Bayerisches Landesamt für
Datenschutzaufsicht

13. Tätigkeitsbericht

2023

13. Tätigkeitsbericht des Bayerischen Landesamts für Datenschutzaufsicht für das Jahr 2023

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

Titelbild: Midjourney „Art drawing a complex labyrinth ballpoint pen"

Vorgelegt im Februar 2024 – Michael Will, Präsident

Das Datenschutzjahr 2023 – voller Herausforderungen

Stand der Tätigkeitsbericht 2022 nicht zuletzt wegen des Marktstarts allgemein zugänglicher KI-Anwendungen noch unter dem Motto „Das Jahr der Zeitenwende", behandelt unser Bericht über das Folgejahr nunmehr einen Abschnitt außerordentlich hoch verdichteter Ereignisse und Entwicklungen. Egal ob in internen Abstimmungen, in unseren zahlreichen Begegnungen mit Vertreterinnen und Vertretern der Datenschutzpraxis oder den (Beratungs-) Gesprächen mit Unternehmen und Vereinen - immer wieder begegnete uns das Wort der „Herausforderungen" gleichsam als Leitmotiv des Datenschutzjahrs 2023.

Weichenstellungen durch den EU-Gesetzgeber und den Europäischen Gerichtshof

Wie ein Konzentrat der unterschiedlichen Diskussionsfelder des zurückliegenden Jahres charakterisieren die letzten Dezembertage ein Jahr, das wie kaum ein anderes durch Entscheidungen des Europäischen Gerichtshofs (EuGH) von unmittelbarer Alltagsrelevanz und den Start neuer europäischer Digital-Rechtsakte geprägt wurde: Während die deutsche Datenschutzfamilie am 15.12.2023 mit Festakten zum 40-jährigen Jubiläum des Volkszählungsurteils des Bundesverfassungsgerichts noch an die Geburtsstunde des Datenschutzes als „Recht auf informationelle Selbstbestimmung" erinnerte, markierten vor allem der 09.12.2023 mit dem Abschluss des Trilogs zur KI-Verordnung und auch der 22.12.2023 mit der Veröffentlichung des Data Act im Amtsblatt der Europäischen Union den Startpunkt neuer, weit über den Datenschutz hinausreichender Regulierungen von Technologien und Datenverarbeitungszwecken.

Anwendungen Künstlicher Intelligenz und neue Geschäftsmodelle des Teilens von Daten schaffen grundlegend veränderte Risiken für den Schutz personenbezogener Daten, die auch dann – oder vielleicht gerade deshalb – Datenschutzaufsicht und Datenschutzpraxis beschäftigten werden, obwohl doch die neuen Regelungen (vordergründig) bestehende datenschutzrechtliche Anforderungen unberührt lassen.

Ebenso bedeuten alleine schon die im Dezember 2023 verkündeten Datenschutz-Entscheidungen des EuGH Weichenstellungen für zentrale Vollzugsfragen des Datenschutzes, die die weitere Anwendung der DS-GVO fünf Jahre nach ihrem Geltungsbeginn bestimmen werden: so klärte der Gerichtshof mit seinen Entscheidungen vom 05.12.2023 (Rs. C-683/21 und C-807/21) die Maßstäbe zur Haftung von Verantwortlichen in datenschutzaufsichtlichen Bußgeldverfahren. Seine weiteren Urteile vom 07.12.2023 (Rs. C-634/21, C-26/22 und C-64/22) definierten die Grenzen der Datenverarbeitungsbefugnisse von Wirtschaftsauskunfteien, konturierte das Verbot automatisierter Einzelfallentscheidungen sowie die Maßstäbe der gerichtlichen Überprüfung datenschutzaufsichtlicher Entscheidungen. Mit seinem Urteil vom 14.12.2023 (C-340/21) ermöglichte der EuGH schließlich, jedenfalls dem Grunde nach, Schadensersatzansprüche Betroffener nach einem im Sinne von Art. 33 DS-GVO meldepflichtigen Cyberangriff. Diese fünf Entscheidungen komplettieren eine mit mehr als 20, teils im Wochentakt ergangenen Entscheidungen, außerordentlich produktive Jahresbilanz des EuGH zum Datenschutz.

Datenschutzaufsicht unter den Bedingungen allgegenwärtigen Wandels

Für den datenschutzaufsichtlichen Alltag ergeben sich allein schon aus der hier nur kurz skizzierten Dynamik von Rechtsprechung und Gesetzgebung neue Aufgabenstellungen: Die hohe Produktivität der Rechtsprechung gibt immer wieder Anlass, Mitarbeitende genauso wie

die Datenschutzpraxis zu sensibilisieren und die Vollzugspraxis laufend anzupassen, so etwa beim nun klaren Erfordernis der Nennung von Datenempfängern nach der grundlegenden Entscheidung des EuGH vom Jahresbeginn zur Reichweite des Auskunftsrechts (Urt. v 12.01.2023, C-154/21). Der vorliegende Tätigkeitsbericht fasst diese im Jahr 2023 sehr konzentriert aufgetretenen Fragestellungen zu Betroffenenrechten daher in einem Querschnittsbeitrag (Abschnitt 5) zusammen.

In gleicher Weise bestimmend für das Jahr 2023 waren technische und rechtliche Fragen der Nutzung von Künstlicher Intelligenz, die nicht nur Gegenstand der Rechtspolitik sind, sondern zunehmend spürbar auch bayerische Unternehmen beschäftigen. Dieser Tätigkeitsbericht behandelt einzelne Facetten dieses Themenkomplexes deshalb sogar in zwei Darstellungen, einer über die Arbeit des BayLDA-Cyberlabors und zur Prüfung von Schwellwertanalysen (Abschnitte 16.1 und 17.1). Letzterer beleuchtet die auch bei der Nutzung von Künstlicher Intelligenz regelmäßig zu prüfende Erforderlichkeit einer Datenschutz-Folgenabschätzung.

Ab März 2024: KI-Beauftragte(r) im BayLDA

Gleichwohl bleibt all dies nur ein erster, kurzer Auftakt und eine Vorausschau auf künftige Handlungserfordernisse. Zwar hat sich das BayLDA im Frühjahr 2023 gemeinsam mit anderen deutschen und europäischen Datenschutzaufsichtsbehörden an der Prüfung des damals noch nicht in der EU ansässigen Unternehmens Open AI als Anbieter des populären KI-Dienstes ChatGPT beteiligt und begleitet diese Prüfverfahren auch weiterhin. Gegenstand dieser Prüfung sind jedoch alleine solche Anforderungen, die sich heute – genauso wie künftig nach Geltungsbeginn der europäischen KI-Verordnung – aus der DS-GVO für die Verarbeitung personenbezogener Daten bei der Nutzung von KI-Anwendungen ergeben.

Ob diese, in der DS-GVO festgeschriebene Überwachungszuständigkeit dann beispielsweise durch Zuweisung von weiteren, aus der KI-Verordnung stammenden Aufgaben an das BayLDA ergänzt und gewissermaßen „in einer Hand" zusammengeführt wird, ist bislang offen.

Zu unserem Bedauern bestehen angesichts der langwierigen Unsicherheiten über die Verabschiedung des KI-Rechtsaktes auf EU-Ebene im Bund und in der Folge auch in den Ländern anscheinend derzeit allenfalls vage politische Vorüberlegungen zur künftigen Verteilung von Aufsichtszuständigkeiten. Demgegenüber sind in anderen Staaten, wie Italien oder Frankreich, bereits heute schon Vorbereitungsarbeiten eingeleitet, um die jeweils heimischen Unternehmen und Behörden wirksam bei ihren Entwicklungs- und Nutzungsentscheidungen im Bereich Künstlicher Intelligenz zu begleiten und zu unterstützen. Gemeinsam mit den übrigen deutschen Datenschutzaufsichtsbehörden sehen wir daher mit Sorge, dass die wichtige und mit zwei Jahren auch knapp bemessene Zeit zum Aufbau funktionsfähiger Vollzugs- und Beratungsstrukturen bislang ungenutzt verstreicht.

Angesichts der erheblichen Bedeutung, die der Koalitionsvertrag der bayerischen Regierungsparteien 2023 der Förderung von Künstlicher Intelligenz, insbesondere auch in den Bereichen wissenschaftlicher Innovation mit hohen Investitionsversprechen, einräumt, wäre es nur folgerichtig, die Entwicklung praxisnaher Beratungs- und Vollzugsstrukturen zur Unterstützung bayerischer Unternehmen bei ihren schon heute anstehenden Nutzungsentscheidungen mindestens genauso nachhaltig einzuleiten. Um trotz der noch offenen Zuständigkeitsabgrenzungen zwischen Bund und Ländern über die künftigen Aufgaben der KI-Aufsicht für ratsuchende Unternehmen jedenfalls eine erste, sichtbare Anlaufstelle zu bieten, wird das BayLDA zum März 2024 die Funktion eines KI-Beauftragten einrichten. Erste Hilfestellungen

zur datenschutzkonformen Nutzung von Künstlicher Intelligenz stehen bereits seit Januar 2024 auf der Homepage des BayLDA bereit.

Datenschutzaufsicht 2023 – immer noch weit unter Sollstärke

Die Dynamik von Gesetzgebung und Rechtsprechung im Jahr 2023 steht weiterhin im scharfen Kontrast zur Entwicklung der Ressourcen des BayLDA. Auch wenn der Bayerische Staatsminister des Innern im Rahmen seiner übergeordneten Ressortverantwortung im Jahresverlauf zumindest zwei zusätzliche Planstellen für das BayLDA im Wege haushaltsrechtlicher Vollzugsentscheidungen zur Verfügung gestellt hat, verbleibt doch weiterhin ein mittlerweile überdeutlicher Aufbau-Rückstand. Dieser zwingt das BayLDA in allen Bereichen und tagtäglich zur Zurückstellung von Vollzugsaufgaben.

Die gegenüber 2023 nochmals angehobene Zahl von 47 angemeldeten Planstellen für den Doppelhaushalt 2024/25 (2023: 28 Planstellenanmeldungen, von denen nur im Rahmen des Haushaltsvollzugs während des Jahres zwei zur Verfügung gestellt wurden) und eine zweistellige Zahl angemeldeter Stellenhebungen sind daher überdeutlicher Beleg eines strukturellen, dennoch vom Haushaltsgesetzgeber über nunmehr mehrere Jahre ausgeblendeten Ausstattungsrückstands, auf den wir bereits in den zurückliegenden Jahren auch an dieser Stelle nachdrücklich hingewiesen haben. Etwaige zusätzliche, neue Vollzugsaufgaben auf Grund der EU-Digitalrechtsakte und insbesondere der KI-Verordnung sind bei diesen Bedarfsanmeldungen noch nicht einmal berücksichtigt, da deren Verabschiedung zum Zeitpunkt der bereits sehr frühzeitigen Haushaltsanmeldung im März 2023 noch nicht hinreichend gesichert war.

Hintergrund und Begründung des Aus- und Umbaubedarfs des BayLDA sind damit alleine die bereits in den vergangenen Jahren aufgezeigten qualitativen und quantitativen Aufgabenzuwächse nach Geltungsbeginn der DS-GVO. Deren haushaltsrechtliche Nichtberücksichtigung über viele Jahre hinweg führt nicht nur zu verfassungsrechtlich fragwürdigen Bewertungen einzelner Funktionsträger, sondern auch zu unionsrechtlich für Betroffene nicht hinzunehmenden Verkürzungen ihres Anspruchs auf aufsichtliche Überprüfung von Datenverarbeitungen durch bayerische Unternehmen.

Mit seiner (weiteren) Entscheidung vom 07.12.2023 in der Rechtssache „Schufa" (C-26/22 und C-64/22) hat der EuGH bestätigt, dass sich die gerichtliche Kontrolle im Falle eines Rechtsbehelfs Betroffener gegen die Zurückweisung ihrer Beschwerde durch die Aufsichtsbehörde nicht darauf beschränken darf, ob sich die Aufsichtsbehörde mit der Beschwerde befasst, diese angemessen untersucht und den Beschwerdeführenden angemessen über ihre Ergebnisse unterrichtet hat. Vielmehr ist, so der EuGH, eine vollständige inhaltliche (!) Überprüfung aufsichtlicher Entscheidungen durch ein Gericht geboten (Rn. 62, 63 der o.g. Entscheidung, siehe hierzu auch bereits unsere Hinweise im Vorwort des 12. Tätigkeitsberichts). Eine Mittelausstattung, die der Aufsichtsbehörde mangels ausreichender Ressourcen keine andere Möglichkeit lässt, als Beschwerden in mehr als einem Drittel der Eingänge ggf. nicht nur inhaltlich zu knapp, sondern schlicht gar nicht innerhalb der von der DS-GVO vorgegebenen Drei-Monatsfrist zu behandeln (so wiederholt auch im Berichtszeitraum geschehen), steht mit diesen Maßstäben des EuGH an unabhängige staatliche Überwachung erkennbar nicht mehr in Einklang.

Der Mitte Februar veröffentlichte Entwurf der Staatsregierung für den Doppelhaushalt 2024/25 bleibt mit der Zuweisung von jeweils nur fünf Planstellen pro Haushaltsjahr an das BayLDA damit kaum mehr als der sprichwörtliche „Tropfen auf den heißen Stein". Er blendet die Handlungserfordernisse bei der staatlichen Kontrolle von Datenmissbrauch, noch mehr aber bei der mittlerweile nahezu zum Erliegen gekommenen Beratungstätigkeit für bayerische

Unternehmen und Vereine im Datenschutz aus und wird damit dem Selbstverständnis eines auf leistungsfähigen staatlichen Rahmenbedingungen aufbauenden, global be- und geachteten Digitalstandortes weiterhin nicht gerecht.

Datenschutzaufsicht 2024 – ein Ausblick

Die Herausforderungen des Datenschutzjahres 2023 mit seiner Verdichtung höchstrichterlicher Entscheidungen hoher Tragweite für die Datenschutzpraxis und den verschiedenen Initiativen des europäischen sowie des nationalen Gesetzgebers, von der KI-Verordnung bis zur BDSG-Novelle, sind nichts anderes als Vorboten eines weiteren Entwicklungssprungs des Datenschutzrechts. Neue technologische Entwicklungen genauso wie neue Geschäftsmodelle der Datenökonomie werden eine Vielzahl neuer Fragestellungen über Verantwortlichkeiten, Rechtsgrundlagen oder Betroffenenrechte nach sich ziehen, während sich gleichzeitig die Anwendung der DS-GVO mehr und mehr von einem traditionellen, noch national geprägten Verständnis der ersten Jahre hin zu einem zunehmend stabilen und kohärenten, europäischen Rahmen des Datenschutzrechts fortentwickelt.

Hohe Bedeutung haben damit weiterhin die Abstimmung zwischen den Datenschutzaufsichtsbehörden auf nationaler genauso wie auf europäischer Ebene, zunehmend aber auch die fachübergreifende Kooperation mit anderen Aufsichtsbehörden, wie sie sich im Wettbewerbsrecht etabliert hat und insbesondere im breit gefächerten Bereich der künftigen KI-Aufsicht sowie bei der Netz- und Informationssicherheit (NIS-2-Richtlinie) geboten sein wird.

Für das BayLDA bleibt damit nur noch mit dem bereits laufenden Jahr 2024 ein schmales Zeitfenster, um Entwicklungsrückstände aufzuholen, seine bisherigen Kernkompetenzen zu stärken und sich für diese gewandelten Vollzugs-, Beratungs- und Kooperationsaufgaben zu wappnen, um so die datenschutzgerechte Digitalisierung von Unternehmen und Vereinen in Bayern effektiv und konstruktiv begleiten zu können.

Ansbach, im Februar 2024

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

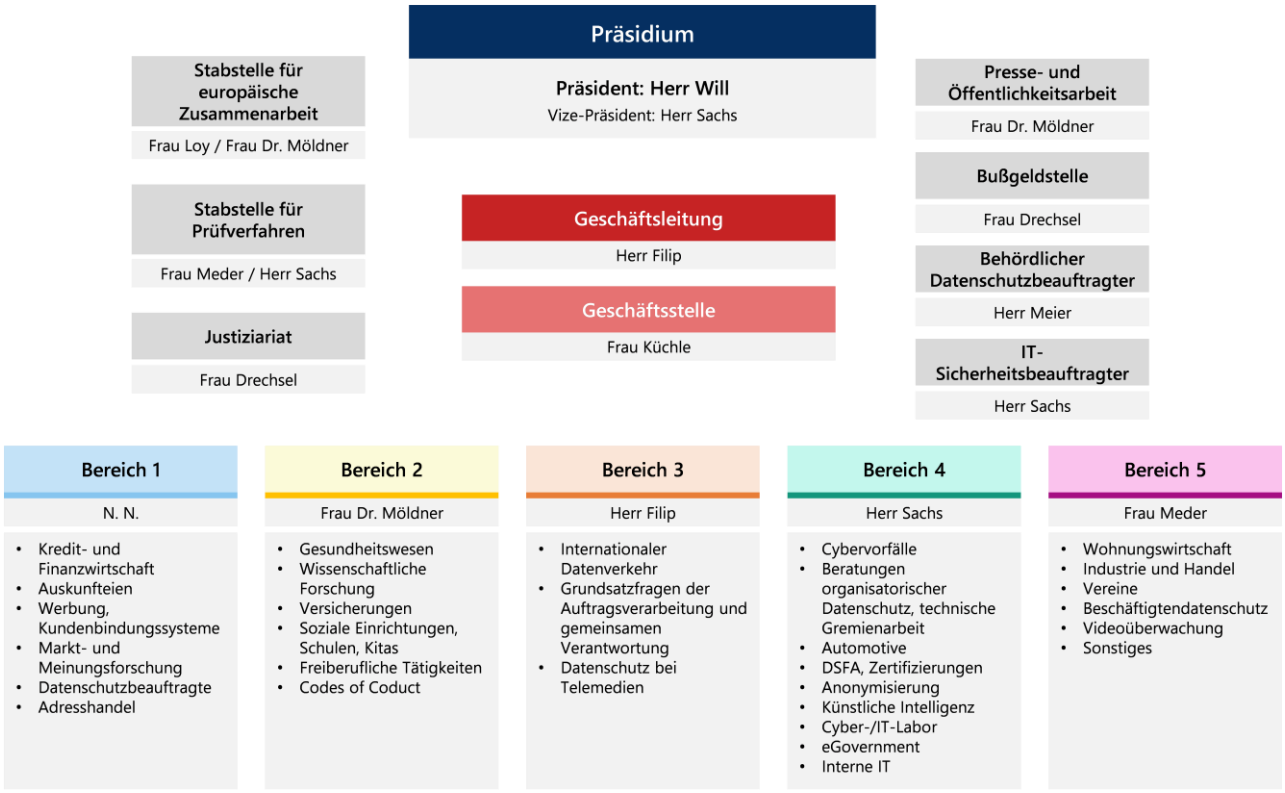
als gleichwertige und gleichrangige Aufsichtsbehörden im Sinne des Art. 51 DS-GVO gesetzlich festgelegt. Vor dem Hintergrund der gemeinsamen Verpflichtung zur einheitlichen Anwendung und Durchsetzung der DS-GVO enthält Art. 21 BayDSG klarstellend einen an alle vier Behörden adressierten Auftrag zur gegenseitigen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

Die Personalausstattung des BayLDA verharrt im Berichtszeitraum bei nominell 31 Planstellen. Die vom bayerischen Haushaltsgesetzgeber auch im sechsten Jahr der Geltung der DS-GVO ignorierten Aufgabenmehrungen ergeben ein nur vordergründig intaktes Gesamtbild, das auf einer Vielzahl von Doppelfunktionen einzelner

Leistungsträger aufbaut. Nachfolgendes Organigramm soll die aktuellen Strukturen unserer Behörde illustrieren:



2

Zahlen und Fakten

2 Zahlen und Fakten

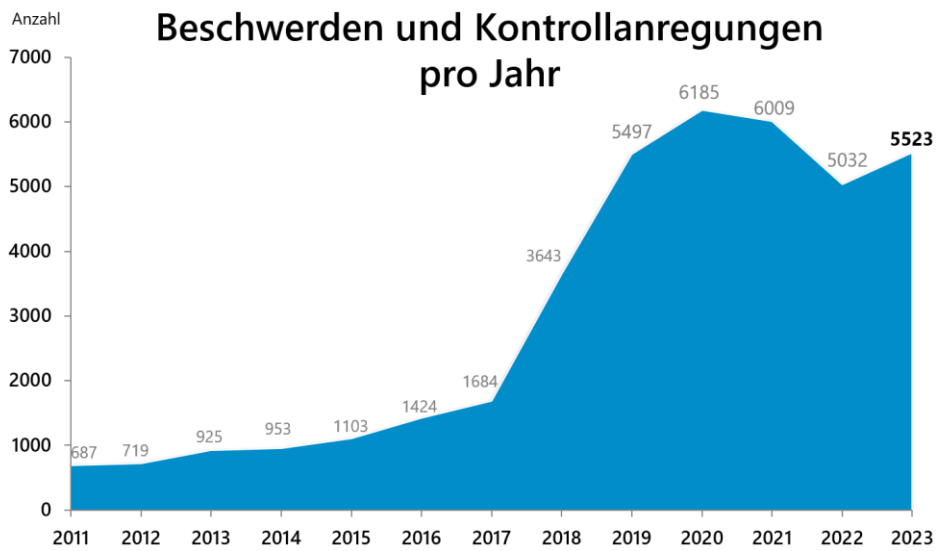
Die Bearbeitung von Datenschutzbeschwerden und Meldungen von Sicherheitsverletzungen beanspruchte auch in 2023 einen überwiegenden Teil unserer Ressourcen. Unser eGovernment-System IGOR, mittlerweile durch umfangreiche Teilautomatisierungstechniken bei der Vorgangsbearbeitung, der Templateerstellung und dem Versand von Briefen gewachsen, stellt nach wie vor das zentrale Rückgrat unserer internen IT und der tagtäglichen Fallbearbeitung dar. Mit diesem können auch die Fallzahlen (fast) durch einen Klick wie folgt ausgewertet werden:

2.1 Beschwerden

Die Gesamtanzahl der Beschwerden und Kontrollanregungen, die 2023 bei uns eingegangen sind, ist der unten folgenden Grafik zu entnehmen. Sie zeigt einen ca. zehnprozentigen Anstieg im Vergleich zu 2022, in dem das BayLDA ebenso wie viele andere Aufsichtsbehörden erstmals rückläufige Eingangszahlen verzeichnet hatte. Die Gesamtzahl von alleine rd. 5500 Beschwerden im Jahresverlauf entspricht damit den Werten von 2019 als erstem Jahr der Geltung der Datenschutzgrundverordnung und vermittelt damit ein zunehmend stabiles Bild der „Grundlast" des BayLDA. Ein dank unseres hohen Digitalisierungsgrades möglicher genauerer Blick auf die Verteilung der Beschwerdegegenstände zeigt allerdings auch durchaus bemerkenswerte Schwerpunktverlagerungen:

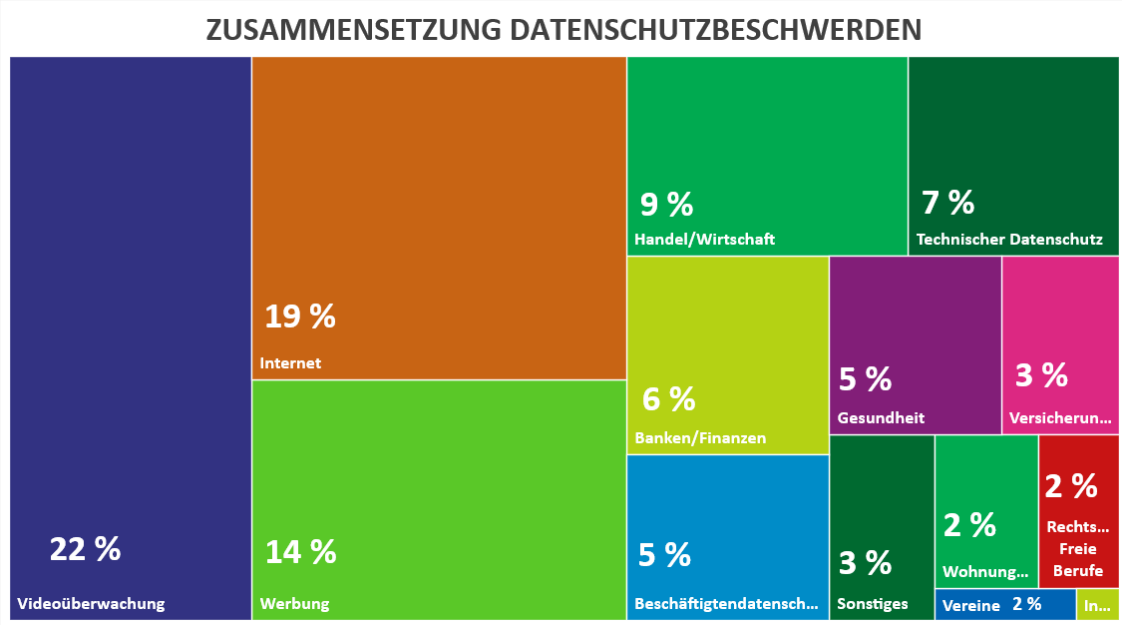
Anders als in den Vorjahren nehmen Beschwerden im Bereich Internet (Tracking, Einwilligungsbanner, Datenschutzerklärungen) quantitativ nicht länger eine Spitzenposition ein, auch wenn ein Gesamtanteil von knapp einem Fünftel aller Beschwerdefälle weiterhin auf ein hohes datenschutzrechtliches Konfliktpotential in diesem Bereich hinweist. An Stelle von Internet-Beschwerden führen die Beschwerdestatistik nunmehr Eingaben zur Videoüberwachung an, die bereits im Vorjahr gegen den Trend um 7 % zugenommen hatten. Zusammen mit Beschwerden aus dem Bereich „Werbung" (14 %) betreffen somit mehr als die Hälfte der Beschwerdevorgänge des BayLDA die Themenbereiche Videoüberwachung, Internet und Werbung (siehe Grafik nachfolgende Seite).

