmäßig, wenn die Verarbeitung zur Wahrung der berechtigten Interessen eines Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Das Interesse der kreditgebenden Wirtschaft sowie der Allgemeinheit an der Vermeidung von Zahlungsausfällen infolge Kreditgewährungen an Zahlungsunfähige und Zahlungsunwillige sowie die Verhinderung von Kreditbetrug ist grundsätzlich ein berechtigtes Interesse in diesem Sinne.

Wenn eine betroffene Person kreditorische Leistungen in Anspruch nehmen will, wie z. B. Bankkredite, Warenlieferungen gegen offene Rechnung usw., kann sie regelmäßig keine überwiegenden Interessen gegen eine Prüfung ihrer Bonität bzw. Kreditwürdigkeit durch den Gläubiger durch Abfrage finanzrelevanter Daten bei einer Auskunftei geltend machen und muss dies grundsätzlich hinnehmen.

Siehe ergänzend zur Einmeldung offener und unbestrittener Forderungen in eine Wirtschaftsauskunftei unter Geltung der DS-GVO den Beschluss der Datenschutzkonferenz vom 23.03.2018:

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

11.2 Verhaltensregeln der Auskunfteien zu Prüf- und Löschfristen

Auskunfteien haben in Abstimmung mit den Datenschutzaufsichtsbehörden Prüf- und Löschfristen für gespeicherte personenbezogene Daten festgelegt.

Im Gegensatz zum früheren BDSG enthält die DS-GVO keine konkreten Prüf- und Löschfristen zu bei Wirtschaftsauskunfteien gespeicherten personenbezogenen Daten.

Damit Wirtschaftsauskunfteien, deren angeschlossene Unternehmen sowie die betroffenen Personen weiterhin Orientierungswerte zur Speicherdauer und Löschung finanzrelevante personenbezogener Daten bei Auskunfteien haben, wurden zwischen dem Verband „Die Wirtschaftsauskunfteien e.V." und den Datenschutzaufsichtsbehörden Verhaltensregeln verhandelt, die die für den Verband zuständige Aufsichtsbehörde, die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, genehmigt hat.

Darin sind für verschiedene Datengruppen, wie z. B. für fällige, offene und unbestrittene Forderungen, für Eintragungen im Schuldnerverzeichnis oder für Veröffentlichungen zu Insolvenzverfahren Prüf- und Löschfristen für die betreffenden Daten festgelegt worden.

Die LDI NRW hat diese Verhaltensregeln und ihre Genehmigung veröffentlicht unter:

www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Verhaltensregeln-_-Code-of-Coduct/

12

Werbung und Adresshandel

12 Werbung und Adresshandel

12.1 Neue Orientierungshilfe der Aufsichtsbehörden

Eine an die DS-GVO angepasste Orientierungshilfe zur werblichen Verarbeitung personenbezogener Daten steht zur Verfügung.

In einer zweitägigen Sitzung am 6. und 7. März 2018 hat die Arbeitsgruppe „Werbung und Adresshandel" der Datenschutzaufsichtsbehörden unter unserer Leitung die bisherigen Anwendungshinweise aus dem Jahre 2014 zur Verarbeitung personenbezogener Daten für werbliche Zwecke unter Berücksichtigung der DS-GVO-Regelungen überarbeitet und in einem anschließenden schriftlichen Verfahren weiter abgestimmt.

Die DSK hat den neuen Text als „Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO)" mit dem Datum vom 7. November 2018 veröffentlicht.

Die neue Orientierungshilfe ist auf der DSK-Website abrufbar:

www.datenschutzkonferenz-online.de/media/oh/20181107_oh_werbung.pdf

12.2 Weihnachts-, Neujahrs- und sonstige Glückwunschkarten

Die Versendung von Weihnachts-, Neujahrs- und sonstigen Glückwunschkarten wird durch die DS-GVO nicht verhindert.

Die allgemeine Verunsicherung nach dem Wirksamwerden der DS-GVO hat gegen Ende des Jahres 2018 zu einer Reihe von Anfragen bei uns geführt, ob denn die Versendung von Weihnachts- und Neujahrswunschkarten an Kunden noch datenschutzrechtlich erlaubt sei.

Nach dem von der Rechtsprechung sehr weit definierten Begriff der Werbung sind Weihnachts- und Neujahrswunschkarten von Firmen an ihre Geschäftspartner als werbliche Maßnahmen anzusehen, die dem Aufbau und der Pflege von Geschäftsbeziehungen dienen und damit das Geschäft fördern sollen.

Allerdings steht das Datenschutzrecht mit der Regelung in Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO der Verwendung von Postadressdaten für die Zusendung von Weihnachts-, Neujahrs- und sonstigen Glückwunschkarten durch Firmen regelmäßig nicht entgegen, solange eventuelle Werbewidersprüche beachtet werden.

Wenn bei bestehenden Geschäfts- oder Kundenbeziehungen die gesetzlich vorgesehenen Informationen nach Art. 13 und Art. 21 Abs. 4 DS-GVO schon im Laufe des Jahres erfolgt sind, können diese Informationen bei den Weihnachts- oder Neujahrsgrüßen unterbleiben (wo sie ohnehin nur störend wirken würden).

12.3 Zustimmung zur Werbung und Koppelungsverbot

Kostenlose E-Mail-Accounts mit einer dazu vereinbarten Werbe-Newsletter-Zusendung sind weiterhin möglich.

In der Praxis gibt es vielfach kostenlose Dienstleistungsangebote, die die Nutzer mit der Zustimmung für eine werbliche Nutzung ihrer Daten „bezahlen", z. B. ein kostenloser E-Mail-Account gegen die Zustimmung für Werbe-Newsletter-Zusendung als „Gegenfinanzierung".

Hierzu wird in Fachkreisen intensiv diskutiert, ob ein solches Geschäftsmodell unter Geltung der DS-GVO noch zulässig ist oder wegen einer nicht freiwillig erteilten Einwilligung zur Verarbeitung der betreffenden personenbezogenen Daten gegen das sog. Koppelungsverbot nach Art. 7 Abs. 4 DS-GVO verstößt.

Wir gehen bei solchen Geschäftsmodellen von einer vertraglichen Grundlage für die Verarbeitung der personenbezogenen Daten gemäß Art. 6 Abs. 1 Satz 1 Buchstabe b DS-GVO aus, wenn die ausbedungene Gegenleistung des Nutzers, d. h. die Zustimmung zur Verarbeitung seiner Daten für die Zusendung eines Werbe-Newsletters, bei Vertragsabschluss über die vereinbarte kostenlose Dienstleistung klar und verständlich dargestellt wird und damit ein Nutzer eine sachgerechte Entscheidungsgrundlage hat.

Ähnlich sieht das auch eine in Italien ergangene Entscheidung zur Frage eines „Koppelungsverbots". Das Urteil vom 2. Juli 2018 des Kassationsgerichtshofs mit Nr. 17278/2018 ist online abrufbar:

www.italgiure.giustizia.it/xway/application/nif/clean/hc.dll?verbo=attach&db=snciv&id=./20180702/snciv@s10@a2018@n17278@tS.clean.pdf

13

Handel und Dienstleistung

13 Handel und Dienstleistung

13.1 Kopieren von Personalausweisen

Eine Kopie des Personalausweises ist nicht in jedem Fall erforderlich und nur mit Zustimmung des Ausweisinhabers zulässig.

Ein datenschutzrechtliches Dauerthema ist und bleibt das Kopieren von Personalausweisen, zu dem uns auch im Berichtszeitraum viele Beschwerden erreichten. Das Thema hat aufgrund einer Änderung der einschlägigen Vorschriften des Personalausweisgesetzes im Jahr 2017 neue Facetten erhalten. § 20 Abs. 2 des Personalausweisgesetzes (PAuswG) lautet nunmehr:

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

Mehrere Beschwerdeführer monierten, dass Unternehmen ihren Personalausweis kopiert hätten oder zumindest kopieren wollten. Entsprechende Beschwerden erreichten uns von Hotelgästen, aber auch von Personen, die als Besucher oder Lieferanten durch den Sicherheits-/Pfortendienst von Unternehmen aufgefordert wurden, ihren Personalausweis kopieren zu lassen.

Durch den geänderten § 20 Abs. 2 PAuswG ist nun klargestellt, dass der Personalausweis nicht ohne Zustimmung des Inhabers kopiert werden darf – niemand darf somit den Ausweisinhaber zwingen, seinen Ausweis zu kopieren oder kopieren zu lassen.

Der datenschutzrechtliche Streit hat sich dadurch allerdings nicht erledigt, sondern lediglich verlagert, denn gemäß § 20 Abs. 2 Satz 4 PAuswG bleiben die allgemeinen datenschutzrechtlichen Vorschriften unberührt, sodass auch dann, wenn die betroffene Person mit der Kopie einverstanden ist, dennoch der Grundsatz der Datenminimierung gilt. Es ist daher zu fragen, welche Daten aus dem Personalausweis der Verantwortliche tatsächlich benötigt. Hierbei ist zu bedenken, dass der Wunsch zur Erstellung einer Kopie des Personalausweises meist dazu dient, die Identität der betroffenen Person zu dokumentieren, beispielsweise um nachvollziehen zu können, welche externen Personen zu einem bestimmten Zeitpunkt das Betriebsgelände eines Unternehmens betreten haben. Indessen können die zur Identifikation benötigten Daten (Name, Vorname, Adresse, Geburtsdatum) auch dadurch gewonnen werden, dass das Pfortenpersonal sich den Personalausweis vorzeigen lässt und die o. g. zur Identifizierung erforderlichen – aber auch ausreichenden – Daten daraus notiert. Eine Kopie hätte demgegenüber das Problem, dass auch darüber hinausgehende und somit nicht erforderliche Daten erhoben würden (z. B. die Ausweisnummer oder die sog. Zugangsnummer), was dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 DS-GVO) widerspricht und daher unzulässig ist. Zulässig wäre eine Kopie lediglich dann, wenn darauf alle anderen als die o. g. zur Identifizierung benötigten Daten geschwärzt werden.

Verfolgt der Verantwortliche lediglich den Zweck, die Identität einer Person zu überprüfen, ohne dass Bedarf an der Speicherung/Dokumentation der Identität besteht, genügt es, den Personalausweis einer Sichtprüfung zu unterziehen. Eine Personalausweiskopie ist in solchen Fällen nicht erforderlich.

13.2 Anlegerdaten in Publikumsgesellschaften

Ein Gesellschafter einer Publikumsgesellschaft kann ein legitimes Interesse an der Kenntnis der Identität der Mitgesellschafter haben.

Ein Gesellschafter X eines als GmbH & Co KG organisierten Fonds erhielt ein Anschreiben eines anderen Gesellschafters Y, worin Y dem X anbot, dessen Anteil an der Publikums-KG aufzukaufen. Hiergegen beschwerte sich X bei uns, weil er darin eine unzulässige Verarbeitung seiner Kontaktdaten sah.

Nach unserer Auffassung lag kein datenschutzrechtlicher Verstoß vor. Wie der Bundesgerichtshof in seinem Urteil vom 5.2.2013 - II ZR 134/11 (Ziffer 1.d) bb)) betont, kann bei einer Publikumspersonengesellschaft ein Gesellschafter aus einer Vielzahl von Gründen ein legitimes Interesse an der Kenntnis der Identität seiner Mitgesellschafter und an der Verwendung dieser Information haben. Dementsprechend hatte der Anleger Y von der Gesellschaft die Herausgabe der Daten der anderen Anleger durchgesetzt und anschließend die Daten – jedenfalls des X – offenbar dazu verwendet, dem X ein Angebot zum Ankauf von dessen Geschäftsanteil zu unterbreiten. Nach unserer Auffassung ist dieser Zweck mit dem ursprünglichen Zweck, zu dem der Fonds die Daten der Anleger verarbeitet, vereinbar, sodass kein Verstoß gegen den Grundsatz der Zweckbindung (Art. 5 Abs. 1 Buchstabe b DS-GVO) vorlag. Denn der von Y verfolgte Zweck, seinen Geschäftsanteil durch Hinzukauf weiterer Geschäftsanteile zu vergrößern, hängt verhältnismäßig eng mit dem Zweck der Verwaltung von Geschäftsanteilen zusammen. Es ist nicht ungewöhnlich, wenn ein Anleger seinen Geschäftsanteil vergrößern möchte. Im konkreten Fall war die Übertragbarkeit der Geschäftsanteile im Gesellschaftervertrag auch nicht ausgeschlossen. Der Hinzuerwerb von Geschäftsanteilen war somit etwas, was nach den vertraglichen Bedingungen im Falle des vorliegenden Fonds als möglich vorausgesetzt war.

Vor diesem Hintergrund stellt das Unterbreiten eines Angebots durch einen Anleger an einen anderen Anleger, dessen Anteil zu kaufen, auch keine Datenverarbeitung zu werblichen Zwecken dar, sondern eine Verarbeitung, die die Vergrößerung des eigenen Geschäftsanteils bezweckt und die mit dem Zweck des Haltens eines eigenen Geschäftsanteils noch verhältnismäßig eng zusammenhängt.

Anlegern, denen auf diese Weise ein Angebot von einem anderen Anleger unterbreitet wird, steht es frei, das Angebot anzunehmen oder abzulehnen; sie können gegenüber dem Anbietenden auch erklären, er möge ihnen künftig keine derartigen Angebote mehr machen. Damit bestehen ausreichende Möglichkeiten, mit denen der Anleger seine schutzwürdigen Interessen in diesem Zusammenhang schützen kann.

Das Urteil des BGH vom 5 Februar 2013 ist im Internet abrufbar:

juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=934b5b228003788f371a65f0c6a9c61d&nr=63465&pos=6&anz=23

13.3 Wahrnehmung von Gesellschafterrechten in einer AG

Ein Verein aus Anlegern einer Aktiengesellschaft kann Anspruch auf Nennung von Namen und Anschriften der anderen beteiligten Aktionäre haben.

Ein Aktionär X einer Aktiengesellschaft (AG) hatte gegen die AG die Herausgabe der Namen und Anschriften der anderen Aktionäre gerichtlich durchgesetzt. In der Folge wurden mehrere Aktionäre durch eine als eingetragenen Verein

organisierte Interessengemeinschaft angeschrieben, in der sich einige Aktionäre organisiert hatten. In dem Schreiben warb die Interessengemeinschaft bei den anderen Aktionären um Unterstützung für eine Reihe von Anträgen, die die Interessengemeinschaft in der Gesellschafterversammlung zu stellen plante.

Einige der angeschriebenen Aktionäre sahen in der Verwendung ihrer Adressen durch die Interessengemeinschaft einen Datenschutzverstoß, insbesondere weil der Verein (d. h. die Interessengemeinschaft) als solcher kein Aktionär der AG sei. Sie vermuteten, dass der Aktionär X die Adressen dem Verein zur Verfügung gestellt hatte. Der von uns zur Stellungnahme aufgeforderte Verein erläuterte, die Adressdaten nicht vom Aktionär X, sondern durch Einsichtnahme in das Handelsregister erhalten zu haben.

Das Vorgehen des Vereins war nach unserer Auffassung datenschutzrechtlich nicht zu beanstanden.

Maßgeblich hierfür war, dass nach der höchstrichterlichen Rechtsprechung zur Publikums-KG jeder Anleger, der sich (ggf. auch nur mittelbar über einen Treuhänder) an einer Publikums-KG beteiligt, gegen die Gesellschaft einen Anspruch auf Nennung von Namen und Anschriften der anderen mittelbar und unmittelbar beteiligten Anleger hat (BGH, Urt. v. 05.02.2013 – II ZR 134/11). Diese Rechtsprechung sehen wir grundsätzlich auch auf eine Aktiengesellschaft wie vorliegend entsprechend anwendbar. Der Verein war hier zwar nicht selbst Anleger der AG, jedoch war er nach seinem Zweck nur ein Instrument, mit dessen Hilfe einige der Aktionäre ihre Interessen gegenüber der AG gemeinsam wahrnahmen. Eine gemeinsame Wahrnehmung von Gesellschafterrechten ist in der Rechtsprechung als berechtigtes Interesse des einzelnen Gesellschafters anerkannt. Der Verein warb in seinem Schreiben um die Erteilung einer Vollmacht für die Ausübung des Stimmrechts zu einer Hauptversammlung; dieser Verarbeitungszweck bewegt sich eindeutig im Rahmen des Zwecks der – legitimen – gemeinsamen Wahrnehmung von Gesellschafterinteressen.

Die zu diesem Zweck vorgenommene Verarbeitung der Namens- und Anschriftendaten der anderen Aktionäre durch die im Verein organisierten Aktionäre war damit datenschutzrechtlich nach Art. 6 Abs. 1 Buchstabe f DS-GVO zulässig, weil sie der gemeinsamen Wahrnehmung von Gesellschafterrechten diente. Die angeschriebenen Aktionäre müssen dies hinnehmen, d. h. überwiegende schutzwürdige Interessen ihrerseits stehen dem nicht entgegen. Dies gilt auch dann, wenn die handelnden Aktionäre einen Verein gründen, dessen Zweck die gemeinsame Wahrnehmung ihrer Gesellschafterrechte in der betreffenden AG ist und zu diesem Zweck die personenbezogenen Daten der anderen Anleger – rechtlich gesehen – an den Verein übermitteln. Der Verein diente insoweit der leichteren Handhabung der Angelegenheit und verfolgte keine über die gemeinsame Wahrnehmung von Gesellschafterrechten hinausgehenden Zwecke.

13.4 Unrichtige Kundendaten bei Energieversorgern

Energieversorger müssen ihrer Verantwortung gerecht werden und sicherstellen, dass die verarbeiteten, personenbezogenen Kundendaten richtig sind.

Mehrfach erreichten uns Beschwerden von Kunden von Energieversorgern, die eine Verarbeitung unrichtiger Daten zu ihrer Person durch den Energieversorger monierten. So trugen Beschwerdeführer vor, von einem Versorgungsunternehmen als Kunde für einen bestimmten Versorgungsanschluss (z. B. für Strom) geführt zu werden, obwohl sie mit der betreffenden Wohnung nichts zu tun hätten.

Unsere Ermittlungen in solchen Fällen zeigten, dass die Gründe, die zu solchen Verwechslungen bzw. unrichtigen Datenbeständen führen,

sehr vielgestaltig sind. In einigen Fällen lag Namensgleichheit zwischen dem Eingabeführer und dem tatsächlichen Anschlussinhaber vor. In einem der bearbeiteten Fälle stellte sich heraus, dass ein Mitarbeiter des Versorgungsunternehmens in einem Fall, in dem das Unternehmen über keine zustellfähige Adresse des Kunden (Anschlussinhabers) mehr verfügte, schlicht den Namen des Kunden „googelte" und dann die Rechnung an eine Person mit gleichem Vor- und Nachnamen schickte, der ausweislich des Suchergebnisses in demselben Ort wohnte, in dem sich die Anschlussstelle befand. Dabei handelte es sich jedoch nicht um den Anschlussinhaber.

Ein derartiges Vorgehen entspricht nicht den datenschutzrechtlichen Anforderungen. Der Verantwortliche unterliegt dem Grundsatz der Datenrichtigkeit (Art. 5 Abs. 1 Buchstabe d DS-GVO) und muss gemäß Art. 5 Abs. 2 und 24 Abs. 1 DS-GVO geeignete technische und organisatorische Maßnahmen implementieren, um sicherzustellen, dass die verarbeiteten personenbezogenen Daten richtig sind. Das „Googeln" nach namensgleichen Personen und die Verwendung der so aufgefundenen Daten zum Zwecke der Rechnungstellung sind keine Maßnahme, die in hinreichendem Maße sicherstellen, dass die verarbeiteten Daten richtig sind.

Allerdings hatte der Mitarbeiter im konkreten Fall eigenmächtig gegen existierende anderslautende schriftliche Anweisungen zum Umgang mit solchen Fällen gehandelt. Wir haben dem Unternehmen nachdrücklich nahegelegt, die Mitarbeiter zu diesem Thema laufend zu sensibilisieren.

13.5 Rechnungen vom Energieversorger an Nachlasspfleger

Verantwortliche benötigen einen zuverlässigen Prozess zum Umgang mit Ansprüchen betroffener Personen auf Datenberichtigung.

Ein Nachlasspfleger erhielt von einem Energie-(Strom-)Versorger eine offene Rechnung bezüglich einer Immobilie (Verbrauchsstelle), die einem Erblasser gehörte, für dessen Nachlass der Nachlasspfleger bestellt war. Trotz mehrfacher Erklärung gegenüber dem Versorgungsunternehmen, dass er lediglich Nachlasspfleger sei und als solcher rechtlich nicht für die offenen Verbindlichkeiten des Erblassers hafte, erhielt der Nachlasspfleger über ein Jahr lang laufend an ihn persönlich gerichtete Zahlungsaufforderungen des Energieversorgers sowie die Androhung, die Forderung an ein Inkassounternehmen abzutreten und an eine Auskunftei zu melden.

Das Unternehmen hatte in dem Datensatz des Erblassers fälschlicherweise den Nachlasspfleger als Rechtsnachfolger/Erben eingetragen. Erst nach unserer Intervention erkannte das Unternehmen seinen Fehler und berichtigte den unrichtigen Datensatz.

Dies ist ein Beispiel dafür, wie auf den ersten Blick kleine Bearbeitungsfehler beim Umgang mit personenbezogenen Daten zu sachlich unrichtigen Daten führen, die für die betroffene Person mit erheblichen Unannehmlichkeiten – Zeitaufwand und Befürchtung, bei einer Auskunftei gemeldet zu werden – verbunden sein können. Im vorliegenden Fall war das Unternehmen augenscheinlich nicht in der Lage, den mehrfach vorgetragenen Argumenten des Nachlasspflegers Rechnung zu tragen und den entsprechenden Datensatz zu berichtigen.

Dies entspricht nicht den Anforderungen der DS-GVO an technische und organisatorische Maßnahmen. Dem Verantwortlichen mangelte es offenbar an einem ausreichend zuverlässigen Prozess zum Umgang mit Ansprüchen betroffener Personen auf Datenberichtigung nach Art. 16 DS-GVO. Hätte es einen ausreichend klar definierten Prozess gegeben, hätte der Verantwortliche den Fehler bereits nach der entsprechenden Aufforderung zur Datenberichtigung durch den Betroffenen entdecken und korrigieren können.

13.6 Daten bei anerkannten Stellen im Sinne der Luftverkehrs-Ordnung

Die Speicherung von Personalausweiskopien im Rahmen der Prüfungsdurchführung bei anerkannten Stellen ist unzulässig.

Für die Steuerung eines sog. unbemannten Fluggeräts mit Startmasse von mehr als 2 kg muss der Steuerer im Wege einer Prüfung eine Bescheinigung zum Nachweis ausreichender Kenntnisse und Fertigkeiten erwerben (§ 21 a Abs. 3 Satz 3 Nr. 2 LuftVO). Diese Prüfung wird gemäß § 21d Abs. 2 LuftVO bei einer sog. anerkannten Stelle abgelegt; hierbei handelt es sich um Stellen, die vom Luftfahrt-Bundesamt als für die Prüfungsdurchführung und Erteilung der Bescheinigung geeignet anerkannt wurden.

Ein Eingabeführer beschwerte sich darüber, dass eine anerkannte Stelle von ihm bei der Abnahme der Prüfung eine Kopie seines Personalausweises sowie die Vorlage eines Führungszeugnisses verlangte. Dies haben wir als unzulässig bewertet. § 21d Abs. 3 LuftVO besagt lediglich, dass der Prüfungsteilnehmer ein gültiges Identitätsdokument sowie (bei erstmaliger Bewerbung um eine Bescheinigung) ein Führungszeugnis nach § 30 Abs. 1 BZRG vorlegen muss. Eine Pflicht zur Erstellung und Aufbewahrung einer Kopie dieser Dokumente lässt sich der genannten gesetzlichen Vorschrift hingegen nicht entnehmen.

Die anerkannte Stelle argumentierte, dass die Anforderung und Speicherung dieser Unterlagen laut einem entsprechenden „Handbuch des Luftfahrt-Bundesamtes" für die Abnahme der Prüfungen so vorgesehen sei. Wir nahmen daraufhin Kontakt zu der für das Luftfahrt-Bundesamt zuständigen Datenschutzaufsichtsbehörde – die Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) – auf und baten um Beurteilung, ob das Luftfahrt-Bundesamt seinerseits von den anerkannten Stellen die Speicherung dieser Dokumente bzw. der darin enthaltenen personenbezogenen Daten verlangen dürfe. Dies wurde von der BfDI mit Berufung auf den Wortlaut des § 21d Abs. 3 LuftVO verneint. Die Speicherung der Kopien der Ausweisdokumente bzw. der darin enthaltenen Daten erfolgte somit ohne Rechtsgrundlage und war unzulässig.

Die BfDI teilte zudem mit, dass sie mit dem Luftfahrt-Bundesamt Kontakt aufnehmen werde, um dafür Sorge zu tragen, dass die entsprechenden Ausführungen im Handbuch des Luftfahrt-Bundesamtes angepasst werden, sodass anerkannte Stellen in den o. g. Fällen künftig nicht mehr Personalausweiskopien und Führungszeugnisse der Prüfungsteilnehmer speichern.

13.7 Datenübermittlung von Reisebüros an Reiserücktrittsversicherung

Nur auf ausdrücklichen Kundenwunsch dürfen Reisebüros die Kundendaten an Reiserücktrittsversicherungen übermitteln.

Der Kunde eines Reisebüros beschwerte sich bei uns darüber, dass das von ihm mit der Organisation einer Pauschalreise beauftragte Reisebüro seine personenbezogenen Daten an ein

Versicherungsunternehmen übermittelt hatte, das eine Reiserücktrittsversicherung anbot. Er war von dem Versicherungsunternehmen angeschrieben worden, das davon ausging, dass er eine solche Versicherung beantragt hatte. Tatsächlich hatte der Kunde jedoch nicht erklärt, eine Reiserücktrittsversicherung abschließen zu wollen.

