Bayerisches Landesamt für
Datenschutzaufsicht

10. Tätigkeitsbericht

2020

10. Tätigkeitsbericht des Bayerischen Landesamts für Datenschutzaufsicht für das Jahr 2020

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 Juli 2021 – Michael Will, Präsident

Bildnachweis Cover: de.123rf.com – Urheber everythingpossible – Dateinummer 45551643

Vorwort

Mit seinem 10. Tätigkeitsbericht legt das Landesamt für Datenschutzaufsicht einen Bericht über ein Jahr grundlegender Veränderungen vor. Der Jubiläumsbericht verweist auf den am 1. August 2021 zu begehenden 10. Jahrestag des Bestands unserer Behörde als verselbstständigte und weisungsfreie, im Sinne des Unionsrechts völlig unabhängige Datenschutzaufsichtsbehörde.

Er ist damit zugleich der erste Bericht, der nicht vom Gründungspräsidenten des BayLDA Thomas Kranig verantwortet wird, der am 31. Januar 2020 in den Ruhestand getreten ist. Sein verdienstreiches Wirken und seine fachliche, organisatorische genauso wie seine menschliche Aufbauarbeit sind auch heute weiterhin für uns alle voll dankbarer Anerkennung nahezu tagtäglich spür- und sichtbar.

Das BayLDA im pandemischen Ausnahmezustand

Auch Dank dieser von Thomas Kranig in langen Jahren gefestigten Fundamente konnte das BayLDA den mit dem Ausbruch der Pandemie im Frühjahr 2020 einsetzenden Prozess nachhaltiger Veränderungen unbeschadet und trotz aller Herausforderungen ohne substantielle Einschränkung seiner Aufgabenwahrnehmung vollziehen.

Nicht anders als bei der Mehrzahl der Behörden und Unternehmen unsers Landes war das Jahr 2020 seit dem ersten Quartal auch für das BayLDA das Jahr des Home-Office. Virtuelle Formate unterschiedlicher Dimension von der Teambesprechung oder dem Konferenzvortrag bis hin zur großen , interaktiven Weihnachtsfeier mit dem gesamten BayLDA-Team haben damit unsere persönlichen internen Treffen genauso nahezu vollständig verdrängt wie die Vielzahl unserer sonstigen Auswärtstermine für nationale und europäischen Abstimmungsgespräche oder Arbeitskreise der Datenschutz-Verbände. Ohne den besonderen Einsatz jeder und jedes Einzelnen sowie die außerordentliche Flexibilität und Agilität gerade unseres technischen Stabes wäre dieser Erfolg kaum vorstellbar gewesen. Er verdient deshalb an dieser Stelle nochmals ganz besonderen Dank und Wertschätzung. Nichts anderes gilt im Übrigen für unsere dem BayLDA durch eine Kooperationsvereinbarung verbundene Nachbarbehörde, die Regierung von Mittelfranken, deren Mitarbeiterinnen und Mitarbeiter trotz der außerordentlichen Zusatzbelastung der bayerischen Mittelbehörden in Pandemie und Katastrophenfall das BayLDA durchgängig mit ihren zentralen Diensten und in der Personalverwaltung unterstützt haben. Umgekehrt hat das BayLDA durch eine Freistellung für ein virtuelles Tracing-Team und eine über mehrere Wochen im Frühjahr ermöglichte Abordnung aus unserem Leitungsbereich versucht, seinen solidarischen Beitrag zur Bewältigung der pandemischen Spitzenbelastung der gesamten bayerischen Staatsverwaltung zu erbringen.

Trotz aller Anpassungserfordernisse und meist vorübergehender Beschwernisse wird im Rückblick aber auch ein Vorzug der veränderten Arbeitsbedingungen deutlich: Auf Grund des Wechsels in virtuelle Formate und der damit verbundenen Reisezeitersparnisse konnte das BayLDA mehr als in allen vorangehenden Jahren seine Aufgaben im Bereich der europäischen Zusammenarbeit genauso wie den damit verbundenen nationalen Abstimmungsaufgaben nachkommen. Die Vielzahl an möglichst einheitlich anzugehenden datenschutzrechtlichen Fragen der Pandemiebekämpfung und die seit dem 2. Halbjahr 2020 mindestens gleichermaßen drängenden Fragen des Internationalen Datenverkehrs haben im Europäischen Datenschutzausschuss auf allen Ebenen zu einer außerordentlichen Verdichtung der Sitzungen und Abstimmungsprozesse geführt.

Die Erwartung, dass dieses neue Niveau der Intensität und Bandbreite der Zusammenarbeit im Jahr vier der DS-GVO nochmals abebbt, erscheint angesichts der allmählich greifenden Mechanismen der Zusammenarbeit auch in Einzelfallfragen weder realistisch noch wünschenswert, ohne das Ziel der einheitlichen Anwendung des europäischen Datenschutzrechts in Frage zu stellen.

Freilich bleibt dann anzuerkennen, dass im Rahmen der traditionellen Präsenzformate kurzfristige Sitzungsterminierungen und Folgeberatungen im Wochentakt für nationale Gremienvertreter kaum zu bewältigen sein werden. Dies gilt erst Recht für Behörden wie das BayLDA, denen jede neue Inanspruchnahme durch Aufgaben der EU-Zusammenarbeit auf Grund nach wie vor allzu knappen Ressourcen stets Kompromisse zu Lasten der übrigen Aufgaben im Bereich der Beschwerdebearbeitung und Beratung abverlangt.

Themenschwerpunkt Internationaler Datenverkehr

Neben der Pandemiebekämpfung hat das Urteil des Europäischen Gerichtshofs (EuGH) vom 16. Juli 2020 in der Rechtssache „Schrems II" unsere Aufgabenschwerpunkte, teils aber auch die Wahrnehmung des Datenschutzes im Jahr 2020 insgesamt bestimmt und bei manchen verändert. Während im Hinblick auf die Pandemiebekämpfung der Datenschutz in vielen Diskussionen immer wieder vorschnell und unberechtigt als Bremser und Hindernis missverstanden wird, erscheint das Urteil des EuGH mit seinen Maßstäben für Datenübermittlungen in Drittstaaten in vielen Analysen und Rückmeldungen aus der Praxis als kaum bewältigbare und letztlich unverständliche bürokratische Belastung. Vergleichbar der Wahrnehmung der DS-GVO in ihrer Startphase im Jahr 2018 spiegeln diese Rückmeldungen für uns in vielen Fällen Unsicherheiten in der Anwendung des geltenden Rechts wieder: ähnlich wie der Kern des materiellen Datenschutzrechts durch die DS-GVO gegenüber dem früheren Recht nicht verändert wurde, hat weder die Pandemie z. B. die Befugnisse von Arbeitgebern beim Umgang mit Gesundheitsdaten von Beschäftigten grundlegend erweitert oder gar relativiert. Ebenso wenig hat der EuGH aus den Anforderungen des Kapitels V der DS-GVO und den bisherigen sog. Standardvertragsklauseln der EU-Kommission substantiell neues entnommen, sondern zunächst nur an bereits bisher explizit ausgestaltete allgemeine Sorgfalts- und Prüfpflichten von Datenexporteuren und -importeuren erinnert.

Allerdings hat der EuGH zugleich mit der Adäquanzentscheidung zum EU-US-Privacy-Shield gerade für die Unternehmen in Bayern mit ihren vielfältigen transatlantischen Verflechtungen ein zentrales Instrument zu praxisgerechten Absicherungen von Datenübermittlungen aufgehoben, dessen Wegfall gerade für kleine und mittlere Unternehmen komplexe Anpassungsaufgaben auslöst. Gemeinsam mit den Verbänden der bayerischen Wirtschaft hat das BayLDA deshalb frühzeitig in mehreren Informationsveranstaltungen für die damit verbundenen Fragestellungen sensibilisiert und Hilfestellungen bereit gestellt, die auch im Jahr 2021 fortgeführt werden.

Ausblick

Im 11. Jahr als eigenständige Datenschutzaufsichtsbehörde und fast zwanzig Jahre nach seiner Gründung zum 1. Januar 2002 als Sonderbehörde unter dem Dach der Regierung von Mittelfranken sieht sich das BayLDA erneut in einer Phase grundlegender Weichenstellungen:

Mit Sorge sehen wir, dass spätestens seit Prüfaufträgen der Datenethikkommission in ihrem Bericht vom Oktober 2019 in der Bundespolitik immer wieder Überlegungen zu einer Zentralisierung der Datenschutzaufsicht im nicht öffentlichen Bereich ausgetauscht werden. Trotz aller Ungenauigkeiten und Defizite in ihren Analysen zum status quo der Datenschutzaufsicht in Deutschland wie auch in der zentralen Frage der

verfassungsrechtlichen Umsetzbarkeit einer in der Fläche präsenten Bundesbehörde für die Datenschutzkontrolle bei Unternehmen – im Kern zeigen uns diese Debatten immer wieder tiefgreifende Vorbehalte gegenüber föderalen Strukturen und ihrer Leistungsfähigkeit bei der Bewältigung gesamtwirtschaftlicher und -gesellschaftlicher Herausforderungen wie der Digitalisierung und globalen Vernetzung. Sie sind uns daher gleichermaßen Mahnung wie Ansporn. Im Mittelpunkt unserer Arbeit steht schon durch die DS-GVO vorgegeben, die programmatisch einfache, in der Praxis aber oft genug herausfordernde Aufgabe der unionsweit einheitlichen Anwendung des europäischen Datenschutzrechts. Unser Ziel bleibt dabei, durch Verständlichkeit, Nachvollziehbarkeit und Rechtssicherheit für Bürgerinnen und Bürger genauso wie für die unserer Aufsicht unterliegenden Unternehmen und Vereine einen Mehrwert für den Schutz personenbezogener Daten zu erreichen.

Diesen Zielen werden die heute bestehenden Strukturen unserer Behörde angesichts stetig ansteigender Fallzahlen und veränderter Funktionsbedingungen der Datenschutzaufsicht in einem europäischen Vollzugsverbund wie die nachfolgenden Kapitel zu unserer Überzeugung zeigen, dank einer Vielzahl tagtäglicher Priorisierungskompromisse noch, aber nicht mehr lange ohne nachhaltige Änderungen gerecht.

Soweit dieser Veränderungsprozess z. B. im Hinblick auf unsere interne Aufgabenverteilung im Rahmen unserer Gestaltungsmöglichkeiten liegt, können wir erste Schritte bereits im Nachfolgenden aufzeigen, die zentralen Weichenstellungen zur Sicherstellung einer zukunftsfähigen Datenschutzaufsicht obliegen aber letztlich alleine dem bayerischen Haushaltsgesetzgeber.

Ansbach, im Juli 2021

Michael Will
Präsident

Inhaltsverzeichnis

Vorwort **1**

Inhaltsverzeichnis **4**

1 Datenschutzaufsicht im nicht-öffentlichen Bereich **8**

1.1 Gesetzliche Grundlage für den Tätigkeitsbericht 8

1.2 Datenschutz in Bayern 8

1.3 Das Bayerische Landesamt für Datenschutzaufsicht 8

2 Zahlen und Fakten **11**

2.1 Beschwerden 11

2.2 Beratungen 14

2.3 Datenschutzverletzungen 15

2.4 Abhilfemaßnahmen; Europäische Zusammenarbeit 15

2.5 Förmliche Begleitung von Rechtsetzungsvorhaben 16

2.6 Ressourcen 16

2.7 Vorträge und Öffentlichkeitsarbeit 17

3 Corona **19**

3.1 Kontaktdatenerfassung zur Pandemiebekämpfung 19

3.2 Zutrittskontrollen durch Fiebermessen, Wärmebildkameras oder Vorzeigenlassen der Corona-Warn-App 20

3.3 Videokonferenzsysteme im Home-Office 21

4 Auftragsverarbeitung **24**

4.1 Auftragsverarbeitung, getrennte Verantwortlichkeit oder doch gemeinsame Verantwortlichkeit? 24

5 Datenschutz im Internet **26**

5.1 Zulässigkeit von Immobilienbewertungsportalen 26

5.2 Google Analytics 26

5.3 Cookies – nur noch mit Einwilligung? § 15 Abs. 3 TMG in richtlinienkonformer Auslegung als Rechtsgrundlage für Webtracking 27

5.4 Apple Kamerafahrten 28

6 Steuerberater und Rechtsanwälte **31**

6.1 Klarstellende Regelungen zur datenschutzrechtlichen Verantwortlichkeit und den Verarbeitungsbefugnissen von Steuerberatern im Steuerberatungsgesetz (StBerG) 31

6.2 Datenerhebungsbefugnisse von Insolvenzverwaltern 31

6.3 Datenschutzrechtliche Verantwortlichkeit und Verarbeitungsbefugnisse gerichtlich bestellter Sachverständiger 32

7 Versicherungswirtschaft und Banken 35
7.1 Hinweis- und Informationssystem (HIS) der deutschen Versicherungswirtschaft 35
7.2 Kontoauszüge im Rahmen des Auskunftsanspruchs 36
7.3 Gutachten zur Beleihungswertermittlung im Rahmen des Auskunftsanspruchs 37
7.4 Positivdaten bei Energieversorgungsverträgen 37
8 Werbung und Adresshandel 40
8.1 Koppelungsverbot bei Newsletter-Anmeldungen 40
9 Handel und Dienstleistung 42
9.1 Nutzung personenbezogener Daten für das Anbieten von „Hilfe in einer Notlage" 42
10 Internationaler Datenverkehr 44
10.1 Binding Corporate Rules – ein Wachstumsmarkt 44
10.2 Neue Standarddatenschutzklauseln für Übermittlungen in Drittländer veröffentlicht 45
10.3 Das Schrems-II-Urteil: Datenübermittlungen in Drittländer grundsätzlich nicht ohne Prüfung der Rechtslage im Empfängerland 46
11 Beschäftigtendatenschutz 50
11.1 Aushang von Dienstplänen 50
11.2 Datenschutzrechtlicher Auskunftsanspruch von (ehemaligen) Beschäftigten 50
11.3 Corona-Tests von Beschäftigten 51
11.4 Zeiterfassung mittels Fingerabdruck 52
12 Gesundheit und Soziales 54
12.1 Nachweispflicht der Masernschutzimpfung 54
12.2 Videosprechstunde beim Arzt 54
12.3 Glaubhaftmachung eines Befreiungsgrundes von der „Maskenpflicht" 55
12.4 Anwendbarkeit der für öffentliche Schulen geltenden datenschutzrechtlichen Regelungen auf private Schulen 56
12.5 Einsatz digitaler Werkzeuge im pandemiebedingten Distanzunterricht 56
13 Vereine und Verbände 59
13.1 Segelflieger - Veröffentlichung von Flugdaten auf einer Internetplattform 59
13.2 Veröffentlichung von Videoaufnahmen einer Veranstaltung eines Selbsthilfevereins im Internet 59
14 Wohnungswirtschaft und Mieterdatenschutz 62
14.1 Mitteilung von Rückständen bei der Hausgeldzahlung in der Eigentümergemeinschaft 62
14.2 Umgang mit Adressdaten bei Energieversorgern 62
14.3 Überwachung der Wasserentnahme in einer Eigentümergemeinschaft 63
14.4 Weitergabe von Kontaktdaten eines Mieters durch Vermieter an Handwerker 64
15 Videoüberwachung 66

15.1 Fotografien von Kfz-Kennzeichen von Falschparkenden durch Privatpersonen ... 66
15.2 Videoüberwachung in Fitnessstudios ... 67
15.3 Videoüberwachung von Privatpersonen ... 68
16 Datenschutzverletzungen ... 70
17 Technischer Datenschutz und Informationssicherheit ... 73
17.1 Windows 10 – Umgang mit Telemetriedaten ... 73
17.2 Ransomware-Trojaner stehlen zunehmend auch personenbezogene Daten ... 74
17.3 Datenverarbeitung durch Tesla-Fahrzeuge ... 75
17.4 Cyberabwehr Bayern ... 76
18 Bußgeldverfahren ... 78
18.1 Bericht aus der Zentralen Bußgeldstelle ... 78
Stichwortverzeichnis ... 81

1

Datenschutzaufsicht im nicht-öffentlichen Bereich

1 Datenschutzaufsicht im nicht-öffentlichen Bereich

1.1 Gesetzliche Grundlage für den Tätigkeitsbericht

Seit Geltungsbeginn der DS-GVO ist jede Aufsichtsbehörde durch Art. 59 DS-GVO verpflichtet, einen Jahresbericht über ihre Tätigkeit zu erstellen.

Wie bisher vermittelt unser Bericht nicht nur unsere rechtliche Beurteilung bestimmter Fallkonstellationen, sondern insbesondere auch statistische Angaben, die ein Gesamtbild unserer Schwerpunkte und Arbeitsbedingungen abgeben sollen.

1.2 Datenschutz in Bayern

Im Einklang mit Art. 51 DS-GVO hat der bayerische Gesetzgeber

- uns, das Bayerische Landesamt für Datenschutzaufsicht (BayLDA), für nicht-öffentliche Stellen in Bayern (Art. 18 Bayerisches Datenschutzgesetz - 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. Vor dem Hintergrund der gemeinsamen Verpflichtung zur einheitlichen Anwendung und Durchsetzung der DS-GVO enthält Art. 21 BayDSG letztlich klarstellend einen an alle vier Behörden adressierten Auftrag zur gegenseitigen Zusammenarbeit und Unterstützung. Im aufsichtlichen Alltag wird diesem Auftrag durch einen stetigen Informationsaustausch vor allem in Querschnittsbereichen wie dem Gesundheitswesen oder dem Internetrecht und regelmäßige Positionsabstimmungen insbesondere mit dem Bayerischen Landesbeauftragten für den Datenschutz und dem Medienbeauftragten für den Datenschutz für die Bayerische Landeszentrale für neue Medien Rechnung getragen.

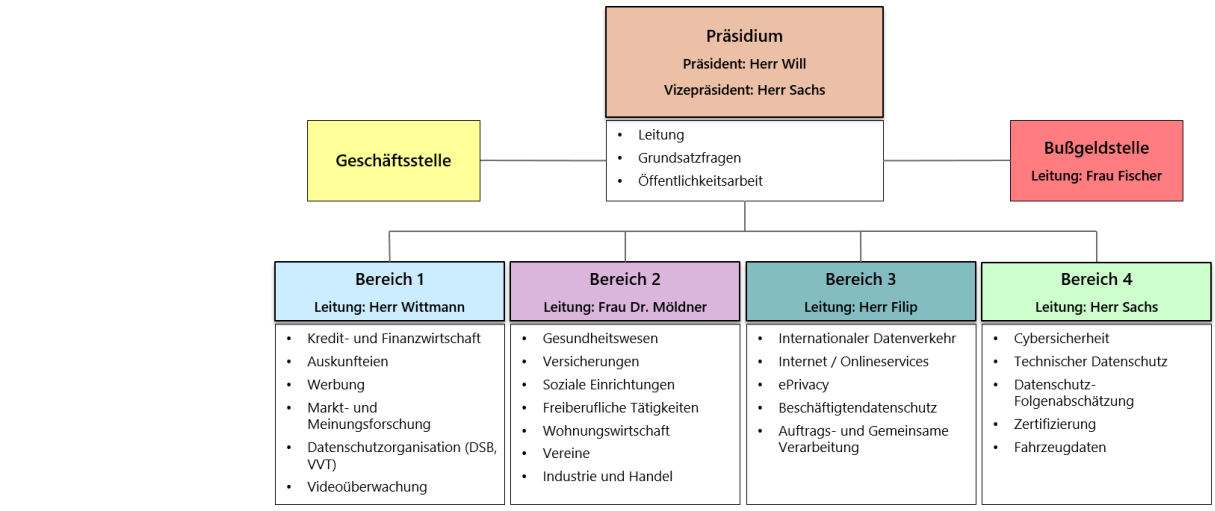
Darüber hinaus haben Kirchen, religiöse Vereinigungen oder Gemeinschaften gemäß Art. 91 DS-GVO, die Möglichkeit eine spezifische Aufsichtsbehörde einzurichten, die dann als Aufsichtsbehörde anzusehen ist, wenn sie die in Art. 51 ff. DS-GVO genannten Voraussetzungen, insbesondere der Unabhängigkeit, erfüllen.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

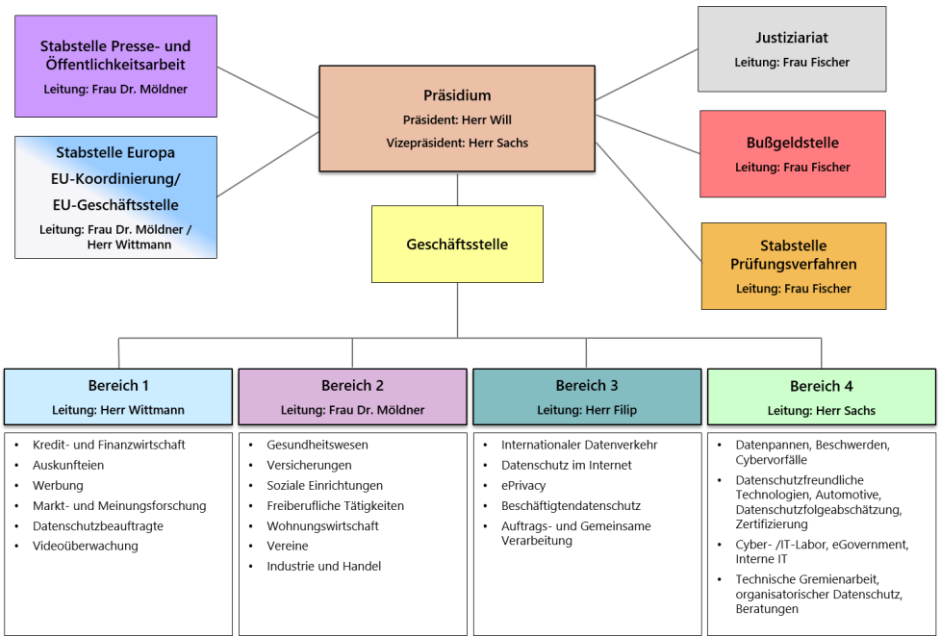
1.3 Das Bayerische Landesamt für Datenschutzaufsicht

Unabhängig von allen Sonderbedingungen hat alleine die im folgenden Kapitel aufzuzeigende Entwicklung der Fallzahlen das Jahr 2020 erneut zu einer enormen Herausforderung werden lassen. Stärker als in ihren Anfangsjahren ist in allen Bereichen zudem spürbar geworden, dass die DS-GVO unsere bisherigen Arbeitsbedingungen verändert und uns mit der Aufgabe der Zusammenarbeit mit den anderen Aufsichtsbehörden der Mitgliedsstaaten neue Handlungsformen, Abläufe und letztlich auch Organisationsstrukturen abverlangt.

Parallel dazu haben Entwicklungen außerhalb des Datenschutzrechts wie der Brexit sowie weitere – vor allem mit der später noch detailliert anzusprechenden „Schrems II-Entscheidung" des EuGH verbundene - Rechtsunsicherheiten und Anpassungserfordernisse im Internationalen Datenverkehr und schließlich einmal mehr die Rückwirkungen der Digitalisierung auf das Datenschutzrecht letztlich strukturelle Veränderungen innerhalb unsere Behörde erforderlich gemacht. Auch wenn diese – wie wir hoffen: nur vorläufig – trotz aller Belastungen alleine im bisherigen Personalbestand und damit erstmals im BayLDA mit der Übernahme von Mehrfachfunktionen umgesetzt werden können, soll der Umbauprozess des Jahres 2020 das BayLDA für seine gewandelten Aufgaben im europäischen Vollzugsverbund der Datenschutzaufsichtsbehörden ertüchtigen und Schwerpunktverlagerungen gerecht werden. Zuletzt soll er aber auch Defiziten entgegen wirken, die wir uns gerade im Bereich unserer strategischen Prüfaufgaben eingestehen mussten.

