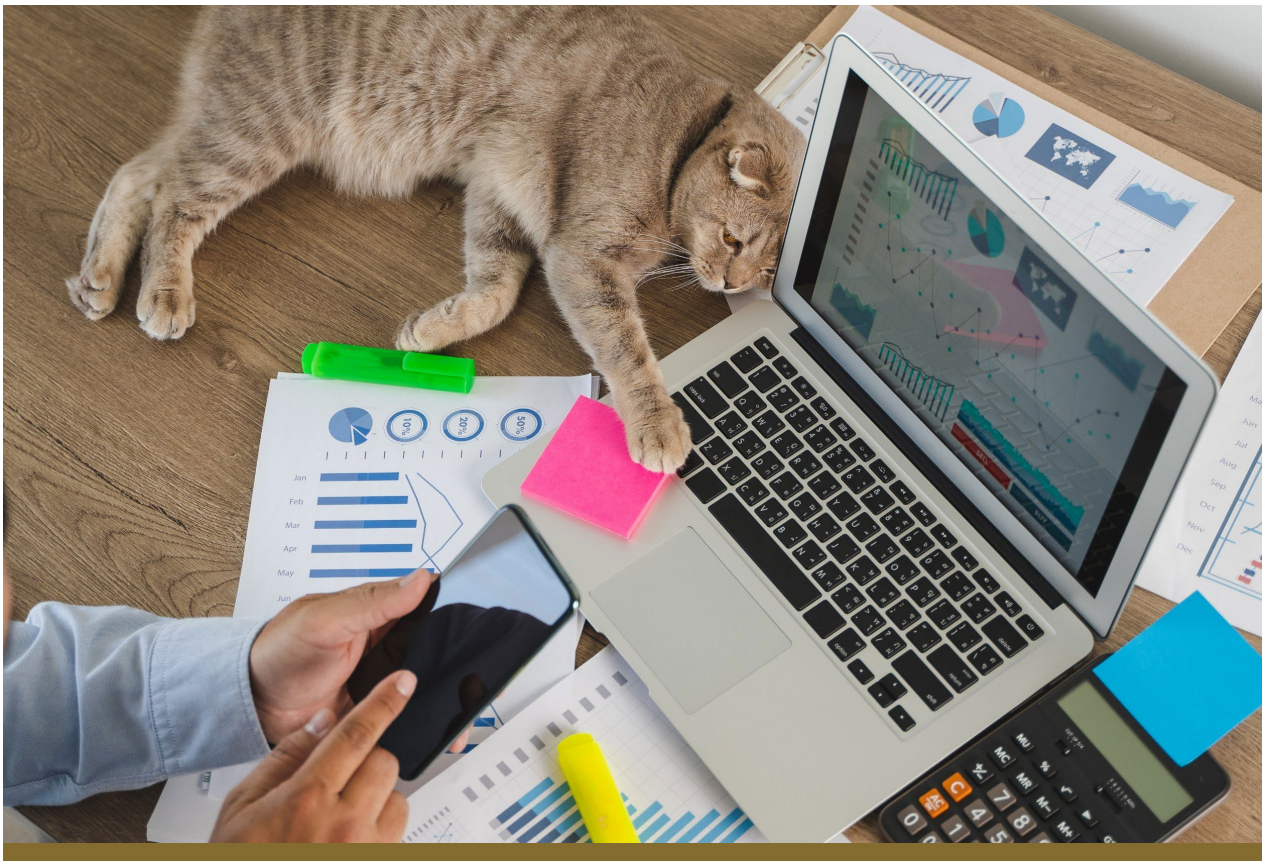
Bayerisches Landesamt für
Datenschutzaufsicht



11. Tätigkeitsbericht

2021

11. Tätigkeitsbericht des Bayerischen Landesamts für Datenschutzaufsicht für das Jahr 2021

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 September 2022 – Michael Will, Präsident

Bildnachweis Cover: de.123rf.com – Urheber adiruch – Dateinummer 147403445

Vorwort

Der Berichtszeitraum für diesen 11. Tätigkeitsbericht für das Jahr 2021 war wie bereits das Vorjahr inhaltlich und strukturell von der Corona-Pandemie geprägt.

Das LDA im zweiten Pandemiejahr

Strukturell haben wir die Situation andauernder Kontakt- und Reisebeschränkungen für uns bestmöglich genutzt und unsere technische Ausstattung und Möglichkeiten virtuellen Arbeitens weiter ausgebaut. Die nahezu vollständige Digitalisierung unserer Prozesse ermöglicht es uns, auch der weiteren Verdichtung von Abstimmungsprozessen und Sitzungsterminen insbesondere auf europäischer Ebene gerecht zu werden, ohne dabei beim Infektionsschutz in Zeiten der Pandemie Abstriche wagen zu müssen. Diese Möglichkeiten sind zum einen dem enormen Einsatz unserer Kolleg:innen des technischen Datenschutzes zu verdanken, die diese Digitalisierung ermöglicht und begleitet haben. Genauso bleibt an dieser Stelle wieder der Regierung von Mittelfranken danken, die das LDA durchgängig mit ihren zentralen Diensten und in der Personalverwaltung unterstützt haben.

Ein für uns erfreulicher Nebeneffekt der weitgehenden Möglichkeiten von Home-Office in unserer Behörde ist es, dass wir so auch für Mitarbeiter:innen, die ihren persönlichen Lebensmittelpunkt nicht in Mittelfranken haben, ein attraktiver Arbeitgeber sein können – angesichts des angespannten Bewerbermarktes ein entscheidendes, trotzdem leider allzu oft nicht alleine für das LDA überzeugendes Kriterium.

Angesichts der positiven Erfahrungen mobilen Arbeitens werden wir uns bemühen, diese Erkenntnisse und Flexibilisierungsmöglichkeiten auch nach dem Ende der pandemischen Ausnahmebedingungen weiter zu nutzen, um unsere Abläufe und Arbeitsbedingungen weiter anforderungsgerecht zu optimieren.

Wir erwarten etwa, dass die eben genannte Termindichte vor allem der europäischen Gremien auch nach der Pandemie erhalten bleiben wird.

Auch inhaltlich hat die Corona-Pandemie erneut das Datenschutzjahr 2021 geprägt. Insbesondere im Bereich der Impf- und Testzentren, Schulen und Kitas, besonders aber im Beschäftigtendatenschutz haben wir fortlaufend Ministerien und Verantwortliche bei der datenschutzkonformen Ausgestaltung und Umsetzung infektionsschutzrechtlicher Regelungen beraten und unterstützt – sei es mit praxisorientierten Hinweisen zu den mehrfach modifizierten „3G"-Anforderungen des Infektionsschutzrechts oder mit Hilfestellungen zur datenschutzgerechten Gestaltung von Homeoffice, auf deren sehr alltagsnahe Handlungsempfehlungen auch das Titelbild unseres Tätigkeitsberichts 2021 verweist.

Da wir im Rahmen des Projekts „Datenschutz geht zur Schule" im Jahr 2021 pandemiebedingt nicht persönlich an Schulen gehen durften, um vor Ort Schüler:innen für Themen des Datenschutzes zu sensibilisieren, haben wir uns an der Produktion von Unterrichtsmaterialien, insbesondere von Videos beteiligt.

https://www.datenschutz-leicht-erklaert.de/

Daneben hat das LDA durch eine Freistellung für das Contact-Tracing-Team auch außerhalb der eigenen Behörde seinen solidarischen Beitrag zur Bewältigung der pandemischen Spitzenbelastung der gesamten bayerischen Staatsverwaltung erbracht.

Themenschwerpunkte TTDSG und Schrems II

Neben der Pandemiebekämpfung hat weiterhin das Urteil des Europäischen Gerichtshofs (EuGH) vom 16. Juli 2020 in der Rechtssache „Schrems II" unsere Aufgabenschwerpunkte bestimmt. Parallel zu den Abstimmungen auf europäischer

Ebene über die Ergebnisse des Konsultationsverfahrens zu den Handlungsempfehlungen des Europäischen Datenschutzausschusses hat das Landesamt in einer Vielzahl von Einzelfällen über die praxisgerechte Umsetzung der EuGH-Entscheidung beraten und sich an einem gemeinsamen anlasslosen Prüfverfahren der deutschen Aufsichtsbehörden beteiligt.

Ein weiterer Schwerpunkt der Beratungs- und Sensibilisierungsarbeit des Landesamts bildet ab der zweiten Jahreshälfte das am 1. Dezember 2021 in Kraft getretene „Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien"(TTDSG). Zusammen mit den Datenschutzaufsichtsbehörden Berlins und Niedersachsens und Sachsens hat das Landesamt mit Rücksicht auf die große Zahl bayerischer Anbieter die Arbeiten an datenschutzrechtlichen Anwendungshinweisen zum TTDSG begleitet, die zeitgerecht zum Dezember 2021 für die Datenschutzpraxis bereit gestellt werden konnten.

Zunahme von komplexen Cybervorfällen

Die digitale Vernetzung von IT-Systemen und mobilem Arbeiten bringt zugleich die Möglichkeit internetbasierter Angriffe mit sich – die bereits vorhandene hohe Bedrohungslage wurde durch Angriffsvektoren erweitert, die sich durch die zunehmend dauerhaft etablierte Nutzung von Homeoffice bei bayerischen Unternehmen ergeben. Insbesondere der Bereich Ransomware und Cyberattacken auf Cloud-Systeme erfordern von den Angreifern ein hohes technisches Know-How, entsprechend komplex und zeitlich aufwändig ist die Aufarbeitung solcher bei uns gemeldeter Sicherheitsverletzungen bayerischer Unternehmen. Hervorzuheben ist dabei, das wir durch die hohe Anzahl von Meldungen zu Cyberattacken ein gutes Bild von der Sicherheitslage bayerischer Unternehmen – insbesondere kleine und mittlere – haben und durch Kenntnisse von Angriffsmethoden neben derer Einbringung in die Cyberabwehr Bayern auch präventive Kontrollmaßnahmen zum wirksamen Schutz gegen derartige Cyberangriffe durchführen können.

LDA prüft jetzt anlasslos.

Anlasslose Kontrollmöglichkeiten gehören zu den Kernaufgaben einer Datenschutzaufsichtsbehörde. Aus diesem Grund haben wir – trotz sehr hoher personeller Auslastung - Ende 2021 die neue Stabsstelle Prüfverfahren etabliert, die sektor- oder themenspezifische anlasslose Datenschutzprüfungen bei bayerischen Unternehmen auf den Weg bringen soll. Zielsetzung ist dabei auch ein hohes Maß an Transparenz indem Prüfbögen und Musteranschreiben auf unserer Webseite veröffentlicht werden. Wir erhoffen uns dadurch auch, die Datenschutzbeauftragten bayerischer Unternehmen als Multiplikatoren gewinnen können, die unsere veröffentlichten Checklisten für deren eigene präventive Kontrollen mit aufnehmen und damit Datenschutzverletzungen im Vorfeld verhindern können.

Ansbach, im September 2022

Michael Will
Präsident

Inhaltsverzeichnis

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 enthält insbesondere auch statistische Angaben, die ein Gesamtbild unserer Schwerpunkte und Arbeitsbedingungen vermitteln sollen.

1.2 Datenschutz in Bayern

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

- das Bayerische Landesamt für Datenschutzaufsicht (LDA), 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)

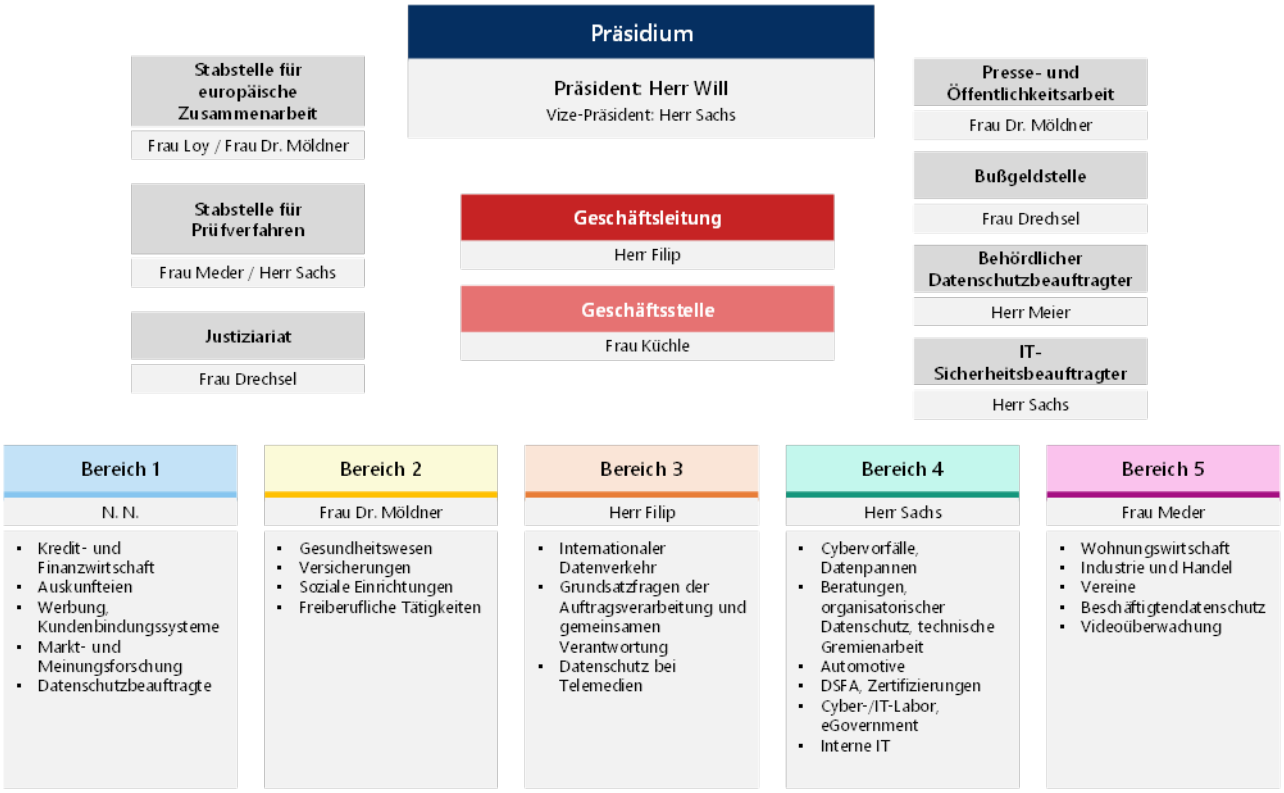
als gleichwertige und gleichrangige Aufsichtsbehörden im Sinne des Art. 51 DS-GVO gesetzlich festgelegt. Vor dem Hintergrund der gemeinsamen Verpflichtung zur einheitlichen Anwendung und Durchsetzung der DS-GVO enthält Art. 21 BayDSG letztlich klarstellend einen an alle vier Behörden adressierten Auftrag 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

Fallzahlen im Spitzenniveau der Vorjahre lassen ahnen, dass auch das Jahr 2021 alle Bereiche des Landesamts Woche für Woche vor enorme Herausforderungen gestellt hat, um den vielfältigen Aufgaben der Datenschutzaufsicht letztlich gerecht zu werden. Auch im vierten Jahr ihrer Geltung ist in jedem der fünf Fachbereiche nach wie vor spürbar, 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.

Die Änderung dieser Organisationsstrukturen haben wir bereits im letzten Berichtszeitraum vorgestellt und im Jahr 2021 fortgeführt. Nachfolgendes Organigramm soll die aktuellen Strukturen unserer Behörde illustrieren:



2

Zahlen und Fakten

2 Zahlen und Fakten

Wie schon in den letzten Tätigkeitsberichten gezeigt, verfügt das LDA 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 in den letzten Jahren derart an Bedeutung gewonnen, dass er schon zur Komplettierung des Gesamtbildes als „34. Mitarbeiter des LDA" näher vorzustellen bleibt:

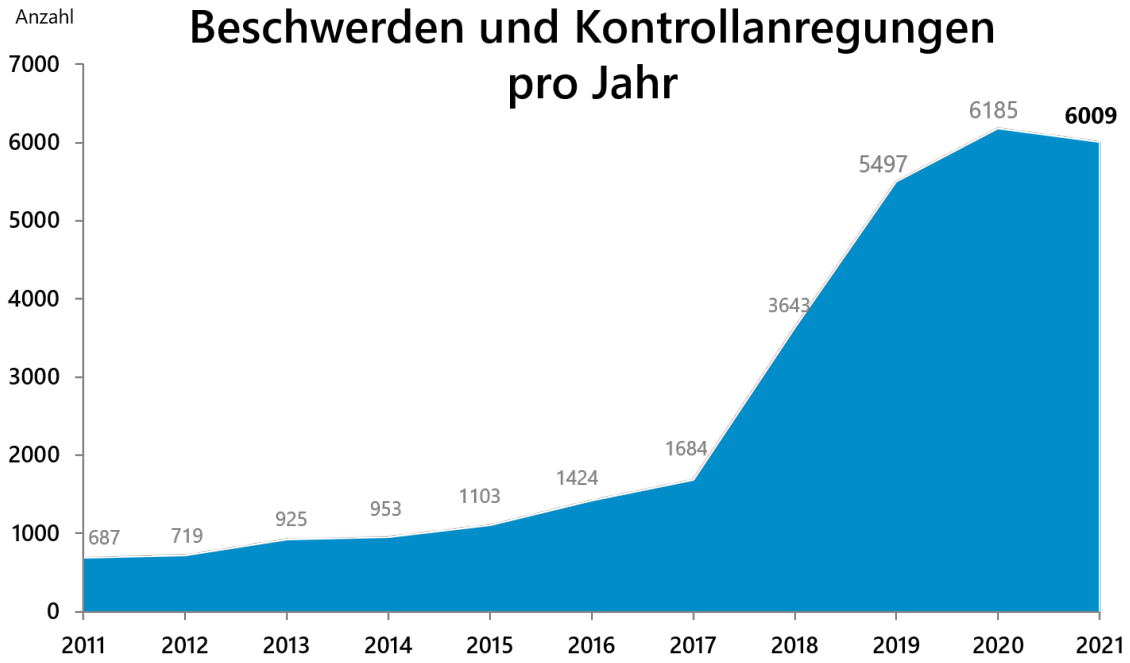
„IGOR" ist gleichsam das digitale Rückgrat des LDA. Das im LDA eigenständig entwickelte und kontinuierlich passgenau ausgebaute Programm erlaubt als Ausprägung von eGovernement für zahlreiche Fallgestaltungen eine weitgehend elektronische, standardisierte Fallbearbeitung. Gleichzeitig war es das Fundament für den pandemiebedingten Rückzug nahezu sämtlicher Mitarbeiter:innen ins Home-Office bei Fortführung der bisherigen Produktivität, da zentrale Scan- und Druckmöglichkeiten geschaffen und damit technisch betrachtet eine Fallbearbeitung von „überall auf der Welt" möglich wäre.

Beschwerden

Die Gesamtanzahl der Beschwerden und Kontrollanregungen, die 2021 bei uns eingegangen sind, ist der unten folgenden Grafik zu entnehmen. Sie zeigt weiterhin, dass im Vergleich zu dem Jahrzehnt zuvor, fast eine Verzehnfachung der Fallzahlen bewältigt werden muss.

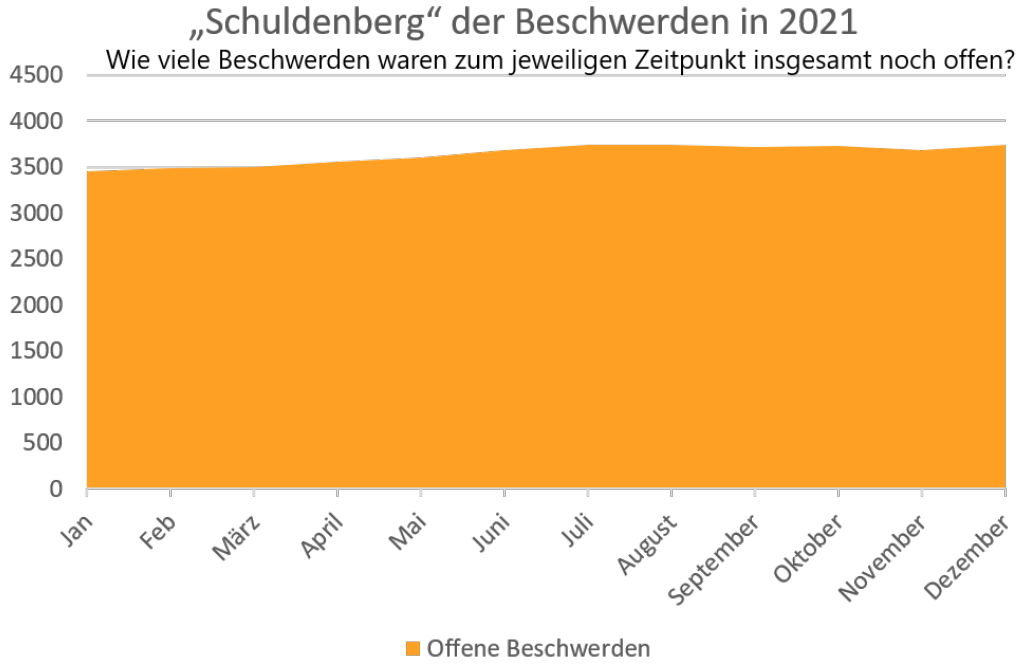
Als Beschwerden werden dabei zum einen solche Vorgänge gezählt, die schriftlich eingehen und bei denen eine natürliche Person eine persönliche Betroffenheit darlegt, für die Art. 78 DS-GVO anwendbar ist. Dies schließt Abgaben ein. Telefonische „Beschwerden" werden dann gezählt, wenn sie z. B. durch einen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

Unter dem Obergriff „Beschwerden" erhielten wir auch im Jahr 2021 eine erhebliche Anzahl von Meldungen über Datenschutzverstöße, bei denen die Eingabeführer:innen 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, den Zielwert der Drei-Monatsfrist des Art. 78 Abs. 2 DS-GVO nicht zu verfehlen.