Unsere Überprüfung ergab, dass das Reisebüro sich offenbar nicht in ausreichendem Maße darüber im Klaren war, dass es Daten eines Kunden nur dann an das mit ihm kooperierende Versicherungsunternehmen übermitteln darf, wenn der Kunde den Abschluss einer Reiserücktrittsversicherung wünscht. Das Reisebüro hatte kürzlich ein neues Buchungssystem eingeführt und dabei augenscheinlich vorgesehen, dass bei Buchung einer Pauschalreise die Daten des Kunden automatisch an das die Reiserücktrittsversicherung anbietende Versicherungsunternehmen übermittelt werden. Im Rahmen unserer Prüfung erklärte das Reisebüro, es sei schließlich nach Art. 250 § 3 Nr. 8 EGBGB gesetzlich verpflichtet, dem Kunden bei Vermittlung einer Pauschalreise den Abschluss einer Reiserücktrittsversicherung anzubieten.

Diese Übermittlung war datenschutzrechtlich eindeutig unzulässig. Wir erläuterten dem Reisebüro, dass es keinesfalls die Daten aller Pauschalreisekunden an den Anbieter der Reiserücktrittsversicherung übermittelt darf, sondern nur die Daten derjenigen Kunden, die im Rahmen der Buchung der Pauschalreise tatsächlich den Abschluss einer Reiserücktrittsversicherung wünschen. Auch aus Art. 250 § 3 Nr. 8 EGBG ergibt sich nicht Gegenteiliges, da hiernach das Reisebüro dem Kunden den Abschluss einer Reiserücktrittsversicherung lediglich anbieten muss, dies jedoch noch nicht gleichbedeutend damit ist, dass tatsächlich ein Versicherungsvertrag zustande kommt. Der Buchungsprozess muss so gestaltet sein, dass Daten von Kunden nur und erst dann an den Versicherer übermittelt werden, wenn der Kunde erklärt, eine Reiserücktrittsversicherung abschließen zu wollen.

13.8 Datenübermittlung durch Auftragsverarbeiter aufgrund einstweiliger Verfügung

Eine einstweilige Verfügung kann eine fehlende Weisung des Verantwortlichen, Daten durch den Auftragsverarbeiter auf einen anderen Verantwortlichen zu übertragen, ersetzen.

Ein Steuerberaterbüro X, das Steuerberatungsleistungen und Lohnbuchhaltung für eine Apotheke durchführte, nahm einen IT-Dienstleister als Auftragsverarbeiter in Anspruch, auf dessen Servern die entsprechenden Daten gespeichert waren. Das Steuerberaterbüro X beschwerte sich bei uns darüber, dass der IT-Dienstleister ohne Zustimmung des Steuerbüros den Datensatz zu der betreffenden Apotheke auf ein anderes Steuerberaterbüro Y übertragen hatte. Vorausgegangen war eine von der Apotheke gegen das erste Steuerberaterbüro X erstrittene einstweilige Verfügung, wodurch das Steuerberaterbüro X verpflichtet wurde, der Übertragung des Datensatzes auf das neue Steuerberaterbüro Y zuzustimmen. Diese einstweilige Verfügung hatte die Apotheke durch den Gerichtsvollzieher direkt dem IT-Dienstleister vorgelegt, der daraufhin den Datensatz an Y übertragen hatte, indem er die vormaligen Zugriffsrechte des Steuerberaterbüros X aufhob und nunmehr dem Steuerberaterbüro Y Zugriffsrechte einräumte.

Die einstweilige Anordnung war einige Monate später in der zweiten Instanz aufgehoben worden. X sah nun in der zwischenzeitlich auf Basis der einstweiligen Anordnung erfolgten Übertragung der Daten durch seinen Auftragsverarbeiter an Y ein eigenmächtiges Handeln des Auftragsverarbeiters und damit einen Verstoß gegen die Pflicht des Auftragsverarbeiters, nur gemäß den Weisungen des Verantwortlichen zu handeln (Art. 28 Abs. 2 Satz 2 Buchstabe a DS-GVO).

Nach unserer Bewertung hatte sich der Auftragsverarbeiter datenschutzrechtlich korrekt verhalten. Zwar hatte der Verantwortliche – sein Auftraggeber, das Steuerberaterbüro X – der Übertragung der Daten an Y nicht zugestimmt, sodass keine Weisung von X zur Übertragung des Datenbestands vorlag. Die von der Apotheke erstrittene einstweilige Verfügung fingierte jedoch entsprechend § 894 ZPO die (fehlende) Zustimmungserklärung zur Übertragung des Datenbestands; zwar ist in der zivilrechtlichen Literatur die analoge Anwendung der Zustimmungsfiktion nach § 894 ZPO auf eine einstweilige Verfügung streitig; im konkreten Fall hatte jedoch das zuständige Gericht eine solche einstweilige Verfügung getroffen. Der Auftragsverarbeiter handelte somit bei der Datenübertragung nicht ohne oder entgegen der Weisung seines Auftragsverarbeiters, sondern die einstweilige Verfügung ersetzte die fehlende Weisung des Verantwortlichen, wonach die Daten auf Y zu übertragen sind.

13.9 Verweigerung der Herausgabe von Informationen über Datenabruf

Plattformbetreiber müssen grundsätzlich Kunden die Herausgabe von Informationen über Datenabrufe anderer Kunden verweigern.

Ein Unternehmen bietet eine Internetplattform an, bei der unter Eingabe der Fahrzeugidentifikationsnummer (FIN) kostenpflichtig eine Fahrzeughistorie (Report) von in den USA zugelassenen Fahrzeugen abgerufen werden kann. Das Angebot ist registrierungspflichtig, d. h. der Abrufende muss seinen Namen angeben. Die Plattform ist vor allem für Käufer von aus den USA importierten Gebrauchtwagen interessant.

Ein Kunde kaufte bei einem deutschen Händler ein solches Fahrzeug; der Händler legte dem Kunden einen – dem Anschein nach aus der o. g. Datenbank stammenden – an einem bestimmten Tag X abgerufenen Report über das betreffende Fahrzeug vor, der keine Vorschäden für das Fahrzeug auswies. Nachdem der Kunde mehrere Mängel des Fahrzeugs festzustellen glaubte, rief er selbst in der genannten Datenbank anhand der FIN den Report zu dem Fahrzeug ab und stellte fest, dass dieser erheblich von dem Report abwich, den ihm der Händler vorgelegt hatte. Der Kunde vermutete, dass ihm der Händler einen gefälschten Report vorgelegt hatte und wollte nunmehr von dem Plattformbetreiber wissen, ob zu diesem Fahrzeug am Tag X ein Abruf des Reports in der Datenbank stattgefunden hatte. Der Plattformbetreiber verweigerte die Auskunft mit dem Hinweis auf Datenschutz.

Der Kunde frage uns, ob der Plattformbetreiber ihm die Informationen tatsächlich aus Datenschutzgründen nicht herausgeben dürfe. Der Plattformbetreiber hatte sich datenschutzrechtlich korrekt verhalten. Auch wenn aus dem Abruf der Name des Abrufenden nicht unmittelbar erkennbar ist, wäre zumindest für den Plattformbetreiber die Identität des Abrufenden bekannt, sodass es sich insoweit um personenbezogene Daten handelt. Schon die Information, dass an einem bestimmten Tag zu dem betreffenden Fahrzeug (FIN) ein Abruf stattgefunden hat, ist damit als personenbezogenes Datum anzusehen. Grundsätzlich haben Nutzer der Plattform die berechtigte Erwartung, dass der Plattformbetreiber als Verantwortlicher diese Information nicht an Dritte weitergibt. Selbst wenn der Kunde im vorliegenden Fall möglicherweise ein nachvollziehbares Interesse daran hat, zu wissen, ob am dem besagten Tag X tatsächlich ein Abruf zu diesem Fahrzeug stattgefunden hat, muss dieses Interesse gegenüber dem Interesse der betroffenen Person an der vertraulichen Nutzung der Internetplattform zurückstehen. Die Datenübermittlung durch den Plattformbetreiber wäre daher nicht zulässig, auch nicht auf Grundlage von Art. 6 Abs. 1 Buchstabe f DS-GVO, da schutzwürdige Interessen der betroffenen Person am Unterbleiben der

Übermittlung überwiegen. Dem (möglicherweise) geprellten Kunden steht es freilich frei, auf zivilrechtlichem Wege seine Interessen zu verfolgen und ggf. dort Beweiserhebung betreffend des besagten Abrufs aus der Datenbank zu beantragen.

14

Internationaler Datenverkehr

14 Internationaler Datenverkehr

14.1 Standardvertrag und Auftragskette

Auftragsverarbeiter dürfen nicht ohne Weiteres Unterauftragsverarbeiter einsetzen, sondern müssen dabei einige Vorschriften berücksichtigen.

Bereits in unserem 5. Tätigkeitsbericht für 2011/2012 hatten wir unter Ziff. 12.1 berichtet, dass wir mehrfach festgestellt hatten, dass der Umgang mit den Standardvertragsklauseln für Auftragsverarbeiter vielen Unternehmen bei Auftragsketten Probleme bereitet. Besonders fehleranfällig ist die Konstellation, bei der ein in der EU niedergelassener Auftragsverarbeiter einen oder mehrere Unterauftragsverarbeiter in Drittländern ohne angemessenes Datenschutzniveau in die Auftragserbringung einschaltet. Auf diese Konstellation sind die EU-Standardvertragsklauseln für Auftragsverarbeiter (Kommissionsbeschluss 2010/87/EU) nicht zugeschnitten, vielmehr setzen diese einen nicht in der EU niedergelassenen Auftragsverarbeiter (nachfolgend: „Non-EU-Auftragsverarbeiter") voraus, sodass die „Lösung" in solchen Fällen nur so aussehen kann, dass der EU-Verantwortliche die Standardvertragsklauseln selbst mit dem Unterauftragsverarbeiter abschließt.

Dies wird von vielen Unternehmen nach wie vor als umständlich kritisiert. Es besteht aber kein anderer Lösungsweg – jedenfalls keiner, der ohne Genehmigung der Aufsichtsbehörden auskäme –, solange keine EU-Standardvertragsklauseln für diese Fallkonstellation zur Verfügung stehen.

Mehrfach haben wir im Berichtszeitraum feststellen müssen, dass dennoch in solchen Fällen der erste (d. h. der in der EU niedergelassene) Auftragsverarbeiter selbst – also als Datenexporteur – die o. g. Standardvertragsklauseln mit dem „Non-EU-Unterauftragsverarbeiter" abschließt. Dies mag naheliegen, weil es leicht handhabbar ist, führt jedoch zu einem datenschutzrechtlichen Verstoß, da der EU-Auftragsverarbeiter sich somit als Verantwortlicher geriert, was nicht den Tatsachen entspricht. Nur Verantwortliche können die EU-Standardvertragsklauseln für Auftragsverarbeiter (KOM-Beschluss 2010/87/EU) als Datenexporteure abschließen. Dieses Vorgehen führte in einem untersuchten Fall noch zu einem weiteren Problem: Der EU-Auftragsverarbeiter informierte die Verantwortlichen überhaupt nicht darüber, dass er die Daten an einen Unterauftragsverarbeiter weiterleitet. Dies widerspricht Art. 28 Abs. 2 Satz 1 DS-GVO, wonach der (erste) Auftragsverarbeiter einen weiteren Auftragsverarbeiter nur mit einer vorher eingeholten gesonderten oder allgemeinen schriftlichen Genehmigung des Verantwortlichen einschalten darf; wenn der Verantwortliche eine lediglich allgemeine Genehmigung erteilt hat, muss der Auftragsverarbeiter den Verantwortlichen gemäß Art. 28 Abs. 2 Satz 2 DS-GVO immer über jede beabsichtigte Hinzuziehung oder Ersetzung eines weiteren Auftragsverarbeiters informieren, sodass der Verantwortliche die Möglichkeit hat, dagegen Einspruch zu erheben.

Dass die hier geschilderten Verstöße seit langem immer wieder in der Praxis festzustellen sind, mag auch daran liegen, dass die korrekte Lösung – der Direktabschluss der Standardvertragsklauseln zwischen dem EU-Verantwortlichen und dem „Non-EU-Unterauftragsverarbeiter" – nicht parallel zu den zivilrechtlichen Vertragsbeziehungen läuft, bei denen in der Regel der entsprechende Vertrag zwischen dem EU-Auftragsverarbeiter und dem „Non-EU-Unterauftragsverarbeiter" abgeschlossen wird.

Nichtsdestotrotz liegt hierin ein datenschutzrechtlicher Verstoß. Solange keine Standardvertragsklauseln (ab 25.5.2018: „Standarddaten-

schutzklauseln") gemäß Art. 46 Abs. 2 Buchstabe c bzw. d DS-GVO zur Verfügung stehen, die zwischen EU-Auftragsverarbeiter und „Non-EU-Unterauftragsverarbeiter" abgeschlossen werden können, werden wir derartige Fehlgestaltungen, soweit sie uns bekannt werden, unterbinden. Inwieweit darüber hinausgehende Maßnahmen und ggf. Sanktionen angezeigt sind, werden wir jeweils anhand der Umstände des Einzelfalls bewerten.

14.2 Genehmigung von Binding Corporate Rules

Datenschutzaufsichtsbehörden können nach DS-GVO verbindliche interne Vorschriften zum Datenschutz beim Verantwortlichen prüfen und genehmigen.

Binding Corporate Rules (BCR) – verbindliche interne Datenschutzvorschriften – erfreuten sich auch im Berichtszeitraum stetig wachsender Beliebtheit als Instrument für konzerninterne Übermittlungen personenbezogener Daten in Drittländer ohne angemessenes Datenschutzniveau. Vor dem Geltungsbeginn der DS-GVO waren BCR zwar nicht ausdrücklich im Gesetz erwähnt, jedoch von den Datenschutzaufsichtsbehörden der weitaus meisten EU- und EWR-Staaten als mögliche Instrumente zur Erbringung ausreichender Datengarantien für Datenübermittlungen in Drittländer ohne angemessenes Datenschutzniveau anerkannt. Die Datenschutzbehörden der Mitgliedstaaten hatten ein Verfahren zur koordinierten Prüfung von BCR entwickelt, anhand dessen vor dem 25. Mai 2018 die BCR von mehr als 100 Unternehmensgruppen von den jeweils zuständigen Aufsichtsbehörden koordiniert, geprüft und anerkannt wurden.

Die DS-GVO erwähnt nun in Art. 46 Abs. 2 Buchstabe b BCR ausdrücklich als geeignete Garantien für Datenübermittlungen in Drittländer und regelt in Art. 47 DS-GVO inhaltliche Anforderungen, die weitestgehend die in den existierenden Arbeitspapieren der Datenschutzbehörden (Artikel-29-Datenschutzgruppe) aufgestellten, inhaltlichen Anforderungen bestätigen und nur um einige spezifisch durch die DS-GVO neu eingeführte datenschutzrechtliche Anforderungen ergänzen.

Mit Blick auf das Verfahren der Genehmigung von BCR hat die DS-GVO einige Änderungen gebracht: Art. 57 Abs. 1 Buchstabe s DS-GVO besagt, dass jede Aufsichtsbehörde in ihrem Gebiet die Aufgabe hat, BCR zu genehmigen. Würde dies bedeuten, dass ein und dieselbe BCR eines gesonderten Genehmigungsaktes jeder Aufsichtsbehörde, in deren Zuständigkeitsbereich die BCR Geltung haben soll, bedarf, würde dies einer Erschwerung und Verkomplizierung gegenüber der bisherigen Praxis gleichkommen, bei der sich die meisten Aufsichtsbehörden der EU-Mitgliedstaaten eines Verfahrens der gegenseitigen Anerkennung (mutual recognition) bedienten, indem eine BCR allein von einer federführenden Aufsichtsbehörde und mit Unterstützung von 2 Co-Prüfer-Behörden geprüft wurde. Dieses schlanke Verfahren hat sich aus Sicht der Aufsichtsbehörden bewährt und zur erheblichen Beschleunigung der Prüfung von BCR geführt.

Die Aufsichtsbehörden haben sich nun mit Blick auf das Prüfverfahren unter Geltung der DS-GVO im Working Paper 263 der Artikel-29-Datenschutzgruppe (das vom Europäischen Datenschutzausschuss bestätigt wurde) dahin gehend geäußert, dass sie das bisherige Verfahren jedenfalls faktisch auch unter der DS-GVO mit nur geringfügigen Änderungen beibehalten. Nach dem Gesetzeswortlaut muss jedoch zu jeder BCR vor ihrer Genehmigung gemäß Art. 64 Abs. 1 Buchstabe f DS-GVO eine förmliche Stellungnahme des Europäischen Datenschutzausschusses (EDSA) eingeholt werden. Um alle Aufsichtsbehörden bereits vor dieser förmlichen Beschlussfassung mit der BCR vertraut zu machen und Last-Minute-Interventionen nach Möglichkeit zu vermeiden, ist vorgesehen, die BCR nach der durch die Federführung und die

zwei Co-Prüfer-Behörden geleisteten Prüfung, aber noch vor förmlicher Zuleitung an den EDSA an alle Aufsichtsbehörden der Mitgliedstaaten zur dortigen Vorabprüfung mit Frist von einem Monat zuzuleiten.

Bei diesem Vorgehen gehen die Aufsichtsbehörden davon aus, dass auch unter Geltung der DS-GVO eine zügige Prüfung der BCR sichergestellt sein wird. Im Übrigen sind die Aufsichtsbehörden der Auffassung, dass BCR auch unter der DS-GVO keiner parallelen Genehmigungen durch jede zuständige Aufsichtsbehörde bedürfen, sondern dass die Genehmigung durch die für das jeweilige Verfahren federführende Aufsichtsbehörde genügt (vgl. das Arbeitspapier 263 rev.01 der Artikel-29-Datenschutzgruppe, Ziff. 2.6-2.7). Ein Widerspruch zu Art. 57 Abs. 1 Buchstabe s DS-GVO wird darin nicht gesehen. Vielmehr interpretieren die Aufsichtsbehörden diese Vorschrift (nur) in dem Sinne, dass darin die Genehmigung von BCR allgemein als eine Aufgabe jeder Aufsichtsbehörde definiert ist, ohne jedoch besagen zu wollen, dass eine BCR durch jede der Aufsichtsbehörden für ihren örtlichen Zuständigkeitsbereich gesondert genehmigt werden müsste.

15

Beschäftigtendatenschutz

15 Beschäftigtendatenschutz

15.1 Widerruf der Einwilligung zur Veröffentlichung von Mitarbeiterfotos

Widerruft ein Mitarbeiter seine Einwilligung zur Veröffentlichung seines Fotos in bereits gedruckten Broschüren, so ist für die weitere Verwendung eine Interessenabwägung durchzuführen, die auch zugunsten des Arbeitgebers ausfallen kann.

Ein Unternehmen trägt vor, es habe Einwilligungen seiner Mitarbeiter eingeholt, Fotos in Broschüren und Flyern des Unternehmens abbilden zu dürfen. Die Broschüren und Flyer seien in hoher Stückzahl gedruckt worden und dazu vorgesehen, z. B. auf Veranstaltungen bzw. Messen an Kunden oder Interessenten verteilt zu werden. Ein Mitarbeiter habe seine Einwilligung widerrufen. Das Unternehmen fragt nun an, ob es aufgrund der hohen Kosten die Broschüren und Flyer weiter verwenden könne oder ob die noch nicht ausgegebenen Exemplare vernichtet werden müssen.

Der Widerruf einer Einwilligung entfaltet Wirkung für die Zukunft (ex nunc). Bei der Frage der weiteren Verwendung der Fotos des betroffenen Mitarbeiters wird eine Abwägung der Interessen der Beteiligten vorzunehmen sein. Dabei ist zugunsten des Unternehmens der Aufwand bei der Herstellung der Broschüren und Flyer zu berücksichtigen. Die weitere Verwendung der bereits gedruckten Exemplare haben wir als vertretbar angesehen, da die Herstellungskosten sehr hoch waren und der Mitarbeiter keine besonders herausgehobene Funktion im Unternehmen bekleidete und die Darstellung in den Veröffentlichungen ebenfalls nicht besonders herausgehoben war. Bei einer Neuproduktion dürfen die Fotos des betreffenden Mitarbeiters aber nicht mehr verwendet werden.

15.2 Fragen im Bewerbungsverfahren

Manche Fragen darf ein Arbeitgeber zwar einem neu einzustellenden Mitarbeiter stellen, nicht aber jedoch einem Bewerber.

Ein Bewerber, der sich auf eine Stelle bei einem Unternehmen beworben hatte, beschwerte sich bei uns über das Unternehmen, weil dieses ihm in einem auszufüllenden Bogen Fragen stellte, die er für nicht zulässig hielt.

Tatsächlich ergab sich im Rahmen des Beschwerdeverfahrens, dass das Unternehmen für Bewerber und für neu einzustellende Mitarbeiter den gleichen Fragebogen verwendete. Dieser enthielt demgemäß Fragen, die zwar zulässigerweise an einen neu einzustellenden Mitarbeiter gestellt werden konnten, nicht aber an einen Bewerber, weil es in diesem Stadium dafür keinerlei sachliche Notwendigkeit gab. Dies betraf bspw. Fragen nach der Krankenversicherung oder nach der Bankverbindung.

Wir forderten das Unternehmen daher auf, einen eigenen Fragebogen für Bewerbungsverfahren zu konzipieren und uns diesen zur Begutachtung vorzulegen. Das Unternehmen kam dem nach. Der konzipierte Fragebogen für Bewerber entsprach den rechtlichen Vorgaben.

15.3 Videointerviews bei Personalentscheidungen

Videointerviews in Bewerbungsverfahren können zulässig sein, wenn sie in der eigenen Infrastruktur des Unternehmens ablaufen, andere Alternativen (persönliches Gespräch) zur Verfügung stehen und für die nötige Transparenz gesorgt ist.

Ein Unternehmen wandte sich an uns, weil es beabsichtigte, in Bewerbungsverfahren und bei der Auswahl von Trainees Videointerviews durchzuführen. Es war vorgesehen, dass Bewerber vor Vereinbarung des Interviewtermins noch Datenschutzhinweise und Informationen zu den technischen Voraussetzungen erhalten, um entsprechende Einstellungen an ihren Endgeräten vornehmen zu können. Die Kommunikation zwischen Arbeitgeber und Bewerber sei während des Videointerviews verschlüsselt. Es finde keine Übermittlung von Gesprächsinhalten und personenbezogenen Daten an Dritte statt, da die Durchführung der Videointerviews über die unternehmenseigene Infrastruktur mit eigenen On-Premise-Servern erfolge. Es würden auch keine Gesprächsinhalte aufgezeichnet. Sollte ein Bewerber über keinen Internetanschluss verfügen oder die Durchführung von Videointerviews ablehnen, kämen auch weiterhin andere Alternativen, z. B. persönliche Interviews, zum Einsatz.

Nach § 26 Abs. 1 Satz 1 BDSG ist das Verarbeiten von Mitarbeiterdaten durch den Arbeitgeber zulässig, wenn es für die Entscheidung über die Begründung des Beschäftigungsverhältnisses erforderlich ist.

Ein Bewerbungsgespräch ist ein geeignetes Instrument für Arbeitgeber, die richtige Person für die zu besetzende Stelle herauszufinden. Gerade bei einer großen Zahl von Bewerbern ist es oft nicht möglich, alle in Betracht kommenden Personen zu einem persönlichen Gespräch einzuladen. Insbesondere wenn Bewerber aus weiter Distanz anreisen müssen, kann eine digitale Lösung im beiderseitigen Interesse liegen. Für potentielle Bewerber kann ein Videointerview eine einfache, erste Möglichkeit sein, die schriftlich erfolgte Bewerbung ohne großen Aufwand zu vertiefen. Dies könnte dazu führen, dass mehr Bewerber die Möglichkeit haben, sich persönlich darzustellen und der Arbeitgeber im Interesse beider Beteiligten dadurch eine qualifiziertere Auswahlentscheidung treffen kann.

Wir betrachten es daher im Interesse beider Beteiligter als eine datenschutzrechtlich zulässige Lösung, wenn sich der Arbeitgeber mittels des Videointerviews einen persönlichen Eindruck von einem Bewerber verschaffen kann und seine Entscheidung nicht nur anhand von Bewerbungsunterlagen trifft.

Da keine Aufzeichnungen erfolgen, werden auch nicht mehr oder andere Daten erhoben als bei einem persönlichen Gespräch. Zu berücksichtigen ist auch, dass es weiterhin Alternativen zu den Videointerviews gibt.

Wir gingen davon aus, dass die nötige Datensicherheit gewährleistet ist, weil die Kommunikation verschlüsselt ist und die Durchführung der Videointerviews über die Unternehmensinfrastruktur auf eigenen Servern läuft.

Eine Information der Bewerber über die o. g. Rahmenbedingungen der Videointerviews hielten wir im Hinblick auf die Anforderungen des Art. 13 DS-GVO für notwendig. Unter Transparenzgesichtspunkten hielten wir es schließlich auch für nötig, dass die Bewerber während des Interviews sämtliche Gesprächspartner auf Seiten des Unternehmens sehen können.

Insgesamt gesehen bewerteten wir die geplante Durchführung von Videointerviews für Bewerber wie oben beschrieben für datenschutzrechtlich zulässig.

16

Gesundheit und Soziales

16 Gesundheit und Soziales

16.1 Rechtsgrundlage der Verarbeitung in Arztpraxen

Sehr häufig werden in Arztpraxen von Patienten unnötige Einwilligungen für die Datenverarbeitung verlangt.

Zahlreiche Arztpraxen gingen davon aus, dass sie mit Geltung der DS-GVO nur noch mit Einwilligung der Patienten deren Daten verarbeiten dürfen. Sie formulierten deshalb Einwilligungen, die neben der eigenen Datenverarbeitung alle möglichen, denkbaren Datenübermittlungen abdecken sollten. Darüber hinaus informierten uns einige Patienten sogar, dass ihr Arzt eine Behandlung abgelehnt hatte, weil sie eine solche Einwilligungserklärung nicht unterschrieben hatten.