Obgleich letzte Nachjustierungen erst im Jahresverlauf 2021 vollzogen wurden und damit jenseits des Stichtages des Berichtszeitraums liegen, sollen die beiden nachfolgenden Organigramme mit den bisherigen und den aktuellen Strukturen unserer Behörde diesen Veränderungsprozess illustrieren:





2

Zahlen und Fakten

2 Zahlen und Fakten

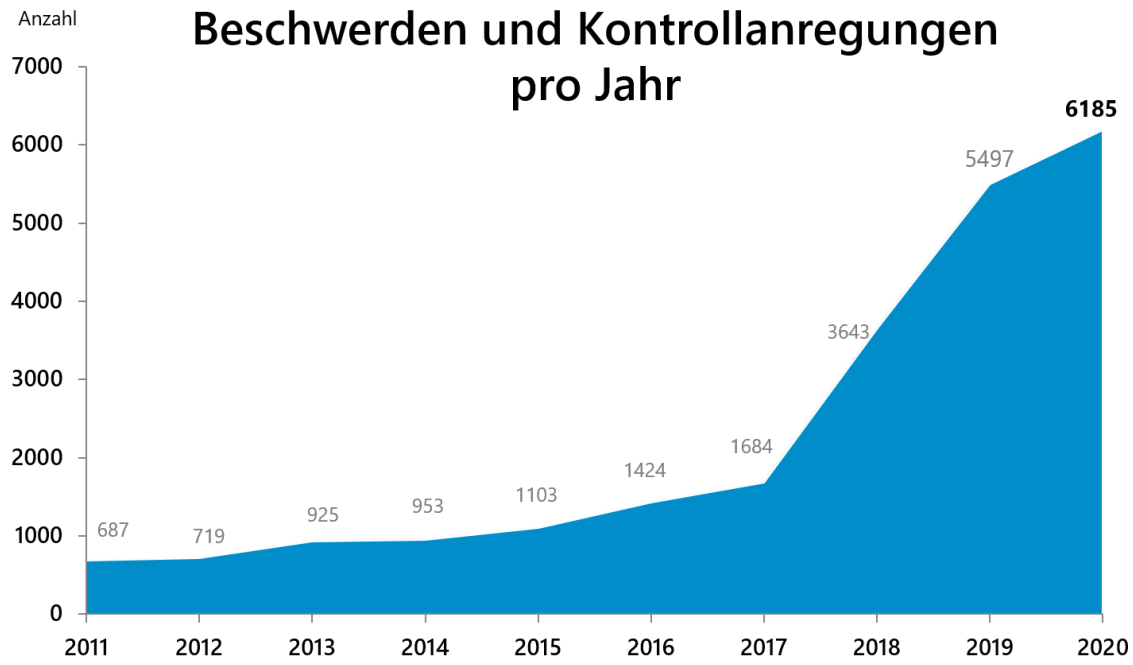
Wie schon in den letzten Tätigkeitsberichten gezeigt, verfügt das BayLDA aufgrund seines bereits seit Jahren aufgebauten elektronischen Vorgangsverwaltungssystems „IGOR" über sehr detailgenaue statistische Auswertungsmöglichkeiten, die weit über die in Art. 59 der DS-GVO aufgenommenen Mindestinformationen hinausgehen. „IGOR" hat unter den besonderen Bedingungen des Jahres 2020 derart an Bedeutung gewonnen, dass er schon zur Komplettierung des Gesamtbildes als „34. Mitarbeiter des BayLDA" näher vorzustellen bleibt:

„IGOR" ist gleichsam das digitale Rückgrat des BayLDA. Das im BayLDA eigenständig entwickelte und kontinuierlich passgenau ausgebaute Programm erlaubt als frühe Ausprägung von eGovernement für zahlreiche Fallgestaltungen einfacher Komplexität eine weitgehend elektronische, standardisierte Fallbearbeitung. Gleichzeitig war es damit das Fundament für den pandemiebedingten Rückzug nahezu sämtlicher Beschäftigter ins Home-Office bei Fortführung der bisherigen Produktivität. Mit geringfügigen Ergänzungen vor allem im Bereich der Archivierung soll es bis spätestens Jahresende 2021 eine vollelektronische Aktenführung bieten.

2.1 Beschwerden

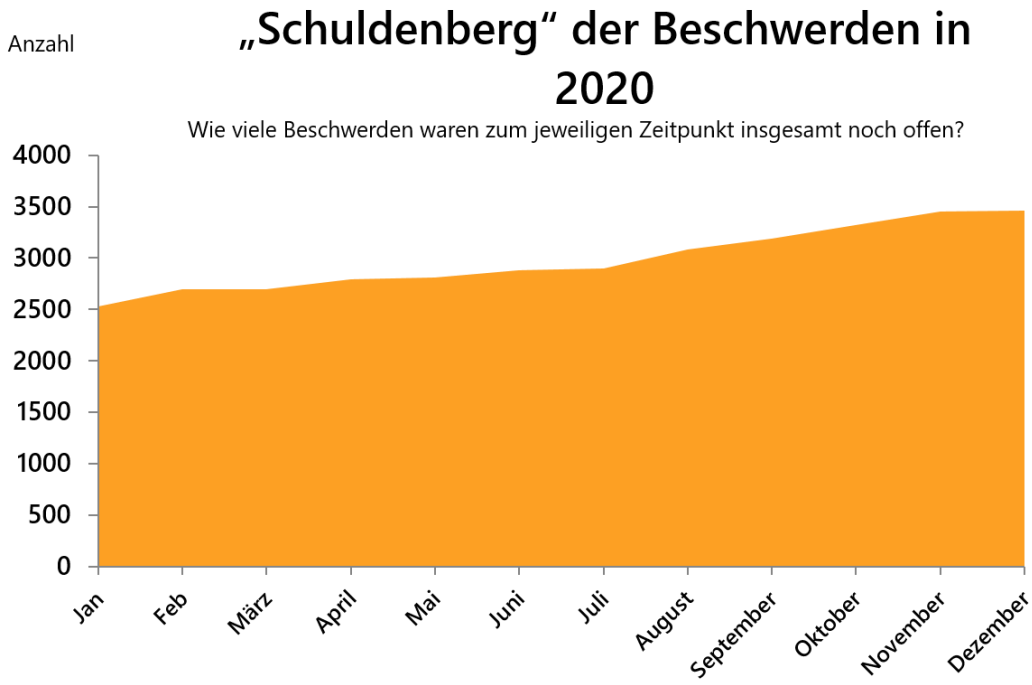
Die Gesamtanzahl der Beschwerden und Kontrollanregungen, die 2020 bei uns eingegangen sind, ist der unten folgenden Grafik zu entnehmen. Sie zeigt im Vergleich zu den bereits singulären Vorjahreszahlen einen abermaligen Anstieg, der sich einer Verzehnfachung der Fallzahlen im zurückliegenden Jahrzehnt annähert.

Als Beschwerden werden dabei zum einen solche Vorgänge gezählt, die schriftlich eingehen und bei denen eine natürliche Person eine persönliche Betroffenheit darlegt, für die Art. 78 DS-GVO anwendbar ist. Dies schließt Abgaben ein. Telefonische „Beschwerden" werden dann gezählt, wenn sie z. B. durch einen Vermerk verschriftlicht werden.



Unter dem Obergriff „Beschwerden“ erhielten wir auch im Jahr 2020 eine erhebliche Anzahl von Meldungen über Datenschutzverstöße, bei denen die Eingabeführer nicht glaubhaft gemacht haben, durch den vorgetragenen Sachverhalt in den eigenen Rechten verletzt zu sein. Diese Eingänge bezeichnen wir nicht als Beschwerden, sondern als Kontrollanregungen.

Die Notwendigkeit einer Unterscheidung zwischen Kontrollanregung und Beschwerden ergibt sich aus ihren unterschiedlichen Rechtsfolgen: Art. 78 Abs. 2 DS-GVO verlangt, betroffene Personen innerhalb von drei Monaten über den Stand oder das Ergebnis des Beschwerdeverfahrens in Kenntnis zu setzen.



Kann die Aufsichtsbehörde dieser Verpflichtung nicht nachkommen, steht dem Betroffenen eine (Untätigkeits-)Klage offen. Zu berücksichtigen bleibt freilich, dass im Wege der Untätigkeitsklage lediglich die gerichtliche Feststellung erreicht werden kann, dass die Aufsichtsbehörde zur umgehenden Prüfung des Beschwerdevorbringens verpflichtet ist, nicht aber eine Sachentscheidung z. B. in Gestalt einer Untersagung der strittigen Datenverarbeitung. Im allseitigen Interesse an der Vermeidung solch eigentlich unproduktiver Streitigkeiten sind wir daher trotz aller Fallbelastungen vorrangig bestrebt, der Drei-Monatsfrist des Art. 78 Abs. 2 DS-GVO gerecht zu werden.

Demgegenüber besteht bei Kontrollanregungen kein Anspruch darauf, vom BayLDA innerhalb einer bestimmten Frist über den Stand des Verfahrens unterrichtet zu werden. Bei Kontrollanregungen erhält der Mitteilende daher regelmäßig nur eine Bestätigung, dass wir seine Mitteilung als Kontrollanregung erfasst haben und nach pflichtgemäßem Ermessen entscheiden werden, ob und inwieweit wir dieser Anregung nachgehen.

Der abermalige Anstieg der Beschwerdezahlen kann mittlerweile nicht mehr als Sondereffekt der DS-GVO betrachtet werden. Er ist gleichermaßen Spiegelbild einer wünschenswerten Sensibilität für Datenschutzfragen wie Konsequenz einer alle Lebensbereiche durchdringenden Digitalisierung. Dieser Grundlast ist freilich auch der seit Jahresende 2019 um sieben Beschäftigte angewachsene Personalkörper des BayLDA nicht gewachsen. Wie im Jahr 2019 gab es auch 2020 kaum einen Monat, in dem es gelang, mehr Beschwerdeverfahren abzuschließen als

neue Vorgänge eingingen. Bestanden bereits zum Jahresende 2019 rund 2500 offene Vorgänge, wurde dieser Wert zum Jahresende 2020 nochmals mit mehr als 3100 offenen Verfahren übertroffen. Statistisch entspricht dieser Rückstand etwa 75 % eines derzeitigen jährlichen Gesamteingangs aller Beschwerden.

Dieser Rückstand verschlechtert unsere durchschnittliche Bearbeitungsdauer erheblich, enttäuscht die berechtigten Erwartungen der Bürgerinnen und Bürger in eine effektive Durchsetzung ihrer durch das Unionsrecht gewährleisteten Rechte und wird unserem Selbstverständnis als Teil eines bürgernahen und leistungsfähigen Rechtsstaates nicht gerecht. Überdies führt er zum Gesamtbefund einer reaktiv-verwaltenden statt proaktiv-gestaltenden Datenschutzaufsicht. Je stärker der datenschutzaufsichtliche Alltag durch Fristen im Grenzbereich und alle Ressourcen ausschöpfenden Eingangszahlen bestimmt wird, desto mehr droht die Zurückstellung notwendiger strategischer Schwerpunkte insbesondere im Bereich von Prävention und Beratung. Ungeachtet der Sonderbedingungen der Pandemie zeigt dies die Jahresbilanz 2020 mit einer weiteren „0“ bei anlasslosen Prüfungen und Vor-Ort-Kontrollen überdeutlich. Einer unserer Handlungsschwerpunkte des Jahres 2021 wird deshalb die Wiederaufnahme solcher Prüfungen sein, für die wir alle organisatorisch machbaren Ansätze wie z. B. Online-Prüfungen oder Fragebogenversendungen ausschöpfen werden.

2.2 Beratungen

Um die Vergleichbarkeit mit den Berichten anderer Aufsichtsbehörden sicherzustellen, verstehen wir unter Beratungen im vorliegenden Bericht nur die schriftliche Beantwortung von Anfragen von Verantwortlichen, betroffenen Personen und der eigenen Regierung, sowie telefonische Beratungen, die im Vorgangsverwaltungssystem erfasst wurden. Schulungen, Vorträge etc. werden nicht mehr berücksichtigt, aber derzeit dennoch von uns separat erfasst.

In der nebenstehenden Tabelle sind die Beratungen im Berichtszeitraum aufgeführt. Sie umfasst wie in den Vorjahren auch telefonische Beratungen im eben genannten Sinne. Abermals ist die Anzahl der Beratungen im Verhältnis zum letzten Jahr deutlich gesunken. Diese Entwicklung ist im Ergebnis nicht Grund zur Besorgnis, sondern gerade im Rückblick auf ein Jahr mit einer Unzahl neuer Fragen und Fallgestaltung des pandemischen Infektionsschutzes ermutigend:

Mit dem kontinuierlichen Ausbau unserer Online-Informationen, z. B. detailgenauen Hinweisen auf die sich mit der Pandemielage stetig wandelnden Fragestellungen im Bereich des Beschäftigtendatenschutzes, privater Schulen oder bei Handel und Dienstleistungen genauso wie im Bereich der Cybersicherheit, versuchen wir weiterhin, absehbaren Wellen neuer Beratungsanfragen zuvorzukommen.

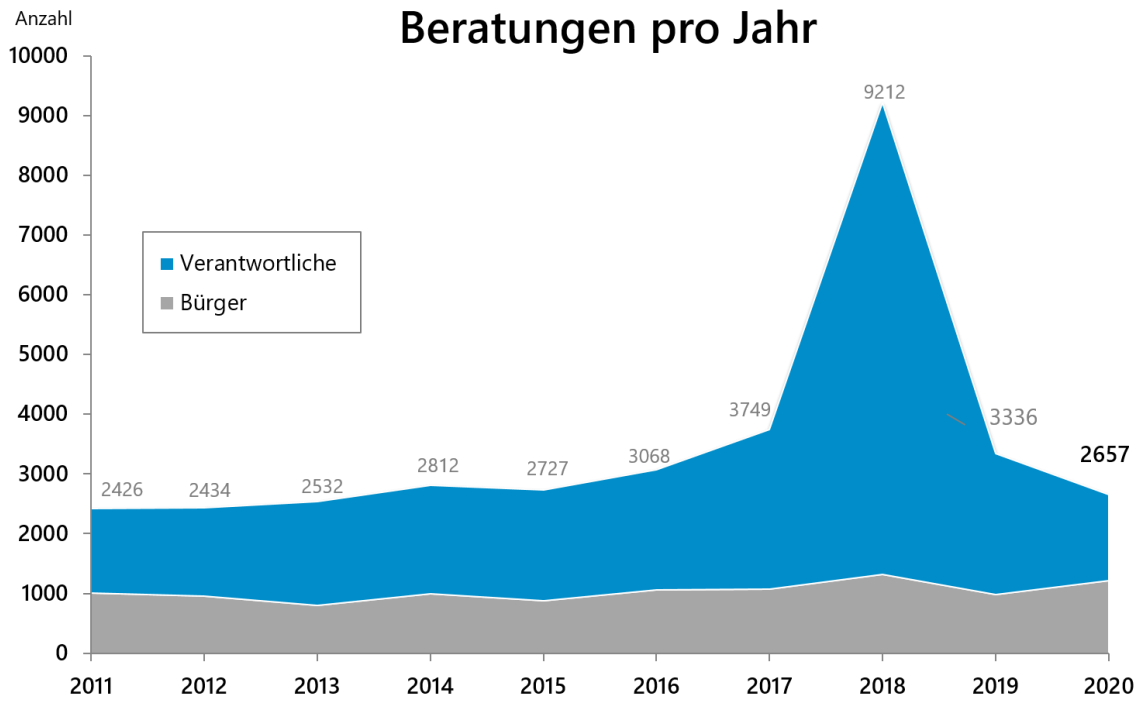
Beratungen im Berichtszeitraum

Verantwortliche	2020
Telefonische Beratungen	233
Schriftliche Beratungen	1212

Bürger	2020
Telefonische Beratungen	273
Schriftliche Beratungen	844

Weiterhin bietet unsere Webseite die Möglichkeit der Online-Beratung. Interessierte Personen können dabei zu bestimmten Themenbereichen Fragen an uns schicken. In diesem Prozess werden ihnen dann vor Eingabe der Frage die FAQs zu dem ausgewählten Thema angegeben, die wir erstellt haben.

www.lda.bayern.de/de/beratung.html



2.3 Datenschutzverletzungen

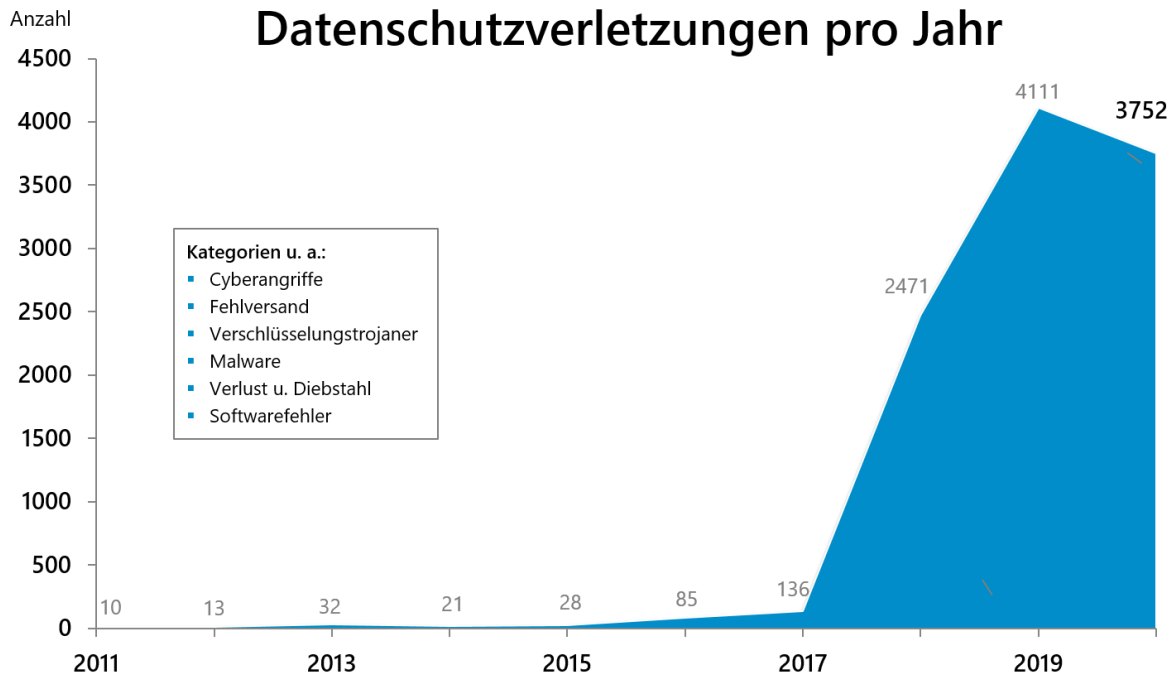
Wie schon in den vorangegangenen Jahren ist die Zahl der Meldungen von Verletzungen der Sicherheit bei der Verarbeitung personenbezogener Daten weiterhin hoch. Datenschutzverletzungen bestimmten damit neben den Beschwerden und den Beratungen unseren Arbeitsalltag. Trotz ihrer Masse verlangen sie Fall für Fall eine genaue, aufmerksame Untersuchung, um frühzeitig neue Angriffsstrategien von Cyberkriminellen genauso wie strukturelle Defizite einzelner Verantwortlicher zu identifizieren.

In der unten aufgeführten Grafik werden die bei uns eingegangenen Meldungen nach Art. 33 DS-GVO, die von den jeweiligen Verantwortlichen abgegeben wurden, dargestellt. Weitere Informationen zum Thema Datenschutzverletzungen im Allgemeinen sind im Kapitel 16 dieses Berichts zu finden.

2.4 Abhilfemaßnahmen; Europäische Zusammenarbeit

Entsprechend einer im Kreis der Aufsichtsbehörden festgelegten, von statistischen Befunden der einzelnen Behörde zunächst losgelösten formalen Struktur soll bei der Darstellung der Abhilfemaßnahmen grundsätzlich der Befugniskatalog des Art. 58 Abs. 2 DS-GVO abgebildet werden. Im Einzelnen handelt es sich dabei um:

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



Trotz seiner zu Beginn des Kapitels dargestellten Vorzüge und Fortentwicklungen erlaubt es unser internes Fachverfahren IGOR auch 2020 noch nicht, diese Angaben automatisiert auszuwerten. Da die Dimension unserer Fallzahlen die Möglichkeiten einer manuellen Auswertung bei weitem übersteigt, bleibt unser Ziel, diese Angaben zu Abhilfemaßnahmen im Tätigkeitsbericht 2021 präsentieren zu können. Entsprechendes gilt für Verfahren der europäischen Zusammenarbeit, für die wir ebenfalls noch keine belastbaren Zahlen liefern können, die jedoch ebenfalls in nicht unerheblichem Umfang anfallen.

2.5 Förmliche Begleitung von Rechtsetzungsvorhaben

Anders als im Vorjahr hatte das BayLDA aufgrund der Sonderbedingungen der Pandemie im Jahresverlauf 2020 in einer statistisch bislang nicht erfassten Größenordnung Gelegenheit, zu den zahlreichen vor allem untergesetzlichen infektionsschutzrechtlichen Neuregelungen und ihrer wiederholten Fortschreibung durch den Landesgesetzgeber Stellung zu nehmen. Gleiches gilt für die nicht unerhebliche Zahl ergänzender exekutivischer Regelungen in Gestalt von Ministerialverfügungen, Rahmenplänen oder sonstigen Schutzkonzepten, in deren Abstimmung das BayLDA häufig zwar außerordentlich kurzfristig, aber unkompliziert und weit über die Grenzen der formalen Unterrichtungspflicht des Art. 16 Abs. 3 BayDSG hinaus einbezogen wurde.

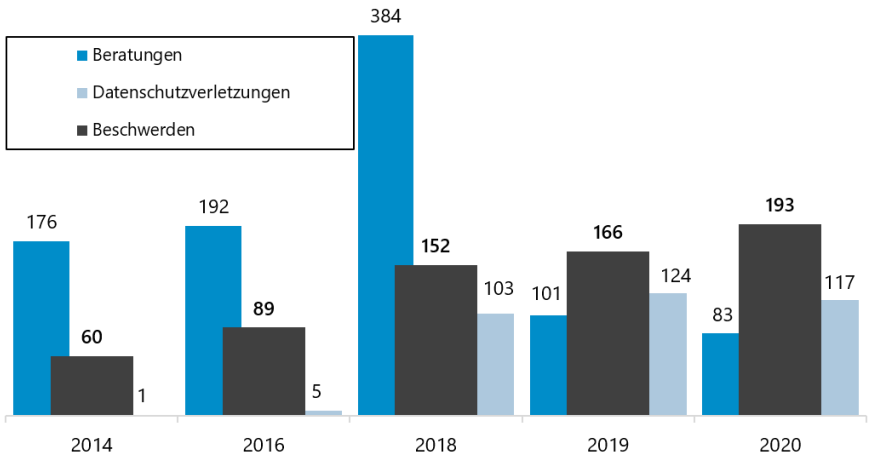
Neben der Wahrung datenschutzrechtlicher Grundprinzipien, insbesondere der klaren Grenzen des Erforderlichkeitsgrundsatzes standen dabei regelmäßig die Praxistauglichkeit und damit die Gewährleistung datenschutzgerechter Verarbeitungsbedingungen für nicht öffentliche Stellen wie z. B. Arztpraxen, Gastwirte oder Vereine im Vordergrund.

2.6 Ressourcen

Im Berichtszeitraum konnte das BayLDA auf Grundlage der bereits im vorangehenden Bericht ausführlicher dargestellten Stellenumschichtungen eine zusätzliche Kraft für seine Geschäftsstelle gewinnen, die die bisherigen Strukturen entlasten und die Einführung einer vollständigen elektronischen Aktenführung unterstützen soll.

Weitere Verstärkungen, die eine quantitative und qualitative Fortentwicklung der bestehenden Strukturen eröffnen würden, waren mit Rücksicht auf die auch für den Haushaltsgesetzgeber durch die Pandemie grundlegend veränderten Rahmenbedingungen nicht durchsetzbar.

Durchschnittliche Vorgänge pro Planstelle



Angesichts der in diesem Kapitel aufgezeigten Fallzahlen müssen und werden sie von uns mit Nachdruck in die kommenden Haushaltsaufstellungsverfahren eingebracht werden.

2.7 Vorträge und Öffentlichkeitsarbeit

Wir haben auch im Jahr 2020 eine erhebliche Anzahl von Vorträgen gehalten und dabei überwiegend Datenschutzbeauftragte geschult bzw. informiert. Ein besonderes Anliegen war es uns wieder, die meist von den Industrie- und Handelskammern und der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) organisierten ERFA-Kreise in München, Nürnberg, Würzburg, Coburg und Bayreuth zu besuchen und dort die zahlreich vorab eingereichten Fragen zu beantworten.

Im Rahmen unserer Öffentlichkeitsarbeit erweiterten wir fortlaufend unser Angebot auf unserer Webseite, damit Interessierte einfach und schnell Antworten auf ihre Fragen finden konnten. Dabei war es uns wichtig, die Informationen so praxisgerecht zu kondensieren und mit Mustern zu ergänzen, dass Vereine, freiberuflich Tätige und auch sehr kleine Unternehmen eine effektive alltagstaugliche Unterstützung in der Wahrnehmung ihrer datenschutzrechtlichen Verantwortlichkeit finden konnten.

3

Corona

3 Corona

3.1 Kontaktdatenerfassung zur Pandemiebekämpfung

Zur Nachverfolgung von Infektionsketten zur Bekämpfung der COVID-19-Pandemie wurden Gastronomie- und einige andere Betriebe durch Landesverordnung zur Erfassung der Kontaktdaten von Kunden verpflichtet. Wir haben die Unternehmen hierbei intensiv beraten. Dennoch kam es immer wieder zu datenschutzrechtlichen Beschwerden, insbesondere wenn zur Erfassung Listen eingesetzt und so die erforderliche Vertraulichkeit nicht gewahrt wurde.

Im Rahmen der Bekämpfung der COVID-19-Pandemie wurde durch den Landesgesetzgeber im Rahmen der Infektionsschutzmaßnahmenverordnung unter anderem die Erfassung von Kontaktdaten in zahlreichen Bereichen des öffentlichen Lebens vorgeschrieben. Danach wurden u. a. Gastronomen und später auch Friseur- und andere Betriebe verpflichtet, Namen, Aufenthaltszeitraum und entweder Telefonnummer oder E-Mail- oder postalische Adresse von Kunden zu erfassen, für vier Wochen aufzubewahren und dem Gesundheitsamt auf Verlangen zum Zwecke der Nachverfolgung von Infektionsketten vorzulegen.

Unser Haus wurde von der Staatsregierung im Rahmen der Erarbeitung der entsprechenden Rechtsgrundlage einbezogen. Zudem haben wir Kontakt mit den Berufsverbänden der Gastronomie sowie den Industrie- und Handelskammern aufgenommen, um auf diesem Weg die Gastronomen für die datenschutzkonforme Umsetzung der Kontaktdatenerfassung zu sensibilisieren.

Dennoch ging während der Zeiträume, in denen die Gastronomiebetriebe geöffnet waren (bis zum Spätherbst 2020), eine erhebliche Anzahl von Beschwerden bei uns ein. In den meisten Fällen beschwerten sich Gäste darüber, dass die Kontaktdaten mittels (oft auf den Tischen ausliegenden) Listen erfasst wurden, d. h. so, dass jede sich eintragende Person Kenntnis von den personenbezogenen Daten anderer Personen nehmen konnte. Wir sind jeder Beschwerde dieser Art nachgegangen und haben darauf hingewirkt, dass für die Erfassung Einzelformulare verwendet werden. Wir haben auch entsprechende Muster bereitgestellt und über die o. g. Multiplikatoren bekannt gemacht. In diese Muster haben wir auch die den betroffenen Personen nach Art. 13 DS-GVO zu erteilenden Informationen über die Verarbeitung ihrer Daten aufgenommen, da es nach unserer Beobachtung in den von den Betrieben verwendeten Mustern gerade hieran vielfach gefehlt hat.