Demgegenüber besteht bei Kontrollanregungen kein Anspruch darauf, vom LDA 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.



Die Vervielfachung 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 der Personalkörper des LDA mit 33 Planstellen weiterhin nicht gewachsen. Ende 2021 waren erneut rund 3500 Vorgänge nicht abgeschlossen.

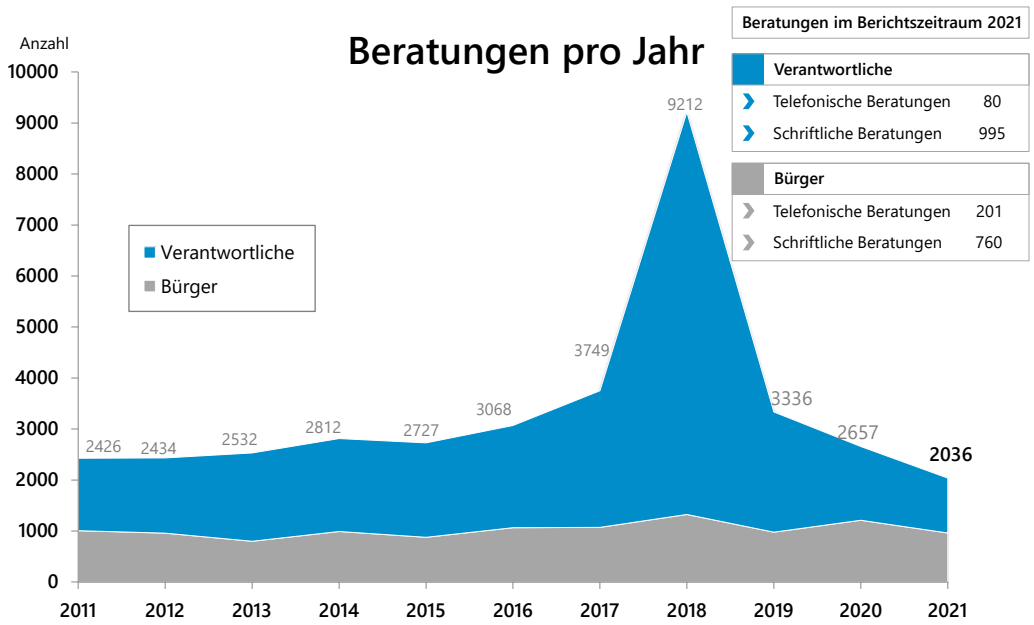
Dieser Rückstand verschlechtert unsere durchschnittliche Bearbeitungsdauer erheblich, enttäuscht die berechtigten Erwartungen der Bürgerinnen und Bürger in eine effektive Durchsetzung ihrer durch das Unionsrecht gewährleisteten Rechte und wird unserem Selbstverständnis als Teil eines bürgernahen und 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. Dass wir trotz der hohen Falllasten wie angekündigt im Jahr 2021 beginnen konnten, anlasslose Prüfverfahren durchzuführen, ist insoweit nicht Ausdruck verbesserter Ressourcen sondern ausschließlich Beleg für die außerordentliche Einsatzbereitschaft der Kolleginnen und Kollegen, die diesen bei unseren europäischen Partnerbehörden längst selbstverständlichen Aufgabenbereich nun auch für das LDA aufgebaut haben.

2.1 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 nachstehenden 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 Vorjahr gesunken.

Während wir uns im vorherigen Berichtszeitraum ein Absenken der Beratungsanfragen mit den spezifischen Online-Beratungen erklärt haben, gehen wir mittlerweile davon aus, dass sich unsere mangelnden Ressourcenmöglichkeiten „herumgesprochen" haben und Verantwortliche zunehmend weniger Anfragen an uns stellen. Auch wenn es durchaus in unserem Interesse läge, jede Individualanfrage angemessen oder



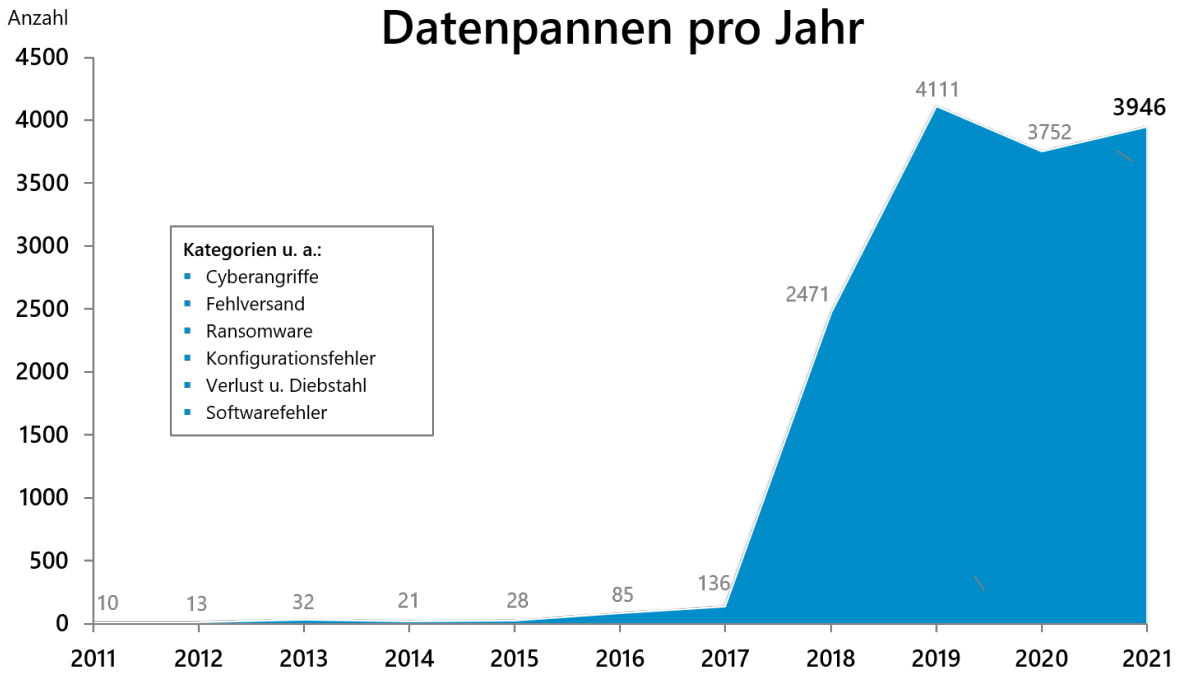
überhaupt zu beantworten – lassen sich so neben der Rechtssicherheit für die Unternehmen häufig Datenschutzverstöße im Vorfeld verhindern – müssen wir der Realität ins Auge blicken, dass die Vielzahl von Datenschutzbeschwerden und Meldungen von Sicherheitsverletzungen kraft gesetzlicher Verpflichtungen eine höhere Priorität beanspruchen. Sorge bereitet uns, dass damit der bislang erfolgreiche „bayerische Weg", der rechtzeitige Beratung statt Sanktionen vorsieht, insbesondere mit Blick auf innovative und datengetriebene Geschäftsfelder aufgrund unserer nicht aufgabengerechten Ressourcen zunehmend erodieren könnte. Während es bspw. bei kleineren Vereinen oder Handwerksbetrieben keine nennenswerten Datenschutzvorfälle gibt, wird bei einem weiteren Einbruch der Beratungsmöglichkeiten in allen übrigen Bereichen auch die Frage genauer zu prüfen sein, wie durch Sanktionen generalpräventive Abschreckung und damit Datenschutzkonformität erreicht werden kann.

Dabei 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. So positiv der Rückgang der unter Gesichtspunkten der Arbeitsbelastung erscheinen mag, so notwendig bleibt eine kritische Analyse der Gründe des Rückgangs. Auch wenn reaktive Beratungen nicht ausdrücklich im Aufgabenkatalog der Aufsichtsbehörden in der DS-GVO enthalten sind, haben sie für die Gewährleistung hoher Datenschutzstandards in der Praxis eine essentielle Bedeutung. Beratungen unterstützen oft mehr als repressives aufsichtliches Handeln effektive datenschutzfreundliche Lösungen und schaffen im Interesse von Verantwortlichen und Betroffenen gleichermaßen Planungs- und Rechtssicherheit. Insoweit bewerten wir den anhaltenden Rückgang der Beratungszahlen nicht als Gewinn, sondern als Risiko für den Datenschutz.

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

2.2 Datenschutzverletzungen

Wie schon in den vorangegangenen Jahren ist die Zahl der Meldungen von Verletzungen der Sicherheit bei der Verarbeitung personenbezogener Daten weiter gestiegen. 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 oben aufgeführten Grafik werden die bei uns eingegangenen Meldungen nach Art. 33 DS-GVO dargestellt. Weitere Informationen zum Thema Datenschutzverletzungen im Allgemeinen sind im Kapitel 16 dieses Berichts zu finden.

2.3 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 2021 aufgrund der Priorisierung auf die Aufarbeitung von Cybervorfällen bei bayerischen Unternehmen noch nicht, diese Angaben automatisiert auszuwerten. Das LDA hatte im Berichtszeitraum weiterhin zwei Subgroupvertretungen im Europäischen Datenschutzausschuss inne. Daneben wirkten wir mehrfach mit an Leitlinien durch Berichterstattungen und Kommentierungen und in weiteren Taskforces oder Ausschuss-Delegationen (beispielsweise die Taskforce „Schrems II" oder als Vertretung der europäischen Aufsichtsbehörden im Rahmen der Evaluation der Adäquanzentscheidung für Japan durch die EU-Kommission). Bei der Stellungnahme des Europäischen Datenschutzausschusses zum Digital Covid Certificate waren wir Berichterstatter. Weiterhin wurden durch das LDA zwei CoCs überprüft und zahlreiche BCR.

2.4 Förmliche Begleitung von Rechtsetzungsvorhaben

Auch 2021 hatte das LDA 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 LDA häufig zwar außerordentlich kurzfristig, aber unkompliziert und weit über die Grenzen der formalen Unterrichtungspflicht des Art. 16 Abs. 3 BayDSG hinaus einbezogen wurde.

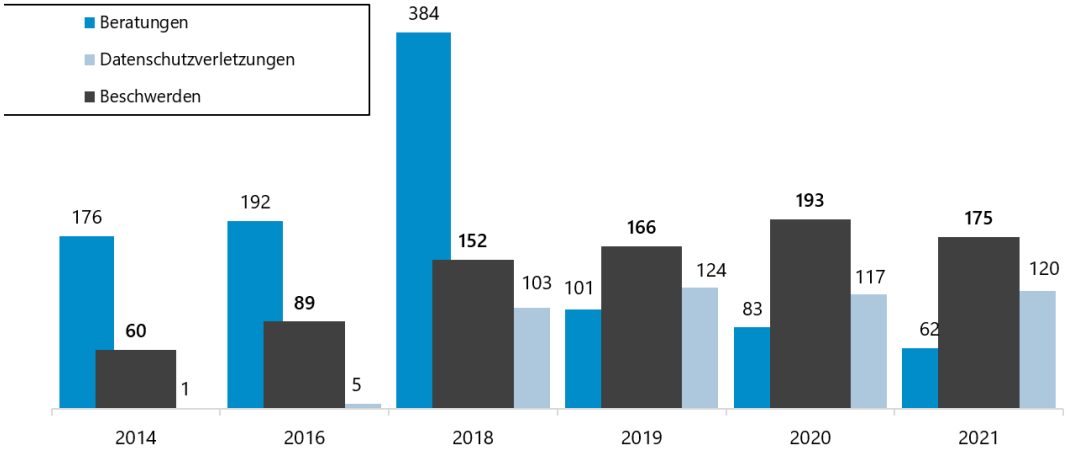
Neben der Wahrung datenschutzrechtlicher Grundprinzipien, insbesondere der klaren Grenzen des Erforderlichkeitsgrundsatzes standen dabei regelmäßig die Praxistauglichkeit und damit die Gewährleistung datenschutzgerechter Verarbeitungsbedingungen für nicht öffentliche Stellen wie z. B. Arztpraxen, Gastwirte oder im Beschäftigtendatenschutz im Vordergrund. Weitere Ausführungen dazu finden Sie im Abschnitt 3.1.

2.5 Ressourcen

Im Berichtszeitraum konnte das LDA auf Grundlage der bereits im vorangehenden Bericht ausführlicher dargestellten Stellenumschichtungen eine zusätzliche Kraft für seine Geschäftsstelle gewinnen, die die dortigen 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. Angesichts der in diesem Kapitel aufgezeigten Fallzahlen müssen und werden sie von uns mit Nachdruck in die kommenden Haushaltsaufstellungsverfahren eingebracht werden.

Durchschnittliche Vorgänge pro Planstelle



2.6 Vorträge und Öffentlichkeitsarbeit

Wir haben auch im Jahr 2021 eine deutliche 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, genauso aber auch die Regional-Gliederungen des Berufsverbands der Datenschutzbeauftragten e.V. (BvD) virtuell oder im Rahmen der Möglichkeiten genauso persönlich zu besuchen. Die regelmäßig in großer Zahl vorab eingereichten Fragen geben wichtige Hinweise auf aktuelle Praxisanliegen und werden von uns gerne zur Erläuterung unserer Vollzugspraxis genutzt.

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 Ausgestaltung und Umsetzung infektionsschutzrechtlicher Vorgaben

Zur Bekämpfung der COVID-19-Pandemie wurden verschiedene Maßnahmen getroffen, deren datenschutzkonforme Umsetzung wir begleitet haben. Wir haben für die Unternehmen diesbezüglich umfangreiche Informationen bereitgestellt.

Im Rahmen der Bekämpfung der COVID-19-Pandemie wurde durch den Landesgesetzgeber im Rahmen der Infektionsschutzmaßnahmenverordnung unter anderem das Tragen einer medizinischen bzw. FFP2-Maske in zahlreichen Bereichen des öffentlichen Lebens vorgeschrieben. Der Nachweis der Befreiung von dieser Tragepflicht bereitete dabei Umsetzungsschwierigkeiten. In Zusammenwirken mit dem Bayerischen Landesbeauftragten für den Datenschutz und dem Beauftragten für die Belange von Menschen mit Behinderung der Bayerischen Staatsregierung haben wir Nachbesserungen der gesetzlichen Regelungen erwirkt und gemeinsam mit dem Bayerischen Landesbeauftragten Hinweise zur datenschutzkonformen Umsetzung dieser Regelung entwickelt. Hierzu haben wir auch bereits im Tätigkeitsbericht 2020 detailliert Stellung genommen, worauf an dieser Stelle verwiesen wird (siehe dort Ziff. 12.3). Die jeweils gültigen Hinweise finden Sie auf unserer Homepage.

https://www.lda.bayern.de/media/LDA_report_10.pdf

In verschiedenen infektionsschutzrechtlichen Regelungen wurden Testpflichten und kostenlose Testmöglichkeiten etabliert und zu diesem Zwecke verschiedene Testzentren errichtet, deren datenschutzkonformer Betrieb zum Teil Schwierigkeiten bereitete. Insbesondere kamen hier Fragen zur datenschutzkonformen Ausgestaltung der Testung selbst und zum sicheren Versand der Ergebnisse auf. Für die Folgeberichtszeiträume haben wir uns vorgenommen, die datenschutzkonforme Aufbewahrung und Löschung der Dokumente eingehend zu prüfen.

Parallel wurden Pooltestungen in Schulen und Kindertageseinrichtungen eingeführt, deren Ausgestaltung wir datenschutzrechtlich begleitet haben.

Auch die Umsetzung von Vorgaben im Bereich des Beschäftigtendatenschutzes führte immer wieder zu Unsicherheiten bei den Verantwortlichen. So musste hier zum Teil der Nachweis einer aktuellen Corona-Impfung, des Genesenenstatus oder eines aktuellen negativen Testergebnisses (geimpft, genesen, getestet, kurz: 3G) erbracht und datenschutzkonform dokumentiert werden. Durch zahlreiche FAQs, Beratungen der betroffenen Ministerien und Verbände und Einzelauskünfte sind wir hier tätig geworden. Auch hier lohnt sich der Blick auf die ständig aktualisierten Inhalte unserer Homepage.

https://www.lda.bayern.de

Im Folgenden finden Sie zu einem Teil der eben angesprochen sowie zu weiteren Problemkreisen nähere Ausführungen. Im Übrigen verweisen wir auf unseren letzten Tätigkeitsbericht.

3.2 Kopieanfertigung von Corona-Impfnachweisen in Beherbergungsbetrieben

Die Anfertigung einer Kopie eines negativen Corona-Testergebnisses, eines Genesenennachweises bzw. eines Impfnachweises (Nachweis über das Vorliegen einer vollständigen Schutzimpfung gegen das Coronavirus SARS-CoV-2) ist ohne explizite Rechtsgrundlage in der Regel unzulässig.

Mehrfach wurde uns der Sachverhalt vorgetragen, dass vorwiegend im Bereich der Beherbergung Kopien von Corona-Impf-, Test- und Genesenennachweisen beim Einchecken

angefertigt wurden bzw. bereits eine Zusendung im Vorfeld der Übernachtung verlangt wurde. Von den Mitarbeiter:innen des Beherbergungsbetriebs wurde dieses Vorgehen gegenüber den Gästen damit begründet, dass man aufgrund der jeweils geltenden Fassung der Bayerischen Infektionsschutzmaßnahmenverordnung (BayIfSMV) zur Dokumentation verpflichtet sei. In der Korrespondenz mit den Verantwortlichen wurde uns von diesen dargelegt, dass dort Unsicherheit im Hinblick auf die Umsetzung der in der BayIfSMV aufgeführten Vorgaben und insbesondere bezüglich etwaiger Anforderungen an eine Dokumentation bestand. Durch das Anfertigen von Kopien wollte man jeglichen Aufsichtsbehörden gegenüber nachweisen können, dass die geltenden infektionsschutzrechtlichen Regelungen eingehalten werden. Aufgrund des dynamischen Pandemieverlaufs und den dadurch bedingten Änderungen sowie Anpassungen der Regelungsinhalte der jeweils geltenden Fassung der BayIfSMV waren den Verantwortlichen ihre Verpflichtungen in Bezug auf die konkrete Umsetzung oftmals nicht klar. Dieser Umstand wurde von uns im Rahmen unseres Ermessens beim Verfahrensabschluss berücksichtigt. In 2021 wurde in der jeweils geltenden Fassung der BayIfSMV nicht explizit geregelt, dass Kopien über den Impf-, Test- oder Genesenennachweis einer Person angefertigt werden sollten. In den Regelungen war es vielmehr vorgesehen, dass ein entsprechender Nachweis lediglich vorgelegt werden muss. Damit war aus datenschutzrechtlicher Sicht zulässig, aber auch ausreichend, dass entsprechende Nachweise von den Verantwortlichen eingesehen und ggf. eine Dokumentation darüber gemacht wurde, dass eine Einsichtnahme erfolgte. Die zuletzt genannte Dokumentation beinhaltet jedoch gerade nicht das Kopieren oder Scannen von Nachweisen bzw. den Vermerk, welcher Nachweis und mit welcher Gültigkeitsdauer vorgelegt wurde.

Lediglich bei Dauerverhältnissen (z.B. regelmäßige Besuche einer Sportstätte) sahen wir es als zulässig an, dass die Tatsache des Vorhandenseins eines (Dauer-)Nachweis sowie die Gültigkeitsdauer mit Einwilligung gem. Art. 4 Nr. 11, 7 DS-GVO der Betroffenen hinterlegt werden konnte.

Es wird darauf hingewiesen, dass die vorstehenden Ausführungen nicht gelten, soweit explizit eine Dokumentation des konkreten Nachweises gefordert wurde. So wurde beispielsweise im Rahmen der 3G-Regelung am Arbeitsplatz zumindest die Dokumentation der Nachweisart und der Gültigkeitsdauer für zulässig angesehen.