Art. 9 Abs. 2 Buchstabe h DS-GVO erlaubt die erforderliche Verarbeitung von Gesundheitsdaten (besonderer Kategorien von personenbezogenen Daten) z. B. für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin sowie für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheitsbereich, wenn dies auf der Grundlage nationaler Vorschriften oder eines Behandlungsvertrages erfolgt und wenn die Daten durch Personen oder unter der Verantwortung von Personen verarbeitet werden, die einem Berufsgeheimnis oder einer Geheimhaltungspflicht unterliegen.

Auf diese Rechtsgrundlage können Ärzte die für eine Behandlung erforderliche Datenverarbeitung stützen, vor allem die Dokumentation der Behandlung und die Abrechnung mit der Krankenkasse. Auch ein medizinisch erforderlicher Datenaustausch mit vor-, mit- oder nachbehandelnden Ärzten kann auf diese Rechtsgrundlage gestützt werden.

Daneben legitimieren verschiedene Rechtsnormen die Übermittlung personenbezogener Daten gem. Art. 9 Abs. 2 Buchstabe h i. V. m. Art. 6 Abs. 1 Buchstabe b DS-GVO, § 22 Abs. 1 Nr. 1 Buchstabe b BDSG, so zum Beispiel die §§ 294 ff. SGB V.

Ist die Verarbeitung personenbezogener Daten nicht zur Erfüllung des Behandlungsvertrages erforderlich und gibt es keine Rechtsnorm, die die Verarbeitung legitimiert (bzw. sogar spezifische Pflichten, um eine solche einzuholen), muss die Einwilligung des Patienten eingeholt werden. So muss beispielsweise bei externer Abrechnung durch private Abrechnungsstellen eine solche Einwilligung (wie auch bereits nach alter Rechtslage) eingeholt werden, sofern kein Fall der Auftragsverarbeitung vorliegt.

Eine Einwilligung ist weiterhin erforderlich, falls im Einzelfall nationale Vorschriften eine Einwilligung des Patienten verlangen, wie z. B. § 73 Abs. 1 Buchstabe b SGB V.

16.2 Diskretion bei der Anmeldung und im Sprechzimmer

Im Hinblick auf Diskretion in Arztpraxen besteht immer noch deutlicher Verbesserungsbedarf.

Bei einem Blick auf die Diskretion in Arztpraxen fällt auf, dass Patienten mit Geltung der DS-GVO wesentlich sensibler geworden sind. Sie fordern deutlich öfters einen vertrauensvollen Umgang mit ihren Patientendaten in der Arztpraxis ein und machen uns durch Datenschutzbeschwerden auf Diskretions-Missstände an der Anmeldung und im Sprechzimmer aufmerksam.

Die Situation an der Anmeldung wird oft so geschildert:

- Unterlagen anderer Patienten sind einsehbar.
- Telefonate können mitgehört werden, in denen die Beschäftigten Namen und Krankheiten nennen.
- Patienten werden an der Anmeldung im Beisein anderer Personen dazu aufgefordert, ihre Beschwerden zu schildern.
- Der Wartebereich ist nicht ausreichend von der Anmeldung getrennt, sodass alle Gespräche mitgehört werden können.
- Auch soll es vorkommen, dass die Türen der Sprechzimmer während der Behandlung nicht geschlossen sind.
- Gespräche zwischen Arzt und Patient werden im Flur fortgesetzt.
- In den Sprechzimmern kommt es vor, dass Unterlagen des vorherigen Patienten offen auf dem Schreibtisch liegen und von wartenden Patienten eingesehen werden können.
- Der Bildschirm am Arbeitsplatz des Arztes oder sonstige medizinische Geräte sind nicht gesperrt und Daten anderer Patienten werden dort noch „offen" angezeigt.

Diese Punkte sind alle nicht neu. Wir hatten bereits in den vergangenen Tätigkeitsberichten diese Problemfelder behandelt und zudem durch Vor-Ort-Kontrollen bei verschiedenen Arztpraxen geprüft. Auch die erforderlichen Abhilfemaßnahmen sind hinlänglich bekannt und oft mit einfachen Mitteln umzusetzen. Umfangreiche Hilfestellungen bieten hier Veröffentlichungen der Kassenärztlichen Vereinigung Bayerns (KVB) sowie der Ärztekammern.

Wir forderten auf Grund der nach wie vor verbesserungswürdigen Zustände die jeweiligen Verantwortlichen auf, die Missstände zu beheben, was in allen Fällen meist sehr gut gelungen ist.

Wir empfehlen Ärzten auch weiterhin (vermeidbare) Datenschutzbeschwerden von Patienten zuvorzukommen, indem sie mit offenen Augen durch die eigene Praxis gehen und die Verhältnisse vor Ort einmal durch die „Diskretions-Brille" betrachten.

16.3 Ansprache von Patienten in Arztpraxis

Die namentliche Ansprache von Patienten in der Arztpraxis ist auch nach Geltung der DS-GVO weiter zulässig – andere Informationen hierzu entstammen der Panikmache rund um die DS-GVO.

Eine namentliche Ansprache von Patienten in der Arztpraxis halten wir weiterhin für zulässig. Dies ist gesellschaftsüblich und dient dazu, dass sich Patienten als Menschen wahrgenommen fühlen. Wir halten es deshalb nicht für erforderlich, in Arztpraxen ein Nummern-System einzuführen oder auf eine unpersönliche Ansprache auszuweichen.

Bittet ein Patient bei der Anmeldung aber darum, dass sein Name nicht im Beisein anderer Patienten genannt wird, sollte dem nach Möglichkeit Rechnung getragen werden.

Arztpraxen müssen also nicht den jahrelang praktizierten persönlichen Umgang mit dem Patienten auf Grund der DS-GVO ändern, wenn man bereits im Vorfeld auf die datenschutzrechtlichen Vorgaben geachtet hat.

16.4 Schweigepflichtentbindungserklärung bei Anfragen von Gerichten

Entscheidungen eines Gerichts über Schweigepflichtentbindung sind für Ärzte verbindlich.

Mehrere Ärzte baten uns um Unterstützung, weil sie Patientendaten an ein Gericht übermitteln sollten, das Gericht sich aber weigerte, die Schweigepflichtentbindungserklärung des Patienten durch Übersendung einer Kopie zu belegen.

Die Frage, ob ein Arzt, wenn er als Zeuge einem Gericht Patientenunterlagen zur Verfügung stellen oder Patientendaten übermitteln soll, vom Gericht die Vorlage einer Schweigepflichtentbindungserklärung verlangen kann oder muss, betrifft in erster Linie die berufsrechtliche Schweigepflicht. Wir haben uns deshalb mit der Bayerischen Landesärztekammer abgestimmt und von dort die Aussage erhalten, dass ein Arzt, der vor Gericht als sachverständiger Zeuge aussagen soll, sich nicht auf ein Zeugnisverweigerungsrecht berufen kann, wenn er vom Patienten von der Schweigepflicht entbunden wurde (§ 53 Abs. 1 Nr. 3 und § 53 Abs. 2 StPO sowie § 383 Abs. 1 Nr. 6 ZPO). Wenn ein Gericht dem Arzt mitteilt, dass der Patient ihn von der ärztlichen Schweigepflicht entbunden hat, ist diese Aussage für den Arzt verbindlich. Er kann vom Gericht nicht verlangen, dass ihm eine schriftliche Schweigepflichtentbindung vorgelegt wird.

Auch das SG Frankfurt am Main hat in einem Beschluss vom 24. September 1998 ausgeführt:

> *„Der Arzt ist nicht berechtigt, das Zeugnis mit dem Argument zu verweigern, das Gericht habe ihm gegenüber die Schweigepflichtentbindung nicht nachgewiesen. Es ist ausreichend, wenn das Gericht dem Arzt mitteilt, dass die entsprechende Erklärung vorliegt."*

Der Arzt kann demnach nicht verlangen, dass ihm die Schweigepflichtentbindungserklärung vorgelegt wird – dies gilt auch unter der DS-GVO. Ihm muss aber die ausdrückliche Aussage/Bestätigung des Gerichtes vorliegen, dass der Patient ihn von der Schweigepflicht entbunden hat. Die Dokumentation dieser Bestätigung sehen wir in diesen Fällen für die Erfüllung der Rechenschaftspflicht als ausreichend an.

16.5 Abholung von Rezepten und Vereinbarung von Arztterminen durch den Ehepartner

Grundsätzlich sind eine Einwilligung und eine Schweigepflichtentbindungserklärung des Patienten nötig, wenn dem Ehepartner gegenüber Gesundheitsdaten durch die Arztpraxis offenbart werden sollen.

In der Vergangenheit wurde offenbar häufiger nicht weiter hinterfragt, wenn Ehepartner Arzttermine für einen Patienten vereinbart oder Rezepte oder Untersuchungsergebnisse abgeholt haben. Die hierfür nötige Einwilligung oder eine Bevollmächtigung wurde dabei nicht immer eingeholt oder verlangt. Entsprechend irritiert waren einige Patienten, als Arztpraxen mit Geltung der DS-GVO zunehmend dazu übergingen, für eine Korrespondenz mit Ehepartnern oder für die Herausgabe von Unterlagen an Ehepartner die Einwilligung des Patienten einzuholen.

Zunächst ist hier festzuhalten, dass Ehepartner (wenn sie nicht gesetzliche Betreuer sind) datenschutzrechtlich als Dritte anzusehen sind, auch wenn dies manchen Patienten befremdlich erscheinen mag. Deshalb gilt die ärztliche Schweigepflicht auch ihnen gegenüber. Es ist demnach an sich richtig, wenn Ärzte nicht ohne Weiteres mit dem Ehepartner ihres Patienten kommunizieren und damit Gesundheitsdaten an Ehepartner übermitteln. Während für die Entbindung von der ärztlichen Schweigepflicht

dabei grundsätzlich auch ein konkludentes Handeln ausreichen kann, bedarf es datenschutzrechtlich gemäß Art. 9 Abs. 2 Buchstabe a DS-GVO einer ausdrücklichen Einwilligung des Patienten.

Für eine solche ausdrückliche Einwilligung genügt es nicht, wenn der Ehepartner bei der Behandlung des Patienten üblicherweise mit anwesend war und man deshalb unterstellen könnte, er werde mit einer Übermittlung an den Ehepartner schon einverstanden sein. Allerdings muss die Einwilligung nicht schriftlich sein, d. h. der Patient kann sich auch mündlich (z. B. bei der telefonischen Bestellung eines Folgerezeptes) ausdrücklich damit einverstanden erklären, dass es von seinem Ehepartner abgeholt wird. Zudem muss eine ausdrückliche Einwilligung des Patienten, dass der Ehepartner Rezepte bei der jeweiligen Praxis stets abholen darf, nicht bei jedem Besuch wiederholt werden.

16.6 Einwilligung für Behandlung durch Heilpraktiker

Heilpraktiker benötigen als Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten eine ausdrückliche Einwilligung der betroffenen Person.

Heilpraktiker benötigen seit Inkrafttreten der DS-GVO als Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten eine ausdrückliche Einwilligung der betroffenen Personen, denn sie unterliegen keinem Berufsgeheimnis und keiner Geheimhaltungspflicht im Sinne von Art. 9 Abs. 3 DS-GVO und § 22 Abs. 1 Nr. 1 Buchstabe b BDSG. Sie können sich daher nicht auf den gesetzlichen Erlaubnistatbestand des Art. 9 Abs. 2 Buchstabe h DS-GVO (Behandlungsvertrag) berufen.

16.7 E-Mail-Kommunikation zwischen Arzt und Patient

Ein Patient kann bei der E-Mail-Kommunikation mit dem Arzt auf eigenen Wunsch auf eine Ende-zu-Ende-Verschlüsselung verzichten.

Nach Art. 32 DS-GVO haben Verantwortliche, wie z. B. Ärzte, technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dies spielt auch bei der E-Mail-Kommunikation eine wesentliche Rolle. Unverschlüsselte E-Mails können viele datenschutzrechtliche Anforderungen nicht erfüllen, z. B. die Vertraulichkeit und die Integrität der Daten.

Ein Arzt, der seinen Patienten E-Mail-Kommunikation anbietet, hat Sicherheitsmaßnahmen nach dem Stand der Technik und der Schutzwürdigkeit der Daten zu treffen. Im Verhältnis Arzt – Patient geht es um Gesundheitsdaten und damit um besondere Arten personenbezogener Daten (Art. 9 DS-GVO), die zusätzlich auch nach § 203 StGB einem besonderen rechtlichen Schutzbereich unterliegen.

Wir sehen es beim E-Mail-Verkehr mit solchen Daten als notwendig an, eine Transport- und eine Inhaltsverschlüsselung (Ende-zu-Ende-Verschlüsselung) vorzunehmen. Eine Verschlüsselung mittels PGP oder SMIME würde beispielsweise den Anforderungen an die Inhaltsverschlüsselung entsprechen. Die opportunistische Transportverschlüsselung wird durch eine entsprechende Konfiguration des E-Mailservers erreicht und ist inzwischen weitestgehend Standard.

Zusätzlich müsste sichergestellt sein, dass die E-Mail-Adresse, an die Informationen gesendet werden, auch tatsächlich von demjenigen stammt, mit dem man kommunizieren will. Es wäre bspw. denkbar, dass sich Unbefugte eine E-Mail-Adresse mit dem Namen eines Patienten

generieren und von dort aus versuchen, Informationen vom Arzt anzufordern und unbefugt zu erlangen. Diesem Risiko muss durch eine vorherige Verifikation der Adresse begegnet werden.

Das angemessene Schutzniveau (Ende-zu-Ende-Verschlüsselung) kann unserer Auffassung nach von dem betroffenen Patienten nur unter folgenden Umständen abgesenkt werden:

- Der Wille des Patienten muss frei und informiert gebildet und geäußert werden. Der Arzt muss daher den Patienten darauf aufmerksam machen, dass die E-Mail-Kommunikation ohne Ende-zu-Ende-Verschlüsselung nicht ausreichend sicher sein kann (z. B. wenn ein E-Mail-Konto gehackt ist) und er auf diesem unsicheren Weg nur ausnahmsweise kommuniziert, wenn der Patient (in Kenntnis dieser Information) es wünscht, nicht Ende-zu-Ende verschlüsselt per E-Mail zu kommunizieren.
- In keinem Fall ist ein völliges Absenken des Schutzniveaus möglich: Es gibt einen Mindeststandard (derzeit opportunistische Transportverschlüsselung), der eingehalten werden muss.
- Zudem muss eine dem Risiko der Rechte und Freiheiten entsprechende sichere Alternative ohne Medienbruch angeboten werden. Dies kann z. B. ein ausreichend sicheres Onlineportal oder ein inhaltsverschlüsselter E-Mail-Verkehr sein.

Dies gilt jedoch nur in der Kommunikation zwischen Arzt und Patient, nicht jedoch zwischen zwei Ärzten. Verantwortliche haben auf jeden Fall den Stand der Technik einzuhalten und die Sicherstellung eines angemessenen Schutzniveaus zu gewährleisten. Hier ist kein Raum für eine Absenkung der Sicherheit, selbst wenn der betroffene Patient sein Einverständnis erklärt hat, dass die Ärzte unsicher miteinander kommunizieren dürfen. Weitere Ausführungen hierzu sind im Kapitel 23.9 dieses Berichts zu finden.

16.8 Verarbeitung von Gesundheitsdaten bei Optikern und Sanitätshäusern

Auch Verantwortliche aus dem Gesundheitshandwerk benötigen eine ausdrückliche Einwilligung der betroffenen Person für die Verarbeitung von Gesundheitsdaten.

Eine große Neuerung hat die DS-GVO für die Verantwortlichen aus dem Gesundheitshandwerk gebracht. Diese benötigen für die Verarbeitung von Gesundheitsdaten eine ausdrückliche Einwilligung der betroffenen Personen, denn sie unterliegen keinem Berufsgeheimnis und keiner Geheimhaltungspflicht im Sinne von Art. 9 Abs. 3 DS-GVO und § 22 Abs. 1 Nr. 1 Buchstabe b BDSG. Folglich können sie sich nicht auf den gesetzlichen Erlaubnistatbestand des Art. 9 Abs. 2 Buchstabe h DS-GVO berufen (siehe Parallelen zum Kapitel 16.6).

Da ein Optiker bspw. keine passende Lesebrille für die betroffene Person ohne Einwilligung in die Verarbeitung der Sehschärfe anfertigen kann, ist diese Einwilligung für die Erfüllung des Vertrages erforderlich. Es bestehen deshalb keine Zweifel an der Freiwilligkeit dieser Einwilligung (Art. 7 Abs. 4 DS-GVO).

16.9 Telefonverzeichnis, Türschilder und Briefkästen im Seniorenheim

In Heimen ist das Anbringen von Türschildern und individuellen Briefkästen ebenso datenschutzrechtlich zulässig wie das Führen eines internen Telefonverzeichnisses.

Die Betreiber eines Seniorenheimes fragten an, ob es stimme, dass auf Grund der DS-GVO kein

internes Telefonverzeichnis unter den Bewohnern mehr herausgegeben werden dürfe. Auch die Postzustellung an die Bewohner und die Türschilder mit den Namen der Bewohner waren Gegenstand von Diskussionen. So äußerten die Betreiber zum Teil Bedenken, ob Briefkästen für Bewohner DS-GVO-konform seien. Postzusteller verweigerten die Aushändigung von Post für Bewohner an die Verwaltung der Einrichtung.

Hier ist zunächst festzuhalten, dass wir uns lediglich zur datenschutzrechtlichen Zulässigkeit äußern können. Häufig handelte es sich bei diesen Sachverhalten jedoch nicht vordergründig um datenschutzrechtliche Sachverhalte, sondern um grundsätzliche Leitungs- und Organisationsentscheidungen.

In einem Seniorenheim, in dem persönliche Kontakte zwischen den Bewohnern üblich und gewünscht sind, kann es ein Interesse daran geben, unter den Bewohnern ein Telefonverzeichnis zu verteilen und die Kontaktaufnahme zu erleichtern. Um auch die Interessen derjenigen zu berücksichtigen, die dies nicht möchten, sehen wir es als gangbaren Weg an, über die Herausgabe eines Telefonverzeichnisses zu informieren und den Bewohnern ein Widerspruchsrecht einzuräumen.

Ebenso verhält es sich mit den Türschildern. War das Anbringen eines Türschildes mit dem Vor- und Nachnamen des Zimmerbewohners in einem Seniorenheim bisher üblich, bestand kein Anlass, diese zum 25. Mai 2018 zu entfernen. Hier haben wir bei der Anfrage eines Seniorenheimes allerdings darauf verwiesen, dass auch für diejenigen Bewohner, die dies (nicht mehr) möchten, eine für alle passende Lösung gefunden wird, z. B. die Abkürzung des Namens.

Auch das Anbringen von mit den Bewohnernamen beschrifteten Briefkästen im Eingangsbereich ist auf datenschutzrechtlich zulässige Weise möglich. Je nach Sachverhaltskonstellation lässt sich dies auf Art. 6 Abs. 1 Buchstabe f bzw. auf Art. 9 Abs. 2 Buchstabe a DS-GVO stützen.

16.10 Fotos aus Kindertagesstätten für Eltern

Auch nach Erlass der DS-GVO dürfen in Kindertagesstätten Fotografien der Kinder angefertigt werden.

Uns erreichten mehrere Anfragen aus Kindertagesstätten. Dort war es bisher üblich, dass von den Kindern das ganze Jahr über Fotos gemacht und diese zum Jahresende an die Eltern gegeben wurden. Mit Verweis auf die DS-GVO sollte dies nun, trotz schriftlicher Zustimmung der Eltern, in Zukunft nicht mehr möglich sein.

Das Anfertigen von Fotos in der Kindertagesstätte und das Verteilen an die Eltern sehen wir weiterhin als zulässig an. Kindertagesstätten und Eltern sollten sich nicht durch kursierende Falschmeldungen verunsichern lassen.

Fotos zur internen Verwendung wie Portfolios, kita-interne Aushänge, Diashows auf Elternabenden lassen sich im Regelfall auf die berechtigten Interessen der Kindertagesstätte und der jeweils anderen Eltern als Dritte stützen, die Eltern am Alltag ihrer Kinder teilhaben zu lassen und Entwicklungsfortschritte zu dokumentieren. Rechtsgrundlage ist hierfür Art. 6 Abs. 1 Buchstabe f DS-GVO. In Einzelfällen ist ein zu begründender Widerspruch gem. Art. 21 DS-GVO möglich.

Anders stellt sich die Situation dagegen bei Veröffentlichungen (Zeitung, Radio, Website etc.) und Weitergabe an Dritte dar. Hierfür ist eine konkrete Einwilligungserklärung der Eltern nach Art. 6 Abs. 1 Buchstabe a DS-GVO erforderlich.

16.11 Kindernamen in Kindertagesstätten

Kindernamen müssen nicht mittels Tierbildern o. ä. pseudonymisiert werden. Namensnennungen sind auch nach Erlass der DS-GVO in vielen Fällen unproblematisch zulässig.

Uns erreichten Anfragen aus Kindertagesstätten, wonach zum Teil in diesen mit Verweis auf die DS-GVO keinerlei Vornamen der Kinder mehr sichtbar verwendet werden. So wurden beispielsweise die Namensschilder an den Garderoben entfernt und Bilder oder Basteleien der Kinder nur noch ohne Namen aufgehängt.

Wir halten diese Maßnahmen weder für sinnvoll noch für erforderlich. Aus unserer Sicht ist die Nennung von Namen in den genannten und vergleichbaren Konstellationen auch nach Inkrafttreten der DS-GVO unproblematisch zulässig. Rechtsgrundlage ist Art. 6 Abs. 1 Buchstabe b (Betreuungsvertrag) bzw. f DS-GVO (berechtigte Interessen).

16.12 Elternbeirat kein eigener Verantwortlicher

Elternbeiräte an Schulen sind nicht als datenschutzrechtlich Verantwortlicher anzusehen – Verantwortlicher im Sinne der DS-GVO ist immer die jeweilige Schule.

Mit der DS-GVO kam die Frage auf, wie es sich mit Elternbeiräten an Schulen verhält. Nach unserer mit dem Bayerischen Staatsministerium für Unterricht und Kultus sowie dem Bayerischen Landesbeauftragten für den Datenschutz abgestimmten Auffassung ist der Elternbeirat einer Schule kein eigener Verantwortlicher im Sinne der DS-GVO.

Verantwortlicher ist vielmehr die Schule, welche die datenschutzrechtlichen Vorgaben auch in Bezug auf die Arbeit des Elternbeirats umzusetzen hat.

17

Vereine und Verbände

17 Vereine und Verbände

17.1 Informationspflicht für Bestandsmitglieder

Bestandsmitglieder von Vereinen müssen nicht wegen der DS-GVO über die Verarbeitungen im Verein neu informiert werden.

Zahlreiche Vereine fragten uns, ob sie mit Geltungsbeginn der DS-GVO zum 25. Mai 2018 ihre Bestandsmitglieder anhand der Vorgaben der Art. 12 bis 14 DS-GVO über die Verarbeitung ihrer Daten informieren müssten. Wir wiesen jeweils darauf hin, dass dies nicht erforderlich ist.

Der Verantwortliche muss der betroffenen Person die Informationen gemäß Art. 13 DS-GVO nach dem eindeutigen Wortlaut der Vorschrift zum Zeitpunkt der Datenerhebung erteilen. Personen, deren Daten ein Verein bereits vor dem 25. Mai 2018 erhoben hat, mussten vom Verein seinerzeit anhand des Maßstabs der damals geltenden Informationspflicht (§ 4 Abs. 3 BDSG-alt, d. h. in der bis zum 24. Mai 2018 geltenden Fassung) über die Verarbeitung ihrer Daten informiert werden. Der DS-GVO lässt sich keine allgemeine Pflicht entnehmen, Personen, deren Daten ein Verantwortlicher vor dem Geltungsbeginn der DS-GVO erhoben hat, nachträglich anhand der Vorgaben der Art. 12 bis 14 DS-GVO zu informieren.

Allerdings muss ein Verein – wie jeder Verantwortliche – betroffene Personen gemäß Art. 13 Abs. 3 bzw. Art. 14 Abs. 4 DS-GVO informieren, wenn er beabsichtigt, ihre Daten für einen anderen Zweck weiterzuverarbeiten als für die Zwecke, für die er die Daten erhoben hat. Wenn ein Verein beispielsweise ab einem bestimmten Zeitpunkt neu beabsichtigt, Mitgliederdaten an einen Dachverband weiterzugeben, weil der Dachverband ab einem bestimmten Zeitpunkt verbandsweit Ehrungen o. ä. gegenüber Mitgliedern der im Verband organisierten Vereine ausspricht, muss der Verein die Mitglieder gemäß diesen Vorschriften über den neuen Verarbeitungszweck und den Verband als neuen Datenempfänger informieren.

17.2 Umgang mit Kontaktdaten von Vereinsmitgliedern

Zur Weitergabe der Kontaktdaten an andere Vereinsmitglieder ist eine Einwilligung erforderlich, sofern ein Vereinszweck nicht primär auf Kontaktpflege gerichtet ist.

Häufig wurden wir im Berichtszeitraum von den unterschiedlichsten Vereinen gefragt, ob der Verein E-Mail-Adressen oder andere Kontaktdaten von Vereinsmitgliedern an alle Vereinsmitglieder zur Verfügung stellen dürfe.

Grundsätzlich sind die Vereinsmitglieder untereinander Dritte. Es ist mithin keinesfalls selbstverständlich, dass ein Verein die Kontaktdaten von Mitgliedern, über die er selbst verfügt, anderen Vereinsmitgliedern zur Verfügung stellt. Dies ist zur Durchführung des Mitgliedschaftsverhältnisses, jedenfalls in den meisten Vereinen, auch nicht erforderlich, sodass die Übermittlung nicht auf Art. 6 Abs. 1 Buchstabe b DS-GVO gestützt werden kann. Die Herausgabe von Mitgliederdaten wie z. B. E-Mail-Adressen zur Kommunikation der Mitglieder untereinander ist daher grundsätzlich nur im Hinblick auf Daten von Mitgliedern zulässig, die hierzu ihre Einwilligung gegeben haben. Es sollte den Mitgliedern die Wahlmöglichkeit gegeben werden, welche Daten für die Kommunikation untereinander genutzt werden dürfen. Hierbei ist darauf zu achten, dass diese Daten zweckgebunden übermittelt wurden und daher grundsätzlich nur zu vereinsinternen Zwecken genutzt werden dürfen. Vereinsmitglieder sind ausreichend über die Zwecke zu informieren und im Zweifel zur Ordnung zu rufen.