Zwischenzeitlich war im Jahr 2020 auch die Ausübung von Wettkampf- und Trainingsbetrieb im Freizeitsport in gewissen Umfang zulässig, wobei eine Kontaktdatenerfassung jedoch nicht vorgeschrieben war, sondern lediglich die Maßgabe bestand, dass Personen mit typischen COVID-19-Krankheitssymptomen der Zugang zu Sportanlagen zu verwehren war. In solchen und anderen Fällen, in denen die Erfassung von Kontaktdaten rechtlich nicht vorgeschrieben war bzw. ist, darf diese auch nicht stattfinden, weil hierfür keine datenschutzrechtliche Rechtsgrundlage besteht. Soweit keine ausdrückliche gesetzliche Verpflichtung zur Kontaktdatenerfassung besteht, lässt sich diese insbesondere auch nicht etwa auf Art. 6 Abs. 1 Buchst. e DS-GVO stützen, weil bei Fehlen einer ausdrücklichen gesetzlichen Pflicht gerade nicht davon ausgegangen werden kann, dass die Erfassung im Rahmen einer Aufgabenwahrnehmung im öffentlichen Interesse geschieht. Sportvereine, Trainingsgruppen und andere Akteure, die sich mit der Frage nach der Zulässigkeit der Erfassung von Kontaktdaten an uns gewandt haben, haben wir entsprechend beraten.

3.2 Zutrittskontrollen durch Fiebermessen, Wärmebildkameras oder Vorzeigenlassen der Corona-Warn-App

Zahlreiche Anfragen erreichten uns im Zusammenhang mit Überlegungen, den Zutritt von Kundinnen und Kunden und/oder Beschäftigten zu Geschäftsräumen aller Art durch Fiebermessen – oft mittels Wärmebildkameras – zu regeln. Dadurch erhofften sich manche Unternehmen, das Risiko des Zutritts von mit SARS-CoV-2 infizierten Personen zu reduzieren. Doch datenschutzrechtlich ist diese Zutrittskontrolle in aller Regel unzulässig.

Zahlreiche Unternehmen wollten angesichts der Pandemie den Zutritt von Beschäftigten und/oder der Kundinnen und Kunden zu ihren Geschäftsräumen von einer Kontrolle auf – tatsächliche oder vermeintliche – Verdachtsmomente auf eine Corona-Infektion abhängig machen. Uns erreichten zahlreiche Anfragen zur Zulässigkeit kontaktloser Temperaturerfassungen – meist per Infrarotmessung mittels Thermometer oder Wärmebildkameras. Da auch andere Aufsichtsbehörden Anfragen dieser Art erhielten, hat sich die Datenschutzkonferenz hierzu am 10.09.2020 in einem Beschluss geäußert:

https://www.datenschutzkonferenz-online.de/media/dskb/20200910_beschluss_waeremebildkameras.pdf

Ausgangspunkt für die datenschutzrechtliche Bewertung der Datenschutzkonferenz war der Umstand, dass für nicht-öffentliche Stellen – etwa Unternehmen – zwar grundsätzlich ein für sich gesehen berechtigtes Interesse im Sinne von Artikel 6 Abs. 1 Buchst. f DS-GVO in Betracht käme, durch die Verhinderung des Zutritts infizierter Personen Gefährdungen für die Beschäftigten und/oder die übrige Kundschaft zu vermeiden. Jedoch kann die Fiebermessung in aller Regel nicht als „erforderlich" zur Verfolgung dieses Interesses gelten. Denn eine erhöhte Körpertemperatur ist kein ausreichend klares Indiz auf eine Infektion mit SARS-CoV-2, denn eine Reihe von Infektionen verlaufen symptomlos. Zudem kann eine erhöhte Temperatur auch auf anderen Gründen als gerade einer Infektion mit diesem Virus beruhen. Darauf hat die Datenschutzkonferenz im o. g. Beschluss hingewiesen. Entsprechend haben wir die bei uns eingehenden Beratungsanfragen beantwortet.

Diese Erwägungen gelten gleichermaßen, soweit Fiebermessung von Beschäftigten als betriebliche Maßnahme des Arbeitsschutzes durch Arbeitgeber erwogen und somit datenschutzrechtlich als Rechtsgrundlage § 26 BDSG in Betracht gezogen wird. Zudem stehen mildere Mittel zur Verfügung, etwa nach gesundheitlichen Beeinträchtigungen der Arbeitsfähigkeit zu fragen, soweit diese für die auszuübenden Tätigkeiten relevant sind, so dass es auch deshalb in aller Regel an der Erforderlichkeit fehlt. In Betracht kommen können jedoch ggf. bei Beschäftigten Befragungen zu etwaigen Aufenthalten in einem Corona-Risikogebiet.

Ein Unternehmen wollte im Rahmen der Zutrittskontrolle von Kunden verlangen, die Corona-Warn-App vorzuzeigen. Auch dies haben wir als datenschutzrechtlich unzulässig bewertet. Die App zeigte (im Berichtszeitraum) lediglich „Risikobegegnungen" an, indes liefert auch diese Information keinen ausreichenden Anhaltspunkt für eine Infektion mit SARS-CoV-2, so dass die Verarbeitung dieser Information ebenso wenig als „erforderlich" im Sinne der Wahrnehmung eines berechtigten Interesses des Unternehmens gelten kann. Der Anwendungsbereich der DS-GVO ist bei diesem Vorgehen im Übrigen eröffnet, denn das kontrollierende Unternehmen verwendet durch das Anschauen der Informationen in der App zweifellos personenbezogene Daten. Zweck der Verarbeitung ist die Entscheidung über die Zugangsgewährung etwa zu Geschäftsräumen. Es handelt sich somit um eine „teilweise automatisierte

Verarbeitung, für die die DS-GVO gemäß ihrem Artikel 2 Abs. 1 gilt. Nicht maßgeblich ist der Umstand, dass sich die technischen Mittel der Verarbeitung nicht „in den Händen" des kontrollierenden Unternehmens befinden; letzteres ist keine Voraussetzung für die Anwendbarkeit der DS-GVO.

3.3 Videokonferenzsysteme im Home-Office

Die Datenschutzkonferenz hat eine Orientierungshilfe und eine ergänzende Checkliste zum Einsatz von Videokonferenzsystemen veröffentlicht.

Die Corona-Pandemie hat in vielen Branchen zu einer massiven Ausweitung der Arbeit von Beschäftigten im Home-Office geführt. Viele Unternehmen waren dadurch kurzfristig vor die Notwendigkeit gestellt, interne Besprechungen oder Besprechungen mit Geschäftspartnern als Telefon- oder Videokonferenzen durchzuführen. Gerade der Einsatz von Videokonferenzsystemen wirft eine Vielzahl datenschutzrechtlicher Fragen auf. Die Konferenz der Datenschutzaufsichtsbehörden von Bund und Ländern hat daher in ihrer Orientierungshilfe „Videokonferenzsysteme" und einer ergänzenden Checkliste Antworten auf die wichtigsten datenschutzrechtlichen Fragen für die Nutzung von Videokonferenzsysteme gegeben:

https://www.datenschutzkonferenz-online.de/orientierungshilfen.html

Unser Haus hat im Rahmen einer „Checkliste zu datenschutzrechtlichen Regelungen bei Home-Office" die zentralen datenschutzrechtlichen Anforderungen, die neben Videokonferenzen insbesondere technische und organisatorische Maßnahmen in den Blick nehmen, im Rahmen einer praxisnahen Übersicht zusammengefasst:

https://www.lda.bayern.de/de/checklisten.html

Die zahlreichen bei uns eingegangenen Beratungsanfragen zeigten, dass gerade kleine und mittlere Unternehmen, aber auch Vereine und andere Akteure aus dem nichtöffentlichen Bereich (im Folgenden: nutzende Unternehmen) keine eigenen Videokonferenzsysteme betreiben, sondern auf Systeme externer Anbieter zurückgreifen. Den nutzenden Unternehmen muss bewusst sein, dass sie hierbei als datenschutzrechtlich Verantwortliche für die Verarbeitung der Daten ihrer Beschäftigten und ggf. Kundinnen und Kunden agieren und mit Dienstleistern einen Vertrag zur Auftragsverarbeitung abschließen müssen.

Soweit eine Besprechung aufgrund der Home-Office-Situation als Videokonferenz durchgeführt werden muss, legitimiert § 26 Abs. 1 Satz 1 BDSG als Rechtsgrundlage für den Arbeitgeber die zur Durchführung der Besprechung notwendige Verarbeitung personenbezogener Daten seiner Beschäftigten. Eine Einwilligung der Beschäftigten ist daher insoweit nicht erforderlich. Dabei ist jedoch im Einzelfall zu prüfen, ob neben der Übertragung von Ton auch die Übertragung von Bilddaten erforderlich ist.

Besonders wichtig ist es, den betroffenen Personen gemäß Art. 13 DS-GVO die Informationen über die im Rahmen der Videokonferenz stattfindenden Verarbeitungen ihrer personenbezogenen Daten zu erteilen. Hierbei muss auch transparent informiert werden, ob eine Aufzeichnung erfolgen soll. In den meisten Fällen wird eine Aufzeichnung nicht erforderlich sein und es somit an einer Rechtsgrundlage für die Aufzeichnung fehlen. Eine Aufzeichnung darf dann nur stattfinden, wenn alle Beteiligten hierzu ihre Einwilligung erteilen.

Beim Einsatz von Videokonferenzsystemen externer Anbieter ist darauf zu achten, ob der Anbieter sich vorbehält, die anfallenden personenbezogenen Daten auch für eigene Zwecke zu verwenden. In solchen Fällen würde der Arbeitgeber bzw. das nutzende Unternehmen eine

Rechtsgrundlage benötigen, um die personenbezogenen Daten zu diesen – meist anderen – Zwecken an den Anbieter zu übermitteln. Hieran wird es häufig fehlen. Daher ist diese Frage anhand der Nutzungsbedingungen und des Auftragsverarbeitungsvertrags des Anbieters besonders sorgfältig zu prüfen.

Ferner muss das nutzende Unternehmen darauf achten, ob das eingesetzte System zu Übermittlungen personenbezogener Daten in Drittländer führt. Das ist häufig der Fall, insbesondere werden zahlreiche der am Markt befindlichen Dienste von US-Unternehmen angeboten. Finden Übermittlungen in Drittländer statt, sind die hierfür geltenden besonderen Anforderungen nach Kapitel V der DS-GVO zu erfüllen. Diese Fälle haben aufgrund der Schrems-II-Entscheidung des Europäischen Gerichtshofs vom 16.07.2020 eine zusätzliche Brisanz bekommen (vgl. dazu die Ausführungen in unserem Kapitel zum Internationalen Datenverkehr).

4

Auftragsverarbeitung

4 Auftragsverarbeitung

4.1 Auftragsverarbeitung, getrennte Verantwortlichkeit oder doch gemeinsame Verantwortlichkeit?

Wirken mehrere Beteiligte an einer Verarbeitung personenbezogener Daten mit, ist für die Abgrenzung zwischen Auftragsverarbeitung, gemeinsamer Verantwortlichkeit und getrennter Verantwortlichkeit die Beteiligung der Akteure an der Entscheidung über die Zwecke und wesentlichen Mittel der Verarbeitung maßgeblich.

Schon vor Geltungsbeginn der DS-GVO erhielten wir viele Anfragen zu den unterschiedlichsten Praxiskonstellationen der Verarbeitung personenbezogener Daten unter Mitwirkung mehrere Akteure, verbunden mit der Bitte um Einschätzung, ob es sich um Auftragsverarbeitung handele. Unter der DS-GVO ist nun verstärkt auch die Abgrenzung zur gemeinsamen Verantwortlichkeit sehr relevant, zumal der Europäische Gerichtshof bereits in mehreren Fällen aus dem Internetbereich eine gemeinsame Verantwortlichkeit bejaht hat.

Wichtige Hinweise für die Einordnung der Akteure als getrennte oder gemeinsame Verantwortliche oder als Auftragsverarbeiter gibt das Leitlinienpapier Nr. 7/2020 des Europäischen Datenschutzausschusses (EDSA), das die maßgeblichen Kriterien für die datenschutzrechtliche Rollenzuweisung erläutert. Das Papier berücksichtigt auch die einschlägigen Entscheidungen des Europäischen Gerichtshofs (EuGH) in den Rechtssachen „Fashion ID", „Wirtschaftsakademie" und „Zeugen Jehovas".

https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_de

Nach dem Gesetzeswortlaut (Art. 26 DS-GVO) liegt eine gemeinsame Verantwortlichkeit vor, wenn zwei oder mehr Verantwortliche die Zwecke und wesentlichen Mittel der Verarbeitung gemeinsam festlegen. Dies wiederum kommt in zwei Varianten vor: in der „einfachen" Variante verfolgen die Beteiligten einen gemeinsamen Zweck. Gemeinsame Verantwortlichkeit gibt es aber – so der Europäische Gerichtshof – auch dann, wenn mehrere Beteiligte zwar jeweils unterschiedliche Zwecke festlegen, die Zwecke sich jedoch ergänzen, weil die Verarbeitung nur deshalb stattfinden kann, weil jeder Beteiligte jeweils seinen Zweck festgelegt und zudem einen Beitrag zur Festlegung der wesentlichen Mittel der Verarbeitung geleistet hat (etwa einen Social Media Button in seine Webseite eingebunden hat). Die Abgrenzung zur getrennten Verantwortlichkeit ist in dieser zweiten Variante der gemeinsamen Verantwortlichkeit nicht immer ganz einfach.

Der Umstand, dass alle Beteiligten ein wirtschaftliches Interesse an der Verarbeitung haben, reicht für sich gesehen nicht aus, um gemeinsame Verantwortlichkeit zu begründen. Dienstleister, die lediglich Verarbeitungsleistungen gegen Entgelt erbringen, haben zwar naturgemäß hieran ein wirtschaftliches Interesse, sie sind jedoch – soweit sie die Zwecke der Verarbeitung nicht festlegen – nicht (gemeinsam) Verantwortliche, sondern Auftragsverarbeiter. Darauf weist das oben zitierte EDSA-Leitlinienpapier (Rn. 60) ausdrücklich hin. Im Ergebnis bestätigt diese Aussage das von uns schon vor Geltungsbeginn der DS-GVO vertretene maßgebliche Abgrenzungskriterium zwischen Verantwortlichkeit und Auftragsverarbeitung. Die größere Herausforderung für die Praxis dürfte es demgegenüber sein, wie oben dargestellt zwischen getrennter und gemeinsamer Verantwortlichkeit zu unterscheiden.

5

Datenschutz im Internet

5 Datenschutz im Internet

5.1 Zulässigkeit von Immobilienbewertungsportalen

Bei der Veröffentlichung von Immobilienschätzwerten auf einem Internetportal kann Art. 6 Abs. 1 Buchst. f DS-GVO als Rechtsgrundlage in Betracht kommen.

Die Veröffentlichung von Immobilienschätzwerten kann auf die datenschutzrechtliche Rechtsgrundlage des Art. 6 Abs. 1 Buchst. f DS-GVO gestützt werden, wonach eine Verarbeitung personenbezogener Daten dann rechtmäßig ist, wenn diese „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich" ist und „sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen."

Im Rahmen der gemäß dieser Vorschrift vorzunehmenden Abwägungsentscheidung sind die Interessen der von einer Veröffentlichung eines Schätzwertes Betroffenen in ausreichendem Maße zu berücksichtigen. Dies kann unter anderem dadurch erfolgen, dass kein konkreter Immobilienwert veröffentlicht wird, sondern nur eine Wertspanne, deren Berechnungsmethode ausreichend transparent dargestellt werden sollte. Hierzu ist insbesondere über die herangezogenen Parameter zu informieren und ob es sich hierbei um öffentlich zugängliche Informationen handelt. Weiterhin sollte den Interessen der Betroffenen dadurch Rechnung getragen werden, dass ein voraussetzungsloses Widerspruchsrecht gewährt wird, welches auf einfache Art und Weise ausgeübt werden kann.

Hinsichtlich der Erfüllung der Informationspflichten nach Art. 14 DS-GVO sehen wir es als möglich an, die Ausnahmevorschrift des Art. 14 Abs. 5 Buchst. b DS-GVO heranzuziehen. Danach ist die Informationspflicht ausgeschlossen, sofern die Erteilung der Information sich als unmöglich erweisen oder einen unverhältnismäßigen Aufwand erfordern würde. Die Unmöglichkeit bzw. Unverhältnismäßigkeit sind nicht objektiv zu bestimmten, sondern subjektiv auf den Verantwortlichen bezogen. In diesen Fällen muss der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Personen treffen, einschließlich der Bereitstellung der Informationen für die Öffentlichkeit, beispielsweise durch regionale Presse- oder Fernsehbeiträge und durch bereitgestellte Informationen auf der jeweiligen Internetseite.

In diesem Kontext hat unsere Behörde wiederholt datenschutzrechtliche Fragestellungen mit der Scoperty GmbH erörtert, welche das Immobilienbewertungsportal

www.scoperty.de

betreibt. Dabei haben wir mehrfach Nachbesserungen zu Gunsten der Nutzenden und betroffenen Grundstückseigentümerinnen und -eigentümer durchgesetzt, sodass angesichts der dadurch erreichten gegenwärtigen Ausgestaltung des Internetdienstes aktuell kein Anlass besteht, weitere aufsichtliche Schritte zu ergreifen.

5.2 Google Analytics

Der Einsatz von Google Analytics ist nur mit Einwilligung erlaubt.

Wie in unserem letzten Tätigkeitsbericht unter Punkt 6.3 dargestellt, ist im Regelfall für die Nutzung des Dienstes „Google Analytics" eine Einwilligung des Betroffenen erforderlich.

Dennoch berufen sich auch weiterhin noch immer viele Webseitenbetreiber darauf, dass der Dienst als „unbedingt erforderlich" oder „notwendig" zu qualifizieren sei und daher keiner

Einwilligung bedürfe, sondern auf ein berechtigtes Interesse gemäß Art. 6 Abs. 1 Buchst. f DS-GVO gestützt werden könne.

Durch den Beschluss der DSK vom 12.05.2020 haben die deutschen Aufsichtsbehörden ihre einheitliche Auffassung dargestellt, dass dies bei Einsatz des Dienstes in der Standardkonfiguration nicht möglich ist. Sofern abweichende Einstellungen vorgenommen werden oder beispielsweise auch Google Analytics 360 eingesetzt wird, konnte in der Vergangenheit Art. 6 Abs. 1 Buchst. f DS-GVO als Rechtsgrundlage in Betracht kommen, allerdings wird dies im Hinblick auf die Rechtsprechung zu „Planet49" und auf das am 01.12.2021 in Kraft tretende Telekommunikations-Telemedien-Datenschutzgesetzes (TTDSG) zukünftig zu verneinen sein.

Der Beschluss hat in der Praxis sehr große Relevanz, da es in nahezu allen Zuschriften, die wir in Bezug auf Tracking bei Webseiten erhalten, um den Einsatz von Google Analytics geht.

Häufigster Fehler bei der Einbindung des Dienstes ist das Aktivieren des Tools noch bevor eine aktive Einwilligung im Sinne von Art. 4 Nr. 11 und Art. 7 DS-GVO erteilt wird. Wird so vorgegangen, kann der Einsatz und die nachfolgende Verarbeitung auf keine Rechtsgrundlage gestützt werden.

Durch den Beschluss der DSK wird auch klargestellt, dass die Kürzung der IP-Adresse durch Ergänzung des Trackingcodes um die Funktion „_anonymizeIp()" lediglich eine zusätzliche Maßnahme gem. Art. 25 Abs. 1 DS-GVO darstellt und nicht dazu führt, dass die vollständige Datenverarbeitung anonymisiert erfolgt.

https://www.datenschutzkonferenz-online.de/media/dskb/20200526_beschluss_vorabwiderspruche_bei_streetview_und_vergleichbaren_diensten.pdf

5.3 Cookies – nur noch mit Einwilligung? § 15 Abs. 3 TMG in richtlinienkonformer Auslegung als Rechtsgrundlage für Webtracking

Der Zugriff in Form des Auslesens oder Speicherns von Informationen auf Endgeräten kann nicht auf ein berechtigtes Interesse gestützt werden.

Wie im vorangehenden Berichtszeitraum hat auch im Jahr 2020 der Einsatz von Cookies Rechtsprechung und Rechtsanwender gleichermaßen intensiv beschäftigt. Zugleich sind erstmals seit vielen Jahren klare Vorgaben zumindest des nationalen Gesetzgebers absehbar: Nach der EuGH-Entscheidung im Verfahren C-673/17 - Planet49 - vom 01.10.2019 folgte am 28.05.2020 das Urteil des Bundesgerichtshof im nationalen Verfahren (I ZR 7/16 - Cookie-Einwilligung II). In dem zugrunde liegenden Sachverhalt musste darüber entschieden werden, ob für das Setzen von Cookies mit dem Zwecke der Profilbildung eine Einwilligung erforderlich ist.

Bisher wurden diese Cookies oder ähnliche Technologien häufig bereits beim ersten Aufruf der Webseite eingesetzt und dem Nutzenden lediglich ein Widerspruchsrecht (Opt-Out) eingeräumt und in den Datenschutzhinweisen darüber informiert. Diese Vorgehensweise wurde rechtlich auf § 15 Abs. 3 Telemediengesetz (TMG) gestützt, welcher ein Opt-Out, dem Wortlaut nach, als ausreichend erachtet. Bislang war umstritten, ob diese Regelung eine ausreichende Umsetzung der ePrivacy-Richtlinie 2002/58/ EG in Form der sog. Cookie-Richtlinie 2009/136/EG darstellt. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hatte am 26. April 2018 eine Positionsbestimmung zur Anwendbarkeit des Telemediengesetztes (TMG) für nicht-öffentliche Stellen ab dem 25.05.2018 veröffentlicht, in welcher die Auffassung vertreten wurde, dass Art. 5 Abs. 3 ePrivacy-Richtlinie in Deutschland nicht

umgesetzt worden sei. Im Ergebnis wurde daher durch die deutschen Datenschutzbehörden eine generelle Anwendung der Regelungen der DS-GVO bejaht.

Entgegen dieser Auffassung hat der BGH nun im vorliegenden Verfahren § 15 Abs. 3 TMG als Umsetzung des Art. 5 Abs. 3 ePrivacy-Richtlinie und damit als wirksame Rechtsgrundlage angesehen, da § 15 Abs. 3 TMG nach Ansicht des Gerichts richtlinienkonform auszulegen ist. Diese Auslegung wurde durch den BGH wie folgt vorgenommen:

> *„Im Fehlen einer (wirksamen) Einwilligung kann im Blick darauf, dass der Gesetzgeber mit § 15 Abs. 3 Satz 1 TMG das unionsrechtliche Einwilligungserfordernis umgesetzt sah, der nach dieser Vorschrift der Zulässigkeit der Erstellung von Nutzungsprofilen entgegenstehende Widerspruch gesehen werden."*

Damit ergibt sich für den Einsatz von Cookies und anderen Technologien, welche der Erstellung von Nutzerprofilen zum Zwecke der Werbung oder Marktforschung dienen, dass diese einer Einwilligung bedürfen. Damit ist der Einsatz nicht notwendiger Dienste, welche Informationen auf Endgeräten speichern oder auslesen, nicht mehr auf Grundlage eines berechtigten Interesses nach Art. 6 Abs. 1 Buchst. f DS-GVO möglich. Eine Diskrepanz hinsichtlich der Folgen, die aus der Orientierungshilfe für Anbieter von Telemedien und den Folgen des BGH-Urteils resultieren, besteht daher nur bei Diensten, welche bisher auf Grundlage eines berechtigten Interesses Cookies auf den Endgeräten platziert haben, beispielweise zur reinen Reichweitenanalyse.

Um in diesen Bereichen Rechtsunsicherheit zu vermeiden, raten wir Webseitenbetreibern für alle im Sinne des Art. 5 Abs. 3 ePrivacy- Richtlinie einwilligungspflichtigen Zugriffe auf Endgeräte eine Einwilligung nach den Voraussetzungen von Art. 6 Abs. 1 Buchst. a i.V.m. Art. 4 Nr. 11 und Art. 7 DS-GVO einzuholen. Soweit der Einsatz von Cookies und ähnlichen Technologien noch auf Art. 6 Abs. 1 Buchst. f DS-GVO gestützt wird, gibt uns dies aufgrund des durch die Orientierungshilfe für Anbieter von Telemedien geschaffenen Rechtscheintatbestands zu keinen aufsichtlichen Schritten Anlass, soweit ein berechtigtes Interesse nachgewiesen wird und eine ordnungsgemäße Interessenabwägung erfolgt ist.

Die Anforderungen an die dann nachfolgenden Datenverarbeitungen, welche an das Speichern von Informationen oder den Zugriff auf Informationen anschließen, die bereits im Endgerät eines Nutzers gespeichert sind, richten sich auch weiterhin ausschließlich nach der DS-GVO.

Mit dem zukünftigen Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG) zeichnet sich im Vorgriff auf eine europäische Gesamtregelung im Rahmen der ePrivacy-Verordnung eine kohärente gesetzliche Regelung des Zugriffs auf Endeinrichtungen und damit auch der sog. Cookie-Nutzung ab. Die Darstellung ihrer Auswirkungen im Einzelnen bleibt unserem nachfolgenden Tätigkeitsbericht vorbehalten.