3.3 Kopie von Personalausweisen in Corona-Testzentren

Der Grundsatz, dass der Personalausweis gemäß § 20 Abs. 2 Personalausweisgesetz (PAuswG) nicht ohne Zustimmung bzw. Einwilligung des Inhabers kopiert werden darf, wurde in Corona-Testzentren oftmals nicht eingehalten.

Uns wurde vorgetragen, dass Mitarbeiter:innen von Corona-Testzentren Kopien von Personalausweisen getesteter Personen anfertigen würden. Begründet wurde dieses Vorgehen häufig damit, dass das Gesundheitsamt diesen Nachweis für die Abrechnung benötige oder die Identität bei einem positiven Corona-Testergebnis konkret festgestellt werden müsse.

Generell gilt, dass gemäß § 20 Abs. 2 PAuswG die Ablichtung eines Personalausweises nur mit Zustimmung bzw. Einwilligung des Ausweisinhabers erfolgen darf. Die Ablichtung muss zudem eindeutig und dauerhaft als Kopie erkennbar sein. Andere Personen als der Ausweisinhaber dürfen die Kopie nicht an Dritte weitergeben. Werden durch Ablichtung personenbezogene Daten aus dem Personalausweis erhoben oder verarbeitet, so darf die datenerhebende oder -verarbeitende Stelle dies nur mit Einwilli-

gung des Ausweisinhabers tun. Daneben bleiben die Vorschriften des allgemeinen Datenschutzrechts nach § 20 Abs. 2 Satz 4 PAuswG über die Erhebung und Verwendung personenbezogener Daten unberührt, sodass auch dann, wenn die betroffene Person mit der Kopie einverstanden ist, dennoch der Grundsatz der Datenminimierung nach Art. 5 Abs. 1 Buchst. c) DSGVO gilt.

Eine Kopie des Personalausweises birgt das Problem, dass auch über die eigentlich notwendigen Daten hinausgehende und somit nicht erforderliche Daten erhoben werden (z. B. die Ausweisnummer oder die sog. Zugangsnummer, die Augenfarbe, die Körpergröße), was dem Grundsatz der Datenminimierung widerspricht und daher unzulässig ist. Zulässig wäre eine Kopie lediglich dann, wenn die Zustimmung bzw. Einwilligung des Inhabers vorliegt und auf der Kopie alle nicht für den Zweck der Datenverarbeitung benötigten Daten geschwärzt werden.

Sofern die Kopie des Personalausweises dem Zweck der Identifikation der zu testenden bzw. getesteten Person dienen soll, können die dafür benötigten Daten (Name, Vorname, Adresse, Geburtsdatum) auch dadurch gewonnen werden, dass die Mitarbeiter:innen des Testzentrums sich den Personalausweis vorzeigen lassen und die o. g. zur Identifizierung erforderlichen – aber auch ausreichenden – Daten daraus notieren oder abgleichen. Eine Sichtkontrolle ist für die Überprüfung der Identität ausreichend.

Dem Infektionsschutzgesetz (IfSG) ist nicht zu entnehmen, dass bei Vorliegen eines positiven COVID19-Testergebnisses eine Kopie des Personalausweises der positiv getesteten Person angefertigt werden müsste. Auch der Testverordnung (TestV) kann zum Zweck der Abrechnung kein Erfordernis der Anfertigung einer Kopie des Personalausweises der getesteten Person entnommen werden.

3.4 Zulässige Datenverarbeitung von Apotheken bei digitalen Impfzertifikaten

Das Anfordern von Kopien von Impfpässen und Personalausweisen ist für die Erstellung digitaler Corona-Impfzertifikate nicht zulässig.

In § 22 Abs. 5 Nr. 2 Infektionsschutzgesetz (IfSG) war vorgesehen, dass Apotheker:innen zur Erstellung eines digitalen COVID-19-Impfzertifikates eine Impfdokumentation über die Schutzimpfung gegen das Coronavirus vorgelegt wird und diese unter Verwendung geeigneter Maßnahmen die Identität der geimpften Person und die Authentizität der Impfdokumentation überprüfen zur Vermeidung der Ausstellung eines unrichtigen digitalen COVID-19-Impfzertifikats.

Um sich bei diesem Vorgehen vor eventuellen strafrechtlichen Folgen bzw. Regressansprüchen schützen zu können, wollten Apotheken darüber hinausgehend jedoch auch Impfpässe und Personalausweise kopieren. Aus unserer Sicht, sowie auch der der anderen deutschen Aufsichtsbehörden, ergab sich aus § 22 Abs. 5 Nr. 2 IfSG allerdings eine reine Vorlage- und Prüfbefugnis des Impfpasses und keine Befugnis zum Anfertigen einer Kopie und Speichern dieser. Auch hielten wir das Anfertigen einer Kopie des Personalausweises nach dieser Vorschrift nicht für zulässig. Die Anfertigung einer Kopie des Impfpasses schien zudem keine geeignete Maßnahme zu sein, da im Zweifel gerade nur auf Basis des Originaldokuments die Echtheit von Arztstempel und bspw. Chargenbezeichnung überprüft werden kann. Geeignete und im Sinne der Datensparsamkeit zulässige Maßnahme war vielmehr die sorgfältige Sichtung des Impfpasses sowie des Personalausweises und jedenfalls in Zweifelsfällen der Anruf in der Arztpraxis, die die Impfung durchgeführt hat.

3.5 Übermittlung von Corona-Testergebnissen per E-Mail

Für die Übermittlung von Corona-Testergebnissen reicht eine Transportverschlüsselung aus.

Die Durchführung von Testungen auf das COVID-19-Virus erfolgte in der Regel bei Testzentren, die das Ergebnis nach Testauswertung übermittelten. Dabei war es in den meisten Fällen so, dass eine E-Mail mit dem Testergebnis, sei es als PDF-Anhang oder eindeutigem Link zur Webseite des Testzentrums versendet wurde. Mitunter musste zum Öffnen der PDF-Datei oder zum Abruf des Ergebnisses auf der Webseite noch ein Passwort eingegeben werden - häufig das Geburtsdatum der getesteten Person.

Datenschutzbeschwerden, die einen derartigen Sachverhalt adressierten, wurden von uns so bewertet, dass kein Datenschutzverstoß gegen die Sicherheit der Verarbeitung nach Art. 32 DS-GVO beim Versand per E-Mail vorliegt, sofern eine Transportverschlüsselung der am Versand beteiligten Email-Server nach Stand der Technik umgesetzt war.

Damit wird sichergestellt, dass beim Transport über das Internet keine unverschlüsselten personenbezogenen Daten übertragen werden. Allerdings ist die E-Mail auf dem Server der beteiligten Email-Provider im Klartext vorhanden. Mit Blick auf den risikoorientierten Ansatz der DS-GVO bei der Auswahl von technischen und organisatorischen Maßnahmen sind hierbei spezifische Risiken zu bewerten: Eine Ausleitung der Corona-Testergebnisse bei Internetknotenpunkten ist insbesondere dann nicht möglich, wenn die kryptographischen Algorithmen die Perfect Forward Secrecy Eigenschaft (PFS) unterstützen – diese ist Stand der Technik und mittlerweile bei den meisten Email-Servern vorhanden. Der Zugriff auf Email-Konten bei Hostern ist durch starke Passwörter und ggf. dem Einsatz von Zwei-Faktor-Authentifizierungsmethoden abzusichern. Der Fehlversand an falsche Mail-Empfänger kommt bei einer digitalen Terminvergabemaske und geeigneter Software in der Regel nicht vor. Weitere Restrisiken, die ein hohes Risiko mit sich bringen und eine zusätzliche Inhaltsverschlüsselung (z.B. PDF mit von der getesteten Person vergebenem Passwort) erforderlich machen, sind unserer Ansicht nach nicht vorhanden.

Für Corona-Testzentren gilt demnach aber, dass diese gründliche Sorgfalts- und Nachweispflichten bei der Auswahl eines Email-Providers bzw. der Konfiguration eines selbst betriebenen Systems haben – bei letzterem ist auch auf ein wirksames Patch-Management zu achten.

4

Betroffenenrechte

4 Betroffenenrechte

4.1 Recht auf Auskunft gemäß Art. 15 DS-GVO

Die neuen Leitlinien 01/2022 zu den Rechten betroffener Personen – Auskunftsrecht haben das öffentliche Konsultationsverfahren durchlaufen. Die im Anschluss an die Auswertung der im Konsultationsverfahren eingegangenen Stellungnahmen und nach entsprechender Anpassungen bzw. Ergänzungen der Leitlinien angenommene Version wird für unsere Bearbeitung von Eingaben zum Auskunftsrecht maßgeblich sein. Hier möchten wir häufig auftretende Fragestellungen und Beschwerdeinhalte im Zusammenhang mit dem Auskunftsrecht darstellen.

Im Berichtszeitraum erhielten wir zahlreiche Beschwerden und Beratungsanfragen, die das Auskunftsrecht gem. Art. 15 DS-GVO betrafen.

Die häufigsten Inhalte dieser Eingaben waren die Nicht-Erteilung einer Auskunft bzw. die Erteilung einer unzureichenden bzw. unvollständigen Auskunft. Dabei zeigte sich insbesondere auch eine hohe Unsicherheit hinsichtlich des Umfangs der zu erteilenden Auskunft, zu der möglicherweise auch die heterogene Rechtsprechung verschiedener Gerichte beiträgt.

Mit dem Ziel einer europaweit einheitlichen Anwendung des Art. 15 DS-GVO hat der Europäische Datenschutzausschuss Leitlinien zum Auskunftsrecht veröffentlicht. Nach einem vom 28. Januar 2022 bis zum 11. März 2022 stattgefundenen öffentlichen Konsultationsverfahren werden derzeit (Zeitpunkt der Erstellung dieses Beitrages) die darin abgegebenen Stellungnahmen ausgewertet. Die Leitlinien mit dem Stand 28. Januar 2022, d.h. zu Beginn des Konsultationsverfahrens, sowie die hierzu abgegebenen Stellungnahmen sind abrufbar unter

> *https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_de*

Die im Anschluss an die Auswertung der im Konsultationsverfahren eingegangenen Stellungnahmen und nach entsprechender Anpassungen bzw. Ergänzungen der Leitlinien angenommene Version wird für unsere Bearbeitung von Eingaben zum Auskunftsrecht maßgeblich sein. Was gerichtliche Entscheidungen zu Streitigkeiten betreffend das Auskunftsrecht angeht, so ist zu berücksichtigen, dass solche Entscheidungen immer nur den konkreten Einzelfall mit seinen Besonderheiten betreffen und nur Rechtswirkung zwischen den daran beteiligten Parteien entfalten, sodass wir diese grundsätzlich nicht als für unsere Bewertung allgemein anwendbare Maßstäbe betrachten.
Folgende in der Vorgangsbearbeitung während des Berichtszeitraums häufig auftretende Fragestellungen möchten wir besonders hervorheben:

- **Motivation der Geltendmachung des Auskunftsrechts:**

  Art. 15 DS-GVO sieht nicht vor, dass die Gründe für die Geltendmachung eines Auskunftsbegehrens gegenüber dem Verantwortlichen dargelegt werden müssten. Eine betroffene Person soll gerade auch die Möglichkeit haben, ohne Darlegung einer wie auch immer gearteten Erforderlichkeit bzw. deren Preisgabe für einen bestimmten Zweck Auskunft zu erhalten.

- **Pauschale Auskunft:**

  Die Beantwortung eines Auskunftsersuchens erfordert die konkrete Benennung der gespeicherten personenbezo-

genen Daten sowie die konkrete Benennung etwaiger Datenflüsse (Übermittlungen der Daten). Insbesondere sind nicht nur die Datenkategorien zu benennen, sondern auch welche Daten im Klartext hierunter abgespeichert sind; die konkreten Empfänger, an die die Daten offengelegt wurden oder noch werden sollen, sind in der Regel zu benennen, wenn diese bereits bekannt sind.
Die Zusendung eines Auszugs aus den Datenschutzhinweisen (d.h. den Informationen nach Art. 13 DS-GVO), in denen z.B. die Datenkategorien und – ggf. zum Zeitpunkt der Erstellung derselben noch nicht bekannten – Empfängerkategorie oder -kategorien pauschal und umfassend beschrieben werden, genügt somit nicht. Verarbeitet ein Verantwortlicher eine große Menge an Daten, so kann er z.B. die betroffene Person auffordern, die Informationen oder die Verarbeitung, auf die sich der Antrag bezieht, anzugeben, bevor die Informationen übermittelt werden (siehe Erwägungsgrund 63 DS-GVO, Leitlinien 1/2022, Version zur public consultation, S. 15, Rn. 35).

- **Aufbereitung der Daten** (Sprache, Sortierung, Kontext, Auskunft über einen Online-Account):

  In der Praxis ist zu beobachten, dass Beschwerdeführer als Reaktion auf ihr Auskunftsersuchen häufig unaufbereitete Daten erhalten, die für sie oft nicht aus sich heraus verständlich sind. Nach Art. 12 Abs. 1 S. 1 DS-GVO muss die Auskunft in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" erteilt werden. D.h. die Daten müssen häufig zwecks Verständlichkeit aufbereitet und/oder erläutert werden (so jetzt auch Leitlinien 1/2022, Version zur public consultation, S. 42). Des Weiteren ist bisweilen zu beobachten, dass betroffene Personen nur Auskunft auf Englisch erhalten; dies genügt in aller Regel nicht im Sinne der gesetzlichen Anforderung an eine „verständliche" Auskunft.

  Eine weitere Schwierigkeit tritt häufig bei Online-Diensten auf: hier bieten Verantwortliche den betroffenen Personen oft routinemäßig an, sich zum Zwecke der Auskunft in ihren Account einzuloggen und dort die zu ihrer Person gespeicherten Daten einzusehen. Dieser Weg steht jedoch Personen, die keinen Account haben, nicht zur Verfügung. Daher muss der Verantwortliche in diesen Fällen die Auskunft auf anderem Weg erteilen. Ähnlich ist es bei Personen, deren Account – aus welchen Gründen auch immer – gesperrt wurde; auch hier muss der Verantwortliche (nicht erst beim Einschreiten der Aufsichtsbehörde), sofern die betroffene Person die Situation erklärt, von sich aus Auskunft auf anderem Wege anbieten.

- **Identitätsdiebstahl**:

  Häufiger Hintergrund von Auskunftsbegehren gerade in Onlineshops sind Fälle von Identitätsdiebstahl in der Form, dass ein Unbefugter einen Account „gekapert" hat bzw. über einen fremden Account etwa eine Bestellung auslöst. Betroffene Personen möchten hier häufig mittels des Auskunftsanspruchs die Identität des Täters in Erfahrung bringen. Der EDSA hat sich in Randnummer 105 der Leitlinien 1/2022 (unter Subsumtion unter die Rechtsprechung des Europäischen Gerichtshofs zum Personenbezug) dahingehend geäußert, dass die Daten, die im Zusam-

menhang mit einem „gekaperten" Account verwendet werden, vom Auskunftsanspruch des regulären Account-Inhabers umfasst sind, da der Verantwortliche diese Daten in einem Zusammenhang mit dem Accountinhaber verarbeitet und die Daten somit auch auf den Accountinhaber bezogen sind (Rn. 105). Auch wenn wir selbst in unserer bisherigen Praxis noch keinen Fall dieser Art zu entscheiden hatten, werden wir derartige Fälle – vorbehaltlich der Verabschiedung der finalen Fassung des Leitlinienpapiers - entsprechend dieser Aussage im Leitlinienpapier behandeln.

- **Auskunft zu Bild- und Sprachaufnahmen:**

  Umfasst ein Auskunftsersuchen auch Bildaufnahmen und Sprachaufnahmen, ist der betroffenen Person eine Kopie der Bildaufnahmen oder – entsprechend den Leitlinien, Stand 18.01.2022 - Sprachaufnahmen zur Verfügung zu stellen, es sei denn, die Rechte und Freiheiten anderer Personen werden hierdurch beeinträchtigt. Soweit eine solche Beeinträchtigung (z.B. bei mitabgebildeten Personen bzw. Gesprächspartnern) zu bejahen ist, kann eine Schwärzung oder ggf. eine Beschreibung des Bildinhaltes sowie ein (ggf. teilweise geschwärztes) Transkripts einer Tonaufnahme zur Erfüllung des Anspruchs auf Auskunft genügen. Allein der Umstand, dass bei dem Gespräch noch die Stimme eines oder einer anderen Beschäftigten des Verantwortlichen zu hören ist, führt nach unserer Auffassung dabei in der Regel noch nicht zu einem Schwärzungsanspruch.

- **Löschung personenbezogener Daten statt Auskunftserteilung**:

  Immer wieder sehen wir uns mit der Situation konfrontiert, dass Verantwortliche in Reaktion auf ein Auskunftsersuchen personenbezogene Daten löschen anstatt Auskunft zu erteilen. Den auskunftsersuchenden Personen wird sodann mitgeteilt, dass die Daten gelöscht wurden und eine Auskunft somit nicht mehr erteilt werden kann. Dieses Vorgehen widerspricht dem Sinn und Zweck des Rechts auf Auskunft, denn dem Auskunftssuchenden wird damit die Möglichkeit genommen, zu erfahren, welche personenbezogenen Daten verarbeitet werden und die in Art. 15 Abs.1 Buchstabe a bis h DS-GVO ergänzenden Informationen, wie beispielsweise auch die Herkunft und die Empfänger der Daten zu erhalten. Eine solche Tatsachen schaffende Löschung personenbezogener Daten durch einen Verantwortlichen im Rahmen eines Auskunftsersuchens kann aufsichtliche sowie ordnungswidrigkeitsrechtliche Maßnahmen nach sich ziehen. Auch der Europäische Datenschutzausschuss betont, dass der Verantwortliche diejenigen Daten beauskunften muss, die er im Zeitpunkt des Zugangs des Auskunftsbegehrens besitzt (EDSA-Leitlinien 01/2022, Stand 18.01.2022, Rn. 37-39). Verantwortlichen raten wir deshalb dringend davon ab, bei Vorliegen von Auskunftsersuchen gem. Art. 15 DS-GVO Daten noch vor Auskunftserteilung zu löschen. Dies gilt selbst dann, wenn mit dem Auskunftsersuchen ein Antrag auf Löschung etwaig vorhandener Daten gem. Art. 17 DS-GVO verbunden ist

5

Datenschutz im Internet

5 Datenschutz im Internet

5.1 Web-Tracking nach TTDSG

Kein „berechtigtes Interesse“ mehr für Cookies.

Die weit überwiegende Anzahl von Beschwerden im Bereich Internet betrifft den Einsatz diverser Tracking-Tools auf Webseiten. Sehr häufig werden Tools eingesetzt, bei denen unter dem Schlagwort „Reichweitenmessung“ über die reine Reichweitenmessung einer Webseite hinaus die Nutzerdaten an eine Vielzahl von Dritten weitergegeben werden und letztlich zu Zwecken der Profilbildung verwendet werden. In der Praxis werden hierzu meist „Cookies“ eingesetzt, deren rechtliche Bewertung in der Vergangenheit nicht immer eindeutig möglich war.

Aufgrund der fehlenden nationalen Umsetzung von Art. 5 Abs. 3 der ePrivacy- Richtlinie 2009/136/EG wurde das Setzen von Cookies in der Vergangenheit oftmals auf die Rechtsgrundlage des berechtigten Interesses Art. 6 Abs. 1 lit. f DS-GVO gestützt.
Dies ist seit 01.12.2021 nun nicht mehr möglich, da zu diesem Zeitpunkt das Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG) in Kraft getreten ist. Dieses setzt nun die europäischen Vorgaben in nationales Recht um und regelt in § 25 die „Integrität von Endeinrichtungen“ und damit das Setzen von Cookies. Danach ist das Setzen von Cookies in der Regel einwilligungspflichtig, es sei denn eine der in Absatz 2 genannten Ausnahmen ist einschlägig.

Es muss daher zwischen dem Setzen der Cookies und der nachfolgenden Verarbeitung der daraus gewonnenen personenbezogenen Daten, z.B. Cookie-ID differenziert werden. Ersteres richtet sich nun ausschließlich nach § 25 TTDSG, während letzteres – wie bisher – der DS-GVO unterliegt. In den Fällen, in denen bereits vor Geltung des TTDSG eine Einwilligung nach DS-GVO erforderlich war, beispielsweise bei Marketingcookies, ändert sich daher nur die Rechtsgrundlage für das Setzen der Cookies.