Bei Vereinen, deren satzungsmäßiger Zweck auf die persönliche Kontaktpflege ausgerichtet ist und bei denen die Satzung hinreichend deutlich erläutert, dass zu diesem Zweck die Kontaktaufnahme untereinander möglich sein soll, kann die Herausgabe von Kontaktdaten von Vereinsmitglieder durch den Verein auch ohne Einwilligung des einzelnen Mitglieds stattfinden. Rechtsgrundlage hierfür ist in einem solchen Fall in der Regel Art. 6 Abs. 1 Buchstabe f DS-GVO. Der Verein muss die Mitglieder hierüber gemäß Art. 13 Abs. 1 Buchstabe e DS-GVO informieren. Dem einzelnen Mitglied steht in einem solchen Fall gemäß Art. 21 DS-GVO ein Recht auf Widerspruch gegen die Weitergabe seiner Kontaktdaten zu, sofern es einen speziellen, in seiner Person liegenden Grund vorweisen kann, der ausreichend gewichtig ist und gegen die Herausgabe seiner Kontaktdaten an andere Vereinsmitglieder spricht. Auch über dieses Widerspruchsrecht muss der Verein die Mitglieder informieren (Art. 21 Abs. 4 DS-GVO).

17.3 Feuerwehrvereine

Als Verantwortliche müssen auch Feuerwehrvereine datenschutzrechtlichen Anforderungen genügen.

Das Thema Feuerwehr hat uns im Berichtszeitraum auf Grund mehrerer Anfragen im Speziellen beschäftigt. In Bayern muss unterschieden werden zwischen den gemeindlichen Feuerwehren, die gemäß Art. 4 Abs. 1 des Bayer. Feuerwehrgesetzes (BayFwG) öffentliche Einrichtungen der Gemeinden sind und den Feuerwehrvereinen, die gemäß Art. 5 Abs. 1 BayFwG in der Regel das Personal der gemeindlichen Feuerwehren stellen.

Während die gemeindliche Feuerwehr datenschutzrechtlich eine öffentliche Stelle im Sinne des Datenschutzrechts (§ 2 Abs. 2 BDSG) ist, sind die Feuerwehrvereine datenschutzrechtlich nicht-öffentliche Stellen (§ 2 Abs. 4 BDSG). Dies wird bestätigt durch Nr. 5 zu Art. 5 BayFwG in der Bekanntmachung des Bayerischen Staatsministeriums des Innern vom 28. Mai 2013 zum Vollzug des Bayerischen Feuerwehrgesetzes (VollzBekBayFwG), wonach die

> *"innere Organisation der Feuerwehrvereine (...) durch das BayFwG nicht erfasst und (...) auch durch Satzungen gemäß Nr. 5.1 nicht geregelt werden (kann). Einschlägig sind vielmehr die vereinsrechtlichen Vorschriften des Bürgerlichen Gesetzbuchs. In diesem Rahmen können die Mitglieder der Feuerwehrvereine ihr Vereinsleben selbstständig und eigenverantwortlich gestalten. (...) Die rechtliche Trennung zwischen der gemeindlichen Einrichtung Freiwillige Feuerwehr und dem privatrechtlichen Feuerwehrverein bedeutet auch, dass zwischen Vereinsmitgliedschaft und Zugehörigkeit zur öffentlichen Einrichtung unterschieden werden muss."*

Datenschutzrechtlich bedeutet dies, dass stets unterschieden werden muss, ob die Feuerwehr als gemeindliche Einrichtung oder aber der Verein handelt. Die Feuerwehrvereine, die unserer Aufsicht unterliegen, müssen sich bewusst sein, dass sie, soweit sie personenbezogene Daten ihrer Vereinsmitglieder verarbeiten, datenschutzrechtlich Verantwortliche sind. Gleiches gilt etwa, wenn sie im Rahmen der eigenverantwortlichen Organisation ihres Vereinslebens personenbezogene Daten von Gästen einer Veranstaltung verarbeiten.

Die Verarbeitung der personenbezogenen Daten, für die der Verein datenschutzrechtlich Verantwortlicher ist, ist von der Verarbeitung personenbezogenen Daten durch die Gemeinde (als Trägerin der gemeindlichen Feuerwehr) zu trennen. Der Feuerwehrverein muss – wie jeder Verantwortliche – hinsichtlich der Daten, für die er Verantwortlicher ist, selbst ein Verzeichnis der Verarbeitungstätigkeiten führen und darüber hinaus die weiteren Verpflichtungen eines datenschutzrechtlich Verantwortlichen erfüllen.

Wir haben daher für eher kleinere Unternehmen und Vereine, zu den auch Feuerwehrvereine

zählen, Informationen zur einfachen Umsetzung der Vorgaben aus der DS-GVO auf unserer Website veröffentlicht:

www.lda.bayern.de/de/kleine-unternehmen.html

17.4 Fotos im Vereinsleben

Gerade in Vereinen werden bei Veranstaltungen und sonstigen Vereinsaktivitäten zahlreiche Fotos gemacht, für die nicht immer eine Einwilligung der Abgebildeten benötigt wird.

Wie bereits im Kapitel 8.5 beschrieben, war Datenschutz rund ums Fotografieren und Veröffentlichen der Fotos ein sehr häufiger Anfragegegenstand. Auch bei Vereinen war dies wohl ein besonderer Diskussionspunkt. Zu kaum einem anderen Thema erhielten wir nämlich im Berichtszeitraum so viele Anfragen wie dazu, ob ein Verein – z. B. auf seiner Homepage - Fotos über seine Aktivitäten veröffentlichen darf, auf denen Personen erkennbar sind. Viele Vereine fühlten sich in dieser Frage aufgrund des Geltungsbeginns der DS-GVO offenbar stark verunsichert.

Wir haben deshalb bei Vereinen noch einmal grundsätzlich über die datenschutzrechtlichen Hintergründe hierzu aufgeklärt. Bei Bildern, auf denen Personen erkennbar sind, handelt es sich um personenbezogene Daten. Sofern nicht die Voraussetzungen des sog. Medienprivilegs nach Art. 38 BayDSG gegeben sind, kommt als Rechtsgrundlage für die Erstellung und Veröffentlichung von Personenbildern meist (nur) Art. 6 Abs. 1 Buchstabe f DS-GVO in Betracht. Vereine haben im Sinne dieser Vorschrift ein berechtigtes Interesse daran, über ihre Veranstaltungen (Mitgliederversammlung, Tag der offenen Tür, Sportereignisse einschließlich Siegerehrung, Vereinsausflug, Musikaufführung, Trachten- oder Faschingsumzug, Vereinsjubiläum usw.) auch durch Bilder zu berichten. Dies bringt es mit sich, dass auch Personen – Vereinsmitglieder, aber auch Zuschauer und Gäste – erkennbar abgebildet sind. Gemäß Art. 6 Abs. 1 Buchstabe f DS-GVO muss das Veröffentlichungsinteresse des Vereins mit den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Personen, die fotografiert und deren Bilder veröffentlicht werden sollen, abgewogen werden.

In aller Regel wird man davon ausgehen, dass das Interesse des Vereins an der Veröffentlichung überwiegt, wenn es sich um Fotos handelt, die im Zusammenhang mit dem Vereinsleben stehen. Insbesondere bei öffentlichen Veranstaltungen entspricht es den vernünftigen Erwartungen der Teilnehmer an der Veranstaltung, dass Bilder gemacht und veröffentlicht werden. Die Anfertigung und Veröffentlichung der Bilder ist daher datenschutzrechtlich in der Regel nach Art. 6 Abs. 1 Buchstabe f DS-GVO zulässig. Nach unserer Auffassung gilt dies grundsätzlich auch, wenn Kinder zu den betroffenen Personen zählen, sofern das Foto einen Zusammenhang mit dem Vereinsleben besitzt (z. B. Fußballturnier der F-Jugend, Ausflug der Jugendfeuerwehr etc.). Sofern der Verein mit dem nötigen Fingerspitzengefühl handelt, darf er daher Fotos über seine Aktivitäten auch dann veröffentlichen, wenn dabei (auch) Kinder abgebildet sind.

Dagegen überwiegen die Interessen der betroffenen Personen beispielsweise dann, wenn es sich um Fotos aus der Intimsphäre (Nacktbilder) oder diskriminierende oder diskreditierende Bilder („Bierleiche" bei einer Vereinsfeier) handelt.

Vorsicht ist zudem angezeigt, wenn es sich um besondere Arten personenbezogener Daten im Sinne von Art. 9 DS-GVO handelt. Wir wurden beispielsweise von einem Selbsthilfeverein, in dem sich Menschen mit einer bestimmten Erkrankung organisiert haben, gefragt, ob der Verein Fotos einer von ihm organisierten Tagung auch ohne Einwilligung der Abgebildeten veröffentlichen dürfe. Dies haben wir verneint, da davon ausgegangen werden konnte, dass es

sich bei einem (Groß-)Teil der abgebildeten Personen um Menschen handelt, die von der Erkrankung betroffen sind, sodass die Personenfotos im Zweifel als Angaben über die Gesundheit nach Art. 9 Abs. 1 DS-GVO einzuordnen wären. Die Anfertigung und Veröffentlichung von Fotos ist in solchen Fällen daher nur bei Vorliegen eines der Tatbestände des Art. 9 Abs. 2 DS-GVO zulässig. Eine Verarbeitung von Fotos, auf denen (auch) Vereinsmitglieder zu sehen sind, ist auf Grundlage berechtigter Interessen des Vereins an Öffentlichkeitsarbeit nicht möglich, da Art. 9 Abs. 2 DS-GVO eine solche Grundlage der Verarbeitung nicht vorsieht. Da in aller Regel auch keiner der anderen Tatbestände nach Art. 9 Abs. 2 DS-GVO greift, wird die Anfertigung und Veröffentlichung von Fotos einer solchen Veranstaltung nur mit ausdrücklicher Einwilligung nach Art. 9 Abs. 2 Buchstabe a DS-GVO zulässig sein.

17.5 Datenverarbeitung in einem Drittland durch einen Entwicklungshilfeverein

Maßgeblich für die Anwendung der DS-GVO ist, ob die Datenverarbeitung im Rahmen der Tätigkeit einer europäischen Niederlassung des Verantwortlichen stattfindet.

Ein in der Entwicklungshilfe tätiger bayerischer Verein fragte uns, ob er bei seinen Aktivitäten in Afrika der DS-GVO unterliege. In der Sache ging es um Ehrenamtliche, die für den bayerischen Verein tätig sind, die in Afrika – aufgrund verschiedener Kooperationen insbesondere auch mit öffentlichen Stellen – Befragungen von Dorfbewohnern zu bestimmten Projekten durchführen. Im konkreten Fall war es notwendig, die Angaben der Befragten in personenbezogener Form zu verarbeiten. Gefragt wurden wir, ob die DS-GVO für diese Verarbeitung der Daten gemäß Art. 3 Abs. 1 DS-GVO anwendbar war.

Für die Anwendung des Art. 3 Abs. 1 DS-GVO ist maßgeblich, ob die Datenverarbeitung im Rahmen der Tätigkeit einer europäischen Niederlassung des Verantwortlichen stattfindet. Das ist dann der Fall, wenn ein enger, untrennbarer Zusammenhang zwischen der Verarbeitung und den Aktivitäten der Niederlassung besteht (so der EuGH im sog. Costeja-Urteil vom 13.05.2014 – Rechtssache C-131/12). Für den vorliegenden Fall hieß das, dass dann, wenn die Befragungen im Rahmen der Tätigkeit des nur in Deutschland niedergelassenen Vereins stehen, die DS-GVO Anwendung findet, auch wenn die Befragungen und weitere Verarbeitungsschritte physisch in Afrika stattfinden. Dies war in dem an uns herangetragenen Fall gegeben.

Hingegen wäre Art. 3 Abs. 1 DS-GVO beispielsweise dann nicht anwendbar, wenn die Befragungen durch eine in dem Drittland befindliche Niederlassung eines Partnervereins durchgeführt würde; denn in einem solchen Fall erfolgt die Datenverarbeitung – anders als in Art. 3 Abs. 1 DS-GVO vorausgesetzt – nicht im Rahmen der Tätigkeiten einer EU-Niederlassung, sondern wäre der afrikanischen Niederlassung zuzuordnen.

Siehe EuGH vom 13. Mai 2014:

curia.europa.eu/juris/liste.jsf?language=de&num=C-131/12

17.6 Informationskampagne zur DS-GVO für Vereine und Ehrenamt

Eine bayernweite, umfangreiche Informationskampagne zu den datenschutzrechtlichen Anforderungen der DS-GVO bei Vereinen und Ehrenamtlichen trug erheblich zur beruhigenden Aufklärung bei.

Der Geltungsbeginn der DS-GVO hat bei uns zu einer überaus großen Anzahl von Anfragen von Vereinen geführt. Augenscheinlich waren viele Vereine durch die Presseberichterstattung, zum

Teil wohl auch durch Aussagen diverser „Berater", stark verunsichert darüber, was künftig einem Verein datenschutzrechtlich erlaubt ist und inwieweit sich für einen Verein neue Verpflichtungen ergeben. Für den einen oder anderen Verein waren die Informationen aus der Presse zur DS-GVO vermutlich Anlass, sich zum ersten Mal überhaupt detaillierter mit dem Datenschutz auseinanderzusetzen. Dies war für uns daran zu erkennen, dass viele Vereine zu Themen bei uns angefragt haben, die sie bereits nach dem bis zum 24. Mai 2018 geltenden Datenschutzrecht hätten erfüllen müssen.

Die Furcht, aus Unkenntnis gegen datenschutzrechtliche Anforderungen zu verstoßen, die Sanktionen in Millionenhöhe nach sich ziehen könnten, zeigte sich gerade im ehrenamtlichen Bereich als besonders stark ausgeprägt. Wir haben auf diesen Beratungsbedarf im Bereich Vereine und Ehrenamt in vielfältiger Weise reagiert:

- **Informationsmaterialien im Web**

  Wir haben auf unserer Homepage speziell auf Vereine zugeschnittene Handreichungen bereitgestellt, darunter „Häufig gestellte Fragen" sowie Muster (z. B. für typisches Verzeichnis der Verarbeitungstätigkeiten).

- **Zusammenarbeit mit Dachverbänden**

  Wir haben proaktiv eine Reihe von großen bayerischen Dachverbänden, in denen Vereine organisiert sind, angesprochen und ihnen angeboten, die von diesen für die Information ihrer Mitgliedsvereine erstellten Informationsmaterialien und Muster zum Datenschutz zu sichten und bei Bedarf Anpassungsvorschläge zu unterbreiten. Diesen Ansatz werden wir auch in der kommenden Zeit weiter verfolgen und ausbauen.

- **Vorträge vor Ort**

  Als weiteren Baustein unserer Informationskampagne haben wir in einer Vielzahl von Vorträgen über die Anforderungen der DS-GVO an Vereine und Ehrenamtliche informiert. In vielen Fällen gab es dabei Teilnehmerzahlen im dreistelligen Bereich, was das überaus große Interesse an diesem Thema unterstreicht, auf das der Datenschutz mit dem Geltungsbeginn der DS-GVO bei Vereinen und Ehrenamtlichen trifft.

- **Telefon-Hotline**

  Da jedoch, insbesondere ab Mai 2018, trotz dieser vielfältigen von uns erteilten Informationen dennoch täglich in großer Zahl Anfragen von Vereinen bei uns eingingen (an manchen Tagen weit über 20 Anfragen aus dem Vereinsbereich), haben wir eine spezielle Telefon-Hotline eingerichtet, unter der vom Juli bis zum Oktober 2018 Fragen zum Datenschutz im Verein und Ehrenamt gestellt werden konnten. In den meisten Fällen konnten die Fragen telefonisch erschöpfend beantwortet werden. Bei umfangreicheren oder spezielleren Fragen haben wir die Fragen im Nachgang schriftlich beantwortet. Fragen, die besonders häufig gestellt wurden, haben wir zum Anlass genommen, (sofern noch nicht vorhanden) hierzu entsprechende Informationen auf unserer Website zu veröffentlichen. Die Einrichtung der zeitlich begrenzten Hotline als spezielle Maßnahme aus Anlass des ungewöhnlich großen Beratungsbedarfs im ehrenamtlichen Bereich hat sich aus unserer Sicht bewährt.

Im Bereich der Vereine und Ehrenamtlichen wird es voraussichtlich auch mittelfristig noch Informations- und Beratungsbedarf zur DS-GVO geben, dem wir insbesondere durch Kontakt mit den großen bayerischen Dachverbänden und der gezielten Erweiterung des Informationsangebots im Web weiter Rechnung tragen werden.

18

Wohnungswirtschaft und Mieterdatenschutz

18 Wohnungswirtschaft und Mieterdatenschutz

18.1 Einzelabrechnungen in Eigentümergemeinschaften

In einer Eigentümergemeinschaft ist die Bekanntgabe von Einzelabrechnungen an alle Eigentümer erforderlich.

Im Berichtszeitraum beschwerten sich in mehreren Fällen Wohnungseigentümer in Eigentümergemeinschaften darüber, dass der Verwalter im Rahmen der Jahresabrechnung allen Eigentümern die sie betreffende Einzelabrechnung – also eines einzelnen Eigentümers – zur Kenntnis gegeben habe.

Wir haben diese Beschwerden geprüft und im Ergebnis abgelehnt. Solche Eingaben beruhen letztlich auf einem nicht zutreffenden Verständnis der Rechte und Pflichten in einer Eigentümergemeinschaft im Sinne des Wohnungseigentumsgesetzes (WEG). Die Eigentümer sind gemäß Art. 28 Abs. 5 WEG sogar gesetzlich verpflichtet, über die vom Verwalter (gemäß Art. 28 Abs. 3 WEG) erstellte Jahresabrechnung zu beschließen; der Beschluss muss gemäß § 23 WEG grundsätzlich in der Eigentümerversammlung erfolgen. Die Jahresabrechnung umfasst zum einen die Gesamtabrechnung, zum andern aber auch die Einzelabrechnungen. Die Einzelabrechnungen leiten sich anhand des geltenden Kostenverteilungsschlüssels aus der Gesamtabrechnung ab. Sie sind objektbezogen und stellen damit die Beitragsleistung des einzelnen Eigentümers verbindlich fest. Da die Eigentümer diejenigen sind, die über die Jahresabrechnung beschließen, muss ihnen der Verwalter als Beschlussvorlage naturgemäß neben der Gesamtabrechnung auch die Einzelabrechnungen als Beschlussgegenstand vorlegen, weil sie andernfalls über etwas beschließen müssten, was ihnen nicht bekannt ist. Es liegt mithin in der rechtlichen Konstruktion der Eigentümergemeinschaft begründet, dass jeder Eigentümer über alle Einzelabrechnungen informiert werden muss. Dies umfasst naturgemäß auch die Information über der anteilig auf das einzelne Wohnungseigentum entfallende Abrechnungssaldo, d. h. die Differenz zwischen den von dem Eigentümer der jeweiligen Einheit anteilig zu tragenden Ausgaben und den betreffenden anteiligen Einnahmen (insbesondere den vom jeweiligen Eigentümer geleisteten Vorschusszahlungen).

Die Eigentümergemeinschaft muss im Übrigen auch in der Lage sein, den Ausgleich etwaiger Beitragsrückstände einzelner Eigentümer nötigenfalls gerichtlich durchzusetzen, was einen Beschluss der Eigentümer erfordert (§ 27 Abs. 3 S. 1 Nr. 7 WEG) und somit ebenfalls voraussetzt, dass die einzelnen Eigentümer über die Einzelabrechnungssalden informiert werden.

18.2 Abrechnungsdaten eines früheren Eigentümers

Ein aus der Eigentümergemeinschaft ausgeschiedener Wohnungseigentümer hat keinen Anspruch auf eine gesonderte Abrechnung für seine Wohnung, wodurch dem Neueigentümer unter Umständen personenbezogene Daten des Alteigentümers bekannt werden können.

In einem uns vorgetragenen Fall verkaufte ein Wohnungseigentümer seine Wohnung und schied damit aus der Eigentümergemeinschaft aus. Er verlangte vom Verwalter eine anteilige Abrechnung für seine Wohneinheit mit Wirkung zum Zeitpunkt des Eigentumswechsels der Wohnung, was der Verwalter jedoch mit Hinweis darauf verweigerte, dass er dazu nicht verpflichtet sei.

Der (frühere) Eigentümer beschwerte sich deshalb bei uns darüber, dass bei dieser Handhabung dem neuen Eigentümer auch personenbezogene Daten zu ihm, dem früheren

Eigentümer, zur Kenntnis gelangen würden, nämlich die ihn bis zum Ausscheiden anteilig nach § 16 Abs. 2 WEG treffenden Lasten- und Kostenbeiträge sowie die von ihm geleisteten Vorschusszahlungen. Dies empfand der Beschwerdeführer als Datenschutzverstoß.

Die Überprüfung der Rechtslage ergab jedoch, dass sich der Verwalter rechtlich – auch datenschutzrechtlich – einwandfrei verhalten hatte. Nach der Rechtsprechung geht mit dem Ausscheiden eines Eigentümers der Anspruch auf Abrechnung gezahlter Beitragsvorschüsse auf dessen Nachfolger über (siehe z. B. OLG Hamm ZMR 2008, S. 228f; KG ZWE 2000, S. 224f.; KG, ZWE 2000, 274, 276); der ausgeschiedene Eigentümer hat somit entgegen der Annahme des Beschwerdeführers in einem solchen Fall keinen Anspruch auf eine gesonderte Abrechnung. Da der Neueigentümer gemäß der genannten Rechtsprechung somit zivilrechtlich Anspruchsinhaber wird, müssen ihm die Angaben zu den Beitragspflichten des Voreigentümers (d. h. die von diesem geschuldeten und geleisteten Lasten- und Kostenbeiträge) bekannt gegeben werden.

Die Bekanntgabe dieser Daten durch den Verwalter an den Neueigentümer ist daher nach Art. 6 Abs. 1 Buchstabe b DS-GVO legitimiert, weil es sich ab dem Eigentumsübergang rechtlich um Daten zu einem Rechtsverhältnis zwischen der Eigentümergemeinschaft und dem Neueigentümer handelt. Der Alteigentümer hat es hinzunehmen, dass diese Daten dem Neueigentümer zur Kenntnis gelangen. Nach der zivilrechtlichen Rechtsprechung hat indes der ausgeschiedene Eigentümer ein Recht auf Einsichtnahme in die Verwaltungsunterlagen, damit er in der Lage ist, etwaige Ausgleichsansprüche gegenüber seinem Rechtsnachfolger – dem neuen Eigentümer – geltend zu machen (KG ZWE 2000, 226, 227).

18.3 Weitergabe von Eigentümer-Daten durch den Verwalter an andere Eigentümer

Die E-Mail-Adressen und Telefonnummern der Eigentümer dürfen ohne deren Einwilligung nicht vom Verwalter bekannt gegeben werden.

Mehrfach erreichten uns Beschwerden einzelner Eigentümer in Eigentümergemeinschaften nach dem Wohnungseigentumsgesetz darüber, dass der Verwalter ihre E-Mail-Adresse und/oder Telefonnummer an andere Eigentümer in der Eigentümergemeinschaft weitergegeben habe. Die den Beschwerden zugrunde liegenden Sachverhalte waren unterschiedlich; bisweilen hatte der Verwalter solche Daten an einen einzelnen Eigentümer auf dessen gezielte Anfrage hin weitergegeben, in anderen Fällen hatte der Verwalter eine E-Mail an mehrere oder alle Eigentümer verschickt und dabei die E-Mail-Adressen der Eigentümer für alle sichtbar verwendet.

Grundsätzlich muss es der einzelne Eigentümer in einer Eigentümergemeinschaft nicht hinnehmen, dass der Verwalter seine E-Mail-Adresse und/oder Telefonnummer anderen Eigentümern aktiv übermittelt. Zwar ist in der zivilrechtlichen Rechtsprechung anerkannt, dass jeder Eigentümer in einer Eigentümergemeinschaft Anspruch auf Kenntnis der Identität der anderen Eigentümer hat; hierzu genügt jedoch grundsätzlich die Kenntnis des Namens und der postalischen Adresse (vgl. BGH, Urt. v. 14.12.2013 – V ZR 162/11). Hintergrund hiervon ist, dass die Eigentümer in der Eigentümergemeinschaft miteinander verbunden sind, sodass die einzelnen Eigentümer aus vielfältigen Gründen die Möglichkeit haben müssen, miteinander in Kontakt zu treten. Dem datenschutzrechtlichen Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchstabe c DS-GVO) entsprechend muss dies jedoch auf die personenbezogenen Daten

beschränkt sein, die zur Kontaktaufnahme erforderlich sind. In aller Regel genügt die Möglichkeit der Kontaktaufnahme auf postalischem Weg. Die Kenntnis darüber hinausgehender Kontaktdaten, etwa von Telefonnummer oder E-Mail-Adresse, ist zu diesem Zweck hingegen in der Regel nicht erforderlich. Ausnahmen können zwar im Einzelfall denkbar sein, jedoch gilt der Grundsatz, dass der Verwalter im Normalfall keine Telefonnummern und/oder E-Mail-Adressen der Eigentümer an die anderen Eigentümer streuen darf, sofern der einzelne Eigentümer dazu nicht seine Einwilligung gemäß Art. 6 Abs. 1 Buchstabe a DS-GVO erteilt hat.

18.4 Fotografieren der Wohnung zu Dokumentationszwecken

Um Instandhaltung- und Instandsetzungspflichten nachzukommen und diese zu dokumentieren, kann das Fotografieren der Wohnung aus Datenschutzsicht zulässig sein.