5.4 Apple Kamerafahrten

Für die von Apple veranlassten Videoaufnahmen von Straßen und Häusern zur Verbesserung der eigenen Kartendienste kann Art. 6 Abs. 1 Buchst. f DS-GVO als Rechtsgrundlage in Betracht kommen. Betroffene können die Unkenntlichmachung ihrer personenbezogenen Daten verlangen.

Am 12.05.2020 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder einen Beschluss zu Vorabwidersprüchen bei (Google) StreetView und vergleichbaren Diensten veröffentlicht, welcher auch im Hinblick auf die durch Apple durchgeführten Kamerafahrten Bedeutung erlangt. Über

dieses Thema haben wir im letzten Tätigkeitsbericht unter Punkt 16.2 berichtet

Der Beschluss stellt klar, dass bei Veröffentlichung von Straßenansichten, einschließlich teilweiser Abbildungen von Häuserfassaden und privaten Grundstücksbereichen, welche an den öffentlichen Straßenraum angrenzen, im Rahmen von StreetView und ähnlichen Diensten Art. 6 Abs. 1 Buchst. f DS-GVO als Rechtsgrundlage in Betracht kommen kann.

Neben dem Hinweis auf die generellen Anforderungen, die sich aus dieser Rechtsgrundlage ergeben, stellt der Beschluss besonders heraus, dass betroffene Personen auch die Unkenntlichmachung personenbezogener Daten verlangen können. Hiervon umfasst sind auch Abbildungen von Häuserfassaden und privaten Grundstücksbereichen, welche nicht automatisiert unkenntlich gemacht werden.

Betroffene Personen können diese Möglichkeit ab dem Zeitpunkt der Anfertigung der Aufnahmen durch den Dienst wahrnehmen. Unabhängig hiervon besteht bei Vorliegen einer besonderen persönlichen Situation auch das Widerspruchsrecht nach Art. 21 DS-GVO. Das Verlangen nach Unkenntlichmachung gemäß Art. 17 Abs. 1 DS-GVO und der Widerspruch nach Art. 21 DS-GVO müssen sowohl online als auch postalisch eingelegt werden können. Auf diese Rechte muss ausdrücklich hingewiesen werden.

Im Zuge dessen hat Apple auf unser Ersuchen hin mittlerweile auch eine postalische Adresse für die Einreichung des Widerspruchs bereitgestellt, zu finden unter:

https://www.lda.bayern.de/de/thema_apple_kamerafahrten.html

Für Beschwerden ist unsere Behörde, aufgrund der deutschen Niederlassung in München, innerdeutsch zuständig. Wir leiten diese Eingaben zur federführenden Bearbeitung der irischen Aufsichtsbehörde zu, da der Sitz der europäischen Hauptniederlassung in Irland ist.

6

Steuerberater und Rechtsanwälte

6 Steuerberater und Rechtsanwälte

6.1 Klarstellende Regelungen zur datenschutzrechtlichen Verantwortlichkeit und den Verarbeitungsbefugnissen von Steuerberatern im Steuerberatungsgesetz (StBerG)

Der Gesetzgeber hat unsere Auffassung bestätigt, wonach Steuerberater eigenständige Verantwortliche sind, welche die zur Erfüllung ihrer Aufgaben nach dem StBerG erforderlichen Daten verarbeiten dürfen.

Uns erreichen nach wie vor Eingaben, in denen die Beauftragung von Steuerberatern insbesondere zum Zwecke der Lohnbuchhaltung thematisiert wird. Schwerpunktmäßig geht es dabei um die Frage, ob die Beauftragung des Steuerberaters datenschutzrechtlich als Auftragsverarbeitung i. S. d. Art. 28 DS-GVO zu qualifizieren ist, die den Abschluss eines Auftragsverarbeitungsvertrags zwischen den Beteiligten erfordern würde.

Bereits in der Vergangenheit haben wir die Auffassung vertreten, dass Steuerberater in diesen Fällen nicht als Auftragsverarbeiter, sondern als eigenständige Verantwortliche gem. Art. 4 Nr. 7 DS-GVO zu qualifizieren sind (siehe unseren 8. Tätigkeitsbericht 2017/2018, dort Punkt 9.1). Grund hierfür ist ihre Weisungsunabhängigkeit, die dem Wesen der Auftragsverarbeitung widerspricht (vgl. Art. 28 Abs. 3 Satz 2 Buchst. a DS-GVO).

Unsere Auffassung wurde zwischenzeitlich durch den Gesetzgeber bestätigt. Aufgrund Art. 23 des Gesetzes zur weiteren steuerlichen Förderung der Elektromobilität und zur Änderung weiterer steuerlicher Vorschriften vom 12.12.2019 (BGBl. I S. 2451), in Kraft getreten am 18.12.2019, wurde u. a. § 11 StBerG neu gefasst. § 11 Abs. 2 Satz 2 StBerG stellt klar, dass die zur unbeschränkten Hilfeleistung in Steuersachen befugten Stellen (also u. a. Steuerberater, vgl. § 3 Nr. 1 StBerG) bei Verarbeitung sämtlicher personenbezogener Daten ihrer Mandanten Verantwortliche gem. Art. 4 Nr. 7 DS-GVO sind. Die Weisungsfreiheit dieser Stellen wird in § 11 Abs. 2 Satz 1 StBerG nochmals festgehalten.

Darüber hinaus enthält § 11 Abs. 1 StBerG detailliertere Angaben zu den Datenverarbeitungsbefugnissen von Steuerberatern und vergleichbaren Stellen. Personenbezogene Daten dürfen demnach verarbeitet werden, soweit es zur Erfüllung der Aufgaben nach dem StBerG erforderlich ist (§ 11 Abs. 1 Satz 1 StBerG). Dies gilt auch, soweit die Daten für Zwecke künftiger Verfahren verarbeitet werden (§ 11 Abs. 1 Satz 2 StBerG). Ebenso wird klargestellt, dass auf der Grundlage des StBerG auch besondere Kategorien personenbezogener Daten verarbeitet werden dürfen (Art. 9 Abs. 2 Buchst. g DS-GVO i.V.m. § 11 Abs. 1 Satz 3 StBerG). Diese Auffassung haben wir ebenfalls bereits in der Vergangenheit vertreten.

6.2 Datenerhebungsbefugnisse von Insolvenzverwaltern

Insolvenzverwalter sind spätestens ab Eröffnung des jeweiligen Insolvenzverfahrens eigenständige Verantwortliche gem. Art. 4 Nr. 7 DS-GVO. Sie haben daher einerseits die von den Insolvenzgläubigern angemeldeten Forderungen einzutragen und können anderseits Forderungen des Insolvenzschuldners gegen Dritte geltend machen.

Aufgrund der Sars-CoV-2-Pandemie ist – trotz der vorübergehenden Aussetzung der Insolvenzantragspflicht – in den nächsten Jahren mit

einem Anstieg von Insolvenzverfahren zu rechnen. Im Rahmen dieser Verfahren stellen sich oft auch datenschutzrechtliche Fragen, da der zu bestellende Insolvenzverwalter notwendigerweise personenbezogene Daten (des Insolvenzschuldners, von Insolvenzgläubigern sowie ggf. Dritten) verarbeitet.

Obgleich es zu Einzelheiten der datenschutzrechtlichen Einordnung von Insolvenzverwaltern im Detail noch offene Fragen gibt, besteht Einigkeit dahingehend, dass diese spätestens mit Eröffnung des Insolvenzverfahrens als eigenständige Verantwortliche gem. Art. 4 Nr. 7 DS-GVO anzusehen sind. Denn in diesem Zeitpunkt geht das Recht des Schuldners, das zur Insolvenzmasse gehörende Vermögen zu verwalten und über es zu verfügen, auf den Insolvenzverwalter über (§ 80 Abs. 1 VwGO).

Gemäß § 175 Abs. 1 Satz 1 Insolvenzordnung (InsO) hat der Insolvenzverwalter jede von einem Insolvenzgläubiger angemeldete Forderung mit den Angaben nach § 174 Abs. 2, Abs. 3 InsO in die Insolvenztabelle einzutragen und diese gem. § 175 Abs. 1 Satz 2 InsO zur Einsicht der Beteiligten niederzulegen. In die Tabelle einzutragen sind insbesondere der Grund und Betrag der Forderung sowie die vollständige Bezeichnung des Gläubigers. Die damit notwendigerweise verbundenen Datenverarbeitungen können auf Art. 6 Abs. 1 Satz 1 Buchst. c DS-GVO als eine rechtliche Verpflichtung des Insolvenzverwalters gestützt werden.

Spiegelbildlich hat der Insolvenzverwalter aufgrund des auf ihn übergegangenen Verwaltungs- und Verfügungsrechts auch die Befugnis, die Forderungen des Insolvenzschuldners gegen Dritte geltend zu machen und in diesem Zusammenhang ggf. Inkassounternehmen einzuschalten. Rechtsgrundlage ist insoweit Art. 6 Abs. 1 Satz 1 Buchst. b DS-GVO.

6.3 Datenschutzrechtliche Verantwortlichkeit und Verarbeitungsbefugnisse gerichtlich bestellter Sachverständiger

Gerichtlich bestellte Sachverständige sind als eigenständige Verantwortliche einzuordnen, die grundsätzlich auch ohne Einwilligung Betroffener personenbezogene Daten verarbeiten dürfen.

Mitunter beschweren sich Eingabeführende bei uns darüber, dass im Rahmen einer gerichtlichen Auseinandersetzung ihre personenbezogenen Daten von einer bzw. einem Sachverständigen ohne Einwilligung verarbeitet worden seien. In erster Linie geht es dabei um die Einholung eines Gutachtens, mit dessen Erstellung die jeweiligen Sachverständigen vom Gericht per Beweisbeschluss beauftragt worden sind.

Die in diesem Zusammenhang vorgenommenen Datenverarbeitungen unterfallen der Zuständigkeit der Datenschutzaufsichtsbehörden. Die Bereichsausnahme des Art. 55 Abs. 3 DS-GVO greift insoweit nicht, da es nicht um den Kernbereich richterlicher Unabhängigkeit geht (vgl. Erwägungsgrund 20 Satz 2 zur DS-GVO).

Gerichtlich bestellte Sachverständige sind ferner als eigenständige Verantwortliche gem. Art. 4 Nr. 7 DS-GVO zu qualifizieren. Ihre Aufgabe liegt nämlich gerade darin, dem Gericht Expertise in einem unbekannten Fachgebiet beizubringen. Hiermit verbunden ist die Weisungsfreiheit der jeweiligen Sachverständigen, was Inhalt und Ergebnis des Gutachtens sowie die dabei angewandte wissenschaftliche Methodik anbelangt. Die Sachverständigen bestimmen damit zumindest die Mittel der Datenverarbeitung selbst. Da sie keine Aufgaben der öffentlichen Verwaltung wahrnehmen, sind sie ferner nichtöffentliche Stellen.

Dies bedeutet jedoch nicht, dass gerichtlich bestellte Sachverständige für die von ihnen vorgenommenen Datenverarbeitungen eine Einwilligung der Betroffenen einholen müssten. Vielmehr stellt der Beweisbeschluss eine hinreichende Rechtsgrundlage i. S. d. Art. 6 Abs. 1 Satz 1 Buchst. c DS-GVO dar, aufgrund derer der/die jeweilige Sachverständige tätig werden darf bzw. muss. Soweit besondere Kategorien personenbezogener Daten verarbeitet werden, kann auf Art. 9 Abs. 2 Buchst. f DS-GVO zurückgegriffen werden.

7

Versicherungswirtschaft und Banken

7 Versicherungswirtschaft und Banken

7.1 Hinweis- und Informationssystem (HIS) der deutschen Versicherungswirtschaft

Gegen die im Rahmen der Nutzung des HIS erfolgenden Datenverarbeitungen bestehen im Grundsatz keine Bedenken.

Wir erhalten nach wie vor einige Eingaben, in denen die Übermittlung personenbezogener Daten an das Hinweis- und Informationssystem (HIS) der deutschen Versicherungswirtschaft durch Versicherungsunternehmen moniert wird.

Das HIS wird seit 01.04.2011 als Auskunftei von der informa HIS GmbH betrieben, einer eigenständigen Tochter von arvato infoscore.

Das HIS ist, mit Ausnahme der privaten Krankenversicherung, für alle Versicherungssparten (Kraftfahrt-, Unfall-, Rechtsschutz-, Sach-, Lebens-, Transport- und Haftpflichtversicherung) konzipiert. In jeder Sparte sind zwei getrennte Pools eingerichtet, ein Pool für die Antragsbearbeitung (A-Pool) und ein Pool für die Leistungsfallbeurteilung (L-Pool).

Eine Einmeldung in das HIS erfolgt, wenn einer der vordefinierten Meldegründe vorliegt. Dabei handelt es sich im Wesentlichen um zwei Kategorien von Gründen, nämlich einmal allgemeine risikorelevante Informationen sowie betrugsgeneigte Auffälligkeiten im konkreten Einzelfall. Berechtigt zur Einmeldung sind diejenigen Unternehmen, die mit der informa HIS GmbH einen entsprechenden HIS-Nutzungsvertrag geschlossen haben. Die von der Einmeldung betroffenen Personen werden über die Übermittlung ihrer Daten an das HIS durch das einmeldende Unternehmen informiert. Die Einmeldung als solche hat dagegen nicht automatisch zur Folge, dass der Abschluss eines Versicherungsvertrags oder die Schadensregulierung abgelehnt wird.

Sachbearbeiter der beteiligten Versicherungsunternehmen können entsprechend ihrer jeweiligen Berechtigungen auch Anfragen an das HIS richten, um Informationen über bestehende Einmeldungen zu erhalten. Auch hierüber werden die Betroffenen informiert. Die anfragenden Unternehmen müssen bei Anfragen jeweils ein berechtigtes Interesse im Einzelfall geltend machen. Dies wird von der informa HIS GmbH im Rahmen stichprobenartiger Kontrollen geprüft.

Bereits in der Vergangenheit haben wir klargestellt, dass die im Rahmen der Nutzung des HIS stattfindenden Datenverarbeitungen grundsätzlich zulässig sind (siehe unseren 5. Tätigkeitsbericht 2011/2012, dort Punkt 7.3). Dies hat sich auch seit Geltung der DS-GVO nicht geändert. Rechtsgrundlage für die jeweiligen Datenverarbeitungen im Rahmen des HIS ist nunmehr Art. 6 Abs. 1 Satz 1 Buchst. f DS-GVO. Die Verarbeitung ist regelmäßig zur Wahrung berechtigter Interessen der Versicherungsunternehmen erforderlich, da es um die Erkennung, Verhinderung und Aufklärung von Versicherungsbetrug geht (vgl. insoweit Erwägungsgrund 47 Satz 6 zur DS-GVO). Eine Einwilligung der Betroffenen ist daher nicht erforderlich, besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO werden nicht eingemeldet.

Das HIS wird auch den Vorgaben der Art. 12 ff. DS-GVO zur Transparenz hinreichend gerecht. Sowohl im Vorfeld als auch bei konkreten Einmeldungen und Anfragen erfolgt eine Information des Betroffenen. Die Betroffenen können sowohl gegenüber der informa HIS GmbH als auch gegenüber den jeweiligen Versicherungsunternehmen ihr Auskunftsrecht gem. Art. 15 DS-GVO geltend machen, um sich, sofern nicht ohnehin bekannt, über die Hintergründe ihrer Einmeldung zu informieren. Eine Verweigerung der Auskunft ist nur ausnahmsweise denkbar, wenn die jeweiligen Daten geheim gehalten

werden müssen, da anderenfalls die Abwehr unberechtigter Ansprüche gefährdet wäre (§ 29 Abs. 1 Satz 2 BDSG). Bei Vorliegen der entsprechenden Voraussetzungen können von den Betroffenen auch die Rechte auf Berichtigung, Löschung und Einschränkung der Verarbeitung (Art. 16 – 18 DS-GVO) geltend gemacht werden.

7.2 Kontoauszüge im Rahmen des Auskunftsanspruchs

Die DS-GVO gewährt betroffenen Personen zwar einen Anspruch auf Auskunft über ihre Kontobewegungen. Die Auskunft muss jedoch nicht in Form von Kontoauszugsduplikaten erfolgen.

Im Jahr 2020 hat das BayLDA über mehrere Beschwerden entschieden, in welchen sich betroffene Personen jeweils an eine Bank gewandt hatten, um im Rahmen des Auskunftsrechts nach Art. 15 DS-GVO Duplikate von bereits früher in Ausübung des Kontovertrags von der Bank bereitgestellten Kontoauszügen zu erhalten. Die Banken lehnten eine kostenlose Nacherstellung der Auszüge jeweils unter Verweis auf die eigenen Gebührenregelungen ab.

Ein Anspruch auf die kostenfreie Herausgabe von Zweitschriften von Kontoauszügen besteht durch Art. 15 DS-GVO nicht, da es sich bei den Kontoauszügen um eine besonders aufbereitete Form von Daten (hier: Kontobewegungen) handelt und die betroffene Person im Rahmen des Auskunftsrechts keinen Anspruch darauf hat, dass ihre Daten in eine solche besonders aufbereitete Form gebracht werden.

Insofern muss ein Recht auf Zweitschriften bzw. Kopien von Kontoauszügen nach Datenschutzrecht verneint werden. Damit unterliegt es auch nicht dem Datenschutzrecht darüber zu bestimmen, ob die für eine Nacherstellung von Kontoauszügen erhobenen Gebühren angemessen sind. Dies ist vielmehr eine vertragsrechtliche Fragestellung, die ggf. vor einem Zivilgericht zu klären ist.

Es handelt sich bei den in den Auszügen enthaltenen Kontobewegungen jedoch grundsätzlich um personenbezogene Daten, sodass im Rahmen des Auskunftsrechts durchaus ein Anspruch auf Herausgabe einer Auflistung dieser Kontobewegungen besteht; dies aber, wie oben geschildert, nicht in der aufbereiteten Form des ursprünglichen Kontoauszugs.

Ein Auskunftsersuchen, das sich nicht konkret auf diese Daten in Form von nacherstellten Kontoauszügen richtet, sondern auf eine bloße Auflistung der Kontobewegungen, wäre also entsprechend zu beantworten.

Eine Gebührenerhebung im Sinne des Art. 15 Abs. 3 DS-GVO wäre hier nur dann möglich, wenn dieses Ersuchen wiederholt erfolgt, da die erstmalige Bereitstellung von Kontoauszügen im Rahmen der Vertragsbeziehung nicht gleichzeitig eine erstmalige Erfüllung der datenschutzrechtlichen Auskunftsansprüche darstellt.

Wenn sich die Bank aus Gründen der Praktikabilität (z. B. aufgrund genereller Archivierung in Form des Kontoauszugs) dazu entscheidet, zur Erfüllung des Auskunftsanspruchs dennoch Kontoauszugsduplikate bereitzustellen, ist dies natürlich möglich.

Diese Entscheidung der Bank über die Bereitstellung in dieser besonders aufbereiteten Form dürfte dann jedoch nicht der betroffenen Person angelastet werden, sodass ein erstmaliges auf diese Daten gerichtetes Auskunftsersuchen weiterhin gebührenfrei bleiben muss.

Diese Entscheidung steht auch in Einklang mit einer zu diesem Sachverhalt im gleichen Jahr ergangenen Entscheidung des Amtsgerichts Bonn (Urt. v. 30.07.2020, Az. 118 C 315/19). Nach Auskunft des Gerichts ist das Urteil bestandskräftig.

7.3 Gutachten zur Beleihungswertermittlung im Rahmen des Auskunftsanspruchs

Interne Gutachten einer Bank zur Beleihungswertermittlung enthalten personenbezogene Daten, die auf Anforderung zu beauskunften sind. Im Rahmen der Auskunft muss jedoch nicht erkennbar sein, auf welche Art und Weise der Marktwert ermittelt wurde.

Eine Beschwerde im Jahr 2020 bezog sich darauf, dass eine Bank bei einem Kreditnehmer ein Gutachten zur Beleihungswertermittlung seiner Immobilie erstellt hat. Hierbei gestattete der Kreditnehmer der Bank auch freiwillig, die Innenräume der Immobilie zu betreten und Fotos der Wohnräume anzufertigen. Der Kreditnehmer wollte nun von der Bank im Rahmen des Datenschutzrechts eine Auskunft zu den Inhalten des Gutachtens erhalten. Die Bank gewährte ihm eine solche Auskunft nur teilweise und schwärzte beispielsweise den ermittelten Gesamtwert und die in der Wohnung angefertigten Fotos.

In einem Gutachten zur Beleihungswertermittlung sind unzweifelhaft personenbezogene Daten des Immobilieneigentümers enthalten, welche diesem auf Anforderung zu beauskunften sind. Eine Bank kann sich hier nicht darauf berufen, dass das Gutachten lediglich zu internen Zwecken bzw. zur Erfüllung gesetzlicher Verpflichtungen erstellt wurde. Dies schließt auch den ermittelten Gesamtwert der Immobilie mit ein, da dieser durch den direkten Bezug zu den Vermögensverhältnissen des Eigentümers ebenfalls ein personenbezogenes Datum darstellt. Obwohl er sich primär auf die Immobilie bezieht, handelt es sich hier noch nicht um ein Sachdatum ohne Personenbezug.

Dies gilt jedoch lediglich für den ermittelten Gesamtwert der Immobilie. Es besteht dagegen aus Art. 15 DS-GVO kein Anspruch darauf, dass aus der Auskunft auch ersichtlich sein müsste, auf welche Art und Weise der Marktwert ermittelt wurde. Hier besteht kein ausreichender Personenbezug mehr und die Bank könnte sich zudem bzgl. ihrer betriebsinternen Berechnungsmethodik auf Art. 15 Abs. 4 DS-GVO berufen.

Auch bei den in den Wohnräumen angefertigten Fotos handelt es sich jedenfalls bei einer selbstgenutzten Immobilie um personenbezogene Daten des Eigentümers. Auch wenn die Fotos für sich allein genommen nicht unbedingt eine Identifikation der betroffenen Person ermöglichen würden, werden sie vorliegend im Gesamtzusammenhang der übrigen Wertermittlung verarbeitet, was durch die anderen enthaltenen personenbezogenen Daten unzweifelhaft eine Zuordnung der Fotos zum Eigentümer und Rückschlüsse auf dessen Wohnsituation zulässt.

Bei fremdgenutzten Immobilien (Mietobjekte) hätte der Eigentümer jedoch aus Art. 15 DS-GVO keinen Anspruch auf die Beauskunftung enthaltener Fotos, da dies die Datenschutzrechte der Bewohner beeinträchtigen würde (Art. 15 Abs. 4 DS-GVO).

7.4 Positivdaten bei Energieversorgungsverträgen

Von Energieversorgungsunternehmen dürfen aufgrund von Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO keine Daten zu ungestört laufenden Verträgen an Wirtschaftsauskunfteien gemeldet werden.

Das BayLDA hat sich mit der Frage befasst, ob Energieversorgungsunternehmen auf Grundlage von Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO Positivdaten an Wirtschaftsauskunfteien melden dürfen. Zur bundeseinheitlichen Klärung wurde diese Streitfrage im Arbeitskreis Auskunfteien der DSK erörtert. Positivdaten sind Daten

über ungestört laufende Verträge. Im DSK-Beschluss vom 11.06.2018 werden Positivdaten bei Kredit- und Giroverträgen konkretisiert als Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung von solchen Verträgen. Allgemein versteht man also unter Positivdaten Daten zu ungestört laufenden Vertragsverhältnissen. Ungestört bedeutet hier, dass keine Vertragsstörungen, wie Zahlungsstörungen, aufgetreten sind. Im Gegensatz hierzu sind Negativdaten bestimmte Kriterien, bei denen ein Ereignis, welches eine vertragliche Störung, insbesondere eine Zahlungsstörung, begründet, aufgetreten ist. Dadurch kann die Zahlungsfähigkeit und Zahlungswilligkeit beurteilt werden.

https://www.datenschutzkonferenz-online.de/media/dskb/20180611_dskb_verarbeitung_positivdaten.pdf

Wir sehen als maßgebliches Kriterium für die Beurteilung der Zulässigkeit der Positivdatenspeicherung durch Wirtschaftsauskunfteien das kreditorische Risiko an. Dies ist das Risiko, das ein Vertragspartner eingeht, wenn dieser in Vorleistung geht und die Leistung vom anderen Vertragspartner erst im Nachhinein bezahlt wird. Bei Energieversorgungsverträgen liegt insofern ein kreditorisches Risiko vor, dass Energieversorgungsunternehmen mit der Energielieferung in Vorleistung gehen und Kunden diese erst im Nachhinein bezahlen. Allerdings ist dieses kreditorische Risiko stark begrenzbar durch Abschlagszahlungen oder Vorauszahlungen der Kunden. Daher wird das kreditorische Risiko von unserer Seite bei Energieversorgungsverträgen als nicht ausreichend hoch angesehen, als dass dieses ein berechtigtes Interesse gem. Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO an der Einmeldung von Positivdaten an Auskunfteien rechtfertigen könnte. In der Abwägungsentscheidung überwog das Interesse der Betroffenen dasjenige der Verantwortlichen.

8

Werbung und Adresshandel

8 Werbung und Adresshandel

8.1 Koppelungsverbot bei Newsletter-Anmeldungen

Anmeldungen zu einem Newsletter im Gegenzug für ein kostenloses Produkt sind nur dann freiwillig, wenn das gleiche Produkt auf derselben Plattform kostenpflichtig und ohne Pflicht zur Newsletter-Anmeldung angeboten wird.

Bei werblichen Sachverhalten stellt sich oftmals die Frage des Koppelungsverbots im Rahmen der Einwilligung gem. Art 6 Abs. 1 UAbs. 1 Buchst. a DS-GVO, insbesondere bei der Anmeldung zu einem Newsletter. Dabei spielt bei der Beurteilung der Freiwilligkeit der Einwilligung das Vorhandensein von Wahlmöglichkeiten eine zentrale Rolle.