Größere Auswirkungen hat die neue Regelung auf Cookies, die bisher auf die Rechtsgrundlage des berechtigten Interesses nach Art. 6 Abs. 1 lit. f DS-GVO gestützt wurden, da diese nun für das Setzen der Cookies, nicht mehr angewendet werden kann. Es ist daher zu prüfen ist, ob eine der in § 25 Abs. 2 TTDSG genannten Ausnahmen einschlägig ist. Relevant ist hier vor allem Nr. 2, welche eine Ausnahme von der Einwilligungspflicht vorsieht, wenn dies unbedingt erforderlich ist um den vom Nutzer gewünschten Dienst zur Verfügung zu stellen.

Unter die Ausnahme des § 25 Abs. 2 Nr. 2 TTDSG können daher beispielsweise Cookies fallen, die erforderlich sind um Chatbots, Kartendienste oder vergleichbare Dienste einzusetzen, jedoch nur und erst dann, wenn dies von Nutzer:innen ausdrücklich gewünscht ist. Ausdrücklich gewünscht ist ein Dienst dann, wenn Nutzer:innen selbst etwas unternommen haben, um den Dienst in klar definiertem Umfang anzufordern, z.B. für Warenkorb-Cookies durch Klick auf „Zum Warenkorb hinzufügen“ (Artikel-29-Datenschutzgruppe Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, WP 194 v. 07.06.2012, S. 3.).

Vom Nutzerwunsch umfasst können zudem auch Cookies sein, welche dazu dienen, eine fehlerfreie Auslieferung der Webseite zu gewährleisten und Navigationsproblemen vorzubeugen. Hierfür kann sich, unter engen Voraussetzungen eine reine Reichweitenmessung eignen, insbesondere dürfen in diesem Fall keine Daten an Dritte übermittelt werden oder ein webseitenübergreifendes Tracking erfolgen. Der Einsatz von Cookies zu weitgehenden Analyse- und Marketingzwecken kann jedoch nicht als unbedingt erforderlich angesehen werden, selbst wenn dies der Finanzierung der Webseite

dient und unterliegt daher im Allgemeinen der Einwilligungspflicht nach § 25 Abs. 1 TTDSG und im Hinblick auf die nachfolgende Verarbeitung Art. 6 Abs. 1 lit. a DS-GVO.

Für ein besseres Verständnis hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder daher am 20.12.2021 die Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 (OH Telemedien 2021) veröffentlicht:

https://datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf

5.2 Einsatz von Google Analytics

Datenübermittlungen in Drittländer im Rahmen von Google Analytics verstoßen gegen Artikel 44 DS-GVO.

„Google Analytics" zählt zu den am weitesten verbreiteten Drittdiensten, die auf Webseiten eingesetzt werden. Dementsprechend häufig erreichten uns im Berichtszeitraum auch Beschwerden und - seitens von Unternehmen - Anfragen zu diesem Tool. Webseitenbetreiber setzen Google Analytics in aller Regel ein, um Informationen über die Nutzung ihrer Webseite zu gewinnen, etwa über die Zusammensetzung des Kreises von Webseitenbesuchern und deren Verhalten auf der Webseite. In der herkömmlichen Einsatzvariante von Google Analytics werden dem Nutzerrechner, der die Webseite aufsucht, einzigartige Kennungen (ID) zugeteilt. Die IDs befinden sich in Cookies, die beim Aufsuchen der Webseite in den Browser des Nutzerrechners gesetzt werden. Mit Hilfe der IDs wird der einzelne Nutzerrechner von anderen Rechnern unterschieden, die die Webseite aufsuchen. Das Tracking des Nutzers selbst beruht auf einem JavaScript-Code, der in den Quelltext der Webseite eingebaut wird und das Herunterladen einer JavaScript-Datei auf den Rechner des Nutzers veranlasst, die es dann ihrerseits veranlasst, dass beim Aufsuchen der Webseite eine Reihe von Daten über die Webseiten-Benutzung vom Nutzerrechner abgerufen und an Google-Server übermittelt werden. Zu diesen Daten zählen Informationen über die HTTP-Anfrage des Nutzers, Informationen über den vom Nutzer eingesetzten Browser und das eingesetzte System (darunter Host-Name, Typ des Browsers, Referrer, genutzte Sprache) sowie ferner etwaige im Browser vorhandene First-Party-Cookies, die es ermöglichen, den Webseitenbesuch (Sitzung) und weitere Informationen zu messen. Auch die IP-Adresse des Nutzerrechners wird an Google-Server übertragen, wobei Google eine Möglichkeit zur Kürzung der IP-Adresse anbietet, nachdem das Google-Analytics Datenpaket an einem Google Server angekommen ist. Die dem Nutzerrechner zugewiesene einzigartige ID kann mit weiteren der o.g. gewonnenen und an Google übermittelten Informationen kombiniert werden, etwa mit der IP-Adresse oder mit Browser- und anderen der oben genannten Daten. Ist ein Besucher während des Besuchs einer solchen Webseite zudem in sein Google-Konto eingeloggt, kann die Information über den Besuch der Webseite zudem von Google direkt dem jeweiligen Google-Konto zugeordnet werden.

Die Datenschutzaufsichtsbehörden mehrerer Mitgliedstaaten haben sich anlässlich einer Beschwerdeserie, die sich gegen Webseitenbetreibern in mehreren EU-Mitgliedstaaten richtete, in einer gemeinsamen Arbeitsgruppe mit Google Analytics beschäftigt. An dieser Arbeitsgruppe hat sich auch das LDA beteiligt. Im Rahmen dieser Befassung wurde von Google gegenüber den Aufsichtsbehörden im April 2021 bestätigt, dass es in der oben beschriebenen Einsatzvariante von Google Analytics zu einer Übermittlung der oben beschriebenen Daten an Google-Server (auch) in Staaten außerhalb des Europäischen Wirtschaftsraums (u.a. in den USA) kommt. Die übermittelten Daten stellen personenbezogene Daten im Sinne der DS-GVO dar. Dies gilt jedenfalls für die o.g. eindeutigen Google-Analytics-Kennungen (IDs), die in den Browser des Nutzers gesetzt werden, denn mit

Hilfe dieser IDs wird der einzelne Nutzerrechner von anderen Rechnern unterschieden. Eine solche Nutzerindividualisierung reicht aus, um das entsprechende Datum als personenbezogenes Datum einzustufen, denn von Personenbezug ist nicht erforderlich, dass einzelne Nutzer:innen mit ihrem bürgerlichen Namen identifiziert werden können, vielmehr genügt die so herbeigeführte Unterscheidbarkeit der Nutzer voneinander (so bereits die Orientierungshilfe der DSK für die Anbieter von Telemedien vom März 2019, Seite 15). Personenbezug besteht daher auch mit Blick auf solche Nutzer:innen, die beim Besuch der betreffenden Webseite nicht in ein Google-Konto eingeloggt sind (und die vielleicht auch gar kein Google-Konto besitzen).

In der Konsequenz daraus sind auch alle weiteren Daten, die zusammen mit der jeweiligen ID an Google-Server übermittelt werden, als personenbezogene Daten einzustufen, da sie durch die gemeinsam mit der ID stattfindende Übermittlung mit der ID verknüpft und damit ebenfalls vom Personenbezug umfasst sind.

In der o.g. Stellungnahme vom April 2021 hat Google mitgeteilt, dass beim Einsatz von Google Analytics personenbezogene Daten auf der Basis der EU-Standardvertragsklauseln gemäß Kommissionsbeschluss 2010/87/EU in Drittländer übermittelt werden. Die Standardvertragsklauseln wurden nach den damals von Google angebotenen Vertragsbedingungen zwischen dem Webseitenbetreiber (Datenexporteur) und Google LLC (Datenimporteur) abgeschlossen. Aufgrund des sog. Schrems-II-Urteils des EuGH vom 16.07.2020 (C-311/18) genügen Standarddatenschutzklauseln jedoch nicht in jedem Fall schon für sich alleine, um bei einer Drittlandsübermittlung den von der DS-GVO geforderten mit dem EU-Schutzniveau gleichwertigen Schutz für die Daten zu gewährleisten; vielmehr muss bei Übermittlungen auf Grundlage vertraglicher Garantien nach Art. 46 DS-GVO stets geprüft werden, ob die Vertragsparteien aufgrund etwa geltenden Rechts ihres Heimatstaats überhaupt in der Lage sind, die in den Garantien eingegangenen Verpflichtungen einzuhalten – hieran fehlt es z.B. dann, wenn Behörden des Drittlands Zugriffe auf die Daten in einem Umfang nehmen können, der nach EU-Recht nicht zulässig wäre, etwa weil er den Grundsatz der Verhältnismäßigkeit nicht wahrt. In solchen Fällen muss der Datenexporteur prüfen, ob es gelingt, sog. zusätzliche Maßnahmen zu ergreifen, um solche nach EU-Recht unzulässige Datenzugänge durch Behörden des Drittlandes zu verhindern. Sind keine effektiven zusätzlichen Maßnahmen möglich, ist die Übermittlung auf Grundlage von Artikel 46 DS-GVO unzulässig.

Google ist – auch nach unserer Überzeugung – als sog. Electronic Communications Service Provider im Sinne des US-amerikanischen Rechts einzustufen, unterfällt daher der Regelung in 50 U.S. Code § 1881 a („FISA 702") und kann somit von US-Behörden zur Datenherausgabe nach dieser Regelung verpflichtet werden. Der Europäische Gerichtshof hat in seinem Schrems-II-Urteil (C-311/18, Rn. 180, 181) entschieden, dass FISA 702 den US-Behörden Datenzugriffe in einem Umfang ermöglich, der dem Grundsatz der Verhältnismäßigkeit nicht entspricht, das nach europäischem Recht zu wahren wäre. Infolgedessen ist eine Übermittlung personenbezogener Daten an Empfänger, die unter FISA 702 fallen, auf Grundlage etwa von Standarddatenschutzklauseln nicht zulässig, wenn es nicht gelingt, die Datenzugriffe der US-Behörden mittels „zusätzlicher Maßnahmen" zu verhindern (oder ineffektiv zu machen).

Mit Blick auf „zusätzliche Maßnahmen" verwies Google im April 2021 gegenüber den Aufsichtsbehörden unter anderem darauf, dass mit Blick auf „Daten im Ruhezustand" (data at rest) eine mehrschichtige AES256-Verschlüsselung zum Einsatz komme; auch für die Kommunikation zwischen den Google-Datenzentren komme Verschlüsselung zum Einsatz.

Eine vom Datenempfänger im Drittland angebotene Verschlüsselung der Daten genügt jedoch, – wie der Europäische Datenschutzausschuss betont hat - nicht, wenn der Empfänger zumindest zeitweilig die Möglichkeit hat, auf die Daten im Klartext zuzugreifen, etwa weil die angebotenen kryptografischen Schlüssel vom Datenempfänger gehalten werden (EDSA, Empfehlungen 1/2020, Rn. 72, 76). Im Falle von Google Analytics in der oben beschriebenen herkömmlichen Einsatzvariante – wie etwa die österreichische oder die französische Datenschutzbehörde in entsprechenden Entscheidungen Anfang 2022 festgestellt haben, – war es daher nicht möglich, solche Zugriffe auszuschließen.

Der Europäische Datenschutzausschuss hat in seinen Empfehlungen 1/2020 (Rn. 43.3) betont, dass dann, wenn die übermittelten Daten in den Anwendungsbereich eines Gesetzes eines Drittlands fallen, das seinem Wortlaut nach den dortigen Behörden Datenzugang in einem nach EU-Datenschutzrecht nicht akzeptablen Umfang grundsätzlich ermöglicht, nicht darauf ankommt, wie „wahrscheinlich" solche Zugriffe erscheinen; vielmehr ist die Übermittlung in solchen Fällen in aller Regel schon deshalb unzulässig, weil das „problematische" Gesetz seinem Wortlaut nach auf die Daten anwendbar erscheint. Allenfalls dann, wenn die Beteiligten in einem solchen Fall überzeugend darlegen können, dass ein nach seinem Wortlaut an sich auf die Daten anwendbares Gesetz in der Praxis auf Fälle der in Rede stehenden Art schlicht von den Behörden des Drittlands nicht angewendet wird (und somit Zugriffe in der Praxis entgegen dem Anschein des Gesetzeswortlauts nicht stattfinden werden), kann die Übermittlung in solchen Fällen doch noch als zulässig gelten.

Die von Google - jedenfalls nach den bis September 2021 angebotenen Vertragsbedingungen - ins Feld geführten Verschlüsselungsmaßnahmen stellen daher keine hinreichend effektiven „zusätzliche Maßnahmen" im Sinne des Schrems-II-Urteils dar, da. Daher verstößt die Übermittlung gegen Artikel 44 DS-GVO, da für die Daten kein mit dem EU-Schutzniveau gleichwertiger Schutz gewährleistet ist. Dieser Auffassung schließen auch wir uns jedenfalls in der nach den bis zum September 2021 von Google angebotenen vertraglichen Bedingungen an. Diese Position haben wir gegenüber den unserer Aufsicht unterliegenden Stellen im Rahmen unserer Fallbearbeitung – etwa anlässlich von Beschwerden gegen den Einsatz von Google Analytics auf Webseiten, die bei uns eingegangen sind – entsprechend kommuniziert und darauf hingewirkt, dass die rechtswidrigen Übermittlungen beendet wurden. Förmliche Anordnungen sind dabei nicht notwendig geworden. Ob dieser Mangel durch die von Google im September 2021 durchgeführte Überarbeitung der Vertragsbedingungen behoben wurde, bleibt einer gesonderten Analyse überlassen.

5.3 Gestaltung von Cookie-Bannern

Für eine rechtswirksame Einwilligung ist eine Ablehnmöglichkeit auf erster Ebene erforderlich.

Bei den im Zeitraum des Tätigkeitsberichts vorliegenden Beschwerden, Kontrollanregungen und Beratungsgesuchen im Bereich Internet, stellten sich immer wieder Fragen im Hinblick auf die Gestaltung der „Consent"-Banner. Diese dienen generell dazu eine Einwilligung (Consent) einzuholen. Die Voraussetzungen für eine rechtswirksame Einwilligung richten sich bei Verarbeitungstätigkeiten nach Art. 4 Nr. 11, Art. 7 und ggfs. Art. 8 DS-GVO. Dies gilt nicht nur für eine Einwilligung nach Art. 6 Abs. 1 lit a DS-GVO, sondern entsprechend § 25 Abs. 1 S. 2 TTDSG auch für Zugriffe auf Endeinrichtungen, wie beispielsweise das Setzen von Cookies.

Hierin enthalten sind jedoch keine konkreten Gestaltungsvorgaben, sodass ein gewisser Gestaltungsspielraum auf Seiten der Verantwortlichen verbleibt. Dieser findet jedoch seine Gren-

zen dort, wo eine freie, informierte, unmissverständliche Wahl nicht mehr möglich ist oder Nutzer:innen bewusst in die Irre geführt werden, um deren Einwilligung zu erhalten. Pauschale Aussagen, wie Kontraste oder Farben gewählt werden dürfen, Einwilligungstexte oder Buttons gestaltet werden dürfen sind nur schwer möglich, da es in der Regel immer einer Einzelfallentscheidung bedarf. Diese ist auch dahingehend zwingend erforderlich, da die Rechtsfolgen gravierend sein können: Wurde die Einwilligung nicht rechtswirksam eingeholt, sind alle darauf basierenden Verarbeitungen rechtswidrig. Es ist daher darauf zu achten, dass die Voraussetzungen an eine rechtswirksame Einwilligung nicht durch die Gestaltung des „Consent"-Banners unterlaufen werden.

Von großer Praxisrelevanz ist vor allem die Frage, ob es für eine rechtswirksame Einwilligung erforderlich ist eine Ablehnmöglichkeit für einwilligungspflichtige Dienste auf erster Ebene vorzuhalten. Dies ist bei einem Großteil der aktuell gängigen „Consent- Banner" zu bejahen, da hier keine andere Möglichkeit besteht das Banner zu schließen, ohne Einwilligung zu erteilen oder eine weitere Ebene aufzusuchen. Die Möglichkeit „Einstellungen oder Ablehnen" als Alternative zur Einwilligungserteilung ist im Regelfall nicht ausreichend.

Wir haben daher im letzten Jahr eine Vielzahl von Verantwortlichen aufgefordert eine gleichwertige Ablehnmöglichkeit in den Consent-Bannern vorzuhalten und sehen auch außerhalb von aufsichtlichen Verfahren hier eine positive Entwicklung.

Darauf aufbauend folgen weitere Gestaltungsfragen, insbesondere was unter einer „gleichwertigen" Ablehnmöglichkeit zu verstehen ist. Dies muss grundsätzlich anhand einer Einzelfallbetrachtung entschieden werden. Allgemein lässt sich sagen, dass die Alternative zur Einwilligung als solche eindeutig erkennbar sein muss und von Nutzer:innen als solche wahrgenommen werden kann. Nicht ausreichend ist es beispielsweise, wenn die Möglichkeit abzulehnen außerhalb des Consent-Banners auf der Webseite dargestellt ist oder dies im Text des Banners ohne Hervorhebung oder Kenntlichmachung „versteckt" ist, wenn dagegen die Möglichkeit der Einwilligungserteilung prominent als Button unter dem Text erscheint. Auch ein identischer Button, der allerdings erst nach Scrollen durch den Consenttext ersichtlich ist, während die Möglichkeit zur Einwilligung direkt zu Beginn des Banners sichtbar ist, stellt keine gleichwertige Option dar.

Um in diesem Bereich eine größtmögliche Harmonisierung der Mitgliedstaaten zu erreichen hat der Europäische Datenschutzausschuss den gemeinsamen Diskurs zu Verstößen in diesem Bereich die sog. „Cookie-Banner"-Taskforce eröffnet, an welcher wir aktiv mitwirken. Ziel ist es möglichst einheitliche Bewertungen zu finden, wenngleich ein gewisser Entscheidungsspielraum auch in Zukunft bei den einzelnen Behörden verbleibt.

Weiterhin ist für Verantwortliche, im Regelfall die Webseitenbetreiber, in diesem Kontext auch darauf zu achten, dass sie allein durch den Einsatz von Consent- Management- Plattformen nicht von ihrer datenschutzrechtlichen Verantwortung entbunden sind. Sowohl für die eigene Datenerhebung als auch die Offenlegung von Daten der Endnutzer:innen an jeden einzelnen Drittanbieter bleibt der Webseitenbetreiber rechenschaftspflichtig.

5.4 Apple AirTags – Ausspähung?

Die datenschutzrechtlichen Anforderungen richten sich nicht an Hersteller von Produkten, sondern an datenschutzrechtlich Verantwortliche und Auftragsverarbeiter.

Das so genannte Apple AirTag ist ein Tool, das von Apple insbesondere als Hilfsmittel zum Auffinden verlorener Gegenstände wie etwa

Schlüssel beworben wird. Der Aufenthaltsort des AirTags wird dabei etwa mit Hilfe des sog. Find-My-Netzwerks festgestellt, und Nutzer:innen des AirTags werden auf ihrem iPhone über den Aufenthaltsort des AirTags informiert. Eine Reihe von Presseberichten über unerwünschtes Ausspähen des Aufenthaltsorts von Personen unter Nutzung des AirTags führte auch zu Presseanfragen bei uns.

Der Sachverhalt zeigt exemplarisch die Risiken missbräuchlicher Nutzung digitaler Technologien und gleichzeitig die Grenzen des Anwendungsbereichs des Datenschutzrechts und damit auch der Aufsicht durch die Datenschutzaufsichtsbehörden auf. Die datenschutzrechtlichen Anforderungen der DS-GVO richten sich an Verantwortliche und Auftragsverarbeiter, die Verarbeitungen personenbezogener Daten durchführen, nicht jedoch an Hersteller, die Produkte anbieten, mit denen personenbezogene Daten verarbeitet werden können. Wie auch andere Hersteller vergleichbarer Tools unterliegt damit nicht Apple in seiner Eigenschaft als Hersteller des AirTags unserer Aufsicht, vielmehr wären etwa Unternehmen oder andere Organisationen, die ein solches Tool im Rahmen ihrer Tätigkeit verwenden, als datenschutzrechtlich Verantwortliche einzustufen und damit Adressaten der datenschutzrechtlichen Verpflichtungen und der datenschutzrechtlichen Aufsicht.

Die Anforderungen der DS-GVO gelten dabei nicht, soweit personenbezogene Daten ausschließlich zur Ausübung persönlicher oder familiärer Tätigkeiten verarbeitet werden (sog. Haushaltsausnahme, Artikel 2 Abs. 2 lit. c DS-GVO). Ausspähungen etwa des Aufenthaltsorts im familiär-privaten Umfeld unterfallen nach unserer Beurteilung der sog. Haushaltsausnahme; so sehr ein unerwünschtes Ausspähen daher als missbilligungswürdig erscheinen mag, können wir als Datenschutzaufsichtsbehörde daher solche Fälle mangels Zuständigkeit nicht mit den in der DS-GVO zur Verfügung gestellten aufsichtlichen Befugnissen aufgreifen. Gleichwohl gelten auch für Ausspähungen im familiären Umfeld selbstverständlich die allgemeinen zivilrechtlichen und strafrechtlichen Grenzen zum Schutz der Persönlichkeitsrechte und Privatsphäre einschließlich der jeweiligen Rechtsdurchsetzungsverfahren, mit denen Betroffene gegen Ausspähungen wirksam entgegentreten können.