Uns erreichten verschiedene Beschwerden von Wohnungsmietern, bei denen es in der Sache darum ging, dass der Eigentümer den Zustand bestimmter baulicher Anlagen (z. B. tragende Wände, Türen, Fenster) in einer Wohnung überprüfen und durch Fotos dokumentieren wollte. Der Mieter monierte dabei, dass auf den Bildern seine persönlichen Lebensumstände – etwa seine in der Wohnung befindlichen Gegenstände oder die Art und Weise, wie er seine Wohnung nutzt – festgehalten und diese Informationen vom Vermieter verwendet werden.

Derartige Fotos können in der Tat personenbezogene Daten des Mieters enthalten, wenn sie Rückschlüsse auf die persönliche Lebenssituation des Mieters bzw. die Nutzung der Mietsache durch den Mieter ermöglichen, was in vielen Fällen nicht auszuschließen sein wird. In diesem Zusammenhang spielen die gesetzlichen Regelungen des Bürgerlichen Gesetzbuchs (BGB) zum Wohnraummietrecht eine Rolle. In der mietrechtlichen Rechtsprechung ist anerkannt, dass der Vermieter zur Wahrung seiner Eigentümerrechte und -pflichten und um seiner Erhaltungspflicht aus dem Mietverhältnis (§ 535 Abs. 1 Satz 2 BGB) nachkommen zu können, bei Bestehen eines sachlichen Grundes das Recht hat, die Mietsache (nach entsprechender Ankündigung) zu betreten oder zu besichtigen. Dies ist u. a. der Fall, wenn dem Vermieter Mängel bekannt geworden sind, wenn Anhaltspunkte für einen vertragswidrigen Gebrauch der Wohnung bestehen oder ein Mietwertgutachten nach § 558a BGB erstellt werden soll (Münchner Kommentar zum BGB, § 535, Rn. 134 ff.). Hiernach hat der Vermieter einer Mietwohnung ein berechtigtes Interesse daran hat, sich ein Bild von dem Zustand der Wohnung zu machen und den Zustand zu dokumentieren, wozu auch Bildaufnahmen gehören können. Sofern sich die Fotos darauf beschränken, das Wohneigentum – etwa die reparaturbedürftigen Stellen wie z. B. Schimmelbefall – zu dokumentieren, bestehen daher gegen die Anfertigung und Verwendung der Bilder zu diesem Zweck in datenschutzrechtlicher Hinsicht keine Bedenken.

Nicht zulässig wäre es für den Vermieter hingegen, Bilder anzufertigen, bei denen nicht die Mietsache und ihr Zustand, sondern die persönlichen Lebensumstände des Mieters im Vordergrund stehen – also etwa die in seinem Haushalt lebenden Personen, die im Haushalt befindlichen Sachen oder sonstige Umstände, die nicht unmittelbar mit der Instandhaltungs- und Instandsetzungspflicht des Vermieters zusammenhängen.

18.5 Datenerhebung von Mietbewerbern

Von Mietbewerben werden immer noch sehr häufig viele persönliche Daten unzulässiger Weise abgefragt.

Beschwerden von Mietbewerbern über den Umfang an Daten, die Vermieter oder die vom Vermieter beauftragten Immobilienmakler von ihnen bei der Bewerbung um eine Mietwohnung verlangen, gehörten auch im Berichtszeitraum erneut zu den Dauerbrennern. Am häufigsten beschwerten sich die Mietbewerber darüber, dass der Vermieter oder Immobilienmakler von ihnen bereits vor der Besichtigung einer bestimmten Wohnung außer den Kontaktdaten bereits eine Reihe weiterer Informationen verlangt, häufig durch die Aufforderung, einen Fragebogen auszufüllen. In mehreren von uns bearbeiteten Fällen wurden die Mietbewerber gebeten, bereits vor Wohnungsbesichtigung Angaben zu Arbeitgeber, Einkommensverhältnissen und etwaigen abgegebenen Vermögensauskünften und/oder nach Räumungstiteln wegen Mietzahlungsrückständen zu machen.

Solche Angaben sind aber frühestens erforderlich, wenn der Bewerber nach Besichtigung der Wohnung erklärt, diese anmieten zu wollen (vgl. Orientierungshilfe zur „Einholung von Selbstauskünften bei Mietinteressenten" der Datenschutzkonferenz. Diese Orientierungshilfe ist auf der DSK-Website abrufbar:

www.datenschutzkonferenz-online.de/orientierungshilfen.html

Häufig werden auch Daten abgefragt, deren Erhebung generell – unabhängig vom Zeitpunkt – unzulässig ist, weil sie weder zur Durchführung des avisierten Mietverhältnisses erforderlich sind noch daran ein berechtigtes Vermieterinteresse besteht. So wurde in mehreren Fällen nicht nur (was zulässig ist, jedenfalls wenn der Bewerber nach Besichtigung noch an der Anmietung interessiert ist) nach der Anzahl der in den Haushalt einziehenden Personen, sondern auch nach deren Namen sowie nach dem Familienstand des Bewerbers gefragt (was unzulässig ist, vgl. Ziff. B.1 der o. g. Orientierungshilfe). In mehreren Fällen wurde auch undifferenziert nach Haustieren gefragt, obwohl die Frage nach Kleintieren nicht zulässig ist, da Kleintiere noch vom bestimmungsgemäßen Gebrauch einer Mietwohnung umfasst sind.

In den entsprechenden Fällen haben wir von den Vermietern bzw. Immobilienmaklern verlangt, künftig von den unzulässigen Datenerhebungen Abstand zu nehmen, was uns in allen Fällen umgehend versichert wurde, sodass weitergehende Maßnahmen oder Sanktionen nicht angezeigt waren. Wiederholungsfälle wurden uns bislang nicht bekannt. Die festgestellten Verstöße beruhten nach unserem Eindruck in aller Regel entweder auf Unkenntnis oder darauf, dass insbesondere Privatvermieter ohne nähere Prüfung Vorlagen oder Muster aus dem Internet verwendeten. Häufig fehlte es augenscheinlich auch noch an der gebotenen Sensibilität für die datenschutzrechtliche Problematik.

19

Videoüberwachung

19 Videoüberwachung

Auch im Berichtszeitraum 2017/2018 war die Videoüberwachung ein Schwerpunkt unserer aufsichtlichen Tätigkeit. Die Anzahl der bei uns eingegangenen Beschwerden, die Videoüberwachung zum Gegenstand haben, war wie schon in den vorangegangenen Berichtszeiträumen sehr hoch. Wir haben deshalb neben der Bearbeitung von eingegangenen Beschwerden auch Prüfungen vor Ort in mehreren Gastronomiebetrieben vorgenommen (dazu siehe Kapitel 4.1 dieses Tätigkeitsberichts). Nachfolgend listen wir vier Kernbereiche auf, die immer wieder bei uns Grundlage von Beschwerden oder Datenschutzverstößen waren.

19.1 Dashcams

Aufzeichnungen des Verkehrsgeschehens mittels Dashcams können im Einzelfall zulässig sein, wenn diese kurzzeitig und anlassbezogen, z. B. wegen eines zu dokumentierenden Unfalls, stattfinden.

Breits in unserem letzten Tätigkeitsbericht 2015/2016 hatten wir uns zur datenschutzrechtlichen Rechtslage bei der Nutzung so genannter Dashcams geäußert. Inzwischen hat sich der Bundesgerichtshof (BGH, Urteil vom 15.05.2018 – VI ZR 233/17) mit prozessualen und datenschutzrechtlichen Fragen rund um Dashcams befasst. Zwar verneinte der BGH in seinem o. g. Urteil ein generelles Beweisverwertungsverbot für datenschutzrechtlich unzulässig erstellte Videoaufnahmen durch Dashcams im Rahmen eines Zivilprozesses und betonte, dass die Frage der Verwertbarkeit nur im Einzelfall entschieden werden kann. Gleichzeitig lassen sich der Entscheidung des BGH jedoch grundlegende, datenschutzrechtliche Anforderungen an die Anfertigung und Verwendung von Dashcam-Aufnahmen entnehmen. Demnach kann eine Aufzeichnung des Verkehrsgeschehens mittels einer Dashcam zum Zweck der Beweissicherung für den Fall eines Verkehrsunfalls allenfalls dann als datenschutzrechtlich zulässig in Betracht kommen, wenn mit technischen Mitteln sichergestellt wird, dass lediglich eine kurzzeitige anlassbezogene Speicherung im Zusammenhang mit einer Kollision oder mit einer starken Verlangsamung des Fahrzeugs stattfindet und so eine dauerhafte Aufzeichnung vermieden wird. Gegebenenfalls, so der BGH, seien auch weitere Maßnahmen wie Verpixelung von Personen oder automatisiertes und dem Eingriff des Verwenders entzogenes Löschen erforderlich. Fehlen beim Betrieb einer Dashcam derartige technische Vorkehrungen, so überwiegen laut BGH bei der datenschutzrechtlich gebotenen Interessenabwägung in jedem Fall die schutzwürdigen Interessen der anderen Verkehrsteilnehmer am Unterbleiben der Aufzeichnung gegenüber dem Aufzeichnungsinteresse des Kamerabetreibers.

Maßgebliche Voraussetzungen für ein datenschutzrechtlich zulässiges Betreiben einer Dashcam sind demnach laut BGH eine Verkürzung der Aufzeichnungsdauer sowie die zwingende Verknüpfung der Aufzeichnung mit einem konkreten Anlass.

Zusammenfassend lässt sich sagen, dass eine permanente, anlasslose Aufzeichnung des Verkehrsgeschehens mit einer Videokamera wie bisher datenschutzrechtlich unzulässig ist. Bei Betrieb einer Dashcam müssen technische Möglichkeiten zum Einsatz gebracht werden, mit denen gewährleistet ist, dass eine dauerhafte Sicherung eines Aufzeichnungsintervalls nur anlassbezogen erfolgt – etwa bei Aktivierung eines Crash-Sensors oder bei starkem Bremsen. Darüber hinausgehende Aufzeichnungen, die etwa laufend in einem Ringspeicher/Kurzzeitspeicher erstellt werden, müssen binnen einer kurzen Zeitspanne automatisch gelöscht werden. Hierbei wäre eine sog. Blackbox eine datenschutzrechtlich akzeptable Lösung, bei der nur im Fall eines Unfalls auf die

speziellen dauerhaft aufgezeichneten Bildsequenzen zugegriffen werden kann (z. B. durch die Polizei), während ein Zugriff des Nutzers auf den Kurzzeitspeicher nicht möglich bzw. technisch unterbunden ist.

Zwar ist die Entscheidung des BGH noch zu der bis zum 24. Mai 2018 geltenden Rechtslage ergangen, jedoch haben sich die maßgeblichen Kriterien für die datenschutzrechtliche Bewertung durch die DS-GVO nicht verändert.

19.2 Videoüberwachung durch Privatpersonen

Vorschriften der DS-GVO können auch für privat betriebene Videoüberwachungsanlagen gelten.

Eine große Anzahl von Beschwerden betraf Videoüberwachungsanlagen, die auf Wohnanwesen betrieben wurden. Dort erfassten die Kameras jedoch auch angrenzende Grundstücke und/oder öffentlich zugängliche Bereiche wie z. B. eine öffentliche Straße, einen Gehsteig, eine öffentlich zugängliche Zufahrt.

Dem sog. Rynes-Urteil des EuGH (Rs. C-212/13 vom 11.12.2014) ist zu entnehmen, dass eine Videoüberwachung, die sich auf öffentlichen Raum erstreckt, nicht mehr als persönliche oder familiäre Tätigkeit angesehen werden kann und damit den Vorschriften des Datenschutzrechts unterliegt – seit 25.05.2018 somit vor allem den Vorschriften der DS-GVO. Dem Urteil lässt sich entnehmen, dass dies auch für Videoüberwachung gilt, die zwar nicht den öffentlichen Raum, jedoch (ggf. zusätzlich zu dem Grundstück des Kamerabetreibers) Nachbargrundstücke erfasst.

In den meisten von uns bearbeiteten Fällen gaben die Kamerabetreiber uns gegenüber an, ihr Eigentum gegen Betreten durch Unbefugte oder gegen Beschädigung und Vandalismus schützen zu wollen. Häufig bestanden in den von uns geprüften Fällen zudem verhärtete Konflikte im Nachbarschaftsverhältnis, die bisweilen wohl als (zusätzlicher) Motivationsfaktor für die Videoüberwachung wirkten.

Der Schutz des Eigentums vor Beschädigungen sowie das Hausrecht sind zwar berechtigte Interessen für eine Videoüberwachung. Sie reichen jedoch nicht aus, um die Videoüberwachung des Gehwegs, der Straße oder auch eines Nachbargrundstücks zu legitimieren, da demgegenüber die Grundrechte und Grundfreiheiten der von der Überwachung betroffenen Personen überwiegen und die Überwachung somit nicht auf Art. 6 Abs. 1 Buchstabe f DS-GVO als Rechtsgrundlage gestützt werden kann. Unsere Tätigkeit bestand und besteht in derartigen Fällen darin, den Kamerabetreibern die datenschutzrechtlichen Grenzen einer zulässigen Videoüberwachung zu erläutern und für die Herstellung eines datenschutzkonformen Zustands zu sorgen. Sofern erforderlich ließen wir uns Nachweise – z. B. Bildausdrucke – dahin gehend zuschicken, dass die Kameras so ausgerichtet sind, dass davon nur (noch) das eigene Grundstück erfasst war.

19.3 Videoüberwachung in Schwimmbädern

In Sammelumkleiden und anderen sensiblen Bereichen eines Schwimmbads ist die Überwachung der Schwimmbadbesucher durch Videoaufnahmen nicht gestattet.

Wie schon im vorangegangenen Berichtszeitraum gab es für uns erneut Anlass, die Videoüberwachung in Schwimmbädern zu prüfen. In den jeweiligen Fällen wurde Videoüberwachung typischerweise in Eingangsbereichen, in den Zugängen zu den Umkleidebereichen, in Bereichen, in denen sich Spinde befinden, zum Teil auch im Bade- bzw. Beckenbereich und in Einzelfällen sogar in Sammelumkleiden durchgeführt.

In vielen Bädern gab es in den Sammelumkleiden Schließfächer für die Badegäste. Dieser Bereich wurde in manchen Fällen videoüberwacht. Die Schwimmbadbetreiber argumentierten hier damit, dass in der Vergangenheit Spinde von Unbefugten (die z. B. dem Badegast den Spindschlüssel entwendet hatten) geöffnet worden seien. Zudem würden die Badegäste durch entsprechende Ausschilderung auf die Videoüberwachung in der Sammelumkleide hingewiesen. Diese Argumente vermögen eine Videoüberwachung in einer Sammelumkleide nicht zu rechtfertigen, jedenfalls nicht in den Bereichen, in denen sich die Gäste umziehen. Es handelt sich um einen besonders sensiblen Bereich – betroffen ist die Intimsphäre –, in dem die Gäste zu Recht die Erwartung haben, nicht überwacht zu werden. Bei der nach Art. 6 Abs. 1 Buchstabe f DS-GVO gebotenen Interessenabwägung überwiegen daher die Interessen der betroffenen Personen am Unterbleiben der Videoüberwachung. Die Hinweisbeschilderung ändert daran nichts, da es sich hierbei lediglich um die Erfüllung der Transparenzanforderungen nach Art. 13 DS-GVO handelt, dies jedoch das Vorliegen einer Rechtsgrundlage für die Videoüberwachung nach Art. 6 DS-GVO nicht entbehrlich macht. Da es in den konkreten Fällen auch nicht möglich war, das Kamerablickfeld in der Sammelumkleide so auszurichten, dass ausschließlich die Spinde erfasst wurden, nicht mehr jedoch auch der eigentliche Umkleidebereich, haben wir die Beendigung der Videoüberwachung in diesem Bereich durchgesetzt.

Die Videoüberwachung von Schwimmbecken und Beckenbereichen kann dagegen zulässig sein, sofern sie erforderlich ist, um Gefahrensituationen rechtzeitig zu erkennen und darauf reagieren zu können. Hierfür genügt grundsätzlich das Monitoring durch das zuständige Personal, d. h. die reine Videobeobachtung ohne Aufzeichnung. Zudem muss die Überwachung erforderlich sein, was grundsätzlich nur für Bereiche der Fall ist, zu denen das für die Gewährleistung der Sicherheit zuständige Personal (Bademeister) aufgrund baulicher Gegebenheiten nicht unmittelbar Sichtkontakt hat. In den von uns überprüften Schwimmbädern haben wir die mit Blick auf diese Grundsätze notwendigen Änderungen durchgesetzt.

19.4 Videoüberwachung in der Gastronomie

Sitzbereiche von Gästen und Arbeitsplätze von Mitarbeitern dürfen im Regelfall nicht Gegenstand von Videoüberwachung sein.

Es erreichten uns einige Beschwerden im Zusammenhang mit Videoüberwachungsanlagen in Gaststätten und anderen gastronomischen Einrichtungen. Problematisch war hier in vielen Fällen, dass Videokameras häufig zumindest teilweise Sitz- und Bar-Bereiche oder dauerhafte Arbeitsplätze mit erfassten, auch wenn dies in den von uns überprüften Fällen nicht der eigentliche Zweck der Videoüberwachung war. Der Zweck lag nach Angaben der Betreiber meist darin, die (hinter bzw. auf) dem Tresen befindliche Kasse zu überwachen, insbesondere um sog. Wechselgeldbetrug oder andere schädigende Handlungen zu dokumentieren. In vielen Fällen waren die Kameras allerdings so ausgerichtet, dass sie außer der Kasse auch Bereiche hinter und/oder vor dem Tresen erfassten und somit Gäste oder Mitarbeiter, die einen Großteil ihrer Arbeitszeit dort verbringen, zum Gegenstand der Videoüberwachung wurden. Beides ist unzulässig. Denn Besucher einer Gaststätte haben eine berechtigte Erwartung dahin gehend, an diesem Ort – der der Freizeitgestaltung dient – nicht überwacht zu werden. Der Bereich hinter dem Tresen in einer Gaststätte oder Bar (ohne den unmittelbaren Kassenbereich) wiederum darf als solcher grundsätzlich nicht von Videokameras erfasst sein, da sich Beschäftigte dort typischerweise während eines Großteils ihrer Arbeitszeit aufhalten und somit einem permanenten Überwachungsdruck ausgesetzt wären, was – wie auch in der arbeitsgerichtlichen Rechtsprechung anerkannt ist – unzulässig ist. Wir haben in den von uns überprüften Fällen

die Änderung der Ausrichtung bzw. des Erfassungsbereichs der entsprechenden Kameras durchgesetzt.

20

Fahrzeugdaten

20 Fahrzeugdaten

20.1 Mustertexte zur Kfz-Halter- und Fahrerinformation

Die Datenschutzaufsichtsbehörden haben mit dem Verband der Automobilindustrie einen Informations-Mustertext für Kfz-Halter und -Fahrer vereinbart.

Jedes Fahrzeug ist in Deutschland mit einer eindeutigen Fahrzeugidentifizierungsnummer (FIN) und einem Kfz-Kennzeichen versehen. Über diese Merkmale und eventuelle weitere Informationen sind Daten, die in einem Fahrzeug gespeichert oder daraus übermittelt werden, auf den gegenwärtigen oder auf ehemalige Halter bzw. Fahrer des Fahrzeugs rückführbar und können daher personenbezogene Daten im Sinne des Datenschutzrechts sein.

Solche Daten lassen je nach Ausstattung und eventueller Online-Anbindung eines Fahrzeugs gegebenenfalls Rückschlüsse auf das Fahr- und Nutzungsverhalten, den Standort oder die Fahrtroute zu. Um hier für eine angemessene Transparenz zu sorgen, haben die Datenschutzaufsichtsbehörden im Arbeitskreis Verkehr mit dem Verband der Automobilindustrie (VDA) einen Mustertext für die Information von Kfz-Haltern und -Fahrern entwickelt, den die Datenschutzkonferenz im Februar 2018 veröffentlicht hat.

Der Mustertext Kfz ist auf der Website der DSK abrufbar:

www.datenschutzkonferenz-online.de/media/ah/201802_ah_vda_mustertext.pdf

20.2 Kameranutzung im Kfz für Forschungszwecke

Unter Berücksichtigung bestimmter datenschutzrechtlicher Rahmenbedingungen können Forschungsfahrzeuge zur Entwicklung von Systemen für das automatisierte Fahren auch mit Videokameras ausgestattet werden.

Zur sachgerechten Bewegung der künftig automatisiert fahrenden Kraftfahrzeuge ist die Verarbeitung einer großen Menge von personenbezogenen „Umfelddaten" im Bewegungsbereich des Fahrzeugs erforderlich, wie z. B. Bilder mit anderen Fahrzeugen, Fußgängern, Radfahrern usw. Es stellt sich deshalb für die Forschung dazu die Frage, wie die Projekte zur Entwicklung entsprechender Steuerungssysteme datenschutzkonform möglich sind.

Personenbezogene Videoaufnahmen aus Kraftfahrzeugen heraus für Forschungs- und Entwicklungszwecke im Sinne von Art. 89 DS-GVO und Nrn. 156 sowie 159 der ErwGr. für das automatisierte Fahren sehen wir dann als datenschutzrechtlich zulässig an, wenn die Grundsätze von Art. 5 Abs. 1 DS-GVO eingehalten werden, nämlich

- Transparenz (Hinweis-Aufkleber),
- strenge Zweckbindung ausschließlich für die festgelegten Forschungszwecke und
- Datenminimierung auf das unbedingt notwendige Maß.

Wir gehen dabei von einer Informationspflicht zu den Videoaufnahmen nach Art. 13 DS-GVO aus, zur deren Umsetzung ein Aufkleber mit Kamerasymbol oder dem Begriff „Videoüberwachung" und einem Hinweis auf den Forschungszweck der Firma XY sowie einem Internet-Link für weitere Informationen verwendet werden

kann. Gerade wenn solche Fahrzeuge an Ampeln stehen, langsam fahren, halten oder parken, können sich Passanten informieren bzw. sich auf eventuelle Videoaufnahmen einstellen.

Es müssen hierzu außerdem geeignete technische und organisatorische Maßnahmen getroffen werden, um die Rechte und Freiheiten der natürlichen Personen (z. B. Passanten, Fahrzeuginsassen etc.) zu schützen. Neben Maßnahmen zur Datensicherheit sehen wir insbesondere die Gewährleistung der Zweckbindung der Forschungs- und Entwicklungsdaten als wichtigen Punkt an. Allgemeine Maßnahmenklassen hierzu sind z. B. die Pseudonymisierung (sofern machbar), der Einsatz von Rollen- und Rechtekonzepten, geeignete Richtlinien samt Schulungen der Mitarbeiter, eine revisionsfeste Protokollierung der Zugriffe auf diese Daten sowie die Sicherstellung, dass auch eventuell eingebundene Dienstleister sich an diese technischen und organisatorischen Maßnahmen halten.

21

Datenschutzverletzungen

21 Datenschutzverletzungen

Eine Verpflichtung für datenschutzrechtlich Verantwortliche, Vorfälle im Umgang mit personenbezogenen Daten bei der Aufsichtsbehörde zu melden, gab es in Deutschland bereits unter dem BDSG-alt und dem TMG. Gemäß § 42a BDSG-alt bzw. § 15a TMG waren Datenschutzverletzungen, umgangssprachlich auch Datenpannen genannt, vereinfacht gesagt dann zu melden, wenn zwei wesentliche Voraussetzungen erfüllt waren: Zum einen mussten bestimmte Datenkategorien bei dem Vorfall betroffen sein (z. B. Gesundheitsdaten, Kreditkarteninformationen), zum anderen mussten auch schwerwiegende Beeinträchtigungen für die betroffenen Personen drohen.

Unter der DS-GVO wurde die bestehende Meldeverpflichtung bei Datenschutzverletzungen geändert und an den neuen, risikoorientierten Ansatz der DS-GVO angepasst. So mussten sich nicht nur die Verantwortlichen, sondern auch wir an die neuen Abläufe bei Sicherheitsvorfällen gewöhnen.

Es wird nun zwischen einer Meldung an die zuständige Aufsichtsbehörde (Art. 33 DS-GVO) und einer Benachrichtigung der betroffenen Personen (Art. 34 DS-GVO) in Abhängigkeit des Risikos für deren Rechte und Freiheiten unterschieden:

- Bei einem hohen Risiko (vergleichbar mit den schwerwiegenden Beeinträchtigungen nach § 42a BDSG-alt) müssen sowohl die Aufsichtsbehörde als auch die betroffenen Personen benachrichtigt werden.
- Bei einem (normalen) Risiko ist nur die Aufsichtsbehörde zu benachrichtigen, nicht aber die betroffenen Personen.
- Falls bei einer Datenschutzverletzung kein Risiko vorliegt, besteht keine Meldeverpflichtung – die interne Dokumentation des Vorfalls muss trotzdem durchgeführt werden.

Folglich führte die neue Meldeverpflichtung nach Art. 33 DS-GVO bei uns seit dem 25. Mai 2018 zu einer unausweichlichen, signifikanten Steigerung der eingehenden Meldungen von Datenschutzverletzungen. Dabei fand bei uns nicht nur ein reines Verwalten und Abheften der Meldungen statt, sondern immer auch eine Prüfung nach folgendem groben Grundschema:

- Wurde die Risikoeinschätzung vom Verantwortlichen richtig durchgeführt?
- Wurden bei hohem Risiko die betroffenen Personen informiert?
- Sind die eingeleiteten Abhilfemaßnahmen zur Schadenseindämmung ausreichend?
- Wurde die Ursache der Datenschutzverletzung, sofern strukturell bedingt, durch geeignete technische und organisatorische Maßnahmen zur Minderung der Wahrscheinlichkeit zukünftiger Vorfälle erkannt und beseitigt?