In einem konkreten Fall hat ein Verlag eine nahezu kostenlose Software auf einem Online-Portal im Gegenzug zu einer verpflichtenden Einwilligung in die Newsletter-Anmeldung zur Verfügung gestellt. Alternativ konnte die Software auf einem eigenen Portal des Verlags kostenpflichtig ohne Einwilligung in die werbliche Nutzung erworben werden.

Der EDSA vertritt in den Guidelines zur Einwilligung die Ansicht, dass eine Einwilligung nicht als freiwillig angesehen werden kann, wenn zwischen einer Dienstleistung, zu der die Einwilligung in die Nutzung personenbezogener Daten für zusätzliche Zwecke gehört und einer vergleichbaren Dienstleistung, die von einem anderen Verantwortlichen angeboten wird, eine Wahlmöglichkeit besteht. Wir verstehen dies so, dass Anmeldungen zu einem Newsletter im Gegenzug zu einen kostenlosen Produkt nur dann freiwillig sind, wenn das gleiche Produkt auf derselben Plattform kostenpflichtig und ohne Pflicht zur Newsletter-Anmeldung angeboten wird. Es reicht dabei nicht aus, dieses Produkt kostenpflichtig auf einer völlig anderen Plattform von einem Drittanbieter anzubieten. Andernfalls würde dies bedeuten, dass der Verantwortliche die Entwicklungen des Marktes verfolgen müsste, um eine fortgesetzte Gültigkeit der Einwilligung in die Datenverarbeitungstätigkeiten sicherzustellen, da der Drittanbieter seine Dienstleistungen zu einem späteren Zeitpunkt ändern könnte.

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_de

9

Handel und Dienstleistung

9 Handel und Dienstleistung

9.1 Nutzung personenbezogener Daten für das Anbieten von „Hilfe in einer Notlage“

Unternehmen dürfen Daten über eine Person, die ihnen durch einen anderen Kunden mitgeteilt werden, nicht für eine werbliche Ansprache dieser Person verwenden.

Ein Beschwerdeführer hatte ein Schreiben eines kleinen Einzelunternehmens erhalten, das nach eigenen Angaben Personen Hilfe anbietet, die in sog. Schrottimmobilien investiert hatten. Das Unternehmen gab in seinem Anschreiben an, einen anderen Kunden beraten und dabei von diesem erfahren zu haben, dass sich auch sein Nachbar – der spätere Beschwerdeführer – in derselben Situation befand. Es bot an, ihn dabei zu unterstützen, mit dem Immobilienfonds Schriftverkehr zu führen und gemeinsam mit anderen Anlegern gegenüber der Geschäftsführung aufzutreten.

Der Beschwerdeführer wandte sich in seiner Beschwerde dagegen, dass das Unternehmen augenscheinlich seine Adressdaten und die Information über seine Immobilienbeteiligung erhoben und dazu verwendet hatte, ihn anzuschreiben und seine Dienste anzubieten. Im Rahmen unserer Prüfung teilte das Unternehmen mit, die Wohnanschrift anhand des Namens des Beschwerdeführers in einem Online-Telefonverzeichnis recherchiert zu haben. Dieses Vorgehen haben wir als datenschutzrechtlich unzulässig bewertet. Weder die Erhebung und Verwendung des Namens und der Information über die Immobilienbeteiligung noch das Recherchieren und Verwenden der Adressdaten des Beschwerdeführers lassen sich auf eine datenschutzrechtliche Rechtsgrundlage stützen, insbesondere auch nicht auf Artikel 6 Abs. 1 Buchst. f DS-GVO, da hier die schutzwürdigen Interessen des Betroffenen überwiegen. Die Daten wurden letztlich für werbliche Zwecke verwendet. Betroffene müssen es nicht hinnehmen, dass Unternehmen auf sie bezogene, von anderen Kunden erfahrene Daten dazu verwenden, diesen ihre Dienste anzubieten. Gleiches gilt für das Recherchieren und Verwenden von Adressdaten in einem Online-Telefonverzeichnis zu diesen Zwecken. Dass das Unternehmen vorliegend – wie es angab - nach eigenem Verständnis lediglich aus edlen Motiven heraus „geprellte Anleger“ unterstützen wollte und als Entgelt lediglich die Erstattung seiner Aufwendungen verlangte, führt zu keiner anderen Bewertung.

10

Internationaler Datenverkehr

10 Internationaler Datenverkehr

10.1 Binding Corporate Rules – ein Wachstumsmarkt

Der Trend zu Binding Corporate Rules (BCR) ist ungebrochen. Die Datenschutzaufsichtsbehörden sehen sich mit einer immer weiter steigenden Anzahl an BCR-Genehmigungsverfahren konfrontiert. Unser Haus war im Berichtszeitraum in zahlreichen dieser Genehmigungsverfahren involviert.

Eine stetig wachsende Anzahl an Unternehmensgruppen und Konzernen möchte Binding Corporate Rules als Grundlage für die konzerninternen Übermittlungen personenbezogener Daten einführen. Möglicherweise erhoffen sich Unternehmen davon mehr Rechtssicherheit für Datenübermittlungen in Drittländer verglichen mit dem Einsatz von Standarddatenschutzklauseln. Diese Hoffnung ist jedoch in dieser Pauschalität nicht berechtigt, da BCR gegenüber Standarddatenschutzklauseln keine geringeren Anforderungen mit Blick auf die Problematik von Datenzugriffe durch Behörden des Drittlandes stellen. Wie bei Standarddatenschutzklauseln müssen somit auch beim Einsatz von BCR Unternehmen mit Blick auf etwaige Datenzugriffe drittstaatlicher Behörden ggf. in Ergänzung zu den BCR zusätzliche Maßnahmen ergreifen, um Zugriffe, die nach EU-Recht nicht zulässig wären, auszuschließen.

Unser Haus war auch im Berichtszeitraum an vielen BCR-Genehmigungsverfahren beteiligt. Die DS-GVO sieht in Artikel 64 Abs. 1 Buchst. f vor, dass für jede BCR eine Stellungnahme des Europäischen Datenschutzausschusses einzuholen ist. Mithin sind spätestens im Europäischen Datenschutzausschuss bei jeder BCR die Aufsichtsbehörden aller EU- und EWR-Mitgliedstaaten zu befassen. Liegt die wichtigste deutsche Niederlassung des betreffenden Antragstellers in Bayern, ist nach derzeitiger Praxis unter den deutschen Aufsichtsbehörden demgemäß das BayLDA für diese Prüfung zuständig. Da Bayern wichtiger deutscher Standort vieler großer global agierender Unternehmensgruppen ist, ist das BayLDA entsprechend deutlich überproportional an BCR-Genehmigungsverfahren beteiligt.

Um das Verfahren effizient zu gestalten, haben die Aufsichtsbehörden vor das oben genannte Stellungnahmeverfahren im Europäischen Datenschutzausschuss ein informelles Verfahren zur koordinierten Prüfung von BCR-Genehmigungsanträgen geschaltet. Auf diese Weise wird erreicht, dass das förmliche, an enge Fristen gebundene Verfahren im Europäischen Datenschutzausschuss (EDSA) erst dann gestartet wird, wenn eine BCR nach Auffassung der Aufsichtsbehörden die gesetzlichen Anforderungen erfüllt und somit eine positive Stellungnahme des EDSA ergehen kann.

Unternehmen, deren BCR bereits vor Geltungsbeginn der DS-GVO durch die Aufsichtsbehörden genehmigt worden waren, mussten (und müssen, soweit noch nicht geschehen) ihre BCR an die DS-GVO anpassen. Die Aufsichtsbehörden haben in den Arbeitspapieren WP256 und WP257 den Anpassungsbedarf an die DS-GVO aufgezeigt. Die Arbeitspapiere sind abrufbar auf der Website des Europäischen Datenschutzausschusses:

https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines

Die Anpassungen an die DS-GVO müssen vom Unternehmen der jeweiligen federführenden Aufsichtsbehörde vorgelegt werden. Sie führen als solche nicht zur Notwendigkeit einer neuen Genehmigung, sofern sich durch sie keine signifikanten Änderungen beim durch die BCR gewährleisteten Schutzniveau ergeben (was bei

bloßen Anpassungen zur Abbildung des DS-GVO-Standards nicht der Fall ist). Unser Haus war auch noch im Berichtszeitraum mit der Prüfung mehrere derartiger Anpassungen befasst und war darüber hinaus sowohl als federführende Aufsichtsbehörde als auch als sonstige beteiligte Aufsichtsbehörde in die Prüfung zahlreicher neuer BCR im Rahmen des o. g. europäischen Genehmigungsverfahrens eingebunden.

10.2 Neue Standarddatenschutzklauseln für Übermittlungen in Drittländer veröffentlicht

Rund ein halbes Jahr nach der Vorstellung erster Entwürfe der EU-Kommission im Herbst 2020 wurden am 7. Juni 2021 die lange erwarteten neuen Standarddatenschutzklauseln der Europäischen Kommission für die Übermittlung personenbezogener Daten in Drittländer veröffentlicht. Die neuen Klauseln können ab dem 27. Juni 2021 verwendet werden. Datenübermittlungsverträge, die unter Verwendung der Vorgänger-Standardvertragsklauseln abgeschlossen worden sind, können bis zum 27. Dezember 2022 auf die neuen Klauseln umgestellt werden. Die neuen Standarddatenschutzklauseln entbinden Datenübermittler jedoch nicht von der Verpflichtung, das Schutzniveau im Drittland insbesondere mit Blick auf Datenzugriffsmöglichkeiten der Behörden im Drittland zu überprüfen.

Die Europäische Kommission hat Ende 2020 angekündigt, neue Standarddatenschutzklauseln gemäß Artikel 46 Abs. 2 Buchst. c DS-GVO für die Übermittlung personenbezogener Daten in Drittländer zur Verfügung zu stellen. Diese Klauseln wurden lange erwartet, weil die derzeit noch gültigen Standarddatenschutzklauseln aus den Jahren 2001 bis 2010 stammen und nicht alle Übermittlungskonstellationen abdecken. Insbesondere gab es bislang keine Standarddatenschutzklauseln für Übermittlungen durch in der EU niedergelassene Auftragsverarbeiter an Unterauftragsverarbeiter in Drittländer – gerade dieses Szenario findet sich in der Praxis aber überaus häufig und lässt sich gegenwärtig nur mittels umständlicher „Direktvertragskonstruktionen" als genehmigungsfreier Datentransfer realisieren (vgl. dazu unseren Tätigkeitsbericht 2017/2018, Ziffer 14.1).

Die Kommission hat nun jeweils Klauseln für folgende Übermittlungskonstellationen zur Verfügung gestellt:

- Übermittlung durch Verantwortlichen an Verantwortlichen (Controller-Controller)
- Übermittlung durch Verantwortlichen an Auftragsverarbeiter (Controller-Processor)
- Übermittlung durch Auftragsverarbeiter an (Unter-)Auftragsverarbeiter (Processor-Processor)
- Übermittlung durch Auftragsverarbeiter an Verantwortlichen (Processor-Controller)

All diese Übermittlungsszenarien kommen in der Praxis vor, sodass Bedarf an den jeweiligen Standarddatenschutzklauseln besteht. Die letztgenannte Konstellation mag etwas überraschen, ist aber dadurch bedingt, dass in der Konzeption der DS-GVO auch ein in der EU niedergelassener Auftragsverarbeiter, der etwa personenbezogene Daten in der EU im Auftrag seines Drittlands-Verantwortlichen erhebt und an letzteren übermittelt, eine „Übermittlung an ein Drittland" im Sinne des Kapitels V der DS-GVO vornimmt. Die Kommission hat für jeden der vier o. g. Fälle jeweils eigene, auf die entsprechenden datenschutzrechtlichen Rollen zugeschnittene Klauseln vorgeschlagen.

Der Europäische Datenschutzausschuss hatte im Vorfeld eine Stellungnahme zum Vorschlag der

Kommission veröffentlicht und an mehreren Stellen Änderungen angeregt. Das BayLDA war an den entsprechenden Arbeiten in den Gremien des Europäischen Datenschutzausschusses aktiv beteiligt. Unternehmen, die ihre laufenden Datentransfers in Drittländer auf die „alten" Standarddatenschutzklauseln stützen, haben bis zum 27.12.2022 Zeit, die Übermittlungen auf die neuen Klauseln umzustellen.

Die neuen Standarddatenschutzklauseln vermitteln im Übrigen – anders als mitunter erwartet – keine „einfache Lösung" für die vom Europäischen Gerichtshof im Rahmen der Schrems-II-Entscheidung (Rechtssache C-311/18, Urteil vom 16.07.2020) aufgezeigte Problematik möglicher Datenzugriffe von Behörden des Drittlands. Denn naturgemäß sind Behörden eines Drittlands nicht an die vertraglichen Vereinbarungen zwischen Datenexporteur und Datenimporteur gebunden. Auch bei Einsatz der neuen Standarddatenschutzklauseln bleibt der Datenexporteur daher verpflichtet, immer zu prüfen, ob Behörden des Drittlandes möglicherweise Zugriff auf die Daten in einem Umfang nehmen könnten, der über das nach EU-Recht akzeptable Maß hinausgeht und gegebenenfalls zusätzliche Garantiemaßnahmen zu ergreifen. Diese Prüfpflicht ist in den neuen Standarddatenschutzklauseln auch explizit so festgehalten.

Die Europäische Kommission hat angekündigt, zeitnah noch begleitende FAQs für die Anwendung der neuen Standarddatenschutzklauseln zu veröffentlichen.

10.3 Das Schrems-II-Urteil: Datenübermittlungen in Drittländer grundsätzlich nicht ohne Prüfung der Rechtslage im Empfängerland

Der Europäische Gerichtshof (EuGH) hat einmal mehr die hohen Hürden für die Übermittlung personenbezogener Daten in Nicht-EU-Länder („Drittländer") betont. Wer personenbezogene Daten z. B. „in die Cloud" an Dienstleister in Drittländer übermittelt, muss vorher prüfen, ob die Daten dort einen gleichwertigen Schutz genießen wie innerhalb der Europäischen Union.

Mit dem sog. Schrems-II-Urteil vom 16.07.2020 ("Schrems II") hat der EuGH die erhöhten Prüfpflichten betont, denen Datenexporteure unterliegen, die personenbezogene Daten in Drittländer übermitteln möchten. Datenexporteure müssen prüfen, ob der Datenempfänger aufgrund der auf ihn anwendbaren Rechtsvorschriften des Drittlands daran gehindert sein könnte, seine im vereinbarten Übermittlungsinstrument (z. B. Standarddatenschutzklauseln) übernommenen Verpflichtungen zum Schutz der Daten einzuhalten. Letzteres kann vor allem dann der Fall sein, wenn Behörden im Drittland Zugriff auf die Daten in einem Umfang nehmen könnten, der das nach EU-Recht akzeptable Maß übersteigt („problematische Datenzugriffe").

Es ist daher Aufgabe jedes Unternehmens und jeder sonstigen Stelle, die personenbezogene Daten an ein Drittland übermittelt - also jedes sog. Datenexporteurs - zu prüfen, welche Zugriffsmöglichkeiten für Behörden des Drittlandes aufgrund der dort bestehenden Gesetze und Praktiken bezogen auf die zu übermittelnden Daten bestehen können und inwieweit diese Zugriffe aus Sicht des europäischen Datenschutzrechts im o. g. Sinne problematisch sind.

Der Datenexporteur muss den Umfang und das Ergebnis dieser Prüfung dokumentieren und auf Verlangen der Datenschutzaufsichtsbehörde vorlegen. Es genügt mithin nicht, wenn Datenexporteur und Datenimporteur lediglich die Standarddatenschutzklauseln unterzeichnen und „in die Schublade legen" Der Europäische Datenschutzausschuss (EDSA) hat in seinem

Empfehlungspapier Nr. 1/2020 im Sinne eines Entscheidungsbaums aufgezeigt, welche Prüfschritte ein Datenexporteur absolvieren muss:

https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_en

Kommt der Datenexporteur bei dieser Prüfung zum Ergebnis, dass für die übermittelten Daten kein mit dem EU-Schutzniveau im Wesentlichen gleichwertiger Schutz gewährleistet werden kann – etwa weil „problematische Datenzugriffe" stattfinden könnten - darf er die Daten nicht übermitteln, es sei denn, er kann mit Hilfe so genannter zusätzlicher Maßnahmen doch noch den geforderten gleichwertigen Schutz erreichen. Beruht das Problem auf „problematischen Datenzugriffen" von Behörden im Drittland, muss der Datenexporteur daher nach Maßnahmen suchen, mit denen er ggf. solche Zugriffe verhindern kann - etwa Verschlüsselung; ggf. kann auch Pseudonymisierung eine Lösung bieten, sofern die „problematischen Zugriffe" nur pseudonymisierte Daten umfassen würden und die Behörden die pseudonymen Daten in keiner Weise einzelnen Personen zuordnen könnten.

Wir erwarten von Unternehmen und sonstigen Stellen, die personenbezogene Daten in Drittländer übermitteln, dass sie die o. g. Prüfung durchführen und dokumentieren. Bei uns ist bereits eine Reihe von Beschwerden zu Übermittlungen in Drittländer eingegangen, und wir sind verpflichtet, jeder dieser Beschwerden nachzugehen. Wir fordern dann vom Datenexporteur den Nachweis der Prüfung insbesondere der Zugriffsmöglichkeiten der Behörden im Drittland, und dass die Daten auch in Anbetracht dieser Zugriffsmöglichkeiten einen mit dem EU-Schutzniveau vergleichbaren Schutz genießen. Kann das Unternehmen dies nicht nachweisen, sind wir grundsätzlich verpflichtet, die Übermittlung zu untersagen – sofern das Unternehmen nicht von sich aus darauf verzichtet.

Der Europäische Datenschutzausschuss hat in seinem o. g. Empfehlungspapier einige typische Übermittlungsszenarien („Use Cases") mit Blick auf die hier skizzierten Anforderungen bewertet, darunter

- Übermittlung an Cloud-Dienstleister zwecks bloßer Speicherung (storage)
- Übermittlung pseudonymisierter Daten
- Übermittlung an Cloud Service Provider, der Zugriff auf Daten im Klartext benötigt
- Fernzugriff (remote access) aus einem Drittland, etwa für Wartung/Support

Unternehmen und sonstige Stellen, die personenbezogene Daten an Drittländer übermitteln möchten, sollten sich die im o. g. Papier des EDSA dargestellte datenschutzrechtliche Bewertung dieser Szenarien ansehen. Demnach gibt es viele sehr praxisrelevante Fälle, für die es in aller Regel nicht möglich ist, „problematische Zugriffe" zuverlässig auszuschließen. Dies gilt insbesondere, wenn die Daten beim Empfänger im Klartext benötigt werden, weil dies Voraussetzung für die Funktionalität des Dienstes ist; letzteres dürfte bei Software as a Service der Regelfall sein. Ähnlich dürfte es in aller Regel beim Remote-Access aus einem Drittland etwa für Supportzwecke sein.

Für viele Übermittlungen in Drittländer, an die sich Unternehmen in der EU in den letzten Jahren gewöhnt haben, wird es somit nicht gelingen, die datenschutzrechtlichen Anforderungen zu erfüllen. Viele Unternehmen werden aus diesem Grund beim Einsatz von Dienstleistern aus Drittländern erhebliche Umstellungen vornehmen müssen, um Daten ausschließlich in der EU zu speichern und darüber hinaus auch im Rahmen des Supports grundsätzlich ohne Übermittlungen in Drittländer auszukommen. Der Europäische Gerichtshof hat keine „Übergangsfrist" für die Geltung der o. g. Anforderungen gewährt und hat die Vollzugsverpflichtung der

Datenschutzaufsichtsbehörden betont. Wir erwarten von den betroffenen Unternehmen daher, ihre Übermittlungen in Drittländer einer Bestandsaufnahme zu unterziehen und dort, wo es angesichts des oben Gesagten notwendig ist, die notwendigen Umstellungen unverzüglich in die Wege zu leiten.

Das o. g. Empfehlungspapier des EDSA war Gegenstand einer öffentlichen Konsultation und wurde im Sommer 2021 in einer Endfassung verabschiedet. Die hier geschilderten Kernaussagen des Papiers beruhen jedoch unmittelbar auf dem Schrems-II-Urteil des Europäischen Gerichtshofs.

11

Beschäftigtendatenschutz

11 Beschäftigtendatenschutz

11.1 Aushang von Dienstplänen

Das Aushängen von Dienstplänen kann datenschutzrechtlich auch dann zulässig sein, wenn möglicherweise auch Beschäftigte Einblick nehmen können, bei denen keine sachliche Notwendigkeit für eine Kenntnisnahme vorliegt.

Uns erreichen immer wieder Anfragen von Unternehmen, aber auch von sozialen Einrichtungen dazu, ob und unter welchen Voraussetzungen und ggf. an welchem Ort Dienstpläne ausgehängt werden dürfen. Nach § 26 Abs.1 Satz 1 BDSG darf der Arbeitgeber Beschäftigtendaten u. a. dann verarbeiten, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. Eine Kenntnisnahme von ausgehängten Dienstplänen ist an sich nur durch diejenigen Beschäftigten notwendig, die direkt davon betroffen sind, also auf die Information angewiesen sind. Da es sich aber um Daten handelt, deren Schutzwürdigkeit nicht besonders hoch einzuschätzen ist, würden wir es als unschädlich ansehen, wenn gelegentlich Personal in den betreffenden Raum kommt, das nicht der dortigen Abteilung angehört. Dagegen wäre es unzulässig, wenn die Dienstpläne in Bereichen aufgehängt werden, zu denen Externe wie etwa Kundschaft oder Lieferanten oder auch in Krankenhäusern die Patientinnen und Patienten, in Alten- oder Pflegeheimen die Bewohnerinnen und Bewohner oder in Kitas die Eltern der Kinder vom Inhalt der Pläne Kenntnis nehmen können. Ebenso wäre es unzulässig, wenn die Dienstpläne auch die Abwesenheitsgründe enthalten würden, weil dann das schutzwürdige Interesse der betroffenen Beschäftigten zu stark beeinträchtigt wäre.

11.2 Datenschutzrechtlicher Auskunftsanspruch von (ehemaligen) Beschäftigten

Wenn Beschäftigte von ihren Arbeitgebern pauschal Auskunft über die zu ihrer Person gespeicherten Daten begehren, genügt es, wenn Arbeitgeber zunächst eine konkrete Auskunft zu den Personalstammdaten und im Übrigen zu den Kategorien verarbeiteter personenbezogener Daten erteilen. Für eine weitergehende Auskunft dürfen Arbeitgeber die Betroffenen bitten, ihren Anspruch zu präzisieren.

Uns erreichen immer wieder Anfragen und Beschwerden zu Auskunftsansprüchen gemäß Art. 15 DS-GVO von Beschäftigten, auch ehemaligen, gegenüber ihrem Arbeitgeber. Häufig begehren diese pauschal Auskunft über die zu ihrer Person im Unternehmen gespeicherten Daten.

Zunächst ist darauf hinzuweisen, dass der Arbeitgeber in jedem Fall innerhalb der Monatsfrist des Art. 12 Abs. 3 DS-GVO reagieren muss, also entweder die Auskunft erteilen oder eine Verlängerung um zwei weitere Monate ankündigen muss, wenn dies wegen der Komplexität oder der Anzahl von Anträgen erforderlich ist. Gar nicht zu reagieren wäre unzulässig.

Was den Inhalt und den Umfang der Auskunft betrifft, so halten wir in einem solchen Fall – angesichts der typischerweise größeren Anzahl unterschiedlicher vom Arbeitgeber durchgeführten Verarbeitungstätigkeiten und von verarbeiteten Daten der Beschäftigten - eine gestufte Vorgehensweise für gut vertretbar. Es reicht demnach grundsätzlich in einem ersten Schritt aus, wenn der Arbeitgeber zunächst die Personalstammdaten des die Auskunft Begehrenden

im Klartext beauskunftet, so dass der Beschäftigte erkennen kann, ob sie richtig sind und ggf. einen Berichtigungsanspruch geltend machen kann. Das betrifft also Name, Vorname, Geburtstag, Adresse und Geburtsort. Ansonsten genügt es zunächst, wenn Auskunft zu den Kategorien von personenbezogenen Daten, die zum Betroffenen gespeichert sind, sowie zu den anderen in Art.15 DS-GVO aufgeführten Aspekten erteilt wird.

Sollte die betroffene Person damit nicht zufrieden sein, müsste diese ihren Auskunftsanspruch gemäß Erwägungsgrund 63 Satz 7 dahingehend präzisieren, auf welche Informationen und/oder Verarbeitungstätigkeiten sich das Auskunftsersuchen bezieht. Erst nach dieser erfolgten Präzisierung ist dann der Arbeitgeber in der Pflicht, die entsprechenden Auskünfte mit konkreten Daten zu erteilen.

11.3 Corona-Tests von Beschäftigten

Im Berichtszeitraum bestand für Arbeitgeber – bis auf ganz wenige Ausnahmen – keine gesetzliche Pflicht zum Angebot von Corona-Tests für Beschäftigte. Für Arbeitgeber, die solche Tests mangels Rechtspflicht anbieten wollten, kommt als datenschutzrechtliche Rechtsgrundlage nur die Einwilligung der Beschäftigten in Betracht.

Die Corona-Pandemie hat zu einer Fülle datenschutzrechtlicher Fragen geführt. Ein Themenbereich betrifft Corona-Tests und andere Methoden zur Aufdeckung tatsächlicher oder vermeintlicher Verdachtsmomente auf eine Covid-Infektion bei Beschäftigten oder Kunden. Zum Zeitpunkt des Redaktionsschlusses haben einige Bundesländer eine Verpflichtung für Arbeitgeber eingeführt, Beschäftigten Schnelltests anzubieten bzw. für einzelne Beschäftigtengruppen sogar eine Testpflicht angeordnet. In Bayern bestand im Berichtszeitraum jedenfalls keine generelle Arbeitgeberpflicht zum Anbieten von Tests.