Aus den dargestellten Gründen haben wir bislang keinen Anlass gesehen, die Nutzung von AirTags in unseren regelmäßigen Gesprächen mit Vertretern von Apple genauer zu analysieren. Bislang liegen uns hierzu auch keine spezifischen Beschwerdevorgänge vor, während z.B. der Einsatz sonstiger Trackingtechnologien im unternehmerischen Umfeld in der Vergangenheit wiederholt Gegenstand von aufsichtlichen Verfahren war.

Bürger:innen, die befürchten durch AirTags ausgespäht zu werden, können auf die von Apple bislang zu einzelnen Details bereit gestellten Informationen über Kontroll- und Abwehrmöglichkeiten verwiesen werden, die nach unserer Kenntnis noch weiter ausgebaut werden sollen:

https://support.apple.com/de-sg/HT212227
https://support.apple.com/de-de/HT211658

6

Rechtsanwälte und andere freie Berufe

6 Rechtsanwält:innen und andere freie Berufe

6.1 Abtretung offener Honorarforderungen durch Rechtsanwält:innen

Ein:e Rechtsanwält:in darf Honorarforderungen auch ohne Einwilligung des Mandanten an andere Rechtsanwält:innen oder an rechtsanwaltliche Berufsausübungsgemeinschaften abtreten.

Ein Beschwerdeführer monierte uns gegenüber, dass sein Rechtsanwalt eine gegen ihn bestehende Honorarforderung an eine andere, ihm unbekannte Kanzlei abgetreten habe. Hierzu habe er weder seine Einwilligung erteilt noch sei er vorab über die Abtretung informiert worden.

Die Beschwerde blieb erfolglos, da der deutsche Gesetzgeber die Abtretung von Vergütungsforderungen sowie die Übertragung ihrer Einziehung an Rechtsanwält:innen oder rechtsanwaltliche Berufsausübungsgemeinschaften auch ohne Einwilligung der betroffenen Person für zulässig erachtet. Die entsprechenden Regelungen finden sich in § 49b Abs. 4 der Bundesrechtsanwaltsordnung (BRAO). Die mit der Abtretung verbundene Übermittlung personenbezogener Daten kann nach unserer Auffassung auf Art. 6 Abs. 1 S. 1 f) DS-GVO gestützt werden. Ein Widerspruchsrecht der betroffenen Person besteht in diesen Fällen nicht, vgl. Art. 21 Abs. 1 S. 2 DS-GVO a.E. Informationspflichten des abtretenden Rechtsanwalts sind oftmals nach § 32 Abs. 1 Nr. 4 BDSG ausgeschlossen.

Anders wäre der Sachverhalt zu beurteilen gewesen, wenn die Forderung an eine sonstige Stelle (also keinen Rechtsanwalt) abgetreten worden wäre; dann hätte eine ausdrückliche, schriftliche Einwilligung des Mandanten eingeholt werden müssen, sofern die Forderung nicht bereits rechtskräftig festgestellt wurde.

6.2 Übermittlung personenbezogener Daten im Rahmen der Insolvenzverwaltung an Vermieter:innen

Die Nichthaftungserklärung nach § 109 Abs. 1 S. 2 Insolvenzordnung (InsO) kann auch dann abgegeben werden, wenn die Insolvenzschuldnerin nicht im Mietvertrag benannt ist.

Eine Privatperson, über deren Vermögen das Insolvenzverfahren eröffnet worden war, beschwerte sich bei uns über eine durch die Insolvenzverwalterin erfolgte Übermittlung ihrer personenbezogenen Daten. Konkret hatte sich die Insolvenzverwalterin an die Eigentümerin der von der Schuldnerin genutzten Wohnung gewandt, diese über das laufende Insolvenzverfahren informiert sowie darauf hingewiesen, dass das Mietverhältnis nicht gekündigt werde und Ansprüche, die nach Ablauf der gesetzlichen Kündigungsfrist des Mietverhältnisses fällig werden, nicht im Insolvenzverfahren geltend gemacht werden können.

Die Insolvenzverwalterin berief sich in ihrem Schreiben an die Eigentümerin auf die Regelung des § 109 Abs. 1 S. 2 InsO. Ihrem Wortlaut nach setzt die Norm voraus, dass der Insolvenzschuldner Partei des Mietvertrags ist. Gerade dies wurde durch die Beschwerdeführerin bestritten, die ggü. der Insolvenzverwalterin argumentierte, dass lediglich ihr Ehemann, aber nicht sie selbst Vertragspartei sei.

Gleichwohl haben wir die vorliegende Datenverarbeitung als zulässig erachtet: Denn nach höchstrichterlicher Rechtsprechung können auch nicht im Vertrag benannte Personen stillschweigend Mietvertragsparteien werden. Dies konnte die Insolvenzverwalterin trotz der gegenlautenden Erklärungen der Schuldnerin

nicht mit Sicherheit ausschließen. Gleichzeitig hat sie die Pflicht, die Insolvenzmasse zu sichern und zu verhindern, dass diese durch entstehende Forderungen geschmälert wird. Anderenfalls würde sie sich schadensersatzpflichtig machen (vgl. § 60 Abs. 1 InsO). Vor diesem Hintergrund gingen wir davon aus, dass die Datenverarbeitung auf Art. 6 Abs. 1 S. 1 c) DS-GVO i.V.m. den Regelungen der InsO gestützt werden konnte.

7

Versicherungswirtschaft und Banken

7 Versicherungswirtschaft und Banken

7.1 Informationspflichten bei Wechsel des Versicherungsvertreters

Auch wenn die Übermittlung personenbezogener Daten an Versicherungsvertreter:innen ohne Einwilligung zulässig sein kann, müssen Versicherungsunternehmen ihre diesbezüglichen Informationspflichten beachten.

Im Berichtszeitraum erreichten uns verschiedene Eingaben betreffend die Übermittlung personenbezogener Daten durch Versicherungsunternehmen an Versicherungsvertreter:innen. In einem Fall beschwerte sich eine Kundin bei uns darüber, dass die Betreuung ihres Versicherungsvertrags nunmehr durch einen ihr bislang unbekannten Versicherungsvertreter erfolge, sie hierüber jedoch nicht vorab informiert worden sei. Wir kontaktierten das betreffende Versicherungsunternehmen daraufhin, welches uns den Beschwerdesachverhalt bestätigte. Offenbar war in diesem konkreten Fall das eigentlich standardmäßig vorgesehene Benachrichtigungsschreiben nicht versandt worden. Die Betreuung der Kundin war zwischenzeitlich auf die Hauptverwaltung umgestellt worden.

Zwar bedarf die Übermittlung personenbezogener Daten an Versicherungsvertreter:innen grundsätzlich keiner Einwilligung, sondern kann vielfach auf Art. 6 Abs. 1 S. 1 f) DS-GVO gestützt werden. Hiervon bleiben jedoch die durch das Versicherungsunternehmen zu beachtenden Transparenzpflichten unberührt. Es muss daher dafür Sorge getragen werden, dass in derartigen Fällen grundsätzlich vor Übermittlung der personenbezogenen Daten eine ausreichende Information der Versicherungsnehmer:innen erfolgt. Im Regelfall muss dann auch auf das Widerspruchsrecht der betroffenen Person hingewiesen werden.

7.2 Bankseitige Meldung der Beendigung von Vertragsverhältnissen an Wirtschaftsauskunfteien

Soweit Kreditinstitute von der Möglichkeit Gebrauch machen, Daten über die Begründung und ordnungsgemäße Durchführung von Kredit- und Giroverträgen an Auskunfteien zu übermitteln, haben sie dafür Sorge zu tragen, dass ebenso auch die Beendigung dieser Verträge zuverlässig dorthin gemeldet wird.

Im Rahmen einer Interessensabwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO sind Kreditinstitute in aller Regel berechtigt, Daten über die Begründung und ordnungsgemäße Durchführung solcher Verträge und Garantiegeschäfte an Auskunfteien zu übermitteln, bei denen ein kreditorisches Risiko besteht (insb. Giroverträge mit Überziehungsmöglichkeit und Kreditverträge; vgl. hierzu DSK-Beschluss vom 11.06.2018).

Im Jahr 2021 sind wir vermehrt auf Fälle aufmerksam geworden, bei welchen es nach ordnungsgemäßer Beendigung solcher Verträge unterblieben ist, auch diese Beendigung entsprechend zu melden, um der Auskunftei die dortige Löschung des Vertragsverhältnisses zu ermöglichen.

Wenn ein Kreditinstitut von der Möglichkeit der Meldung solcher Verträge Gebrauch macht und damit eine Verarbeitung zu betroffenen Personen bei der Auskunftei veranlasst, hat es besonders dafür Sorge zu tragen, dass der Auskunftei auch die Beendigung zur Kenntnis gelangt, da die übermittelten Daten dort ansonsten in Annahme eines noch bestehenden Vertrags weiter vorgehalten werden.
Kommt ein Kreditinstitut dem nicht nach,

begeht es in Bezug auf die von ihm bei der Auskunftei veranlasste Verarbeitung mangels Aktualität einen Verstoß gegen den Grundsatz der Richtigkeit. Zudem besteht mit ordnungsgemäßer Beendigung des Vertrags auch keine Rechtsgrundlage mehr, die eigene Vertragsmeldung an die Auskunftei weiter aufrechtzuerhalten.

8

Werbung und Auskunfteien

8 Werbung und Auskunfteien

8.1 Bonitätsabfragen im Onlinehandel

Insbesondere wenn Onlinehändler:innen bereits vor Abschluss des Bestellprozesses Daten an Wirtschaftsauskunfteien zur Bonitätsabfrage übermitteln wollen, bestehen erhöhte Anforderungen an die Erfüllung der Informationspflichten.

Wir haben im Berichtszeitraum beanstandet, dass mehrere Onlineshops unzulässige Bonitätsabfragen bei einer Wirtschaftsauskunftei durchgeführt haben. Die Unzulässigkeit hatte jeweils ähnliche Ursachen in der grundsätzlichen Prozessgestaltung und Mängel bei Erfüllung der Informationspflichten der jeweiligen Verantwortlichen.

Meist erfolgte die Übermittlung an die Wirtschaftsauskunftei bereits zu einem Zeitpunkt, zu welchem die betroffene Person im Kassenvorgang - nach Eingabe der Rechnungs- und Lieferdaten - eine risikobehaftete Zahlungsart (z.B. Rechnungskauf) ausgewählt hatte. Es erfolgte aber gleichzeitig keine hinreichende Information darüber, dass bereits zu diesem Zeitpunkt eine Bonitätsprüfung erfolgt.
In einigen Fällen änderten die betroffenen Personen die gewählte Zahlungsart noch zu einer anderen, welche kein solches kreditorisches Risiko barg, und bestätigten erst dann den Bestellabschluss. In anderen Fällen entschieden sich die betroffenen Personen letztlich doch noch dagegen, die Bestellung überhaupt abzusenden.

Die Bestellungen wurden also am Ende mit einer Zahlungsart getätigt, bei der für sich betrachtet keine hinreichende Rechtsgrundlage vorgelegen hätte, um eine Bonitätsabfrage bei einer Wirtschaftsauskunftei zu tätigen. Andere Bestellungen wurden letztlich gar nicht vollendet, aber es fanden dennoch vor Abschluss Bonitätsanfragen statt.

Gleichzeitig war jeweils vor Bestellabschluss bereits eine Bonitätsabfrage erfolgt, ohne dass in den betrachteten Fällen die jeweiligen Betroffenen durch Informationen nach Art. 13 DS-GVO oder entsprechende Hinweise im Kassenvorgang erwarten konnten, dass eine Abfrage bereits bei Auswahl der Zahlungsart und nicht erst nach Bestellabschluss erfolgt.

Bei dieser intransparenten Ausgestaltung und dem vorliegenden Abfragezeitpunkt, überwogen bei der im Rahmen des Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO vorzunehmenden Abwägungsentscheidung die schutzwürdigen Interessen der betroffenen Personen an der Vertraulichkeit ihrer Daten die Interessen der Händler:innen an der Durchführung einer Bonitätsprüfung. Die betroffenen Personen konnten und mussten, insbesondere zum Zeitpunkt der Abfrage, anhand der Begleitumstände nicht nachvollziehbar davon ausgehen, dass eine Bonitätsabfrage bereits zum Zeitpunkt der Auswahl einer Zahlungsart erfolgt. Letztlich waren die Abfragen damit in den behandelten Fällen unzulässig, aber auch die grundsätzliche Prozessgestaltung mangelhaft.

Wir veranlassten deshalb unter anderem, dass die Händler:innen ihren Bestell- und Abfrageprozess derart umgestalten, dass betroffene Personen entweder hinreichend sichtbar und konkret in den Informationen nach Art. 13 DS-GVO und im Kassenvorgang darüber informiert werden, bei Auswahl welcher Zahlungsarten bereits zu einem Zeitpunkt vor Bestellabschluss die Übermittlung an eine Wirtschaftsauskunftei zur Bonitätsabfrage erfolgt, oder dass die Bonitätsermittlung alternativ erst nach Bestellabschluss ausgeführt wird, wenn die Auswahl einer risikobehafteten Zahlungsart unveränderlich

feststeht. Von der Verpflichtung zur Bereitstellung der grundlegenden Informationen nach Art. 13 DS-GVO befreit aber natürlich auch letztere Variante nicht.

8.2 Orientierungshilfe Direktwerbung

Die neue Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO) stellt auch anhand praktischer Fallgestaltungen die datenschutzrechtlichen Grundlagen für die Direktwerbung dar.

Der Arbeitskreis „Werbung und Adresshandel" der Datenschutzkonferenz (DSK) hat in einer zweitägigen Sitzung im September 2021 unter unserer Leitung die bisherigen Anwendungshinweise aus dem Jahre 2018 zur Verarbeitung personenbezogener Daten für werbliche Zwecke unter Berücksichtigung der DS-GVO-Regelungen überarbeitet und in einem anschließenden schriftlichen Verfahren weiter abgestimmt.

Abweichend von der Version 2018 wird das Thema „Adresshandel" in der aktuellen Orientierungshilfe nicht erörtert, da zu einem späteren Zeitpunkt gesonderte Beratungen folgen werden.

Die DSK hat den neuen Text als „Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO)" mit dem Datum 18.2.2022 veröffentlicht.

Die neue Orientierungshilfe ist auf der DSK-Website abrufbar:

https://www.datenschutzkonferenz-online.de/media/oh/OH-Werbung_Februar%202022_final.pdf

9

Handel und Dienstleistung

9 Handel und Dienstleistung

9.1 Nachfragen bei Kund:innen– Nutzung einer Telefonnummer aus dem Telefonbuch

Das Heraussuchen der Telefonnummer von Kund:innen aus dem Telefonbuch anhand deren Wohnort und Namen ist datenschutzrechtlich nicht geeignet, um die Richtigkeit der erhobenen Daten zu gewährleisten.

Eine Beschwerdeführerin monierte, dass ein Unternehmen, bei dem sie online Waren bestellt hatte, bei einer namensgleichen, verwandten Person angerufen hätte, um sich danach zu erkundigen, ob diese noch Interesse an der aufgegebenen Bestellung habe. Die Beschwerdeführerin habe die Bestellung online aufgegeben und als Zahlungsart Vorkasse gewählt. Im Zuge der Bestellung hat sie ihre E-Mail-Adresse angegeben. Da die Beschwerdeführerin den ausstehenden Betrag noch nicht überwiesen hatte, habe das Unternehmen im Telefonbuch nach der Telefonnummer der Kundin recherchiert, was dazu führte, dass eine namensgleiche, im gleichen Ort wie die Kundin wohnende Person vom Unternehmen kontaktiert und über die Bestellung informiert wurde.

Gemäß Art. 5 Abs. 1 Buchst. d und f DS-GVO unterliegt der Verantwortliche bei der Verarbeitung personenbezogener Daten dem Grundsatz der Richtigkeit und der Vertraulichkeit und muss diese durch entsprechende technische und organisatorische Maßnahmen sicherstellen (Art. 24 Abs. 1 DS-GVO). Das Heraussuchen einer Telefonnummer einer namensgleichen Person aus dem Telefonbuch und die Verwendung dieser Daten zum Zwecke der Nachfrage zu einer von dieser aufgegebenen Bestellung stellen keine geeignete technische und organisatorische Maßnahme dar, um die Richtigkeit der erhobenen Daten zu gewährleisten. Allein anhand des Wohnorts und Namens kann eine eindeutige Identifizierung der betroffenen Person nicht erfolgen und somit kann auch eine Weitergabe von Daten an unberechtigte Dritte nicht ausgeschlossen werden. Eine telefonische Kontaktaufnahme war überdies im vorliegenden Fall nicht notwendig, da dem Unternehmen bereits eine andere Kontaktadresse (E-Mail-Adresse) vorlag, über die es die Kundin hätte erreichen können. Eine zusätzliche, nicht notwendige Datenerhebung bzw. -verarbeitung verstößt daher auch gegen den Grundsatz der Datenminimierung nach Art. 5 Abs. 1 Buchst. c DS-GVO.

9.2 Offenlegung von Geldforderung durch Inkassobüro gegenüber Arbeitgeber:in

Soweit nicht strenge Voraussetzungen im Vorfeld einer Lohnpfändung erfüllt sind, hat ein Inkassobüro keine Rechtsgrundlage, eine gegenüber Beschäftigten geltend gemachte Forderung an Arbeitgeber:innen offenzulegen.

Ein Inkassobüro kontaktierte im Rahmen seiner Forderungsbearbeitung die Arbeitgeber:innen der Forderungsschuldner:innen.

Inhalt der Schreiben war, dass ermittelt worden sei, dass die jeweils betroffene Person dort beschäftigt sei. Zur Vermeidung weiterer Kosten und zur Umgehung einer ansonsten erfolgenden Lohnpfändung wurde darum gebeten, mit den jeweils Beschäftigten in Verbindung zu treten, ob diese noch eine freiwillige Zahlung leisten würden. Zusätzlich waren eine Frist zur Rückmeldung und eine vollständige Forderungsaufstellung enthalten. Gerechtfertigt wurde dieses Vorgehen uns gegenüber als letzte Möglichkeit vor einer Lohnpfändung und als Maßnahme zur Ermittlung des pfändbaren Einkommensanteils.

Es ist zwar grundsätzlich korrekt, dass es für ein Inkassobüro datenschutzrechtlich zulässig sein kann, im Vorfeld einer Lohnpfändung Arbeitgeber:innen zu befragen, ob und in welcher Höhe pfändbares Einkommen vorliegt. Jedoch müssen entsprechende Voraussetzungen hierbei beachtet werden:

- Die Anfrage beschränkt sich auf die erforderliche Information des pfändbaren Anteils am Arbeitseinkommen (ggf. mit Informationen, wie dieser zu berechnen ist).
- Auf die Freiwilligkeit der Rückmeldung des Arbeitgebers wird hingewiesen.
- Dem Arbeitgeber wird versichert, dass
  - vorher versucht wurde, die Informationen beim Arbeitnehmer selbst zu erheben (was dementsprechend auch passiert sein muss).
  - die Voraussetzungen für den Erlass eines Pfändungs- und Überweisungsbeschlusses vorliegen, eine Pfändung beabsichtigt ist und unmittelbar bevorsteht.

Bei der im vorliegenden Fall angewandten Vorgehensweise war eine Erfüllung dieser Voraussetzungen jedoch nicht gegeben, zumal schon nicht einmal eine Fragestellung bezüglich des pfändbaren Einkommensanteils enthalten war. Stattdessen wurde lediglich darum gebeten, mit den Beschäftigten in Verbindung zu treten, ob eine freiwillige Zahlung geleistet wird.

Wenn ein Inkassobüro zahlungssäumigen Personen vor dem Hintergrund einer bevorstehenden Lohnpfändung nochmals die Gelegenheit geben will, eine Forderung letztlich doch noch freiwillig zu begleichen, kann dies direkt der betroffenen Person mitgeteilt werden. Ein Erfordernis, alleine hierfür Arbeitgeber:innen über die Forderung zu informieren, besteht objektiv nicht, sodass im behandelten Fall letztlich ein Datenschutzverstoß durch die unzulässige Offenlegung von Daten vorlag.

9.3 Frei zugängliche Daten aus Sozialen Netzwerken

Die Veröffentlichung von frei im Internet zugänglichen personenbezogenen Daten ermächtigt Verantwortliche in der Regel nicht dazu, diese für eigene Interessen und Zwecke zu verarbeiten. Hier muss zuvor genau geprüft werden, inwieweit eine datenschutzrechtliche Grundlage zur Verfügung steht.