Als Beschwerden werden dabei nach wie vor 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

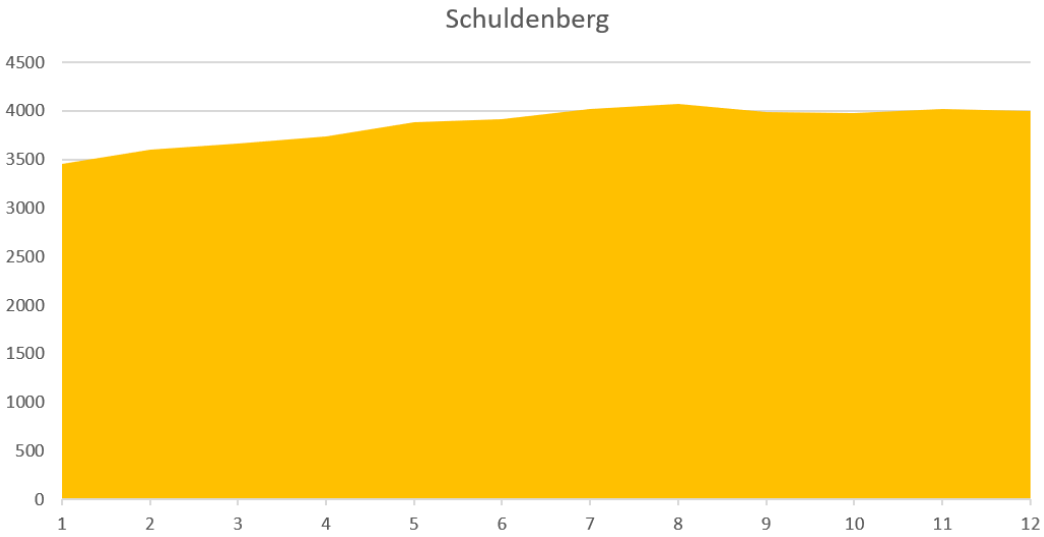


gezählt, wenn sie z. B. durch einen Vermerk verschriftlicht werden.

deres als ein Spiegelbild des in den zurückliegenden Haushaltsjahren stagnierenden Stellenplans des BayLDA.



Der Blick auf unsere Bearbeitungsrückstände („Schuldenberg") in 2023 zeigt angesichts unveränderter Ressourcen und gleichbleibend hoher Fallzahlen einen vorhersehbaren Befund, nämlich konstant hohe „Altfälle" von insgesamt rd. 4000 Vorgängen zum Jahresende. Trotz aller sonst erfolgreichen Bemühungen um Effizienz und Teilautomatisierung ist dieses ebenso unveränderte wie unbefriedigende Bild nichts an-



2.2 Beratungen

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

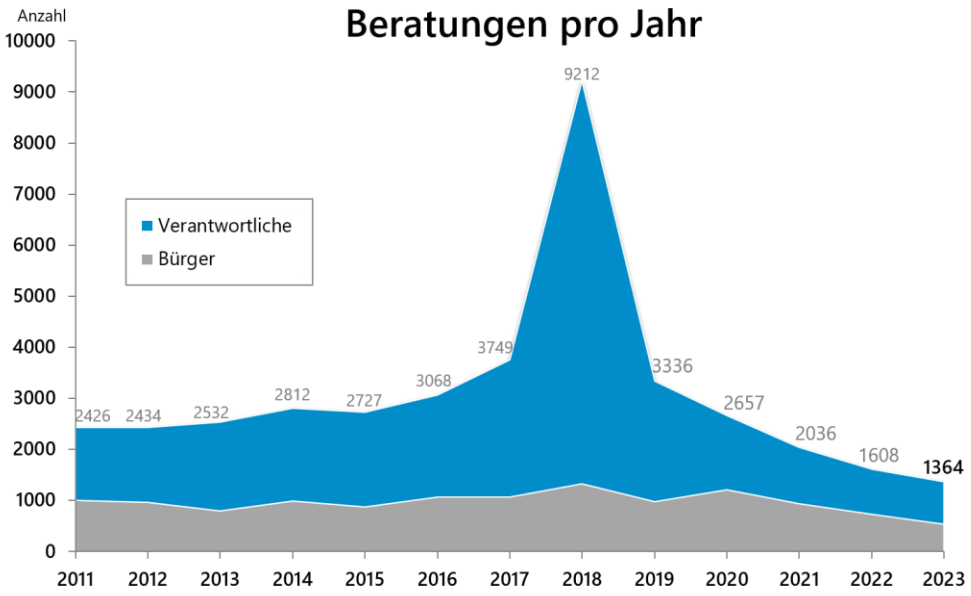
In der nachstehenden Tabelle sind die Beratungen im Berichtszeitraum aufgeführt. Sie umfasst wie in den Vorjahren auch telefonische Beratungen im eben genannten Sinne. Wie im Berichtszeitraum 2021 und 2022 ist die Anzahl der Beratungen im Verhältnis zum Vorjahr erneut gesunken.

Damit hat sich unserer Einschätzung aus dem Vorjahr be- und verstetigt, dass unsere Ressourcenlage kaum mehr eine rechtzeitige und bedarfsgerechte Beratung von datenschutzrechtlichen Anliegen zulassen. Mit der Zahl von 1364 Beratungsanfragen in 2023 wird das Jahresergebnis 2022 nochmals unterboten.

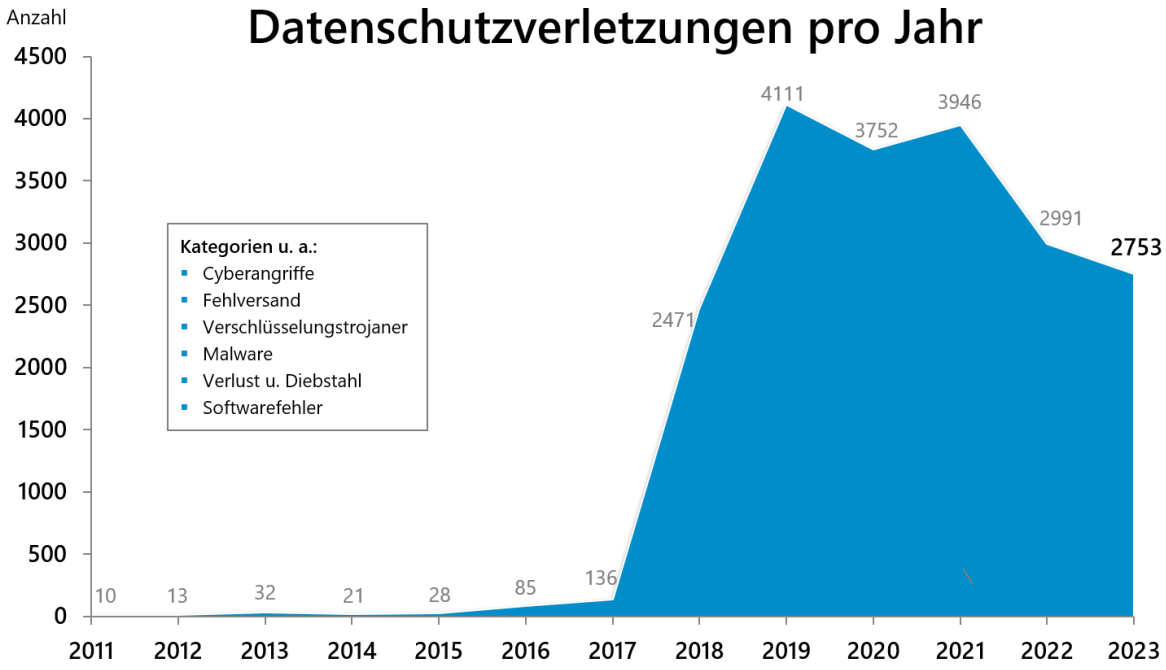
Angesichts unzureichender Ressourcen unterliegen Beratungsanliegen einer klaren Priorisierung: Dies bedeutet, dass spezifischen Beratungsanliegen von betrieblichen Datenschutzbeauftragten und Betroffen regelmäßig Vorrang vor einer individuellen Konzeptberatung von Unternehmen zukommt, so dass Beratungsanliegen von Unternehmen derzeit aufgrund der Ressourcenengpässe des Landesamts in aller Regel nicht erfüllt werden können.

2.3 Datenschutzverletzungen

Wie bereits im Vorjahr ist die Zahl der Meldungen von Verletzungen der Sicherheit bei der Verarbeitung personenbezogener Daten in 2023 erneut auf nunmehr 2753 gesunken. Datenschutzverletzungen bestimmten dennoch weiterhin unseren Arbeitsalltag insbesondere im Bereich 4 des BayLDA („Cybersicherheit und technischer Datenschutz“). Auch die gesunkene Zahl erfordert nach wie vor eine strenge Priorisierung der genauer zu prüfenden Meldungen und der ihnen zu Grunde liegenden Ursachen einer Datenschutzverletzung. Mit der Rechtsprechung des EuGH, der in seiner Entscheidung vom 14.12.2023 (C-340/21) dem Grunde nach jedem Betroffenen einer Datenschutzver-



letzung die Möglichkeit eines Schadensersatzanspruchs zugebilligt hat, wenn zu befürchten ist, dass die daten missbräuchlich verwendet werden, ist eine derartige ressourcenbedingte Priorisierung aufsichtlicher Überwachung freilich schwer zu vereinbaren.



3

Europäische Zusammenarbeit

3 Europäische Zusammenarbeit

3.1 Verfahren der Zusammenarbeit und Kohärenz

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

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

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

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

Erst wenn klar ist, welche Aufsichtsbehörde die Federführung innehat, kann das eigentliche Verfahren nach den Art. 60 ff. DS-GVO angestoßen werden. Die federführende Aufsichtsbehörde prüft den Vorgang und entwirft eine Entscheidung. Diese muss den betroffenen Aufsichtsbehörden vorgelegt werden (vgl. Art. 60 Abs. 3 Satz 2 DS-GVO), was ebenfalls über das IMI-System erfolgt. Anschließend kann dann von den betroffenen Aufsichtsbehörden ein maßgeblicher und begründeter Einspruch gegen diesen Entscheidungsentwurf eingelegt werden (Art. 60 Abs. 4 DS-GVO).

Sobald die federführende Behörde einen Entscheidungsentwurf entsprechend Art. 60 Abs. 3 und 4 DS-GVO vorgelegt hat, können die betroffenen Behörden innerhalb einer Frist von 4 Wochen einen maßgeblichen und begründeten Einspruch erheben. Die federführende Behörde kann sich daraufhin dem Einspruch anschließen und einen überarbeiteten Beschlussentwurf herausgeben oder das Verfahren wird im Rahmen des Kohärenzverfahrens weitergeführt. Bei letzterem wird der Einspruch dann entsprechend Art. 65 Abs. 1 Buchstabe a DS-GVO dem Ausschuss zur Entscheidung zugeführt.

Unsere Behörde hat sich im vergangenen Jahr an mehreren Einsprüchen beteiligt oder diese koordiniert. Die Form der Beteiligung ist im Regelfall davon abhängig, in welchem Bundesland die innerdeutsche Federführung für den Verantwortlichen liegt. Dieser Behörde obliegt es dann einen Entwurf eines Einspruches mit den anderen deutschen Aufsichtsbehörden abzustimmen

und diesen dann über das Binnenmarktinformationssystem der federführenden Aufsichtsbehörde zuzuleiten.

Die Einsprüche müssen „maßgeblich und begründet" sein, dies bedeutet vor allem, dass der Einspruch darlegen muss, weshalb die federführende Aufsichtsbehörde nicht oder nicht angemessen auf einen Verstoß nach der DS-GVO eingeht und/oder keine angemessenen Maßnahmen gegen den Verantwortlichen vorsieht.

Sollte es den Aufsichtsbehörden daraufhin nicht möglich sein, sich auf einen Standpunkt zu einigen, so leitet die federführende Aufsichtsbehörde ein Kohärenzverfahren nach den Art. 63 ff. DS-GVO ein, das, wenn zwischendurch keine Einigung erfolgt, durch einen Mehrheitsbeschluss des Europäischen Datenschutzausschusses abgeschlossen wird und dann von der federführenden Aufsichtsbehörde so zu vollziehen ist.

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

Die Gesamtzahl aller von Deutschland initiierten IMI-Verfahren lag im Jahr 2023 bei 3317 Verfahren. Im Jahr 2022 lag sie knapp darunter, bei 2891. Damit liegt Deutschland auch weiterhin auf Platz 2 nach Irland. Auch die innerdeutsche Verteilung ist weitgehend unverändert geblieben, in etwa die Hälfte aller IMI- Fälle entfallen auf die Berliner Behörde (ca. 35 %) und das BayLDA (ca. 19 %).

Bei rund 17 % der Verfahren bei denen Deutschland federführend war, lag die innerdeutsche Zuständigkeit bei uns, womit das BayLDA den zweiten Platz nach der Berliner Aufsichtsbehörde (30 %) belegt.

3.2 Mitwirkung in Subgroups des EDSA

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

In der Geschäftsordnung des EDSA (vgl. Art. 72 Abs. 2 DS-GVO) ist vorgesehen, dass der Ausschuss Unterarbeitsgruppen (englisch: Expert Subgroups) einsetzt, die ihn bei der Erfüllung seiner Aufgaben unterstützen sollen (Art. 25 Abs. 1 der Geschäftsordnung des EDSA). Eine ähnliche Organisation und Arbeitsweise war auch für das Vorgängergremium des EDSA, die Artikel-29-Datenschutzgruppe, unter der Datenschutzrichtlinie etabliert. Die Struktur der Unterarbeitsgruppen wurde unter dem Regime der DS-GVO weitestgehend übernommen – lediglich kleinere Änderungen wurden durchgeführt

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

Die Vertretung der deutschen Datenschutzaufsichtsbehörden in diesen Unterarbeitsgruppen erfolgt, wie auch zuletzt im Rahmen der Art. 29-Gruppe, immer durch einen Vertreter/ einer Vertreterin des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) sowie einen Vertreter/eine Vertreterin einer Aufsichtsbehörde eines Landes sowie eines stellvertretenden Landesvertreters oder einer

stellvertretenden Landesvertreterin. Hierbei sollen die von der DSK ernannten Vertreter und Vertreterinnen Deutschland als Ganzes repräsentieren und nicht (nur) die eigene Behörde.

Im Berichtszeitraum stellten wir weiterhin den Landesvertreter in der International Transfer Expert Subgroup und eine Landesvertreterin für die Compliance, eGovernance and Health Subgroup. Durch die Mitarbeit auf europäischer Ebene ist es uns möglich, an der Erstellung von Leitlinien, Empfehlungen und anderen Papieren des EDSA direkt mitzuarbeiten und die maßgeblichen Entscheidungen auf europäischer Ebene unmittelbar mitzugestalten.
Wir haben in den vergangenen Jahren in den Unterarbeitsgruppen für eine Reihe von Papieren (Leitlinien, interne Arbeitsanweisungen etc.) die Berichterstattung übernommen. Dies umfasst insbesondere die Erstellung von Entwürfen und die Koordinierung des Erarbeitungsprozesses sowie die Präsentation der finalen Version vor dem Plenum des EDSA.

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

Im Berichtszeitraum umfasste dies auch in Form einer federführenden Berichterstattung mehrere wichtige Hilfestellungen aus dem Bereich Internationaler Datentransfers wie die Leitlinien zum Verhältnis zwischen Art. 3 und Kapitel V der DS-GVO, die Empfehlungspapiere des EDSA zu den Inhalten von Binding Corporate Rules für Verantwortliche sowie für Auftragsverarbeiter und die Evaluation der Adäquanzentscheidung für Japan.

Die Mitwirkung in Angelegenheiten des Europäischen Datenschutzausschusses steht unter den Bedingungen unzureichender Ressourcenausstattung im ständigen Spannungsverhältnis zur Erfüllung einzelfallbezogener Aufgaben. Gleichwohl bleibt sie, nicht anders als die Erfüllung der Rechte von Beschwerdeführern, eine Pflichtaufgabe aufsichtlichen Handelns, wie Art. 51 Abs. 2 DS-GVO unterstreicht.

4

Allgemeines

4 Allgemeines

4.1 Untätigkeit der Aufsichtsbehörde bei grenzüberschreitenden Verfahren

Bei Beschwerdeverfahren, in denen mehrere Aufsichtsbehörden mitwirken müssen, ist die Ausgangsbehörde nicht automatisch untätig, wenn die federführende Behörde das Verfahren nicht zügig bearbeitet. Der Beschwerdeführende muss nicht alle drei Monate über den Stand der Beschwerde unterrichtet werden.

Grenzüberschreitende Verfahren sind aufgrund der Beteiligung mehrerer Behörden in der Regel etwas langwieriger als rein nationale Verfahren. Doch gibt es hier nur teilweise konkrete Vorgaben, in welchem Zeitraum die einzelnen Verfahrensschritte zu erfolgen haben.

In Art. 60 Abs. 3 DS-GVO heißt es beispielsweise:

> *„Die federführende Aufsichtsbehörde übermittelt den anderen betroffenen Aufsichtsbehörden unverzüglich die zweckdienlichen Informationen zu der Angelegenheit.*
>
> *Sie legt den anderen betroffenen Aufsichtsbehörden unverzüglich einen Beschlussentwurf zur Stellungnahme vor und trägt deren Standpunkten gebührend Rechnung."*

Jedoch sieht die DS-GVO keine Maßnahmen für betroffene Aufsichtsbehörden vor, wenn die federführende Behörde nicht tätig wird bzw. das Verfahren nicht weiter betreibt. Die Aufsichtsbehörde, bei der die Beschwerde eingegangen ist (Ausgangsbehörde), sowie andere betroffene Behörden können daher keinen Einfluss auf die Bearbeitungsdauer nehmen.

In einem Fall kam es daher dazu, dass der Beschwerdeführer, der eine Beschwerde in Bezug auf eine grenzüberschreitende Verarbeitung bei uns eingereicht hatte, eine Untätigkeitsklage gegen uns erhoben hat.

Wir hatten in dem streitgegenständlichen Verfahren in regelmäßigen Abständen Sachstandsmitteilungen bei der federführenden Behörde angefragt und diese, wenn auch teilweise nach mehrmaligen Nachfragen, auch erhalten. Weiterhin haben wir den Austausch zu den rechtlichen Fragestellungen vorangetrieben. Ein Entscheidungsentwurf lag aber auch nach mehreren Jahren noch nicht vor und damit konnte auch keine abschließende Entscheidung getroffen werden.

Der Beschwerdeführer hatte, nachdem er die Beschwerde bei uns eingereicht hatte, eine Eingangsmitteilung, sowie die Informationen zum Vorgehen bei grenzüberschreitenden Vorgängen von uns innerhalb der Dreimonatsfrist erhalten. Weitere Sachstandsmitteilungen erfolgten daraufhin – wie in diesen Verfahren üblich – nur dann, wenn wir neue Informationen von der federführenden Behörde erhalten haben oder auf Nachfrage des Beschwerdeführers. Von automatisierten Nachrichten, die lediglich aussagen, dass das Verfahren noch in Bearbeitung ist, haben wir abgesehen.

Der Beschwerdeführer hat im Zuge dessen Klage vor dem Verwaltungsgericht Ansbach wegen Untätigkeit eingereicht. Als Ausgangsbehörde war das BayLDA der richtige Klagegegner, auch wenn die federführende Behörde eine andere europäische Aufsichtsbehörde war.

Eine Pflicht der Aufsichtsbehörden aus Art. 78 Abs. 2 Alt. 2 DS-GVO, dass Beschwerdeführende fortlaufend im Dreimonatsrhythmus über den Stand des Verfahrens informiert werden müssen, verneinte das Gericht.

Auch ein weitergehender Anspruch des Klägers auf weitere Befassung bzw. weiteres Vorantreiben der Beschwerde wurde in dem Beschluss verneint. Das Gericht führte hierzu aus, dass nicht ersichtlich war, dass das BayLDA in größerem Umfang hätte tätig werden müssen, sondern das Verfahren mit den Zwischenmitteilungen und Beantwortung der Nachfragen ordnungsgemäß betrieben hat.

Weiterhin führte das Gericht aus, dass ein Anspruch eines Beschwerdeführers dahingehend, dass die Behörde verpflichtet wäre, jede einzelne Sachstandsanfrage (auch bei Fristsetzung seitens des Beschwerdeführers) zu beantworten, mit Blick auf die Ressourcen und Möglichkeiten der Aufsichtsbehörde mit Verweis auf Art. 57 Abs. 1 Buchstabe f DS-GVO („in angemessenem Umfang") ebenfalls zu verneinen ist.

Noch bevor das Gericht darüber entscheiden konnte, ist ein Entscheidungsentwurf der federführenden Behörde und kurz darauf eine Entscheidung zu der Beschwerde ergangen. Daraufhin wurde die Klage beidseitig für erledigt erklärt.

Das Gericht hatte daraufhin nur noch über die Kostentragung per Beschluss zu entscheiden.

Bei Erledigung von Untätigkeitsklagen i. S. d. § 75 VwGO sind die Kosten entsprechend § 161 Abs. 3 VwGO vom Klagegegner zu tragen, wenn der Kläger vor der Klageerhebung mit einer Bescheidung rechnen durfte.

Vorliegend hat das VG Ansbach allerdings das Vorliegen einer Untätigkeitsklage verneint, da der Kläger hier nicht eine bestimmte, als Verwaltungsakt zu qualifizierende Maßnahme seitens der Behörde begehrt hat, sondern ein Tätigwerden der Behörde bzw. eine abschließende Entscheidung im Rahmen der Datenschutzbeschwerde des Klägers nach Art. 77 f. DS-GVO. Nach bisheriger Rechtsprechung der Kammer sind die ein Beschwerdeverfahren beendenden Entscheidungen der Aufsichtsbehörde regelmäßig nicht als Verwaltungsakt zu qualifizieren (vgl. VG Ansbach, U. v. 07.12.2020 – AN 14 K18.02503; VG Ansbach, B. v. 03.08.2023 – AN 14 K 19.01313).

Die weitere Bearbeitung und schließlich die Entscheidung über seine Datenschutzbeschwerde, wäre daher im Rahmen der allgemeinen Leistungsklage geltend zu machen.

Auch eine analoge Anwendung der Kostentragungsregelung aus § 161 Abs. 3 VwGO war hier nach Auffassung des Gerichts nicht möglich, da eine solche von der Kammer bislang nur für den Fall bejaht wurde, dass ein Beschwerdeführer entgegen Art. 78 Abs. 2 Alt. 2 DS-GVO nicht innerhalb von drei Monaten entweder eine Sachstandsmitteilung oder eine Ergebnismittelung über sein Beschwerdeverfahren vom Beklagten erhält. Im Ergebnis führte dies, mangels Untätigkeit unserer Behörde, zu einer Kostentragungspflicht des Klägers.

4.2 Keine Anwendbarkeit der DS-GVO bei Verstorbenen

Bei Veröffentlichungen im Internet, die personenbezogene Daten Verstorbener zum Gegenstand haben, findet die DS-GVO keine Anwendung.

Sachverhalte, die die Verarbeitung von personenbezogenen Daten Verstorbener zum Gegenstand haben, finden sich auch immer häufiger in unserem Arbeitsbereich Telemedien. So haben wir im Jahr 2023 verschiedene Beschwerden und Kontrollanregungen zu solchen Fällen erhalten.

In einem Fall wurde z. B. gerügt, dass ein Verantwortlicher mit Sitz in einem anderen EU-Mitgliedstaat auf seiner Webseite Fotos von Grabstätten bayerischer Friedhöfe veröffentlichte

und zudem die auf den Grabsteinen verzeichneten Angaben in durchsuchbaren Datenbanken aufbereitete.

In einem weiteren Fall hatte ein Beschwerdeführer bemängelt, dass ein Nachruf auf der Homepage eines Verantwortlichen veröffentlicht wurde, für den sein verstorbener Angehörige zu Lebzeiten ehrenamtlich tätig gewesen war.

Darüber hinaus gab es noch weitere Einzelfälle wie beispielsweise die Veröffentlichung eines Videos von der Abholung eines Verstorbenen aus einer Leichenhalle in sozialen Medien.

All diesen Zuschriften war gemein, dass von den Eingabeführern die Rechtmäßigkeit der Verarbeitung personenbezogener Daten von Verstorbenen in Frage gestellt wurde.