Einzelne Unternehmen in Bayern wollten bereits im Berichtszeitraum Mitarbeitern Tests anbieten, darunter eine größere Unternehmensgruppe mit Verantwortlichen in mehreren Bundesländern. Zu dem von der Unternehmensgruppe vorgelegten Konzept haben wir eine mit allen anderen für die gruppenangehörigen Unternehmen örtlich zuständigen Landesdatenschutzaufsichtsbehörden abgestimmte Bewertung abgegeben. Das Konzept sah die Durchführung von PCR-Tests (keine „Schnelltests“) vor, und gewollt war, dass bestimmte Funktionsträger in der Personalabteilung des jeweiligen Arbeitgebers über die Testergebnisse informiert werden, um bei positivem Ergebnis u. a. etwaige Kontaktpersonen der infizierten Person im Unternehmen zu identifizieren.

Die Testergebnisse stellen Gesundheitsdaten im Sinne von Art. 9 Abs. 1 DS-GVO dar. Als einzig tragfähige Rechtsgrundlage für die Verarbeitung dieser Daten kam nach Auffassung der beteiligten Aufsichtsbehörden die Einwilligung der betroffenen Beschäftigten (Art. 6 Abs. 1 Buchst. a in Verbindung mit Art. 9 Abs. 2 Buchst. a und mit § 26 Abs. 3 Satz 2 und Abs. 2 BDSG) in Betracht. Hingegen konnten – mangels einer im Berichtszeitraum in den betroffenen Bundesländern bestehenden arbeitgeberseitigen Pflicht zum Anbieten von Tests – Art. 9 Abs. 2 Buchst. b DS-GVO, § 26 Abs. 3 BDSG nicht als Grundlage der Verarbeitung dieser Gesundheitsdaten herangezogen werden. Nicht einschlägig waren ferner Art. 6 Abs. 1 Buchst. c DS-GVO mit Art. 9 Abs. 2 Buchst. i, § 22 Abs. 1 Nr. 1 Buchst. c, Abs. 2 BDSG; diese Vorschriften setzen eine Verarbeitung voraus, die „aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit“ erforderlich ist; hierfür müsste jedoch nach Art. 6 Abs. 2 und 3 DS-GVO eine Rechtsgrundlage bestehen, die ausreichend klar eine Aufgabe statuiert, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und damit eine Verarbeitung zu diesem Zweck

abzudecken vermag. Im Wesentlichen beziehen sich diese Vorschriften nach ihrem Wortlaut und ihrer Entstehungsgeschichte auf das öffentliche Gesundheitswesen und die Gesundheitsverwaltung. Eine allgemeine Befugnis von Unternehmen zur Verarbeitung von Gesundheitsdaten lässt sich jedoch auch den geltenden Rechtsvorschriften – auch denjenigen zur Pandemiebekämpfung – zum maßgeblichen Zeitraum der Bewertung des vorliegenden Testkonzepts nicht entnehmen.

Der Unternehmensgruppe haben wir daher die notwendigen Hinweise erteilt, um sicherzustellen, dass die datenschutzrechtlichen Anforderungen an eine Einwilligung zur Verarbeitung der Testergebnisse und somit von Gesundheitsdaten gewahrt sind. Insbesondere muss die Freiwilligkeit der Einwilligung und somit der Wahrnehmung des Testangebots gewahrt werden. Zu vermeiden ist daher jeglicher – auch nur mittelbarer – Druck, solche Tests durchzuführen. Ferner sind die Informationspflichten nach Art. 13 DS-GVO zu erfüllen, und die Beschäftigten sind nach Art. 7 Abs. 3 Satz 1 DS-GVO auf die Widerruflichkeit ihrer Einwilligungserklärungen hinzuweisen.

11.4 Zeiterfassung mittels Fingerabdruck

Arbeitszeiterfassung mittels Fingerabdruck im Beschäftigungsverhältnis ist unzulässig.

Ein Unternehmen beabsichtigte, bei sich die Arbeitszeiterfassung von Beschäftigten mittels Fingerabdruck einzuführen, und fragte bei unserer Behörde nach, ob dies zulässig sei. Nach § 26 Abs. 3 BDSG darf ein Arbeitgeber abweichend von Art. 9 Abs. 1 DS-GVO besondere Kategorien personenbezogener Daten seiner Beschäftigten für Zwecke des Beschäftigungsverhältnisses u. a. verarbeiten, wenn dies zur Ausübung einer sich aus dem Arbeitsrecht ergebenden Befugnis erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person am Ausschluss der Verarbeitung überwiegt.

Daktyloskopische Daten gehören gemäß Art. 4 Nr. 14 DS-GVO zu den biometrischen Daten und somit zu den besonderen Kategorien personenbezogener Daten im Sinne von Art. 9 DS-GVO, sofern sie, wie vorliegend, zum Zwecke der eindeutigen Identifizierung verarbeitet werden. Ihre Verarbeitung zum Zwecke der Arbeitszeiterfassung muss sich somit an § 26 Abs. 3 BDSG messen lassen.

Zwar ist der Arbeitgeber arbeitsrechtlich befugt zu kontrollieren, ob die Mitarbeiter die arbeitsvertraglich geschuldete Arbeitszeit erbringen. Allerdings ist es nicht erforderlich, dies mittels Fingerabdruck zu tun, weil es mit herkömmlichen Zeiterfassungssystemen eine geeignete Alternative der Zeiterfassung gibt, die ohne eine Verarbeitung von Daten besonderer Kategorien im Sinne von Art. 9 DS-GVO auskommt. Die Verwendung von Fingerabdruckdaten zu diesem Zweck ist daher nicht im Sinne von § 26 Abs. 3 BDSG erforderlich und damit datenschutzrechtlich unzulässig.

12

Gesundheit und Soziales

12 Gesundheit und Soziales

12.1 Nachweispflicht der Masernschutzimpfung

Im Rahmen der Nachweispflicht des Masernschutzes ist das Anfertigen von Kopien des Impfausweises oder eines Attestes unzulässig.

Die Pflicht zum Nachweis des Masernschutzes ergibt sich aus § 20 des Infektionsschutzgesetzes (IfSG). Danach müssen Betreute, die in einer sogenannten Gemeinschaftseinrichtung (Kindertageseinrichtungen und -horte, Kindertagespflege im Sinne von § 43 Sozialgesetzbuch VIII (SGB VIII), Schulen und sonstige Ausbildungseinrichtungen) aufgenommen werden sollen, und die in solchen Gemeinschaftseinrichtungen beschäftigten bzw. tätigen Personen, die jeweils nach dem 31. Dezember 1970 geboren wurden, seit dem 1. März 2020 einen ausreichenden Masernschutz nachweisen. Dazu ist ein Nachweis (Impfpass oder ärztliche Bescheinigung) über den vorhandenen Masernschutz vorzulegen. Der Nachweis ist durch den Verantwortlichen geeignet zu dokumentieren. Wird kein Nachweis vorgelegt oder ist ein Impfschutz erst zu einem späteren Zeitpunkt möglich bzw. kann er erst zu einem späteren Zeitpunkt vervollständigt werden, so hat die Leitung der jeweiligen Einrichtung unverzüglich das Gesundheitsamt darüber zu informieren. Dabei sind nach § 20 Abs. 9 Satz 4 IfSG personenbezogene Angaben zu übermitteln. Auch eine Befreiung von der Impfpflicht ist nachzuweisen.

Werden einer Schule Nachweise zum Masernschutz vorgelegt, werden diese lediglich geprüft. Nach erfolgter Prüfung werden die Nachweise nicht gespeichert. Es erfolgt nur eine Dokumentation darüber. Rechtsgrundlage für die Datenverarbeitung ist § 2 Nr. 16, § 20 Abs. 8 bis 10, 13 IfSG.

12.2 Videosprechstunde beim Arzt

Durch zertifizierte Videodienstanbieter ist es möglich, digitale ärztliche Sprechstunden wahrzunehmen.

Grundlegendes Erfordernis für die Zulässigkeit einer Videosprechstunde ist die Einwilligung der Patientin bzw. des Patienten. Sofern diese vorliegt, kann eine Videosprechstunde stattfinden.

Dafür sollten Räumlichkeiten von der Ärztin bzw. dem Arzt gewählt werden, die Privatsphäre bieten. Auch eine digitale Sprechstunde hat vertraulich und störungsfrei stattzufinden. Die Verarbeitung der personenbezogenen Daten hat hier grundsätzlich entsprechend den Vorgaben der DS-GVO, des BDSG sowie des Fünften Sozialgesetzbuchs (SGB V) und – soweit anwendbar – des SGB X zu erfolgen.

Der Videodienstanbieter muss gemäß Anlage 31b des Bundesmantelvertrags-Ärzte (BMV-Ä) zur IT-Sicherheit und zum Datenschutz zertifiziert sein sowie die Anforderungen zu den Inhalten erfüllen. Über die Zertifizierung und die Erfüllung der Anforderungen muss er eine Bescheinigung gemäß § 5 Absatz 2 der Anlage 31b zum BMV-Ä bei der Kassenärztlichen Bundesvereinigung (KBV) sowie beim GKV-Spitzenverband einreichen (siehe Anlage 2 der Anlage 31b zum BMV-Ä).

https://www.kbv.de/media/sp/Anlage_31b_Videosprechstunde.pdf

Daneben müssen Videodienstanbieter u. a. gewährleisten, dass die Videosprechstunde während der gesamten Übertragung Ende-zu-Ende verschlüsselt ist und keine Werbung geschalten wird. Für die Wahl der Serverstandorts weisen wir insoweit auf § 2a Absatz 3 der Anlage 31b zum BMV-Ä hin, wonach dieser sich nur in sehr eingeschränkten Voraussetzungen in einem Drittland befinden darf.

12.3 Glaubhaftmachung eines Befreiungsgrundes von der „Maskenpflicht“

Personen können aufgrund einer Behinderung oder aus gesundheitlichen Gründen von der Pflicht zum Tragen einer Mund-Nasen-Bedeckung (Maskenpflicht) befreit sein. Die Glaubhaftmachung der Befreiung erfolgt ausschließlich gegenüber den für den Vollzug des Infektionsschutzrechts zuständigen Behörden. Hierbei ergeben sich Unterschiede zur Glaubhaftmachung zwischen dem privaten und schulischen Bereich.

Bereits im Berichtszeitraum erreichten uns zahlreiche Eingaben zur Befreiung von der Maskenpflicht.

Von der Maskenpflicht sind Personen nach der Bayerischen Infektionsschutzmaßnahmenverordnung befreit, sofern sie glaubhaft machen können, dass ihnen das Tragen einer Mund-Nasen-Bedeckung aufgrund einer Behinderung oder aus gesundheitlichen Gründen unmöglich oder unzumutbar ist. Dabei verlangt eine Glaubhaftmachung zwar mehr als eine Behauptung, jedoch keinen Vollbeweis. Die Glaubhaftmachung erfolgt bei gesundheitlichen Gründen insbesondere durch eine ärztliche Bescheinigung.

Streitgegenstand war hier zum einen immer wieder, wer die ärztliche Bescheinigung aufgrund welcher Rechtsgrundlage einsehen darf, zum anderen Fragen der dafür erforderliche Inhalt der Bescheinigung. Die Bayerische Infektionsschutzmaßnahmenverordnung hat hier die inhaltlichen Anforderungen bis zum Redaktionsschluss dieses Tätigkeitsberichts immer wieder verändert. Unser ständiger Appell nach datenschutzfreundlichem Regelungsinhalt, gemeinsam mit dem Bayerischen Landesbeauftragten für den Datenschutz und dem Beauftragten für die Belange von Menschen mit Behinderung, wurde schließlich in der 13. Infektionsschutzmaßnahmenverordnung aufgenommen. Darin wurde u. a. auf das Erfordernis der Nennung einer Diagnose wieder verzichtet.

Die Verpflichtung zur Glaubhaftmachung über eine Befreiung von der Maskenpflicht gilt ausschließlich gegenüber den für den Vollzug des Infektionsschutzrechts zuständigen Behörden (siehe nunmehr BayVGH, Beschluss vom 01.02.2021, Aktenzeichen 20 NE 21.172, Rn. 4). Demzufolge haben beispielsweise Betreiberinnen und Betreiber von Einrichtungen, in denen für Kundschaft bzw. Gäste eine (ggf. FFP2-)Maskenpflicht gilt, diesen gegenüber die Maskenpflicht weder durchzusetzen noch etwaige Verstöße zu sanktionieren. Sofern z. B. ein Betreiber eines Ladengeschäfts dennoch von seinen Kundinnen und Kunden einen Nachweis oder die Glaubhaftmachung eines Befreiungstatbestands verlangt bzw. den Zugang zum Laden davon abhängig machen sollte, so wäre die Berechtigung, wie der BayVGH feststellt, hierzu allein im Rahmen einer zivilrechtlichen Auseinandersetzung zwischen Ladeninhaberin oder -inhaber und Kunden zu klären.

Mit Blick auf den Grundsatz der Datenminimierung ist darauf zu achten, dass eine so gering wie möglich gehaltene Personenzahl (in der Regel nur eine Mitarbeiterin bzw. ein Mitarbeiter) in die Überprüfung der Maskenbefreiung eingebunden sein sollte. Auch ist daran zu denken, dass die damit befassten Personen hier besonders zur Verschwiegenheit verpflichtet werden müssen. Eine Kopie der ärztlichen Bescheinigung darf im Rahmen der Überprüfung nicht angefertigt werden.

Im schulischen Bereich gibt es dagegen für eine solche Dokumentation und Aufbewahrung eine gesonderte Rechtsgrundlage gemäß der Bayerischen Schulordnung.

Aktuelle Hinweise finden Sie unter Maskenpflicht (Befreiung), siehe

https://www.lda.bayern.de/media/veroeffentlichungen/20210628_Befreiung_MNB.pdf

12.4 Anwendbarkeit der für öffentliche Schulen geltenden datenschutzrechtlichen Regelungen auf private Schulen

Auf die unserer Zuständigkeit unterfallenden privaten Schulen können die für öffentliche Schulen geltenden datenschutzrechtlichen Regelungen großteils ebenfalls angewandt werden.

Da sich unsere sachliche Zuständigkeit auf nicht öffentliche Stellen beschränkt (Art. 18 Abs. 1 Satz 1 Bayerisches Datenschutzgesetz), dürfen wir uns im schulischen Bereich nur zu privaten, nicht-kirchlichen Schulen äußern. Bei der Bearbeitung entsprechender Eingaben stellt sich mitunter die Frage, inwieweit die für öffentlichen Schulen geltenden datenschutzrechtlichen Regelungen zur Anwendung kommen.

Das Bayerische Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG) differenziert insoweit zwischen Ersatz- und Ergänzungsschulen. Ersatzschulen entsprechen in ihren Bildungs- und Erziehungszielen den öffentlichen Schulen (Art. 91 BayEUG), Ergänzungsschulen sind alle privaten Schulen, die keine Ersatzschulen in diesem Sinne darstellen (Art. 102 Abs. 1 BayEUG).

Für beide Schularten findet Art. 85 BayEUG Anwendung, der die Verarbeitung personenbezogener Daten regelt und damit die wesentlichen datenschutzrechtlichen Spezialnormen enthält (vgl. Art. 92 Abs. 5 Satz 1 bzw. Art. 102 Abs. 4 BayEUG). Für Ersatzschulen gelten darüber hinaus die Vorgaben der Bayerischen Schulordnung, die weitere datenschutzrechtliche Konkretisierungen enthält. Soweit den Ersatzschulen der Charakter einer öffentlichen Schule verliehen wurde, haben sie diese Schulordnung ohnehin vollumfänglich anzuwenden (Art. 101 Abs. 2 BayEUG, § 1 Satz 1 BaySchO). Für die übrigen Ersatzschulen gilt die BaySchO im Rahmen des Art. 92 Abs. 5 BayEUG (§ 1 Satz 2 BaySchO), der seinerseits auf den eben angesprochenen Art. 85 BayEUG verweist.).

12.5 Einsatz digitaler Werkzeuge im pandemiebedingten Distanzunterricht

Die Nutzung von digitalen Lernplattformen und Videokonferenzsystemen durch Schulen ist nur unter bestimmten Umständen ohne Einwilligung der Betroffenen zulässig.

Die Sars-CoV-2-Pandemie war mit massiven Auswirkungen auf den regulären Schulbetrieb verbunden, da die angeordneten Schulschließungen bzw. der Unterricht im Wechselmodell die Durchführung von Distanz-unterricht erforderlich machten. In diesem Zusammenhang erreichten uns auch verschiedene Eingaben betreffend den Einsatz digitaler Werkzeuge durch Schulen, insbesondere durch Nutzung von Videokonferenzsystemen und digitalen Lernplattformen.

Beim Einsatz derartiger Werkzeuge sind in jedem Fall datenschutzrechtliche Vorgaben zu beachten, da eine Verarbeitung personenbezogener Daten von Schülern und Lehrkräften stattfindet.

Nach Art. 85 Abs. 1 Satz 1 BayEUG dürfen Schulen die zur Erfüllung der ihnen durch Rechtsvorschriften zugewiesenen Aufgaben erforderlichen Daten verarbeiten. Art und Umfang des Einsatzes von Verfahren zur Verarbeitung personenbezogener Daten werden durch die auf Grundlage von Art. 89 Abs. 1 Satz 1, Satz 3 Nr. 10a BayEUG erlassene Bayerische Schulordnung

(BaySchO) festgelegt. § 46 Abs. 1 Satz 1 BaySchO verweist insoweit auf die in Anlage 2 zur BaySchO gemachten Vorgaben. Ergänzend stellt § 46 Abs. 1 Satz 3 BaySchO klar, dass insbesondere die Geltung der DS-GVO unberührt bleibt. Damit gilt insb. die Vorgabe des Art. 6 Abs. 1 Satz 1 DS-GVO zur Rechtmäßigkeit der Datenverarbeitung.

Soweit der Einsatz digitaler Werkzeuge den Vorgaben der genannten Anlage 2 zur BaySchO entspricht, ist die damit in Zusammenhang stehende Datenverarbeitung gesetzlich legitimiert und bedarf keiner Einwilligung. Hervorzuheben sind dabei die in den Abschnitten 4 und 7 getroffenen Vorgaben. Unter anderem muss die Freigabe des Videobildes jeweils freiwillig sein, es dürfen grundsätzlich keine besonderen Kategorien personenbezogener Daten verarbeitet und auch keine Aufzeichnungen gefertigt werden.

Werden personenbezogene Nutzerkonten erstellt, die eine Nutzung des jeweiligen Tools über den Distanzunterricht hinaus ermöglichen, bedarf die Datenverarbeitung einer wirksamen Einwilligung der Betroffenen bzw. ggf. der Erziehungsberechtigten. Dies gilt insbesondere für das Videokonferenztool Microsoft Teams for Education, welches vom Bayerischen Staatsministerium für Unterricht und Kultus den weiterführenden Schulen temporär zur Verfügung gestellt wurde. Um die insoweit maßgeblichen Vorgaben von Art. 4 Nr. 11, 7 DS-GVO zu erfüllen, müssen den Betroffenen für den Fall der Nichtabgabe oder des Widerrufs der Einwilligung Alternativangebote gemacht werden, bspw. durch die Zurverfügungstellung von Leihgeräten durch die Schule.

Mittlerweile wurde seitens des Bayerischen Staatsministeriums für Unterricht und Kultus mit Visavid eine für alle Schularten geltende, bayernweite Videokonferenzlösung zur Verfügung gestellt, die eine Datenverarbeitung ausschließlich in Rechenzentren innerhalb der Europäischen Union garantiert.

13

Vereine und Verbände

13 Vereine und Verbände

13.1 Segelflieger - Veröffentlichung von Flugdaten auf einer Internetplattform

Stellt ein Nutzer oder eine Nutzerin einer Internetplattform Daten über von ihm bzw. von ihr durchgeführte Sportflüge zur Verfügung und ist in den Nutzungsbedingungen die Veröffentlichung dieser Daten auf der Internetplattform vorgesehen, kann diese Person grundsätzlich nicht nachträglich deren Entfernung verlangen.

Eine in Bayern ansässige Internetplattform bietet Segelfliegern und anderen Akteuren aus Flugsportvereinen die Möglichkeit an, Daten zu von ihnen ausgeführten Flügen auf der Internetplattform zu veröffentlichen. Auf der Basis der übermittelten Flugdaten erstellt der Plattformbetreiber zudem diverse Auswertungen und Ranglisten, die ebenfalls veröffentlicht werden. Ein Beschwerdeführer verlangte vom Plattformbetreiber die Löschung der von ihm übermittelten Flugdaten von der Plattform, was der Verantwortliche unter Verweis auf ausdrückliche Regelungen seiner Nutzungsbedingungen verweigerte.

Nach unserer Bewertung stand dem Beschwerdeführer kein Löschungsanspruch zu. Die Veröffentlichung der Flugdaten war gemäß Nutzungsbedingungen ausdrücklicher Gegenstand des Nutzungsverhältnisses, das der Nutzer mit dem Plattformbetreiber einging. Datenschutzrechtlich ist damit die Veröffentlichung als „für die Erfüllung eines Vertrags erforderlich" anzusehen und nach Artikel 6 Abs. 1 Buchst. b DS-GVO zulässig. Auf die Erteilung einer Einwilligung nach Art. 6 Abs. 1 Buchst. a DS-GVO kam es daher nicht an. Es ist nicht zu übersehen, dass bei einer derartigen Gestaltung von Nutzungsverhältnissen die Gefahr besteht, dass Nutzende von Online-Diensten Schwierigkeiten haben, von ihnen bereitgestellte personenbezogene Daten von einer solchen Plattform wieder entfernen zu lassen. Daher ist gerade bei Online-Veröffentlichungen sorgfältig zu prüfen, ob die Verarbeitung im Einklang mit allen in Art. 5 DS-GVO geregelten Datenschutzgrundsätzen steht. Im konkreten Fall konnten wir keinen Grund für aufsichtliche Maßnahmen erkennen. Insbesondere war der Zweck der Verarbeitung bei Datenerhebung – die o. g. Veröffentlichung, einschließlich im Rahmen von Auswertungen – gemäß Art. 5 Abs. 1 Buchst. b DS-GVO festgelegt und gegenüber der betroffenen Person kommuniziert worden.

Im Ergebnis steht und fällt die Zulässigkeit der Veröffentlichung mit dem Nutzungsverhältnis, das als vertragliches Verhältnis im Sinne des Art. 6 Abs. 1 Buchst. b DS-GVO einzustufen ist. Inwieweit die Nutzungsbedingungen einer zivilrechtlichen Prüfung standhalten, kann jedoch nicht von uns als Datenschutzaufsichtsbehörde rechtsverbindlich entschieden werden, vielmehr liegt dies allein in der Zuständigkeit der ordentlichen Gerichte.

13.2 Veröffentlichung von Videoaufnahmen einer Veranstaltung eines Selbsthilfevereins im Internet

Bild- oder Videoaufnahmen einer Veranstaltung eines Selbsthilfevereins, in dem Personen mit einer bestimmten Krankheit organisiert sind, stellen eine Verarbeitung von Gesundheitsdaten dar. Deren Veröffentlichung im Internet ist daher an den hohen Hürden von Art. 9 DS-GVO zu messen.

Ein Selbsthilfeverein für Menschen mit einer bestimmten Krankheit fragte uns, ob er eine Vor-

tragsveranstaltung mit einem externen Referenten aufzeichnen und auf der Vereinshomepage veröffentlichen dürfe. Thema des Vortrags betraf die Krankheit, der die Tätigkeit des Vereins gewidmet war, und es stellte sich die Frage, ob im Rahmen der Aufzeichnung und Veröffentlichung auch die Teilnehmenden zusätzlich zum Vortragenden im Bild gezeigt werden durften.

Nach unserer Bewertung wäre in einem solchen Fall bereits die Anfertigung von Bild- oder Videoaufnahmen – und erst recht deren Veröffentlichung im Internet – nur auf Grundlage einer Einwilligung aller betroffenen Personen zulässig (Art. 6 Abs. 1 Buchst. a DS-GVO); zudem müsste die Einwilligung ausdrücklich erteilt werden und müsste sich auch auf Gesundheitsdaten beziehen (Art. 9 Abs. 1 Buchst. a DS-GVO). Letzteres ist deshalb der Fall, weil nicht ausgeschlossen werden kann, dass zumindest ein Teil der Teilnehmenden selbst von der in Rede stehenden Krankheit betroffen ist.

Zwar wird ein Betrachter der Aufzeichnungen bezogen auf den einzelnen Teilnehmenden nicht mit Sicherheit sagen können, ob dieser von der Krankheit betroffen ist. Jedoch muss berücksichtigt werden, dass die DS-GVO das Ziel verfolgt, ein hohes Datenschutzniveau zu gewährleisten. Vor dem Hintergrund dieses Gesetzeszwecks muss schon die Anwesenheit einer abgebildeten Person an einer solchen Vortragsveranstaltung so behandelt werden, als könnte die Person selbst von der Krankheit betroffen sein.

Die Aufzeichnung und Veröffentlichung der gewonnenen personenbezogenen Daten über die Besucher der Veranstaltung müssen daher in diesem Kontext als Gesundheitsdaten im Sinne von Art. 9 Abs. 1 DS-GVO behandelt werden. Schon die Herstellung von Bild- oder Videoaufnahmen, auf denen Teilnehmende der Veranstaltung zu sehen wären, würde daher eine Einwilligung des einzelnen Teilnehmenden im Sinne von Art. 6 Abs. 1 Buchst. a und von Art. 9 Abs. 1 DS-GVO erfordern.