Ein Marktleiter eines Supermarktes sammelte auf Facebook Daten und Informationen, um bestimmten Kund:innen ein Hausverbot erteilen zu können. Konfrontiert mit dem Sachverhalt der bei uns eingegangenen Beschwerde teilte uns der Verantwortliche mit, dass der Erteilung des Hausverbots eine Meinungsverschiedenheit vorausgegangen sei. In dem betreffenden Markt bestehe ein Betretungsverbot für Kund:innen, die mit nacktem Oberkörper oder barfuß einkaufen würden. Die Person, die Beschwerde erhob und auch direkt vom Hausverbot betroffen war, fühlte sich allerdings durch das Verbot, nicht im Markt barfuß laufen zu dürfen, diskriminiert und nahm deshalb per E-Mail Kontakt zum Marktleiter auf. Die Antwort des Verantwortlichen hat er daraufhin in einer öffentlichen Facebook-Gruppe gepostet und ferner in einem Kommentar zu einer Protestbewegung gegen den Supermarkt aufgerufen. Der Protestgedanke wurde von anderen Mitgliedern aufgegriffen und ein Flashmob vorgeschlagen. Ein Mitglied kündigte sogar an, dafür von Hamburg nach Bayern reisen zu wollen. Um auf etwaige Protestaktionen vorbereitet zu sein, hat der Verantwortliche die für jedermann zugänglichen Fotos auf Facebook ausgedruckt und an sein Sicherheitspersonal ausgehändigt. Dabei hätte es sich um eine einmalige Aktion gehandelt. Die Fotos seien zudem nicht gespeichert worden.

Für die Verarbeitung von personenbezogenen Daten bedarf es einer datenschutzrechtlichen

Grundlage i. S. v. Art. 6 Abs. 1 DS-GVO. Die Tatsache, dass jemand seine Daten öffentlich im Internet preisgibt, ermächtigt hingegen nicht, diese für jegliche Zwecke verarbeiten zu dürfen. In dem vorliegenden Fall stützte sich der Verantwortliche auf Art. 6 Abs. 1 Buchst. f DS-GVO. Es entspräche dem berechtigten Interesse des Marktleiters, sich vor massiven Störungen des Betriebsablaufes, wie es ein Flashmob darstellen würde, zu schützen. Das Sammeln und Ausdrucken der auf Facebook veröffentlichten Fotos in dieser Gruppe diente dazu, das Hausrecht durchzusetzen. Diese Bewertung wurde durch uns geteilt – überwiegende schutzwürdige Interessen der betroffenen Personen waren nicht ersichtlich. Allerdings hätte der Verantwortliche die jeweiligen betroffenen Personen gemäß Art. 14 DS-GVO datenschutzrechtlich informieren müssen. Darauf haben wir den Verantwortlichen entsprechend hingewiesen.

10

Internationaler Datenverkehr

10 Internationaler Datenverkehr

10.1 "Schrems II" und die hohen Anforderungen an Datenübermittlungen in Drittländer

Die Folgen der „Schrems-II-Entscheidung" des Europäischen Gerichtshofs vom 16.07.2020 (C-311/18) sind kaum zu überschätzen und waren auch im Berichtszeitraum 2021 massiv in unserer aufsichtlichen Tätigkeit zu spüren.

Der Europäische Datenschutzausschuss hat in einem grundlegenden Papier (Empfehlungen 1/2020, Endfassung vom 18.06.2021) aufgezeigt, wie die Datenschutzaufsichtsbehörden das Urteil interpretieren und welche Prüfung Datenexporteure – also Stellen, die personenbezogene Daten in Drittländer übermitteln – durchführen müssen, um solche Übermittlungen im Einklang mit der DS-GVO durchführen zu können. Das LDA hat sich maßgeblich an den Arbeiten an dem o.g. EDSA-Papier auf europäischer Ebene beteiligt.

Die DS-GVO verlangt von jedem Datenexporteur, vor einer Übermittlung personenbezogener Daten an ein Drittland zu prüfen, ob die Daten etwa Gegenstand von Zugriffen durch Behörden des Drittlandes werden können, die nach den Maßstäben des EU-Rechts nicht zulässig wären. Diese Überprüfungspflicht des Datenexporteurs hat der EuGH in seiner o.g. Entscheidung betont. Der Datenexporteur muss auch prüfen, ob für betroffene Personen Rechtsschutzmöglichkeiten im Drittland in dem nach EU-Recht vorgesehenen Mindestumfang zur Verfügung stehen. Diese Prüfung ist bei jeder Übermittlung durchzuführen, die auf sog. geeignete Garantien (Art. 46 DS-GVO, z.B. Standarddatenschutzklauseln) gestützt wird. Für Datenexporteure bedeutet dies, dass der Abschluss etwa der Standardvertragsklauseln nicht mehr per se genügt, sondern dass sie sich vor der Übermittlung mit der Rechtslage und Praxis des Drittlands auseinandersetzen müssen – insbesondere mit den Datenzugriffsmöglichkeiten dortiger Behörden sowie der o.g. Frage entsprechenden Rechtsschutzes. Gerade kleine und mittlere Unternehmen dürften durch diese Prüfverpflichtung vor massive Herausforderungen stehen. Gleichzeitig besitzt die Problematik höchste Praxisrelevanz, da quer durch zahlreiche Branchen und auch bei kleinen und mittleren Unternehmen oft in großem Umfang personenbezogene Daten in Drittländer übermittelt werden, etwa bei der Nutzung von Software as a Service oder auch nur von Speicherplatz „in der Cloud", denn solche Dienste werden am Markt in großen Teilen von US-Unternehmen angeboten und führen häufig zur Speicherung personenbezogener Daten auf Servern in Drittländern (etwa den USA) und/oder zu Fernzugriffen auf in der EU gespeicherte Daten aus Drittländern im Rahmen von Wartung und Support; auch ein solcher Fernzugriff aus einem Drittland stellt rechtlich eine „Übermittlung an ein Drittland" dar.

Der EDSA hat in seinem Papier „Empfehlungen Nr. 01/2020" (das keineswegs einen bloß empfehlenden Charakter hat, sondern die Rechtsauffassung der Datenschutzbehörden darstellt) aufgezeigt, welche Prüfschritte ein Datenexporteur durchführen muss. Letztlich muss er prüfen, welche Rechtsvorschriften (und Praktiken) im Zielland auf die zu übermittelnden Daten Anwendung finden können und ob (und in welchem Umfang) die Daten zum Gegenstand von Zugriffen der Behörden des Drittlands werden können. Hier sind insbesondere Zugriffsmöglichkeiten von Nachrichtendiensten, Sicherheits- und Strafverfolgungsbehörden in den Blick zu nehmen, da typischerweise in diesen Bereichen Behörden besonders weitgehende Möglichkeiten zum Zugriff auf personenbezogenen Daten eingeräumt werden. Sind solche Zugriffe nach Maßstäben des europäischen Rechts als zu weitgehend zu bewerten, etwa

weil sie den Grundsatz der Verhältnismäßigkeit nicht wahren, genügen vertragliche Garantien nach Art. 46 DS-GVO wie bspw. der Abschluss von Standarddatenschutzklauseln für sich gesehen nicht, um die Übermittlung rechtskonform durchführen zu können; vielmehr muss der Datenexporteur dann prüfen, ob es gelingt, zusätzliche Maßnahmen zu finden, mit deren Hilfe solche Zugriffe verhindert oder ineffektiv gemacht werden. Benötigt der Datenempfänger im Drittland für seine Leistungserbringung jedoch Zugriff auf die Daten im Klartext, und unterfällt er gesetzlichen Regelungen des Drittlandes, die derartige zu weitgehende Datenzugriffe von Behörden ermöglichen, so ist die Übermittlung (jedenfalls unter Nutzung von Garantien nach Art. 46 DS-GVO) unzulässig, da aufgrund der Notwendigkeit des Zugriffs auf Klartextdaten durch den Datenempfänger auch nicht ausgeschlossen werden kann, dass es zu den nach EU-Recht unzulässigen Zugriffen durch die Behörden des Drittlands kommt. Der EDSA hat anhand mehrerer Praxisfallgruppen (Use Cases) aufgezeigt, inwieweit es je nach Fallgruppe überhaupt möglich ist, effektive „zusätzliche Maßnahmen" gegen derartige Zugriffe zu finden. Demnach können allein Verschlüsselung und Pseudonymisierung – und auch dies nur unter bestimmten Voraussetzungen – je nach Fallgruppe effektive „zusätzliche Maßnahmen" darstellen; bei einigen der Fallgruppen kommen aber gerade diese Maßnahmen nicht in Betracht – so etwa bei der Übermittlung an Cloud-Provider, die für ihre Leistungserbringung Zugang zu Klartextdaten benötigen (Use Case 6 in den EDSA-Empfehlungen 1/2020). Dies bedeutet, dass etwa bei den – in der Praxis weit verbreiteten – Diensten von Software as a Service, sofern der Dienstleister unter ein „problematisches Gesetz" im Drittland fällt, keine effektiven zusätzlichen Maßnahmen gefunden werden können und die Übermittlung somit nicht auf Grundlage von Garantien nach Art. 46 DS-GVO stattfinden darf. Eine Übermittlung kommt in solchen Fällen allenfalls in den – engen – Grenzen der Ausnahmetatbestände nach Art. 49 DS-GVO in Betracht (die jedoch für große Teile der praktischen Einsatzfälle nicht greifen).

Für die Praxis besondere Probleme stellen sich deshalb, weil Anbieter von Cloud-Diensten häufig US-amerikanische Unternehmen sind und nach US-Recht in aller Regel als sog. Electronic Communications Service Provider im Sinne der Regelungen in 50 U.S. Code § 1881 a („FISA 702") einzustufen sind. Unternehmen, die unter diese Regelung fallen, können von US-Behörden zur Datenherausgabe verpflichtet werden. Problematisch ist dies deshalb, weil der Europäische Gerichtshof in seinem Schrems-II-Urteil (C-311/18, Rn. 180, 181) entschieden hat, dass die von FISA 702 den US-Behörden eingeräumten Datenzugangsmöglichkeiten über das nach EU-Recht zulässige Maß hinausgehen. Infolgedessen ist eine Übermittlung personenbezogener Daten an Empfänger, die unter FISA702 fallen, auf Grundlage etwa von Standarddatenschutzklauseln oder anderen Garantien im Sinne des Artikels 46 DS-GVO nicht zulässig, wenn es nicht gelingt, die Datenzugriffe der US-Behörden mittels „zusätzlicher Maßnahmen" zu verhindern (oder ineffektiv zu machen).

Aufgrund der besonderen Bedeutung von Datenübermittlungen in die USA in der Praxis hat die Datenschutzkonferenz Anfang 2022 ein von dem renommierten US-Datenschutzexperten Stephen Vladeck angefertigtes Gutachten zur Reichweite des Begriffs „Electronic Communication Services Provider" und von Section 702 FISA veröffentlicht, um auf diese Weise Unternehmen und anderen Daten übermittelnden Stellen bei der von ihnen durchzuführenden Analyse der Rechtsordnung und Praxis – jedenfalls bezogen auf Übermittlungen in die USA – zu unterstützen:

https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_de.pdf

Ein wesentliches Ergebnis des Gutachtens war, dass unter die o.g. Regelung nicht nur klassische

IT- und Telekommunikationsunternehmen gehören, sondern durchaus auch Unternehmen aus anderen Branchen sein können. Von der mit Section 702 FISA verbundenen Problematik sind somit wesentlich mehr Datenübermittlungen betroffen als möglicherweise auf den ersten Blick vermutet werden könnte.

Von Unternehmens- und Beraterseite wird gelegentlich argumentiert, eine Übermittlung auf Grundlage von Garantien nach Art. 46 DS-GVO müsse als zulässig betrachtet werden, wenn die übermittelten Daten für Nachrichtendienste und Sicherheitsbehörden „ihrer Art nach nicht interessant" seien und daher ein Datenzugang dieser Behörden unwahrscheinlich sei. Als Argument für diese Sichtweise wird oft der „risikobasierte Ansatz" (risk based approach) ins Feld geführt, der in der DS-GVO (etwa in Artikel 32 DS-GVO) enthalten sei. Der Europäische Datenschutzausschuss hat in den Empfehlungen Nr. 01/2020 dieser Argumentation indes eine Absage erteilt, da sich im Schrems-II-Urteil des Europäischen Gerichtshofs hierfür kein Ansatz finden lässt. Vielmehr hat der EuGH betont, dass für Übermittlungen in Drittländer auf Basis von Garantien nach Art. 46 DS-GVO stets ein mit dem EU-Schutzniveau im Wesentlichen gleichwertiger Schutz gewährleistet werden muss. Ein risikobasierter Ansatz im Sinne einer Abschätzung, wie wahrscheinlich es erscheint, dass die vom Datenexporteur ergriffenen Garantien nach Art. 46 DS-GVO durch Datenzugriffe von Behörden des Drittlandes konterkariert werden könnten, lässt sich dem Urteil des Europäischen Gerichtshofs nach dem Verständnis des Europäischen Datenschutzausschusses nicht entnehmen. Eine solche Prognose wäre kaum seriös möglich und dem Bereich der Spekulation zuzuordnen.

Andererseits können - auch nach Auffassung der Aufsichtsbehörden (EDSA-Empfehlungen 01/2020, Rn. 47) - die bisherigen praktischen Erfahrungen des Datenempfängers mit behördlichen Datenzugangsersuchen im Drittland als eines von mehreren Elementen im Einzelfall eine gewisse Bedeutung spielen – allerdings nicht als einziges entscheidendes Element, sondern nur neben anderen (bestätigenden) Elementen im Rahmen der vom Datenexporteur durchzuführenden umfassenden Analyse der Rechtslage und Praxis des Drittlands, der die zu übermittelnden Daten unterfallen. Teilt der Datenempfänger, etwa im Rahmen sog. Transparenzberichte, mit, dass er in der Vergangenheit noch nicht Adressat eines Datenherausgabeersuchens auf Grundlage eines „problematischen Gesetzes" war (der er dem Buchstaben des Gesetzes nach möglicherweise zunächst unterfällt), so genügt diese Aussage für sich gesehen nicht, um die Datenübermittlung doch noch zu „retten", sondern nur wenn bei einer umfassenden Betrachtung der Situation im Drittland – insbesondere bei Betrachtung auch vergleichbarer anderer Datenempfängen (selbe Branche, vergleichbare Verarbeitungen) im betreffenden Drittland die Aussage möglich erscheint, dass das betreffende „problematische Gesetz" auf Akteure und Daten der in Rede stehenden Art entgegen der ersten abstrakten Betrachtung augenscheinlich de facto nicht zur Anwendung kommt und somit die belastbare Aussage möglich erscheint, dass die Daten faktisch nicht zum Gegenstand der datenschutzrechtlich inakzeptablen Zugriffe werden können (EDSA-Empfehlungen 01/2020, Rn. 47).

Die hier geschilderte vom EDSA vertretene Position steht auch im Einklang mit dem von der Europäischen Kommission in ihren neuen Standardvertragsklauseln für Datenübermittlungen in Drittländer („SCC", Kommissions-Durchführungsbeschluss (EU) 2021/914 vom 04.06.2021) enthaltenen Ansatz (Fußnote 12 zu Klausel 14). Die SCC sehen in Klausel 14 vor, dass Datenexporteur und Datenimporteur bereits vor Abschluss der Vertragsklauseln die Rechtslage und Praxis des Drittlandes geprüft haben und keinen Grund zur Annahme haben, dass daraus Aspekte erwachsen, die den Vertragsparteien die Einhaltung ihrer Verpflichtungen aus den SCC unmöglich machen können. Mit anderen Wor-

ten dürfen die SCC überhaupt erst abgeschlossen werden, wenn der Datenexporteur – ggf. mit Hilfe des Datenimporteurs – die Rechtslage und Praxis im Zielland (jedenfalls diejenigen Regelungen und Praktiken, in deren Anwendungsbereich die zu übermittelnden Daten fallen) bereits geprüft und keine Hinderungsgründe festgestellt haben – etwa keine Datenzugriffsmöglichkeiten, die über das nach europäischem Recht zulässige Maß hinausgehen. Klausel 14 der SCC bestätigt somit, dass auch die neuen SCC die Datenexporteure nicht von der Prüfung der Rechtslage und Praxis des Drittlandes entbinden.

11

Beschäftigtendatenschutz

11 Beschäftigtendatenschutz

11.1 Einreichung der Arbeitsunfähigkeitsbescheinigung bei den Vorgesetzten

Es ist nicht zulässig, wenn Vorgesetzte, die auch die Lohnabrechnung ihrer Mitarbeiter:innen vornehmen, diese auffordern, ihre Arbeitsunfähigkeitsbescheinigungen bei ihnen einzureichen.

Ein Mitarbeiter eines Unternehmens trug vor, die Vorgesetzten, die gleichzeitig auch die Lohnabrechnung für ihn und weitere Kollegen vornähmen, würden ihn auffordern, seine Arbeitsunfähigkeitsbescheinigungen (AU-Bescheinigungen) bei ihnen einzureichen. Sie würden dies damit begründen, dass sie die Information über die Arbeitsunfähigkeit und die Dauer der Krankschreibung möglichst rasch benötigen würden, um diese bei der Lohnabrechnung berücksichtigen zu können. Er fragte an, ob dies datenschutzrechtlich zulässig sei.

Nach § 26 Abs. 3 BDSG dürfen besondere Arten personenbezogener Daten der Beschäftigten u.a. verarbeitet werden, wenn dies zur Ausübung von Rechten oder zur Erfüllung von Pflichten aus dem Arbeitsrecht erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Die (ordnungsgemäße) Lohnabrechnung ist eine Pflicht des Arbeitgebers, doch ist es nicht erforderlich, dass die Vorgesetzten, die auch die Lohnabrechnung durchführen, die AU-Bescheinigungen der krankgeschriebenen Beschäftigten erhalten. Diese sind bei der Personalstelle einzureichen, die dann die Tatsache der Krankschreibung und deren Dauer zeitnah an die Vorgesetzten weiterleiten kann, so dass auch auf diese Weise der Umstand bei der Lohnabrechnung berücksichtigt werden kann. Es ist aber im Hinblick auf die Lohnabrechnung nicht erforderlich, dass die Vorgesetzten über die anderen, in der AU-Bescheinigung enthaltenen personenbezogenen Daten, wie Krankenkasse, Versichertennummer, Name und Fachrichtung des die Bescheinigung ausstellenden Arztes, Kenntnis erhalten.

11.2 Einträge im Outlook-Kalender zu Bewerbungsgesprächen

Einträge im Outlook Kalender zu Bewerbungsgesprächen sollten keine weitergehenden Notizen und Informationen zu den teilnehmenden Bewerber:innen enthalten.

Ein Unternehmen teilte im Rahmen einer Beratungsanfrage mit, dass es die Termine für Bewerbungsgespräche im Outlook-Kalender eintrage. Es würden dort nur Vermittlungen der Agentur für Arbeit vermerkt werden. Konkret würden der Name des Bewerbers und für welche Stelle die Zuweisung sei sowie z.B. Informationen darüber wie oft ein Bewerber schon eingeladen worden und eventuell nicht gekommen sei, hinterlegt werden. Das Unternehmen fragte an, ob diese Informationen im Outlook Kalender belassen werden dürfen.

Grundsätzlich weisen wir darauf hin, dass beim Verarbeiten von Bewerber:innendaten ein geeigneter Speicherort für diese Daten zu wählen ist. Ein solcher Speicherort zeichnet sich einerseits durch ein wirksames Zugriffskonzept aus, andererseits verfügt dieser aber auch über ein passendes Löschkonzept, damit sensible Daten nicht länger als nötig aufbewahrt werden. Ein Eintragen von Bewerber:innendaten bzw. Informationen zu Bewerber:innen in den Outlook-Kalender und eine etwaige Versendung derselben im Rahmen einer Einladung weiterer Teilnehmer:innen betrachten wir als kritisch, da die beiden zuvor genannten Kriterien bei Outlook-

Kalendern in den meisten Anwendungsfällen der Praxis nicht erfüllt werden.

Regelmäßig genügt es stattdessen für die Erstellung und Versendung eines Termins, den Betreff und den Namen des/der Bewerber:in zu benennen. Bewerbungsunterlagen, aber auch Gesprächsnotizen bzw. Vermerke zu den Bewerber:innen oder geführten Bewerbungsgesprächen, sind entsprechend der Organisationsstruktur bei der für Personalangelegenheiten zuständigen Stelle sicher vor unbefugten Zugriffen aufzubewahren. Die an der Durchführung eines Bewerbungsverfahrens Beteiligten erhalten sodann die hierfür notwendigen Unterlagen bzw. ein Zugriffsrecht hierauf. Soweit im Rahmen des Bewerbungsverfahrens Notizen angefertigt werden, bedarf es diesbezüglich ebenso eines Berechtigungskonzeptes, so dass ein unbefugter Zugriff ausgeschlossen werden kann.