Wir haben im Berichtszeitraum 2017/2018 insgesamt 2607 Meldungen erhalten, wobei 2376 davon gemäß Art. 33 DS-GVO seit dem 25. Mai 2018 eingingen. Die Kategorien der Vorfälle sind vielfältig, wobei bereits Tendenzen und Muster hinsichtlich zu meldender Vorfälle erkennbar sind. Über 90% davon lassen sich in die Kategorien Cyberangriffe, Phishing, Verschlüsselungstrojaner, Malware, Verlust, Diebstahl, Fehlversendung, Fehlentsorgung und Softwarefehler einordnen. Dabei kommt weit über die Hälfte dieser Datenschutzverletzungen tatsächlich aus dem Bereich der fehlerhaften Versendungen von Daten (z. B. per Post), die jedoch meist ein nicht allzu hohes Risiko für die betroffenen Personen besitzen und daher bei uns auch schnell abgeschlossen werden können.

Demgegenüber stehen Vorfälle, die als deutlich kritischer einzustufen sind: Cyberattacken mit hohem Risiko – oftmals sogar mehrere tausend

betroffene Personen. Hier haben meist Kriminelle eine klare Schadensabsicht, um gezielt an Daten zukommen und diese dann für verschiedene Zwecke zu missbrauchen. Wir haben in den vergangenen zwei Jahren einen rasanten Anstieg solcher Cyberangriffe in Bayern registriert. Es ist nun auch keine Seltenheit mehr, dass dabei Vereine, Selbstständige, kleine Betriebe und Ärzte Opfer dieser kriminellen Machenschaften werden. In den nachfolgenden Ausführungen widmen wir uns daher speziell ausgewählten Vorfällen aus dem Cybersicherheitsumfeld, um zu zeigen, dass dort eine ernstzunehmende Bedrohung für Verantwortliche vorhanden ist und wir mit einem weiteren Anstieg der Meldungen von Cyberattacken rechnen.

21.1 Sicherheitslücke bei Hotelbuchungssoftware

Gerade durch die Eingabe von Kreditkartendaten ist Hotelbuchungssoftware für Cyberkriminelle besonders attraktiv.

Im Jahr 2017 erhielten wir Meldungen von verschiedenen bayerischen Hotels, die auf dem gleichen Sachverhalt beruhten. Cyberkriminellen war es gelungen, in eine weit verbreitete Hotel-Management-Software, mit der auch Online-Buchungen auf den jeweiligen Hotel-Websites durchgeführt wurden, Schadcode einzuschleusen. Dadurch konnten die Angreifer die Kreditkartendaten von Übernachtungsgästen bei Buchungen abfangen und an einen ausländischen Server übertragen.

Während von einem deutschen Landeskriminalamt die Abteilung Cyberkriminalität tätig wurde und die Strafverfolgung bzw. die Ermittlung der Tätergruppe anging, haben die vom Hacking-Vorfall betroffenen Hotels eine Meldung nach § 42a BDSG-alt durchgeführt. Als Datenschutzaufsichtsbehörde war es unser Hauptanliegen zu prüfen, wie es zu dem Vorfall kam und welcher Schaden für die betroffenen Personen eingetreten war.

Der Dienstleister, der Anbieter der Hotel-Software ist, hat sich im Rahmen der Aufarbeitung transparent verhalten und die Hotels zeitnah und umfassend über den Vorfall unterrichtet. Somit verfügten die Hotels über die notwendigen Angaben, um bei uns eine formelle Meldung durchzuführen.

Im Ergebnis war festzustellen, dass die gehackten Hotels eine veraltete Version der Software einsetzten, die eine Schwachstelle besaß. Die Vorfallsaufarbeitung zeigte jedoch, dass der Informationsaustausch zwischen dem Anbieter der Software und seinen Kunden, den Hotels, über neue Software-Releases und bestehende Sicherheitslücken in den älteren Versionen in der Vergangenheit keinesfalls ausreichend war. Manche Hotels gaben uns gegenüber an, überhaupt nicht gewusst zu haben, dass es eine neuere Version gab. Entsprechend gab es hier zwischen den Vertragspartnern eine lebendige Diskussion über den Vertragsgegenstand, insbesondere wer dafür verantwortlich ist, die eingesetzte Software bei bekannten Lücken zeitnah zu patchen.

Von den Vorfällen waren tausende Personen betroffen, von denen sich auch einige direkt bei den Hotels meldeten (Anzahl im dreistelligen Bereich) und über unberechtigte Abbuchungen von ihren Kreditkarten beschwerten. Die Hotels, die sich bei uns meldeten, informierten alle betroffenen Gäste über den Datenschutzvorfall. Zudem gab es Hotels, die sich hervorragend um eine Schadensbegrenzung bemüht hatten, indem den Gästen alle Aufwendungen im Zusammenhang mit dem Kreditkartenmissbrauch ersetzt wurden (u. a. für die Sperrung der Kreditkarte und die Rückforderung von unerlaubt abgebuchten Beträgen). Im Nachgang des Sicherheitsvorfalls wurden von den Verantwortlichen

alle technischen und organisatorischen Maßnahmen einer erneuen Überprüfung unterzogen und an die aktuelle Situation angepasst.

Gegen Ende des Berichtszeitraums wurde ein umfassender Datendiebstahl bei einem sehr großen, ausländischen Hotelkonzern bekannt. Dort wurden hunderte Millionen Datensätze von Hotelgäste ebenfalls über das Reservierungssystem abgegriffen. Da auch bayerische Hotels zu der Hotelkette gehörten, baten uns einzelne davon um Unterstützung. Die Aufarbeitung war zum Zeitpunkt des Drucks dieses Tätigkeitsberichts jedoch nicht abgeschlossen, sodass aktuell noch nicht absehbar ist, welche bayerischen Hotels und wie viele Gäste dort betroffen waren.

21.2 Kryptomining auf Webservern

Unzureichend geschützte Serverressourcen werden von Kriminellen auch zum Schürfen von Kryptowährungen verwendet.

Kryptowährungen sind seit einigen Jahren auf dem Vormarsch. Da solche Währungen nicht von Banken oder Staaten ausgegeben werden und das Mining (Schürfen der Währung) an sich von jedem selbst durchgeführt wird, aber recht ressourcenaufwendig ist, nutzen manche Kriminelle die Ressourcen fremder Hardware, um dort Mining zu betreiben.

In einem uns vorgetragenen Fall wurde bei einem Verantwortlichen eine Sicherheitslücke auf der eigenen Website entdeckt. Im verwendeten Content Management System wurden durch die Lücke fremde PHP-Dateien eingeschleust und ausgeführt, um ein solches Mining zu betreiben. Dadurch kam es zu einer enorm hohen CPU-Last, weshalb das Server-Monitoring-System Alarm schlug.

Es konnten zwar schnell die schadhaften Dateien entdeckt und entfernt werden, jedoch stellte sich die Frage, ob und in welchem Umfang personenbezogene Daten involviert waren. Die Website verfügte über einen Kundenlogin-Bereich, sodass der Verdacht im Raum stand, dass dort Nutzerkennungen mit Passwörtern abgefangen und womöglich auch Account-Daten abhandengekommen waren.

Nach näherer Untersuchung durch einen Dienstleister gab es im Ergebnis allerdings keine Anzeichen für einen Diebstahl von Nutzerdaten. Durch die zeitnah ergriffenen technischen und organisatorischen Maßnahmen sahen wir kein nennenswertes Risiko für die Nutzer, da durch den schadhaften Code nicht die Nutzerdaten im Angriffsfokus standen, sondern die Serverressourcen.

Festzuhalten ist allerdings, dass eine pauschale datenschutzrechtliche Bewertung solcher Sicherheitsvorfälle nicht möglich und auch nicht zielführend ist. Die einzelnen Sachverhalte müssen individuell geprüft werden, um festzustellen (oder auszuschließen), dass der Schutz personenbezogener Daten nach Art. 33 DS-GVO verletzt wurde.

21.3 Erpressung nach Cyberangriff

Nach erfolgtem Datendiebstahl verlangen kriminelle Hacker oft ein Lösegeld dafür, dass die entwendeten Daten nicht veröffentlicht werden.

Wir erhielten zuletzt einige Meldungen über verschiedene Erpressungen bayerischer Firmen, bei denen personenbezogene Daten im Mittelpunkt standen. In den meisten Fällen lief dies wie folgt ab: Ein Angreifer nutzte eine vorhandene Sicherheitslücke auf einer Website bzw. einen Webserver aus und drang in das System ein. Aus der Datenbank zog er alle Kundendaten samt Passwörtern ab. Anschließend konfrontierte er das Unternehmen damit, dass er im Besitz der Kundendaten war. Dabei wurden entsprechende Screenshots oder andere Auszüge aus der Datenbank als Beweis beigefügt. Der

Angreifer drohte, die Kundendaten zu veröffentlichen, die Presse einzuschalten und die Kunden selbst über die gestohlenen Daten durch die Sicherheitslücke zu informieren, um dadurch dem Unternehmen einen Imageschaden zuzufügen. Als Lösung bot er an, dass das Unternehmen ihm mehrere tausend Euro in Form von Bitcoins innerhalb weniger Stunden überweist – dann würde er von einer Veröffentlichung absehen.

Die Unternehmen verweigerten jeweils die Zahlung und schalteten stattdessen die Polizei ein. Da nachweislich eine Verletzung des Schutzes personenbezogener Daten stattgefunden hat, machten sie auch eine Meldung nach Art. 33 DS-GVO bei uns als zuständige Aufsichtsbehörde.

Wir waren bemüht herauszufinden, wie schwerwiegend der Vorfall war. Relevant war dabei insbesondere, ob die Sicherheitslücke noch besteht, sichergestellt werden kann, dass keine Systeme mehr infiziert bzw. infiltriert sind und wie hoch die Schwere des Schadens für die betroffenen Personen ist. In einigen Fällen waren die Passwörter nicht sonderlich gut verschlüsselt, sodass davon auszugehen war, dass auch viele von den Passwort-Hashes mühelos geknackt werden konnten. Im Ergebnis bedeutete das, dass Art. 34 DS-GVO erfüllt war und die Verantwortlichen die betroffenen Nutzer bzw. Kunden aktiv über den Datendiebstal unterrichten mussten.

21.4 Kundendaten aus Shop-System online einsehbar

Mangelnde Sorgfalt bei Konfigurations- und Wartungsarbeiten am Server können dazu führen, dass Kundendaten im Internet öffentlich einsehbar sind.

Gelegentlich werden wir von Unternehmen darüber informiert, dass durch fehlerhafte Konfigurationen Daten ungewollt im Internet abrufbar waren. Bei einem solchen uns vorgetragenen Sachverhalt kam es durch eine technische Nachlässigkeit des beauftragten Dienstleisters zu einem Fehler im Umgang mit der Kundendatenbank. Ein Datenbankdump, in dem unter anderem die E-Mail-Adressen und Passwörter der Kunden gespeichert waren, lag ohne Zugriffsschutz öffentlich zugänglich auf dem Webserver.

Nach Kenntniserlangung wurde der Datensatz unverzüglich entfernt und eine umfassende Sicherheitsanalyse samt Penetrationstest durchgeführt. Um festzustellen, ob der Dump überhaupt von jemanden gefunden und abgerufen wurde, fand eine Analyse der Logfiles statt. Diese ergab, dass einzelne Downloads stattfanden und somit tatsächlich Unbefugte Einblick in die Daten genommen hatten. Insgesamt waren von diesem Vorfall mehrere tausend Kundenaccounts betroffen.

Sicherheitsvorkommnisse dieser Art sind keine Seltenheit. In der Vielzahl der Fälle ist die Meldepflicht nach Art. 33 DS-GVO uns gegenüber erfüllt. Ob jedoch auch die betroffenen Personen nach Art. 34 DS-GVO informiert werden müssen, hängt u. a. stark davon ab, wie das Verfahren zur Passwortspeicherung ausgestaltet war. Hier zeigt sich, wie wertvoll präventive Maßnahmen zur Sicherheit der Verarbeitung personenbezogener Daten nach Art. 32 DS-GVO sind, die bei Cyberangriffen schadenshemmende Wirkung entfalten können.

21.5 Phishing-Attacke bei KRITIS-Einrichtungen

Energieversorger und andere KRITIS-Einrichtungen waren Ziel von großangelegten Cyberangriffskampagnen.

Im Sommer 2018 warnte das Bundesamt für Sicherheit in der Informationstechnik (BSI) öffentlich, dass deutsche Unternehmen aus der Energiewirtschaftsbranche das Ziel eines weltweiten

Angriffs waren. Angreifer nutzten demnach unterschiedliche Methoden, um in die Büro-Netzwerke der Unternehmen einzudringen und dann Vorbereitungen für weitere Angriffe zu treffen, z. B. um auf Produktions- oder Steuerungsnetzwerke zu gelangen.

Die entsprechende Pressemitteilung des BSI ist auf dessen Website öffentlich abrufbar:

www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Cyber_Angriffe_auf_deutsche_Energieversorger_13062018.html

Wir erhielten von verschiedenen Energieversorgen aus Bayern die Information, dass dort solche Angriffsversuche festgestellt werden konnten. In vereinzelten Fällen kam es dazu, dass Mitarbeiter des jeweiligen Verantwortlichen auf Phishing-E-Mails hereinfielen und dort dienstliche Zugangsdaten preisgaben. Anschließend konnten Zugriffe von fremden IP-Adressen registriert werden.

Im Ergebnis zeigte sich bei den Meldungen von Datenschutzverletzungen, die hierzu bei uns eingingen, dass keine kritischen Netzwerke der Verantwortlichen infiltriert werden konnten. Die betroffenen Energieversorger reagierten unverzüglich mit geeigneten Maßnahmen, um die angegriffenen Rechner zu schützen und die Mitarbeiter zu sensibilisieren. Bei den wenigen, erfolgreichen, unbefugten Zugriffen auf das Büro-Netzwerk konnte kein weiterer Schaden angerichtet werden. Somit waren unseres Wissens nach zu keinem Zeitpunkt die Daten der Kunden der Energieversorger gefährdet noch die Energieversorgung selbst. Dennoch zeigt sich dadurch, dass die Bedrohungslage im Cyberraum gerade für KRITIS-Betreiber eine ernstzunehmende Gefahr darstellt.

21.6 Hacking von eBay-Accounts

Wichtige Online-Zugänge sollten nicht nur mit einem Passwort geschützt werden, sondern am besten auch mit einem zweiten Faktor oder anderen Sicherheitsmaßnahmen.

Bayerische Firmen berichteten uns im Rahmen der Meldung von Datenschutzverletzungen darüber, dass ihr Zugang zum eigenen geschäftlichen Konto auf der Verkaufsplattform eBay unbefugt übernommen wurde. Dabei fand entweder ein schlichtes Passwort-Hacking (bzw. auch Erraten) statt oder es wurde durch Social Engineering (Spear-Phishing-Attacken) versucht, an die Zugangsdaten zu gelangen. Der Angreifer konnte dann im jeweiligen Firmenaccount die Zahlungsdaten ändern, um dadurch den Betrag für ersteigerte bzw. gekaufte Artikel an das eigene Konto zu überweisen.

Während als Sofortmaßnahme der eBay-Account erst kurz gesperrt wurde und dann durch ein neu vergebenes Passwort wieder im Besitz des Verantwortlichen war, wurden die Käufer informiert, die bereits einen Betrag an das falsche Konto überwiesen hatten. Im Fokus des Angreifers stand somit die finanzielle Bereicherung und nicht das Abgreifen von personenbezogenen Daten.

Die betroffenen eBay-Accounts der Unternehmen enthielten auch eine Bestellhistorie, die Kundendaten zu vergangenen Käufen umfasste – insgesamt mehrere tausend Kunden. Hierbei wurde durch den Verantwortlichen jeweils gemeinsam mit eBay geklärt, ob Zugriffe durch die fremde IP-Adresse des Angreifers in diesem Bereich, d. h. auf diese Daten, registriert wurden. In allen Fällen konnte dies ausgeschlossen werden, sodass Art. 34 DS-GVO nicht erfüllt war.

Im Ergebnis zeigte sich hier, dass ein geeigneter Zugangsschutz für Online-Accounts von großer

Bedeutung ist. Mit einer Zwei-Faktor-Authentifizierung (z. B. SMS-Code oder App-Token) kann man vielen klassischen Online-Passwortattacken vorbeugen. Leider bieten immer noch verhältnismäßig wenige Websites diesen erhöhten Schutz an, obwohl gerade im geschäftlichen Umfeld, wenn bspw. Firmen große Accounts bei eBay nutzen, dadurch Angreifern der Zugriff deutlich erschwert werden würde. Falls Online-Zugänge dagegen nur durch ein einzelnes Passwort abgesichert werden, muss dieses zwangsläufig von ausreichender Stärke sein, damit zumindest klassische Passwortattacken keine ernst zu nehmende Gefahr darstellen.

21.7 Angriffe auf den Login bei Online-Shops

Online-Shops stehen im Dauerfeuer von Angriffen – nur aktuell gehaltene Systeme können diesen effektiv standhalten und Kundenlogins angemessen schützen.

Mehrfach meldeten uns Betreiber von Online-Shops, dass Cyberangriffe gezielt auf die Zugänge ihres Shops stattgefunden haben. Meist wurden innerhalb sehr kurzer Zeitintervalle tausende Angriffsversuche gestartet, indem mit bekannten Kombinationen aus E-Mail-Adressen und Passwörter der Login von verschiedenen IP-Adressen angesteuert wurde. Hintergrund dazu ist, dass durch vergangene Hacking-Vorfälle und Leaks bereits Milliarden von Zugangsdaten im Internet kursieren. Auszüge davon probieren die Angreifer bei verschiedenen Websites aus, da manche Nutzer dazu neigen, dasselbe Passwort bei mehreren Diensten zu nutzen.

In den uns gemeldeten Fällen konnten die Angreifer erfolgreich in einige Accounts gelangen und dort entweder Datendiebstahl betreiben oder versuchen, Bestellungen auf fremde Rechnungsadressen durchzuführen. Die jeweiligen Accounts wurden zwar sehr schnell gesperrt, jedoch war davon auszugehen, dass zumindest die Daten der Kunden vollständig eingesehen bzw. kopiert wurden. Die Shop-Anbieter haben in diesen Fällen die betroffenen Kunden informiert und ihren Support angewiesen, für Rückfragen der Kunden bereitzustehen. Im Hinblick auf die technischen Maßnahmen zum Schutz personenbezogener Daten wurde eine Überprüfung durchgeführt und festgestellt, dass eine Nachbesserung notwendig ist.

Wir wurden in den vergangenen beiden Jahren bestätigt, dass die Angriffe auf Websites weiter zunehmen und Online-Shops besonders gefährdet sind. Entsprechend wichtig war und ist es, alle dazugehörigen Systeme aktuell zu halten – unabhängig davon, ob es sich um das Betriebssystem des Webservers handelt, die Software des Content Management Systems oder die Datenbankversion zur Verwaltung der Kundendaten. Cyberangriffe auf Logins bei Websites sind vielfältig – entsprechend vielfältig müssen daher auch die Schutzmaßnahmen sein, die der Verantwortliche proaktiv und präventiv ergreift.

21.8 Ransomware-Befall

Ransomware verursacht bei Ärzten und Betrieben nicht nur Probleme im Tagesablauf, sondern zum Teil auch ganze Behandlungs- bzw. Produktionsausfälle.

Das BSI informierte öffentlich über die Gefahren sog. Ransomware. Gemeint sind damit Schadprogramme, die das Ziel haben, Dateien auf privaten oder dienstlichen Arbeitsplatzrechnern zu verschlüsseln und die Daten nur gegen Zahlung eines Lösegelds wieder freizugeben. Es handelt sich somit schlichtweg um Erpressungssoftware.

In den letzten beiden Jahren haben wir einige Meldungen zu Datenschutzverletzungen erhalten, deren Gegenstand eine solche Ransomware war. Durch den Befall mit dieser Schadsoftware war die Verfügbarkeit personenbezogener Daten nicht mehr gewährleistet und somit oft die Meldepflicht nach Art. 33 DS-GVO erfüllt. Ursache war in einigen Fällen wohl der Faktor

Mensch: Ein Mitarbeiter klickte unvorsichtig auf einen präparierten Link oder öffnete schadhafte Dateianhänge in E-Mails. Kurze Zeit später stellten die Organisation dann fest, dass der Zugriff auf Dateien am Arbeitsplatz nicht mehr wie gewohnt möglich war, die Dateien kryptische Dateiendungen besaßen und plötzlich Lösegeldforderungen auf Englisch am Desktop erschienen. Man wurde aufgefordert, per Bitcoin einen Betrag für die Wiederfreigabe der Daten zu überweisen.

In den uns vorgetragenen Fallkonstellationen war größtenteils ein relativ aktuelles Backup vorhanden, so dass die Unternehmen nach Bereinigung der Systeme durch einen spezialisierten IT-Dienstleister wieder den Betrieb in gewohnter Weise aufnehmen konnten. Die Kosten durch die Ransomware-Attacke waren dort dann meist eher niedrig und im hohen dreistelligen oder niedrigen vierstelligen Euro-Bereich anzusiedeln.

Bei den Firmen, die jedoch entweder sehr viele infizierte Arbeitsplatzrechner hatten oder bei denen zentrale Fileserver betroffen waren, dauerte die Aufarbeitung deutlich länger. Zum Teil musste auch neue Hardware beschafft werden. Die Kosten dafür waren dann nicht mehr so gering, sondern schnell im mittleren fünfstelligen Bereich. In wenigen Einzelfällen war in Produktionsbetrieben durch die Cyberattacke sogar der Produktionsablauf gestört. Hier wurden dann deutlich größere wirtschaftliche Schäden spürbar.

Überraschend viele Meldungen gingen von Ärzten bei uns ein: Gerade im medizinischen Umfeld kann sich Ransomware besonders kritisch auswirken, da sich durch den fehlenden Zugriff auf Patientendaten oftmals keine gezielten Behandlungen mehr durchführen lassen. Nicht alle Arztpraxen waren gut auf solche Sicherheitsvorfälle vorbereitet: Entweder war keine aktuelle Datensicherung verfügbar oder man hatte Anlaufschwierigkeiten, das Backup in das zurückgesetzte System einzuspielen. Die betroffenen Ärzte mussten dadurch erkennen, wie abhängig mittlerweile die Behandlung von IT-Systemen ist und wie fragil dieses Gebilde sein kann. Dies war auch Anlass unserer Datenschutzprüfung zu Ransomware bei Ärzten im Herbst 2018, siehe Kapitel 4.9 dieses Berichts.

Da solche Vorkommnisse mittlerweile keine Seltenheit mehr sind, fangen viele Großbetriebe und Kliniken an, sich gezielt auf den Befall mit Ransomware vorzubereiten, damit die Abläufe im Ernstfall funktionieren und eingespielt sind. Wir haben 2018 im Rahmen einer solchen Cybersicherheitsübung eines Klinikums die Meldung einer Datenschutzverletzung des Verantwortlichen entgegengenommen und bei der datenschutzrechtlichen Aufarbeitung des Sicherheitsvorfalls unterstützt.

21.9 Hacking eines Webhosting-Providers

Durch Sicherheitsvorfälle bei Hosting-Anbietern kann eine Meldekette ausgelöst werden, da dortige Firmenkunden meist als Verantwortliche agieren und unter Umständen selbst die Aufsichtsbehörden informieren müssten.

Ein sehr großer Hosting-Anbieter aus Bayern wurde Mitte 2018 Opfer eines Cyberangriffs. Über öffentlich verfügbare Informationen bestand zunächst erst das Verdachtsmoment, dass ein Unbefugter sich Zugang zu den Systemen des Hosters verschafft haben könnte. Im Laufe der anschließenden Untersuchung stellte das Unternehmen fest, dass sich tatsächlich ein Krimineller Zugang zu den Systemen des Hosters verschafft hatte.

Das Unternehmen führte daher eine Meldung nach Art. 33 DS-GVO bei uns durch, da der Sitz des Hosting-Unternehmens in Bayern war. Bei solchen Dienstleistern, die Auftragsverarbeitung für Unternehmen anbieten, besteht jedoch

eine Besonderheit: Sollte es dort zu einer Datenschutzverletzung im Umgang mit den Kundendaten der Auftraggeber kommen, so müssen auch die Auftraggeber selbst als Verantwortliche eine Meldung nach Art. 33 DS-GVO durchführen, nachdem sie vom Dienstleister über den Vorfall unterrichtet wurden. Art. 33 Abs. 2 DS-GVO führt dies entsprechend aus:

> *„Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich."*

Unser Anliegen war es daher, schnell zu klären, ob die Datenschutzverletzung nur den Hoster selbst betraf oder womöglich auch die Kundendaten dessen Kunden. In der Presse wurde umfangreich über die Datenschutzverletzung – dem Hack des Dienstleisters – berichtet. Ein regelrechtes Mediengewitter brach über den Hoster herein. Auf Grund dessen machten deutschlandweit einige Unternehmen, die Dienste bei dem Hoster angemietet hatten, eine vorsorgliche Meldung nach Art. 33 DS-GVO bei der jeweils zuständigen Aufsichtsbehörde – ohne jedoch genau angeben zu können, was überhaupt passiert war. Dementsprechend meldeten sich die anderen Aufsichtsbehörden, die eine solche Meldung erhielten, wiederum bei uns als die für den Hoster zuständige Aufsichtsbehörde und erkundigten sich nach dem Sachstand.

Trotz intensiven Schriftverkehrs und vieler Telefonate mit der Geschäftsführung des Hosters gab es Fragen, die wir nicht klären konnten. Wir sahen uns deshalb veranlasst, im Rahmen einer Vor-Ort-Kontrolle alle erforderlichen Punkte persönlich zu klären. Das Hosting-Unternehmen zeigte sich dabei um eine transparente Aufarbeitung bemüht. Die mit dem Unternehmen verbundenen Konzern- und Systemstrukturen machten eine schnelle, abschließende datenschutzrechtliche Bewertung für uns unmöglich. Nach kurzer Zeit erschien jedoch absehbar, dass die Meldekette wohl nicht ausgelöst wird und die Kunden des Hosters selbst daher keine Meldung nach Art. 33 DS-GVO bei deren Aufsichtsbehörde machen mussten. Es waren zwar umfangreiche Kundendaten des Hosters betroffen, nicht jedoch Kundendaten der Hosting-Kunden selbst. Eine vom Hoster hinzugezogene externe Sicherheitsfirma untersuchte den Sachverhalt und konnte keinerlei Hinweise finden, dass außer des einen kriminellen Täters weitere Personen Zugriff auf die Systeme des Hosters hatten. Somit konnten wir uns auf die fachlich Aufarbeitung des Vorfalls bei dem Dienstleister konzentrieren.