14

Wohnungswirtschaft und Mieterdatenschutz

14 Wohnungswirtschaft und Mieterdatenschutz

14.1 Mitteilung von Rückständen bei der Hausgeldzahlung in der Eigentümergemeinschaft

Die Hausverwaltung darf alle Eigentümerinnen und Eigentümer innerhalb einer Eigentümergemeinschaft darüber informieren, inwieweit die einzelnen Eigentümer ihre Hausgeldzahlungspflichten erfüllt haben.

Zu diesem Thema haben wir uns bereits im Tätigkeitsbericht 2015/2016 geäußert. Jedoch erreichten uns dazu regelmäßig auch im Jahre 2020 wieder Beschwerden. Augenscheinlich empfinden es manche Eigentümerinnen und Eigentümer in der Eigentümergemeinschaft als Datenschutzverstoß, wenn die Hausverwaltung alle Eigentümer darüber informiert, inwieweit einzelne Eigentümer ihre Pflicht zur Zahlung von Hausgeld erfüllt haben. Vor diesem Hintergrund möchten wir erneut auf die im o. g. Tätigkeitsbericht dargestellte datenschutzrechtliche Rechtslage hinweisen.

Demgemäß darf die Hausverwaltung alle Eigentümerinnen und Eigentümer im Vorfeld der Eigentümerversammlung über den Stand der Begleichung der Hausgeldzahlungen durch die einzelnen Eigentümer informieren. Dies deshalb, weil die Eigentümer gemäß § 28 Abs. 5 WEG a. F. über die Abrechnung der Hausverwaltung beschließen müssen. Um dies in informierter Art und Weise tun zu können, müssen sie den Stand der Erfüllung der Hausgeldzahlungspflichten durch die einzelnen Eigentümer kennen, da die Beschlussfassung über die Abrechnung auch diese Zahlungen umfasst. Die Mitteilung des Stands der Erfüllung der Hausgeldzahlungen an alle Eigentümer ist daher datenschutzrechtlich nach Art. 6 Abs. 1 Buchst. b DS-GVO zulässig, weil sie als zur Durchführung des Verwaltervertrags erforderlich anzusehen ist.

Im Übrigen ist alleine die Eigentümergemeinschaft befugt, im Falle von Hausgeldrückständen den säumigen Eigentümer zu verklagen (vgl. BGH, Urt. v. 10.02.2017 – V ZR 166/16), was zumindest in der Regel einen entsprechenden Beschluss der Eigentümergemeinschaft voraussetzt. Auch aus diesem Grunde muss der Verwalter alle Eigentümer über den Stand der Hausgeldzahlungen aller Eigentümer informieren und die Verarbeitung auch aus diesem Grund nach Art. 6 Abs. 1 Buchst. b DS-GVO zulässig ist.

14.2 Umgang mit Adressdaten bei Energieversorgern

Energieversorger müssen geeignete Prozesse implementieren, um Berichtigungsersuchen hinsichtlich unrichtiger personenbezogener Daten umzusetzen, und müssen laufend überprüfen, ob ihre Beschäftigten die Prozesse korrekt befolgen.

Strom- oder Gasversorger verfügen über große Bestände an Kundendaten. Entsprechend erreichten uns auch im Beschwerdezeitraum zahlreiche Beschwerden gegen solche Unternehmen. Darin ging es meist darum, dass die Beschwerdeführenden als vermeintliche Anschlussinhaber zur Zahlung von Strom- bzw. Gasentgelt für Objekte herangezogen wurden, die jedoch in Wahrheit nicht von ihnen genutzt wurden. Im Rahmen unserer Ermittlungen stellte sich in einigen Fällen heraus, dass der Heranziehung ein unrichtiger Datenbestand beim Versorger zu Grunde lag. In mehreren von uns bearbeiteten Fällen hatten die betroffenen Personen im Vorfeld der Beschwerde bereits selbst Kontakt mit dem Energieversorger aufgenommen und Datenberichtigung verlangt, letztere wurde dann aber beim Versorger nicht oder nicht richtig umgesetzt, so dass die Betroffenen später doch wieder anhand des unrichtigen Da-

tenbestands als vermeintliche Schuldner herangezogen wurden. In den bearbeiteten Fällen konnten die Unternehmen jedoch belegen, dass intern sachgerechte Vorgaben zur korrekten Umsetzung von Datenberichtigungsersuchen implementiert sind, diese jedoch in den entsprechenden Einzelfällen nicht befolgt worden waren. Die Unternehmen müssen auch laufend stichprobenartig überprüfen, ob die zuständigen Beschäftigten Berichtigungsersuchen korrekt umsetzen.

In einigen anderen Beschwerdefällen war die Inanspruchnahme des Beschwerdeführenden durch den Versorger zulässig. Dies betraf häufig sog. Leerstands-Fälle. Hierbei geht es um Fälle, in denen nach Beendigung eines Lieferverhältnisses (etwa bei Auszug eines Mieters aus einer Mietwohnung) dem zuständigen Grundversorger nach § 36 des Gesetz über die Elektrizitäts- und Gasversorgung (EnWG) nicht bekannt ist, wer die Wohnung nutzt und wen er daher mit Strom oder Gas versorgt: Die Versorger müssen in solchen Fällen Recherchen betreiben, um den sog. Inhaber der tatsächlichen Verfügungsgewalt über die versorgte Wohnung zu ermitteln. Dies deshalb, weil kraft Gesetzes ein Grundversorgungsvertrag mit demjenigen zustande kommt, der Elektrizität bzw. Gas tatsächlich entnimmt (§ 2 Abs. 2 Stromgrundversorgungsverordnung (StromGVV) bzw. Gasgrundversorgungsverordnung (GasGVV)): Die Versorger treten dann häufig an den Immobilieneigentümer heran, um zu ermitteln, wer die Wohnung nutzt – etwa ein Mieter oder der Eigentümer selbst. Die Verwendung der Adressdaten des Eigentümers durch den Versorger zum Zweck dieser Ermittlungen ist schon deshalb zulässig, weil für den Fall, dass Gas/Strom entnommen wird und die Wohnung nicht vermietet ist, der Versorgungsvertrag nach oben Gesagtem mit dem Eigentümer zustande kommt. Ist die Wohnung vermietet, so ist die auf diese Weise erfolgende Erhebung der Identitäts- und Kontaktdaten des Mieters beim Wohnungseigentümer gemäß Art. 6 Abs. 1 Buchst. b DS-GVO zulässig, weil dann der Versorgungsvertrag wie dargestellt mit dem Mieter zustande kommt.

14.3 Überwachung der Wasserentnahme in einer Eigentümergemeinschaft

In Ausnahmefällen kann die zählergenaue Auswertung der Wasserentnahme an den Entnahmestellen eines Mehrfamilienhauses zulässig sein, wenn dies erforderlich ist, um die Erfolgsaussichten einer kostenintensiven Dekontamination zwecks Legionellenbekämpfung deutlich zu verbessern.

Ein Eigentümer beschwerte sich darüber, dass seine Eigentümergemeinschaft per Beschluss festgelegt hatte, dass die Verbrauchsdaten aller einzelnen verbauten Funkwasserzähler in der Eigentümergemeinschaft durch die Hausverwaltung in einem Vierzehn-Tage-Turnus abgerufen werden können. Hierdurch fühlte sich der Beschwerdeführer in unverhältnismäßigem Umfang überwacht. Diese in der Tat ungewöhnliche Maßnahme stellte sich im Rahmen unserer Ermittlungen aus unserer Sicht im konkreten Einzelfall als datenschutzrechtlich vertretbar heraus. Hintergrund der beschlossenen „zählerscharfen Überwachung" der Wasserverbräuche war ein hartnäckiger Legionellenbefall der Trinkwasseranlage der Immobilie. Zahlreiche andere Maßnahmen, die seitens der Eigentümergemeinschaft im Vorfeld ergriffen worden waren, hatten den Legionellenbefall nicht reduzieren können. Daher hatte die Eigentümerversammlung nach fachkundiger Beratung zuletzt eine Maßnahme der Dekontaminierung aller Wasserleitungen mit Natriumhypochlorit für die Dauer von sechs Monaten beschlossen. Von Fachseite war darauf hingewiesen worden, dass während der gesamten Dauer der – recht kostspieligen – Dekontaminierung regelmäßig an allen Verbrauchsstellen (etwa: allen Wasserhähnen) Wasser entnommen werden müsse, um so für eine ausreichende Durchspülung aller Teile

der Trinkwasseranlage zu sorgen, da sonst der Erfolg der Dekontaminationsmaßnahme gefährdet sei. Dies war Grund für die Eigentümergemeinschaft, die Hausverwaltung zu ermächtigen, im 14-Tage-Turnus die Wasserverbräuche aller verbauten Wasserzähler zu kontrollieren, um so zu überprüfen, ob an einzelnen Entnahmestellen sehr wenig oder gar kein Wasser entnommen wird und ggf. reagieren zu können.

Unter diesen besonderen Umständen haben wir die beschriebene „zählerscharfe" Überwachung des Wasserverbrauchs während eines auf sechs Monate begrenzten Zeitraums als datenschutzrechtlich vertretbar erachtet. Maßgeblich hierfür war insbesondere, dass andere erfolgversprechende Maßnahmen nicht mehr erkennbar waren, und dass die Dekontaminationsmaßnahme mit erheblichen Kosten für die Eigentümergemeinschaft verbunden war, so dass die Eigentümergemeinschaft ein ganz erhebliches Interesse an ihrem Gelingen hatte.

14.4 Weitergabe von Kontaktdaten eines Mieters durch Vermieter an Handwerker

Vermieter dürfen die Telefonnummer von Mietern an Handwerker auch ohne Einwilligung weitergeben, wenn dies zum Zweck der Vereinbarung eines Termins für eine Reparatur erforderlich ist.

Regelmäßig erreichen uns Beschwerden von Mietern darüber, dass Vermieter ihre Telefonnummer (seltener: E-Mail-Adresse) an einen Handwerker weitergegeben haben, damit letzterer mit dem Mieter Kontakt aufnehmen kann, um einen Termin wegen einer in der Mietwohnung durchzuführenden Reparatur zu vereinbaren.

Eine solche Datenweitergabe ist zumindest in der Regel auch ohne Einwilligung des Mieters aufgrund von Artikel 6 Abs. 1 Buchst. f DS-GVO zulässig, weil es einem berechtigten Interesse des Vermieters entspricht, dass der Handwerker zwecks Vereinbarung eines Reparaturtermins mit dem Mieter Kontakt aufnimmt. Zwar wäre es auch denkbar, dass der Handwerker ausschließlich gegenüber dem Vermieter einen oder mehrere aus seiner Sicht passende Termine nennt, und der Vermieter diese mit dem Mieter abzustimmen versucht und dann dem Handwerker entsprechende Rückmeldung gibt. Erfahrungsgemäß ist es aber oft nicht ganz einfach, Termine abzustimmen, ohne direkt miteinander in Kontakt zu sein. Daher ist es aus unserer Sicht grundsätzlich legitim, wenn der Vermieter durch Weitergabe der Telefonnummer an den Vermieter die direkte Kontaktaufnahme ermöglicht.

Schutzwürdige Interessen des Mieters stehen jedenfalls im Regelfall der Weitergabe nicht entgegen; in außergewöhnlich gelagerten Fällen steht dem Mieter ein Widerspruchsrecht nach Art. 21 Abs. 1 DS-GVO gegen die Weitergabe zu, und hierüber muss der Vermieter den Mieter gemäß Art. 21 Abs. 4 DS-GVO informieren – idealerweise bereits bei Abschluss des Mietvertrags. Hieran scheint es nach unseren Erfahrungen in der Praxis oft zu fehlen, was dann immer wieder - auch im Berichtszeitraum - zu Beschwerden bei uns führt.

15

Videoüberwachung

15 Videoüberwachung

15.1 Fotografien von Kfz-Kennzeichen von Falschparkenden durch Privatpersonen

Privatpersonen dürfen nicht ohne vorliegendes berechtigtes Interesse nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO Fotografien von Kfz-Kennzeichen an Behörden weitergeben.

Privatpersonen fertigen häufig Fotografien von falsch parkenden Fahrzeugen und deren Kfz-Kennzeichen an, etwa auf Fahrradwegen oder in Einfahrten, und leiten diese an Polizei und Ordnungsämter weiter. Dies ist unzulässig, sofern kein berechtigtes Interesse gem. Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO vorliegt.

Die Motivation der Verantwortlichen bestand hier darin, Ordnungswidrigkeiten zur Anzeige zu bringen und diese mittels eigenen Fotografien zu beweisen. Übergeordnetes Ziel war es dabei, für die Einhaltung der Gesetze zum Wohle der öffentlichen Sicherheit und Ordnung zu sorgen. Eine individuelle Betroffenheit der Einzelnen, beispielsweise durch eine individuelle Behinderung durch die parkenden Fahrzeuge oder die Geltendmachung möglicher Schadensersatzansprüche auf dem Zivilrechtsweg, lag dagegen häufig nicht vor.

Vor dem Hintergrund des staatlichen Strafverfolgungsmonopols besteht für das systematische Anfertigen von Fotoaufnahmen, die allein darauf gerichtet sind, Beweismaterial zur Verfolgung von Straßenverkehrsordnungswidrigkeiten zu liefern, kein überwiegendes, die Datenverarbeitung erforderndes Interesse des Einzelnen.

Berechtigtes Eigeninteresse einer betroffenen Person kann dann vorliegen, wenn etwa eine eigene Einfahrt zugeparkt ist, also eine privatrechtliche Besitzstörung vorliegt. Ausschlaggebend ist eine eigene Betroffenheit.

Auch berechtigte Drittinteressen mussten regelmäßig verneint werden. In Abgrenzung zu Art. 6 Abs. 1 Buchst. e DS-GVO können lediglich Individualinteressen privater Dritter und keine Allgemeininteressen Berücksichtigung finden. Ein anderes Verständnis der Rechtsgrundlage würde es dem Verantwortlichen entgegen der Systematik des Art. 6 Abs. 1 DS-GVO ermöglichen, sich zum selbsternannten Sachwalter von Allgemeininteressen im Einzelfall auf die Wahrnehmung von eigentlich staatlich zu schützenden Rechten und Interessen zu berufen.

Als berechtigtes Interesse eines privaten Dritten wird beispielsweise angesehen, eine persönliche Information über eine Person zu erlangen, die sein Eigentum verletzt hat, um gegen sie eine Schadensersatzklage zu erheben. Dabei wird gefordert, dass der Dritte zumindest Kenntnis von den verarbeiteten Daten und deren Inhalt erlangen sollte. Dies ist nur möglich, wenn der Dritte vom Verantwortlichen identifizierbar ist und eine Art Beziehung, zumindest ein Bekanntheitsverhältnis, zum Dritten besteht. Zudem muss auch ein Wille des Dritten an der Datenverarbeitung erkennbar sein. Eine aufgedrängte Datenerhebung für einen Dritten, möglicherweise völlig ohne dessen Wissen um die Datenerhebung, kann schon aufgrund der nachfolgenden Pflichten nicht durch eine Interessenabwägung legitimiert werden. Ist der Wille eines Dritten nicht geäußert oder nicht erkennbar, kann eine Datenverarbeitung für diesen nicht unter den Zulässigkeitstatbestand des berechtigten Interesses fallen.

15.2 Videoüberwachung in Fitnessstudios

Videoüberwachung von Trainingsflächen in Fitnessstudios kann nicht auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO gestützt werden und ist daher unzulässig.

Uns wurden vermehrt Fragen zur Zulässigkeit von Videoüberwachung in Fitnessstudios vorgelegt. Dabei ist Videoüberwachung in Fitnessstudios nicht generell unzulässig. Vielmehr muss zwischen den verschiedenen Bereichen unterschieden werden. Die Überwachung der Trainingsflächen mittels Kameratechnik kann jedoch nicht auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO gestützt werden und ist daher unzulässig.

Die Verantwortlichen gaben eine Reihe an Interessen an, die mit der Videoüberwachung der Studios verfolgt werden sollten. Die Zwecke der Videoüberwachung der Trainingsflächen sollten danach die Folgenden sein: Sicherheit der Kunden (Diebstähle, Übergriffe), Diebstahlsprävention sowie Ermittlung eines Schadenshergangs.

Eine Videoüberwachung der Trainingsflächen ist zur Erreichung der angegebenen Zwecke schon nicht erforderlich, vielmehr überwiegen die Betroffeneninteressen.

Erforderlichkeit ist nur dann gegeben, wenn die berechtigten Interessen mit weniger intensiver Datenverarbeitung nicht in etwa gleichem Maße erreicht werden können. Es bestanden jedoch nach unserer Ansicht zahlreiche Möglichkeiten, diese Zwecke zu erreichen, ohne dass eine Videoüberwachung der Trainingsflächen notwendig wäre. Für die Sicherheit der Kundinnen und Kunden vor Diebstahl kann durch die Zurverfügungstellung von abschließbaren Spinden und Schließfächern gesorgt werden. Für deren Sicherheit vor Übergriffen kann durch Einsatz von Personal gesorgt werden. Diese können sich weiterhin an das Personal an der Empfangstheke wenden. Notfalls muss diese so positioniert werden, dass der Trainingsbereich überblickt werden kann oder die betreffenden Mitarbeiterinnen und Mitarbeiter müssen sich durch mehrmalige Rundgänge durch das Studio einen Überblick verschaffen. Diebstähle am Inventar des Studios müssen anderweitig, etwa durch Diebstahlssicherungen wie in Kaufhäusern oder durch Blickkontrolle am Ausgang verhindert werden. Ein Fitnessstudio besteht typischerweise nicht aus vielen kleinteiligen Elementen, die einfach gestohlen werden können. Diebstähle können hier vielmehr durch organisatorische Maßnahmen verhindert werden. Für den Fall, dass Schäden an Trainingsgegenständen oder der Studioeinrichtung entstehen, muss auf die im Zivilrecht übliche Beweislastverteilung zurückgegriffen werden. Etwa besteht die Möglichkeit der Zeugenaussagen. Für nicht aufklärbare Fälle kann sich das Studio versichern lassen oder dies als finanzielles Risiko hinnehmen.

Zudem überwogen bei der Videoüberwachung der Trainingsfläche die schutzwürdigen Interessen der Betroffenen. Für die Betroffenen gibt es keine Ausweichmöglichkeiten, denn wer die überwachte Trainingsfläche betritt, hält sich stets im Erfassungsbereich der Kameras auf. Insofern entsteht ein permanenter flächendeckender Überwachungsdruck, dem sich die Besucher des Fitnessstudios nicht entziehen können. Es besteht die Gefahr eines Gefühls der Unsicherheit der Betroffenen. Denn eine permanente Beobachtung ist geeignet, das Verhalten der Betroffenen zu beeinflussen. Damit einher geht möglicherweise der Verlust der Unbefangenheit und auch ein gewisser Anpassungsdruck ist nicht auszuschließen. Besonders ins Gewicht fällt, dass sich die Betroffenen auf der Trainingsfläche nicht nur kurz, sondern über einen längeren Zeitraum aufhalten.

15.3 Videoüberwachung von Privatpersonen

Videoüberwachung außerhalb des eigenen Grundstücks ist in aller Regel unzulässig.

Uns erreichen weiterhin eine erhöhte Anzahl von Beschwerden von Anwohnern, Passanten aber auch von Ordnungsbehörden, welche sich über an Privatgebäuden montierten Videokameras (welche oftmals so ausgerichtet sind, dass damit vermeintlich oder auch tatsächlich Bereiche außerhalb des Grundstücks des Kamerabetreibers überwacht werden) beschweren bzw. uns mitteilen, dass Bereiche außerhalb des eigenen Grundstücks überwacht werden.

Hierzu weisen wir darauf hin, dass eine Videoüberwachung durch Privatpersonen nur zulässig ist, soweit sie zur Wahrung der berechtigten Interessen des Kamerabetreibers erforderlich ist und, sofern nicht die Rechte der betroffenen Personen überwiegen (Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO).

Dies bedeutet, dass die Überwachung eines eigenen Grundstücks datenschutzrechtlich zulässig ist, während dagegen eine Videoüberwachung angrenzender Grundstücke bzw. Straßen, Plätze oder Gehwege datenschutzrechtlich in aller Regel unzulässig ist. In engen Ausnahmefällen kann auf einem angrenzenden Streifen von etwa einem Meter hinter der Grundstücksgrenze gefilmt werden. Maßgeblich ist hier eine Abwägung im Einzelfall.

Als Zweck der Videoüberwachung jenseits des beschriebenen zulässigen Bereichs wird häufig angeführt, diese sei zum Schutz des auf öffentlichen Bereichen abgestellten Fahrzeugs oder zum Schutz vor Einbruch und Vandalismus an den Gebäuden erforderlich.

Ein Hausrecht in Bereichen außerhalb des eigenen Grundstücks besteht allerdings nicht. Eine Überwachung von solchen Bereichen ist auch zu präventiven Zwecken unzulässig.

Die Kameras sind daher so einzurichten, dass nur das eigene Grundstück, bzw. nur solche Bereiche überwacht werden, welche dem alleinigen Nutzungsrecht des Kamerabetreibers unterliegen. Ist dies nicht möglich, sind die Kameras abzumontieren.

Eine datenschutzrechtlich unzulässige Videoüberwachung stellt grundsätzlich eine Ordnungswidrigkeit dar und kann als solche nach Art. 83 Abs. 5 Buchst. a DS-GVO mit einem Bußgeld geahndet werden.

Da wir auch immer wieder Nachfragen zur Einrichtung von Kameras bzw. fehlerhafte Einschätzungen zum Betrieb von Überwachungskameras erhalten, nennen wir hier zusammenfassend, was erlaubt ist und was nicht:

- Die Kamera darf nur das eigene Grundstück filmen.
- Aufnahmen von Bereichen außerhalb des eigenen Grundstücks, wie z. B. Straßen und Gehwege, sind in der Regel nicht zulässig.
- Wer unrechtmäßig gefilmt wird, kann Unterlassung und Schadenersatz verlangen.
- Werden Bereiche im datenschutzrechtlich zulässigen Umfang außerhalb des eigenen Grundstücks überwacht, ist auf die Videoüberwachung auf Grundlage des Art. 13 DS-GVO hinzuweisen.

Wir verweisen hierzu auch auf unsere Homepage, wo wir weitere Informationen zu diesem Thema eingestellt haben:

www.lda.bayern.de/de/thema_videoueberwachung.html

16

Datenschutzverletzungen

16 Datenschutzverletzungen

Die Bearbeitung der Meldungen nach Art. 33 DS-GVO hat sich auf hohem Niveau eingependelt und beschäftigten nach wie vor fast unseren kompletten technischen Bereich.

Eine Sicherheitsverletzung nach DS-GVO umfasst nicht nur unbefugte oder ungewollte Übermittlungen oder Zugangsmöglichkeiten zu personenbezogenen Daten, sondern auch Störungen der Verfügbarkeit, die mit einer risikobehafteten Beeinträchtigung der betroffenen Person einhergeht.

Sobald eine Meldung bei uns eingeht, erfolgt eine strukturierte Bearbeitung nach folgendem Schema:

1. Schadensbegrenzung

   Kernfrage ist, ob die Ursache eines Vorfalls noch fortbesteht (z. B. Fehlkonfiguration eines Webservers oder Cyberattacke) und ein Eingreifen im Sinne einer beratenden Unterstützung oder gar aufsichtlicher Abhilfemaßnahmen von unserer Seite aus erforderlich ist. In den meisten der gemeldeten Fällen waren die „Datenpannen" aber Chefsache bei den Unternehmen und ursächliche Lücken, sofern machbar, entsprechend unverzüglich abgestellt worden.

2. Risikovalidierung

   Prüffrage ist, ob ein „Risiko" oder ein „hohes Risiko" vorliegt. Bei einem hohen Risiko müssen die Betroffenen nach Art. 34 DS-GVO über den Vorfall informiert werden.

3. Zukünftige Risikominimierung

   Im Sinne einer „Lesson Learned" schauen wir, ob ggf. weitere technische und organisatorische Maßnahmen getroffen werden können, um einen derartigen Vorfall möglichst in der Zukunft zu vermeiden. Aber: Einen hundertprozentigen Schutz vor Sicherheitsvorfällen gibt es auch im Datenschutz nicht immer, da insbesondere menschliche Fehlhandlungen zwar durch Schulungen reduziert, nie aber garantiert abgestellt werden können.

4. Formaler Abschluss oder weitere Ermittlungen

   Mit einem formalen Abschluss wird die Meldung nach Art. 33 DS-GVO abgeschlossen. In wenigen Fällen, insbesondere wenn die Aufarbeitung einer Sicherheitsverletzung schleppend oder kaum vorangeht, leiten wir zusätzliche aufsichtliche Ermittlungen mit Fragebögen und teils Vor-Ort-Kontrollen ein.

Die Art der Meldungen nach Art. 33 DS-GVO strukturieren wir nach folgenden Kategorien:

- Cyberattacken

  Kriminelle Angriffe über das Internet auf Firmennetzwerke, Webanwendungen oder mittels Social Engineering auf Mitarbeiter.

- Schadcode

  Schadcodevorfälle, die nicht verlässlich von einem Virenscanner unterbunden und durch die Zugang zu bspw. Dateien, E-Mails oder IT-Systemen erlangt wurde. Dazu gehört auch die Verschlüsselung mit dem Ziel der Erpressung, zu der wir einen neuen Trend beobachten (Kapitel 18.2).

- Fehlkonfiguration

  Meist Berechtigungsfehler, die zum Zugang zu personenbezogenen Daten wie bspw. interne Gehaltslisten oder über das Internet erreichbare Datenbankbackups führen. Ursache sind keine kriminelle Angriffe sondern meist menschliche Fehlhandlungen

- Diebstahl/Verlust

  Dokumente oder Datenträger mit personenbezogenen Daten kommen abhanden. Sofern nicht verschlüsselt, muss das Schadenspotential abgeschätzt und ggf. eine Meldung bei uns eingereicht werden.