Ein datenschutzrechtlicher Verstoß konnte jedoch in keinem der Fälle festgestellt werden. Entsprechend Art. 1 Abs. 1 DS-GVO schützt die DS-GVO die Verarbeitung von personenbezogenen Daten natürlicher Personen. Der Begriff der natürlichen Person ist in Art. 4 Nr. 1 DS-GVO definiert und bezieht sich allein auf lebende Personen. Damit ist der sachliche Anwendungsbereich der DS-GVO in den oben genannten Fällen nicht eröffnet. Dies bestätigt auch Erwägungsgrund 27, der ausdrücklich klarstellt, dass „diese Verordnung nicht für die personenbezogenen Daten Verstorbener gilt". Zwar sieht Erwägungsgrund 27 vor, dass die Mitgliedstaaten Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen können, von dieser Möglichkeit hat die Bundesrepublik jedoch bislang jedenfalls für den hier vorliegenden Verarbeitungskontext keinen Gebrauch gemacht (anders etwa als gemäß § 35 Abs. 5 SGB I für die Verarbeitung von Sozialdaten Verstorbener durch Leistungsträger für Sozialleistungen).

5

Betroffenenrechte

5 Betroffenenrechte

5.1 Ausnahme vom Auskunftsrecht

Die Voraussetzungen einer Ausnahme vom Auskunftsrecht nach Art. 15 DS-GVO gemäß § 34 Abs. 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) sind vielen Verantwortlichen im Berichtszeitraum nicht ausreichend klar gewesen.

Auch in diesem Berichtszeitraum erreichten uns Beschwerden dazu, dass Auskunftsersuchen gem. Art. 15 DS-GVO nicht beantwortet wurden bzw. eine Auskunft seitens des Verantwortlichen verweigert wurde. Dies wurde durch die Verantwortlichen insbesondere im Beschäftigtenkontext oftmals mit der Ausnahme gem. § 34 Abs. 1 Nr. 2 BDSG begründet. Hiernach besteht das Recht auf Auskunft der betroffenen Person gem. Art. 15 DS-GVO nicht, wenn die Daten entweder nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen (Buchstabe a) oder die Daten ausschließlich Zwecken der Datensicherung oder Datenschutzkontrolle dienen (Buchstabe b) und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

Die Verantwortlichen waren sich dabei jedoch zum Teil nicht im Klaren darüber, dass die Voraussetzungen kumulativ vorliegen müssen. Es genügt also nicht, dass gesetzliche oder satzungsmäßige Aufbewahrungspflichten einer Löschung entgegenstehen oder aber die Daten ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle verarbeitet werden. Vielmehr setzt die Ausnahme darüber hinaus einen unverhältnismäßigen Aufwand für die Auskunftserteilung sowie geeignete technische und organisatorische Maßnahmen, die eine Verarbeitung zu anderen Zwecken ausschließt, voraus.

Zum Teil war dies in den uns vorliegenden Beschwerden den Verantwortlichen zwar bewusst, allerdings wurde die Voraussetzung eines unverhältnismäßigen Aufwandes durch Verantwortliche als vorliegend angesehen, weil letztlich nur rudimentäre Archivierungs- und Löschkonzepte bei den Verantwortlichen existierten bzw. umgesetzt wurden. Führt eine mangelnde Datenschutzorganisation bei dem Verantwortlichen dazu, dass der Aufwand für die Erteilung einer Auskunft gesteigert wird, ist die Ausnahme des § 34 Abs. 1 Nr. 2 BDSG in der Regel nicht einschlägig.

Aber auch dann, wenn die Voraussetzungen des § 34 Abs. 1 Nr. 2 BDSG vorlagen, bedeutet dies nicht, dass eine Kommunikation mit der auskunftsersuchenden Person nicht erfolgen muss. Vielmehr muss gem. § 34 Abs. 2 S. 2 BDSG der Verantwortliche die Ablehnung der Auskunftserteilung gegenüber der betroffenen Person begründen, soweit nicht der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. Zwar sieht § 34 BDSG keine Frist für die Begründung vor, allerdings muss diese gem. Art. 12 Abs. 4 DS-GVO ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrages erfolgen. Ebenfalls gem. Art. 12 Abs. 4 DS-GVO muss der Verantwortliche die betroffene Person zudem innerhalb der genannten Frist über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen, informieren.

5.2 Auskunft nach Identitätsdiebstahl

Bei Warenbestellungen im Internet durch Unbefugte unter Verwendung von personenbezogenen Daten der geschädigten Person hat die geschädigte Person im Rahmen der Auskunft gemäß Art. 15 DS-GVO Anspruch auf alle Informationen, die mit ihr im Rahmen der Bestellung in Verbindung gebracht wurden, soweit sie beim Verantwortlichen vorhanden sind.

Uns erreichten einige Beschwerden, bei denen die beschwerdeführenden Personen angaben, Opfer eines Identitätsdiebstahls geworden zu sein, woraufhin sie ein Auskunftsersuchen gem. Art. 15 DS-GVO bei dem für die Verarbeitung ihrer personenbezogenen Daten Verantwortlichen gestellt hätten, welcher sich jedoch weigere, Informationen zu dem Täter zu beauskunften.

In den meisten der an uns herangetragenen Vorgängen wurden online Waren unter Verwendung von personenbezogenen Daten der Opfer in betrügerischer Absicht bestellt, die in der Folge entweder abgefangen wurden, bevor die Opfer diese in Empfang nehmen konnten, oder die Bestellung erfolgte unter Angabe einer anderen Lieferadresse als derjenigen des Opfers. In anderen Fällen boten die Täter selbst Waren an, die sie später, nach Erhalt der Bezahlung durch die Opfer, mit den Daten der Opfer bei einem weiteren Händler zahlungspflichtig bestellten. In der Folge erhielten die Opfer zwar die Ware, jedoch sahen sie sich einer (weiteren) Forderung des „richtigen" Verkäufers ausgesetzt.

Neben einer Anzeigeerstattung bei der Polizei, versuchten die Opfer des Identitätsdiebstahls insbesondere mithilfe des Auskunftsanspruches gem. Art. 15 DS-GVO Informationen zu den Tätern zu erhalten. In den uns vorgetragenen Vorgängen verwehrten die Verantwortlichen jedoch eine entsprechende Auskunft. Sie begründeten dies damit, dass es sich nicht um personenbezogene Daten zur auskunftsersuchenden Person handele bzw. Art. 15 Abs. 4 DS-GVO einer Beauskunftung entgegenstehe.

Nach Art. 15 Abs. 1 DS-GVO kann eine betroffene Person von dem Verantwortlichen Auskunft über sie betreffende personenbezogene Daten verlangen. Soweit Informationen einer bestimmten Person zugeordnet sind bzw. mit ihr in Verbindung gebracht werden, beispielsweise weil sie im Kunden-Account des Opfers zu diesem gespeichert sind, handelt es sich um sie betreffende personenbezogene Daten gem. Art. 4 Nr. 1 DS-GVO. Es ist also auch dann, wenn dem Verantwortlichen der Identitätsdiebstahl bekannt ist, eine Auskunft gem. Art. 15 DS-GVO zu den Daten, die ein Verantwortlicher im Zusammenhang mit der betrügerischen Handlung erhalten hat, zu geben. Dies hat der Europäische Datenschutzausschuss ausdrücklich betont (vgl. hierzu Guidelines 01/2022 on data subject rights - Right of access, Version 2.0, Rn. 107).

Der Verantwortliche kann wiederum nur Daten, die bei ihm auch vorhanden sind, beauskunften. In einem Beschwerdefall wurde bei einem Onlinehändler durch den Täter eine Ware unter Verwendung von Kreditkartendaten des Opfers bestellt, die sich der Täter augenscheinlich bei anderer Gelegenheit beschafft hatte. Neben der Kreditkartennummer gab der Täter bei der Bestellung noch den Namen des Opfers an. Der Verantwortliche teilte dem Opfer auf dessen Auskunftsersuchen keine Kreditkartennummer mit, woraufhin letzterer Beschwerde bei uns erhob, weil er vermutete, dass der Verantwortliche die Kreditkartennummer besitzen müsse und die Auskunft daher unvollständig sei. Die Kreditkartennummer lag jedoch alleine dem für die Zahlung eingeschalteten (für Kreditkartenzahlungen akkreditierten) Zahlungsdienstleister vor und wurde beim verantwortlichen Online-Händler nicht gespeichert. Dass der Verantwort-

liche diese im Rahmen der Auskunft nicht genannt hatte, stellte daher keinen Verstoß gegen die Auskunftserteilungspflicht nach Art. 15 DS-GVO dar.

Die Ausnahme gem. Art. 15 Abs. 4 DS-GVO greift, wenn die Rechte und Freiheiten anderer Personen – hier des Täters – beeinträchtigt sind. Der Umstand, dass es sich bei den in Frage stehenden personenbezogenen Daten (auch) um personenbezogene Daten anderer Personen handelt, führt für sich gesehen nicht dazu, dass eine Auskunft nicht erteilt werden dürfte. Vielmehr bedarf es einer Abwägung zwischen den Rechten der betroffenen Personen. Bei der vorliegenden Konstellation fällt diese Abwägung regelmäßig zu Gunsten des Opfers aus.

5.3 Auskunftsrecht und Löschungsersuchen nach Webseiten-Besuchen

Bei Auskunftsersuchen zu Webseiten-Besuchen ist häufig ein Zusammenwirken des Verantwortlichen mit dem Betroffenen erforderlich, um eine vollständige, den Interessen des Betroffenen gerechte Auskunft erteilen zu können.

Neben den klassischen Eingaben zu Tracking auf Webseiten und in Apps gab es auch im Jahr 2023 eine Vielzahl von Beschwerden in Bezug auf Betroffenenrechte im Onlinebereich. Während sich bei Diensten, bei denen eine Registrierung erfolgt, zumeist im Wesentlichen dieselben Themen wie in der „Offline-Welt" ergeben, stellen beispielsweise Auskunftsersuchen im Webseitenkontext Verantwortliche und Betroffene vor einige spezifische Fragestellungen.

So haben wir Beschwerden erhalten, in denen Betroffene eine unzutreffend erteilte Auskunft rügten, da ihnen der Webseitenbetreiber mitgeteilt hatte, er könne alleine mit der Angabe des Klarnamens und einer E-Mail-Adresse keine Auskünfte über etwaige Webseitenbesuche und damit einhergehende Datenverarbeitungen treffen. Oft wurde aber auch nur mitgeteilt, dass keine Daten zu der betroffenen Person vorliegen, obwohl diese angegeben hatte, die Webseite des Verantwortlichen besucht zu haben, und laut Datenschutzerklärung dadurch Datenverarbeitungen stattgefunden haben.

Das Problem in diesen Fällen ist, dass hier personenbezogene Daten wie beispielsweise die IP-Adresse oder Cookie-IDs verarbeitet werden, die vom Webseitenbetreiber nicht direkt einem Klarnamen zugeordnet werden können. Diese Daten werden auf den Servern des Betreibers der Webseite oder der eingebundenen Drittdienste verarbeitet.

Damit ein Auskunftsersuchen vollständig bearbeitet werden kann, ist es daher im Regelfall erforderlich, dass der Verantwortliche weitere Identifikationsmerkmale abfragt, um eine Zuordnung vornehmen zu können. Siehe hierzu auch die Ausführungen in der, "Orientierungshilfe für Anbieter:innen von Telemedien 2021", Rn. 139:

> *„In diesen Fällen können vom Verantwortlichen andere eindeutige Identifikationsmerkmale des Nutzers nachgefragt werden, um über diese die Zuordnung eines Datenbestands zu der anfragenden Person zu ermöglichen. Die Abfrage der Daten zur Identifizierung kann der Verantwortliche auf Art. 11 Abs. 2 S. 2 DS-GVO stützen. […]".*

Die Betroffenen sollten allerdings darauf hingewiesen werden, dass durch die Bereitstellung der zur Bearbeitung ihres Auskunftsersuchens erforderlichen Informationen, wie beispielsweise der IP-Adresse zum Zeitpunkt des Webseitenbesuchs oder auch einer Cookie-ID, jeweils ein neues (personenbezogenes) Datum geschaffen wird, nämlich die Verbindung dieser Daten mit dem Klarnamen.

Kann der Verantwortliche nachweisen, dass er nicht in der Lage ist, die betroffene Person zu

identifizieren, so muss er gemäß Art. 11 Abs. 2 DS-GVO die betroffene Person hierüber unterrichten, sofern möglich.

Unabhängig davon ist es zumindest empfehlenswert, wenn der Webseitenbetreiber bei Auskunftsersuchen schon in einer ersten Rückmeldung allgemein darüber informiert, welche Datenverarbeitungen bei Besuch der Webseite stattfinden, auch wenn mit dem Auskunftsersuchen selbst noch keine individuelle Zuordnung zu einem konkreten Besuch vorgenommen werden kann.

In den von uns bearbeiteten Fällen konnten nach den von uns erteilten Hinweisen die Auskunftersuchen erfüllt werden, sodass keine weiteren Maßnahmen erforderlich waren.
Verantwortliche müssen jedoch wie erläutert bei derartigen Auskunftersuchen direkt mit den Betroffenen kommunizieren und darstellen, dass ihnen eine Auskunftserteilung im Hinblick auf Datenverarbeitungen einer Webseite im Regelfall nicht möglich ist, wenn die betroffene Person zu ihrer Identifizierung lediglich ihren Klarnamen angibt.

Darüber hinaus kann es in diesem Zusammenhang auch zu Problemen bei Löschungsersuchen kommen. Dies besonders deshalb, weil die Webseitenbetreiber nur bedingt in der Lage sind, beispielsweise Cookies und damit die dazugehörige ID auf den Endeinrichtungen der Nutzenden zu löschen. Ein Löschersuchen wird daher ausreichend erfüllt, wenn der Verantwortliche die personenbezogenen Daten bei sich löscht und ggfs. die Löschung entsprechend Art. 17 Abs. 2 DS-GVO veranlasst. Der Verantwortliche ist nicht verpflichtet sicherzustellen, dass betroffene Personen die entsprechenden Cookies von ihren Endgeräten selbst löschen.

5.4 Exzessivität von Auskunftsersuchen

Der exzessive Charakter eines Auskunftsantrags kann sich daraus ergeben, dass die betroffene Person die Rücknahme des Antrags gegen Zahlung einer Geldsumme in Aussicht stellt.

Im Berichtszeitraum wurden von uns zwei Beschwerden wegen vermeintlicher Verletzung des Auskunftsrechts als exzessiv abgewiesen.

In beiden Fällen ergab sich aus den uns vorgelegten Unterlagen, dass die betroffene Person dem Verantwortlichen in Aussicht gestellt hatte, ihren Auskunftsantrag gegen die Zahlung einer Geldsumme (im vier- bzw. fünfstelligen Bereich) zurückzuziehen. Die Verantwortlichen waren auf dieses Angebot jeweils nicht eingegangen, woraufhin sich die betroffenen Personen bei uns beschwerten.

Der Verantwortliche kann sich bei exzessiven Anträgen weigern, tätig zu werden (Art. 12 Abs. 5 S. 2 Buchstabe b DS-GVO). Die Exzessivität eines Auskunftsersuchens kann sich nicht nur aus der häufigen Wiederholung eines Auskunftsersuchens ohne ersichtlichen Grund ergeben, sondern auch durch andere Umstände begründet werden. In den Leitlinien 01/2022 des Europäischen Datenschutzausschusses zum Auskunftsrecht wird u. a. explizit der Fall benannt, in dem die betroffene Person die Rücknahme ihres Auskunftsersuchens im Gegenzug für einen vom Verantwortlichen gewährten Vorteil in Aussicht stellt (dort Rn. 188).

In derartigen Fällen kann sich die Aufsichtsbehörde ferner weigern, die von der betroffenen Person erhobene Beschwerde zu bearbeiten (Art. 57 Abs. 4 S. 1 DS-GVO).

6

Finanzwirtschaft

6 Finanzwirtschaft

6.1 Offenlegung von Inkassodaten in Online-Rezensionen

Die Veröffentlichung von Schuldnerdaten aus dem Inkassoverfahren in einer Antwort auf deren Online-Rezensionen ist unzulässig.

Im Rahmen der Bearbeitung einer anderen Fragestellung sind wir darauf aufmerksam geworden, dass ein Inkassobüro sich offenbar veranlasst sah, den bei einer Online-Suchmaschine zum Unternehmen abgegebenen Rezensionen durch Nutzung der Antwortfunktion zu begegnen.

In einem Großteil der Fälle waren diese Antworten hinreichend neutral gehalten, das heißt Offenlegungen personenbeziehbarer Informationen aus dem Inkasso-Geschäft wurden vermieden. Allerdings ergaben unsere Untersuchungen auch Einzelfälle, bei denen in den Antworten des Inkassobüros auch personenbezogene Daten der Betroffenen aus dem Inkassoverfahren offengelegt wurden, beispielsweise Informationen zu Inhalten aus Telefongesprächen, zur Forderungsentstehung oder zum aktuellen Forderungs-/Verfahrensstand.

Für die Veröffentlichung dieser Daten bestand keine Rechtsgrundlage, insbesondere überwiegen die schutzwürdigen Interessen der Betroffenen die Interessen des Unternehmens an einer Richtigstellung oder auch Gegendarstellung. Wir haben daher von Amts wegen aufsichtliche Schritte eingeleitet und das Inkassobüro zur Löschung der problematischen Inhalte veranlasst sowie aufsichtlich verwarnt.

6.2 Umstellung elektronischer Postfächer bei Kreditinstituten von Einzelvertragsbezug zu Personenbezug („Briefkastenlösung“)

Eine Umstellung von nach Verträgen getrennten elektronischen Postfächern auf ein Einzelpostfach mit Personenbezug ist datenschutzrechtlich nicht zu beanstanden.

Mehreren Beschwerdeführenden ist in 2023 aufgefallen, dass sie bei mehreren Banken in den elektronischen Postfächern jeweils nicht mehr lediglich bereitgestellte Unterlagen zu ihren Privatkonten vorfanden, sondern beispielsweise auch Unterlagen zu Geschäftskonten, bei welchen sie nicht selbst den Vertrag abgeschlossen, sondern lediglich eine Bevollmächtigung hatten. Dasselbe wurde auch bei einem Login mit den Zugangsdaten zum Geschäftskonto festgestellt; dort waren neben den Geschäftsunterlagen auch Unterlagen zum Privatkonto vorzufinden.

Hieraus resultierte mehrfach die Befürchtung, dass andere Bevollmächtigte der Geschäftskonten nun auch Unterlagen der Privatkonten der Betroffenen einsehen könnten, oder eine Person, der man selbst eine Vollmacht für eigene Privatkonten eingeräumt hat, nun ebenfalls Zugriff auf die Unterlagen der Geschäftskonten hätte. Teilweise lag der Beschwerdegrund auch in einem Bedürfnis begründet, dass „privat“ und „geschäftlich“ grundsätzlich getrennt werden.

Unsere Ermittlungen ergaben, dass es sich um eine Umstrukturierung der elektronischen Postfächer in der Weise handelte, dass nicht mehr für die jeweiligen Verträge bei der Bank einzelne Postfächer vorgehalten wurden, sondern pro

Einzelperson lediglich noch ein einziges elektronisches Postfach eingerichtet wurde, in welches (vergleichbar einem Briefkasten am Wohngebäude) Korrespondenz verschiedener Verträge zusammengefasst wird, egal mit welchem ihr zur Verfügung stehenden Zugang die Person sich bei der Bank anmeldet.

Wir konnten bei unseren Ermittlungen nicht feststellen, dass mit dieser Umstellung datenschutzrechtliche Anforderungen verletzt werden, da die Betroffenen in ihren jeweiligen Postfächern lediglich Zugang zu solchen Daten erhalten, zu deren Einsicht sie selbst entweder als Vertragspartei oder Bevollmächtigte berechtigt sind.

Andere Personen mit teilweise überschneidenden Berechtigungen sehen demnach nicht dasselbe Postfach, sondern ebenfalls nur eine solche Darstellung von Unterlagen, die ihrer individuellen Berechtigung entspricht.

Durchbrochen werden könnte die Berechtigungslogik nur dadurch, dass Betroffene die ihnen persönlich ausgestellten Zugangsdaten (auch geschäftliche Zugänge sind bei Banken regelmäßig Einzelpersonen zugeordnet) an Dritte geben würden, was jedoch durch die betrachteten Geschäftsbedingungen ausdrücklich ausgeschlossen war und nicht in der Verantwortung der Bank läge.

Ein Verstoß der Bank könnte sich zwar theoretisch weiterhin dadurch verwirklichen, dass diese eine Berechtigung falsch hinterlegen und dadurch einer unberechtigten Person Zugang/Einsicht gewähren würde. Aber alleine das Risiko, dass bei der Verarbeitung bei inkorrekter Ausführung Verstöße verwirklicht werden könnten, genügt nicht, um den Prozess dem Grunde nach zu untersagen, zumal dieses Risiko auf jegliche Datenverarbeitung (auch die vorliegend bisherige Lösung) zutrifft.

Da wir aus dem Datenschutzrecht auch keinen Anspruch darauf erkennen konnten, die Zusendungen zu Privatkonten von solchen zu Geschäftskonten zu trennen, haben wir die Beschwerden zurückgewiesen.

6.3 Meldung der Beendigung von Vertragsverhältnissen durch Kreditinstitute an Wirtschaftsauskunfteien (Fortschreibung zu TB 2021, Kap. 7.2)

Besonderheiten beim Ausgleich einer Restvertragssumme per Lastschrift sind nicht auf eine Überweisung übertragbar.

Wie bereits in unserem Tätigkeitsbericht 2021 unter Kapitel 7.2 ausgeführt, haben Kreditinstitute einer Wirtschaftsauskunftei, bei der sie zulässigerweise einen ordnungsgemäß laufenden Vertrag mit kreditorischem Risiko eingemeldet haben (vgl. DSK-Beschluss vom 11.06.2018), auch zuverlässig die Beendigung eines solchen Vertrags wieder mitzuteilen, um der Auskunftei die dortige Löschung des Vertragsverhältnisses zu ermöglichen.

Diese Beendigungsmeldung hat im Regelfall ohne schuldhaften Zeitverzug zu erfolgen.

Eine lediglich zeitlich aufschiebende Ausnahme hiervon gestehen wir den Kreditinstituten in solchen Fällen zu, in denen der Vertrag aktuell noch offene Zahlungsverpflichtungen hat. Werden verbleibende Zahlungsverpflichtungen per SEPA-Lastschrift beglichen, tolerieren wir zudem einen zeitlichen Versatz der Beendigungsmeldung in Höhe von acht Wochen ab der Lastschrift. Innerhalb dieser Frist kann einer autorisierten Lastschrift widersprochen werden; die Zahlung würde damit vorerst rückgängig gemacht werden.

Im Berichtszeitraum sind wir bei einem Kreditinstitut auf zwei weitere Fragestellungen aufmerksam geworden:

Zum einen erfolgte bei diesem Kreditinstitut die Beendigungsmeldung auch dann erst mit zeitlichem Versatz, wenn der Ausgleich des Vertragskontos per Überweisung erfolgte. Da bei einer Überweisung anders als bei Lastschriften keine Befugnis eingeräumt ist, die Zahlung einseitig rückgängig zu machen, ist hier kein zeitlicher Versatz der Beendigungsmeldung zulässig.

Zum anderen wandte die Bank bezüglich der Dauer des zeitlichen Versatzes generell einen Zeitraum von zwei Monaten statt von acht Wochen an, was in der Berechnung regelmäßig eine längere Frist bedeutet, als bzgl. des Lastschriftrisikos erforderlich wäre. Der Zeitraum, der die acht Wochen übersteigt, ist demnach unzulässig.

7

Werbung

7 Werbung

7.1 Kundenbindungsprogramme – welche Rechtsgrundlage gilt?

Im Rahmen eines Kundenbindungsprogrammes kann es zu vielen unterschiedlichen Verarbeitungsvorgängen kommen. Die taugliche Rechtsgrundlage für den jeweiligen Verarbeitungsvorgang hängt dabei von dem mit der Verarbeitung verfolgten Zweck und den konkreten Umständen ab.

Im Berichtszeitraum haben wir uns wiederholt mit Fragestellungen hinsichtlich der Rechtmäßigkeit von Datenverarbeitungen im Rahmen von Kundenbindungsprogrammen beschäftigt. Zumeist handelte es sich um Beratungsanfragen von Datenschutzbeauftragten, daneben beteiligten wir uns gemeinsam mit den anderen deutschen Aufsichtsbehörden auch an einem Kooperationsverfahren zwischen den mitgliedsstaatlichen Aufsichtsbehörden.