Für uns war diese Art der Datenschutzverletzung neu: Es war die erste große Datenschutzverletzung bei einem Hosting-Anbieter in unserer Zuständigkeit, bei dem unter der DS-GVO zu klären war, ob die Meldekette ausgelöst wird und wir womöglich mit tausenden Meldungen von Unternehmen, den Kunden des Hosters, rechnen müssen. Wir erkannten zudem, dass wir als Aufsichtsbehörden noch keinerlei Erfahrung haben, wie unter uns der einfache und schnelle Informationsaustausch für Hacking-Vorfälle bei Hostern gelingen kann, damit man einerseits eine einheitliche Bewertung des Sachverhalts vornimmt und anderseits auch eine gemeinsame Kommunikationspolitik betreiben kann.

21.10 Cyberangriff durch Emotet

Die gefährliche Schadsoftware Emotet führt bei vielen Verantwortlichen nicht nur zu Datenschutzverletzungen, sondern auch zu immensen wirtschaftlichen Schäden.

Im Berichtszeitraum erhielten wir Meldungen nach Art. 33 DS-GVO über den Befall mit Emotet. Diese Schadsoftware galt 2018 als eine der gefährlichsten Bedrohungen im digitalen Umfeld, da sie sich besonders leicht verbreitet und großen Schaden anrichten kann. Das BSI warnte daher eindringlich vor dem neuen Schädling:

www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/BSI_warnt_vor_Emotet.html

Bayerische Unternehmen – vereinzelt aber auch Ärzte – informierten uns im Konkreten darüber, dass sie sich Emotet „eingefangen" hatten und dies zum Teil erst sehr spät selbst feststellten. Im Regelfall wurden die Verantwortlichen durch Beschwerden von Kollegen, Geschäftspartnern oder Bekannten darauf aufmerksam. Hintergrund dazu ist, dass bei einem Emotet-Befall authentisch aussehende Spam-Mails durch den Schädling an bekannte Kontakte verschickt werden. Emotet liest dafür Kontaktbeziehungen aus der erfolgten E-Mail-Korrespondenz aus. Damit können die hinter Emotet stehenden Cyberkriminellen gezielte Spam-Kampagnen gegen die vorgefundenen Kontakte durchführen und vortäuschen, die E-Mail komme vom jeweiligen Verantwortlichen (Social Engineering). Durch diese fingierten E-Mails kann sich der Schadcode bei den Empfängern weiterausbreiten.

Neben den persönlichen Informationen rund um die Kontakte können bei diesem Angriff auch weitere, unbefugte Zugriffe auf personenbezogene Daten des Verantwortlichen erfolgen. Somit besteht eine Meldeverpflichtung nach Art. 33 DS-GVO.

Emotet kann bei einer Infektion eines Systems, z. B. eines gewöhnlichen Arbeitsplatzrechners, weitere Schadsoftware nachladen, wodurch auch Zugangsdaten abgefangen werden können. Remote-Zugriffe durch die Angreifer sind keine Seltenheit. In einigen Unternehmen kam es deshalb zu ganzen Produktionsverzögerungen oder -ausfällen, da viele Rechner isoliert und bereinigt werden mussten. In uns bekannten Fällen musste meist das infizierte System vollständig neu aufgesetzt werden, da man nicht ausschließen konnte, dass Teile der Schadsoftware auf dem System trotz Löschbemühungen verblieben sind.

Hilfreiche Maßnahmen zum Schutz vor Emotet sowie Hilfe bei Infektion findet man auf der Website der Allianz für Cybersicherheit:

www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/E-Mailsicherheit/emotet.html

22

Zertifizierung

22 Zertifizierung

Die Rechenschaftspflicht der DS-GVO stellt einen Paradigmenwechsel im Umgang mit Datenschutzkontrollen dar. Die dafür erforderliche Nachweisbarkeit von geeigneten Strukturen, Prozessen sowie technischen und organisatorischen Maßnahmen ist dabei zumindest für datengetriebene Unternehmen und Konzerne keineswegs trivial.

Besonders herausfordernd wird es, wenn Dienstleister (z. B. im Rahmen einer Auftragsverarbeitung) eingebunden werden, die deutlich größer als das eigene Unternehmen sind und standardisierte Dienstleistungen anbieten – Cloud-Services sind ein Beispiel hierfür. Jeder Verantwortliche, der einen solchen Dienstleister einbindet, muss dessen datenschutzkonforme Verarbeitung überprüfen – soweit die Theorie. In den meisten Konstellationen ist dies jedoch praktisch unmöglich. Bei der Kontrolle von Dienstleister-Rechenzentren würde dies zudem wohl nur zu einem „Prüftourismus" führen, bei dem außer blinkende Server nicht viel zu sehen wäre.

Der europäische Gesetzgeber hat dieses Kontrollproblem adressiert und eine Lösung gefunden: Speziell genehmigte Datenschutzzertifizierungen, die als Nachweis im Sinne der Rechenschaftspflicht von Verantwortlichen eingesetzt werden können.

Solche Zertifizierungen werden in der DS-GVO explizit für folgende Bereiche genannt:

- Erfüllung der Pflichten des Verantwortlichen (Art. 24 Abs. 3)
- Erfüllung der Anforderungen an Technikgestaltung und datenschutzfreundliche Voreinstellungen des Art. 25 Abs. 1 und 2 (vgl. Abs. 3)
- Garantien des Auftragsverarbeiters nach Art. 28 (vgl. Abs. 5 und 6)
- Sicherheit der Verarbeitung (Art. 32 Abs. 3)
- Datenübermittlung an ein Drittland (Art. 46 Abs. 2 Buchstabe f)
- Datenschutz-Folgeabschätzung (ErwGr. 90)

Durchführen können solche Zertifizierungen entweder die Datenschutzaufsichtsbehörden selbst oder speziell akkreditierte, privatwirtschaftliche Unternehmen. Wir haben uns als BayLDA frühzeitig aus Kapazitätsgründen gegen eine Tätigkeit als Zertifizierungsstelle entschieden, sind jedoch maßgeblich in die Akkreditierung von solchen Stellen eingebunden. Gemäß Art. 43 DS-GVO und § 39 BDSG werden die Zertifizierungsstellen im Datenschutzbereich von der Deutschen Akkreditierungsstelle (DAkkS) gemeinsam mit der zuständigen befugniserteilenden Aufsichtsbehörde akkreditiert – die Zuständigkeit wird über den Hauptsitz der Zertifizierungsstelle bestimmt. Der Arbeitskreis Zertifizierung der deutschen Aufsichtsbehörden befand sich Ende des Berichtszeitraums noch in Abstimmung mit der DAkkS bezüglich der Rahmenbedingungen der Akkreditierung. Dabei werden auch die Entscheidungen des Europäischen Datenschutzausschusses berücksichtigt.

Sobald ein Unternehmen künftig erfolgreich den Akkreditierungsprozess durchläuft, darf es Datenschutzzertifizierungen im Sinne des Art. 42 DS-GVO vergeben. Diese Zertifizierungen muss die zuständige Aufsichtsbehörde im Blick behalten, damit das hohe Niveau, die Aussagekraft und die Anerkennung erhalten bleiben. Mehr Informationen zum Thema „Akkreditierung im Datenschutzbereich" sind auf den Websites der DAkkS und der DSK zu finden:

www.dakks.de/content/projekt-datenschutz
www.datenschutzkonferenz-online.de

23

Technischer Datenschutz und Informationssicherheit

23 Technischer Datenschutz und Informationssicherheit

23.1 Risikoorientierter Ansatz unter der DS-GVO

Der zentrale Risiko-Begriff ist das wesentliche Element für die Auswahl geeigneter Schutzmaßnahmen – Standardchecklisten für technische und organisatorische Maßnahmen haben ausgedient.

Der Begriff des „Risikos" zieht sich wie ein roter Faden durch die DS-GVO. Anhand dessen müssen geeignete und wirksame technische und organisatorische Maßnahmen ausgewählt werden. Es ergeben sich aber auch verschiedene Rechtsfolgen aus der Eingruppierung von Verarbeitungen personenbezogener Daten oder Vorfällen in die Risikoklassen der DS-GVO: kein Risiko, Risiko und hohes Risiko.

Im Rahmen unseres Kurzpapierprojektes haben wir schon im Jahr 2016 eine erste grobe Orientierung gegeben, wie die Risiko-Faktoren Eintrittswahrscheinlichkeit und Schwere eines Schadens nach objektiven Kriterien in Einklang gebracht werden konnten. Die deutschen Datenschutzaufsichtsbehörden haben zur Abstimmung einer gemeinsamen Sichtweise zu diesem Thema im Rahmen der Erstellung eines DSK-Kurzpapiers zusammengearbeitet. Das Ergebnis legt eine handhabbare Methode zur Bestimmung des Datenschutzrisikos unter der DS-GVO fest. Das Kurzpapier Nr. 18 „Risiko für die Rechte und Freiheiten natürlicher Personen" ist auf der DSK-Website zu finden:

www.datenschutzkonferenz-online.de/kurzpapiere.html

In folgenden Bereichen der DS-GVO ist eine Auseinandersetzung mit dem Datenschutzrisiko besonders relevant:

- Auswahl der wirksamen Sicherheitsmaßnahmen zur Risikoeindämmung (Art. 25 und 32 DS-GVO)
- Fragestellung, ob eine Datenschutz-Folgenabschätzung durchzuführen ist (Art. 35 DS-GVO)
- Entscheidung, ob bei nicht regelmäßiger Verarbeitung ein Verzeichnis der Verarbeitungstätigkeiten erstellt werden muss (Art. 30 DS-GVO)
- Meldung einer Datenschutzverletzung bei der Aufsichtsbehörde (Art. 33 DS-GVO) und bei den betroffenen Personen (Art. 34 DS-GVO)

Der risikoorientierte Ansatz bedeutet, dass gerade bei der Auswahl der technischen und organisatorischen Maßnahmen keine standardisierten Maßnahmenkataloge, die für alle Unternehmensgrößen und Arten gelten, verwendet werden können. Stattdessen werden passend für die konkrete Verarbeitung entweder eine detaillierte Risikobeurteilung (eher bei großen und datengetriebenen Unternehmen notwendig) oder Checklisten zugeschnitten auf den Typus des Verantwortlichen (z. B. Arztpraxis, Verein, Immobilienverwaltung, Online-Shop) eingesetzt. Dies ist im Vergleich zum BDSG-alt sowohl für den Verantwortlichen als auch die betroffenen Personen eine Verbesserung, da standardisierte Checklisten häufig manche schutzwürdige Bereiche (noch) nicht berücksichtigen oder schlicht mehr Ressourcen binden als nach dem Risiko notwendig wären.

Es empfiehlt sich, eine Risikobeurteilung nicht völlig unabhängig von der rechtlichen Beurteilung einer Verarbeitung zu sehen. Gerade bei der Interessenabwägung nach Art. 6 Abs. 1 Buchstabe f DS-GVO gibt es deutliche Überschneidungen, da eine Rechtmäßigkeit in der Regel nicht ohne eine Betrachtung des Datenschutzes durch Technikgestaltung (Art. 25 DS-GVO) und der Sicherheit der Verarbeitung (Art. 32 DS-GVO) bewertet werden kann.

23.2 Cybersicherheit als gesetzliche Datenschutzkomponente

Cyberkriminelle abzuwehren dient nicht nur den eigenen wirtschaftlichen Interessen, sondern ist auch gesetzliche Datenschutzanforderung für Verantwortliche zum Schutz personenbezogener Daten.

Auch in den vergangenen zwei Jahren wurde regelmäßig und vielfältig von neuen Sicherheitsvorfällen im Online-Umfeld in den Medien berichtet. Seien es Online-Shops, die gehackt wurden, Krankenhäuser, die aufgrund eines Kryptotrojaners stillstanden oder schwerwiegende Schwachstellen in Softwarekomponenten, über die komplette IT-Systeme übernommen werden konnten. Cybersicherheitsvorfälle dieser Art wurden uns meist im Rahmen von Datenschutzverletzungen direkt gemeldet (siehe Kapitel 21) oder von betroffenen Personen als Beschwerde vorgetragen.

Die Vorfallsaufarbeitung deckt dabei nur die reaktive Seite der Cybersicherheit ab. Nach Art. 32 DS-GVO müssen jedoch grundsätzlich Maßnahmen zur Sicherheit der Verarbeitung vom Verantwortlichen getroffen werden, um solchen Angriffen auch präventiv entgegenzutreten. Sicherheits- und somit auch Datenschutzverletzungen müssen aber nicht immer einen externen Angreifer oder eine kriminelle Datenverarbeitung als Ursache haben – es gibt auch Risiken in der rechtmäßigen Verarbeitung. Die DS-GVO unterscheidet dabei im Prinzip zwischen zwei Arten der Verarbeitung:

- Die rechtmäßige Verarbeitung: Bei dieser soll mittels Einhaltung der Zweckbindung, der Transparenz, einem Löschkonzept, der Sicherstellung der Betroffenenrechte etc. die Grundrechtsbeeinträchtigung für die betroffenen Personen durch die Verarbeitung reduziert bzw. so gering wie möglich gehalten werden.
- Die unrechtmäßige Verarbeitung: Hier ist es entweder nicht erlaubt und/oder zumindest nicht gewollt, dass personenbezogene Daten in einer bestimmten Weise verarbeitet werden, z. B. bei Hacking-Attacken, Hardwaredefekte durch Wasserschaden.

Der Art. 32 DS-GVO zur „Sicherheit der Verarbeitung" greift Punkte auf, die in der Informationssicherheit längst bekannt sind. Erfreulich ist, dass sich die DS-GVO an bewährten Methoden der Informationssicherheit orientiert und unter anderem neben dem risikoorientierten Ansatz und dem Stand der Technik (Art. 32 Abs. 1 DS-GVO) die Sicherheit personenbezogener Daten als Prozess (Art. 32 Abs.1 Buchstabe d DS-GVO) ansieht.

Verantwortliche müssen das Rad nicht neu erfinden, sondern werden in einer Vielzahl an bereits getroffenen IT-Sicherheitsmaßnahmen nun auch Maßnahmen erkennen, die den Anforderungen aus Art. 32 DS-GVO gerecht werden. Zielsetzung der DS-GVO ist die Herstellung eines angemessenen Schutzniveaus, das auch durch die bekannten Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität von Daten, IT-Systemen und Prozessen der Informationssicherheit beschrieben werden kann.

Eine Verletzung dieser Sicherheitsvorgaben kann zu einer Datenschutzverletzung führen, die unter Umständen der Meldepflichten nach Art. 33 und 34 DS-GVO unterliegt. Gravierender ist für Verantwortliche wohl aber, dass Mängel in der Sicherheit nunmehr als Datenschutzverstöße erstmals auch mit einem Bußgeld von bis zu 10 Mio. EUR oder 2% des Umsatzes bedroht sind. Spätestens mit dieser neuen gesetzlichen Sanktionskulisse wird bei vielen Verantwortlichen die Bereitschaft, in Datenschutz- und Sicherheitsmaßnahmen zu investieren, größer werden als unter dem BSDG-alt.

Da die Mehrheit der heutigen Datenverarbeitungen über Systeme und Netze stattfindet, die Bestandteil des Internets sind oder zumindest

an den Cyberraum in irgendeiner Weise angebunden sind, muss folglich die dort erforderliche Cybersicherheit als gesetzliche Datenschutzkomponente angesehen werden – Datenschutz ohne Cybersicherheit ist heutzutage undenkbar.

Gerade aufgrund der gestiegenen Gefährdungslage im Internet haben wir uns im Berichtszeitraum entschieden, unseren Fokus auf Maßnahmen zur Cybersicherheit für bayerische Verantwortliche zu stärken, damit diese personenbezogene Daten zeitgemäß, angemessen und wirksam vor den täglichen Gefahren im digitalen Zeitalter schützen. Cybersicherheit muss aber auch bewusst als gesetzliche Datenschutzkomponente kommuniziert und adressiert werden – ohne eine ausreichende Sicherheit der Datenverarbeitung kann letztendlich keine Compliance im Datenschutzumfeld erreicht werden. Wir haben im Herbst 2017 deshalb eine Cybersicherheitsinitiative gestartet, um den gesteigerten Anforderungen an die Cybersicherheit unter der DS-GVO Rechnung zu tragen. Durch flächendeckende, automatisierte Prüfungen zeigten wir bereits verschiedene Schwachstellen und Sicherheitslücken auf und sensibilisieren dadurch Verantwortliche in ganz Bayern. Nähere Informationen zu diesen Prüfungen im Cybersicherheitsumfeld sind im Kapitel 4 dieses Berichts zu finden.

23.3 Datenschutz durch Technikgestaltung

Der technische Datenschutz durchdringt als wichtiges Datenschutzelement fast alle Verarbeitungsbereiche.

Die Schärfung des technischen Datenschutzes unter der DS-GVO umfasst auch Bereiche abseits der Sicherheit der Verarbeitung. Schwerpunkt ist dabei die rechtmäßige Verarbeitung als solche, d. h. es geht dabei nicht um die Abwehr von Hackern. Stattdessen müssen Verantwortliche für Verarbeitungen, die eine Rechtsgrundlage besitzen, wirksame technische und organisatorische Maßnahmen ergreifen, um das Datenschutzrisiko einzudämmen. Dieses Konzept des „Privacy by Design" wird in Art. 25 DS-GVO durch den deutschen Begriff „Datenschutz durch Technikgestaltung" ausgerückt. Umgangssprachlich könnte man es als nunmehr gesetzlich verankerte Verpflichtung „Datenschutz von Anfang an" bezeichnen.

Eine konkrete Maßnahmenliste findet man – im Vergleich zu der Anlage des früheren § 9 BDSG-alt – nicht. Stattdessen müssen auch hier die Grundsätze der Verarbeitung aus Art. 5 Abs. 1 DS-GVO hergenommen werden, die insbesondere wären:

- Transparenz für die betroffenen Personen
- Datensparsamkeit
- Sicherstellung der Zweckbindung
- Kein Umgang mit personenbezogenen Daten, wenn dies nicht mehr erforderlich sind (z. B. Löschung, Anonymisierung)

Zusätzlich sind auch die Betroffenenrechte der DS-GVO mittels technischer und organisatorischer Maßnahmen wirksam umzusetzen. Zu beachten ist hierbei, dass die Einhaltung dieser Grundsätze auch durch die Rechenschaftspflicht nachgewiesen werden muss.

Die deutschen Aufsichtsbehörden schreiben momentan das schon lange existierende Standard-Datenschutzmodell fort, das sich schwerpunktmäßig auf die rechtmäßige Verarbeitung als solche bezieht und durch die Gewährleistungsziele einen ähnlichen und teils deckungsgleichen Ansatz wie die DS-GVO verfolgt. Technische und organisatorische Maßnahmen, die unter Geltung des BDSG-alt vorgesehen waren, können zum einem großen Teil weiter verwendet werden, wenn sie nachweisbar im Sinne der Grundsätze aus Art. 5 Abs. 1 DS-GVO eingesetzt werden.

23.4 Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung ist eine besondere Herangehensweise bei Verarbeitungen mit hohem Risiko.

Die DS-GVO besitzt durch ihren risikoorientierten Ansatz eine gute Skalierbarkeit zur wirksamen und verhältnismäßigen Auswahl der technischen und organisatorischen Maßnahmen. Sollte eine Verarbeitung in die Kategorie „hohes Risiko" fallen, dann greift Art. 35 DS-GVO zur Datenschutz-Folgenabschätzung, d. h. Verantwortliche sind dazu verpflichtet, diese für die Verarbeitung durchzuführen.

Technische und organisatorische Standardmaßnahmen müssen jedoch bereits angewendet bzw. mit einbezogen werden, bevor die Ermittlung des Risikos überhaupt durchgeführt werden kann. Ansonsten wäre einen Verarbeitungen mit hohen Risiko nicht die Ausnahme, sondern die Regel. Dies bedeutet, dass nach Anwendung von Art. 25 DS-GVO (Datenschutz durch Technikgestaltung) und Art. 32 DS-GVO (Sicherheit der Verarbeitung) im Prinzip eine Restrisikobeurteilung durchzuführen ist, um die Schwelle für ein „hohes Risiko" zu bestimmen. Relevant bei dieser Frage ist dann gerade, ob die getroffenen Standardmaßnahmen ausreichend wirksam und nachweisbar im Sinne der Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO sind.

Bei einer Videoüberwachung mit z. B. 20 Kameras in einem Einkaufszentrum kommt man in der Regel leicht zu einer wirksamen Risikoeindämmung durch technische und organisatorische Maßnahmen und deswegen in der Regel auch nicht zur Verpflichtung, eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO durchzuführen. Beim Einsatz von innovativen Verfahren der künstlichen Intelligenz dagegen dürfte es schwierig werden, das durchaus hohe Risiko mit Standardmaßnahmen einzudämmen. Es bedarf deswegen hier einer Unterstützung durch eine Datenschutz-Folgenabschätzung.

Wir wurden oft gefragt, wann eine Datenschutz-Folgenabschätzung erforderlich ist. Eine Liste mit Verarbeitungen, bei denen in der Regel ein hohes Risiko anzunehmen ist (sogenannte Black-List oder Muss-Liste), haben die deutschen Aufsichtsbehörden entwickelt und veröffentlicht. Diese ist auf der DSK-Website zu finden:

> *www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf*

Diese Liste hat bereits die erste Harmonisierungsrunde auf europäischer Ebene hinter sich gebracht und kann als verlässliche Orientierung für Verantwortliche verwendet werden. Anzumerken ist, dass es eine sogenannte White-List oder Nicht-Muss-Liste, auf der steht, bei welchen Verarbeitungen keine Datenschutz-Folgenabschätzung erforderlich ist, in Deutschland nach einer Mehrheitsentscheidung der deutschen Aufsichtsbehörden vorerst nicht geben wird. Ebenfalls ist zu beachten, dass Verarbeitungen, die sich (noch) nicht in der veröffentlichten Black-List wiederfinden, im Einzelfall durchaus ein hohes (Rest-)Risiko mit sich bringen können.

Basierend auf dieser Sichtweise sehen wir eine Datenschutz-Folgenabschätzung insgesamt als Ausnahme, die nur relativ wenige Unternehmen treffen dürfte. Falls diese durchgeführt werden muss, wird eine sehr umfangreiche Systembeschreibung, eine sorgfältige Modellierung der Datenflüsse sowie eine systematische Risikobeurteilung auch anhand der Ursachen des Risikos einschließlich einer umfangreichen Dokumentation erwartet. Anzumerken sei, dass die einfache Feststellung eines Datenschutzrisikos auf Basis des Verzeichnisses der Verarbeitungstätigkeiten nicht die Anforderungen der DS-GVO erfüllen.

Als Methoden für die Durchführung einer Datenschutz-Folgenabschätzung empfehlen wir

eine Anwendung der ISO-Norm 29134, wobei die gesetzlichen Anforderungen der DS-GVO vorrangig zur ISO-Norm umzusetzen sind. Auch das Standard-Datenschutzmodell sehen wir als geeignet an, sofern der Security-Ansatz durch weitere Methoden (z. B. IT-Grundschutz oder ISO 27001) berücksichtigt wird. Ebenso akzeptieren wir die Methode der französischen Aufsichtsbehörde CNIL, sofern die nicht-sicherheits-basierten Grundsätze angemessen und wirksam nachgewiesen werden. Weitere Verfahren wurden bislang noch nicht von uns bewertet und können selbstverständlich, sofern diese die DS-GVO umsetzen, ebenfalls angewendet werden.

Weitere Informationen zur DSFA sind auf unserer Website zu finden:

www.lda.bayern.de/de/dsfa.html

23.5 Wirksamkeitsprüfung im Rahmen der Rechenschaftspflicht

Technische und organisatorische Maßnahmen müssen auch auditiert und fortwährend angepasst werden.

Die Stärkung des technischen und organisatorischen Datenschutzes unter der DS-GVO trägt der Sichtweise Rechnung, dass Datenschutz als interdisziplinärer Ansatz verstanden und umgesetzt werden soll. Auf eine Neuerung möchten wir aber an dieser Stelle besonders hinweisen, da dies auch ein grundlegendes Detail in zukünftigen Datenschutzkontrollen sein wird.

Bei der Sicherstellung einer datenschutzkonformen Datenverarbeitung müssen technische und organisatorische Maßnahmen nicht nur umgesetzt, sondern deren Wirksamkeit durch einen unternehmensinternen Prozess regelmäßig überprüft und, falls erforderlich, verbessert werden. Dieser Prozess ist als dauerhafter Zyklus – bestehend aus folgende Phasen – zu verstehen:

- Planung und Umsetzung geeigneter technischer und organisatorischer Maßnahmen, einschließlich Planung der zugehörigen Kontrollen
- Betrieb der Verarbeitung personenbezogener Daten
- Bewertung in Form von Kontrollen, internen Audits (Überprüfungen) und Einbindung der Unternehmensleitung (Managementbewertung)
- Verbesserung durch Aktualisierung ungeeigneter technischer und organisatorischer Maßnahmen

Während datengetriebene und große Unternehmen einen besonderen Blick auf die eigenen Prozesse und Richtlinien werfen müssen, können kleine und mittelständische Unternehmen die Wirksamkeitsprüfung durch eine regelmäßige (z. B. jährliche) Bewertung der Verarbeitungsverzeichnisse und der darauf aufbauenden Anforderungen umsetzen. Der Aufwand für „Kleinere" hält sich daher in Grenzen, während von Großunternehmen ein entsprechender, interner Prüfprozess gelebt werden muss.

23.6 Facebook-App-Entwickler im Prüffokus

Ein vermeintlicher Zugriff auf Facebook-Nutzerdaten bei einem Dienstleister konnte durch eine Vor-Ort-Kontrolle von uns bewertet werden.