Gerade wenn Notizen oder Informationen im Outlook-Kalender vermerkt und mittels einer Outlook-Termineinladung versandt werden, kann aufgrund der verschiedenen Speicherorte nur erschwert sichergestellt werden, dass unbefugte Zugriffe verhindert und Bewerber:innendaten später tatsächlich gelöscht werden. Zu beachten ist des Weiteren, dass in vielen Organisationen großzügige Kalenderfreigaben bestehen, um Terminplanungen mit anderen Beschäftigten besser organisieren zu können. Dadurch, aber auch durch Vertretungsregelungen und Zugriffsberechtigungen auf ganze Postfächer, besteht die Möglichkeit, dass eine Einsichtnahme in Kalendereinträge unbeabsichtigt eröffnet wird.

Das anfragende Unternehmen haben wir deshalb ebenso darauf hingewiesen, dass der Verantwortliche nach Art. 17 Abs. 1 Buchstabe a DS-GVO personenbezogene Daten unverzüglich zu löschen hat, wenn sie für den Zweck, für den sie (rechtmäßig) erhoben oder anderweitig verarbeitet wurden, nicht mehr benötigt werden. Gerade auch vor dem Hintergrund der in der gelebten Praxis eher dürftigen Löschkonzepte bei Outlook-Kalender besteht die Gefahr von pauschalen Speicherdauern, die den Anforderungen im Umgang mit Bewerber:innendaten nicht gerecht werden. Wir haben daher das anfragende Unternehmen hinsichtlich der Löschung solcher Bewerber:innendaten aus Termineinträgen im Kalender hingewiesen. Soweit eine datenschutzrechtliche Erlaubnis für das weitere Vorhalten von Bewerber:innendaten geben sollte, müssten diese, wie bereits dargestellt, an anderer geeigneter Stelle, wie z. B. durch die Personalabteilung, sicher aufbewahrt werden, d. h. wie andere Personaldaten auch durch technische und organisatorische Maßnahmen weiterhin ausreichend geschützt werden. Eine Erforderlichkeit für eine Verarbeitung der personenbezogenen Daten könnte sich z. B. aus der Berichtspflicht des Unternehmens gegenüber der Agentur für Arbeit bzw. für den Fall eines Vorgehens gegen eine ablehnende Entscheidung ergeben.

11.3 Verpflichtung auf das Datengeheimnis

Es ist unerheblich, wenn ein:e Mitarbeiter:in sich weigert, die Verpflichtung auf das Datengeheimnis zu unterschreiben.

Ein Unternehmen fragte an, welche Folgen es habe, wenn ein:e Mitarbeiter:in sich weigere, die Verpflichtung auf das Datengeheimnis zu unterschreiben.

Zwar sieht die DS-GVO nur für die Beschäftigten von Auftragsverarbeitern ausdrücklich vor, dass diese auf das Datengeheimnis zu verpflichten sind (Art. 28 Abs. 3 Nr. 2b DS-GVO), doch trifft diese Pflicht auch Verantwortliche, mithin auch Arbeitgeber:innen und Beschäftigte - siehe Kurzpapier Nr. 19 der Datenschutzkonferenz:

https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_19.pdf

Auch wenn eine bestimmte Form der Verpflichtung nicht vorgesehen ist, sollten die Arbeitgeber:innen doch, um ihrer Nachweispflicht gemäß Art. 5 Abs. 2 DS-GVO gegenüber unserer Behörde nachkommen zu können, eine schriftliche oder elektronische Verpflichtungserklärung einholen und hierzu ein entsprechendes Formular verwenden. Die datenschutzrechtlichen Pflichten müssen Mitarbeiter:innen einhalten, unabhängig davon, ob diese die Verpflichtung unterschreiben oder nicht. Liegt ein Weigerungsfall vor, reicht es üblicherweise zur Erfüllung der Nachweispflicht aus, wenn der Arbeitgeber den Mitarbeiter auf seine Pflichten hingewiesen hat und darüber, sowie über den Umstand der Weigerung, einen Vermerk erstellt.

11.4 Kopien von Personalausweisen

Die Verarbeitung von personenbezogenen Daten aus einer Ausweiskopie ist grundsätzlich nur mit Einwilligung gem. Art. 4 Nr. 11 DS-GVO zulässig.

Ein Unternehmen teilte in seiner Anfrage mit, dass seine Außendienstmitarbeiter:innen regelmäßig bei Kund:innen, z.B. Banken oder Versicherungen, vor Ort im Einsatz seien. Die Kund:innen würden im Hinblick auf Terminvereinbarung und Zutrittsberechtigung zum Teil Kopien der Personalausweise anfordern und sich dabei auf ihr Hausrecht und ihre Sicherheitsstandards berufen. Das Unternehmen weigere sich, diese Kopien zur Verfügung zu stellen und fragte an, ob es sich richtig verhalte. Es wies noch darauf hin, dass die betreffenden Mitarbeiter:innen mit Namen, Vornamen, eventuell Geburtsdatum und Wohnort, angemeldet würden, so dass dem Kunden eine Überprüfung möglich sein müsse, dass es sich bei der am Eingang wartenden Person um den angeforderten Mitarbeiter handle.

Das Unternehmen verhielt sich korrekt. Das Kopieren des Personalausweises ist gemäß § 20 Abs. 2 S. 1 Personalausweisgesetz (PAuswG) nur durch den Ausweisinhaber selbst oder von anderen Personen mit seiner Zustimmung zulässig. Die Kopie darf nur durch den Ausweisinhaber an Dritte weitergegeben werden (§ 20 Abs. 2 S. 2 PAuswG). Da der Ausweisinhaber keine Zustimmung gegenüber den Kunden erteilt hat, gelten diese als Dritte.

Zudem bedarf es gem. § 20 Abs. 2 S. 3 PAuswG einer datenschutzrechtlichen Einwilligung des Ausweisinhabers, wenn personenbezogene Daten aus der Ablichtung heraus verarbeitet werden. Die Einwilligung muss den Vorgaben der Art. 4 Nr. 11 und 7 DS-GVO entsprechen. Auch eine Einwilligung in eine entsprechende Datenverarbeitung wurde durch den Ausweisinhaber nicht erteilt.
Spezialgesetzliche Regelungen fanden vorliegend keine Anwendung.
Für die Sicherheitsinteressen der Kund:innenen ist es zudem ausreichend, wenn sie sich den Personalausweis vorzeigen lassen und sich unter Hinzuziehung der im Vorfeld zur Verfügung gestellten Daten von der Identität des Mitarbeiters überzeugen und dies in einem Vermerk festhalten.

12

Gesundheit und Soziales

12 Gesundheit und Soziales

12.1 Reaktion von Ärzt:innen auf Google-Bewertungen im Gesundheitsbereich

Im Rahmen von Reaktionen auf Google-Bewertungen sollten Ärzt:innen genau prüfen, dass diese keine Gesundheitsdaten von Patient:innen im Internet preisgeben.

Zufriedene wie unzufriedene Patient:innen geben gelegentlich über die behandelnden Ärtz:innen Bewertungen auf Google ab. Diese wiederum antworten zum Teil auf die Bewertungen, was ebenso öffentlich im Internet abrufbar ist. Uns lagen hierbei Fälle vor, in denen in Reaktion auf die abgegebene Bewertung gesundheitsbezogene Daten von Patienten von Seiten der Ärzt:innen offengelegt wurden, beispielsweise um potentiell unrichtige Tatsachen zu widerlegen. Hatten die Patient:innen ihre Bewertung unter ihrem Klarnamen abgegeben, konnte hier jedoch ein Personenbezug unmittelbar festgestellt werden und die offengelegten Gesundheitsdaten der Person zugeordnet werden. Eine Rechtsgrundlage hierfür, insbesondere unter Berücksichtigung von Art. 9 Abs. 2 und 3 DS-GVO, gibt es jedoch in der Regel nicht, weshalb wir aufsichtlich tätig wurden. Darüber hinaus können hier auch potentiell Verletzungen der ärztlichen Schweigepflicht vorliegen, deren Feststellung und Ahndung jedoch im Zuständigkeitsbereich der zuständigen Berufskammern liegt.

Für den Fall, dass Patient:innen in der Bewertung selbst Angaben zur eigenen Person machen und Gesundheitsdaten nennen, liegt kein Datenschutzverstoß vor, wenn in der Reaktion seitens des Arztes darauf lediglich Bezug genommen wird ohne zusätzliche Gesundheitsdaten zu offenbaren.

12.2 Whatsapp-Nutzung bei Pflegediensten

WhatsApp darf von Pflegediensten zum Austausch über Patient:innen nicht eingesetzt werden.

Immer wieder wird uns zugetragen, dass Pflegedienste WhatsApp zur internen Kommunikation nutzen und dabei auch personenbezogene, insbesondere gesundheitsbezogene Daten ihrer Patient:innen austauschen. Dabei handelt es sich beispielsweise um konkrete Adressangaben, Schichtpläne, Medikationen, Fotos zur Dokumentation von Wundbehandlungen und Mitteilungen über aktuelle Erkrankungen, die häufig zudem auf Privathandys der Mitarbeiter:innen gespeichert werden. Oftmals kann der Austausch dieser Daten anhand von Chat- bzw. Gruppenchatverläufen belegt werden. Wir möchten betonen, dass wir bereits in unserem 8. Tätigkeitsbericht 2017/2018 auf die datenschutzrechtlichen Bedenken hinsichtlich der Nutzung von WhatsApp im beruflichen Umfeld hingewiesen haben sowie darauf, dass WhatsApp von Berufsgeheimnisträgern grundsätzlich nicht eingesetzt werden darf.

https://www.lda.bayern.de/media/LDA_report_08.pdf

12.3 Verarbeitung von Sozialversicherungsnummern

Sozialversicherungsnummern können auch von privaten Unternehmen verarbeitet werden, wenn die betroffenen Personen ihnen diese freiwillig übermitteln.

Von einer Krankenkasse wurden wir auf die Webseite eines Unternehmens hingewiesen, welches Personen anbietet, bei Verlust ihres Sozialversicherungsausweises in ihrem Namen einen Antrag auf Neuausstellung gegenüber den zuständigen Institutionen zu stellen. Hierzu

können die betroffenen Personen u.a. ihre Versicherungsnummer angeben.

Bei der Versicherungsnummer handelt es sich um ein Sozialdatum, dessen Verarbeitung primär durch die in § 35 SGB I genannten Stellen (sog. Leistungsträger) zu den gesetzlich festgelegten Zwecken (§ 18f SGB IV) zu erfolgen hat.

Allerdings lässt § 18g SGB IV das Recht des Betroffenen, seine Versicherungsnummer freiwillig einem Dritten mitzuteilen, unberührt, solange keine vertragliche Verpflichtung besteht, diese Nummer für eine andere als die gesetzlich vorgesehenen Verarbeitungen anzugeben. Eine solche Verpflichtung ist in den Vertragsbestimmungen des konkret untersuchten Anbieters nicht vorgesehen.

Das Geschäftsmodell des Unternehmens ist damit nicht per se unzulässig. Dennoch raten wir betroffenen Personen dazu, sich genau zu überlegen, ob sie sich nicht selbst den überschaubaren bürokratischen Aufwand der Antragstellung machen möchten und so ihre Sozialdaten nicht gegenüber Dritten preisgeben.

13

Videoüberwachung

13 Videoüberwachung

13.1 Parkraumüberwachung

Die automatisierte Kennzeichenerfassung zur Parkraumüberwachung ist regelmäßig in engen Grenzen zulässig.

Immer mehr Betreiber:innen von Parkhäusern bzw. sonstigen Parkplätzen wie z. B. Einzelhändler:innen stellen ihre Parkraumüberwachung auf automatisierte Kennzeichenerfassung um bzw. beauftragen externe Unternehmen mit einer solchen Parkraumüberwachung.

Ziel der automatisierten Parkraumüberwachung ist es, die ordnungsgemäße Nutzung, insbesondere in Hinblick auf die erlaubte Parkdauer bzw. das zu entrichtende Entgelt für die Parkplatznutzung, möglichst lückenlos zu überwachen. So können die Parkplätze für Kund:innen freigehalten werden und das Parken von Dauerparkern verhindert werden.

Üblicherweise wird dazu beim Einfahren auf den überwachten Parkplatz das Kfz-Kennzeichen erfasst und mitsamt des Datums und der Uhrzeit des Parkvorgangs gespeichert.

Bei Verlassen eines kostenpflichtigen Parkplatzes erfolgt ein Abgleich mit den zu dem Kfz-Kennzeichen hinterlegten Daten, insbesondere aber auch, ob das geschuldete Entgelt entrichtet wurde. Bei Parkplätzen, die für einen bestimmten Zeitraum kostenlos genutzt werden dürfen, erfolgt ein Abgleich dahingehend, inwieweit die vorgegebenen Höchstparkdauer überschritten wurde.

Wird die erlaubte Höchstparkdauer überschritten bzw. der für die jeweilige Parkdauer geschuldete Betrag nicht entrichtet, werden häufig Geldansprüche geltend gemacht. Hervorzuheben ist hierbei insbesondere die Vereinbarung einer Vertragsstrafe mit Hilfe Allgemeiner Geschäftsbedingungen des Parkplatzbetreibers, die bei Überschreiten der Höchstparkdauer anfällt. Zur Durchsetzung dieser Forderung auf Zahlung einer Vertragsstrafe ist es von der Rechtsprechung als zulässig anerkannt, dass das Kfz-Kennzeichen gespeichert und für eine Halterauskunft (sog. einfache Registerauskunft) verwendet werden darf, um den Halter zu ermitteln und zu versuchen, vom Halter oder von einem von diesem benannten Fahrer die Zahlung zu verlangen.

Bei einer automatisierten Parkraumüberwachung, die mit der Verarbeitung personenbezogener Daten einhergeht, kann die Einwilligung (Art. 6 Abs. 1 Buchstabe a DS-GVO) sowie bei Dauerparkern der Mietvertrag als Rechtsgrundlage in Betracht kommen (Art. 6 Abs. 1 Buchstabe b DS-GVO). Bei der Mehrheit der Verarbeitungsvorgänge dürfte als Rechtgrundlage jedoch Art. 6 Abs. 1 Buchstabe f DS-GVO einschlägig sein. Insbesondere kann die Datenverarbeitung bei einer kurzzeitigen kostenfreien Überlassung eines Parkplatzes regelmäßig nicht auf Grundlage des Leihvertrages erfolgen.

Aus datenschutzrechtlicher Sicht ist die Erfassung von Kfz-Kennzeichen durch einen privaten Parkplatzbetreiber in aller Regel nicht zu beanstanden, soweit insbesondere folgende Bedingungen eingehalten werden:

- Es ist eine Karenzzeit einzuräumen, innerhalb welcher der Parkplatz ohne Bezahlverpflichtung wieder verlassen werden kann (z.B. kein freier Parkplatz mehr vorhanden). Die erfassten Daten sind in solchen Fällen ohne Speicherung nach der Ausfahrt des Kfz zu löschen.
- Es werden nur solche Daten verarbeitet, welche für den Zweck erforderlich sind. Für den Zweck der Parkraumüberwachung ist dies das Kfz-Kennzeichen. Die Einstellungen der Kameras

bzw. der Erfassungsgeräte sind entsprechend vorzunehmen und der Erfassungsbereich zu begrenzen.

- Es muss auf die Datenverarbeitung unter Beachtung der Art. 12 ff. DS-GVO hingewiesen werden. Dieser Hinweis sollte, soweit möglich, bereits erfolgen, bevor in den überwachten Bereich eingefahren wir.
- Die gespeicherten Daten werden bei Einhaltung der maximal zulässigen Höchstparkdauer bzw. nach erfolgten Bezahlvorgang nach Verlassen des Parkplatzes, jedoch spätestens mit Ablauf des Tages gelöscht, soweit diese keinen gesetzlichen Aufbewahrungspflichten unterliegen.
- Die gespeicherten Daten bei Nichteinhaltung der Höchstparkdauer bzw. bei Nichtentrichtung der Parkgebühr werden spätestens mit dem Eingang des auf Grundlage zivilrechtlicher Vereinbarungen geforderten Geldbetrages gelöscht, soweit einer Löschung keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

14

Datenschutzverletzungen

14 Datenschutzverletzungen

Die Anzahl von Datenschutzverletzungen verbleibt auf hohem Niveau. Für die gründliche Bearbeitung der Vorfälle ist zu wenig Personal vorhanden.

Wie im vorherigen Berichtszeitraum bindet die Bearbeitung der Meldungen nach Art. 33 DS-GVO fast die kompletten personellen Ressourcen des technischen Bereichs. Trotz Optimierung der Abläufe und einer Teilautomatisierung bei der Erstellung von Abschlussmitteilungen oder Nachfragen sowie einer Spezialisierung der Mitarbeiter:innen auf bestimmte Themenfelder, ist der Berg an Meldungen regelrecht erdrückend und nicht mehr angemessen zu bewältigen.

Mengenmäßig führten die postalischen und elektronischen Fehlversendungen die Meldekategorien nach wie vor an, wenn auch eine Verringerung um 38 % stattgefunden hat. Ob nun die organisatorischen Maßnahmen bei den Verantwortlichen die Situation verbessern oder Kuvertiermaschinen mit weniger Fehlern angeschafft wurden, können wir nicht beurteilen, da derartige Meldungen bei uns bislang noch nicht zu zielgerichteten Datenschutzkontrollen geführt haben. Weiterhin kann es aber nicht ausbleiben, jede Meldung im Einzelfall zumindest kurz zu sichten, da bspw. bei betroffenen Gesundheitsdaten oder Daten von Kindern die Risikoeinschätzung der Verantwortlichen validiert werden muss. Hierbei stellen wir nach wie vor fest, dass insbesondere die Art. 34-Meldungen an die Betroffenen ungern durchgeführt werden.

Cybercrime-Vorfälle sind mit einem Plus von 35% im Jahr 2021 im Vergleich zum Vorjahr gestiegen. Dabei ist es zunehmend so, dass die Angriffe auf sehr hohem technischem Niveau erfolgt sind und die Verantwortlichen meist erst nach einer Verschlüsselung von Daten per Ransomware oder dem Missbrauch eines gekaperten Email-Kontos von der Cyberattacke erfahren. Dies führt auch dazu, dass bei den Art. 33-Meldungen, die in der Regel innerhalb von 72 Stunden nach Erkennung bei uns eingereicht wurden, in den Erstmeldungen mitunter nur wenige brauchbare Informationen enthalten sind, um die Folgen für die betroffenen Personen abzuschätzen. Stattdessen führen wir bei gravierenden Vorfällen meist am Tage des Meldeeingangs einen Erstkontakt durch, gefolgt von Telefongesprächen oder Videokonferenzen mit Geschäftsführer:innen, Datenschutzbeauftragten oder rechtlichen Vertreter:innen des betroffenen verantwortlichen Unternehmens. Durch die damit erlangten Informationen haben die technischen Mitarbeiter:innen des LDA ein bayernweit wohl einmaliges Wissen über Art der Angriffe und ausgenutzte technische und/oder organisatorische Schwachstellen, insbesondere mit Blick auf kleinere und mittlere Unternehmen. Dieses wird in der neu gegründeten Stabsstelle Prüfverfahren mitgenutzt, um Prüfschwerpunkte festzulegen und die Cyberprävention mit dem Ziel des Grundrechtsschutzes der Bürger:innen voranzutreiben.

Folgend möchten wir ein paar Vorfälle hervorheben, die im Berichtszeitraum in der Presse zu lesen waren und von Seiten des LDA aufgearbeitet wurden:

Reiseveranstalter
Ein großer Reiseveranstalter wurde Opfer eines Ransomware-Angriffs durch die Conti-Gruppe. Durch die Cyberattacke kam es nicht nur zu einer erheblichen Betriebsstörung, sondern auch zu einer Veröffentlichung einer großen Menge an personenbezogenen Daten im Darknet durch die Cyberkriminellen.

Handelskette
Ähnliches ist einer Elektro-Handelskette widerfahren: Durch einen Ransomware-Angriff waren europaweit starke Einschränkungen bis in die

lokalen Einkaufsmärkte zu spüren. Die hinter dem Angriff steckende Hive-Gruppe forderte auch hier eine sehr hohe Summe an Lösegeld für die verschlüsselten Daten.

Softwarehersteller Arztsoftware:
Ein Hersteller einer Praxissoftware mit Sitz in Hessen wurde Opfer eines Ransomware-Angriffes, der auch Auswirkungen auf bayerische Arztpraxen hatte. Obwohl der Angriff keine direkten Auswirkungen auf den Betrieb im Hinblick auf die Verfügbarkeit und somit der Arbeitsfähigkeit der bayerischen Praxen hatte, bestand jedoch die Möglichkeit des Datenabflusses, der von uns im Rahmen der Aufarbeitung der eingegangenen Meldungen untersucht wurde, jedoch letztendlich nicht bestätigt werden konnte.