Wie man sich leicht vorstellen kann, können im Rahmen eines Kundenbindungsprogrammes eine Vielzahl unterschiedlicher Verarbeitungen stattfinden (insbesondere Verarbeitungen zur Durchführung des Kundenbindungsprogramms, Verarbeitung zu Werbezwecken, Auswertung von Datensätzen, Einbindung von Dienstleistern). Die Rechtmäßigkeit dieser Verarbeitungen hängt dabei von den konkreten Umständen der jeweiligen Verarbeitung ab, insbesondere dem mit ihr verfolgten Zweck.
Datenverarbeitungen, welche die Erfüllung der sich aus dem Kundenbindungsprogramm ergebenden Verpflichtungen – insbesondere das Sammeln, Einlösen und Verwalten der Punkte – ermöglichen sollen, können nach Art. 6 Abs. 1 Uabs. 1 Buchstabe b DS-GVO gerechtfertigt sein. Hierzu ist es erforderlich, dass mit der Teilnahme am Kundenbindungsprogramm ein Vertrag begründet wird, dass dieser Vertrag gültig ist und dass die Verarbeitung für die Erfüllung des Vertrages objektiv erforderlich ist. Letzteres Kriterium wurde erst kürzlich vom EuGH in seiner Entscheidung vom 04. Juli 2023 (C-252/21 - Meta Platforms u. a., Rn. 98) dahingehend konkretisiert, dass der Verantwortliche nachweisen können muss, inwiefern der Hauptgegenstand des Vertrages ohne die betreffende Verarbeitung nicht erfüllt werden könnte. Zur Bestimmung des „Hauptgegenstandes des Vertrages" können auch die in Rn. 32, 33 der „Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchst. b DS-GVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen" beschriebenen Kriterien herangezogen werden. Dabei ist zu berücksichtigen, dass der Hauptgegenstand des Vertrages nicht einseitig von dem Verantwortlichen festgesetzt oder erweitert werden kann.

Hauptgegenstand des Vertrages über die Teilnahme am Kundenbindungsprogramm ist in der Regel das Sammeln, Einlösen und Verwalten von Punkten. Daher sind grundsätzlich nur Verarbeitungen, die zur Erfüllung dieser Tätigkeiten objektiv unerlässlich sind, nach Art. 6 Abs. 1 Uabs. 1 Buchstabe b DS-GVO gerechtfertigt.

Alle weiteren Datenverarbeitungen bedürfen eines anderen Rechtfertigungsgrundes gem. Art. 6 Abs. 1 Uabs. 1 DS-GVO. In Betracht kommen dabei insbesondere Art. 6 Abs. 1 Uabs. 1 Buchstaben a und f DS-GVO.

So können Verarbeitungen, die der Verhinderung eines Missbrauchs bzw. Betruges dienen, gem. Art. 6 Abs. 1 Uabs. 1 Buchstabe f DS-GVO gerechtfertigt sein, wenn sie objektiv zu diesem Zweck erforderlich und nicht derart intensiv sind, dass die Interessen oder Grundrechte und

Grundfreiheiten der betroffenen Person überwiegen.

Kunden sollen jedoch nicht nur dadurch, dass sie bei ihren regulären Einkäufen Punkte o. ä. sammeln können, sondern auch mit speziellen, möglichst passgenauen Werbeaktionen darüber hinaus motiviert werden, Einkäufe zu tätigen bzw. Dienstleistungen in Anspruch zu nehmen. Hierzu ist es erforderlich, Kunden in Werbezielgruppen einzuteilen, um mit passenden Angeboten und ggf. mit besonderen Angeboten (z. B. günstigeres Angebot, Bonusprodukte, Vielfachpunkte) bewerben zu können. Soweit die personenbezogenen Daten zu Werbezwecken verarbeitet werden, kommt es hinsichtlich der einschlägigen Rechtsgrundlage insbesondere auch auf den Kommunikationsweg und auf die Begleitumstände an, z. B. wie umfassend die Datensätze analysiert werden, ob sich aufgrund einer Selektion vielleicht sogar ein zusätzlicher Erkenntnisgewinn (Wahrscheinlichkeitswerte) ergibt.

Danach ist die Datenverarbeitung zu Zwecken der postalischen Direktwerbung regelmäßig von Art. 6 Abs. 1 Uabs. 1 Buchstabe f DS-GVO gedeckt, soweit keine eingriffsintensiven Maßnahmen, wie z. B. eine eingriffsintensive Auswertung, erfolgt. Allerdings ist zu berücksichtigen, dass die Verarbeitung bei besonders umfassender Personalisierung nach der Rechtsprechung des EuGHs einer Einwilligung der betroffenen Person bedarf (EuGH Urteil vom 04. Juli 2023, C-252/21 - Meta Platforms u. a., Rn. 117 f.).

Bei Werbung per Telefon oder E-Mail sind die Wertungen des § 7 Abs. 2, 3 des Gesetzes gegen den unlauteren Wettbewerb (UWG) zu berücksichtigen, wonach grundsätzlich eine Einwilligung einzuholen ist. Soweit wettbewerbsrechtlich eine Einwilligung gefordert wird, ist eine solche auch datenschutzrechtlich zu fordern. Die Voraussetzungen der Rechtsgrundlage des Art. 6 Abs.1 Uabs. 1 Buchstabe f DS-GVO sind dann gerade nicht erfüllt, da die Interessenabwägung nicht zugunsten des Verantwortlichen ausfallen kann (vgl. auch Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung, Kapitel 1.4).

7.2 Wahlwerbung

Parteien können Adressdaten aus dem Melderegister zu Zwecken der Wahlwerbung nutzen. Die Verarbeitung von Daten aus anderen Quellen zu diesem Zweck ist kritisch zu prüfen.

Mehrere Personen, die im Zusammenhang mit der Landtagswahl von politischen Parteien angeschrieben wurden, wandten sich an uns, um zu erfahren, woher die Parteien ihre personenbezogenen Daten bezogen hatten und ob die Verarbeitung ihrer personenbezogenen Daten zu Zwecken der Wahlwerbung zulässig war.

Im Zusammenhang mit der Verarbeitung personenbezogener Daten zu Zwecken der politischen (Wahl-)Werbung informierten wir regelmäßig über folgendes:

Parteien, Wählergruppen und andere Träger von Wahlvorschlägen dürfen nach dem Melderecht die Adressdaten bestimmter Wählergruppen in den sechs der Wahl oder Abstimmung vorangehenden Monaten aus dem Melderegister für Zwecke der Wahlwerbung erhalten, wobei sich die Auskunft regelmäßig auf die Adressdaten einzelner Altersgruppen (Jungwähler/Senioren o ä.), nicht jedoch auf alle Wahlberechtigte/Betroffene in der jeweiligen Melderegion erstreckt (§ 50 Bundesmeldegesetz - BMG). Die Person oder Stelle, der die Daten übermittelt werden, darf diese nur für die Werbung bei einer Wahl oder Abstimmung verwenden und hat sie spätestens einen Monat nach der Wahl oder Abstimmung zu löschen oder zu vernichten (§ 50 Abs. 1 S. 3 BMG). Wer eine solche Datenübermittlung durch die Meldebehörde für die Zukunft unterbinden möchte, muss direkt gegenüber dem örtlichen Einwohnermeldeamt der

Veröffentlichung / Weitergabe an Dritte widersprechen (§ 50 Abs. 4 BMG).

Zusätzlich verwiesen wir auf die ausführliche Veröffentlichung des Bayerischen Landesbeauftragten für den Datenschutz zur Thematik "Auskunft aus dem Melderegister an politische Parteien vor Wahlen / Wahlwerbung" unter https://www.datenschutz-bayern.de/datenschutzreform2018/aki28.html

In einigen Verfahren stellte sich jedoch heraus, dass die personenbezogenen Daten, die zu Zwecken der politischen Wahlwerbung verarbeitet wurden, nicht aus dem Melderegister, sondern aus anderen Quellen wie z. B. Kundendateien oder für bestimmte andere Zwecke angelegte Verzeichnisse stammten. Die Daten, die in einem anderen Zusammenhang unter Umständen auch von einem anderen Verantwortlichen erhoben wurden, wurden – ohne dass dies für die betroffenen Personen erwartbar war – für die Adressierung von Wahlwerbung verwendet. In derartigen Fällen sehen wir weder die postalische noch die elektronische Bewerbung als zulässig an, es sei denn, es liegt eine Einwilligung der betroffenen Person vor.

7.3 Verwendung von Teststellen-Registrierungsdaten für Werbezwecke

Kontaktdaten, die im Zusammenhang mit der Registrierung bei Corona-Teststellen erhoben wurden, dürfen nicht verwendet werden, um Werbung zu verschicken.

Im Berichtszeitraum erhielten wir mehrere Beschwerden dazu, dass personenbezogene Daten, die im Zusammenhang mit der Registrierung bei einem Corona-Testzentrum in den Jahren 2021 und 2022 angegeben wurden, zur Versendung von Werbung genutzt wurden.

Die Fälle unterschieden sich insofern, als die Daten einerseits von den Teststellenbetreibern selbst, die außerhalb der Corona-Pandemie anderweitig unternehmerisch tätig waren (z. B. Möbelgeschäft), zweckfremd verarbeitet und andererseits von Personen, die für ein Testzentrum gearbeitet hatten, weisungswidrig verarbeitet wurden.

Werden personenbezogene Daten, die ursprünglich durch den Verantwortlichen, hier dem Teststellenbetreiber, rechtmäßig verarbeitet wurden, zweckentfremdet genutzt, bedarf es entweder einer Einwilligung, einer mitgliedstaatlichen oder nationalen Rechtsvorschrift oder muss die Verarbeitung mit dem ursprünglichen Zweck vereinbar sein (Art. 6 Abs. 4 DS-GVO).

Schwingt sich hingegen ein in einem Testzentrum tätiger Mitarbeiter aufgrund einer eigenmächtigen und weisungswidrigen Datenverarbeitung selbst zum Verantwortlichen gem. Art. 4 Nr. 7 DS-GVO auf, so führt die Rechtswidrigkeit der Erhebung regelmäßig auch zu einer Rechtswidrigkeit der weiteren Verwendung.

Die Zusendung von E-Mail-Werbung bedarf hier aber in jedem Fall bereits aufgrund der wettbewerbsrechtlichen Voraussetzungen einer Einwilligung gem. Art. 4 Nr. 11, 7 DS-GVO: Die Wertungen des Gesetzes gegen den unlauteren Wettbewerb (UWG) sind bei der datenschutzrechtlichen Bewertung mit zu berücksichtigen. Da § 7 Abs. 2 Nr. 2 UWG regelt, dass bei Werbung mit elektronischer Post eine vorherige ausdrückliche Einwilligung des Adressaten vorliegen muss, hat dies zur Folge, dass die Voraussetzungen der neben einer Einwilligung einzig in Frage kommenden Rechtsgrundlage – Art. 6 Abs. 1 Uabs. 1 Buchstabe f DS-GVO – nicht erfüllt sind. Vor allem aufgrund des wettbewerbsrechtlichen Einwilligungsbedürfnisses ist nämlich von einem überwiegenden Interesse der betroffenen Personen auszugehen (vgl. hierzu die Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO),

Kapitel 1.4, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/OH-Werbung_Februar%202022_final.pdf

Aber auch bei der Verarbeitung personenbezogener Daten zu Zwecken der postalischen Direktwerbung liegen bei derartigen Konstellationen die Voraussetzungen des Art. 6 Abs. 4 i. V. m. Abs. 1 Uabs. 1 Buchstabe f DS-GVO nicht vor und es bedarf einer Einwilligung. Weder ist die Verarbeitung zu Werbezwecken mit dem ursprünglichen Zweck (Erhebung von Daten zu Abrechnungs- und Nachweiszwecken) vereinbar, noch erwartet ein Kunde eines Testzentrums, dass seine personenbezogenen Daten von dem Teststellenbetreiber oder von weiteren weisungswidrig handelnden Personen für die Zusendung von Werbung genutzt werden.

8

Industrie und Handel, Wohnungswirtschaft

8 Industrie und Handel, Wohnungswirtschaft

8.1 Kaffeebestellung mit Namensaufruf

Selbst in banalen Alltagssituationen wie der Bestellung eines Kaffees, den Kunden an der Theke selbst entgegennehmen, können sich datenschutzrechtliche Fragen stellen. Ein ausschließlich mündlicher und nicht an ein Dateisystem gebundener Gebrauch des Namens führt jedoch nicht zur Anwendung des Datenschutzrechts.

Im Rahmen einer Beschwerde wurde moniert, dass in einem Café die Kundinnen und Kunden, die ihr Heißgetränk an der Theke bestellen, um Nennung ihres Vornamens gebeten werden. Grund hierfür war bzw. ist, die zubereiteten Getränke den an der Theke wartenden Kunden zuordnen zu können.

Das Datenschutzrecht findet auf den beschriebenen Vorgang jedoch keine Anwendung, so dass darin auch kein Datenschutzverstoß liegt. Es fehlt sowohl an einer zumindest teilweise automatisierten Verarbeitung personenbezogener Daten als auch an einer Verarbeitung in einem Dateisystem, was nach Art. 2 Abs. 1 DS-GVO aber Voraussetzung für die Anwendbarkeit der Datenschutz-Grundverordnung wäre. Die von den Kunden genannten Namen wurden nicht mit einer Datenverarbeitungsanlage verarbeitet, auch nicht in das Kassensystem eingegeben, sondern von den Mitarbeitern lediglich mündlich untereinander weitergegeben und beim Aufruf des Namens genannt. Selbst wenn die Vornamen eventuell auf Zetteln unter Angabe des jeweiligen Getränks notiert würden, wäre es eher fernliegend, hier von einem „Dateisystem" auszugehen. Denn nach der gesetzlichen Definition in Art. 4 Nr. 6 DS-GVO ist ein Dateisystem eine strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind. Soweit Namenszettel lediglich ungeordnet auf dem Tresen liegen und nach Namensaufruf entsorgt werden, fehlt es an dem Merkmal der Strukturiertheit einer Datensammlung. Zudem wäre die Sammlung allenfalls nach einem einzigen Kriterium – dem bestellten Getränk – auswertbar, während die gesetzliche Begriffsdefinition die Auswertbarkeit nach mindestens zwei Kriterien voraussetzt, so dass die Zettel auch aus diesem Grund kein Dateisystem im datenschutzrechtlichen Sinne bilden.

Ungeachtet dessen kann Kundinnen und Kunden, die auch jenseits der Anwendbarkeit des Datenschutzrechts auf ihre Anonymität bedacht sind, empfohlen werden, auch in der beschriebenen Situation statt ihres realen Vornamens ein frei gewähltes Pseudonym anzugeben. Denn auch damit lassen sich die bestellten Getränke dem richtigen Kunden und der richtigen Kundin zuordnen, so dass eine Angabe des Vornamens nicht erforderlich ist.

8.2 Online-Formular für die (un-)verbindliche Anfrage bei einem Campingplatz

Bei der Datenverarbeitung im Zusammenhang mit unverbindlichen Verfügbarkeitsanfragen und verbindlichen Reservierungsanfragen über die Homepage ist konkret zu prüfen, auf welcher Befugnisnorm personenbezogene Daten der anfragenden Person sowie der Mitreisenden verarbeitet werden dürfen.

Im Berichtszeitraum beschäftigten wir uns insbesondere im Zusammenhang mit Campingplätzen mit der Frage, welche personenbezogenen Daten und auf welcher Grundlage ein Verantwortlicher bei einer unverbindlichen Platzanfrage sowie bei einer späteren Reservierung eines Platzes verarbeiten darf.

Bei der Überprüfung eines Verantwortlichen, der bundesweit Campingplätze betreibt und der sowohl für die unverbindliche Verfügbarkeitsanfrage als auch für die verbindliche Reservierung bei allen seinen Campingplätzen ein und dasselbe Formular nutzte, mussten wir feststellen, dass personenbezogene Daten im Übermaß von der anfragenden bzw. reservierenden Person sowie Mitreisenden erhoben wurden, ein Bewusstsein für die einschlägige Befugnisnormen nicht vorhanden war und in der Folge nicht nur die Anforderungen des Gesetzes nicht erfüllt und die betroffenen Personen nicht hinreichend über die Datenverarbeitungen informiert wurden.

Insbesondere wurden zahlreiche personenbezogene Daten abgefragt, deren Verarbeitung entgegen der Auffassung der Verantwortlichen nicht mit Art. 6 Abs. 1 Uabs. 1 Buchstabe b DS-GVO gerechtfertigt war. Die Datenverarbeitung auf dieser Grundlage ist nur dann rechtmäßig, wenn die Verarbeitung zur Durchführung eines Vertrages mit der betroffenen Person oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist. Die betroffene Person muss hierzu nachweisen können, dass eine Vertragsanbahnung nicht möglich ist bzw. der Hauptgegenstand des Vertrages ohne die betreffende Verarbeitung nicht erfüllt werden könnte (vgl. EuGH in seiner Entscheidung vom 04. Juli 2023, Rs. C-252/21 - Meta Platforms u. a., Rn. 98). Zur Bestimmung des „Hauptgegenstandes des Vertrages" können auch die in Rn. 32, 33 der „Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DS-GVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen" beschriebenen Kriterien herangezogen werden.

Uns konnte beispielsweise in dem Verfahren die Erforderlichkeit der Verarbeitung sowohl der postalischen Adresse als auch der E-Mail-Adresse und der Telefonnummer im Zusammenhang mit der bloßen Verfügbarkeitsanfrage nicht nachgewiesen werden (vgl. Art. 5 Abs. 2 DS-GVO), so dass die Erhebung allenfalls auf Grundlage einer Einwilligung gem. Art. 6 Abs. 1 Uabs. 1 Buchstabe a DS-GVO der betroffenen Person zulässig gewesen wäre. Aber auch im Zusammenhang mit einer verbindlichen Reservierung eines Platzes sahen wir es als nicht für die Durchführung des Vertrages erforderlich an, zahlreiche Kontaktdaten zu verarbeiten. Zwar mag es Situationen geben, in denen eine schnelle Kontaktaufnahme zielführend ist (z. B. bei Unwetterwarnungen), allerdings sahen wir eine Verarbeitung von Kontaktdaten, die über diejenigen, die zur Vertragserfüllung erforderlich waren, hinausgingen, in dem von uns bearbeiteten Verfahren allenfalls auf Grundlage des Art. 6 Abs. 1 Uabs. 1 Buchstabe f DS-GVO als zulässig an.

Auch hinsichtlich der Verarbeitung des vollständigen Geburtsdatums aller mitreisenden Personen konnten wir in dem Verfahren keine Erforderlichkeit erkennen. Diese Verarbeitung wurde zunächst damit begründet, dass sich die Übernachtungspreise für die Stellplätze aus der Anzahl und dem Alter der Reisenden zusammensetzen würden. Bei Überprüfung der Preisstaffelung stellten wir jedoch fest, dass diese unterschiedliche Preise für verschiedene Altersstufen vorsah (0-3 Jahre, 4-15 Jahre, Erwachsene). Eine Abfrage des vollständigen Geburtsdatums konnte somit hiermit nicht begründet werden, sondern es war hierzu vielmehr ausreichend, das Alter der Mitreisenden zum Zeitpunkt des Aufenthaltes zu erfragen. Auch Ausführungen dazu, dass das Geburtsdatum für die Berechnung einer Kurtaxe erforderlich sei, die teilweise bei den von dem Verantwortlichen betriebenen Plätzen altersabhängig einzuziehen sei, wobei mittels des Online-Systems die Daten automatisch in das auszudruckende und dann vor Ort zu unterschreibende Formular übernommen wurden, konnten eine pauschale Zulässigkeit der Verarbeitung der Geburtsdaten aller Mitreisenden nicht begründen. Vielmehr könnte das Geburtsdatum, soweit es im Zusammenhang mit der konkret anfallenden Kurtaxe in einer Kommune

überhaupt vollständig erforderlich wäre, bei der Reservierung dieses konkreten Platzes erhoben werden. Dies bedingt freilich, dass dann, wenn die Homepage eines bestimmten Campingplatzes aufgerufen wird, sich jedenfalls das Formular von den Formularen für Anfragen und Reservierungen zu den sonstigen Campingplätzen des Verantwortlichen unterscheiden muss und auch die Datenschutzinformationen entsprechend zu gestalten sind.

Soweit zur Begründung der Verarbeitung von personenbezogenen Daten von Mitreisenden über die auf der Homepage befindlichen Formulare das Bundesmeldegesetz angeführt wurde, mussten wir zudem darauf hinweisen, dass gem. § 29 Abs. 2 BMG insbesondere mitreisende Angehörige auf dem Meldeschein nur der Zahl nach anzugeben sind.

8.3 Selbstauskünfte bei Vermietung

Auch 2023 wurden bei der Mietersuche Daten über das erforderliche Maß hinaus verarbeitet.

Trotz unserer fokussierten Prüfung "Selbstauskunftsbögen für Mietinteressenten" und der damit einhergehenden Öffentlichkeitsarbeit, über die wir in unserem letztjährigen Tätigkeitsbericht (12. Tätigkeitsbericht, Kapitel 15.3) berichtet haben, erreichten uns weiterhin Kontrollanregungen und Beschwerden dazu, dass Vermieter und Vermieterinnen, Makler und Maklerinnen sowie Hausverwaltungen bereits bevor ein erster Besichtigungstermin stattfand und die sich interessierende Person ein konkretes, auf die tatsächliche Anmietung abzielendes Interesse an der bestimmten Wohnung gezeigt hat, umfangreiche Fragen an diese gerichtet hatten. Diese enthielten nach unserer Überprüfung häufig zahlreiche, zum Zeitpunkt des Erstkontaktes und teilweise auch für die späteren Auswahlphasen unzulässige Fragen, die dann zu einer Datenverarbeitung im Übermaß führen. Die Konsequenz einer solchen Feststellung ist einerseits, dass wir die Verantwortlichen auffordern, ihre Fragebögen und die damit einhergehenden Datenverarbeitungen in Einklang mit den Vorgaben der DS-GVO zu bringen. Bei einem festgestellten Verstoß drohen darüber hinaus Maßnahmen gem. Art. 58 Abs. 2 Buchstabe b und i DS-GVO (Verwarnung bzw. Bußgeld).

Teilweise stellten wir aber auch fest, dass gerade Verantwortliche, die nur wenige Wohneinheiten vermieten, sich hinsichtlich der Fragestellungen an z. B. online auffindbaren Fragebögen orientieren bzw. diese bei der Erstellung des eigenen Fragebogens heranziehen. Um ein abgestimmtes Muster für eine Selbstauskunft zur Verfügung stellen zu können, erarbeitete eine Unterarbeitsgruppe des Arbeitskreises Wirtschaft der Datenschutzkonferenz, an der wir uns beteiligt haben, einen entsprechenden Vorschlag, der als Anlage an die ebenfalls durch die Unterarbeitsgruppe aktualisierte Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressent:innen beigefügt wurde. Die aktualisierte Orientierungshilfe vom 24.01.2024 mitsamt Anlage ist auf der Homepage der Datenschutzkonferenz veröffentlicht.

9

Beschäftigtendatenschutz

9 Beschäftigtendatenschutz

9.1 Mitnahme von Bewerberdaten eines Personalvermittlungsunternehmens

Wenn ein Mitarbeiter personenbezogene Daten für eigene Zwecke weiterverarbeitet, wird er selbst zum Verantwortlichen.

Im Zuge eines Beschwerdeverfahrens stellte sich heraus, dass ein Mitarbeiter des Personalvermittlungsunternehmens A die Kontaktdaten eines Bewerbers an das Personalvermittlungsunternehmen B übermittelt hatte, zu dem der Mitarbeiter kurze Zeit später wechselte.

Das Personalvermittlungsunternehmen B sprach den Bewerber an, der sich mit einer Beschwerde an uns wandte, weil er zu dem Unternehmen B vorher noch keinen Kontakt hatte und die personenbezogenen Daten insbesondere nicht im Internet öffentlich auffindbar waren. Welche personenbezogenen Daten das Unternehmen B von ihm verarbeitete, hatte er zuvor durch eine Auskunft gem. Art. 15 DS-GVO erfahren. Hierbei wurde ihm jedoch keine Information zur Herkunft der Daten mitgeteilt. Allerdings war ihm der konkrete Mitarbeiter des Unternehmens B bekannt, da er mit diesem, als dieser noch Mitarbeiter des Unternehmens A gewesen ist, Kontakt gehabt hatte.

Uns gegenüber stellten sowohl der Mitarbeiter als auch das Unternehmen B dar, dass die Kontaktdaten des Beschwerdeführers in einem beruflichen Kontaktnetzwerk frei zugänglich gewesen und diese von dort erhoben worden seien. Die Veröffentlichung der in Frage kommenden personenbezogenen Daten in dem Netzwerk wurde jedoch von dem Beschwerdeführer bestritten und konnte weder seitens des Mitarbeiters noch des Unternehmens B nachgewiesen werden. Vielmehr habe der Beschwerdeführer diese an die damalige personalisierte E-Mail-Adresse des Unternehmens A geschickt.

Das Unternehmen A als bisheriger Arbeitgeber des betreffenden Mitarbeiters wies darauf hin, dass es interne Vorgaben gebe, die die Weitergabe von Bewerberdaten an Dritte ausdrücklich untersage und dass dies dem Mitarbeiter auch bekannt und bewusst gewesen sei. Da das Unternehmen nach unserer Prüfung alles Mögliche getan hat, konnte diesem wegen der zweckwidrigen Verwendung der Daten durch den Mitarbeiter kein Vorwurf gemacht werden. Vielmehr handelte es sich um einen Fall des Mitarbeiterexzesses, bei dem der Mitarbeiter sich bewusst über die internen Vorgaben hinwegsetzte und so selbst zum Verantwortlichen gem. Art. 4 Nr. 7 DS-GVO wurde. Seine Datenübermittlung an das Unternehmen B war mangels Befugnis als unzulässig zu bewerten.

9.2 Speicherung von Bewerberdaten nach Absage

Bei Bewerbungen auf konkrete Stellen sind die personenbezogenen Bewerberdaten spätestens sechs Monate nach Ablehnung der sich bewerbenden Person zu löschen.