Die DS-GVO hat als Ziel, ein einheitliches Datenschutzniveau in Europa zu etablieren. Dazu gehört auch, dass die Datenschutzaufsichtsbehörden in Europa zusammenarbeiten, gemeinsame Positionen abstimmen und Datenschutzbeschwerden nachgehen. Die komplizierten Regelungen dieses sogenannten Kohärenzverfahrens betreffen die Verantwortlichen nicht (direkt). Stattdessen müssen die Aufsichtsbehörden eigene, effiziente Prozesse schaffen, wie beispielsweise mit Datenschutzbeschwerden umgegangen wird (siehe Kapitel 3 dieses Berichts).

So erreichte uns über das IMI-Verfahren (Binnenmarkt-Informationssystem) eine Datenschutzbeschwerde aus Spanien. Es stand der Verdacht im Raum, dass ein Unternehmen in Bayern gehackt worden sei. Dabei könnten millionenfache Nutzerdaten von Facebook, die dieses Unternehmen als Facebook-App-Entwickler abgerufen habe, abhandengekommen sein.

Bei der Beschreibung des Sachverhalts schien es Parallelen zum Cambridge-Analytica-Skandal im Frühjahr 2018 zu geben, bei dem eine unbefugte Nutzung von Facebook-Daten zu Wahlkampfzwecken stattfand. Wir haben deshalb bei dem Unternehmen eine Vor-Ort-Kontrolle durchgeführt. Wie üblich wurde – mit einer sehr kurzen Frist – das Verzeichnis der Verarbeitungstätigkeiten zur Vorbereitung angefordert, damit zumindest die grundlegenden Datenverarbeitungen und Geschäftsfelder bewertet werden konnten.

Im Rahmen der Vor-Ort-Kontrolle konnte der Sachverhalt dann aufgearbeitet werden. Dieser stellte sich in zweierlei Hinsicht dann anders als befürchtet dar:

- Es gab eine nicht-triviale Schwachstelle in der Anbindung der Facebook-Profile (hauptsächlich Fotos und Kontakte), die von Facebook mit der Bitte um sofortige Behebung dem Unternehmen mitgeteilt wurde.
- Es gab dabei keine Anzeichen, dass diese Schwachstelle bekannt geschweige denn ausgenutzt werden konnte.
- Ein massenhafter Angriff auf Facebook-Daten wäre mit dieser Schwachstelle nicht möglich gewesen. Ein vereinzeltes Abgreifen von Fotos und Kontaktlisten durch manuelle Aktionen von Facebook-Nutzern (vergleichbar mit dem Klicken auf einen Link) wäre theoretisch möglich gewesen, konnte jedoch nicht festgestellt werden.

Das Unternehmen bereitete sich im Vorfeld gut auf die DS-GVO vor und konnte uns daher auch bei der Vor-Ort-Kontrolle eine Risikobeurteilung nach Art. 33 DS-GVO vorlegen. Diese ging von „keinem Risiko" für die Rechte und Freiheiten der Nutzer aus, da die Schwachstelle zwar vorhanden aber aller Wahrscheinlichkeit nicht ausgenutzt wurde. Diese Sichtweise haben wir bestätigt und den Vorgang damit abgeschlossen.

Auch wenn es im Ergebnis kein datenschutzrechtlich kritischer Vorfall war, so hat sich gezeigt, wie wichtig es ist, dass die Datenschutzaufsichtsbehörden in Europa gut zusammenarbeiten und (potentielle) Datenschutzverstöße oder gar Datenskandale gemeinsam bearbeiten.

23.7 HTTPS-Verschlüsselung

Viele Verantwortliche haben immer noch Probleme damit, eine wirksame Transportverschlüsselung auf ihrer Website einzusetzen.

Das Thema HTTPS-Verschlüsselung haben wir schon in den vorangegangen Tätigkeitsberichten dargestellt. Unter der DS-GVO hat sich diesbezüglich nichts geändert, da zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 DS-GVO) auch Verschlüsselungsverfahren nach Stand der Technik einzusetzen sind. Im Berichtszeitraum wurden bei uns zahlreiche Datenschutzbeschwerden wegen keiner oder nicht ausreichender HTTPS-Verschlüsselung eingereicht.

Erstaunlich ist, dass manche Unternehmen immer noch Probleme mit dem Betrieb einer HTTPS-Konfiguration nach Stand der Technik haben. Wir informierten die verantwortlichen Websitebetreiber daher über die Anforderungen für HTTPS:

- Kein Einsatz veralteter Verschlüsselungsprotokolle (SSL2, SSL3, TLS1.0)
- TLS 1.2 als Standardprotokoll

- Vorrangige Verwendung von Perfect Forward Secrecy (PFS)
- Geeignete Schlüssellänge des SSL-Zertifikats
- Keine SSL-Zertifikate mit SHA-1
- Keine unsicheren Kryptoalgorithmen (z. B. RC4, Export-Chiffren)
- Verwendung aktueller Softwareversionen (z. B. Webserver, Firewall)
- Empfohlene Verwendung von HTTP Strict Transport Security (HSTS)
- Geeignete SSL-Zertifikate (nicht selbst signiert, passend zur Domäne)
- Einsatz von HTTP Public Key Pinning (empfohlen)

Da eine wirksame HTTPS-Verschlüsselung weder unverhältnismäßig aufwendig noch eine unter der DS-GVO neue Anforderung ist, beabsichtigen wir, bei nachgewiesenen Verstößen Bußgeldverfahren einzuleiten. Nicht nur deswegen sollte es sich für Verantwortliche lohnen, mit wenig Konfigurationsaufwand die Basisanforderungen für ihre Website umzusetzen.

23.8 Browser Fingerprinting

Die eindeutige Kennung eines Browser wird von manchen Websites zum Tracking des Nutzers verwendet.

Die Fragestellung, wie Webtracking unter der DS-GVO datenschutzkonform durchgeführt werden kann, ist aufgrund der (noch) nicht verabschiedeten ePrivacy-Verordnung ein aktuelles Diskussionsfeld. Aus technischer Sicht werden bei den meisten Trackingverfahren weiterhin Cookies verwendet, seien es die First-Party-Cookies der aufgerufenen Website oder Third-Party-Cookies von Drittanbietern. Cookies, insbesondere die in der Regel verwendeten HTTP-Cookies, haben den Vorteil für den Nutzer, dass sie im Browser gelöscht (z. B. bei Beenden des Browsers) oder blockiert (anwendbar bei Third-Party-Cookies) werden können. Neue Browser-Generationen beinhalten auch zunehmend Anti-Tracking-Funktionalitäten, die einer möglichst allumfassenden Nutzungsprofilbildung entgegenstehen.

Eine technische Möglichkeit auf Cookies zu verzichten und dennoch einen Browser eindeutig – sogar über Websites hinweg – zu identifizieren, ist das sogenannte Browser-Fingerprinting. Darunter versteht man die Berechnung eines möglichst eindeutigen Hash-Wert eines Browsers, bei dem neben den bekannten Basiswerten wie Betriebssystem und Softwarestand auch Merkmale wie auf dem PC installierte Schriftarten oder das Renderverhalten der Grafikkarte einbezogen werden. Anhand dieses Browser-Fingerabdrucks kann das Surfverhalten ohne wirksame Gegenmaßnahmen eines Nutzers aufgezeichnet und für die Profilbildung verwendet werden.

Wir sind der Auffassung, dass ein Einsatz von Browser-Fingerprinting-Technologien nur mit Einwilligung der Nutzer zulässig ist. Auf eine Interessenabwägung nach Art. 6 Abs. 1 Buchstabe f DS-GVO können sich die Verwender dieser Technologie nicht stützen, da die schutzwürdigen Interessen der Nutzer hier eindeutig überwiegen.

Wir führten im Berichtszeitraum eine Kooperation mit dem Lehrstuhl für IT-Sicherheitsinfrastrukturen der Friedrich-Alexander-Universität Erlangen-Nürnberg durch, die derzeit weiter fortgesetzt wird. Im Rahmen dieser Forschungskooperation wurde evaluiert, inwiefern durch automatische Prüfverfahren der Einsatz von Browser-Fingerprinting-Methoden auf Websites festgestellt werden kann. Mit den bislang gewonnenen Erkenntnissen beabsichtigen wir, einen ersten Feldtest bei Verantwortlichen in Bayern durchzuführen. Sollte dabei festgestellt werden, dass Browser-Fingerprinting-Technologien ohne Einwilligung der Nutzer eingesetzt

werden, ist neben den aufsichtlichen Maßnahmen auch die unmittelbare Einleitung von Bußgeldverfahren geplant.

23.9 E-Mail-Verschlüsselung

Es stellt sich die Frage, welche kryptographische Verfahren bei E-Mails im Alltag verpflichtend sind.

Die Sicherstellung des Schutzes personenbezogener Daten gegen unbefugte Verarbeitungen ist eine wichtige Anforderung aus der DS-GVO. Unter Berücksichtigung des Risikos für die Rechte und Freiheiten natürlicher Personen sind geeignete Schutzmaßnahmen von Verantwortlichen zu treffen. Kryptographische Verfahren können hierbei einen entscheidenden Anteil leisten, so auch bei der E-Mail-Kommunikation.

Ob und wie E-Mails sicher, d. h. verschlüsselt, übertragen werden müssen, war immer wieder Gegenstand von Anfragen und Beschwerden, die uns erreichten. Dass Verschlüsselung von E-Mails immer noch ein Datenschutzthema ist, liegt nicht an der DS-GVO, sondern daran, dass das E-Mail Protokoll SMTP (Simple Mail Transfer Protokoll) nicht nur „steinalt", sondern auch völlig ungeeignet ist, um die Vertraulichkeit, Integrität und Authentizität von E-Mails sicherzustellen. Die kryptographischen Schutzmaßnahmen für E-Mails, die heute existieren, sind zwar wirksam, die flächendeckende Umsetzung in der Praxis scheitert aber an der Infrastruktur für Verschlüsselungsschlüssel und der uneinheitlichen Konfiguration der E-Mail-Infrastruktur bei den Verantwortlichen.

Wie schon unter dem BDSG-alt, sehen wir auch unter der DS-GVO folgende Mindestanforderungen für Unternehmen:

- Der Transport der E-Mails, d. h. die Kommunikation zwischen den E-Mail-Servern, muss nach Stand der Technik (z. B. TLS1.2, PFS, mind. 2048 Bitlänge Zertifikat) immer verschlüsselt werden.
- Eine Inhaltsverschlüsselung (z. B. PGP, S/MIME, verschlüsselte PDF) muss zusätzlich umgesetzt werden, wenn der Bruch der Vertraulichkeit, Integrität und Authentizität ein hohes Risiko zur Folge hätte.

Das Problem bei der Transportverschlüsselung ist, dass dabei alle beteiligten Akteure „mitspielen" müssen. Unterstützt z. B. ein empfangender E-Mail-Server keine Verschlüsselung, müsste entweder der E-Mail-Transport abgebrochen werden (sog. Mandatory-Verschlüsselung) oder eine Zustellung gänzlich unverschlüsselt erfolgen (sog. opportunistische Verschlüsselung). Eine opportunistische Verschlüsselung ist zwar sehr robust gegen passive Angriffe, z. B. durch Abhören eines Netzwerkknotens – sobald ein aktiver Angreifer aber in der „Leitung hängt", kann diese Verschlüsselung ohne Aufwand deaktiviert werden.

Aus diesem Grund sehen wir die Anforderungen an die E-Mail-Kommunikation für bayerische Verantwortliche derart, dass

- immer eine opportunistische Transportverschlüsselung nach Stand der Technik einzusetzen ist,
- bei hohem Risiko zusätzlich eine Inhaltsverschlüsselung verwendet werden muss und
- bei Unternehmen mit erhöhtem Risiko und einer begrenzt bekannten Anzahl von Kommunikationspartnern (z. B. Dienstleister, Konzerntöchter, Geschäftspartner,...) eine verpflichtende Transportverschlüsselung einzusetzen ist, es sei denn, diese ist nachweislich unverhältnismäßig.

In der Kommunikation von Verantwortlichen mit Kunden, Mandanten, Patienten (betroffene Person) gelten an sich die gleichen Anforderungen. Eine Absenkung des Schutzniveaus sehen wir innerhalb sehr enger Grenzen nur dann als möglich an, wenn die betroffene Person damit einen Nutzen verbindet – „Komfort" würden wir

selbstverständlich auch dazu zählen. Allerdings muss dann die Zustimmung für diese Form der E-Mail-Kommunikation eingeholt, die Risiken transparent beschrieben und eine sichere Alternative ohne Medienbruch angeboten werden. Dies wäre beispielsweise dann der Fall, wenn ein Arzt oder eine Versicherung eine sichere Alternative mittels PGP oder einem Online-Portal bieten, ein Patient oder Kunde aber für sich entscheidet, nur mittels „normaler" E-Mail (d. h. opportunistisch transportverschlüsselt) kommunizieren zu wollen. Eine Absenkung unter einer Transportverschlüsselung sehen wir nicht als möglich an, da die Risiken massiv zunehmen würden und eine transparente Zustimmung für die meisten Betroffenen in Anbetracht der Komplexität des weltweiten Internetverkehrs samt Bedrohungsszenarien kaum einzuholen wäre. Eine sichere Alternative zur E-Mail könnte auch der Einsatz eines datenschutzkonformen Messengers oder ein mit Blick auf Sicherheit entwickeltes Online-Portal mit Zwei-Faktor-Authentifizierung sein.

Auch hier zeigt sich die gute Skalierungsmöglichkeit des risikoorientierten Ansatzes mit besonderer Berücksichtigung auf kleine und mittelständische Unternehmen. Gerade die eher „kleineren" Verantwortliche mit „normalen" Daten wie etwa Sportvereine und Handwerksbetriebe, die meist E-Mail-Hosting bei einem Dienstleister nutzen und keinen eigenen Mailserver betreiben, fallen nicht in die Hochrisikokategorie. Damit benötigen sie keine zusätzliche Inhaltsverschlüsselung und können ohne Bedenken ihre Kommunikation per E-Mail abwickeln.

Große Unternehmen (z. B. Versicherungskonzerne) müssen dagegen die E-Mail-Infrastruktur ggf. dezidiert am Datenschutzrisiko ausrichten und z. B. in Kombination mit Online-Portalen die digitale Kommunikation ganzheitlich betrachten, um einen datenschutzkonformen Einsatz sicherstellen und im Sinne der DS-GVO nachweisen zu können.

23.10 Löschen unter der DS-GVO

Mit der DS-GVO endet die Zeit des unter dem BDSG-alt bekannten Sperrens von Daten – Löschkonzepte werden dagegen wichtiges Datenschutzelement.

Der Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 Buchstabe e DS-GVO) legt fest, dass personenbezogene Daten, sofern sie nicht mehr für den Zweck, für den sie erhoben wurden, erforderlich sind und gesetzliche Aufbewahrungsfristen nicht mehr greifen, zu löschen sind. Eine Alternative zum Löschen wäre die Anonymisierung der Daten. Diese wird jedoch zumindest unter den Aufsichtsbehörden intensiv diskutiert, da sie als Verarbeitung im Sinne des Art. 4 Nr. 2 DS-GVO auch eine Rechtsgrundlage benötigen könnte und naturgemäß mit einem deutlichen Informationsverlust einhergehen muss – was die Nutzbarkeit der anonymen Daten in vielen Fällen infrage stellt.

Dass personenbezogene Daten gemäß DS-GVO irgendwann gelöscht werden müssen, ist nichts Neues. Bereits unter BDSG-alt gab es diese Anforderung schon, allerdings auch die Möglichkeit des Sperrens, sofern das Löschen mit einem unverhältnismäßigen Aufwand verbunden war. Aufwände, die bei einer Entwicklung einer softwarebasierten Verarbeitung zu spät eingeplant werden, können leicht und schnell sehr groß werden. Beim Thema „Löschen personenbezogener Daten" scheint dies fast branchenunabhängig so gewesen zu sein, da zu hohe Kosten ein häufiges Argument beim Thema Löschen waren und Daten daher gesperrt anstatt gelöscht wurden.
Unter der DS-GVO ist dies nun anders: Sperren anstelle von Löschen ist nicht mehr möglich – unabhängig vom dazugehörigen Aufwand.

Als risikominimierende, technische Maßnahme (d. h. nicht als Alternative zum Löschen), um Daten z. B. aus einer grafischen Oberfläche auszublenden, ist eine Form des Sperrens durchaus noch möglich.

Ab einer gewissen Unternehmensgröße sind Löschkonzepte für einen nachweisbaren Umgang mit diesem Thema Pflicht. Empfehlenswert ist es, einen Blick in die DIN 66399 zu werfen. Dort werden entsprechende Hilfestellungen bzw. Vorgaben gegeben. Bei unseren Datenschutzkontrollen werden wir das Thema Löschen weiter im Blick haben und den Umsetzungsstand in der Praxis überprüfen.

24

Bußgeldverfahren

24 Bußgeldverfahren

Im Berichtszeitraum 2017/2018 haben wir insgesamt 216 Bußgeldverfahren bearbeitet. Davon wurde in dieser Zeit im Vergleich zu den Vorjahren nur in einer verhältnismäßig geringen Anzahl an Fällen, nämlich 10, auch tatsächlich ein Bußgeldbescheid erlassen. Dies ist zum einen darauf zurückzuführen, dass die Vorbereitung auf die DS-GVO und die damit einhergehenden neuen Aufgaben für uns mit dem zur Verfügung stehenden Personal keine Schwerpunktsetzung im Bereich der Ordnungswidrigkeiten erlaubte. Zum anderen erreichten uns viele Ordnungswidrigkeitenanzeigen von der Polizei, die wir auf Grund der Geringfügigkeit des Verstoßes oder mangels Nachweisbarkeit einstellten bzw. nicht einleiteten und in einem aufsichtlichen Verfahren bearbeiteten. Dies trifft insbesondere auf den Bereich der Videoüberwachung – und hier vor allem den nachbarschaftlichen Bereich – zu.

Einige Bußgeldbescheide wurden jedoch auch in diesem Berichtszeitraum wegen unzulässigen Bertreibens von Dashcams erlassen. Allerdings ging auch in diesem Bereich die Anzahl der Bescheide im Berichtszeitraum zurück, da uns die Erfahrung der letzten Jahre gelehrt hat, dass die gerichtlichen Verfahren immer dann zu einer Einstellung führten, wenn auf den als Beweismittel vorgelegten Videoaufzeichnungen nicht hinreichend viele Kfz-Kennzeichen eindeutig zu erkennen waren. Dies erforderte eine oft recht mühsame Auswertung des uns übermittelten Beweismaterials mit dem Ergebnis, dass die Verfahren meist wegen mangelnder Erkennbarkeit der Kennzeichen eingestellt wurden.

In zwei Fällen wurden unsere Bescheide wegen unbefugter Erhebung und Verarbeitung personenbezogener Daten, die nicht allgemein zugänglich sind (§ 43 Abs. 2 Nr. 1 BDSG-alt), durch das permanente und anlasslose Betreiben einer Dashcam nach Einlegung eines Einspruchs im gerichtlichen Verfahren bestätigt.

Erwähnenswert erscheint ein Fall, in dem wir ein Bußgeld wegen unbefugten Bereithaltens zum Abruf gemäß § 43 Abs. 2 Nr. 2 BDSG-alt verhängt haben. Der Betroffene nutzte die auf einen Mitarbeiter ausgestellte ärztliche Arbeitsunfähigkeitsbescheinigung als sein Profilbild bei WhatsApp, sodass sie für jeden, der mit ihm über WhatsApp Kontakt hatte, sichtbar war.

Eine große Anzahl der von uns im Berichtszeitraum bearbeiteten Bußgeldverfahren wurden uns durch die Staatsanwaltschaften nach Abschluss des dortigen Verfahrens gemäß § 43 OWiG zur Prüfung der Ordnungswidrigkeiten in eigener Zuständigkeit übermittelt.

Gleichzeitig erreichten uns im Berichtszeitraum sieben Vorgänge, die wir entweder wegen des Verdachtes des Vorliegens einer Straftat nach StGB oder Sonderstrafrecht gem. § 41 OWiG und/oder wegen des Vorliegens einer datenschutzrechtlichen Straftat mitsamt Strafantrag gemäß § 44 Abs. 2 BDSG-alt oder § 42 Abs. 3 BDSG an die zuständige Staatsanwaltschaft übermittelt haben. Hierbei handelte es sich beispielsweise um Fälle von unzulässigen Datenverkäufen einer großen Anzahl von Betroffenen oder den Verdacht von Straftaten wegen Verletzung der Vertraulichkeit des Wortes (§ 201 StGB).

Insgesamt bemerken wir im Bereich der Ordnungswidrigkeiten, dass das Thema „Datenschutz“ sowohl bei den Strafverfolgungsbehörden als auch der breiten Öffentlichkeit mehr in den Fokus gerückt ist.

Bußgelder nach der DS-GVO haben wir im Berichtszeitraum noch nicht verhängt, wenngleich bereits einige Verfahren nach DS-GVO abgeschlossen wurden. Vorrangig war und ist es für unsere zentrale Bußgeldstelle, zunächst die noch nicht abgeschlossenen Altfälle zu bearbeiten.

Weitere Hinweise zu den Sanktionen nach der DS-GVO finden Sie im Kurzpapier der DSK unter folgendem Link:

www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_2.pdf

Stichwortverzeichnis

A

Abrechnungsdaten 105
Adresshandel 72
Arztpraxen 34, 91
Auftragskette 84
Auftragsverarbeitung 40, 63, 67, 80
Auskunft 46
Auskunfteien 70
Auskunftsrecht bei Ärzten 46
Ausweiskopien 67
AVV-Formulierungshilfe 40

B

Backup 34
Banken 66
Beratungen BayLDA 16
Berichtigung 47
Berufsgeheimnisträger 63
Beschäftigtendatenschutz 88
Beschwerden BayLDA 14
Betroffenenrechte 43
Bewerbungsverfahren 32, 88
Bewertungsportale 52
Binding Corporate Rules 85
Browser Fingerprinting 136
Bußgeldverfahren 141

C

Callcenter 45
Cookie-Banner 55
Cyberkriminelle 119
Cybersicherheit 119, 131

D

DAkkS 128
Dashcams 110
Datenchutzerklärung 53
Datendiebstahl 120
Datenschutzbeauftragter 37
Datenschutzbestimmungen 53
Datenschutz-Folgenabschätzung 133
Datenschutzverletzungen 18, 118
Datenübertragbarkeit 49
Diebstahl 118
Dienstleister 41
Diskretion 91
DS-GVO-Prüfung 33

E

EDSA 24
Ehrenamt 102
Eigentümergemeinschaften 105
Einwilligung 56, 94, 95, 101
Elternbeirat 97
E-Mail-Kommunikation 94
E-Mail-Verschlüsselung 137
Emotet 125
Energieversorger 77, 78
Entwicklungshilfeverein 102
Erpressung 120
Europäische Zusammenarbeit 19, 23

F

Facebook Custom Audience 58
Facebook-Fanpages 60
Fahrzeugdaten 115
Federführende Aufsichtsbehörde 23
Fehlversendungen 118
Fernidentifikation 67
Feuerwehrvereine 100
Fotos 56, 88, 96, 101

G

Gastronomie 27, 112
Gesellschafterrechte 76
Gesprächsaufzeichnung 45
Gesundheit 91

H

Hacking 122, 124
Handel 75
Hash-Verfahren 59, 60
Heilpraktiker 94
Hotelbuchungssoftware 119
HTTPS 135

I

IMI-System 23

Informationspflichten 32, 43, 99
Informationspflichten am Telefon 44
Informationspflichten bei Ärzten 45
Internationaler Datenverkehr 84
Internet 52
IP-Adressen 54

K

Karten-Zahlungen 43
Kfz-Halter 115
Kfz-Werkstätten 28
Kindergartenfotos 96
Kindernamen 97
Kino 27
Kohärenz 23
Kontaktformulare 55
Kontrollen 27
Kopien 46
Koppelungsverbot 72
KRITIS 121
Kryptomining 120

L

Login 123
Löschfristen 70
Löschung 48, 138

M

Magento 31
Malware 118
Medienbruch 43
Medizinisches Labor 50
Mietbewerber 108
Mieterdatenschutz 105
Mitarbeiterfotos 88

N

Nachlasspfleger 78

O

Öffentlichkeitsarbeit 21
Offline-Tracking 60
Online-Shops 123
Optiker 95
Ordnungswidrigkeiten 141
Organigramm 11

P

Patch Management 29, 31
Patienten 45, 48, 91
Personalausweiskopien 75
Phishing 118, 121
Planstellen BayLDA 20
Plugin 31
Prüfungen 27
Publikumsgesellschaften 76

R

Ransomware 34, 123
Rechenschaftspflicht 33, 134
Rechtsanwälte 63
Reisebüros 79
Reiserücktrittsversicherung 79
Rezeptabholung 93
Risiko 118, 130

S

Sanitätshäuser 95
Schweigepflicht 93
Schwimmbäder 111
Seniorenheim 95
Shop-System 121
Sicherheitslücke 119
Softwarefehler 118
Soziales 91
Sprechzimmer 91
Standardvertrag 84
Statistik BayLDA 14
Steuerberater 63
Subgroups 24

T

Technikgestaltung 132
Telefonverzeichnis 95
Traueranzeigen 44
Türschilder 95

U

Überwachungsaufgaben des DSB 38
Unterauftragsverarbeiter 84

V

Verbände 99
Vereine 99

Verfahren der Zusammenarbeit 23
Verlust 118
Verschlüsselungstrojaner 34, 118
Versicherungsgruppe 66
Versicherungswirtschaft 66
Videoidentifizierung 67
Videointerviews 89
Videoüberwachung 27, 110
Vorträge 21

W

Webserver 120
Websites 29, 31, 52
Werbung 72
Werturteil 47
WhatsApp 58
Widerspruchsmöglichkeit 108
Wohnungswirtschaft 105
WordPress 29, 31

Z

Zahlen und Fakten BayLDA 14
Zertifizierung 128

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