E-Commerce Dienstleister:
Bei einem E-Commerce-Dienstleister mit Sitz in Nordrhein-Westfalen, kam es zu einem massiven Datenleck aufgrund der eingesetzten Software für den Online-Handel. Betroffen waren dabei in Bayern primär kleinere Online-Händler, die ihre Waren auf Verkaufsplattformen angeboten und dafür das Unternehmen als Dienstleister eingesetzt hatten.

IT-Dienstleister:
Ein IT-Dienstleister wurde 2021 Opfer der Ransomware-Gruppierung REvil. Dieser Angriff gehörte zu den sogenannten Supply-Chain-Angriffen, bei denen ein zentraler IT-Dienstleister angegriffen wird und sich dadurch die Schadsoftware auf alle Unternehmen ausbreiten kann, die eben diesen Dienstleister bzw. dessen Software nutzen. Aus diesem Grund hatte der Angriff auch weitreichende Folgen für bayerische Unternehmen, deren Systeme aufgrund der eingesetzten Software ebenfalls verschlüsselt wurden.

Mit Blick auf das hohe technische Niveau und der weiterhin erfolgreichen Angriffe auf bayerische Unternehmen, sei es der Mittelstand oder ein Konzern, stellen wir häufig fest, dass ein Angriff wie aus dem Lehrbuch innerhalb kürzester Zeit erfolgreich durchgeführt wird. Vorhandene Schutzmaßmaßnahmen, die durchaus in den Bereich der Standard-IT-Sicherheit fallen, wurden mitunter in Minuten umgangen. Bei der Analyse der Vorfälle haben wir allerdings festgestellt, dass fast alle Angriffe durch wirksamere technische und organisatorische Maßnahmen zur Cybersicherheit nach Art. 32 DS-GVO, die nicht einmal zwingend teurer gewesen wären, hätten verhindert werden können. Dies bestärkt uns in der Entscheidung der Durchführung von anlasslosen Kontrollen durch die Stabsstelle Prüfverfahren, da ein funktionierender Datenschutz vor Cyberangriffen möglich ist und das LDA durch die Vielzahl unterschiedlicher Meldungen auch effektive Maßnahmenkataloge zur Verfügung stellen kann. Um sicherstellen zu können, dass diese überhaupt umgesetzt werden, ist aber eine deutliche personelle Stärkung des technischen Personals im LDA erforderlich. Denn eines ist gewiss: Hat sich ein Angreifer erstmal im Netzwerk eines Unternehmens eingenistet (was mitunter keine 5 Minuten dauert), dann ist es meistens zu spät und die personenbezogenen Daten der Mitarbeiter:innen und Kund:innen sind in größter Gefahr.

15

Technischer Datenschutz und Informationssicherheit

15 Technischer Datenschutz und Informationssicherheit

15.1 Ransomware-Angriffe

Die Anzahl erfolgreicher Cyberangriffe mit dem Ziel der Verschlüsselung von personenbezogenen Daten bleibt in Bayern auf hohem Niveau.

Auch im Jahr 2021 haben sogenannte Ransomwareangriffe viele Unternehmen in Bayern getroffen. Wir haben insgesamt 314 Meldungen nach Art. 33 erhalten, die in diese Kategorie eingeordnet werden können, was einer Steigerung von 27% zu 2021 entspricht.

Die Vorgehensweise der Angreifergruppierungen ähneln sich dabei zunehmend. Nachdem in einem ersten Schritt meist eine Mail mit einem Schadcodelink geklickt und das im Nachgang sich öffnende Office-Dokument bestätigt wurde, schalten sich die Angreifer:innen „von Hand" auf ein derart kompromittiertes System. Mitunter werden auch Sicherheitslücken in über das Internet erreichbaren Softwarekomponenten ausgenutzt oder Passwörter für den Fernzugang (z.B. aus dem Homeoffice) in Erfahrung gebracht. Nachdem sich die Angreifer:in lokale Administrationsrechte (durch unzureichend konfigurierte interne Systeme oder schwache verwendete Passwörter) beschafft hat, wird im lokalen Netzwerk nach lohnender Beute in Form von Word, Excel, PDF oder Grafikdateien, mitunter sogar komplette Datenbanken gesucht und auf einen Server der Angreifenden im Internet kopiert. Danach werden so viele IT-Systeme und Daten verschlüsselt, wie es unmittelbar möglich ist, ehe sehr prägnant eine Erpressernachricht platziert wird.

In dieser „Ransomware-Note" wird auf einen – meist im Tor-Netzwerk befindlichen – Kommunikationskanal verwiesen, über den mit dem/der Angreifer:in in Form von Chat-Nachrichten in Kontakt getreten werden kann. Die Angreifer:innen verweisen meist darauf, dass die entwendeten Daten auf einer Darknet-Seite veröffentlicht werden, sollte das geforderte Lösegeld in einer bis zu 8-stelligen Größenordnung nicht gezahlt werden (sog. Double-Extorsion). Ziel ist mit dieser Aktion Druck auf die Unternehmen aufzubauen, die Rufschäden und Wettbewerbsnachteile fürchten.

In Einzelfällen wird auch angedroht, dass die entwendeten Daten selbst für weitere Angriffe und Belästigungen auf Kund:innen und Geschäftspartner:innen verwendet würden, sollte – da möglicherweise ein Backup vorhanden ist – von einer Lösegeldzahlung Abstand genommen werden.

Das LDA stuft derartige Ransomwarevorfälle so ein, dass von einer maximalen Eintrittswahrscheinlichkeit eines Datenmissbrauchs der entwendeten Daten ausgegangen werden muss, da diese in die Hände von kriminellen Gruppierungen gefallen sind. Ob dieser Sachverhalt nicht nur eine Meldepflicht nach Art. 33 DS-GVO sondern auch die weitergehenden Pflichten nach Art. 34 DS-GVO auslöst, hängt wesentlich von der Sensitivität der betroffenen Daten ab. Eine Art. 33 Meldung ist damit in der Regel erforderlich, eine Art. 34 Meldung nur bei sehr unsensitiven Daten (z.B. berufliche Kontaktdaten des Vertriebs, die als allgemein bekannt angesehen werden können) nicht.

Lösegeldzahlungen haben unserer Ansicht nach keine risikosenkende Wirkung. Dem Versprechen, diese Daten weder weiterzuverkaufen noch anderweitig zu verwenden, sondern stattdessen zu löschen, kann bei cyberkriminellen Vereinigungen keine hinreichende Bedeutung zuerkannt werden.

Letztendlich bleibt den Verantwortlichen nur übrig, die eigenen Maßnahmen zur Abwehr von Ransomwareangriffen zu überprüfen und ggf.

robuster zu machen. Sollen Angreifer:innen einmal die Kontrolle über das Netzwerk eines Unternehmens erlangt haben, dann ist es meist zu spät. Aus diesem Grund hat das LDA als Auftaktprüfung der neuen Stabsstelle Prüfverfahren auch die Ransomware-Prävention (siehe Kapitel 14) gewählt.

15.2 Exchange-Server Sicherheitslücke

Anfang März 2021 wurde bekannt, dass vier Zero-Day-Sicherheitslücken in Microsoft Exchange-Servern existierten, die in großem Stil automatisiert ausgenutzt wurden.

Professioneller Umgang mit Sicherheitslücken sollte längst zum Alltag jedes IT-Betriebes gehören. Unabhängig von der Art und der Größe des Unternehmens ist es vor allem bei IT-Systemen, die über das Internet erreichbar sind, neben einer richtigen Konfiguration von entscheidender Bedeutung, bekannt gewordene Schwachstellen möglichst zeitnah zu beheben. Automatisierte Scans quer durch das Internet ermöglichen es ansonsten Angreifer:innen aus der Ferne, auf Knopfdruck einen Überblick über verwundbare Server zu erhalten und nach Belieben Cyberattacken darauf zu starten. Das Zeitfenster zum Beheben von Sicherheitslücken ist somit meistens sehr gering.

Mit der Pressemitteilung vom 05.03.2021 informierte das BSI über eine neue, außerordentlich kritische Gefährdungslage, die bei den auch in Deutschland sehr weit verbreiteten Exchange Servern sofortiges Handeln der betroffenen Unternehmen erforderte. Durch die kombinierte Anwendung der neuen Exchange-Schwachstellen war eine Code-Ausführung aus der Ferne für Angreifer möglich. Das BSI ging davon aus, dass die so verwundbaren Systeme mit hoher Wahrscheinlichkeit bereits attackiert und mit Schadsoftware infiziert waren.

Erfolgreiche Attacken setzten allerdings unter anderem voraus, dass eine nicht-vertrauenswürdige Verbindung zu einem Exchange Server etabliert werden konnte, z. B. über Outlook Web Access. Laut Informationen des BSI waren Server, welche nur per VPN erreichbar waren oder eben solche nicht-vertrauenswürdige Verbindungen blockierten, nicht betroffen. Dennoch ging das BSI nach eigenen Schätzungen von einer fünfstelligen Anzahl an betroffenen Systemen alleine in Deutschland aus.

Das Einspielen der von Microsoft bereitgestellten Updates sollte von Exchange-Administrator:innen unverzüglich durchgeführt werden. Microsoft stellte zudem ein eigenes Prüf-Skript für betroffene Betriebe zur Verfügung. Mit diesem konnten die Systemadministrator:innen Anhaltspunkte dafür finden, ob der eigene Exchange Server erfolgreich angegriffen wurde.

Viele Unternehmen waren verunsichert, inwieweit der eigene Betrieb gefährdet ist und personenbezogene Daten tatsächlich abgegriffen worden sind. Während zu Beginn laut Microsoft primär Forschungseinrichtungen mit Pandemie-Fokus, Hochschulen, Anwaltsfirmen und Organisationen aus dem Rüstungssektor angegriffen wurden, stand schnell auch für uns die Annahme im Raum, dass Angriffe branchenunabhängig erfolgten.

Unabhängig von einer genaueren Bewertung eines möglichen datenschutzrechtlichen Schadens einer Cyberattacke waren Verantwortliche mit gefährdeten Systemen zunächst verpflichtet, umgehend die bereitgestellten Patches für ihre Systeme zu installieren und damit ihrer Verpflichtung gemäß Art. 32 DS-GVO nachzukommen. Verantwortliche, die dieser Aufgabe zu spät nachgekommen waren, traf angesichts des auch durch die zentrale Funktion von Exchange Servern im Kommunikationssystem der Unternehmen außerordentlich erhöhten Sicherheitsrisikos unabhängig von weiteren Befunden die Verpflichtung, die Sicherheitslücke als Datenschutzverletzung binnen 72 Stunden zu melden,

da von einer automatisierten Ausnutzung der Lücke ausgegangen werden musste.

Angesichts des hohen Schadenspotentials bei Ausnutzung der Sicherheitslücke und der deutlich erhöhten Wahrscheinlichkeit solcher Angriffe bestanden auch für Verantwortliche, die das erforderliche Update bereits zeitnah durchgeführt hatten, weitere Untersuchungspflichten: Um auszuschließen, dass ein Einspielen der Microsoft-Updates zu spät durchgeführt und zwischenzeitlich Schadcode installiert wurde, waren sämtliche betroffenen Systeme zu überprüfen. Erkannte man bei dieser Überprüfung Hinweise auf Datenschutzverletzungen, etwa sogenannte Hintertüren, war in diesen Fällen eine Meldung an die Datenschutzaufsichtsbehörde durchzuführen, da dann für die betroffenen Personen ein Risiko bestand.

Wir haben das LDA-Cyberlabor eingesetzt, um Schwachstellen zu identifizieren und betroffene bayerische Unternehmen auf die akute Gefährdungslage hinzuweisen. Das LDA hatte dafür in einem ersten Prüflauf am 08.03.2021 stichprobenartig 16.502 bayerische Systeme auf ihre mögliche Verwundbarkeit untersucht. Bei den Organisationen, die auf eine Microsoft Exchange-Kommunikationsstruktur setzten, wurde kontrolliert, ob der notwendige Patch-Level zum Schließen der Lücken vorhanden war. Bereits im ersten Prüflauf wurde eine dreistellige Zahl potentiell verwundbarer Server identifiziert, deren Verantwortliche umgehend über die datenschutzrechtlichen Verpflichtungen und Konsequenzen unterrichtet wurden.

Aufgrund der Vielzahl betroffener Firmen konnte im Regelfall keine Individualberatung stattfinden. Deshalb etablierte das LDA einen Frage-und-Antwort-Bereich (FAQ) auf seiner Website.

.

15.3 Cyberabwehr Bayern

Die im letzten Tätigkeitsbericht bereits vorgestellte Cyberabwehr Bayern, eine Kooperationsplattform bayerischer Behörden mit Cybersicherheitsaufgaben, spielte auch im Berichtszeitraum für den technischen Datenschutz eine wichtige Rolle. Wie in Kapitel 14 Datenschutzverletzungen und Kapitel 16 Datenschutzkontrollen erkennbar, ist der Schutz der Betroffenen vor Cyberangriffen mittlerweile eine der wichtigsten Aufgaben des technischen Datenschutzes. Sicherheitsvorfälle werden dabei zum einen in großer Anzahl von Seiten der Verantwortlichen an uns gemeldet, zum anderen sind viele dieser Sachverhalte insbesondere auch im Rahmen strafrechtlicher Ermittlungen bei anderen Behörden vorhanden. Durch den regelmäßigen Austausch zu Bedrohungslagen trägt die Cyberabwehr Bayern zur effizienten Abstimmung und zur effektiven Bearbeitung deutlich bei. Diese Zusammenarbeit kann als Erfolg auf der ganzen Linie betrachtet werden. Insbesondere die in Artikel 32 DS-GVO benannte Prävention vor Angriffen aus dem Internet stellt einen wichtigen Baustein des Datenschutzes in der Cybersicherheitsarchitektur in Bayern dar, da Maßnahmen zum Schutz personenbezogener Daten nicht nur angeregt, sondern im Zweifelsfall auch aufsichtlich angeordnet werden können.

16

Datenschutzkontrollen

16 Datenschutzkontrollen

16.1 Neu gegründete Stabstelle Prüfverfahren

Regelmäßige fokussierte Prüfungen sollen einer kontinuierlichen Kontrolle bayerischer nicht-öffentlicher Verantwortlicher dienen sowie mit Hilfe der begleitenden Veröffentlichung der Prüfbögen und weiterführender Informationen zur Eigenkontrolle der jeweiligen Prüfungsbereiche anregen.

Mit der Prüfung „Ransomware" hat die im Herbst 2021 neu gegründete Stabstelle Prüfverfahren des LDA den Startschuss für eine Reihe anlassloser fokussierter Kontrollen gegeben. In kurzen Abständen werden seitdem standardisierte schriftliche und auch automatisiert über das Internet ausgeführte Prüfungen mit klarer Schwerpunktsetzung durchgeführt. Begleitend werden die Prüffragen sowie Informationen zu dem jeweiligen Prüfkomplex auf unserer Webseite veröffentlicht. Künftige Themenbereiche werden zudem bereits vorangekündigt.

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

Die Stabsstelle Prüfverfahren wird durch erfahrene Mitarbeiter:innen des LDA geleitet, die sowohl die Seite des technischen Datenschutzes und der rechtlichen Bewertung abdecken. Für die Durchführung einzelner fokussierte Prüfungen findet eine Zusammenarbeit mit den auf das jeweilige Prüfthema spezialisierten Bereiche und Mitarbeiter:innen des LDA statt. Die Prüfthemen der fokussierten Prüfungen sind in die jährlich festgelegte Prüfstrategie des LDA, welche vom Vizepräsidenten verantwortet wird, eingebettet.

Ziel der regelmäßigen fokussierten Prüfungen ist es einerseits, die datenschutzrechtlichen Kontrollen der nicht-öffentlichen Stellen in Bayern auszuweiten. Andererseits soll durch die begleitende Bereitstellung von Informationen das Augenmerk auch der Datenschutzbeauftragten auf die jeweils geprüften oder zur Prüfung anstehenden Thematiken gelenkt werden. Insbesondere sollen die betrieblichen Datenschutzexperten als Multiplikatoren gewonnen werden, um gemeinsam den Schutz der bayerischen Unternehmen zu erhöhen. Die fokussierten Prüfkataloge bieten ihnen einfache Werkzeuge für interne Kontrollen und Schulungen.

Da in zeitlicher Nähe zu der Auftaktprüfung ein verstärktes Aufkommen sogenannter Ransomware-Attacken registriert werden konnten, wurde dies als Prüfthema für die erste fokussierte Prüfung einer ganzen Prüfreihe der Stabsstelle Prüfverfahren ausgewählt. Bei den Ransomware-Attacken handelt es sich um Sicherheitsvorfälle, bei denen Systeme der betroffenen Verantwortlichen angegriffen, die gespeicherten Daten verschlüsselt und die Opfer dadurch zu einer Lösegeldzahlung erpresst werden. Nicht selten führen diese Art von Cyberattacken zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen, häufig zudem zu einem enormen wirtschaftlichen Schaden für die angegriffene Organisation. Ziel der Prüfung ist, mit fünf zielgerichteten Prüffragen die wichtigsten Sicherheitsbereiche abzufragen sowie weitere Informationen für einen umfassenden Schutz anzubieten.

17

Bußgeldverfahren

17 Bußgeldverfahren

17.1 Bericht aus der Zentralen Bußgeldstelle

Im Berichtszeitraum wurden 11 Bußgeldbescheide erlassen. Zwei der elf Bußgeldbescheide wurden jeweils nach Einlegung eines Einspruchs an das zuständige Amtsgericht übersandt. Bis zum Stichtag 31.12.2021 wurden noch keine Entscheidungen gefällt bzw. die Einsprüche auch nicht zurückgenommen.

Zum Ende des Berichtszeitraums befanden sich bei der Zentralen Bußgeldstelle noch ca. 60 weitere Vorgänge in Bearbeitung.

Bei den sanktionierten Verstößen handelte es sich unter anderem um die unbefugte Verwendung von Daten aus Corona-Kontaktlisten, nicht erteilte Auskünfte nach Art. 15 DS-GVO, eine unberechtigte Bonitätsabfrage und den unzulässigen Betrieb von Dashcams, wobei die Verstöße sowohl durch natürliche Personen als auch Unternehmen begangen wurden.

Im Berichtszeitraum mussten wir eine vermehrte Nutzung von Dashcams mit Tonaufnahmen feststellen.

In diesem Zusammenhang ist insbesondere ein Verfahren hervorzuheben:

Nach einem Auffahrunfall, bei dem ein Taxifahrer die Rotschaltung einer Ampel missachtet hat, wurde die Polizei auf eine in dem verunfallten Taxi installierte Dash-Cam aufmerksam. Diese Dashcam filmte eine Vielzahl anderer Fahrzeuge und Passanten/Fahrradfahrende, die sich im öffentlichen Straßenverkehr vor dem Fahrzeug befanden und war mit einer aktivierten Audiofunktion ausgestattet.

Ein nach Abgabe an die zuständige Staatsanwaltschaft eingeleitetes Ermittlungsverfahren gegen den Geschäftsführer persönlich wegen Verletzung der Vertraulichkeit des Wortes wurde eingestellt und zur Verfolgung einer Ordnungswidrigkeit zuständigkeitshalber an uns (zurück)gegeben.

Mit dem von uns erlassenen Bußgeldbescheid gegen das Unternehmen wurden sodann sowohl der Verstoß durch die unzulässigen Bildaufnahmen als auch der Tonaufnahmen geahndet:

Die Anfertigung von Videoaufnahmen bedeuteten einen Verstoß gegen Art. 5 Abs. 1 Buchstabe a) DS-GVO, Art. 6 Abs. 1 DS-GVO, da keine Rechtsgrundlage für die permanente Überwachung des öffentlichen Raumes gegeben war. Insbesondere waren die Voraussetzungen des Art. 6 Abs. 1 Buchstabe f) DS-GVO nicht erfüllt.

Auch in der Anfertigung von Tonaufnahmen wurde eine unzulässige Datenverarbeitung gesehen. Über die in den Verkehrsraum gerichteten Kamera hinaus, stellte die zusätzliche Überwachung der beschäftigten Taxifahrer:innen einen Verstoß gegen Art. 5 Abs. 1 Buchstabe a), Art. 6 Abs. 1 DS-GVO, § 26 BDSG dar. Das Anfertigen der heimlichen Tonaufnahmen konnte weder auf Art. 6 Abs. 1 Buchstabe b) DS-GVO i.V.m. § 26 Abs. 1 S. 1 BDSG noch auf Art. 6 Abs. 1 Buchstabe f DS-GVO gestützt werden.

Gegen diesen Bußgeldbescheid wurde Einspruch eingelegt, der jedoch in der Hauptverhandlung, die außerhalb des Berichtszeitraums stattfand, zurückgenommen wurde. Die Entscheidung ist damit rechtskräftig.

Stichwortverzeichnis

R

S

T

U

V

W

Z

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 18
91522 Ansbach

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