In einem Beschwerdeverfahren beschäftigten wir uns mit einem Bewerbungsportal, das von einem Unternehmen in unserem Zuständigkeitsbereich betrieben wurde. Personen, die sich für eine konkrete Stelle oder allgemein innerhalb der weltweit agierenden Unternehmensgruppe bewarben, mussten ihre Bewerbungsunterlagen zentral auf das Bewerbungsportal hochladen, von wo aus sie sich dann auf verschiedene Stellen innerhalb der Unternehmensgruppe bewerben konnten.

Vor der Verarbeitung der Daten wurde eine Einwilligung der Bewerberinnen und Bewerber eingeholt, wonach die Bewerberdaten drei Jahre gespeichert werden. Soweit eine sich bewerbende Person ihre Daten früher löschen lassen wollte, konnte dies aktiv verlangt werden. Ein Link zum Unterstützungsinstrument, über das die Löschung eingeleitet werden konnte, befand sich in der Einwilligungserklärung. Soweit eine Löschung im Zuge nach der Ablehnung einer sich auf eine konkrete Stelle bewerbenden Person begehrt wurde, erfolgte eine Löschung im Anwendungsbereich des deutschen Rechts, insbesondere des Allgemeinen Gleichbehandlungsgesetzes (AGG) nach Ablauf von sechs Monaten, nachdem die Absage an die sich bewerbende Person erteilt wurde.

Allerdings konnte das Bewerbungsportal ohne eine Einwilligung u. a. in die dreijährige Speicherung der Bewerberdaten nicht genutzt werden. Das Unternehmen wies diesbezüglich darauf hin, dass es bei den im Rahmen der Bewerbungsplattform durchgeführten Datenverarbeitungsvorgängen nicht nur der DS-GVO unterliege, sondern auch den Gesetzen der Staaten, in denen Bewerber ansässig sind oder eine Konzerngesellschaft, die eine Stelle anbietet, niedergelassen ist. Die Bewerber kommen auch aus verschiedenen Ländern außerhalb der EU.

Nach Art. 6 Abs.1 Uabs. 1 Buchstabe b DS-GVO (im Lichte der EuGH-Rspr. C-34/21) können personenbezogene Daten von (künftigen) Beschäftigten, d. h. auch von Bewerbern, zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, verarbeitet werden, wenn dies erforderlich ist.

Nach einer Ablehnung einer sich auf eine konkrete Stelle bewerbenden Person erkennen wir im Anwendungsbereich des AGG die Notwendigkeit an, die personenbezogenen Daten der Bewerber auf Grundlage des Art. 6 Abs. 1 Uabs. 1 Buchstabe b DS-GVO bis zu sechs Monate (ab dem Eingang der Ablehnung) zu speichern, um bei Ansprüchen und Klagen nach dem AGG reagieren zu können. Nach Ablauf dieser Frist müssen die personenbezogenen Daten aktiv durch den Verantwortlichen gelöscht werden. Eine Ausnahme gilt nur dann, wenn eine wirksame Einwilligung in eine weitere Speicherung und Verarbeitung der Bewerberdaten seitens der sich bewerbenden Person abgegeben wurde.

In dem uns vorliegenden Vorgang wurden die personenbezogenen Daten der sich auf eine konkrete Stelle bewerbenden Personen jedoch erst nach drei Jahren automatisiert gelöscht, soweit die betroffene Person nicht aktiv eine frühere Löschung forderte. Diese dreijährige Speicherung wurde mit der Einwilligung der sich auf eine konkrete Stelle bewerbenden Person begründet. Allerdings ist notwendige Voraussetzung für die Wirksamkeit der Einwilligung die Freiwilligkeit sowie eine unmissverständlich abgegebene Willenserklärung in die Datenverarbeitung (Art. 4 Nr. 11 DS-GVO). Die betroffene Person muss danach bei der Erteilung der Einwilligung in die dreijährige Speicherung die freie Wahl haben, d. h. es muss neben der vom Unternehmen praktizierten Vorgehensweise eine Alternative geben. Daran fehlt es jedoch vorliegend. Ganz im Gegenteil, war es nicht möglich, das Bewerbungsportal zur Bewerbung auf eine konkrete Stelle ohne Erteilung der entsprechenden Einwilligung zu nutzen. Die Möglichkeit, eine frühzeitigere Löschung der Bewerberdaten, d. h. nach Ablauf von sechs Monaten nach Absage, verlangen zu können, stellt außerdem lediglich ein sog. „Opt-out" dar, sodass die Voraussetzung der Abgabe einer unmissverständlich abgegebenen Willenserklärung ebenfalls nicht erfüllt gewesen ist.

Die Ermittlungen in dem konkreten Beschwerdeverfahren ergaben, dass die personenbezogenen Daten des Beschwerdeführers jeweils nach Aufforderungen zur Löschung nach Ablauf von sechs Monaten nach erteilter Absage gelöscht worden waren und führten dazu, dass der

Bewerbungsprozess insgesamt neu aufgesetzt wird.

10

Vereine

10 Vereine

10.1 Datenschutzstrukturen in Vereinen

Hoher Bedarf an Unterstützung für Vereine kann nicht gedeckt werden.

Im Berichtszeitraum konnten wir feststellen, dass der Beratungsbedarf in datenschutzrechtlichen Fragestellungen bei Vereinen im Vergleich zu den Vorjahren wieder deutlich angestiegen ist.

Zum Zeitpunkt des Inkrafttretens der DS-GVO haben wir zahlreiche – über die Veröffentlichung von Beiträgen auf der Homepage hinausgehende – Informationsangebote gemacht, um die wichtige Vereinsarbeit mit ihren ehrenamtlichen Strukturen zu unterstützen. So konnten wir z. B. mit unseren bayernweit angebotenen Informationsveranstaltungen gute Erfahrungen machen. Mit diesen erreichten wir eine Sensibilisierung für datenschutzrechtliche Fragen bei den Vereinen, die dann wiederum zu konkreten Beratungsanfragen bei uns führten.

Wir bedauern sehr, dass wir diese wichtige Unterstützung und präventive Tätigkeit aufgrund des bei uns bestehenden Personalmangels und der damit einhergehenden Konzentration auf unsere gesetzlichen Pflichtaufgaben nicht mehr im gebotenen Umfang leisten können. Unsere Beratungstätigkeit reduziert sich aktuell grundsätzlich nur noch auf die Anfragen, zu deren Beantwortung wir gesetzlich verpflichtet sind (z. B. Beratung von Datenschutzbeauftragten gem. § 40 Abs. 6 BDSG). Lediglich in besonderen Einzelfällen beantworten wir darüber hinaus die bei uns eingehenden Beratungsanfragen. Vereine konnten wir deshalb nur bei wenigen Anfragen unterstützen, wie beispielsweise in dem unter Ziffer 10.3 zu findenden Bericht.

Unsicherheiten, zum Teil sogar Unkenntnis hinsichtlich der datenschutzrechtlichen Vorgaben fiel uns jedoch nicht nur aufgrund der vermehrten Anfragen, sondern auch bei der Bearbeitung von Beschwerden im Vereinskontext auf. Ausreichende datenschutzrechtliche Regelungen, Festlegungen und Vorkehrungen im Umgang mit personenbezogenen Daten, insbesondere von (ehemaligen) Mitgliedern, wurden in den von uns bearbeiteten Fällen häufig nicht oder nur rudimentär getroffen.

Oftmals hing das Verständnis davon, wie mit den personenbezogenen Daten umgegangen werden soll, an den mit den Daten umgehenden Personen innerhalb eines Vereins. Nicht selten bestand selbst im Vereinsvorstand und bei weiteren Funktionsträgern keine oder jedenfalls keine einheitliche Vorstellung vom Datenumgang, was vielerlei Konsequenzen nach sich zog.

So führte die Befürchtung, sich nicht datenschutzkonform zu verhalten, dazu, dass manche eigentlich zulässige Verarbeitungen nicht stattfanden und „der Datenschutz" als hindernd und ggf. überflüssig angesehen wurde. Fehlende Absprachen dazu, wie personenbezogene Daten aufbewahrt werden und wie notwendige Zugriffe geordnet erfolgen, hatten zur Folge, dass – teilweise auf privaten Rechnern verschiedener Personen – nicht synchronisierte bzw. nicht aktuell gehaltene Mitgliederdaten gespeichert wurden. Innerhalb des Vereins war dann auch nicht bekannt, wer welche Daten wo speichert.

Insbesondere Personalwechsel, ohne dass klare Regelungen für die Übergabe bzw. die weitere Verarbeitung der personenbezogenen Daten vorhanden waren, führten zu Schwierigkeiten. So hatte sich z. B. ein Verein darauf verlassen, dass das von einem Vereinsmitglied entwickelte Verwaltungsprogramm für Vereinsmitglieder dauerhaft zur Verfügung steht und jedenfalls keine schriftliche Vereinbarung hierzu getroffen. Als das Vereinsmitglied den Verein verließ, fehlte dem Verein die Zugriffsmöglichkeit auf das Mitgliederverwaltungsprogramm und die

alleine dort verarbeiteten personenbezogenen Daten. Es stellte sich sodann die Frage, wie der Verein wieder an „seine" personenbezogenen Daten gelangt und wie sichergestellt werden kann, dass das ausgeschiedene Mitglied die personenbezogenen Daten löscht bzw. tatsächlich gelöscht hat.

Unter anderem solche intransparenten Vorgehensweisen und z. B. die hieraus resultierenden Schwierigkeiten bei der Bearbeitung von Betroffenenersuchen gem. Art. 12 ff. DS-GVO (z. B. Auskunft, Löschung) hatten eine hohe Verunsicherung bei den Mitgliedern und eine Einbindung unsererseits zur Folge.

Konkret stellte sich immer wieder die Frage, wer bzw. welche Funktionsträger in einem Verein personenbezogene Daten wie verarbeiten dürfen, wer welche Daten zur Kenntnis nehmen darf, was veröffentlicht werden bzw. veröffentlicht bleiben darf, wie und wie lange Datenbestände verwaltet und aufbewahrt werden dürfen, um vor allem den Grundsätzen der Richtigkeit, der Speicherbegrenzung sowie der Integrität und Vertraulichkeit (Art. 5 Abs. 1 Buchstabe d bis f DS-GVO) gerecht zu werden.

Für Transparenz und Kontinuität sorgen vereinbarte und niedergeschriebene Regeln, Richtlinien oder Übersichten zur Datenverarbeitung. Sie geben allen im Verein tätigen und sonstigen beteiligten Personen eine Orientierung und sind hilfreich, um zum Beispiel bestimmte Datenverarbeitungsprozesse im Zusammenhang mit einem Mitgliederbei- oder austritt zu definieren, Zugriffsrechte im Verein zu regeln oder Aufbewahrungspflichten festzuhalten. Entsprechende Datenschutzregelungen können entweder teilweise bereits in die Vereinssatzung oder in einem gesonderten Regelwerk („Datenschutzordnung" o ä. bezeichnet) aufgenommen werden.

Mit einer Verschriftlichung erfüllt der Verein mitunter auch seine datenschutzrechtlichen Pflichten. Vereine unterfallen bei der (teil-)automatisierten Verarbeitung bzw. dann, wenn personenbezogene Daten z. B. in Papierakten/Papierordnern aufbewahrt werden, den gleichen datenschutzrechtlichen Pflichten wie andere Verantwortliche gem. Art. 4 Nr. 7 DS-GVO. Sie sind deshalb verpflichtet, sich mit den datenschutzrechtlichen Anforderungen der DS-GVO auseinanderzusetzen und diese einzuhalten. Hierzu gehört es auch, die Datenverarbeitungen im und durch den Verein zu definieren und zu regeln.

Im Regelfall besteht somit auch aufgrund der regelmäßigen Verarbeitung von Mitgliederdaten eine Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten gem. Art. 30 DS-GVO, wonach insbesondere schriftlich festzuhalten ist, welche Daten zu welchem Zweck verarbeitet werden und an welche Stellen diese offenbart werden.

Dabei sollte auch mit Blick auf die jeweils konkrete Verarbeitung geregelt werden, wer zu dem jeweils bestimmten Zweck wie Zugriff auf die personenbezogenen Daten nehmen kann. Hilfreich kann es sein, eine Vereinssoftware zu nutzen und dort z. B. Rollen für die Funktionsträger und deren Vertretungen sowie Löschroutinen einzurichten. Denn gerade dann, wenn an verschiedenen Stellen innerhalb des Vereins z. B. Mitgliederlisten geführt werden, diese jedoch nicht zentral oder gleichlaufend aktualisiert sind, kann es dazu kommen, dass in eiligen Situationen bzw. Situationen „außer der Reihe" nicht aktuell gehaltene Listen oder Verteiler verwendet werden und so z. B. Newsletter oder nur für einen bestimmten Empfängerkreis bestimmte Informationen an einen veralteten Empfängerkreis geschickt werden.

Sowohl die Erarbeitung von Regelungen als auch die (verpflichtende) Dokumentation erfordern, dass man sich mit dem Datenumgang im Verein auseinandersetzt, sowie Zweck und Rechtmäßigkeit der stattfindenden Datenverarbeitungen hinterfragt. Auch wenn die mitunter

aufwändige und zeitintensive Auseinandersetzung mit den eigenen Datenverarbeitungsprozessen eine hohe Belastung für Vereine und Ehrenamtliche bedeutet, kann ein Verein mehrfach hiervon profitieren: Einerseits erfüllt der Verein seine datenschutzrechtlichen Pflichten, andererseits kann aber die damit einhergehende Transparenz das Vertrauen der Mitglieder sowie von Interessenten steigern. Gerade bei der Neugewinnung von Mitgliedern ist das Vertrauen in einen ordentlichen (Daten-)Umgang ein starkes Argument, umgekehrt kann ein zu sorgloser Umgang Vereinsmitglieder abschrecken. Häufig handelt es sich hier auch um Daten von Kindern oder um Gesundheitsdaten, deren Schutzbedarf in der Regel als besonders hoch anzusehen ist.

Auch wenn wir unsere Beratungstätigkeit im Vereinskontext einschränken mussten, veröffentlichen wir weiterhin zahlreiche Informationen zur Datenverarbeitung im Verein auf unserer Homepage (https://www.lda.bayern.de/de/thema_vereine.html, https://www.lda.bayern.de/de/faq.html).

Unter anderem können Sie auf der Informationsseite ein Muster für ein Verzeichnis von Verarbeitungstätigkeiten finden.

10.2 Gefälschte Dokumente bei der Zuchtzulassung

Kopien einer E-Mail (Cc:) dürfen nur an einen berechtigten Empfängerkreis geschickt werden.

Werden E-Mails an mehrere Personen im Verein verschickt, ist nicht immer eindeutig, wer aus welchem Grund im Verteiler aufgenommen wurde.

Gerade die Verwendung privater E-Mail-Adressen im Vereinskontext führt zu einer Verunsicherung bei den betroffenen Personen. Enthält die E-Mail-Adresse nämlich keinen Klarnamen, so ist nicht ohne weiteres ersichtlich, wer sich hinter der E-Mail-Adresse verbirgt und ob diese Person berechtigt Kenntnis von den Kontaktdaten und dem Inhalt der E-Mail erhält.

Exemplarisch möchten wir deshalb über einen Vorgang berichten, bei dem durchaus sensible Informationen an einen Verteilerkreis, der nicht selbsterklärend war, weitergeleitet wurden:

Ein Mitglied eines Hundezuchtvereins beschwerte sich bei uns darüber, dass es eine E-Mail erhalten habe, die in Kopie weiteren Empfängern, die nicht zum Vorstand des Vereins gehörten, gesendet wurde.

Mit der in Rede stehenden E-Mail entzog der Hauptzuchtwart dem Mitglied mit sofortiger Wirkung eine zuvor erteilte Zuchtzulassung. Begründet wurde dies damit, dass im Rahmen der Zuchtprüfung gefälschte Dokumente vorgelegt wurden, um einen zuchtausschließenden Fehler zu vertuschen.

Anlässlich des Vorganges beschäftigten wir uns mit dem Ziel, die Rechtmäßigkeit der Offenlegung der personenbezogenen Daten des Mitglieds bewerten zu können, zunächst mit Fragestellungen rund um die Hundezucht sowie dem entsprechenden Regelwerk.

Unsere Ermittlungen zu dem Sachverhalt ergaben, dass das Mitglied mit einem Hund an einer Zuchtzulassungsprüfung teilgenommen hatte. In der Prüfung wurde festgestellt, dass dem Tier Zähne fehlen. Da dies eigentlich ein Ausschlusskriterium von der Zuchtzulassung darstellt, legte das Mitglied am Prüfungstag ein Gutachten vor, um die Notwendigkeit der Zahnentfernung bei dem Tier zu belegen.
Der Verein forderte jedoch zusätzlich eine Bestätigung des Tierarztes bzgl. der Zahnentfernung. Eine solche Bestätigung wurde im Nachgang der Prüfung vorgelegt. Es stellte sich jedoch heraus, dass es sich um ein gefälschtes Dokument handelte.
Aufgrund der gefälschten Dokumente und des Versuchs, den zuchtausschließenden Fehler zu

vertuschen, wurde die zuvor erteilte Zuchtzulassung mit sofortiger Wirkung entzogen.

Hierzu sandte der Hauptzuchtwart die in Rede stehende E-Mail an das Mitglied sowie in Kopie an den Zuchtrichter, die restlichen Vorstandsmitglieder und die nach der Zuchtordnung in allen züchterischen Fragen mit einzubeziehende Zuchtkommission.

Im Ergebnis konnten wir keinen Datenschutzverstoß feststellen, da die Datenverarbeitung gem. Art. 6 Abs. 1 Buchstabe b DS-GVO zulässig gewesen ist.

10.3 Personalausweiskopie als Identitätsnachweis bei Vereinen

Kopien eines Personalausweises sind regelmäßig nicht erforderlich.

Wir erhalten regelmäßig Nachfragen oder Beschwerden dazu, dass Personalausweise kopiert wurden. Nicht selten geschieht dies trotz eines deutlichen Hinweises darauf, dass der Anfertigung einer Kopie nicht zugestimmt wird. Auch im Vereinskontext erreichten uns im Berichtszeitraum mehrere Beratungsanfragen sowie Beschwerden zu Personalausweiskopien.

Wie bereits unter Ziffer 10.1 dargestellt, fehlen uns leider die Kapazitäten, um Beratungsanfragen, für deren Beantwortung keine gesetzliche Pflicht besteht, zu bearbeiten. In Einzelfällen, z. B. bei folgeschweren Anfragen insbesondere von Vereinen, ist zwar kein ausführlicher Austausch mit dem anfragenden Verein und keine tiefergehende Beratung möglich, allerdings versuchen wir in dem uns möglichen Maß zumindest auf die wichtigsten Aspekte hinzuweisen und die Vereine entsprechend zu sensibilisieren.

Nur in diesem Umfang konnten wir deshalb eine Anfrage eines Vereins, der sozial schwachen Menschen mit schweren Erkrankungen finanzielle Hilfe gewährt, bearbeiten.

Die Anträge auf die finanzielle Unterstützung des Vereins werden von den Kliniken der Region gestellt. Dazu füllen die Sozialarbeiter der Klinik ein Formblatt aus, wobei personenbezogene Daten der antragsstellenden Person angegeben werden. Geht ein Antrag bei dem Verein ein, wird von dort aus mit der unterstützungssuchenden Person Kontakt aufgenommen.

Der Verein wollte wissen, ob er Personalausweiskopien von den Personen, denen eine finanzielle Unterstützung gewährt wird, zu Zwecken der Identifizierung anfordern und aufbewahren darf.

Wir haben den Verein auf die Vorgaben des Personalausweisgesetzes hingewiesen und ihm mitgeteilt, dass das Kopieren eines Personalausweises grundsätzlich nur mit Zustimmung des Personalausweisinhabers zulässig ist (Art. 20 Abs. 2 Sätze 1 und 3 PAuswG). Soweit eine Überprüfung der Identität im Zusammenhang mit der Antragsbewilligung erforderlich sein sollte, empfahlen wir aufgrund des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 Buchstabe c DS-GVO) lediglich eine Sichtprüfung. Diese kann von der abgleichenden Person dokumentiert werden.

11

Videoüberwachung

11 Videoüberwachung

11.1 Bodycam im Einkaufszentrum

Der Umfang der behördlichen Untersuchungspflicht beschränkt sich auf den angemessenen Umfang im jeweiligen Einzelfall.

In einem Verfahren wies das Bayerische Verwaltungsgericht Ansbach eine Klage eines Beschwerdeführers auf aufsichtliches Tätigwerden durch uns im Zusammenhang mit dem Einsatz einer Bodycam ab.

Der Beschwerdeführer hatte sich bereits im Jahr 2021 bei uns darüber beschwert, dass rechtswidrig Aufnahmen mittels Bodycam von ihm angefertigt wurden. Der Beschwerdeführer hatte während der Corona-Pandemie auf einer Bank in einem Einkaufszentrum sein Mittagessen verspeist und wurde aufgrund der geltenden Hausordnung, die den Verzehr von Speisen und Getränken verbot, durch den Sicherheitsdienst des Gebäudes verwiesen. Daraufhin habe sich der Beschwerdeführer auf eine Bank im Außenbereich des Einkaufszentrums niedergelassen. Auch hier sei er von dem Sicherheitsdienst des Platzes verwiesen worden. Der Beschwerdeführer sah den Bereich, in dem die Bank stand, als nicht vom Hausrecht des Einkaufszentrums umfasst, was er auch gegenüber dem Sicherheitsdienst äußerte. Daraufhin habe der Sicherheitsdienst ohne weitere Ankündigung die Bodycam angeschaltet und den Beschwerdeführer beim Essen gefilmt.

Aufgrund eines Nutzungsvertrages für den Außenbereich zwischen der Kommune und dem Betreiber des Einkaufszentrums kamen wir zu dem Ergebnis, dass der Beschwerdegegner dort das Hausrecht hat. Da zudem im Nachgang nicht mehr aufgeklärt werden konnte, inwieweit sich der Beschwerdeführer gegebenenfalls, wie vom Beschwerdegegner vorgetragen, aggressiv verhalten hatte und ob die Bodycam tatsächlich ohne Ankündigung aktiviert worden war, konnten wir keinen datenschutzrechtlichen Verstoß feststellen. Aus diesem Grund ergriffen wir auch keine aufsichtlichen Maßnahmen gegenüber dem Beschwerdegegner.

Hiergegen wandte sich der Beschwerdeführer mit einer Klage auf aufsichtliches Tätigwerden unsererseits an das Gericht.

Das Gericht stellte zunächst fest, dass es unsere Aufgabe ist, den Gegenstand einer Beschwerde in angemessenen Umfang zu untersuchen (Art. 57 Abs. 1 Buchstabe f DS-GVO). Was hierunter zu verstehen sei, sei konkret bezogen auf den jeweiligen Einzelfall durch eine Gegenüberstellung des Untersuchungsaufwands, gegebenenfalls der Eingriffsintensität der Untersuchungsmaßnahme in die Rechte Dritter und des zu erwartenden Untersuchungserfolges zu ermitteln. Dies habe zum Hintergrund, dass die Aufsichtsbehörden darauf angewiesen sind, ihre Ressourcen möglichst effektiv einzusetzen. Zudem ergab die Überprüfung des Gerichts, dass sich ein Verstoß gegen Art. 6 Abs. 1 Uabs. 1 Buchstabe f DS-GVO in Verbindung mit der Orientierungshilfe der Datenschutzaufsichtsbehörden zu dem Einsatz von Bodycams durch private Sicherheitsunternehmen (Stand 22. Februar 2019; zu finden unter https://www.datenschutzkonferenz-online.de/media/oh/20190222_oh_bodycams.pdf) nicht feststellen ließ.

Insbesondere lagen und liegen nach Auffassung des Gerichts keine weitergehenden Untersuchungsmöglichkeiten vor, ob sich der Beschwerdeführer aggressiv verhalten hat, da die Aufnahmen der Bodycam zwischenzeitlich bereits gelöscht worden waren. Weiterhin stellte das Gericht fest, dass der Beschwerdegegner entsprechend unserer Auffassung Inhaber des Hausrechts über die in Rede stehende Fläche gewesen ist. Auch war aus Sicht des Gerichtes aufgrund der sich widersprechenden Aussagen

nicht mehr aufklärbar, ob der Beschwerdeführer über den Bodycam-Einsatz (ausreichend) informiert wurde.

Da ein Verstoß gegen datenschutzrechtliche Bestimmungen seitens des Gerichts nicht festgestellt werden konnte und somit kein Anspruch auf aufsichtlichen Einschreitens bestand, wurde die Klage abgewiesen.

Die Entscheidung des Verwaltungsgerichts ist noch nicht rechtskräftig.

11.2 Verkehrssicherheit durch Videoüberwachung und Datenanalyse

Bei allgemeinen Interessen wie „die Gewährleistung der Verkehrssicherheit", handelt es sich in der Regel um kein konkretes, individuelles berechtigtes Interesse im Sinne des Art. 6 Abs. 1 Uabs. 1 Buchstabe f DS-GVO.

Um die Verkehrssicherheit zu gewährleisten wollte ein Unternehmen Kameras in den Lieferfahrzeugen ihrer Subunternehmer (Auslieferer) anbringen lassen. Die Kameras sollten sowohl den Innen- als auch den Außenbereich der Fahrzeuge erfassen. Das Unternehmen wollte die gewonnenen Videoaufnahmen und die Telematikdaten mittels einer Software auswerten, um unsichere Fahrweisen erkennen zu können.