- Fehlversendung

  Entweder Versand von (postalischen) Schreiben an falsche Empfänger oder fehlerhafte Kuvertierungen, bei denen mehrere Schreiben in einen Brief verpackt werden. Obwohl der Empfängerkreis bei der Schadens- und Eintrittswahrscheinlichkeit berücksichtigt werden kann, machen diese Art der Meldungen von der Anzahl her noch die größte Kategorie aus.

- Sonstige Informationsweitergabe

  Insbesondere die (verbale) Weitergabe von sensitiven Informationen wie bspw. Bankdaten bei Scheidungsverfahren fallen in diese Kategorie. Da dies meist Einzelfälle sind, werden Erstverstöße ohne Einleitung von weiteren Ermittlungsverfahren effizient abgeschlossen

- Buchungs-/Eingabefehler

  Meist sind dies Softwarefehler, die zu einer falschen Belastung von Bank-/Versicherungskonten führen. Da die finanziellen Schäden meist unverzüglich „geheilt" werden, sind Meldungen nach Art. 33 DS-GVO nur bei zusätzlichen Weitergabe von bspw. Überweisungsdaten erforderlich

- Sonstiges

  Alle weiteren Fälle, bei denen es zu einer unbefugten oder ungewollten Verarbeitung personenbezogener Daten kommt.

Wir gehen davon aus, dass die Bearbeitung der Sicherheitsverletzungen trotz bereits durchgeführter Optimierungen auch zukünftig weiterhin den Großteil unseres technischen Personals bindet. Dies mag zum einen daran liegen, dass insbesondere die kriminellen Angriffe zunehmend komplexer werden, andererseits aber auch daran, dass bei bayerischen Unternehmen die Integration der DS-GVO in den Unternehmensalltag meist gut umgesetzt wurde und Sicherheitsverletzungen auch als solche erkannt und gemeldet werden. Eine hohe Anzahl von Art.-33-Meldungen bedeuten deswegen nicht zwingend, dass das Datenschutzniveau in den Unternehmen nicht gut ist. Gerade die Rolle der betrieblichen Datenschutzbeauftragten kann hier nicht hoch genug gewürdigt werden, da diese häufig unsere ersten Ansprechpartner und Fachexperten bei der Vorfallbearbeitung in den betroffenen Unternehmen darstellen.

17

Technischer Datenschutz und Informationssicherheit

17 Technischer Datenschutz und Informationssicherheit

17.1 Windows 10 – Umgang mit Telemetriedaten

Laborprüfungen des BayLDA haben ergeben, dass die Übertragung von Telemetriedaten bei der Enterprise-Version von Windows 10 durch das Level „Security" unterbunden werden kann. Allerdings sind grundsätzliche Fragen offen, die einzuordnen sind.

Seit dem Release von Windows 10 im Jahr 2015 werden insbesondere die Datenflüsse eines Windows-10-Rechners an Microsoft regelmäßig diskutiert. Insbesondere bei den sogenannten Telemetriedaten stellte sich schon früh die Frage, welche Inhalte diese haben und ob eine Übermittlung an Microsoft überhaupt datenschutzkonform ist. Im TB 2019/20 wurde schon über eine Laborprüfung des BayLDA mit Vertretern der deutschen Aufsichts- und Sicherheitsbehörden und Beschäftigten von Microsoft berichtet:

https://www.lda.bayern.de/media/baylda_report_09.pdf

Im Nachgang des Treffens wurden weitere systematische Laborsimulationen durchgeführt, bei denen bestätigt wurde, dass bei Nutzung der Einstellung „Security" eine datenschutzrechtliche Übermittlung von Telemetriedaten unterbunden werden kann. Zeitgleich wurde in einem Kurztest des Bundesamts für Sicherheit in der Informationstechnik (BSI) und später einmal in einer erneuten Analyse des BayLDA ein Aufruf an „settings-win.data-microsoft.com" festgestellt. Dieser gehört zu einem Microsoft-Server, über den Einstellungsdaten für mehrere Windows-10-Komponenten, darunter auch die Telemetrie, von Seiten Microsofts parametrisiert werden können. Auch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat sich in einem Beschluss zu dem Aufruf an „settings-win.data-microsoft.com" positioniert und dargelegt, dass zur Unterbindung der Übermittlung personenbezogener Telemetriedaten neben dem Telemetrielevel „Security" mittels vertraglicher, technischer oder organisatorischer Maßnahmen sicherzustellen ist, dass nachweislich keine Übermittlung von Telemetriedaten an Microsoft stattfindet:

https://www.datenschutzkonferenz-online.de/media/dskb/TOP_30_Beschluss_Windows_10_mit_Anlagen.pdf

Um die Fragestellung des settings-Aufrufes zu erhellen, wurde eine Erweiterung der Analysemöglichkeiten im IT-Labor des BayLDA umgesetzt, mit der festgestellt werden kann, von welchem Windows-Prozess ein Aufruf an den „settings-win.data-microsoft.com" durchgeführt wird. So konnte unter erneut durchgeführten Laboranalysen und Einsatz des Pakets „Restricted Functionality Baseline" von Microsoft weiterhin bestätigt werden, dass bei der Einstellung des Telemetrielevels „Security" keine datenschutzrechtlichen Übermittlungen an die zur Telemetriefunktion von Microsoft gehörenden Server stattfinden. Ein im selben Laborsetup einzelner ausgelöster Aufruf an „settings-win.data-microsoft.com" konnte des Weiteren einem Windows-Prozess zugeordnet werden, der nicht im Zusammenhang mit der Telemetriefunktion stand.

Vom Ergebnis bedeutet dies für bayerische Verantwortliche aus dem nicht-öffentlichen Bereich, dass nach jetzigem Kenntnisstand eine Unterbindung der Telemetriefunktion bei der Enterprise-Edition mittels Konfiguration des Telemetrielevels „Security" als wirksam angesehen wird und keine weiteren Maßnahmen wie bspw. die Trennung von Windows-10-Arbeitsplatzrechnern vom Internet als erforderliche technische Maßnahme notwendig ist. Die Reduktion der Datenflüsse durch einen wohlüberlegten

und ggf. angepassten Einsatz des Pakets „Restricted Functionality Baseline“ wird zusätzlich als Maßnahme für die Stellen empfohlen, die sich einen stabilen IT-Betrieb ohne Telemetrieunterstützung von Microsoft zutrauen.

Anzumerken ist, dass eine Unterbindung der Telemetriefunktion nicht zwingend gefordert wird – es muss nur dann wie bei anderen Datenübermittlungen die Rechtmäßigkeit der Datenübermittlung an Microsoft nachgewiesen werden.

Weitere Fragestellungen zu Windows 10, wie eine Deinstallationsmöglichkeit der Telemetriekomponente oder eine Einordnung der Home-/Pro-Versionen, sind in den Arbeitsplan der DSK aufgenommen und werden vom BayLDA mit begleitet.

17.2 Ransomware-Trojaner stehlen zunehmend auch personenbezogene Daten

Eine Verschlüsselung von personenbezogenen Daten durch Schadcode ist für die betroffenen Bürgerinnen und Bürger und auch Unternehmen meist schon schlimm genug. Ein neuer Trend, zusätzlich personenbezogene Daten zu entwenden, gibt Anlass zu großer Sorge.

Die Verschlüsselung von personenbezogenen Daten mittels Schadcode ist ein seit langem anhaltender Trend. Durch die Möglichkeit der faktisch anonymen Bezahlung per Bitcoin können Erpressungen unmittelbar und meist ohne großes Risiko einer Entdeckung von Cyberkriminellen durchgeführt werden.

Viele Unternehmen begegnen dieser Art der Bedrohung mit zunehmend wirksamen Backup-Konzepten, die einem Angriff mit dem Ziel einer nachhaltigen Datenverschlüsselung standhalten. Der größte Aufwand für die Unternehmen ist dann, das Backup wieder einzuspielen und Schadcodereste von den Rechnern zu entfernen.

Viele Angreifergruppierungen reagieren auf diese verringerte Wirksamkeit ihrer Schadcode-Kampagnen, indem nach einem erfolgreichen Eindringen in das Netzwerk eines Unternehmens oder die Übernahme eines Rechners nach möglichst interessanten Daten wie Office-Dokumente oder Datenbankdateien gesucht wird. Diese werden vor einer Verschlüsselung der Dateien auf Server der Angreifer kopiert.

Die Erpresser drohen im Falle, dass Lösegeldforderungen nicht beglichen werden, damit, dass die derart entwendeten Dateien dann entweder im Internet veröffentlicht oder im Darknet an andere Cyberkriminelle verkauft werden.

Anhand dieses Trends, der sich auch in den Meldungen zu Verletzungen der Sicherheit nach Art. 33 DS-GVO wiederspiegelt, verändert sich auch die datenschutzrechtliche Einschätzung von Verschlüsselungstrojanern. Während bislang noch häufig von einer ausschließlichen Verschlüsselung ausgegangen wurde und sich das datenschutzrechtliche Risiko nach dem Schaden einer Nichtverfügbarkeit von personenbezogenen Daten, IT-Systemen oder Fachprozessen richtete, ist nun auch das Risiko des Verlusts der Vertraulichkeit mit einzubeziehen. Da angenommen werden muss, dass personenbezogene Daten, die von Angreifern im Kontext von Ransomware entwendet wurden, auch missbräuchlich verwendet werden, ist die Eintrittswahrscheinlichkeit des Risikos als hoch anzusehen. Dies bedeutet, dass in den Fällen, bei denen die Erpresser schon von sich aus über einen Datendiebstahl informieren oder bei denen anhand der Schadcode-Klasse davon ausgegangen werden muss, dass Daten üblicherweise auch entwendet werden, das Datenschutzrisiko direkt mit der Datensensitivität zusammenhängt und häufig das Eintreten eines Sachverhalts gemäß Art. 34 DS-GVO angenommen werden muss. Dann sind auch die Betroffenen über den Vorfall zu informieren. Unternehmen, die nicht

von einer Datenausleitung bei derlei Sicherheitsvorfällen ausgehen, haben deshalb erhöhte Nachweispflichten uns gegenüber, dass mit hinreichender Wahrscheinlichkeit keine Datenflüsse an die Angreifer stattgefunden haben (z. B. Webproxy blockt verdächtigen Serveraufruf, Datenvolumen im Auswertezeitraum ist nicht hoch genug,...). Diese Nachweise sind im Rahmen einer Meldung nach Art. 33 DS-GVO beizulegen.

17.3 Datenverarbeitung durch Tesla-Fahrzeuge

Die Verarbeitung personenbezogener Daten bei Tesla-Fahrzeugen beschäftigt uns weiterhin. Eine Analyse von Fahrzeugen konnte 2020 Corona-bedingt noch nicht abgeschlossen werden.

Dass Tesla-Fahrzeuge mit vielen Kameras ausgestattet sind um bspw. Fahrerassistenzsysteme wie Spurhalteassistenten zu ermöglichen, ist grundsätzlich erwartbar. Die Aufzeichnungen von Videosequenzen zu Forschungszwecken durch Tesla und Umgebungsaufnahmen zu eigenen Zwecken eines Tesla-Halters werfen jedoch weiterhin datenschutzrechtliche Fragen auf.

Da Tesla seine Europaniederlassung in den Niederlanden hat, ist die dortige Datenschutzaufsichtsbehörde für eine Prüfung der Zulässigkeit von Kameraaufnahmen (bspw. bei Bremssituationen) durch Tesla zu eigenen Zwecken (z. B. Produktentwicklung) zuständig.

Anders sieht es mit dem sog. Tesla Sentry Mode aus (siehe auch TB 2019), bei dem – sofern ein USB-Datenträger im Fahrzeug angeschlossen wird – die Fahrzeughalter zu eigenen Zwecken mitunter Aufnahmen durchführen. Zuständig ist nach unserer Auffassung hierzu vergleichbar zum Einsatz von Dash-Cams jede deutsche Datenschutzaufsichtsbehörde, in deren Bundesland das konkrete Tesla-Fahrzeug zugelassen ist.

Sobald ein Halter den Sentry Mode aktiviert, wird dieser datenschutzrechtlich Verantwortlicher und muss dann eine Rechtsgrundlage für bspw. eine Aufnahme auf einem Supermarktparkplatz nachweisen können, falls andere Besucher, die das Auto nur in geringem Abstand passieren, von dem Tesla-Fahrzeug aufgezeichnet werden. Neben der Rechtsgrundlage stellt sich auch die Frage, wie dann mit den Informationspflichten umgegangen werden kann, da i. d. R. zwar im Fahrzeuginneren eine Aufnahmeanzeige dargestellt wird, diese aber von Passanten, die keinen Blick in das Fahrzeug werfen, nicht gesehen wird.

Unsere Fallzahlen zu Datenschutzbeschwerden zu Tesla bewegen sich im niedrigen Bereich und bestehen meist aus allgemeinen Fragen zur datenschutzrechtlichen Zulässigkeit der Aufzeichnungsmöglichkeit durch Tesla, die in die Zuständigkeit der niederländischen Datenschutzaufsicht fallen.

Bei Beschwerden zum Tesla Sentry Mode wäre es für uns wichtig, dass Nachweise einer aktiven Aufzeichnung sowie ein Fahrzeugkennzeichen bei der Beschwerde mitgeteilt werden, um hierzu nach Prüfung des spezifischen Einzelfalls auch ein Musterverfahren der Untersagung des Tesla Sentry Mode oder gar ein Bußgeldverfahren gegen den Tesla-Halter, sofern ein gravierender Fall vorliegt, einleiten zu können.

Genauere Analysen der Datenflüsse von Tesla-Fahrzeugen bedürfen auch technischer Prüfungen. Ende 2020 konnten wir bei einem Tesla-Fahrzeug ein erstes Prüfszenario unseres IT-Labors validieren. Eine mehrtägige technische Prüfung eines Tesla-Fahrzeugs ist für 2021 geplant, sobald die Corona-Maßnahmen eine solche Analyse ermöglichen.

17.4 Cyberabwehr Bayern

Die Cyberabwehr Bayern wurde im Januar 2020 ins Leben gerufen, um eine Möglichkeit der Kooperation verschiedener bayerischer Behörden zu schaffen, die mit Cybersicherheitsaufgaben betraut sind.

Die DS-GVO fordert (auch) die Einhaltung der IT-Sicherheitsschutzziele Vertraulichkeit, Verfügbarkeit und Integrität bei der Verarbeitung personenbezogener Daten durch den Verantwortlichen. Bei Sicherheitsverletzungen, bspw. durch Hacking-Angriffe durch Cyberkriminelle oder Ransomware-Vorfälle, besteht eine Meldepflicht für die bayerischen Unternehmen beim BayLDA. Aufgrund der umfangreichen Beratungen sowie der Meldungen, die innerhalb von 72 Stunden nach Kenntnisnahme des Unternehmens bei der zuständigen Aufsichtsbehörde eingehen müssen, gehört die Prävention von und Schadensbegrenzung bei Cybersicherheitsvorfällen zum Schwerpunktthema des technischen Bereichs des BayLDA.

In der Cyberabwehr Bayern werden in regelmäßigen Abständen aktuelle Erkenntnisse zu Themen der Cybersicherheit ausgetauscht. So sollen Synergieeffekte bezüglich Bedrohungen und aktuellen Entwicklungen im Bereich Cyberkriminalität geschaffen werden, um effizient und angemessen auf internetbasierte Angriffe reagieren zu können. Auch werden mögliche präventive und reaktive Maßnahmen besprochen und abgestimmt.

Das BayLDA begrüßt die Zusammenarbeit mit an der Cyberabwehr Bayern beteiligten Behörden ausdrücklich und sieht insbesondere den fachlichen Austausch zu Bedrohungslagen und Trends zum Angreifervorgehen als besonders gewinnbringend an.

Des Weiteren hat die Präventionsarbeit bei Cyberattacken insbesondere mit Blick auf kleinere und mittlere Unternehmen weiterhin einen hohen Stellenwert beim BayLDA, das auch zunehmend eigene Checklisten zu technischen und organisatorischen Maßnahmen fachlich mit den an der Cyberabwehr Bayern beteiligten Behörden abstimmt.

18

Bußgeldverfahren

18 Bußgeldverfahren

18.1 Bericht aus der Zentralen Bußgeldstelle

Im Berichtszeitraum wurden in der Zentralen Bußgeldstelle insgesamt 230 Vorgänge abgeschlossen – davon jedoch auch noch einige Altverfahren aus dem Jahr 2018. Vier der bearbeiteten Vorgänge mündeten in den Erlass eines Bußgeldbescheids, wovon drei bereits rechtskräftig sind und einer nach Einspruchseinlegung und erneuter Überprüfung im Zwischenverfahren an das zuständige Amtsgericht abgegeben wurde. Alle erlassenen Bußgeldbescheide betrafen Verstöße gegen Art. 5 Abs. 1 Buchst. a, Art. 6 Abs. 1 DS-GVO (Datenverarbeitungen ohne Rechtsgrundlage) von natürlichen Personen. Des Weiteren waren zum Stichtag 31.12.2020 noch 64 weitere Bußgeldvorgänge in Bearbeitung, die teilweise auch schon das Anhörungsstadium erreicht hatten.

Darüber hinaus ist im Berichtszeitraum eine Entscheidung des zuständigen Amtsgerichts über unseren ersten nach Geltungsbeginn der DS-GVO im Jahr 2019 erlassenen Bußgeldbescheid ergangen, der nach zulässigem Einspruch an das zuständige Amtsgericht abgegeben wurde. Sanktioniert wurde ein Unternehmen, welches uns bei einer unangekündigten Vor-Ort-Kontrolle nach Art. 58 Abs. 1 Buchst. f DS-GVO den Zugang zu den Geschäftsräumen und Datenverarbeitungsanlagen verweigert hatte. Das Amtsgericht ist unserer Argumentation inhaltlich gefolgt, hat das Bußgeld jedoch durch Beschluss von 20.000 Euro auf 7.000 Euro reduziert, was unter anderem mit dem erheblichen Zeitablauf – der Verstoß wurde Ende 2018 begangen – begründet wurde.

Auch in diesem Berichtszeitraum haben uns viele Anzeigen und Ereignismeldungen von Polizeiinspektionen erreicht, die den unrechtmäßigen Einsatz von in Kfz installierten Dashcams im öffentlichen Straßenverkehr betreffen. Neu hinzugekommen im Berichtszeitraum sind jedoch vermehrt Anzeigen gegen Fahrradfahrende, die eine am Fahrradhelm installierte Kamera im Einsatz haben. Die für Dashcams mittlerweile anerkannten Grundsätze, wonach eine anlasslose Überwachung des öffentlichen Straßenverkehrs datenschutzrechtlich nicht zulässig ist, lassen sich ebenso auf den Einsatz von Helmkameras durch Fahrradfahrende übertragen, so dass auch hier bei entsprechenden tatsächlichen Anhaltspunkten für eine anlasslose Überwachung bereits erste Bußgeldverfahren eingeleitet wurden.

Natürlich hat auch die Corona-Pandemie Auswirkungen auf die in der Zentralen Bußgeldstelle zu bearbeitenden Verfahren. So wurden im Berichtszeitraum mehrere Bußgeldverfahren gegen Mitarbeitende von Gastronomiebetrieben eingeleitet, die Gäste per WhatsApp kontaktierten, nachdem sie sich die Handynummern dieser Gäste aus den ausgefüllten Formularen zur Kontaktdatenerhebung in der Gastronomie anlässlich der Corona-Pandemie beschafft hatten.

Zwar wird ein Mitarbeitender beim bloßen Datenabruf aus Datenbanken des Unternehmens, bei dem er beschäftigt ist bzw. der bloßen Einsichtnahme in personenbezogene Daten in entsprechende Unterlagen zu privaten Zwecken nicht zum eigenständig Verantwortlichen im Sinne des Art. 4 Nr. 7 DS-GVO, da die beiden dort genannten Kriterien – Zweck- und Mittelbestimmung – nach dem Wortlaut („und") kumulativ vorliegen müssen. Der Mitarbeitende mag die Daten zwar zweckwidrig verarbeiten, er bestimmt aber nicht über den Mitteleinsatz. Vielmehr stellt das Beschäftigungsunternehmen die Datenbanken zur Verfügung; der Mitarbeitende macht sich die vorhandene Infrastruktur lediglich zunutze.

Dies hatten wir in unserem letzten Tätigkeitsbericht bereits für den Bereich der Beschäftigten bayerischer öffentlicher Stellen so dargestellt. Dies lässt sich aber ebenfalls auf Mitarbeitende nicht öffentlicher Stellen übertragen.

Dagegen werden Mitarbeitende in dem geschilderten Fall, in dem sie die durch Datenabruf bzw. Einsichtnahme erlangten personenbezogenen Daten im Anschluss auf nicht dem Unternehmen zuzurechnenden Ressourcen weiterverarbeiten, zu eigenständigen Verantwortlichen im Sinne der DS-GVO, da sie für diese „zweite Phase" (hier: Kontaktaufnahme über WhatsApp) sowohl über Zwecke als auch Mittel selbst und allein bestimmen.

Auch ist im geschilderten Fall nicht die Haushaltsausnahme nach Art. 2 Abs. 2 Buchst. c DS-GVO einschlägig, wonach die DS-GVO keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten findet. Anhand der im Rahmen dieser Norm vorzunehmenden Gesamtwürdigung aller in Betracht kommender Gesichtspunkte ist zunächst zu berücksichtigen, dass zu den per WhatsApp kontaktierten Gästen keinerlei persönlich-familiäre Beziehung besteht, was bereits gegen einen rein persönlich-privaten Zusammenhang spricht. Darüber hinaus bestimmt Erwägungsgrund 18 der DS-GVO, dass die DS-GVO nur für solche Tätigkeiten nicht greifen soll, die „ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit" vorgenommen werden. Da Art. 2 Abs. 2 Buchst. c DS-GVO als Ausnahmevorschrift eng auszulegen ist, ist für ihre Annahme jedenfalls das vollständige Fehlen jedes beruflichen Bezugs erforderlich, wie auch der Wortlaut des Art. 2 Abs. 2 Buchst. c DS-GVO („ausschließlich") eindeutig bestimmt. Da die Handynummern der Gäste jedoch aus den Formularen zur Kontaktdatenerhebung anlässlich der Corona-Pandemie des Gastronomiebetriebes, in welchem die Betroffenen der Bußgeldverfahren zur Tatzeit jeweils beschäftigt waren, entnommen wurden, stammen diese aus dem beruflichen Bereich. Damit besteht eindeutig ein beruflicher Bezug, sodass auch der Kontext der Verarbeitung kein rein persönlich-familiärer ist.

Stichwortverzeichnis

A

Adressdaten ... 42
Adresshandel ... 40
Apple ... 28
Arzt ... 54
Attest ... 54
Auftragsverarbeitung ... 24, 31
Auskunft ... 36, 37, 50
Auskunfteien ... 37
  Positivdaten ... 37

B

Banken ... 35
Beratungen ... 14
Beschäftigte ... 50, 51
Beschäftigtendatenschutz ... 50
Beschwerden ... 11
Binding Corporate Rules ... 44
Bußgeldverfahren ... 78

C

Cookies ... 27
Corona ... 19, 21
Corona-Test ... 51
Corona-Warn-App ... 20
COVID-19 ... 19
Cyberabwehr Bayern ... 76

D

Datenexporteure ... 46
Datenschutzverletzungen ... 15, 70
Dienstplan ... 50
Distanzunterricht ... 56
Drittländer ... 45

E

Eigeninteresse ... 66
Eigentümergemeinschaft ... 62, 63
Einwilligung ... 40
Energieversorger ... 62

F

Fingerabdruck ... 52
Fitnessstudio ... 67
Foto ... 37, 66
Friseure ... 19

G

Gastronomie ... 19
gemeinsame Verantwortlichkeit ... 24
Gesundheit ... 54
Gesundheitsdaten ... 59
Google Analytics ... 26

H

Handel ... 42
Handwerker ... 64
Hausgeld ... 62
HIS ... 35

I

Immobilienbewertung ... 26
Immobilienwert ... 37
Insolvenzverwalter ... 31
Internationaler Datenverkehr ... 44
Internet ... 26

K

Kamera ... 68
Kamerafahrten ... 28
Kfz-Kennzeichen ... 66
Kontaktdatenerfassung ... 19
Kontoauszug ... 36
  Kontobewegung ... 36
Koppelungsverbot ... 40
Krankenhaus ... 50

L

Legionellen ... 63

M

Masernimpfung ... 54

Maskenpflicht 55
Befreiung 55
Mieter 63
Mieterdatenschutz 62

N

Nachweispflicht 54
Newsletter 40

O

Öffentlichkeitsarbeit 17

P

Personalressourcen 16
Planet49 27

R

Ransomware 74
Rechtsanwälte 31

S

Sachverständige 32
Schrems-II 46
Schule 55, 56
Scoperty 26
Segelflugsport 59
Selbsthilfeverein 59
Sentry-Mode 75
soziale Einrichtungen 50
Soziales 54
Standarddatenschutzklauseln 45
Statistik 11
Steuerberater 31

T

Technischer Datenschutz 73
Telemetrie 73
Tesla 75
Tracking 27

V

Verbände 59
Vereine 59
Vermieter 64
Veröffentlichung 59
Versicherungswirtschaft 35
Videodienstanbieter 54
Videokonferenzsysteme 21
Videosprechstunde 54
Videoüberwachung 29, 66, 68
Vorträge 17

W

Wasserzähler 63
Websites 26
Werbung 40
Wertgutachten 37
Windows 10 73
Wohnungswirtschaft 62

Z

Zahlen und Fakten 11
Zeiterfassung 52
Zentrale Bußgeldstelle 78
Zutrittskontrolle 20

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