Hierzu sollte mit den oben genannten Informationen ein Fahrerscore errechnet werden. Anhand dieses Scores könnten dann die Fahrer in verschiedene Kategorien (gut/mittel/schlecht) eingeteilt werden. Je nach Kategorisierung und Fehlerquellen sah das Konzept vor, den guten und mittleren Fahrern Trainings zum Selbststudium anzubieten, während schlechte Fahrer an den jeweiligen Arbeitgeber (Subunternehmer) gemeldet werden sollten, damit diese speziellen Schulungen angeboten werden konnten.

Die Kameraaufnahmen sollten neben dem Verkehrssicherungszweck auch weiteren Zwecken dienen. Zum Schutz der Fahrer war eine Notfallknopf-Funktion geplant. Außerdem sollten die Kameraaufnahmen zur Beweissicherung bei Unfallgeschehen genutzt werden können (Dashcamfunktion).

Das Unternehmen kam vor Einsatz des Systems mit einer Beratungsanfrage auf uns. Nach Auffassung des Unternehmens ließ sich die Datenverarbeitungen auf Art. 6 Abs. 1 Uabs. 1 Buchstabe f DS-GVO stützen.

Da wir jedoch die Voraussetzungen für eine datenschutzkonforme Verarbeitung der personenbezogenen Daten von Passanten und weiteren Verkehrsteilnehmern sowie bei den Fahrern nicht erkennen konnten, teilten wir dem Unternehmen mit, dass wir den Einsatz eines solchen Systems untersagen werden, sollte dieses zum Einsatz gelangen.

Insbesondere konnten wir in dem Interesse, die Verkehrssicherheit zu gewährleisten, kein konkretes berechtigtes Interesse des Unternehmens erkennen. Das Geschäftsmodell des Unternehmens unterschied sich in keiner Weise von den Modellen anderer ebenso am Markt tätigen Lieferdienste. Ein besonderes individuelles Interesse für die Videoüberwachung und die sich anschließende Verarbeitung konnte nicht erkannt werden. Selbst bei Annahme eines berechtigten Interesses des Unternehmens war die Erforderlichkeit der Datenverarbeitungen nicht hinreichend nachgewiesen.

Hinsichtlich der Verarbeitung zu Beweissicherungszwecken mussten wir feststellen, dass die Voraussetzungen an einen Dashcam-Einsatz nicht eingehalten wurden (vgl. hierzu https://www.datenschutzkonferenz-online.de/media/oh/20190128_oh_positionspapier_dashcam.pdf).

Mit Blick auf die Fahrer, deren Daten zum Zweck der Überprüfung des Fahrverhaltens verarbeitet

werden sollten, die aber durch die Kategorisierung und die ständige Erfassung des Fahrverhaltens nach unserer Einschätzung einem permanenten Überwachungs- und Leistungsdruck ausgesetzt würden, konnten weder das Unternehmen noch die Subunternehmer (Arbeitgeber der Fahrer) die Rechtmäßigkeit der Verarbeitung begründen.

12

Gesundheit und Soziales, Versicherungen

12 Gesundheit und Soziales, Versicherungen

12.1 Umfang des Auskunftsrechts ggü. einer Kieferorthopädiepraxis

Die vom Verantwortlichen unentgeltlich zur Verfügung zu stellende Kopie personenbezogener Daten umfasst weder einen Anspruch auf Herausgabe von kieferorthopädischen Modellen im Original noch auf kostenfreie Anfertigung eines Duplikats.

In einem Fall machte die betroffene Person gegenüber dem Verantwortlichen, einer Praxis für Kieferorthopädie, ihr Auskunftsrecht gem. Art. 15 DS-GVO geltend und forderte u. a. die Herausgabe eines von der Praxis angefertigten kieferorthopädischen Modells im Original, alternativ die kostenfreie Anfertigung eines Duplikats.

Die betroffene Person hatte gegenüber dem Verantwortlichen ein Recht auf Auskunft über die von diesem verarbeiteten personenbezogenen Daten (Art. 15 Abs. 1 DS-GVO). Der Verantwortliche hat auch eine unentgeltliche Kopie dieser Daten zur Verfügung zu stellen (Art. 15 Abs. 3 S. 1 DS-GVO). Dies bedeutet, dass der betroffenen Person eine originalgetreue und verständliche Reproduktion aller vom Verantwortlichen verarbeiteten personenbezogenen Daten ausgefertigt werden muss. Dagegen hat die betroffene Person grundsätzlich keinen Anspruch auf Zurverfügungstellung einer Fotokopie sämtlicher Dokumente, die u. a. sie betreffende personenbezogene Daten enthalten.

Die „Kopie" gem. Art. 15 Abs. 3 S. 1 DS-GVO umfasst nicht die Herausgabe eines Modells im Original oder die kostenfreie Anfertigung eines Duplikats. Zwar wurden im Rahmen der Herstellung des kieferorthopädischen Modells auch personenbezogene Gesundheitsdaten der betroffenen Person verarbeitet. Einer Aushändigung des Modells im Original stehen jedoch bereits berufsrechtliche Aufbewahrungs-/Dokumentationspflichten der Praxis entgegen (Art. 15 Abs. 4 DS-GVO). Die betroffene Person kann nach unserer Einschätzung auch keine kostenfreie Anfertigung eines Duplikats verlangen, denn dies käme letztlich der Zurverfügungstellung einer Fotokopie im o. g. Sinne gleich.

In derartigen Fällen bietet es sich an, dass der Verantwortliche der betroffenen Person die Begutachtung des Modells in den Praxisräumlichkeiten oder die Zurverfügungstellung von Fotografien des Originals in Aussicht stellt.

12.2 Granularität der Nachweispflicht gem. Art. 7 Abs. 1 DS-GVO bei Versicherungen

Der Nachweis einer wirksam eingeholten Einwilligung ist bei mehreren, in einer gemeinsamen Erklärung eingeholten Einwilligungen für jede Einwilligung gesondert zu führen.

Ein Beschwerdeführer monierte, dass seine Versicherung im Rahmen der Leistungsprüfung einen Operationsbericht ohne seine Einwilligung bei Dritten angefordert hatte. Wir forderten den Verantwortlichen zur Stellungnahme auf und wiesen ihn auf die ihm obliegende Nachweispflicht gem. Art. 7 Abs. 1 DS-GVO hin.

Der Verantwortliche hatte dem Beschwerdeführer eine Einwilligungs- und Schweigepflichtentbindungserklärung vorgelegt. Diese – vom Beschwerdeführer in ihrer Gesamtheit unterzeichnete – Erklärung bestand aus mehreren separaten Einwilligungen, teils mit Auswahlmöglichkeiten für die betroffene Person. Hinsichtlich der Abfrage von Gesundheitsdaten bei Dritten im Rahmen der Leistungsprüfung konnte der Be-

schwerdeführer wählen, ob er dem Verantwortlichen eine allgemeine Einwilligungs- und Schweigepflichtentbindungserklärung erteilt oder eine einzelfallbezogene Einholung wünscht. Der Beschwerdeführer hatte jedoch bezüglich dieses Punktes der Erklärung keine Auswahl getroffen.

Die gleichwohl erfolgte Anforderung von Gesundheitsdaten durch die Versicherung war somit rechtswidrig, da der Verantwortliche die Einholung einer wirksamen Einwilligung für die spezielle, vom Beschwerdeführer monierte Verarbeitung nicht nachweisen konnte. Die bloße Unterzeichnung der Erklärung genügte hierfür nicht, da in dieser mehrere separate Einwilligungen eingeholt wurden.

13

Rechtsanwältinnen und Rechtsanwälte

13 Rechtsanwältinnen und Rechtsanwälte

13.1 E-Mail-Kommunikation von Rechtsanwältinnen und Rechtsanwälten

Die E-Mail-Kommunikation von Rechtsanwältinnen und Rechtsanwälten kann auch ohne Einwilligung der betroffenen Person sowie ohne Inhaltsverschlüsselung zulässig sein.

In mehreren Beschwerden monierten die betroffenen Personen, dass die verantwortlichen Rechtsanwältinnen und Rechtsanwälte ohne ihre Einwilligung per E-Mail mit ihnen kommunizierten und die erhaltenen Nachrichten nicht inhaltsverschlüsselt waren.

Nach unserer Auffassung erfordert die E-Mail-Kommunikation von Rechtsanwälten nicht per se eine Einwilligung der betroffenen Person, insbesondere dann nicht, wenn es sich bei der betroffenen Person nicht um die eigene Mandantschaft handelt. Vielmehr kommt in diesen Fällen auch eine Verarbeitung aufgrund berechtigter Interessen des Rechtsanwalts gem. Art. 6 Abs. 1 S. 1 Buchstabe f DS-GVO in Betracht. Falls die betroffene Person der Nutzung ihrer E-Mail-Adresse durch den Rechtsanwalt widerspricht, ist dieser Umstand vom Rechtsanwalt zu prüfen und in der Interessenabwägung entsprechend zu berücksichtigen (Art. 21 Abs. 1 DS-GVO). Gleichwohl kann es Fallgestaltungen geben, in denen auch gegen den Willen der betroffenen Person eine Kommunikation per E-Mail zulässig ist, beispielsweise wenn keine alternativen Kontaktmöglichkeiten der betroffenen Person bekannt sind und im konkreten Einzelfall besondere Eilbedürftigkeit besteht.

Bei Verarbeitung personenbezogener Daten per E-Mail haben Rechtsanwälte geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko im Einzelfall angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen schließen ggf. die Verschlüsselung personenbezogener Daten mit ein (Art. 32 Abs. 1 Buchstabe a DS-GVO). Eine Transportverschlüsselung erachten wir stets für erforderlich; besteht im Einzelfall ein hohes Risiko, muss zusätzlich eine Inhaltsverschlüsselung vorgenommen werden. Der Umstand, dass Rechtsanwälte berufsrechtlich zur Verschwiegenheit verpflichtet sind, führt jedoch nicht dazu, dass bei jeglichem E-Mail-Versand durch diese von einer Hochrisikoverarbeitung auszugehen wäre. So kann beispielsweise eine Terminerinnerung auch lediglich transportverschlüsselt versandt werden.

13.2 Rechtswidrige Offenlegung personenbezogener Daten durch unpräzise Adressierung

Beim Versand von Dokumenten mit personenbezogenen Daten ist darauf zu achten, dass beim Empfänger nur diejenigen Personen Kenntnis erlangen, für die die Unterlagen bestimmt sind.

Eine Rechtsanwaltskanzlei hatte dem Arbeitgeber der betroffenen Person eine Forderungsaufstellung betreffend einen zuvor erlassenen Pfändungs- und Überweisungsbeschluss übersandt. Dieses Schreiben wurde – trotz der im Vorfeld vom Arbeitgeber geäußerten Bitte um Übersendung an die Personalabteilung mit Vertraulichkeitsvermerk – an die allgemeine Firmenadresse versandt. Hierdurch erlangten verschiedene Personen außerhalb der Personalabteilung Kenntnis vom Pfändungsvorgang.

Gemäß den Grundsätzen der Integrität und Vertraulichkeit müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor

unbefugter Verarbeitung (Art. 5 Abs. 1 f) DS-GVO). Werden Dokumente mit personenbezogenen Daten versandt, ist daher darauf zu achten, dass beim Empfänger nur diejenigen Personen Kenntnis erlangen, für die die Unterlagen bestimmt sind. Eine Kenntnisnahme durch Unbefugte ist möglichst auszuschließen. Dies gilt unabhängig von etwaigen seitens der betroffenen Person oder Dritter geäußerten Bitten.

Im Ergebnis hielten wir die Übersendung der Forderungsaufstellung an die allgemeine Firmenadresse für rechtswidrig. Es wäre nach unserer Auffassung erforderlich gewesen, das entsprechende Schreiben an die Personalabteilung zu richten.

14

Datenschutz im Internet

14 Datenschutz im Internet

14.1 App-Prüfung

Fokussierte Prüfung zum Einsatz einwilligungspflichtiger Dienste bei Apps.

Entsprechend unserer Ankündigung im 11. Tätigkeitsbericht 2022 unter Punkt 5, waren Apps im Jahr 2023 verstärkt Gegenstand unserer aufsichtlichen Tätigkeit im Bereich Telemedien.

Im 4. Quartal 2023 wurde eine Prüfung verschiedener Apps aus unterschiedlichen Themenbereichen, wie beispielsweise Parken, Kundenbindungssysteme, Supermärkte oder Versicherungen eingeleitet. Der Fokus der Prüfung liegt auf den Vorgängen, die bei erstem Öffnen der jeweiligen App durchgeführt werden. Oftmals erfolgen bereits einwilligungspflichtige Vorgänge wie beispielsweise das Auslesen von IDs aus dem Smartphone direkt nach Installation der App, ohne dass Nutzende mit einem Einwilligungsbanner interagieren und somit ohne dass über eine rechtswirksame Einwilligung entschieden werden konnte.

Einige App-Betreiber verzichteten sogar komplett auf Einwilligungsbanner und beriefen sich auf Geräteeinstellungen, die das App-Tracking unterbinden könnten. Dies war vor allem bei iOS-Geräten häufiger der Fall, da Apple mit der Funktion „App Tracking Transparency" - kurz ATT - die Möglichkeit bietet, App-Tracking zu erlauben oder zu versagen. Hier ist zu beachten, dass dies keine datenschutzrechtliche Abfrage darstellt, sondern lediglich eine Zusatzfunktion für Nutzende ist, damit deren datenschutzrechtliche Entscheidungen nicht oder nur erschwert umgangen werden können. Eine rechtswirksame Einwilligung kann der App-Betreiber hierüber schon mit Blick auf das Erfordernis der Informiertheit der Einwilligung nicht einholen.

Häufig kamen Dienste wie Google Analytics und Facebook Pixel direkt beim Starten der App zum Einsatz, ohne dass die hierfür notwendige Einwilligung eingeholt wurde. Ob durch diese Dienste personenbezogene Daten verarbeitet werden, bzw. die aus dem Smartphone ausgelesenen Informationen in den Anwendungsbereich der DS-GVO fallen, ist in solchen Fällen zunächst nicht relevant, da in jedem Fall der Anwendungsbereich des § 25 Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) eröffnet ist. Dieser schützt bereits die Integrität des Gerätes an sich und fordert daher regelmäßig eine Einwilligung für das Speichern oder Auslesen von Informationen wie beispielsweise Geräte-IDs.

Den Betreibern der geprüften Apps wurde zwischenzeitlich ein Fragebogen zugesandt, deren Auswertung voraussichtlich im 2. Quartal 2024 erfolgen wird.

14.2 Webtracking nach TTDSG

Wird eine Einwilligung vom Webseiten- oder App-Betreiber nicht eingeholt trotz mittlerweile eindeutiger Rechtslage, prüfen wir die Verhängung eines Bußgelds.

Wie auch in den vergangenen Jahren betraf der Großteil der Eingaben im Bereich Internet den Einsatz von Tracking-Tools auf Webseiten. Wie schon im Tätigkeitsbericht 2021 unter Punkt 5.1 berichtet, besteht für den Einsatz von Cookies und ähnlichen Technologien im Regelfall eine Einwilligungspflicht nach § 25 Abs. 1 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG). Spätestens mit Einführung des TTDSG ist die rechtliche Lage daher eindeutig.

Dennoch betrafen die Eingaben im Bereich Internet zum überwiegenden Teil Webseiten, die einwilligungspflichtige Dienste wie Google Analytics oder Facebook Pixel ohne eine Einwilligung einsetzten.

In den von uns bearbeiteten Fällen haben die Webseiten- und App-Betreiber häufig eine Interessenabwägung, wie sie für Art. 6 Abs. 1 Buchstabe f DS-GVO erforderlich ist, vorgelegt oder damit argumentiert, dass keine personenbezogenen Daten verarbeitet würden.

Wie auch in der „Orientierungshilfe für Anbieter:innen von Telemedien 2021" ausführlich dargestellt, gilt § 25 TTDSG für jede Speicherung von Informationen in der Endeinrichtung eines Endnutzers sowie für jeden Zugriff auf dort gespeicherte Informationen, unabhängig davon, ob personenbezogene Daten verarbeitet werden, und hierbei gilt das Erfordernis einer Einwilligung nach § 25 Abs. 1 TTDSG, sofern nicht die Ausnahmeregelung des Absatz 2 einschlägig ist, d. h. insbesondere wenn der Zugriff auf die Endeinrichtung zur Erfüllung eines Nutzerwunsches unbedingt erforderlich ist.

Das Berufen auf ein berechtigtes Interesse oder die Vornahme einer Interessenabwägung ist daher für die genannten Vorgänge seit Dezember 2021 nicht mehr möglich. Aufgrund der Tatsache, dass § 25 TTDSG nunmehr seit zwei Jahren gilt und auch um zukünftig eine angemessene Abschreckungswirkung zu erzeugen, wurden nun die ersten Fälle in diesem Bereich an die zentrale Bußgeldstelle abgegeben. In den genannten Fällen gehen wir von einem eindeutigen Verstoß gegen § 25 Abs. 1 TTDSG aus.

14.3 Unternehmensverzeichnis der Company Spotter BV

Unternehmensinformationen fallen im Regelfall nicht in den Anwendungsbereich der DS-GVO. Die Verarbeitung personenbezogener Daten bei Unternehmensverzeichnissen kann auf ein berechtigtes Interesse gestützt werden.

Im Berichtszeitraum erreichte uns eine Vielzahl von Eingaben zum Internetauftritt www.companyspotter.com der Company Spotter BV.

Der Verantwortliche betreibt eine Plattform, auf der gezielt nach Unternehmen und Informationen zu diesen Unternehmen gesucht werden kann. Die Unternehmensdaten stammen von den Internetseiten der auf der genannten Webseite gelisteten Firmen, Vereine u. ä. Die Company Spotter BV gibt in ihrer Datenschutzerklärung an, Geschäftszweck sei die Zurverfügungstellung von Datenbanken mit Unternehmensinformationen, insbesondere zur Erleichterung gegenseitiger Kontakte zwischen Unternehmen; Geschäftszweck sei nicht die Zurverfügungstellung von Informationen zu natürlichen Personen.

Anlass für die bei uns eingehenden Beschwerden waren die Informations-E-Mails, die vom Verantwortlichen an jedes betroffene Unternehmen nach der Aufnahme in die Suchmaschine versandt wurde. Die Eingabeführenden bemängelten durchweg, dass sie keine Einwilligung in die Veröffentlichung der Unternehmensdaten erteilt hätten und gingen daher von einem datenschutzrechtlichen Verstoß aus.

Die Company Spotter BV hat ihren Sitz in Den Haag, daher handelte es bei diesen Fällen um grenzüberschreitende Vorgänge. Das bedeutet, dass grundsätzlich die niederländische Datenschutzaufsichtsbehörde federführend für die Bearbeitung dieser Vorgänge zuständig war.

Jedoch haben wir im Rahmen unserer Vorermittlungskompetenz darauf hingewiesen, dass wir in der beschriebenen Verarbeitung von (personenbezogenen) Daten durch die Company Spotter BV aus nachfolgenden Gründen zumindest keinen offensichtlichen Verstoß gegen datenschutzrechtliche Vorschriften sehen:

1. Anwendungsbereich der DS-GVO:

   Nach Art. 1 Abs. 1 enthält die DS-GVO Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung von personenbezogenen Daten und zum

freien Verkehr solcher Daten. Personenbezogene Daten sind nach Art. 4 Nr. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Daher findet die DS-GVO nur dann Anwendung, wenn im betreffenden Einzelfall Daten von natürlichen Personen (nicht z. B. von GmbHs, Vereinen, o. ä.) verarbeitet werden.

2. Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten:

   Soweit im Einzelfall tatsächlich personenbezogene Daten verarbeitet werden, legt die DS-GVO fest, dass personenbezogene Daten nur auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden dürfen, Art. 5 Abs. 1 Buchstabe a) DS-GVO.

   Personenbezogene Daten werden dann rechtmäßig verarbeitet, wenn mindestens eine der Bedingungen des Art. 6 Abs. 1 Buchstabe a) bis f) DS-GVO erfüllt ist. Für die Verarbeitung personenbezogener Daten durch nicht-öffentliche Verantwortliche kommen insbesondere folgende Erlaubnistatbestände in Betracht:

   - die betroffene Person hat ihre Einwilligung gegeben (Art. 6 Abs. 1 Buchstabe a) DS-GVO)
   - die Verarbeitung ist zur Erfüllung eines Vertrages (Art. 6 Abs. 1 Buchstabe b) DS-GVO) oder
   - zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 Buchstabe f) DS-GVO) erforderlich.

Auf ihrer Webseite gibt die Company Spotter BV in ihrer Datenschutzerklärung an, die im Rahmen der Erstellung der Datenbank vorgenommene Verarbeitung von personenbezogenen Daten auf Art. 6 Abs. 1 Buchstabe f DS-GVO (berechtigtes Interesse) zu stützen. Danach ist die Verarbeitung personenbezogener Daten unter folgender Bedingung rechtmäßig: „die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen".

Legale wirtschaftliche Interessen wie das vom Unternehmen verfolgte kommen als berechtigtes Interesse nach Art. 6 Abs. 1 Buchstabe f DS-GVO grundsätzlich in Betracht. Bei der gemäß dieser Vorschrift zudem vorzunehmenden Abwägungsentscheidung finden die Interessen der von einer Veröffentlichung betroffenen Personen aus unserer Sicht in ausreichendem Maße Berücksichtigung, jedenfalls soweit es sich bei den veröffentlichten Daten um Daten handelt, die auch auf andere Weise freiwillig öffentlich zugänglich gemacht wurden, der Verantwortliche die Betroffenen über die Veröffentlichung und die Quelle, aus der die Daten stammen, informiert, ferner keine sensiblen Daten veröffentlicht werden, und den betroffenen Personen im Rahmen der übersandten Informationsmail ein einfach auszuübendes Widerspruchsrecht eingeräumt wird.

Die ausführliche Interessenabwägung des Unternehmens ist ebenfalls Bestandteil der Datenschutzerklärung und kann unter https://www.companyspotter.com/de/legitimate-interest abgerufen werden.

15

Internationaler Datenverkehr

15 Internationaler Datenverkehr

15.1 Binding Corporate Rules – Fortschreibung der Erläuterungen durch den Europäischen Datenschutzausschuss

Zur Unterstützung von antragstellenden Unternehmensgruppen haben die Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten im Jahr 2023 ihre Erläuterungen zu den Anforderungen an BCR weiter präzisiert.

Die Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten waren auch im Berichtszeitraum mit einer großen Anzahl von Genehmigungsverfahren für Verbindliche Unternehmensregelungen zur Übermittlung personenbezogener Daten in Drittländer (Binding Corporate Rules / BCR; Näheres dazu z. B. in unserem 10. Tätigkeitsbericht/2020) befasst. Dieses Übermittlungsinstrument erfreut sich bei Konzernen und konzernähnlichen Unternehmensgruppen ungebrochener Beliebtheit. Da Bayern Standort zahlreicher international tätiger Unternehmensgruppen ist, war unser Haus auch in 2023 erneut an einer Reihe von Genehmigungsverfahren für BCR beteiligt.

Unternehmensgruppen, die Genehmigungsanträge stellen, sollten sich an den Erläuterungen der Aufsichtsbehörden zu den inhaltlichen Anforderungen an BCR orientieren. BCR-Entwürfe werden in einem Verfahren unter Beteiligung der Datenschutzaufsichtsbehörden aller EU-Mitgliedstaaten geprüft und genehmigt. Auf der Basis der laufenden Genehmigungsverfahren haben die Aufsichtsbehörden gemeinsame Maßstäbe zur Prüfung von BCR herausgebildet und entwickeln diese laufend weiter, indem sie gemeinsam die zur Prüfung vorgelegten BCR-Entwürfe mit den darin enthaltenen konkreten Formulierungsvorschlägen auf ihre DS-GVO-Konformität bewerten. So gesehen entsteht auf der Grundlage der in Art. 47 DS-GVO geregelten Anforderungen letztlich Fallrecht, das von einer gemeinsamen Auslegung der gesetzlichen Anforderungen geprägt ist und an dem sich die Aufsichtsbehörden in ihren künftigen Genehmigungsverfahren orientieren.

Um Antragsteller bei der Erstellung von BCR zu unterstützen und ihnen das gemeinsame Verständnis der Aufsichtsbehörden zu den Anforderungen an BCR zu vermitteln, haben die Aufsichtsbehörden schon lange vor Geltungsbeginn der DS-GVO Erläuterungen zu den Anforderungen an BCR sowie entsprechende Antragsformulare in sog. Arbeitsdokumenten (Working Papers) der Artikel-29-Gruppe (des Vorgängergremiums des Europäischen Datenschutzausschusses) veröffentlicht, zuletzt in den Arbeitspapieren 256, 257, 264 und 265 aus dem Jahr 2018. Der Europäische Datenschutzausschuss hatte sich diese Papiere mit Geltungsbeginn der DS-GVO zu eigen gemacht und auf diese Weise seinerzeit für die an BCR interessierte Unternehmensgruppen Kontinuität und Rechtssicherheit gewährleistet.

Im Jahr 2023 hat der EDSA nunmehr auf der Grundlage der Erfahrungen der Aufsichtsbehörden aus der laufenden Genehmigungspraxis seine Erläuterungen an die Anforderungen an BCR (vorerst für die Variante „BCR für Verantwortliche"/BCR-Controllers) weiter fortgeschrieben. Dies erfolgte in Form des am 20.06.2023 beschlossenen Papiers *„Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)"*.

Unser Haus war gemeinsam mit einer weiteren deutschen Aufsichtsbehörde in der Rolle als federführende Berichterstatter im Europäischen Datenschutzausschuss maßgeblich an der Erstellung dieser Erläuterungen beteiligt. Diese mit erheblichem zeitlichem Aufwand verbundene Aufgabe haben wir vor allem aufgrund der

stark überproportionalen Relevanz von BCR für den Zuständigkeitsbereich unseres Hauses sowie unserer praktischen Erfahrungen mit solchen Verfahren übernommen.

Der Einigung im EDSA vorangegangen waren umfangreiche Diskussionen zu zahlreichen Detailfragen, so dass das Papier einen entsprechend hohen Detaillierungsgrad besitzt. Diese Diskussionen waren auch notwendig, weil die Aufsichtsbehörden nur auf diese Weise den gesetzlichen Regelungsauftrag einer gemeinsamen Umsetzung der DS-GVO erfüllen können. Damit ist die Arbeit an diesem Anforderungspapier ein wichtiger Baustein zur einheitlichen Anwendung der DS-GVO durch die Aufsichtsbehörden.

Das Papier enthält zahlreiche Konkretisierungen zu den einzelnen inhaltlichen Anforderungen an BCR, die sich aus den praktischen Erfahrungen mit Genehmigungsanträgen speisen. So wird beispielsweise erläutert, welche Verpflichtungen in BCR zur Umsetzung der vom Europäischen Gerichtshof in seinem Schrems-II-Urteil klargestellten Anforderungen an Drittlandsübermittlungen geregelt werden müssen. Weitere Klarstellungen – um nur einige wenige zu nennen – betreffen etwa die BCR-Klauseln zur Haftung und Durchsetzungsverantwortung für die BCR und zu den Konsequenzen für den Fall der Nichteinhaltung der BCR sowie für den Fall, dass die Bindung eines zunächst an BCR gebundenen Unternehmens endet. Hervorzuheben ist auch, dass die inhaltlichen Anforderungen an BCR sowie das Formblatt für die Antragstellung, die bisher auf unterschiedliche Arbeitspapiere verteilt waren, in einem Papier zusammengefasst wurden. Auch damit soll Antragstellern der Überblick und die Handhabung von BCR erleichtert werden.

Das Papier bewertet auch eine Reihe häufig in BCR-Entwürfen anzutreffender Formulierungsvorschläge mit Blick auf ihre DS-GVO-Konformität. Damit verschafft es Klarheit über die Genehmigungsfähigkeit typischer von Antragstellerseite vorgeschlagener Klauseln und dient auf diese Weise künftigen Antragstellern als Orientierung. Künftige Antragsteller können bei Befolgung der im Papier gegebenen Erläuterungen davon ausgehen, dass die Aufsichtsbehörden BCR-Entwürfe in den entsprechenden Regelungspunkten in aller Regel als genehmigungsfähig betrachten werden. Damit soll das Erläuterungspapier auch einen Beitrag zur Beschleunigung von BCR-Genehmigungsverfahren leisten.

Unternehmen, die bereits genehmigte BCR-C besitzen, müssen nachweisen, dass diese die im verabschiedeten EDSA-Papier dargestellten Anforderungen berücksichtigen. Sie sollten ihre Texte anhand des Anforderungspapiers prüfen und bei Bedarf anpassen; dies gebietet der Grundsatz der Gleichbehandlung der Antragsteller. Die Wirksamkeit bereits erteilter Genehmigungen wird dadurch selbstverständlich nicht angetastet, da solche Anpassungen letztlich lediglich Präzisierungen bestehender BCR im Lichte der laufenden Fallpraxis bzw. zum Teil zur Abbildung neuer Rechtsprechung darstellen. Etwaige notwendig werdende Anpassungen bestehender BCR sind im Zuge der von jedem BCR-Inhaber für das Jahr 2024 turnusmäßig vorzunehmenden Meldung bei der für die BCR federführenden Aufsichtsbehörde anzuzeigen.

Nachdem der EDSA nunmehr die Anforderungen an BCR-Controller präzisiert hat, planen die Aufsichtsbehörden für die Folgezeit eine ähnliche Fortschreibung der inhaltlichen Anforderungen an die zweite „BCR-Variante“, die BCR für Auftragsverarbeiter (BCR-Processor). Auch an diesen Arbeiten, die bereits in der zweiten Jahreshälfte 2023 begonnen haben, ist unser Haus federführend als Berichterstatter im Europäischen Datenschutzausschuss beteiligt.

15.2 EU-U.S. Data Privacy Framework – ist jetzt alles gut?

Für die USA gibt es seit Juli 2023 mit dem sog. Data Privacy Framework einen neuen Angemessenheitsbeschluss der Europäischen Kommission.

Übermittlungen personenbezogener Daten in die USA gehören angesichts der Dominanz großer US-IT-Konzerne im Sektor für Cloud-Dienstleistungen (etwa Hosting oder Software-as-a-Service) bis weit in den Bereich mittelständischer und sogar kleiner Unternehmen in Deutschland und Europa zum Alltag. Diese überaus praxisrelevanten Datenübermittlungen hatte jedoch der Europäische Gerichtshof (EuGH) in seinem „Schrems-II"-Urteil vom 16.07.2020 gehörig durcheinandergewirbelt. In diesem Urteil hatte der EuGH den Angemessenheitsbeschluss der Europäischen Kommission über den sog. EU-U.S. Privacy Shield für ungültig erklärt. Damit galt, gewissermaßen von heute auf morgen, dass in den USA aus Sicht des EU-Datenschutzrechts kein „angemessenes Datenschutzniveau" für personenbezogene Daten mehr bestand. Dies stellte Übermittlungen personenbezogener Daten aus der Europäischen Union an Datenempfänger in den USA vor erhebliche Probleme, zumal der EuGH in demselben Urteil auch die hohen Anforderungen an Übermittlungen unter Verwendung von sog. geeigneten Garantien nach Art. 46 DS-GVO (z. B. Standarddatenschutzklauseln) betont hatte (vgl. dazu unseren 10. und 11. Tätigkeitsbericht für die Jahre 2020 bzw. 2021).

Vor diesem Hintergrund war die Europäische Kommission um eine möglichst schnelle Lösung bemüht. Am 10.07.2023, mit Geltungsbeginn zum selben Tag, erließ die Kommission einen neuen Angemessenheitsbeschluss für die USA – das sog. EU-U.S. Data Privacy Framework (EU-U.S. DPF), in dem sie zu dem Schluss gelangte, dass die USA nach einer Reihe dort erfolgter Anpassungen nunmehr erneut aus EU-Sicht ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten. Die Wirkung des Angemessenheitsbeschlusses erstreckt sich zwar nicht auf die USA als Ganzes, sondern nur auf US-Unternehmen, die sich auf die Einhaltung der in dem Angemessenheitsbeschluss definierten Datenschutzgrundsätze verpflichten, was durch Eintrag des Unternehmens auf einer Liste des US-Handelsministeriums dokumentiert wird. Indes sind dort jedenfalls die allermeisten wichtigen US-Unternehmen und insbesondere die großen Dienstleister aus dem Cloud- und IT-Sektor eingetragen.

Dem Angemessenheitsbeschluss der Europäischen Kommission voraus gegangen waren regulatorische Änderungen auf US-amerikanischer Seite, mit denen den Anforderungen aus dem Schrems-II-Urteils des EuGH Rechnung getragen werden sollte. Hierzu wurde ein neues Rechtsschutzverfahren geschaffen, mit dem betroffene Personen mögliche Zugriffe von US-Behörden zu Zwecken der nationalen Sicherheit auf ihre Daten überprüfen lassen können; weitere Änderungen sollen dem Grundsatz der Verhältnismäßigkeit jeglicher staatlichen Zugriffe auf personenbezogene Daten Rechnung tragen. Dieser neu geschaffene Rechtsschutzmechanismus kann gemäß ausdrücklicher Entscheidung des US-Justizministeriums vom 30.06.2023 unter anderem von Personen genutzt werden, deren Daten aus der Europäischen Union übermittelt wurden.

Zur letztverbindlichen Entscheidung darüber, ob diese auf US-Seite erfolgten Änderungen den Anforderungen des europäischen Rechts tatsächlich genügen, ist allein der Europäische Gerichtshof berufen. Einstweilen ist der Angemessenheitsbeschluss der Kommission jedenfalls – auch für die Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten – ab seinem Geltungsbeginn rechtsverbindlich, so dass auf dieser Grundlage seit diesem Zeitpunkt wieder personenbezogene Daten aus der Europäischen Union in die USA (bzw. genauer: an auf der DPF-

Liste geführte US-Unternehmen) übermittelt werden dürfen, ohne dass Garantieinstrumente nach Ar. 46 DS-GVO wie etwa Standarddatenschutzklauseln und ggf. „zusätzliche Maßnahmen" im Sinne des Schrems-II-Urteils des EuGH zum Einsatz gebracht werden müssten.

Für unsere Tätigkeit als Datenschutzaufsichtsbehörde bedeutet dies, dass wir bei der Prüfung der DS-GVO-Konformität von Übermittlungen personenbezogener Daten in die USA letztlich zu allererst in den Blick nehmen, ob der US-Datenempfänger eine DPF-Zertifizierung besitzt oder nicht und ob die etwaige Zertifizierung die im konkreten Fall übermittelten Daten ihrer Kategorie nach („HR-Data"/Beschäftigtendaten bzw. „Non-HR Data"/sonstige personenbezogene Daten) abdeckt. Besitzt der Empfänger keine Zertifizierung nach dem DPF, so muss das übermittelnde Unternehmen, sofern keiner der Ausnahmetatbestände nach Art. 49 DS-GVO greift, für die Übermittlung geeignete Garantien gemäß Art. 46 DS-GVO verwenden, etwa die Standardvertragsklauseln der Europäischen Kommission für Drittlandsübermittlungen vom 04.06.2021.

Ein „Transfer Impact Assessment" dahingehend, dass der Datenexporteur die Rechtslage im Drittland und ihre Auswirkungen auf den Datenempfänger untersuchen müsste, muss für den Fall, dass eine Datenübermittlung in den Anwendungsbereich des EU-U.S. DPF fällt, nicht durchgeführt werden. Allerdings sollten sich Datenexporteure dennoch Gedanken darüber machen, wie sie auf den Fall eines möglichen Wegfalls eines Angemessenheitsbeschlusses wie etwa des EU-U.S. DPF – etwa einer Ungültigerklärung durch den EuGH wie im Falle des Vorgängerbeschlusses zum EU-U.S. Privacy Shield – reagieren (dazu siehe das nachfolgende Ziffer dieses Tätigkeitsberichts).

15.3 Verhältnis zwischen EU-U.S. Data Privacy Framework und Standarddatenschutzklauseln

Datenübermittlungen auf Grundlage des EU-U.S. Data Privacy Framework benötigen keinen Abschluss von Standarddatenschutzklauseln. Die Standarddatenschutzklauseln können aber vorsorglich für den Fall einer eventuellen späteren Aufhebung des Data Privacy Framework abgeschlossen werden.

Nach Verabschiedung des Angemessenheitsbeschlusses der Europäischen Kommission zum EU-U.S. Data Privacy Framework (EU-U.S. DPF) erreichten uns von Anwenderseite zahlreiche Fragen zum Verhältnis zwischen diesem Instrument und anderen Datenübermittlungsinstrumenten nach Kapitel V der DS-GVO, insbesondere den Standardvertragsklauseln der Europäischen Kommission vom 04.06.2021 für Übermittlungen in Drittländer.

Eine häufige Frage ging dahin, ob Unternehmen, die personenbezogene Daten auf Grundlage des EU-U.S. DPF personenbezogene Daten an US-Empfänger übermitteln, ihre Übermittlungen parallel auch auf Standarddatenschutzklauseln stützen könnten. Hintergrund dieser Frage dürften die Erfahrungen mit der Ungültigerklärung des Vorgänger-Angemessenheitsbeschlusses (EU-U.S. Privacy Shield) durch den Europäischen Gerichtshof (EuGH) im Schrems-II-Urteil vom 16.07.2020 sein. Vor diesem Hintergrund ist verständlich, dass Unternehmen, die Übermittlungen an US-Datenempfänger auf der Grundlage des EU-U.S. DPF vornehmen, für den Fall einer ähnlichen Entwicklung beim EU-U.S. DPF – die nur schwer belastbar vorherzusagen ist – „vorsorgen" möchten.

Nach unserem Verständnis verdrängt ein Angemessenheitsbeschluss nach Art. 45 Abs. 3 S. 1 DS-GVO wie etwa der EU-U.S. DPF in seinem

Anwendungsbereich die in Art. 46 DS-GVO geregelten Garantieinstrumente, darunter auch die Standarddatenschutzklauseln. So verstehen wir den Gesetzeswortlaut von Art. 46 Abs. 1 DS-GVO, denn dieser lautet

> *„Falls kein Beschluss nach Artikel 45 Absatz 3 vorliegt, …".*

Mit Blick auf die oben geschilderten Befürchtungen von Datenexporteuren, sich im Falle einer Ungültigerklärung des EU-U.S. DPF durch den EuGH „über Nacht" in einer Situation wiederzufinden, in der sie personenbezogene Daten ohne eine nach Kapitel V der DS-GVO erforderliche Übermittlungsgrundlage in die USA übermitteln, erscheint indessen ein praxistaugliches Vorgehen dennoch möglich: So spricht aus unserer Sicht nichts dagegen, parallel zu einer auf den EU-U.S. DPF gestützten Übermittlung vorsorglich Standarddatenschutzklauseln abzuschließen, wobei die Klauseln als Übermittlungsinstrument allerdings lediglich unter der Bedingung wirksam sein sollen, dass der Angemessenheitsbeschluss aufgehoben wird. Da es sich hierbei um eine reine Rechtsbedingung handelt, ist ein solch bedingter Abschluss der Standardvertragsklauseln rechtlich möglich. Allerdings muss der datenschutzrechtlich Verantwortliche die betroffenen Personen im Rahmen der ihnen nach Art. 13 Abs. 1 Buchstabe f DS-GVO zu erteilenden Information zutreffend über das verwendete Übermittlungsinstrument informieren, mithin darüber, dass die Übermittlung auf den EU-U.S. DPF gestützt wird, und lediglich für den Fall von dessen Ungültigerklärung auf die Standardvertragsklauseln. Ferner muss sich der Datenexporteur für den Fall, dass für die Übermittlung die Standardvertragsklauseln zum Tragen kommen, im Rahmen eines „Transfer Impact Assessment" (TIA) mit der Rechtslage (und -praxis) des Drittlands auseinandersetzen (siehe dazu den nächsten Beitrag).

15.4 „Transfer Impact Assessment" bei Übermittlungen in die USA auf Grundlage von Art. 46 DS-GVO

Werden personenbezogene Daten in die USA auf Grundlage von Garantien nach Art. 46 DS-GVO übermittelt, muss der Datenexporteur ein „Transfer Impact Assessment" durchführen, bei dem er sich allerdings auf die Feststellungen der Europäischen Kommission aus dem Angemessenheitsbeschluss zum EU-U.S. Data Privacy Framework berufen kann.

Eine weitere uns häufig gestellte Frage zum Verhältnis zwischen EU-U.S. Data Privacy Framework (EU-U.S. DPF) und Garantieinstrumenten nach Art. 46 DS-GVO geht dahin, ob Datenexporteure bei Übermittlungen an US-Empfänger, die nicht auf Grundlage des Angemessenheitsbeschlusses EU-US DPF erfolgen, ein „Transfer Impact Assessment" (TIA) zum US-Recht durchführen müssen. Diese Frage stellt sich für Übermittlungen an US-Empfänger, die keine Zertifizierung nach dem EU-U.S. DPF besitzen und die daher nicht auf den EU-US DPF gestützt werden können und für die daher der Datenexporteur Garantieinstrumente im Sinne von Art. 46 DS-GVO wie etwa Standarddatenschutzklauseln zum Einsatz bringt.

Hintergrund dieser Frage ist das Schrems-II-Urteil des Europäischen Gerichtshofs vom 16.07.2020. Darin hat das Gericht klargestellt, dass Datenexporteure bei allen Übermittlungen in Drittländer, die sie auf sog. geeignete Garantien nach Art. 46 DS-GVO stützen möchten, vorab prüfen müssen, ob der jeweilige Datenempfänger seine im Garantieinstrument eingegangenen Verpflichtungen bei Berücksichtigung der Rechtslage und Praxis im Drittland und insbesondere angesichts des Umfangs des für dortige Behörden möglichen Zugangs zu den übermittelten Daten tatsächlich einhalten

kann. Für diese Prüfung hat sich vielfach der Begriff „Transfer Impact Assessment" eingebürgert. In den Standardvertragsklauseln der Europäischen Kommission (Durchführungsbeschluss Nr. 2021/914 vom 04.06.2021) ist unter Klausel 14 diese Prüfung im Übrigen ausdrücklich vorgeschrieben.

In diesem Zusammenhang kommt dem Umstand Bedeutung zu, dass die Europäische Kommission in ihrem Angemessenheitsbeschluss zum EU-U.S. DPF vom 10.07.2023 zu der Bewertung gelangt ist, dass die auf US-amerikanischer Seite in den letzten Monaten neu eingeführten Rechtsschutzverfahren für betroffene Personen sowie neuer Vorgaben zur Erforderlichkeit und Verhältnismäßigkeit staatlicher Datenzugriffe den Anforderungen des europäischen Rechts genügen. Diese Feststellung der Kommission kommt rechtsverbindliche Wirkung zu, die einzig durch die Kommission selbst oder den Europäischen Gerichtshof aufgehoben werden könnte. Wichtig ist hierbei, dass die auf US-Seite erfolgten regulatorischen Änderungen nach ausdrücklicher Feststellung der Kommission bei jeglicher Übermittlung personenbezogener Daten aus der Europäischen Union in die USA gelten, d. h. unabhängig von dem verwendeten datenschutzrechtlichen Übermittlungsinstrument im Sinne der DS-GVO und somit auch etwa bei Übermittlungen, die auf die Standardvertragsklauseln oder andere Übermittlungsinstrumente nach Art. 46 DS-GVO gestützt werden. Angesichts dessen kann sich der Datenexporteur bei dem ihm abverlangten TIA grundsätzlich auf diese Feststellungen der Kommission berufen und gelangt damit zu demselben Bewertungsergebnis wie die Europäische Kommission. Ein kompletter Verzicht auf die Durchführung eines TIA wäre jedoch auch bei Übermittlungen in die USA nicht möglich. Datenexporteure sollten daher die von ihnen angestellten Überlegungen einschließlich der Bezugnahme auf die Feststellungen der Europäischen Kommission dokumentieren.

15.5 Verhältnis zwischen EU-U.S. Data Privacy Framework und Vertrag zur Auftragsverarbeitung

Der EU-U.S. Data Privacy Framework entbindet nicht von der Notwendigkeit, einen Vertrag zur Auftragsverarbeitung abzuschließen, wenn personenbezogene Daten im Rahmen einer Auftragsverarbeitung in die USA übermittelt werden. In manchen Fällen dieser Art kann es sich anbieten, die auf Übermittlungen an Auftragsverarbeiter in Drittländer zugeschnittenen Module der Standardvertragsklauseln der Europäischen Kommission zu verwenden, da diese auch die Anforderungen an einen Auftragsverarbeitungsvertrag abdecken.

Im Zusammenhang mit dem EU-U.S. DPF erreichte uns von Anwenderseite auch die Frage, ob Datenexporteure bei auf den EU-U.S. DPF gestützten Übermittlungen ungeachtet der DPF-Zertifizierung des US-Datenempfängers mit letzterem einen Vertrag zur Auftragsverarbeitung nach Art. 28 Abs. 3 DS-GVO abschließen müssen, sofern es sich beim US-Datenempfänger um einen Auftragsverarbeiter handelt. Da dies bereits dem Wortlaut des Angemessenheitsbeschlusses selbst ausdrücklich zu entnehmen ist, ist diese Frage zu bejahen. Der Angemessenheitsbeschluss ersetzt mithin nicht die Anforderungen an einen Auftragsverarbeitungsvertrag.

Dies hat vor allem deshalb erhebliche praktische Bedeutung, weil vor Geltungsbeginn des EU-U.S. DPF Übermittlungen an US-Auftragsverarbeiter in der Praxis meist auf die Standardvertragsklauseln der Europäischen Kommission gemäß Kommissionsbeschluss (EU) 2021/914 vom 04.06.2021 gestützt wurden, und die darin enthaltenen Module für Übermittlungen an Auftragsverarbeiter ausweislich von Erwägungsgrund 9 des o. g. Kommissionsbeschlusses die

Anforderungen nach Art. 28 Absätze 3 und 4 DS-GVO an einen Auftragsverarbeitungsvertrag abdecken. Andererseits werden jedoch die Standarddatenschutzklauseln *in ihrer Eigenschaft als Übermittlungsinstrument nach Art. 46 DS-GVO* durch den Angemessenheitsbeschluss zum EU-U.S. DPF verdrängt (dazu siehe oben), soweit der Datenempfänger und die Kategorie der übermittelten Daten vom Anwendungsbereich des Angemessenheitsbeschlusses umfasst sind. Für Übermittlungen, die ab Geltungsbeginns des EU-U.S. DPF und ab Zertifizierung des jeweiligen US-Datenempfängers unter den DPF fallen, könnte vor dem Hintergrund dieser Verdrängungswirkung die Befürchtung Platz greifen, dass ungewollt gegen die Pflicht zum Abschluss eines Auftragsverarbeitungsvertrags verstoßen wird, sobald die Übermittlung nicht mehr auf die Standardvertragsklauseln, sondern auf den DPF gestützt wird. Nach unserem Verständnis kann jedoch mit Blick auf diese Befürchtung Entwarnung gegeben werden, weil der Angemessenheitsbeschluss die Standardvertragsklauseln für Drittlandsübermittlungen *nur in ihrer Wirkung als Übermittlungsinstrument im Sinne von Art. 46 DS-GVO* verdrängt, nicht jedoch soweit die Klauseln die Anforderungen an einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO erfüllen und somit als Auftragsverarbeitungsvertrag zum Einsatz kommen. Dies entspricht augenscheinlich auch dem Verständnis der Europäischen Kommission, die in Ziffer 29 der „Fragen und Antworten" (FAQs) zu ihren Standardvertragsklauseln für Drittlandsübermittlungen vom 04.06.2021 betont hat, dass die Standardvertragsklauseln durchaus auch in Situationen verwendet werden können, in denen der Empfänger in einem Drittstaat befindet, für den ein Angemessenheitsbeschluss nach Art. 45 Abs. 3 DS-GVO besteht; die Kommission betont, dass in diesen Fällen der Datenexporteur die Standardvertragsklauseln zu dem Zweck abschließen kann, die Anforderungen aus Art. 28 DS-GVO zu erfüllen. Auf diese etwas „versteckte" Aussage der Europäischen Kommission sei angesichts der hohen praktischen Relevanz der Frage an dieser Stelle hingewiesen.

16

Technischer Datenschutz und Informationssicherheit

16 Technischer Datenschutz und Informationssicherheit

16.1 Künstliche Intelligenz im Cyberlabor des BayLDA

Hardware-Anschaffungen ermöglichen es dem BayLDA, KI-Modelle lokal zu untersuchen.

Gestartet in den 1950er Jahren als Idee, dass jedes Merkmal von Intelligenz prinzipiell von Maschinen simuliert werden kann, durchlebte der Begriff „Künstliche Intelligenz" (KI) bereits viele Phasen des Auf und Abs. Im letzten Jahrzehnt gab es bei künstlichen neuronalen Netzen einen derartig rasanten Entwicklungssprung, dass darauf basierende Technologien heutzutage nahezu synonym zu KI verwendet werden.

Mit den beeindruckenden Möglichkeiten von Text- und Bildgenerierung ist KI in jüngster Zeit in den Alltag eingekehrt. Immer mehr Unternehmen nutzen KI, um Ihre Produktivität und Effizienz zu steigern. Die Möglichkeiten, Grenzen und Risiken von KI-Modellen sind ein derzeit sehr dynamisches Feld, das auch viele datenschutzrechtliche Fragen mit sich bringt.

Derartige Fragen betreffen etwa die Personenbeziehbarkeit von KI-Daten, den Umgang mit KI-spezifischen Schutzzielen wie Transparenz (z. B. Information der Betroffenen) und Verlässlichkeit (z. B. Schutz vor absichtlicher Manipulation) sowie das Durchführen von Datenschutzfolgenabschätzung bei Verarbeitungstätigkeiten, in denen KI-Technologien benutzt werden.

Um bei der rapiden Entwicklung von künstlicher Intelligenz auf dem aktuellen Stand zu bleiben, haben wir uns dazu entschieden, unser Cyberlabor um eine KI-Komponente zu erweitern. Dazu haben wir spezielle Hardware angeschafft, die es uns ermöglicht, auch die neuesten KI-Modelle wie die sogenannten „Großen Sprachmodelle" in ihren Varianten praxisnah zu untersuchen und ihre Funktionsweise zu analysieren ohne dabei auf Cloud-Dienste zurückgreifen zu müssen. Der damit verbundene Wissenserwerb bezüglich der gesamten Pipeline von KI-Modellen – vom Training bis zur Ausgabe – ermöglicht es uns, auf die anstehenden Herausforderungen der KI-Regulierung vorbereitet zu sein.

Ein KI-Modell benötigt immer Trainingsdaten von großem Umfang, aber insbesondere von sehr guter Qualität (bezüglich dem Einsatzszenario). Ein passend zum KI-Modell ausgewähltes Lernverfahren versucht, den Wesensgehalt der Trainingsdaten in ein KI-Modell zu trainieren, das damit auch bislang nicht in den Trainingsdaten enthaltene Eingaben angemessen verarbeiten können sollte. Ein öffentlich verfügbarer Datensatz, der von einigen großen Sprachmodellen als Quelle für Trainingsdaten genutzt wird, ist der Common Crawl-Datensatz. Dieser enthält mehrere Milliarden Links zu einer Vielzahl von Webseiten und Ressourcen im Internet. Eine Analyse des Datensatzes hat gezeigt, dass die enthaltenen Webseiten – insbesondere auch im deutschsprachigen Bereich – wie erwartet in erheblichen Umfang kritische Inhalte wie Falschmeldungen, abstruse Verschwörungstheorien oder rassistisch motivierte Forenposts enthalten. Um die KI-spezifischen Schutzziele zu erreichen, ist ein sorgfältiger Umgang mit den Trainingsdaten (z. B. Filterung) notwendig.

Eine weitere Herausforderung im Umgang mit künstlicher Intelligenz ist die Möglichkeit der Prüfbarkeit und Bewertung von KI-Modellen. Eine datenschutzfreundliche KI muss personenbezogene Daten fair und transparent verarbeiten. So könnte Voreingenommenheit einer KI beim Einsatz zur Entscheidungsfindung zur Diskriminierung einer betroffenen Person führen. Die Suche nach geeigneten Kennzahlen ist momentan noch aktueller Forschungsstand. In diesem Zusammenhang ist z. B. das HELM-Projekt der Stanford University zu nennen, das wir auf Tauglichkeit zur Bewertung von KI-Modellen

untersucht haben. Dieses verwendet verschiedene Datensätze und Metriken, um Eigenschaften von KI-Modellen wie Fairness, Wissen und Voreingenommenheit automatisiert zu bewerten.

Ebenfalls im Berichtszeitraum hat die Arbeit an einer umfangreichen Checkliste begonnen, die die beschriebenen Fragestellungen (sowie viele weitere) zusammenfassend aufgreift. Dabei stellen wir sowohl für das Training von KI als auch die Bewertung von Risiken sowie den konkreten Einsatz von KI einen Good-Practice-Ansatz auf, der im Sinne einer Soll-Ist-Überprüfung verwendet werden kann. Die Checkliste ist zusammen mit einem begleitenden Informationsflyer abrufbar auf www.lda.bayern.de/ki

16.2 Worldcoin auf dem Prüfstand

Das BayLDA leitete zum „Worldcoin-Projekt" eine detaillierte Prüfung ein.

Eine neue Technologie namens „Worldcoin" startete mit Einführung einer gleichlautenden Kryptowährung in 2023. Laut Anbieter soll es mit der Technologie möglich sein, dass Nutzerinnen und Nutzer die Einzigartigkeit ihrer Person nachweisen können, was insbesondere einen Schutz vor automatisierten Bots, die künstliche Intelligenz einsetzen, ermöglich soll. Dazu ist ein spezieller Registrierungsprozess notwendig, bei dem die Nutzenden an vorgegebenen Orten ihre Iris scannen müssen.

Das BayLDA prüft derzeit aufgrund der hohen Sensibilität der verarbeiteten biometrischen Daten das Vorgehen des Unternehmens und führte im Rahmen der Prüfung im Berichtszeitraum Vor-Ort-Kontrollen, die zum Standardvorgehen bei derartigen innovativen Technologien mit sehr großer Zielgruppe gehören, durch: Zum einen wurde ein Standort in Berlin besucht, an dem Nutzende sich registrieren konnten, zum anderen kontrollierte ein Team des BayLDA den Firmensitz der primär für die Entwicklung und Testung der Technologie zuständig ist.

Die Prüfung ist noch andauernd, weswegen wir für weitere Details auf den zukünftigen 14. Tätigkeitsberichts des Jahres 2024 (bzw. andere Veröffentlichungen im Jahresverlauf) verweisen. Prüfungsschwerpunkte sind neben der Frage nach der grundsätzlichen datenschutzrechtlichen Zulässigkeit unter anderem die Sicherstellung der Betroffenenrechte sowie das vorhandene Schutzniveau bei der Verarbeitung der anfallenden biometrischen Daten.

16.3 Cybersicherheitslage

Die Bedrohungslage ist unverändert hoch.

Auch 2023 hat sich der Trend der vergangenen Jahre fortgesetzt und die Gefährdungslage im Cyberbereich ist weiterhin anhaltend hoch. Dies zeigt sich beim BayLDA vor allem an der konstant hohen Zahl von Meldungen von Datenschutzverletzungen gemäß Art. 33 DS-GVO, die sich dem Bereich „Cyberangriff" im Allgemeinen und dem Bereich „Schadsoftware" bzw. „Ransomware" im Besonderen zuordnen lassen. Insgesamt sind in diesem Zeitraum 926 Meldungen eingegangen, die in Verbindung mit Cybercrime jeglicher Art stehen.

Im Hinblick auf Cyberangriffe allgemein konnte im vergangenen Jahr eine Vielzahl von Angriffen verzeichnet werden, bei denen sich Angreifer über einen E-Mail-Account Zugriff auf Firmennetzwerke verschafft haben. Häufig gelang dies über Phishing-E-Mails und führte in der Konsequenz oft dazu, dass von den entsprechenden Accounts weitere Phishing-E-Mails verschickt wurden.

2023 konnte außerdem beobachtet werden, dass immer mehr Schwachstellen in Softwareprodukten von Angreifern ausgenutzt wurden. Diese Schwachstellen sind entweder von den Software-Anbietern nicht schnell genug geschlossen worden oder die verantwortlichen Unternehmen konnten Sicherheitsupdates aufgrund eines schlechten Patch-Managements

nicht schnell genug einspielen und öffneten so die Tür für die Angreifer.

Besonders große Auswirkungen hatten diese Angriffe vor allem dann, wenn sie die Supply Chain ins Visier nahmen. Hier seien beispielhaft die Ausnutzung von Schwachstellen bei einer weit verbreiteten File-Sharing-Software oder aber auch bei Finanzdienstleistern und Versicherungsplattformen genannt.

Auch bei den Ransomware-Angriffen setzte sich ein Trend der vorherigen Jahre weiter fort: Neben der Verschlüsselung der Daten ist aus datenschutzrechtlicher Sicht besonders schwerwiegend zu bewerten, dass die Daten in aller Regel vor der Verschlüsselung von den Angreifern abgegriffen werden. Dabei handelt es sich um eine sogenannte Double Extortion. Dies bietet den Angreifern eben nicht nur die Möglichkeit, ein Lösegeld für die Wiederherstellung der Daten zu verlangen, sondern auch damit zu drohen, Daten zu veröffentlichen, wenn kein Lösegeld gezahlt wird. Diese drohende – und oft auch tatsächlich stattfindende – Veröffentlichung erhöht natürlich das Risiko für die betroffenen Personen und das vor allem dann, wenn es sich um sensible Daten wie beispielsweise umfangreiche Daten aus der Personalabteilung handelt.

Von den vielen Gruppierungen, die sich Angriffe mit Ransomware zum Geschäftsmodell gemacht hatten, dominierten dabei im Jahr 2023 u. a. Black Basta, LockBit 3.0, Alphv/BlackCat und Royal.

Festgehalten werden kann außerdem, dass die Angreifer bayerische Verantwortliche aus allen Branchen und in allen Größen ins Visier genommen haben – vom kleinen Verein und der Arztpraxis über Handwerksbetriebe bis zum Großkonzern. Daraus ergeben sich natürlich in der Konsequenz ganz unterschiedliche Zahlen an Betroffenen. Diese Zahl kann von einer niedrigen zweistelligen Zahl bis zu einer Zahl in Millionenhöhe reichen.

17

Datenschutzkontrollen

17 Datenschutzkontrollen

17.1 Prüfung zur Schwellwertanalyse bezüglich der Datenschutzfolgenabschätzung

Ende des Jahres wurde eine Prüfung zum korrekten Umgang mit der Frage gestartet, wann eine Datenschutzfolgenabschätzung notwendig ist.

Das BayLDA führt flächendeckende Prüfungen zu verschiedenen Schwerpunktthemen durch, beispielsweise um grundlegende Sicherheitslücken oder organisatorische Defizite aufzuzeigen und Verantwortliche somit auf den Bedarf an durchzuführenden Maßnahmen hinzuweisen. Im Berichtszeitraum hat das BayLDA bei über 50 zufällig ausgesuchten datengetriebenen und innovativen Unternehmen eine Datenschutzprüfung gestartet, um den korrekten Umgang mit der Frage zur Notwendigkeit einer Datenschutzfolgenabschätzung zu untersuchen.

Die Datenschutzgrundverordnung hat mit der Datenschutzfolgenabschätzung ein neues Instrument zum Umgang mit Hochrisikoverarbeitungen personenbezogener Daten eingeführt. Diese ist nach Art. 35 Abs. 1 DS-GVO dann durchzuführen, wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Damit besteht eine Datenschutzfolgenabschätzung bei Blick auf eine Verarbeitung nach Art. 30 Abs. 1 DS-GVO (Verzeichnis der Verarbeitungstätigkeiten) aus zwei Schritten: Zunächst muss für jeden Eintrag des Verzeichnisses der Verarbeitungstätigkeiten geprüft werden, ob für diesen eine Datenschutzfolgenabschätzung durchgeführt werden muss; dies nennt sich Schwellwertanalyse. Hat diese ein voraussichtlich hohes Risiko ergeben, so muss im zweiten Schritt eine Datenschutzfolgenabschätzung durchgeführt werden.

Die Schwellwertanalyse ergibt dabei unter anderem dann eine Pflicht zur Datenschutzfolgenabschätzung, wenn die Einträge aus dem Verzeichnis in gewisse Verarbeitungskategorien fallen, die in Art. 35 Abs. 3 DS-GVO oder der sogenannten Muss-Liste der Datenschutzkonferenz festgelegt sind. Eine derartige Verarbeitungskategorie ist zum Beispiel der Einsatz von künstlicher Intelligenz zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen.

Die geprüften Unternehmen wurden aufgefordert, dem BayLDA diejenigen Einträge des Verzeichnisses der Verarbeitungstätigkeiten zu übermitteln, bei denen die Schwellwertanalyse wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen ergeben hat. Zusätzlich mussten die Unternehmen die übermittelten Einträge daraufhin überprüfen, ob sie in gewisse vom BayLDA vorgegebene Verarbeitungskategorien fallen.

Die bis zum Ende des Berichtszeitraum eingegangen Antworten erlaubten eine Erstsichtung, die zeigt, dass ein großer Teil der geprüften Unternehmen gut mit der Thematik vertraut ist, bei manchen Unternehmen warfen die Antworten jedoch Fragen auf, denen im Jahr 2024 nachgegangen werden wird. Eine detaillierte Auswertung der Antworten wird zu Beginn des Jahres 2024 erfolgen.

17.2 Europaweite Prüfung zu Stellung und Aufgaben von Datenschutzbeauftragten

Mit seiner ersten Beteiligung an einer europaweiten Datenschutzprüfung befasst sich das BayLDA mit der Stellung und den

Aufgaben der Datenschutzbeauftragten in bayerischen Unternehmen.

Das BayLDA hat sich seit März 2023 mit förmlichen Prüfungen bei mehr als 30 bayerischen Unternehmen an der zweiten durch den Europäischen Datenschutzausschuss koordinierten gemeinsamen Prüfaktion beteiligt. Europaweit wurden im Rahmen der koordinierten Prüfung und Befragung bei Organisationen und Datenschutzbeauftragten (sowohl öffentlicher als auch privater Einrichtungen) mehr als 17.000 Einzelfragen beantwortet und analysiert. Die in einem im Januar 2024 veröffentlichten Prüfbericht zusammengefassten Daten vermitteln fünf Jahre nach Inkrafttreten der DSGVO wertvolle Einblicke in das Profil, die Position und die Arbeit der Datenschutzbeauftragten. Sie stehen auch für weiterführende Forschungsarbeiten und Auswertungen zur Verfügung.

In das Prüfverfahren wurden unter den mehr als 36.000 dem BayLDA gemeldeten Datenschutzbeauftragten für die bayerische Wirtschaft repräsentative Unternehmen unterschiedlicher Branchen und Organisationsformen aufgenommen, um so zu einem möglichst breit gefächerten europäischen Gesamtbild beizutragen.

In der deutlichen Mehrzahl der Prüfungen ergaben sich Befunde, die zur Ausräumung möglicher Verstöße Nachfragen erforderlich machten. Schwerpunkt dieser zum Ende des Berichtszeitraums noch nicht abgeschlossenen Anschlussprüfungen waren die Angemessenheit der für die Datenschutzbeauftragten verfügbaren Ressourcen, ihnen zugewiesene Zusatzfunktionen oder auch die Art und Weise, wie Datenschutzbeauftragte der obersten Führungsebene Bericht erstatten können.

Die Prüfungsergebnisse haben gezeigt, dass auch ohne feste Regelsätze für die Beurteilung der Ressourcenausstattung von Datenschutzbeauftragten gem. Art. 38 Abs. 2 DS-GVO zumindest im Rahmen einer Einzelfallbetrachtung belastbare Beurteilungen zu erreichen sind. So gibt z. B. das wiederholte Fehlen von Berichten über eigeninitiative Überwachungsmaßnahmen des Datenschutzbeauftragten nach unserem Verständnis Anlass näher zu überprüfen, ob die für die Tätigkeit als Datenschutzbeauftragter zur Verfügung stehenden Arbeitszeitanteile und Unterstützungskräfte ausreichen.

Für die Prüfung von Interessenkonflikten bestehen auf Grundlage der neueren Rechtsprechung des EuGH und des Bundesarbeitsgerichts zu Betriebsratsvorsitzenden als Datenschutzbeauftragten klare Maßstäbe, ob Verantwortliche mit der Übertragung von Zusatzaufgaben für Datenschutzbeauftragte strukturelle Interessenkonflikte in Kauf nehmen. Solche Konfliktpunkte zeigen sich nach unseren Befunden insbesondere bei Aufgaben aus anderen Compliance-Funktionen oder auch dann, wenn externe Datenschutzbeauftragte zugleich für eigene Auftragsverarbeiter des Verantwortlichen tätig sind.

Wiederholt haben erste Prüfergebnisse schon auf Grund des Organigramms erkennen lassen, dass für den betrieblichen Datenschutzbeauftragten aufgrund seiner organisatorischen Verortung Hindernisse bestehen können, im Einklang mit Art. 38 Abs. 3 Satz 3 DS-GVO einen direkten, anlasslosen Informationsaustausch mit der obersten Führungsebene zu etablieren. Auch wenn die DS-GVO insoweit sicherlich Gestaltungsspielraum für unterschiedliche Organisationsmodelle lässt, werden die weitere Prüfschritte ergänzend zu den Organigrammen vor allem unternehmensinterne Regelwerke zur Datenschutzorganisation aber auch die tatsächliche Umsetzungspraxis im Einzelfall in Blick nehmen. Je mehr Berichtslinien durch verschiedene organisatorische und disziplinarische Ebenen unterbrochen werden, desto mehr werden klare Festlegungen über voraussetzungs- und anlasslose Austauschformate mit der höchsten Managementebene erforderlich, um eine effektive und zugleich benachteiligungsfreie Wahrnehmung der Aufgaben des Datenschutzbeauftragten abzusichern.

Die aus der gemeinsamen Prüfaktion gewonnen Erkenntnisse sollen sowohl auf europäischer Ebene durch eine Überarbeitung der EDSA-„Leitlinien in Bezug auf Datenschutzbeauftragte" als auch durch die Fortentwicklung der Handreichungen des BayLDA für die Datenschutzpraxis nutzbar gemacht werden.

18

Bußgeldverfahren

18 Bußgeldverfahren

18.1 Bericht aus der Zentralen Bußgeldstelle

Höchste Zahl an verhängten Bußgeldern seit Geltungsbeginn der DS-GVO.

Die aufgrund verschiedener personeller Ausfälle im Jahr 2022 angefallenen Rückstände konnten zwischenzeitlich aufgearbeitet und die Zentrale Bußgeldstelle des Bayerischen Landesamts für Datenschutzaufsicht wieder wie bewährt tätig werden. Ein Großteil der von der Zentralen Bußgeldstelle im Berichtszeitraum bearbeiteten Fälle ging auf Ordnungswidrigkeitenanzeigen der Polizei zurück, jedoch konnte im Vergleich zum Vorjahr auch eine weitere Steigerung von Fällen, die aus dem aufsichtlichen Bereich abgegeben wurden, festgestellt werden.

Im Berichtszeitraum wurden Bußgelder gegen Unternehmen und Privatpersonen in einer Höhe von insgesamt ca. 3,8 Millionen Euro festgesetzt. Die Spanne reicht dabei von Bußgeldern in dreistelliger Höhe gegen Privatpersonen bis zu siebenstelligen Geldbußen gegen Unternehmen. Insgesamt wurde im Jahr 2023 die höchste Zahl an Bußgeldern seit Geltungsbeginn der DS-GVO verhängt, wobei noch nicht alle Entscheidungen bis zum Redaktionsschluss rechtskräftig wurden.

Mit Bußgeld geahndet wurden im Jahr 2023 Verstöße gegen Art. 5, 6, 9 und 32 DS-GVO, im Wesentlichen solche gegen Art. 5 Abs. 1 Buchstabe a i. V. m. Art. 6 DS-GVO, weil schon keine Rechtsgrundlage für die Datenverarbeitung gegeben war.

Einer dieser Fälle betraf eine Videoüberwachung durch eine Wildkamera, die von einem Badegast in einem Gebüsch an einem FKK-Badebereich eines Badesees versteckt angebracht wurde. Die Kamera fertigte nicht nur Videoaufnahmen der Badegäste an, die sich auf der Liegewiese aufhielten, sondern auch Tonaufnahmen. Die zuständige Staatsanwaltschaft stellte das Ermittlungsverfahren ein, so dass wegen dieses Sachverhalts ein Bußgeld nach der DS-GVO verhängt werden konnte.

Ein weiteres Bußgeld wurde gegen eine Privatperson verhängt, die einer Verkehrskontrolle durch einen Polizeibeamten unterzogen wurde und anschließend dessen private Handynummer ausfindig machte und zur Kontaktaufnahme mit dem Polizeibeamten nutzte. Da der Betroffene bei den polizeilichen Maßnahmen erheblichen Widerstand leistete und den Polizeibeamten nicht nur mehrfach beleidigte und bedrohte, sondern auch Verletzungen zuführte, fühlte sich dieser durch die Kontaktaufnahme ernsthaft in Gefahr, zumal das Erlangen der Handynummer enormen Zeit- und Recherche-raufwand erforderlich gemacht haben musste.

Häufig erreicht das Bayerische Landesamt für Datenschutzaufsicht Beschwerden oder Anzeigen von Privatpersonen, weil deren Telefon- oder Mobilnummer von Mitarbeitern zweckwidrig Datenbanken ihres Arbeitgebers, beispielsweise Kundendatenbanken, entnommen und zur privaten Kontaktaufnahme genutzt wurde. In zwei dieser Fälle wurde im Berichtszeitraum gegen den Mitarbeiter ein Bußgeldbescheid erlassen. Ein Fall betraf einen Ladendetektiv, der die Kontaktdaten einer Frau, der ein Ladendiebstahl vorgeworfen wurde, zunächst in seiner beruflichen Eigenschaft erhob und anschließend zur privaten Kontaktaufnahme nutzte. In einem weiteren Fall wurde die betroffene Frau von einem Mitarbeiter eines Fachmarktes, bei dem diese Kundin war und deshalb deren Mobilnummer hinterlegt war, unter Zusendung pornographischer Bilder kontaktiert.

Ein Bußgeld in einer vierstelligen Höhe wurde gegen einen Arzt verhängt, der auf die Rezen-

sion eines Patienten im Internet, unter Offenlegung von Gesundheitsdaten des Patienten antwortete, wobei die Antwort, ebenso wie die Rezension selbst, offen und für jedermann einsehbar im Internet veröffentlicht wurde. Auch hier stellte die zuständige Staatsanwaltschaft das Verfahren ein, so dass eine Verfolgung und Ahndung durch das Bayerische Landesamt für Datenschutzaufsicht möglich war.

Erstmalig wurde im Berichtszeitraum auch die Nutzung eines Ortungsgerätes, konkret eines Apple AirTags, mit Bußgeld sanktioniert. In dem zugrunde liegenden Fall brachte der Betroffene das AirTag an dem Fahrzeug der Geschädigten an, um ihre Standortdaten abzurufen, weil er auf diese ein Auge geworfen hatte. Die Haushaltsausnahme sahen wir in diesem Fall aus mehreren Gründen nicht erfüllt und verhängten aufgrund der hohen Eingriffsintensität und der Sensibilität der Daten ein vierstelliges Bußgeld gegen den Betroffenen.

Diese beispielhaft ausgeführten Fälle zeigen, dass es auch durch Privatpersonen zum Teil zu massiven Grundrechtseingriffen kommt, die nicht sanktionslos bleiben können und auch weiterhin konsequent mit Geldbuße geahndet werden.

Im Dezember 2023 fällte der Europäische Gerichtshof zwei für die Sanktionspraxis wegweisende Entscheidungen: Zum einen die Entscheidung in der Rechtssache C-807/21 („Deutsche Wohnen"), zum anderen die in der Rechtssache C-683/21, die auf eine Vorlage eines litauischen Gerichtes zurückgeht. Der EuGH stellte in diesen Entscheidungen klar, dass Adressat einer Geldbuße nach der DS-GVO der Verantwortlichen ist, unabhängig davon, ob es sich bei diesem um eine natürliche oder juristische Person oder eine andere in Art. 4 Nr. 7 DS-GVO genannte Stelle handelt. Für die Verhängung von Geldbußen gegen eine juristische Person ist demnach weder eine Handlung noch eine Kenntnis des Leitungsorgans erforderlich. Vielmehr haftet eine juristische Person sowohl für Verstöße, die von ihren Vertretern, Leitern oder Geschäftsführern begangen wurden, als auch für Verstöße, die von jeder anderen Person begangen wurde, die im Rahmen der unternehmerischen Tätigkeit und im Namen der juristischen Person handelt. Auch dürfe die Verhängung einer Geldbuße gegen eine juristische Person nicht davon abhängig gemacht werden, dass zuvor festgestellt wurde, dass der Verstoß von einer identifizierten natürlichen Person begangen wurde. Nach der Entscheidung des EuGH in der C-683/21 kann gegen einen Verantwortlichen eine Geldbuße auch für Verarbeitungsvorgänge verhängt werden, die von einem Auftragsverarbeiter in seinem Namen durchgeführt wurden, es sei denn, der Auftragsverarbeiter hat im Rahmen dieser Verarbeitungsvorgänge Verarbeitungen für eigene Zwecke vorgenommen oder diese Daten auf eine Weise verarbeitet, die nicht mit dem Rahmen oder den Modalitäten der Verarbeitung, wie sie vom Verantwortlichen festgelegt wurden, vereinbar ist, oder auf eine Weise, bei der vernünftigerweise nicht davon ausgegangen werden kann, dass der Verantwortliche ihr zugestimmt hätte. Die Verhängung einer Geldbuße wegen Verstoßes gegen die DS-GVO sei jedoch, wie der EuGH in beiden Verfahren klargestellt hat, nur dann möglich, wenn der Verstoß schuldhaft, d. h. vorsätzlich oder fahrlässig begangen wurde. Dies sei der Fall, wenn sich der Verantwortliche über die Rechtswidrigkeit seines Verhaltens nicht im Unklaren sein konnte, gleichviel, ob ihm dabei bewusst war, dass es gegen die Bestimmungen der DS-GVO verstößt. Gehört der Adressat einer Geldbuße zu einem Konzern, bemisst sich die Geldbuße, wie der EuGH nun ebenfalls klargestellt hat, nach dem Jahresumsatz des Konzerns im vorangegangenen Geschäftsjahr.

Die Entscheidungen des Europäischen Gerichtshofs haben in wesentlichen Punkten für Klarheit gesorgt und erleichtern den Datenschutzaufsichtsbehörden die Verhängung von Bußgeldern gegen Verantwortliche, die keine natürliche Personen sind. Das BayLDA wird vor dem

Hintergrund dieser Entscheidungen und der damit gewonnenen Rechtssicherheit bußgeldwürdige Verstöße von Unternehmen weiterhin konsequent mit Bußgeldern sanktionieren.

Abschließend ist erneut die gute Kooperation mit den Staatsanwaltschaften und die gute Zusammenarbeit mit den Polizeibehörden, die die Zentrale Bußgeldstelle im Berichtszeitraum wieder mehrfach unterstützten, hervorzuheben.

Stichwortverzeichnis

N

O

P

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